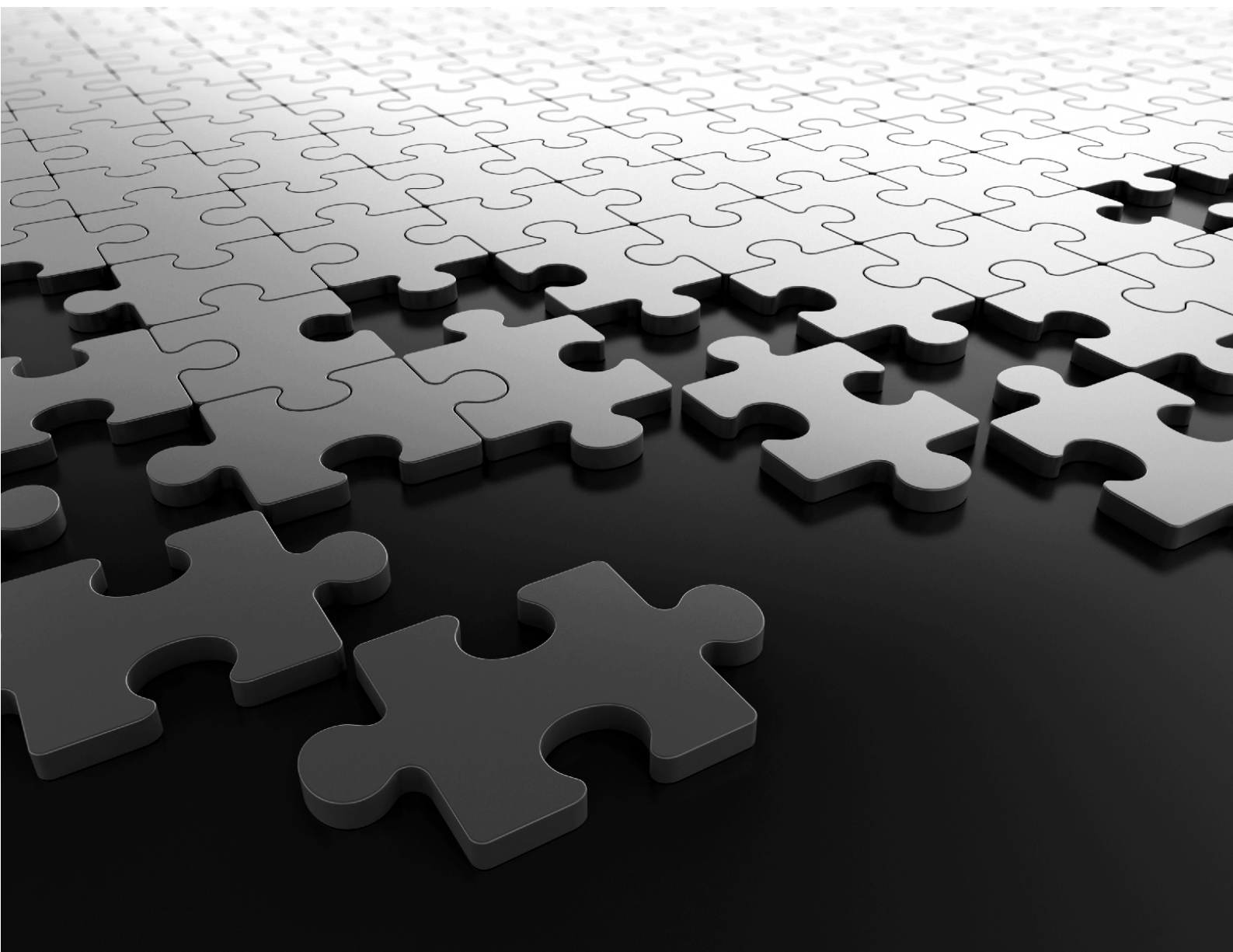


**SETU VTEP
System Manual**



SETU VTEP
An Out-n-Out 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 1

Release date: November 17, 2016



Contents

Introduction	1
Welcome	1
About this System Manual	1
Know Your SETU VTEP	5
Overview of SETU VTEP	5
Applications	6
Installing SETU VTEP	7
Getting Started	7
Protecting SETU VTEP and Yourself	7
Connecting SETU VTEP	9
Accessing Jeeves	17
Basic Settings	21
Region	24
Network Parameters	28
SIP Trunks	33
E1 Port	72
T1 Port	114
Login Password	148
Date-Time Settings	150
Advanced Settings	155
System Parameters	155
Number Lists	165
Automatic Number Translation (ANT)	169
Destination Number Determination	173
Destination Port Determination	180
Group	185
Peer-to-Peer Dialing	188
PIN Authentication	193
Digest Authentication	195
Static Routing	197
Access Codes	200
Emergency Numbers	201
Certificate Manager	204
Call Detail Record	213

Features	221
<i>Making a New Call using Access Code</i>	<i>221</i>
<i>Disconnecting a Call using Access Code</i>	<i>221</i>
<i>IP Dialing</i>	<i>222</i>
<i>Knowing Network Information using Access Codes</i>	<i>222</i>
Maintenance	223
<i>Firmware Upgrade</i>	<i>223</i>
<i>Configuration Upgrade</i>	<i>229</i>
<i>System Debug</i>	<i>235</i>
<i>Simple Network Management Protocol (SNMP)</i>	<i>239</i>
<i>System Port Activity</i>	<i>245</i>
<i>PCAP Trace</i>	<i>247</i>
<i>Manual Call Test</i>	<i>249</i>
<i>Default SETU VTEP</i>	<i>250</i>
<i>Soft Restart</i>	<i>252</i>
<i>T1E1 Port Alarms and Performance Monitoring</i>	<i>253</i>
<i>TR-069</i>	<i>257</i>
Status	259
<i>System Details</i>	<i>259</i>
<i>Firmware</i>	<i>260</i>
<i>Configuration</i>	<i>262</i>
<i>Network Status</i>	<i>263</i>
<i>SIP Trunk</i>	<i>265</i>
<i>T1E1 Port</i>	<i>267</i>
Appendix	269
<i>Acronyms</i>	<i>269</i>
<i>Default Region Table</i>	<i>271</i>
<i>Call Progress Tones</i>	<i>274</i>
<i>Product Specifications</i>	<i>280</i>
<i>System Commands</i>	<i>283</i>
<i>Warranty Statement</i>	<i>284</i>
<i>Disposal of Products/Components after End-Of-Life</i>	<i>285</i>
<i>Regulatory Information</i>	<i>286</i>
<i>Open Source Licensing Terms and Condition</i>	<i>288</i>
Index	301

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. For instructions on quick installation of this product, you may refer the *SETU VTEP Quick Start* shipped with the system.

The documentation can be found at <http://www.matrixtelesol.com/technical-document.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.

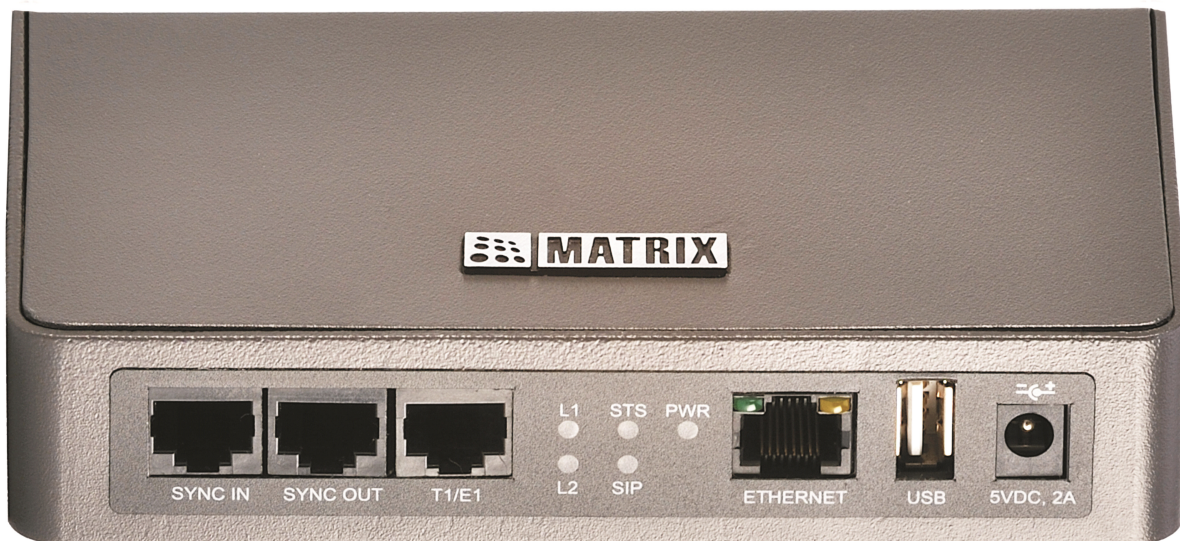
Term	Usage in the document
Caller / Calling party	The person who make calls to SETU VTEP.
Callee / Called party	The person to whom calls are made by SETU VTEP user.
Source / Originating Port	A port from which a call originates.
Destination / Terminating Port	A port on which a call terminates.
Ethernet 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

- Access Codes
- Allowed and Denied Numbers
- Automatic Number Translation
- Call Detail Records (CDR)
- Call Progress Tone
- Daylight Saving Mode
- Digest Authentication
- Dynamic DNS
- Emergency Number Dialing

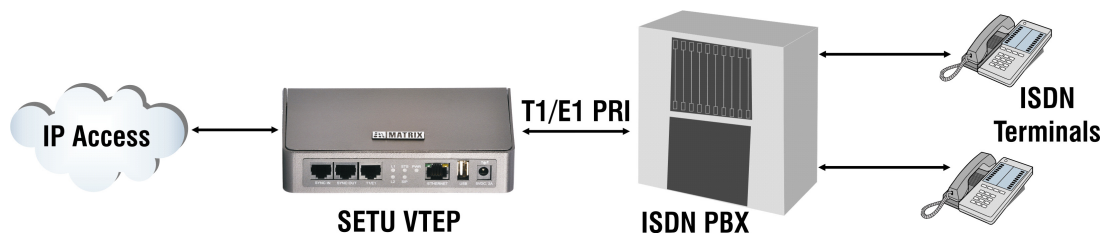
- Fax over IP
- Least Cost Routing
- NAT and STUN Support
- PCAP Trace
- Peer-to-Peer Calling
- Return Call to Original Caller
- VLAN Tagging
- Web based Programming

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

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.

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. See [“Disposal of Products/Components after End-Of-Life”](#).

Connecting SETU VTEP

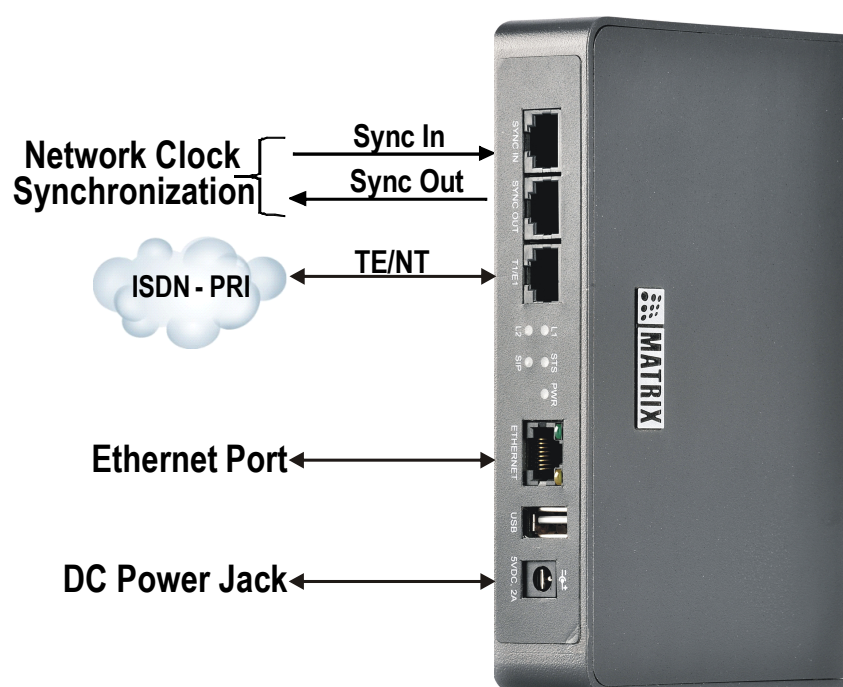
Before installing the SETU VTEP, verify the package contents as given below:

Package Contents

Sr. No.	Item Name	Quantity
01	SETU VTEP unit	1
02	Power Adapter	1
03	Screw M7/30	2
04	Screw Grips	2
05	Ethernet Straight Cable	1
06	PRI Cross Cable	1
07	Wall Mounting Template	1
08	Warranty Card Set	1
09	SETU VTEP Quick Start (printed copy)	1
10	19 inch Rack Mounting Clamp	2

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

SETU VTEP has 32 SIP Trunks, 1 T1/E1 Port, 1 Ethernet Port, SYNC IN Port, SYNC OUT Port, a Power Adapter and LEDs.



- Place the system at the selected site.
- If you are mounting the system on a wall, you may refer to the mechanical dimensions of the product and use the mounting template for drilling holes on the wall.
- Connect the system, refer to the diagram above.

Connecting SETU VTEP to the VoIP Network

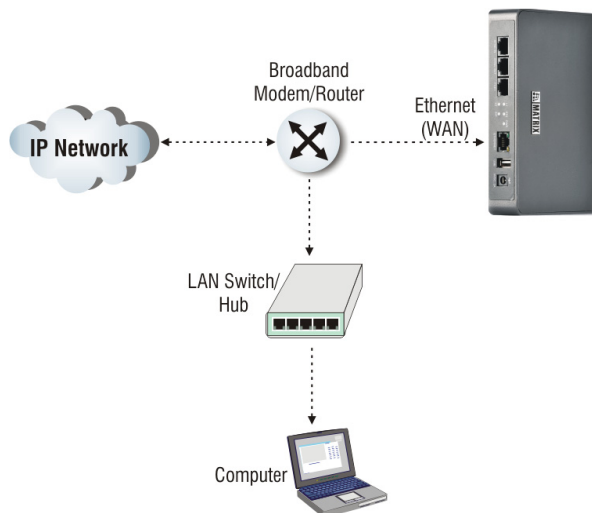


Before you connect the system to WAN, we recommend that you first connect a computer to the Ethernet Port of SETU VTEP, configure the Basic Settings, and then connect to WAN.

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

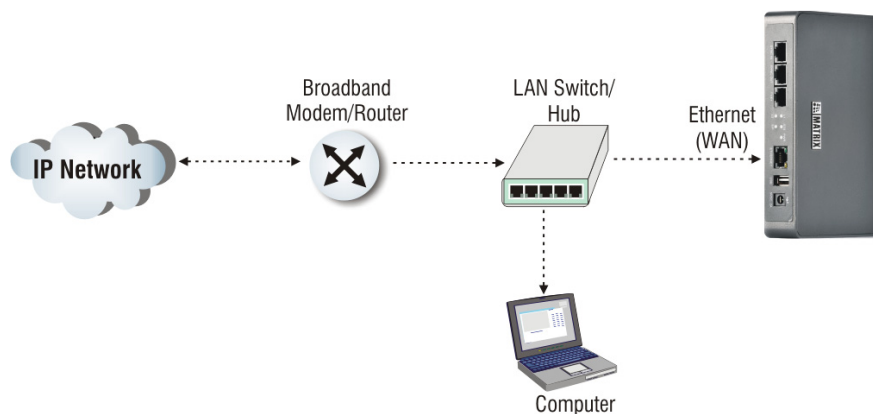
If connecting to the Public IP Network,

- Plug one end of the Ethernet cable into the Ethernet Port of SETU VTEP and the other end into the Broadband Router/Modem.



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

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



Connecting SETU VTEP to the ISDN PRI Network

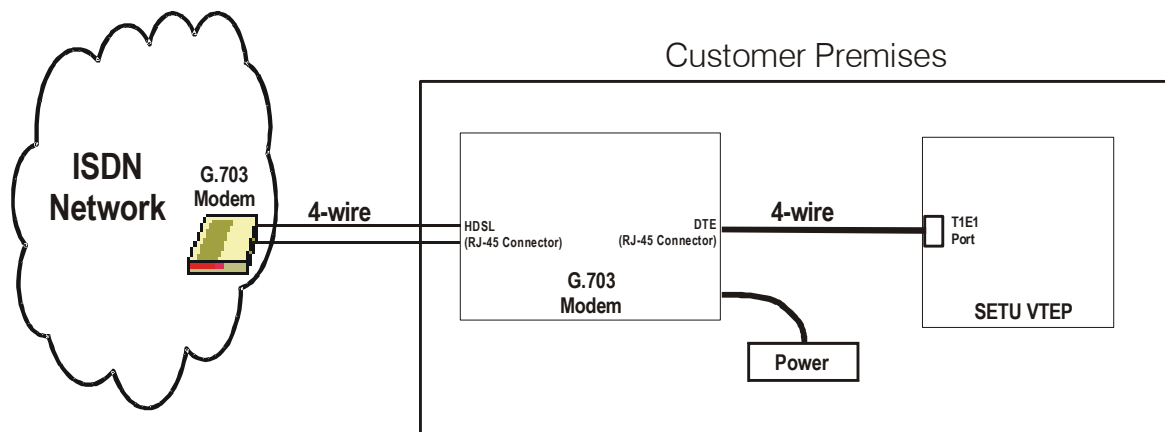
On T1 carrier lines, the system supports the following signaling types:

- 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 HDLSL 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 HDLSL Interface of the G.703 Modem. (HDLSL Network Termination Unit)

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

Pin Number	Pin Details
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 SYNC Ports

The SYNC IN and SYNC OUT ports of SETU VTEP are used for synchronizing the system's clock with that of the Public ISDN Network, to prevent possible clock slips that affect voice quality.

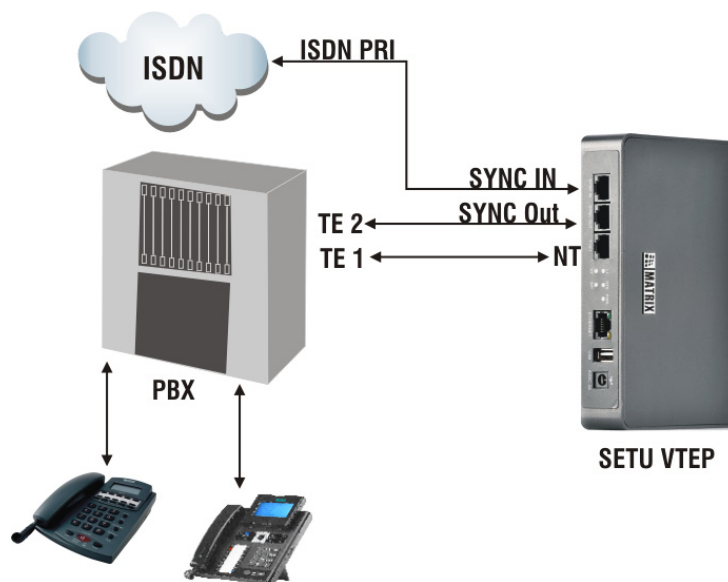
Clock synchronization becomes necessary when the T1/E1 Port is in NT mode and no direct T1/E1 line from the Public ISDN Network is terminated in the SETU VTEP.

Consider the following installation scenario:

- SETU VTEP is integrated with a PBX.
- The T1E1-NT Port of SETU VTEP is connected to a T1E1-TE Port of the PBX
- The T1E1 line from the Public ISDN Network terminates on one T1E1-TE port of the PBX.
- No T1E1 Line from the Public ISDN Network is terminated on the SETU VTEP.

In such an installation scenario, you can prevent clock slips, using the SYNC IN and SYNC OUT ports of SETU VTEP. The SYNC IN and SYNC OUT ports allow SETU VTEP to use the (higher accuracy) Network clock of the Public ISDN Network through the T1/E1 Line terminating on the PBX.

The following figure shows how the SYNC IN and SYNC OUT ports are connected for Network Clock synchronization.



The T1/E1 Line from the Public ISDN Network is connected to the SYNC IN port of SETU VTEP and the same line emerges from SYNC OUT port and terminates on the T1/E1-TE port of the PBX.

Connecting the Power Supply

- Power on the SETU VTEP by connecting the 5V 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.
- All the LEDs of the system are turned on.

Interpreting LEDs

The functioning of the LEDs of the system and their meaning are summarized below.

LED status during Reset Sequence

System Status	Color	L1	L2	STS	Time in msec
Application Load	Green	On	Off	On	200ms
All Init Done, System goes live	Green	On	On	On	1000ms
	Red	On	On	On	1000ms
		Off	Off	Off	1000ms
	Green	Off	On	Off	1000ms
		Off	Off	Off	1000ms (Continuous Last 2 steps)

SIP Trunk - LED Indication

Event/State/Status	Color	Cadence (1 cadence is of 4000msec)			
		ON	OFF	ON	OFF
SIP Disable		OFF			
SIP Registered (Active)	Green	Continuous			
SIP Registration Failed	Red	Continuous			
SIP Authentication Failed	Red	200	200	200	3400

T1/E1 Port - LED Indication

Signaling Type: E1- PRI

LED L1 Indication:

Status	Color	Cadence
No Alarm	GREEN	Continuous ON
CRC4 Alarm	GREEN	100ms ON-100 ms OFF
BFA Alarm	RED	500ms ON-500 ms OFF
LOS Alarm	RED	Continuous ON

LED L2 Indication:

Status	Color	Cadence
No Alarm	GREEN	Continuous ON
RAI Alarm	RED	500ms ON-500 ms OFF
AIS or LOS Alarm	RED	Continuous ON

Signaling Type: E1- CAS

LED L1 Indication:

Status	Color	Cadence
No Alarm	GREEN	Continuous ON
CRC4 Alarm	GREEN	100ms ON-100 ms OFF
MFA Alarm	RED	100ms ON-100 ms OFF
BFA Alarm	RED	500ms ON-500ms OFF
LOS Alarm	RED	Continuous ON

LED L2 Indication

Status	Color	Cadence
No Alarm	GREEN	Continuous ON
Y-Bit Alarm	GREEN	100ms ON-100 ms OFF
AIS16 Alarm	RED	100ms ON-100 ms OFF
RAI Alarm	RED	500ms ON-500ms OFF
AIS or LOS Alarm	RED	Continuous ON

Signaling Type: T1- RBS or T1- PRI

LED L1 Indication:

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

LED L2 Indication:

Status	Color	Cadence
No RAI Alarm	GREEN	Continuous ON
RAI or LOS Alarm	RED	Continuous ON

When the port is disabled, LED L1 is Red continuously and L2 is Off.

System LED Indication

System Status	LED Status	Comment
VoPP Program Down Load Fail	Red ON Continuously	VoPP Program download fail

System Status	LED Status	Comment
Gateway started successfully and NW_Up_SIP_Up_CDR_OK	Green Blinks 1000ms ON - 1000ms OFF	Gateway Started Successfully Network link is Up SIP stack is Up CDR buffer is not full
NW_Down_SIP_down_CDR_OK	Red Blinks 500ms ON - 500ms OFF 500msON - 2500ms OFF	Network link is down SIP stack is down CDR buffer is not full
NW_Up_SIP_down_CDR_OK	Green Blinks 500ms ON - 500ms OFF Red Blinks 500ms ON - 2500ms OFF	Network link is Up SIP stack is down CDR buffer is not full
NW_Down_SIP_down_CDR_Full	Red Blinks 500 ms ON - 500ms OFF 500 ms ON - 500ms OFF 500 ms ON - 1500ms OFF	Network link is down SIP stack is down CDR buffer is full
NW_Up_SIP_down_CDR_Full	Green Blinks 500 ms ON - 500ms OFF Red Blinks 500 ms ON - 500ms OFF 500 ms ON - 1500ms OFF	Network link is up SIP stack is up CDR buffer is full
NW_Up_SIP_Up_CDR_Full	Green Blinks 500 ms ON - 500ms OFF 500 ms ON - 500ms OFF Red Blinks 500 ms ON - 1500ms OFF	Network link is up SIP stack is up CDR buffer is full

Accessing Jeeves

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

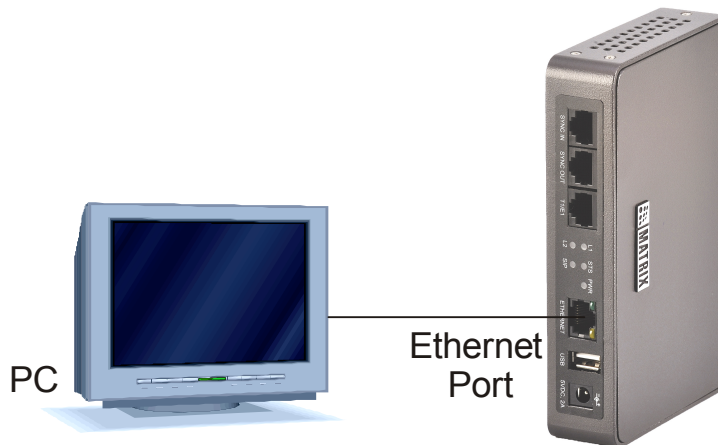
To access Jeeves, you will need to connect a computer to SETU VTEP.

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 Ethernet 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 Ethernet Port of SETU VTEP do not conflict, and that both are in the same Subnet.

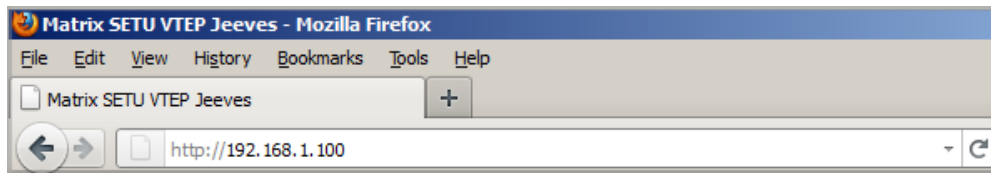
The default IP Address of the Ethernet Port of SETU VTEP is: **192.168.1.100**

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

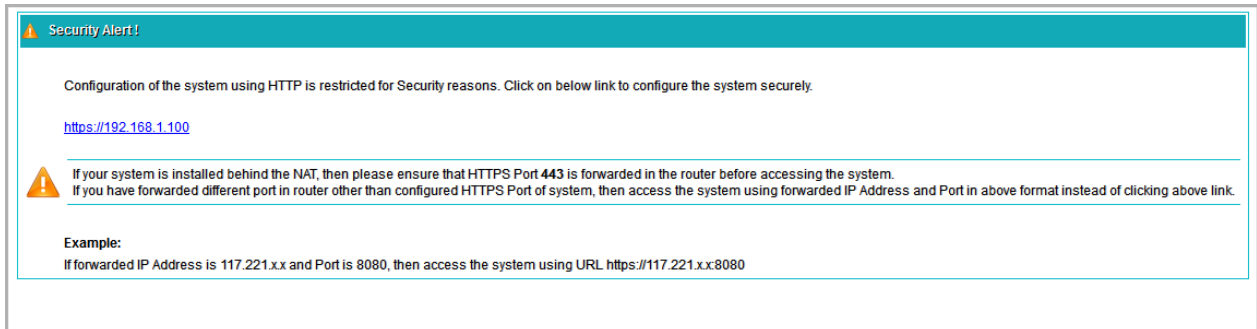
Change the Subnet of the computer, if necessary.

- 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.

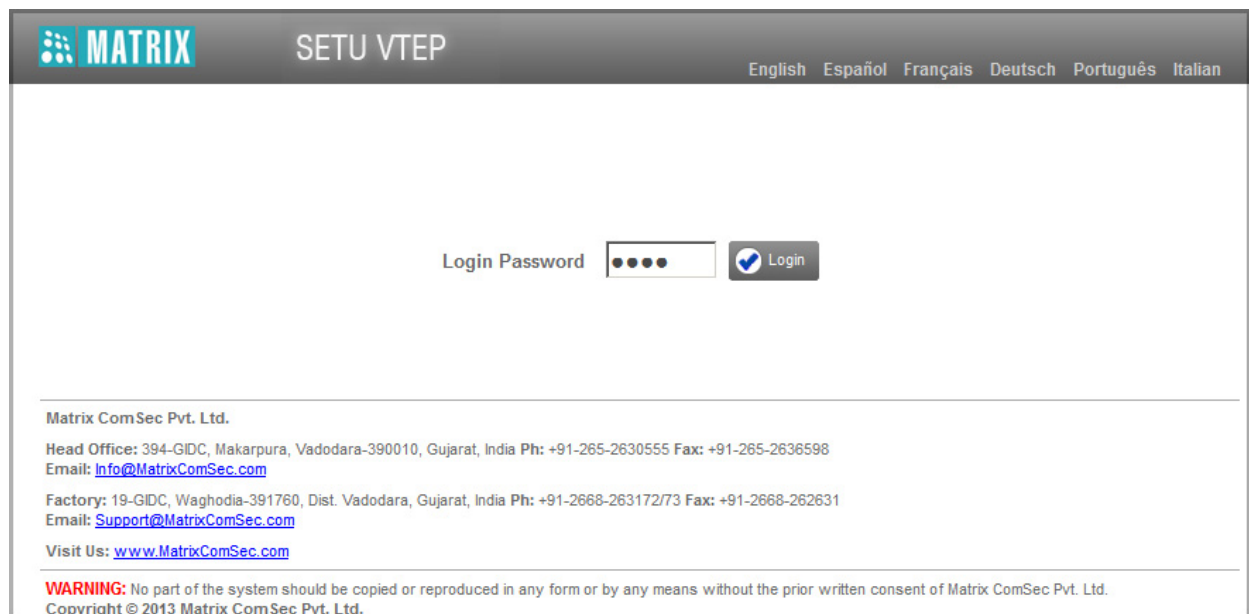
- Enter the default IP address **192.168.1.100** of the Ethernet Port of SETU VTEP in the address bar of the browser.



- You will be redirected to the HTTPS protocol for security reasons.



- Click the <https://192.168.1.100> link.
- The **Login** page will open.
- In **Login Password**, enter **1234**, the default SE Password.
- Click the **Login** button.



- 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.

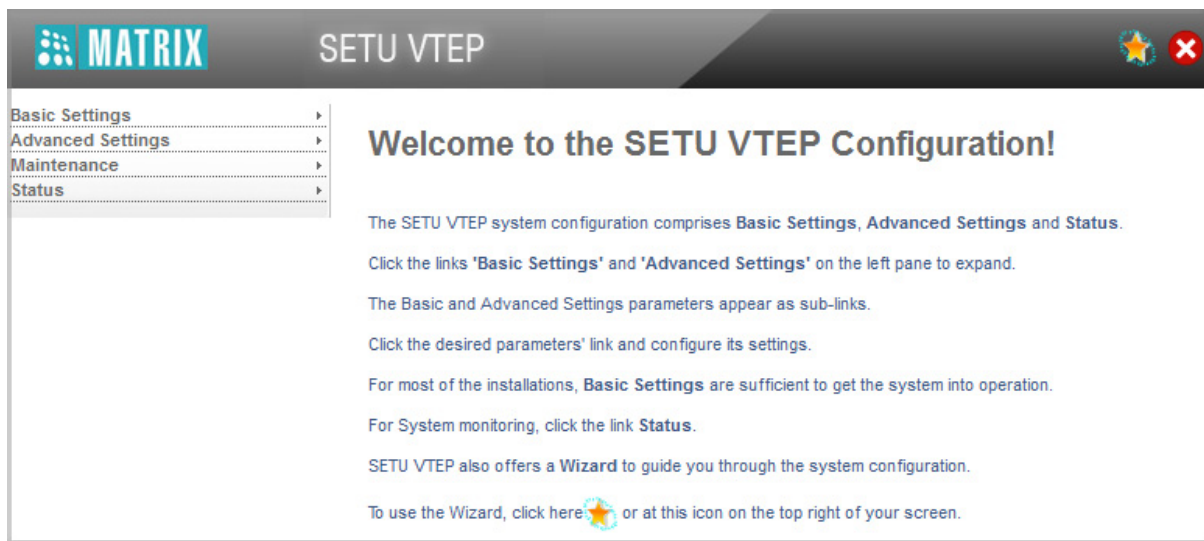


As this password is meant for restricting access to the SE mode, we strongly recommend you to:

- *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 enable you to configure SETU VTEP for basic functions. As Basic Settings cover much of your configuration requirements, you will be able to operate and use the system efficiently, when you configure Basic Settings.

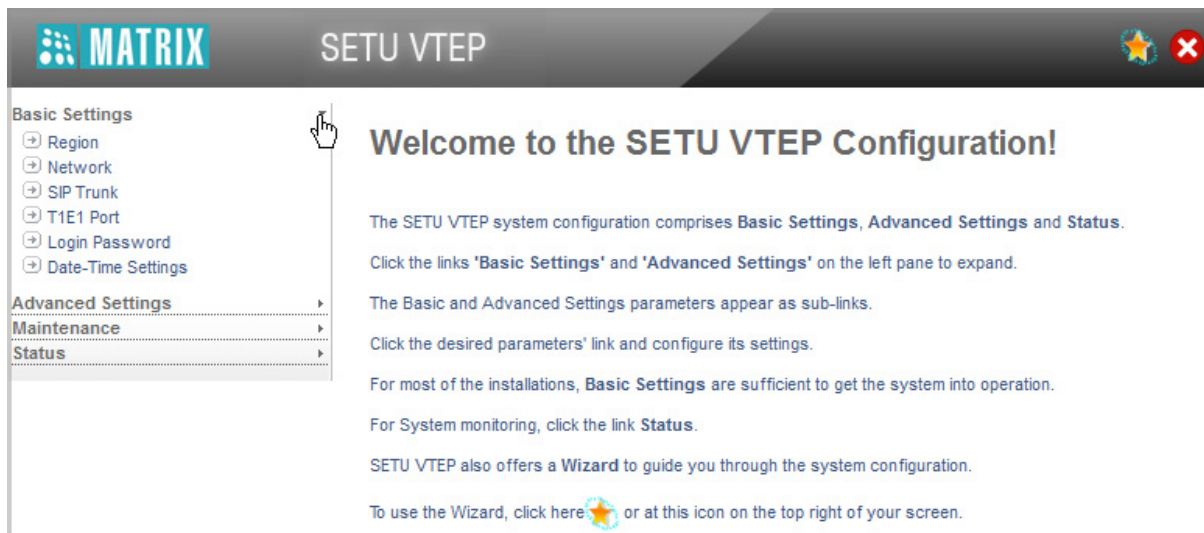
There are two ways to do the basic system configuration using Jeeves:


- using the Wizard.
- Or
- through Selective Configuration of basic settings.

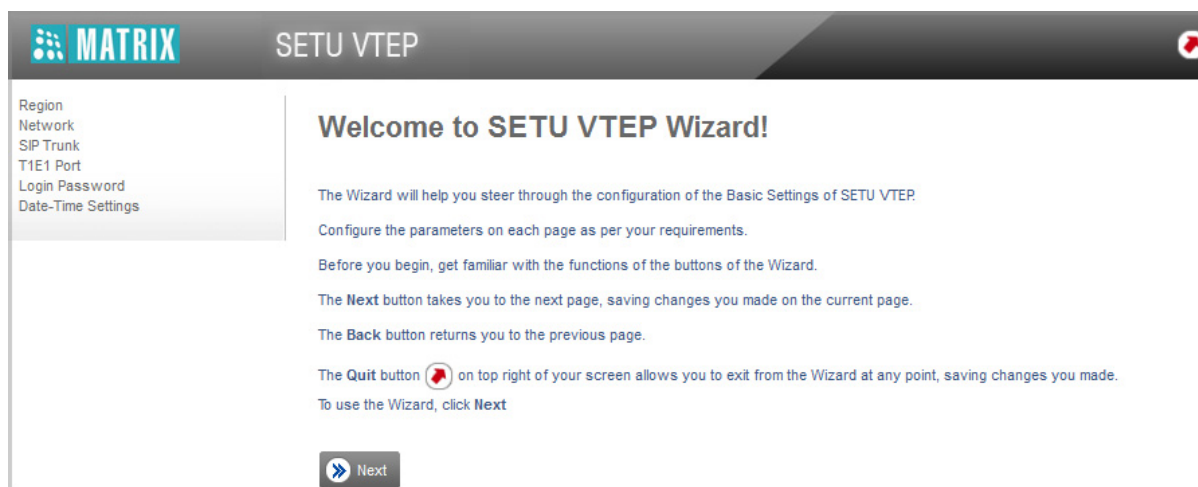
To configure Basic Settings,





- Click the **Basic Settings** link.

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






- Click the Wizard  icon on the top right of your screen. Wizard screen will appear.



- The **Next** button takes you to the next page, saving the changes you made on the current page.
- The **Back** button returns you to the previous page.
- Click  **Expand**, to expand a link to display all parameters under the link.
- Click  **Collapse**, to collapse a link. Hides all parameters under the link.
- Click  **Settings**, to configure / edit the settings of a parameter further or to edit an entry or record.
- The **Default** button assigns factory set values to all the parameters on the page.
- The **Add** button allows you to add a new record.
- The **Delete** button allows you to delete a record.
- The **Cancel** button allows you to exit a window without saving the changes.
- The **Quit**  button allows you to exit the Wizard at any stage, saving changes you made before exiting.

To use selective configuration,

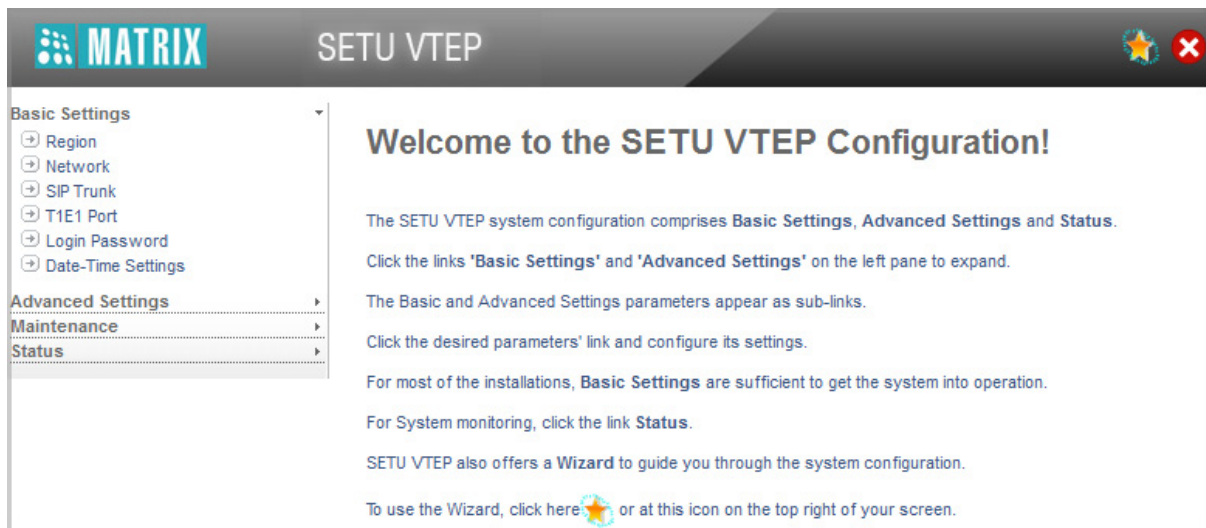
- Click **Basic Settings** link to expand.
- Click each parameter link, **Region**, **T1E1 Port**, **SIP Trunk**, **Login Password**, **Date and Time Settings**, **Network**.
- The selected parameter page opens.
 - Click  **Expand**, to expand a link to display all parameters under the link.
 - Click  **Collapse**, to collapse a link. Hides all parameters under the link.
 - Click  **Settings**, to configure / edit the settings of a parameter further or to edit an entry or record.

- The **Default** button assigns factory set values to all the parameters on the page.
- The **Add** button allows you to add a new record.
- The **Delete** button allows you to delete a record.
- The **Cancel** button allows you to exit a window without saving the changes.
- Set the desired values on the page.
- To save settings, click **Submit**.

You may use the Wizard or selectively configure the Basic Settings pages, whichever works best for you.

The instructions provided in this chapter, describe selective configuration of the Basic Settings pages.

- Click **Basic Settings** to expand.



- The following links appear under Basic Settings:
 - Region
 - Network
 - SIP Trunk
 - T1E1 Port
 - Login Password
 - Date and Time Settings

Each of these are explained in detail in the following.

Region

- Under Basic Settings, click the **Region** link.

The screenshot shows the 'MATRIX SETU VTEP' interface. On the left is a sidebar with 'Basic Settings' expanded, showing links for Region, Network, SIP Trunk, T1E1 Port, Login Password, and Date-Time Settings. Below this are 'Advanced Settings', 'Maintenance', and 'Status'. The main area is titled 'Region' and contains the following fields: 'Region' (text box with 'India'), 'Language' (dropdown with 'English'), 'PCM Companding Type' (dropdown with 'A-law'), 'Call Progress Tone' (radio buttons for 'Country wise' and 'Customized', with 'Country wise' selected and a dropdown showing 'India'), and 'Country Code' (text box with '91'). At the bottom are 'Submit' and 'Default' buttons.

Region

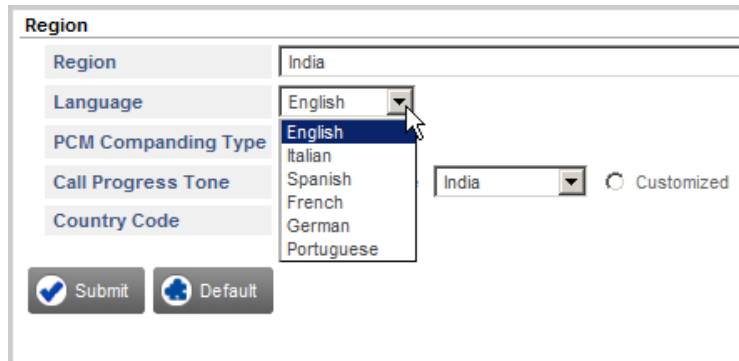
- In the **Region** list, click the name of the country where SETU VTEP is installed. Default: India.

This screenshot shows a scrollable list of countries under the 'Region' header. The list includes: India, Canada (Vancouver), Chile, China, Colombia, Costa Rica, Croatia, Cuba, Cyprus, Czech Republic, Denmark, Egypt, Fiji, Finland, France, Germany, Greece, Guyana, Hong Kong, Hungary, and India (highlighted at the bottom). To the left of the list are labels for 'Region', 'Language', 'PCM Companding Type', 'Call Progress Tone', and 'Country Code'. Below the list are 'Submit' and 'Default' buttons. A mouse cursor is visible at the top right of the list, indicating it is scrollable.

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 their relevant default values. See [“Default Region Table”](#) in the Appendix for country specific default values.

Language

- In the **Language** list, click the language in which you want the pages of the GUI, Jeeves, to be presented. Default: English.



SETU VTEP can display the pages of the GUI, Jeeves, in English, Italian, Spanish, French, German, and Portuguese.

When you login again later, all the pages of the GUI will appear in the language you have selected.

You can also select a Language of your choice on the Login page of Jeeves; however, the language you select will be applied for the current login session only.

PCM Companding Type

If required, you may change the **PCM Companding Type**—A-law or μ -law—set automatically by SETU VTEP according to the Region you have selected. Default: A-law (for India).



*When you submit the Region page after changing the PCM Companding Type, an alert message will appear “Submitting this page will restart the system. Do you want to continue?” Click **OK**. SETU VTEP will restart, and your changes will be saved.*

Call Progress Tones


- Select the **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 [“Call Progress Tones”](#) topic in the Appendix.










- To match the call progress tone of the country where SETU VTEP is installed, select the **Countrywise** option and select the Country from the list box. Default: India




The screenshot shows the 'Region' configuration window. The 'Region' field is set to 'India'. The 'Language' dropdown is set to 'English'. The 'PCM Companding Type' dropdown is set to 'A-law'. The 'Call Progress Tone' section has the 'Country wise' radio button selected, and a dropdown menu is open showing a list of countries including India, Argentina, Australia, Brazil, Canada, China, Egypt, France, Germany, Greece, India (highlighted), Indonesia, Iran, Iraq, Israel, Italy, Japan, and Kenya. The 'Country Code' field is set to '91'. There are 'Submit' and 'Default' buttons at the bottom left.

- If you want to change the cadence for the Call Progress Tones as per your requirement, select **Customized**.

The screenshot shows the 'Region' configuration window. The 'Region' field is set to 'India'. The 'Language' dropdown is set to 'English'. The 'PCM Companding Type' dropdown is set to 'A-law'. The 'Call Progress Tone' section has the 'Customized' radio button selected, and a red box highlights the '+' icon next to it. The 'Country Code' field is set to '91'. There are 'Submit' and 'Default' buttons at the bottom left.

- To customize the Call Progress Tones cadence, click **Settings**  . The **Call Progress Tone Cadence Table** opens.

Tone Type	Frequency1 (Hz)	Operator	Frequency2 (Hz)	Cadence					
				ON Time1 (msec)	OFF Time1 (msec)	ON Time2 (msec)	OFF Time2 (msec)	ON Time3 (msec)	OFF Time3 (msec)
Dial Tone	400	* 	25	9999	0	0	0	0	0
Ring Back Tone	400	* 	25	400	200	400	2000	0	0
Busy Tone	400	No 	0	750	750	0	0	0	0
Error Tone 1	400	No 	0	250	250	0	0	0	0
Confirmation Tone	400	No 	0	100	100	0	0	0	0
Feature Tone/ Programming Tone	400	* 	25	100	900	0	0	0	0
Intrusion Tone	400	No 	0	150	4850	0	0	0	0
Error Tone 2	400	No 	0	1000	1000	0	0	0	0
Routing Tone	400	* 	25	100	1900	0	0	0	0

- Set the cadence of each **Tone Type**, as per your requirement.
- Click **Submit**.
- Close the window to return to the **Region** page.

Country Code

- If required you may change the **Country Code**, set automatically by SETU VTEP for the Region you have selected. 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 **Submit** button to save your changes.

Network Parameters

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

When the SETU VTEP is installed in a Public IP Network,

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

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

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



- When your SETU VTEP is installed in a Private Network, you may have to change the IP Address and Subnet Mask of the Ethernet Port, before connecting it to the LAN Switch/Hub. However, this will not be necessary, if there is a DHCP / PPPoE server on the LAN which will automatically assign an IP Address that does not conflict with any other device on the LAN.
- To know the IP Address assigned to your SETU VTEP, dial **#51**. When the IP address is known, you can log into Jeeves.

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

- Under Basic Settings, click the **Network** link and configure the following parameters.

Connection Type

- Select the **Connection Type** according to the IP addressing scheme of the network which SETU VTEP is connected: DHCP, PPPoE, and Static.

- Select **DHCP**, if the network uses a DHCP server to assign the IP address, Subnet Mask and Gateway address to SETU VTEP.
- Select **PPPoE**, if the network uses PPPoE.

Enter **PPPoE User ID** (max. 64 characters) and **Password** (max. 64 characters). You may also enter the **PPPoE Service Name** (max. 64 characters), if provided.

- Select **Static**, if you want to assign manually the IP address, Subnet Mask and Gateway address.

If you select **Static**, enter the Static **IP Address** (default: 192.168.1.100) and the **Subnet Mask** (default: 255.255.255.0), and the **Gateway Address**.

By default, the Connection Type is Static. IP Address is 192.168.1.100 and Subnet Mask is 255.255.255.0



If you change the Connection Type to DHCP or PPPoE, you will not be able to access Jeeves using the default Static IP Address (192.168.1.100). To access Jeeves, you must know the current IP Address assigned to your SETU VTEP. You can check the current IP Address of your SETU VTEP using command. See "[System Commands](#)".

DNS Settings

DNS stands for Domain Name Server which is used to resolve domain name into IP address. You can select either **Static** or **Automatic**. Default: Static.

- Select **Static** if you want to configure DNS manually.
- Enter **DNS Address**.
- Enter the **DNS Domain Name**.
- Select **Automatic** DNS, if you want DNS Address and Domain name to be assigned by the DHCP/PPPoE server automatically.

This option will be applicable only if you have enabled DHCP or PPPoE as connection type.

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 embed DDNS client in the internet device. By doing so, whenever a new IP Address is assigned to internet host, DDNS client running in the internet host updates its new IP address in the dynamic DNS server.

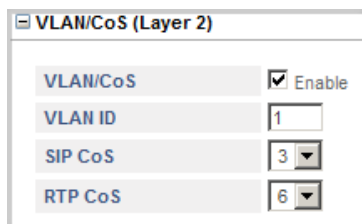
Once the IP Address of the system is updated in the DNS server, any caller on the IP network can reach to the system by dialing the host name/domain of the system.

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

SETU VTEP supports Dynamic DNS Server client of the Service Provider Dynamic DNS.org. If you want to use the DNS Service of DynDNS.org, configure these parameters:

- Select the **Dynamic DNS Enable** check box, if you have taken the services of DynDNS.org.
- Enter the **User Name** you created on DynDNS.org. The name can be of maximum 40 characters.
- Enter the **Password** you created for the User Name on DynDNS.org. The password can be of maximum 24 characters.
- Enter the **Host Name** you created on the DynDNS.org here. The Host Name can be of maximum 40 characters.

VLAN/CoS



- If the SETU VTEP is connected in VLAN network, configure the **VLAN/CoS**.

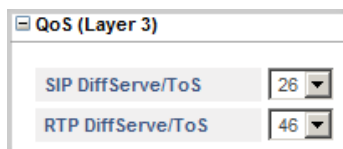
This parameter enables the SETU VTEP to add VLAN header to the packets generated by it. The VLAN header consists of the VLAN ID (12-bit) and Class of Service (CoS, 3-bit) for prioritization of traffic¹.

- Select the **VLAN/CoS** check box to enable VLAN ID tagging on all packets generated by the system. Default: Disabled.
- Enter the **VLAN ID** that you have assigned to the VLAN in which the SETU VTEP is connected. The valid range for this is 0-4094. Default: 1.
- For **SIP CoS**, define the CoS (priority) bits which will be added in all SIP packets. The range of CoS bits is from 0 to 7. Default: 3.

1. The IEEE 802.1P standard allows Layer2 switches to prioritize the traffic, thus providing Quality of Service (QoS), i.e. better handling of data that pass over a network, thereby resulting in greater reliability and quality., thereby resulting in greater reliability and quality. Quality of Service (QoS) on Layer2 is referred to as Class of Service (CoS) which is defined by IEEE 802.1P.

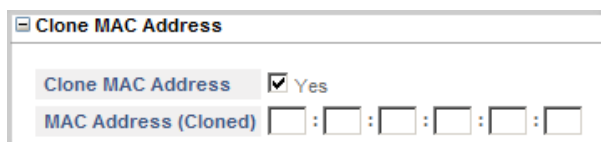
- For **RTP CoS**, define the CoS (priority) bits which will be added in all RTP packets. The range of CoS bits is from 0 to 7. Default: 6.

QoS (Layer 3)



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

MAC Cloning



- If you want to clone the MAC address, select the **Clone MAC Address** check box.
- If you select Clone MAC Address, enter the desired MAC address in the **MAC Address (Cloned)** field. MAC address is in hexadecimal format, e.g. 00:50:c2:55:b0:10.
- After you have set all the parameters as per your requirement, click **Submit** at the bottom of the page.
- You will get a prompt, “Ongoing calls would be disconnected. Do you want to submit this page?”
- Click **OK** to save the settings.

All the ongoing calls will be disconnected and your changes will be saved.

Restoring Default IP Address

You may restore the Default IP Address by changing the position of Jumper **J4** 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 **J4** from **BC** to **AB**.
- Switch ON the system and wait for 15 seconds.
- Switch OFF the system.
- Change the Jumper position from **AB** to the original position **BC**.
- Replace the enclosure cover.
- Switch ON the system.
- The IP Address will be restored to default, **192.168.1.100**.



When you restore the default IP Address (192.168.1.100) 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 Trunks

SETU VTEP supports thirty-two SIP trunks, which may be configured as Proxy or Non-Proxy (Peer-to-Peer) trunks.

You may register them with different ITSPs and use their services.

Follow the instructions provided below to configure the SIP Trunks.

- Under Basic Settings, click the **SIP Trunk** link.

The screenshot shows the SETU VTEP web interface. On the left is a sidebar with a 'MATRIX' logo and a menu under 'Basic Settings' including Region, Network, SIP Trunk (selected), T1E1 Port, Login Password, and Date-Time Settings. Below this are links for Advanced Settings, Maintenance, and Status. The main content area is titled 'SETU VTEP' and shows a tabbed interface for SIP 1 through SIP 5. The 'SIP 1' tab is active, displaying 'SIP Trunk - 1' configuration. It includes an 'Enable' checkbox, input fields for 'Name' and 'SIP ID', and a list of expandable sections: Registrar Settings, Vocoder Preference, Handling of Incoming Calls, Handling of Outgoing calls, Advanced, Jitter Buffer Setting for Speech, and Jitter Buffer Setting for Passthrough. At the bottom are 'Submit', 'Default', and 'Copy' buttons.

- For each SIP Trunk, configure the following parameters:
- Select the **SIP Trunk Enable** check box to use 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 of this trunk. Default: Blank.

You may assign the name of the ITSP with which the trunk is registered, or any other name of your choice.

The name you assign to the SIP Trunk will appear on the display of the remote party's phone when a call is made through this Trunk.

- In the **SIP ID** field, the SIP ID that you assign under *Registrar Settings* will appear.

Registrar Settings

Registrar Settings

SIP Trunk Mode	<input type="radio"/> Proxy <input checked="" type="radio"/> Peer-to-Peer <input type="button" value="→"/>
SIP ID	<input type="text"/>
Authentication ID	<input type="text"/>
Authentication Password	<input type="text"/>
Allowed IP Address for Incoming SIP Message	As per Peer-to-Peer table <input type="button" value="▼"/>
Digest Authentication	<input type="checkbox"/> Apply

- **SIP Trunk Mode:** Select SIP Trunk Mode according to your installation. Default: Peer-to-Peer.
 - Select **Proxy**, if you want to register this SIP Trunk with an ITSP or a Registrar Server.
 - Select **Peer-to-Peer**, if you want to use the trunk for Peer-to-Peer (non-proxy) calls.
- To configure **SIP Trunk Mode** as **Proxy**, configure the following parameters:

Registrar Settings

SIP Trunk Mode	<input checked="" type="radio"/> Proxy <input type="radio"/> Peer-to-Peer
SIP ID	<input type="text"/>
Authentication ID	<input type="text"/>
Authentication Password	<input type="text"/>
SIP Registration	<input checked="" type="checkbox"/> Enable
Registrar Server Address : Port	<input type="text"/> : 5060
Outbound Proxy	<input type="checkbox"/> Enable
Outbound Proxy Server Address : Port	<input type="text"/> : 5060
Add 'instance' in REGISTER	<input checked="" type="checkbox"/> Yes
Allowed IP Address for Incoming SIP Message	As per Trusted IP Address table <input type="button" value="▼"/> <input type="button" value="→"/>
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
Re-Registration Timer	3600 Seconds
Registration Retry Timer	10 Seconds

- In the **SIP ID** field, 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.
- **SIP Registration:** Keep the **SIP Registration** check box enabled. Default: Enabled.

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

You may clear the check box to disable SIP Registration, if required.

- If you have defined the SIP trunk mode as Proxy or Gateway, in the **Registrar Server Address: Port** field, 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. Default: Blank. The Registrar Server Address may be of maximum 64 characters. The valid port range is: 1025–65534. Default: 5060.

- Enable **Outbound Proxy** check box, if your service provider uses an outbound proxy for handling voice calls. Default: Disabled.
- In the **Outbound Proxy Server Address: Port** field, enter the IP address or domain name of the Outbound Proxy Server and the number of the Outbound Proxy Server's Listening Port for SIP. Default: Blank.

The Outbound Proxy Server Address may be of maximum 64 characters. The valid range for the port is 1025–65534. Default: 5060.

- To add '**rinstance**' in the **REGISTER** Message, keep this check box enabled. Default: Enabled.

'rinstance' is any random value which can be used by the SETU VTEP to fetch its own contact binding, i.e. 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 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 Address:Port1* and *2*, if configured for this SIP Trunk. If you do not configure the Trusted IP Address table, incoming calls will be allowed from the last three IP Addresses only.

To configure Trusted IP Address table, click **Settings** .

The **Trusted IP Address Table** opens in a new window.

IP Address : Port

- 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 want to allow incoming calls on this SIP Trunk only after the callers authenticate themselves with their User ID and Password, enable **Digest Authentication**. Default: Disabled.

If you enable Digest Authentication feature on the SIP Trunk, you must configure the Digest Authentication Table. See ["Digest Authentication"](#) for more details.

- Keep the **Check SIP ID for Incoming SIP Message** check box enabled, if you want SETU VTEP to validate the SIP ID during an incoming call. Default: Enabled.
- Keep the **Check Proxy Address for Incoming SIP Message** check box enabled, if you want SETU VTEP to validate the Proxy Address during an incoming call. Default: Enabled.
- Keep the **Check Proxy Port for Incoming SIP Message** check box enabled, if you want SETU VTEP to validate the Proxy Port during an incoming call. Default: Enabled.
- Select **Send OPTIONS message as Heartbeat** check box, if you want SETU VTEP to send OPTIONS messages periodically to the Proxy Server to monitor its availability. Default: Disabled.

Calls can be made and received only if the Proxy Server is alive. If the Proxy Server is unavailable (no response is received from the server), the status of the SIP Trunk will display *"Inactive"* along with the Reason for Failure.



- To view status of the Proxy Server, go to *"SIP Trunk" Status*.
- The **Send OPTIONS message as Heartbeat** will work only if,
 - **SIP Trunk Mode** is configured as Proxy.
 - **SIP Registration** is disabled.

If you enable *Send OPTIONS message as Heartbeat*, you must configure the **Heartbeat Interval**.

- Set the **Heartbeat Interval** (Seconds). It is the time period after which SETU VTEP will send the OPTIONS message to the Proxy Server to check its availability. Valid range of Heartbeat Interval is from 10 to 999 seconds. Default: 60 seconds.
- Set 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.

The valid range of this timer is 00001- 65535. Default: 3600 seconds.



*The **Re-registration Timer** will be applicable only if, **SIP Registration** is enabled.*

- Define 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.

The valid range of this timer is from 00001- 65535. Default: 10 seconds.



*The **Registration Retry Timer** will be applicable only if, **SIP Registration** is enabled.*

- If you want the system to send DNS SRV query to the configured domain server, enable **DNS SRV**. 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.

- 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 port range: 1025–65534. Default Port: 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 port range: 1025–65534. Default Port: 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 **No Response Timer**. It is the time 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: 01–99 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.



*If you have disabled **SIP Registration**, it is recommended that you enable **Send OPTIONS message as Heartbeat** to use Fallback facility efficiently.*

- Click **Submit**.
- Select **Peer-to-Peer**, if you want to use the SIP trunk for Peer-to-Peer (non-proxy) calls.

Registrar Settings

SIP Trunk Mode

☐ Proxy
☒ Peer-to-Peer

SIP ID

Authentication ID

Authentication Password

Allowed IP Address for Incoming SIP Message

As per Peer-to-Peer table

Digest Authentication

☐ Apply

- In the **SIP ID** field, enter the desired SIP ID which the remote parties will use to call this SIP Trunk. Default: Blank.

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

- In the **Authentication ID** field, enter the ID of your preference as Authentication ID. Default: Blank.
- In the **Authentication Password**, enter a password of your choice as Authentication Password for the Authentication ID you have assigned. Default: Blank.
- To configure the number strings in the Peer-to-Peer Table, click **Settings** . A new window opens.

Peer-to-Peer Dialing

	Edit	Destination Number	Minimum Digits	Maximum Digits	Destination Address	Name
		No Match Found	3	16	192.168.1.147	

Total Records : 11

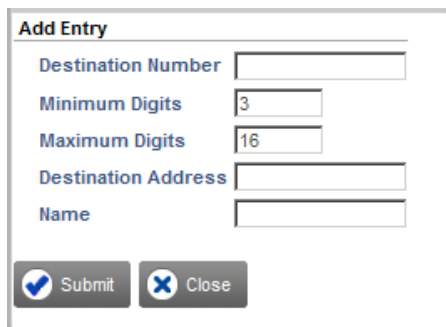
Add

Delete

Close

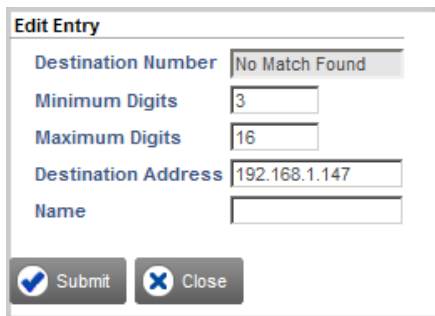
You can configure as many as 500 number strings.

- Click **Add** to enter a new record.

A dialog box titled "Add Entry" with a light gray border. It contains five input fields: "Destination Number" (empty), "Minimum Digits" (containing "3"), "Maximum Digits" (containing "16"), "Destination Address" (empty), and "Name" (empty). At the bottom left are two buttons: "Submit" with a blue checkmark icon and "Close" with a blue X icon.

OR

- Click **Settings**  to edit the No match found entry.

A dialog box titled "Edit Entry" with a light gray border. It contains five input fields: "Destination Number" (containing "No Match Found"), "Minimum Digits" (containing "3"), "Maximum Digits" (containing "16"), "Destination Address" (containing "192.168.1.147"), and "Name" (empty). At the bottom left are two buttons: "Submit" with a blue checkmark icon and "Close" with a blue X icon.

- In the **Destination Number** field, enter the peer-to-peer number string—prefix or entire number—that will be dialed. The number string must not exceed 24 characters. Default: Blank.

If the number to be dialed out is <dialednumber@destination address>, for example, 123@abc.com, you must enter 123 in this field.

- As **Minimum Digits**, define the minimum length of the number string that must be dialed for the system to consider it as a valid number. Default: 03.

If the peer-to-peer number string you dial is shorter than the Minimum Digits you have configured, the system will not dial out the number.


- As **Maximum Digits**, define the maximum length of the number string that must be dialed out for the system to consider it the complete number string. Default: 16.

If the peer-to-peer number string you dial is longer than the Maximum Digits you have configured, the system will strip off the additional digits and dial out the number.

- In the **Destination Address** field, enter the domain name or IP Address to where the dialed peer-to-peer number string is to be sent. The Destination Address may consists of up to 40 characters. Default: Blank.

For example, if the peer-to-peer number to be dialed out is 123@abc.com, enter abc.com as Destination Address. If the number is 123@ 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.


- To identify the number string you configured, enter a name in the **Name** field. It may be the name of your contact or any name you wish to assign to the number string. The name may consist of 12 characters (maximum). Default: Blank.
- Click **Submit** to save entries. The window closes.
- The records appear in the table.
- To edit any entry, click **Edit**.
- To delete an entry, select the check box and click **Delete**.
- Close the window to return to the main page. To know more about the Peer-to-Peer application, see [“Peer-to-Peer Dialing”](#) under *Advanced Settings*.
- Select desired option in the **Allowed IP Address for Incoming SIP Message**, from the following.
 - **As per Trusted IP Address table:** If you select this 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.



IP Address : Port

 Submit  Close

- 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.
- **As per Peer-to-Peer table:** If you select this 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.
- **Any:** If you select this option, **Digest Authentication** will be enabled automatically. The system will allow incoming calls only after the callers authenticates 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 Peer to Peer table**.

- If you set *Allowed IP Address for Incoming SIP Message* to *As per Trusted IP Address table* or *As per Peer to Peer table*, you may also enable the **Digest Authentication**. Incoming calls on this SIP Trunk will be allowed only after the callers authenticate themselves with their User ID and Password. Default: Disabled.

If you enable Digest Authentication feature on the SIP Trunk, you must configure the Digest Authentication Table. See “[Digest Authentication](#)” for more details.

Vocoders

- Click **Vocoder Preference**.

- Select **Vocoders** in the order of preference from the multiple selection box.

Vocoders are the various voice codecs used to compress the data in RTP packets for optimum use of bandwidth and for ensuring voice quality. You can set 8 Vocoder options in the order of preference.

The Vocoders supported by SETU VTEP in the order of preference, from 1st to 8 th, listed in the **Selected Codecs** box are:

1. G.729
 2. G.723
 3. GSM FR
 4. iLBC 30ms
 5. iLBC 20ms
 6. GSM EFR
 7. G.711 (μ -Law)
 8. G.711 (A-Law)
- To remove a Vocoder from the **Selected Codecs** list, click the Vocoder you want to remove, and then click the LEFT ARROW. The Vocoder is moved to the **Available Codecs** list.
 - To move a Vocoder from the **Available Codecs** list to the **Selected Codecs** list, click the Vocoder you want to move, and then click the RIGHT ARROW.
 - Click the UP/DOWN ARROW to move the Vocoder to the desired position in the list.
 - If you select G.723 as a Preferred Vocoder, also select **G.723 Bit Rate**. You may select: **5.3 Kbps** or **6.3 Kbps**. Default: 6.3kbps.

When G.723 is negotiated, the selected Bit Rate will be applied only when sending the RTP packets. When receiving RTP packets from the remote end, both Bit Rates of G.723 will be accepted.



The maximum simultaneous calls that can be made, differs according to the type of Vocoder you select. Refer the table below.

Vocoder	Maximum Simultaneous calls
G.729	16
G.723	30
GSM FR	30
iLBC 30ms	30
iLBC 20ms	26
GSM EFR	24
G.711 (μ -Law)	30
G.711 (A-Law)	30

- Enable **Silence Suppression** flag, if you want SETU VTEP to suppress the *Silence* packets and allow only the *Voice* packets to pass through. Default: Disabled.



Silence Suppression is applicable only when you have selected G.729 as Preferred Vocoder.

- 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 **Send VAD** check box, if you want SETU VTEP to send *VAD = no* in the SDP for any offer and answer. Default: Disabled.

SETU VTEP will send *VAD = no* only if G.711 (μ - Law) or G.711 (A - Law) codec is present in the SDP offer or answer.

- Select the **Send ptime header** check box, if you want SETU VTEP to add ptime header in the SDP offer and answer. Default: Disabled.
- You must select the **ptime value**, if you have enabled *Send ptime header* check box and have selected codec as—G. 729 and/or G.711 (μ - Law) and/or G.711 (A - Law). You can select from the following:
 - 10 msec
 - 20 msec
 - 30 msec
 - 40 msec

Default: 20 msec



For Passthrough FAX, SETU VTEP will use the default ptime value (20 msec) only.

Handling of Incoming Calls

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

- Select the **Block all calls received on this SIP Trunk** check box, if you do not want to route calls received on this SIP Trunk. Default: Disabled.
- 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 **Use Called Party Number From**, 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:
 - 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.

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

Route to the Fixed Destination Number

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

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 a Fixed Destination 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
Fixed Destination Number	
Fixed Destination Number	
Select Destination Port for routing calls	Fixed
Allowed-Denied Logic	<input type="checkbox"/> Apply
Reject Calls from Blacklisted Callers	<input type="checkbox"/> Apply

If you select this method,

- 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. 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.

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

If you select this method,

- Click the **Settings** and configure the **Calling Number Based** table for the SIP Trunk.

The Calling Number Based Table page opens. You can store 500 entries in this table.

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		

☒ Submit ☒ Default All ☒ Close

- Configure following parameters in this table:
 - Calling Number:** Enter the calling party numbers in the column Calling Numbers. Calling numbers may consist of a maximum of 24 characters. All ASCII characters are allowed. Default: Blank.

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

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 port.
- **If no match found in the Calling Party Number Table**, you may select any of 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
- Click **Submit** to save.

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

Route on the basis of DDI Number

In this method, a call received on the SIP Trunk is routed to a specific number as per the DDI number received in the SIP INVITE message.

You must configure the DDI numbers in the DDI Number Based Table. When there is an incoming call on the SIP Trunk, SETU VTEP will match the CLI of the number received with the entries of this table. If a match is found for the number in the table, the call is routed to the destination port.

To apply this method, do the following:

- In the **Route all Incoming calls with CLI** list, click on the **Basis of DDI Number**.
- Click **Settings** .



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)	on the basis of DDI 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

The **DDI Number Based Table** page opens. You can store up to 100 numbers in this table.

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

- There are two ways to generate the DDI Numbers:
 - Using the **DDI Number Generation** Button to automatically generate the DDI Number Table. See [“Configuring SIP-DDI Number Based Table”](#) in Destination Number Determination topic for instructions.

OR

- Entering each DDI Number manually.
 - In the **DDI Number** column, enter the DDI numbers allotted by your service provider. The DDI numbers may consist of a maximum of 24 characters. Characters 0-9, +, * and # are allowed. Default: Blank.
 - In the **Destination Number** column, enter a corresponding destination number for each DDI number. Destination numbers may consist of a maximum of 24 characters. Characters 0 to 9, * and # are allowed. Default: Blank.
 - To apply **Reverse DDI** for each number, select the **Reverse DDI Apply** check box and select the **Reference ID** for the number. Default: Apply Reverse DDI is disabled and Reference ID is 1.
- Click **Submit** to save your entries. Close the window to return to the SIP Trunk page.

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

Route 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

In this method, a call is routed to a specific number depending upon the called party number received in the SIP ID of the Request URI of the INVITE message.

Route After Answering the Call and Collecting the Digits

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)	after Answering the Call and Collecting the Digits
Block Calls received without CLI on this SIP Trunk	<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
First Digit Wait Timer	7 Seconds
Inter Digit Wait Timer	5 Seconds
End Of Dialing Digit	#
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

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 the destination number.

If you select this option, configure the following:

- **Prompt caller to enter PIN:** if you want to enable “PIN Authentication”, select this check box.
- **First Digit Wait Timer (FDWT):** Define the number of seconds the system should wait for the user to dial the destination number. Default: 7 seconds. You may change this timer, if required. The valid range of this timer is 01 to 99 seconds.
- **If No Digit dialed during First Digit Wait Timer (FDWT)** by the user, you may either **Disconnect the Call** or **Use Fixed Destination Number** to route the call. 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. Default: Blank.

You may configure the following options as end-of-dialing indication:

- **Inter Digit Wait Timer:** Define the number of seconds the system should wait while receiving the dialing digits, to consider it as end-of-dialing. You may change this timer, if required. The valid range is 01 to 99 seconds. Default: 05 seconds.
- **End of Dialing Digit (Termination digits):** Select whether the system should consider # or * as termination digit to detect end of dialing. Default: #
- **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. The 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.

- Select the **Allow making New Call using Access code**, if you want to enable the feature Making New Call using Access Code on the SIP Trunk. See [“Making a New Call using Access Code”](#).
- Click **Submit** to save settings.
- Select the **Block Calls received without CLI on this SIP Trunk** check box, if you do not want to route calls without CLI through this port.

Route all Incoming calls (without CLI)

- To **Route all Incoming calls (without CLI)**, you may select from any of the following methods:

- to a Fixed Destination Number, see [“Route to the Fixed Destination Number”](#).
- to the Called Party Number, see [“Route To the Called Party Number”](#).
- on the basis of DDI Number, see [“Route on the basis of DDI 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 for routing calls



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 Fixed

Reject Calls from Blacklisted Callers On the basis of Destination Number
On the basis of Calling Party Number

Select the Destination Port for routing calls for the SIP Trunk. You may select from any of the following options:

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



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 selected for IP Dialing. (Refer “IP Dialing” feature for more details).

Fixed

In this method, calls received on the SIP Trunk are routed to a fixed destination port, irrespective of the number dialed on the source port.



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

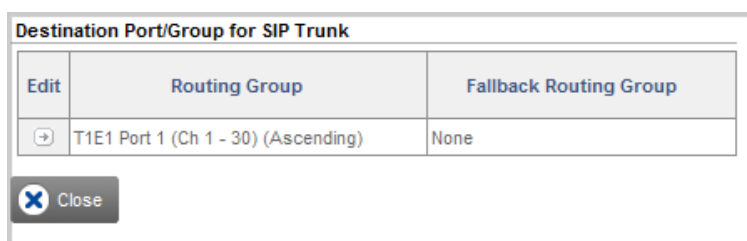
Select Destination Port for routing calls Fixed

Allowed-Denied Logic ☐ Apply


Reject Calls from Blacklisted Callers ☐ Apply


If you select this option,

- Click **Settings**  . A new window opens.




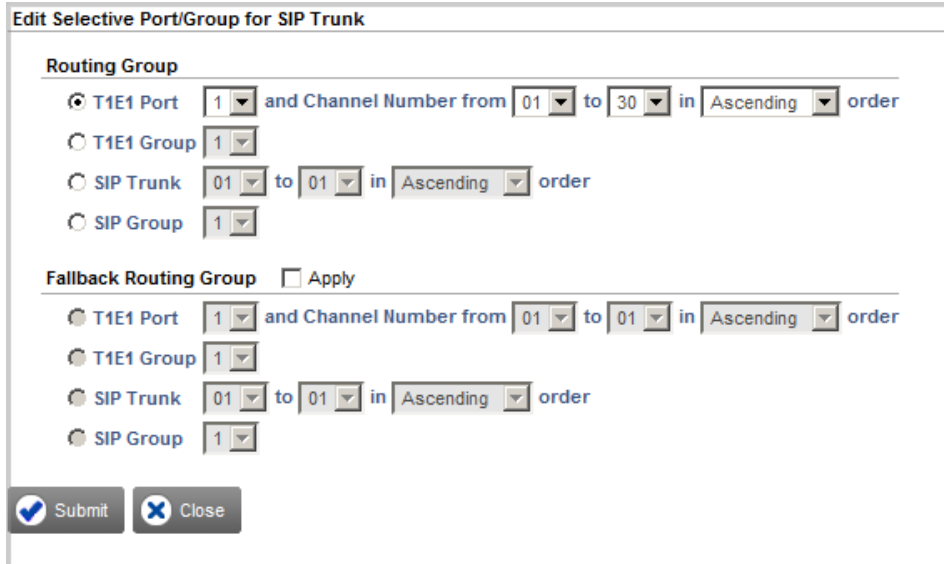
Destination Port/Group for SIP Trunk

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

 Close

The default Routing Group and Fallback Routing Groups appear.

- Click **Settings**  under Edit, if you wish to change the default Routing Group options. A new window opens.



- Create the **Routing Group**.
 - To create a routing group of *sequential* T1/E1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* T1/E1 channels as members, select a **T1E1 Group** Number.

Click the settings icon and create the T1/E1 Group. See [“Group”](#) for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group Number**.

Click the settings icon and create the SIP Group. See “[Group](#)” for further instructions.

- To create the **Fallback Routing** Group,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and the SIP Trunks.
- Click **Submit** to save changes. The **Edit** window closes.
- The Routing and Fallback Groups you created appear. Close the window to return to the main page.

On the basis of Destination 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	On the basis of Destination Number
Allowed-Denied Logic	<input type="checkbox"/> Apply
Reject Calls from Blacklisted Callers	<input type="checkbox"/> Apply

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.

- If you select this option, you must configure the **Destination Number Based** table.
- Click **Settings** . A new window opens.

SIP Trunk - Destination Port Determination - Destination Number Based						
	Edit	Destination Number	Minimum Digits	Maximum Digits	Routing Group	Fallback Routing Group
		No Match Found	3	16	T1E1 Group 1	None
Total Records : 1		1				
	Add		Delete		Close	

- Click **Add** to add an entry. A new window opens.

- In the **Destination Number**: Enter the number (max. 24 characters) you expect callers to dial. Valid characters: 0 to 9, +, * and #. Default: blank.
- In the **Minimum Digits** field, enter the minimum digits for the system to consider the destination number as a valid number. Range: 01 to 24. Default: 03.

If the dialed number string is less than the configured minimum length, the call will be rejected.

- In the **Maximum Digits** field, enter the maximum number of digits of the destination number the caller must dial for the system to route the call.

If the number string dialed by the caller exceeds the maximum length configured, the system will strip off the extra digits, and route the call. Maximum length range: 01 to 24. Default: 16.

- Create the **Routing Group**.
 - To create a routing group of *sequential* T1/E1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* T1/E1 channels as members, select a **T1E1 Group** Number.

Click the settings icon and create the T1/E1 Group. See [“Group”](#) for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group** Number.

Click the settings icon and create the SIP Group. See [“Group”](#) for further instructions.


- To create the **Fallback Routing** Group,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and the SIP Trunks.
- Click **Submit** to save changes. The **Add Entry** window closes.
- The Routing and Fallback Groups you created appear.
- To edit an entry, click **Edit**, a new window opens. Make the changes as per your requirement and click **Submit**.
- To delete an entry, select the check box and click **Delete**.
- Close the window to return to the main page.



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

On the basis of Calling 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	On the basis of Calling Party Number
Allowed-Denied Logic	<input type="checkbox"/> Apply
Reject Calls from Blacklisted Callers	<input type="checkbox"/> Apply

In this method, Incoming calls on the source port will be routed to the destination port on the basis of the calling party's number.

- If you select this option, you must configure the **Calling Number Based** table.
- Click **Settings** . A new window opens.

SIP Trunk - Destination Port Determination - Calling Number Based			
	Calling Number	Routing Group	Fallback Routing Group
	No Match Found	T1E1 Group 1	None

Total Records : 1 1

 Add  Delete  Close

- Click **Add** to add an entry. A new window opens.

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 the **Calling Number** field, enter numbers (max. 24 characters) from which you expect calls to be received. All ASCII characters are allowed. Default: blank.
- Create the **Routing Group**.
 - To create a routing group of *sequential* T1/E1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* T1/E1 channels as members, select a **T1E1 Group Number**.

Click the settings icon and create the T1/E1 Group. See [“Group”](#) for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group Number**.

Click the settings icon and create the SIP Group. See [“Group”](#) for further instructions.

- To create the **Fallback Routing** Group,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and the SIP Trunks.
- Click **Submit** to save changes. The **Edit** window closes.
- The Routing and Fallback Groups you created appear.
- To edit an entry, click **Edit**, a new window opens. Make the changes as per your requirement and click **Submit**.
- To delete an entry, select the check box and click **Delete**.
- Close the window to return to the main page.

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

Allowed - Denied Logic (Toll-Control)

With the Allowed-Denied Numbers feature you can permit and restrict the dialing of particular numbers from the SIP Trunks.

Allowed Denied Number Logic makes use of two predefined Number lists:

- **Allowed Numbers List:** This is the list of numbers that can be dialed out from SIP Trunk. By default, List Number 7 is assigned to the SIP Trunk.

- **Denied Numbers List:** This list contains the numbers that are to be restricted from being dialed out from the SIP Trunk. By default, List Number 8 is assigned to the SIP Trunk.

Both lists must be programmed first and then applied on the SIP Trunk. For instructions, see [“Number Lists”](#).

To apply Allowed - Denied Logic on the SIP Trunk,

- Click the Allowed - Denied Logic **Enable** check box.

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 On the basis of Calling Party Number

Allowed-Denied Logic ☒ Apply

Allowed Number List 07

Denied Number List 08

Reject Calls from Blacklisted Callers ☐ Apply

- As **Allowed Numbers List**, select the number of the Number List, which you have programmed as Allowed Number List. By default, Number List 7 is assigned as Allowed Number List.

If you have not configured the Allowed Numbers List,

- Click **Settings** . The Number List page will open in a new window.

Number Lists


Location	List 5	List 6	List 7	List 8
01				
02				
03				
04				
05				
06				
07				
08				
09				
10				
11				
12				
13				

Submit Default Close

- You may configure the default Number List 7 or any other Number List as Allowed Number List.

- Click **Submit** to save Number List and close the window.
- Return to Allowed - Denied Logic parameter and assign the Number List you configured.
- **Denied Number List:** Select the number of the Number List, which you have programmed as Denied Number List. By default, Number List 8 is assigned as Denied Number List.

If you have not configured the Denied Number List,

- Click **Settings**  .
- The Number List page will open in a new window.
- You may configure the default Number List 8 or any other Number List as Denied Number List.
- Click **Submit** to save Number List and close the window.
- Return to Allowed - Denied Logic parameter and assign the Number List you configured.
- Click **Submit** to apply the changes. See [“Allowed - Denied Logic”](#) under [“Number Lists”](#).

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.

Black List Callers feature makes use of a predefined Number lists. You must enter such unwanted callers in this list.

For instructions refer [“Black Listed Callers”](#) under [“Number Lists”](#).

To apply Black Listed Callers on SIP Trunk,


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

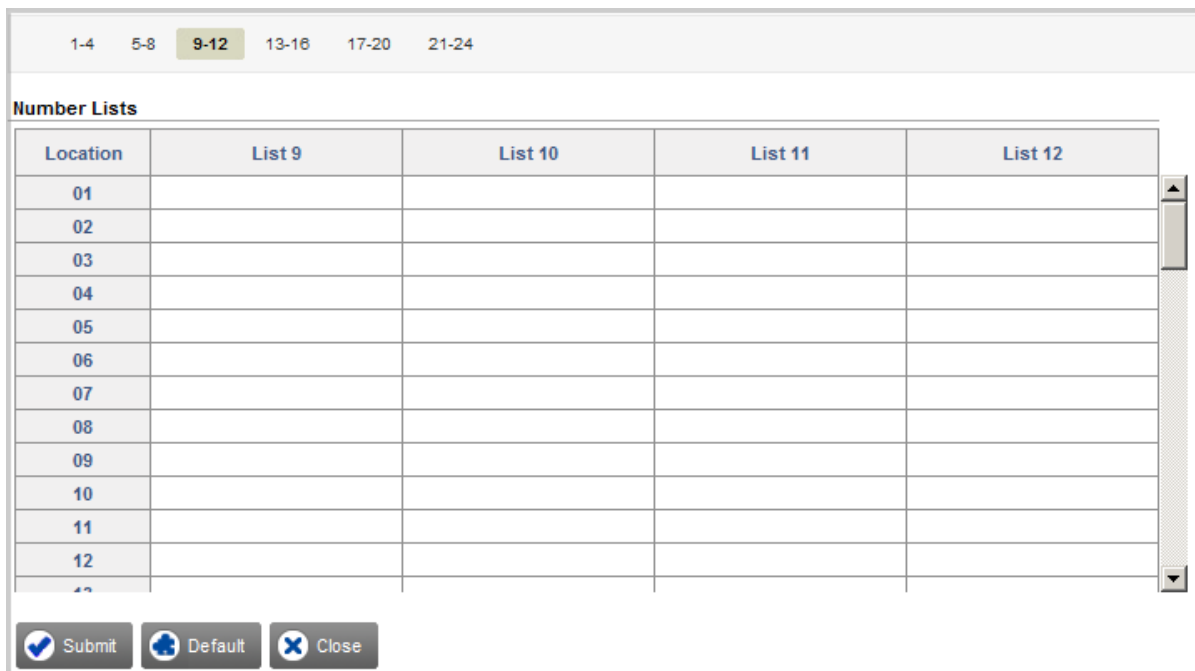


Handling of Incoming Calls	
Block all calls received on this SIP Trunk	<input type="checkbox"/> Yes
Use Called Party Number from	Request-URI
Route all Incoming calls (with CLI)	to the Called Party Number
Block Calls received without CLI on this SIP Trunk	<input type="checkbox"/> Yes
Route all Incoming 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 checked="" type="checkbox"/> Apply
Blacklisted Callers Number List	11

- As **Black List Callers**, select the Number List in which you have configured the numbers of Black listed callers. By default, Number List 11 is assigned as Black Listed Callers List.

If you have not configured the Black List Callers,

- Click **Settings**  . The Number List page opens in a new window.



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

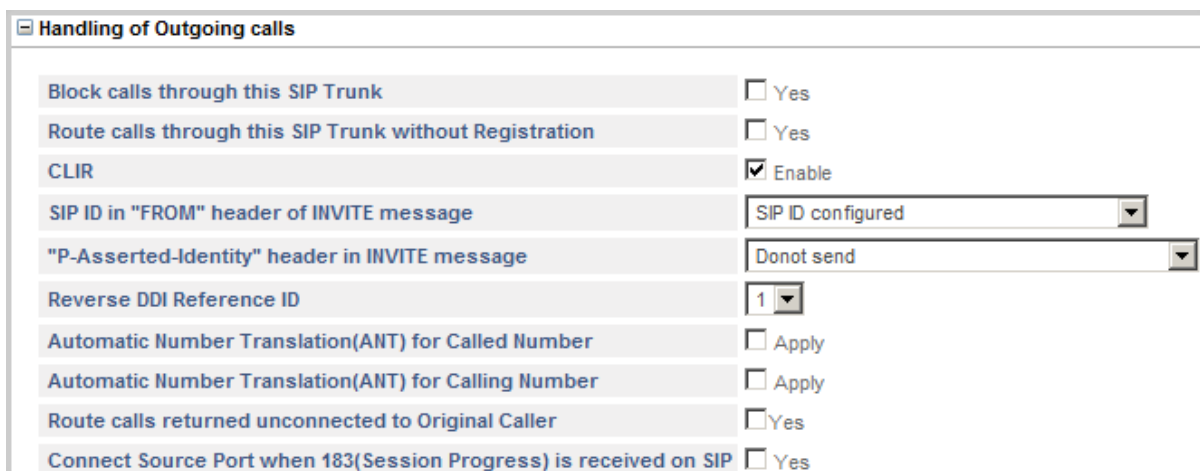
- You may configure the default Number List 11 or any other Number List as Black Listed Callers List.
- Configure the numbers of unwanted callers in a Number List.



Make sure you have configured the full SIP URI (for example: 12345@abc.com) of the unwanted callers in the Blacklisted Callers Number List.

- Click **Submit** to save Number List and close the window.
- Return to the Black Listed Callers option and assign the Number List.
- Click **Submit** to apply the changes.

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 checked="" type="checkbox"/> Enable
SIP ID in "FROM" header of INVITE message	SIP ID configured
"P-Asserted-Identity" header in INVITE message	Donot send
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

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

For outgoing calls from SIP Trunk the features Send Caller ID, CLIR, Automatic Number Translation (ANT) and Route Calls Returned Unconnected to Original Caller may be applied.

- Select the **Block calls through this SIP Trunk** check box, if you do not want to route outgoing calls through this port.
- Select the **Route Calls through this port without Registration** 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.

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.
- Select an option you want to send as **SIP ID in "FROM" header of INVITE message**. You may select:
 - SIP ID configured
 - Caller ID received on Source Port
 - Caller ID after applying Reverse DDI logic

Default: SIP ID configured

- Select an option you want to send as **"P-Asserted-Identity" header in INVITE message**. You may select:
 - Do not send
 - Send SIP ID configured
 - Send Caller ID received on Source Port
 - Send Caller ID after applying Reverse DDI logic
 - Configure an option you want to send as **"P-Asserted-Identity" header in INVITE message, If no match found using Reverse DDI logic**. You may select:
 - Send SIP ID configured.
 - Send Caller ID received on Source Port
 - Send Fixed Number.
 - Send Fixed Number

Default: Do not send

- If you have selected *Send Fixed Number* as an option for **"P-Asserted-Identity" header in INVITE message** or *If no match found using Reverse DDI logic*, configure the **Fixed Number**. The Fixed Number can be a maximum of 24 characters. Characters 0-9, +, * and # are allowed. Default: Blank.



*If you have enabled **CLIR** and **"P-Asserted-Identity" header in INVITE message** is configured other than Do not send, then SETU VTEP will add **Privacy = ID** header in the INVITE message during an outgoing call from SIP Trunk.*

- Select the **Reverse DDI Reference ID**, if you have selected *Caller ID after applying Reverse DDI logic* as SIP ID in "FROM" header of INVITE message and/or *Send Caller ID after applying Reverse DDI logic* as "P-Asserted-Identity" header in 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 (ANT) logic on the outgoing calls made from the SIP Trunk.
 - To apply ANT logic on the Called Numbers, click the **Automatic Number Translation (ANT) for Called Number** check box. Default: Disabled.

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
"P-Asserted-Identity" header in INVITE message	Donot send
Reverse DDI Reference ID	1
Automatic Number Translation(ANT) for Called Number	<input checked="" type="checkbox"/> Apply
Use Automatic Number Translation Table	1
Pause Timer	2 Seconds
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

- In the **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 page will open in a new window.

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	

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

- You may configure the default Automatic Number Translation Table 1 or any other Table (2 to 8). 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.
- Configure the **Pause Timer**, if you have configured ^ (Pause) in the Add Prefix column of the ANT Table. The valid range of the Pause Timer 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.

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
"P-Asserted-Identity" header in INVITE message	Donot send
Reverse DDI Reference ID	1
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Apply
Automatic Number Translation(ANT) for Calling Number	<input checked="" type="checkbox"/> Apply
Use Automatic Number Translation Table	5
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

- 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 page will open in a new window.

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	
13		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.
- Click **Submit** to apply List.
- Enable **Route calls returned unconnected to Original Caller**, if you want SETU VTEP to route outgoing calls made from this port that return unconnected back to the original caller.

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, this incoming call is placed to the original calling party. You can change the duration of this timer and delete records of such calls. 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 183(Session Progress) is received on SIP** 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.



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

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

Advanced

- Click **Advanced** and configure the following parameters:

Advanced	
SIP Transport	<input checked="" type="radio"/> UDP <input type="radio"/> TCP <input type="radio"/> TCP (with fallback to UDP) <input type="radio"/> TLS
Maximum Calls	30
Symmetric RTP	<input type="checkbox"/> Enable
Secure RTP (SRTP) Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable and Optional <input type="radio"/> Enable and Forced
NAT Type	<input checked="" type="radio"/> Disable <input type="radio"/> Router Public IP Address <input type="radio"/> STUN
DTMF	Outband
FAX Protocol	<input checked="" type="radio"/> T.38 (UDPTL) <input type="radio"/> Pass Through
Convert FAX call to Speech call when FAX is complete	<input type="checkbox"/> Yes
Passthrough FAX Codec	G.711 (μ-law)
Call Hold Methods	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
Call Hold using Inactive	<input type="checkbox"/> Yes
Send Re-INVITE when multiple codec is received in 200(OK)	<input checked="" type="checkbox"/> Yes
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Send "user=phone" in SIP URI	<input type="checkbox"/> Yes

- SIP Transport:** 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.
 - TCP (Fallback to UDP):** TCP is used for outgoing messages. However, if the TCP connection fails, the system will attempt to send the message again over UDP.
 - TLS:** Outgoing messages are transported using TLS.

Default: UDP



- To use *TCP* or *TCP (Fallback to UDP)*, to must enable **SIP over TCP** in the “[System Parameters](#)” page.
- To use *TLS*, you must enable **SIP over TLS** in “[System Parameters](#)”.
- Maximum Calls:** Configure the number of simultaneously calls you want to allow on this SIP Trunk. Default: 30.

The number of simultaneous SIP calls depends on the number of simultaneous calls allowed by the ITSP with whom you have subscribed this SIP Trunk.

The SETU VTEP supports 30 simultaneous calls. Ask your ITSP about the number of simultaneous SIP calls supported on this SIP Trunk.

- **Symmetric RTP:** If you want the system to send RTP packets to original IP and Port from where RTP packets are received, by ignoring the contact information received in SDP, enable the **Symmetric RTP** check box. Default: Disabled
- Select the appropriate **Secure RTP (SRTP)** mode from the following options:
 - **Disable:** SRTP will not be used.
 - **Enable and optional:** Either RTP or SRTP will be used. If you select this mode, you must select the SRTP Media Type. You can select AVP or SAVP. Default: AVP.
 - **Enable and forced:** Only SRTP will be used.

Default: Disabled.

- **NAT Type:** 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 configure 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 configure the STUN Server Address and port in "[System Parameters](#)".
- **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 is 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 is negotiated, SIP INFO will have priority over Outband.

Default: Outband

- **FAX Protocol:** To send and receive the Fax over IP, select the desired Fax over IP protocol:
- **T.38(UDPTL):** 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 (UDPTL).



If the FAX sent using T.38 is rejected, SETU VTEP will use Pass Through as the Fall Back protocol to send the fax.

- Select the **Convert FAX call to Speech call when FAX is complete** check box, if you want SETU VTEP to convert the fax call to a speech (voice) call after the fax complete event is received. Default: Disabled.
- If you have selected *Pass Through* as Fax Protocol, you must select an appropriate **Passthrough FAX Codec** that is compatible with your ITSP proxy server/remote peer. You may select the Codec as:
 - G.711 (μ-law)
 - G.711 (A-law)

Default: G.711 (μ-law)

- Select an appropriate **Call Hold Method** that is compatible with your ITSP proxy server/remote peer. You may select:
 - RFC 2543
 - RFC 3261

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.
- 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 codec received in 200(OK). Default: Enabled.
- Select the **Allow Call Disconnection using Access code**, if you want to enable the feature Disconnect Call using Access Code on the SIP Trunk. See ["Disconnecting a Call using Access Code"](#).
- 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. Default: Disabled.

SETU VTEP will send user=phone in SIP URI, only if the SIP ID is numeric.

Jitter Buffer Setting for Speech

The speed at which the voice packets travel through a network depends on the condition of the network. All voice packets may not come at the same speed. This variation in receiving the packets, known as Jitter, affects the voice quality. You may resolve this by configuring Jitter Buffer Settings for Speech. Jitter Buffer receives voice packets, stores them and sends it to the DSP to process it at specified intervals, thus improving the voice quality.

- Click **Jitter Buffer Setting for Speech** and configure the following parameters:

- Mode:** Select the mode of Jitter Buffer, you want to set for Speech from the following.
 - Static:** Jitter Buffer will receive and store the voice packets, and then send it to the DSP to process it at a fixed interval, you set as Average Delay. Once the delay is set, Jitter Buffer will not change it.
 - Full Adaptive:** Jitter Buffer will receive and store the voice packets, and then send it to the DSP to process it at required intervals depending on the network condition. This condition is controlled by the system by setting the boundaries—Minimum, Maximum, Average Delay—for the Jitter Buffer and deciding the number of packets outside these boundaries. Jitter Buffer adapts to the changing network conditions by adjusting these delays.
 - Short Adaptive:** Jitter Buffer will receive and store the voice packets, and then send it to the DSP to process it at a fixed interval, unless a crises is detected. A crises is detected when the packets are dropped by the Jitter Buffer because they arrive too early or too late. This condition is controlled by the system by setting the boundaries—Minimum, Maximum, Average Delay—for the Jitter Buffer and deciding the number of packets outside these boundaries.

Default: Full Adaptive

- Min Delay:** It sets the lower boundry for the Full and Short Adaptive mode of Jitter Buffer. The valid range of Minimum Delay is: 000–180 msec. Default: 040 msec.
- Max Delay:** It sets the upper boundry for the Full and Short Adaptive mode of Jitter Buffer. The valid range of Maximum Delay is: 000–300 msec. Default: 300 msec.
- Avg Delay:** It sets the average delay that the Jitter Buffer adds to the packets received. It is applicable for both Static and Adaptive mode of Jitter Buffer. The valid range of Average Delay is: 000–180 msec. Default: 040 msec.

Jitter Buffer Setting for Passthrough

You may configure the Jitter Buffer settings for Fax Passthrough in the same way as for Speech.

- Click **Jitter Buffer Setting for Passthrough** and configure the following parameters:

- Mode:** Select the mode of Jitter Buffer, you want to set for the Fax Passthrough from the following.
 - Static:** Jitter Buffer will receive and store the voice packets, and then send it to the DSP to process it at a fixed interval, you set as Average Delay. Once the delay is set, Jitter Buffer will not change it.
 - Full Adaptive:** Jitter Buffer will receive and store the voice packets, and then send it to the DSP to process it at required intervals depending on the network condition. This condition is controlled by the system by setting the boundaries—Minimum, Maximum, Average Delay—for the Jitter Buffer and deciding the number of packets outside these boundaries. Jitter Buffer adapts to the changing network conditions by adjusting these delays.
 - Short Adaptive:** Jitter Buffer will receive and store the voice packets, and then send it to the DSP to process it at a fixed interval, unless a crises is detected. A crises is detected when the packets are dropped by the Jitter Buffer because they arrive too early or too late. This condition is controlled by the system by setting the boundaries—Minimum, Maximum, Average Delay—for the Jitter Buffer and deciding the number of packets outside these boundaries.

Default: Short Adaptive

- Min Delay:** It sets the lower boundry for the Full and Short Adaptive mode of Jitter Buffer. The valid range of Minimum Delay is: 000–180 msec. Default: 040 msec.
- Max Delay:** It sets the upper boundry for the Full and Short Adaptive mode of Jitter Buffer. The valid range of Maximum Delay is: 000–300 msec. Default: 180 msec.
- Avg Delay:** It sets the average delay that the Jitter Buffer adds to the packets received. It is applicable for both Static and Adaptive mode of Jitter Buffer. The valid range of Average Delay is: 000–180 msec. Default: 040 msec.
- If you have completed the configuration of SIP Trunk 1, click **Submit** to save settings.
- To configure another SIP trunk, click the SIP Trunk Number tab.
- Follow the same instructions as described here to configure the next SIP trunk.

Copy Port Settings

- 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.



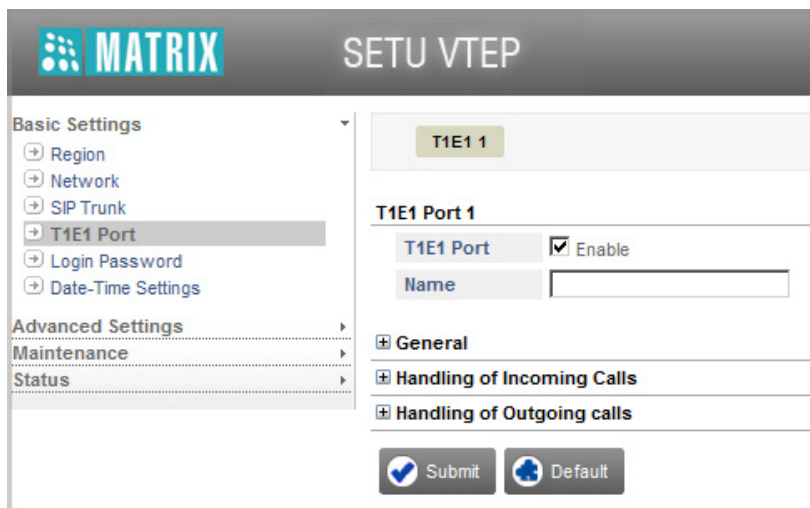
- In the **Copy SIP Trunk** box, select the number of the port you want to copy settings *From*. In the **to SIP Trunk** box, select the number of the port you want to copy the settings *To*.
- Click **OK** and close the window.
- Once you have copied the settings, you can again edit the specific parameters of the SIP Trunk, if required.

E1 Port

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

If you have connected SETU VTEP to a E1-PRI network,

- Under Basic Settings, click **T1E1 Port** link.

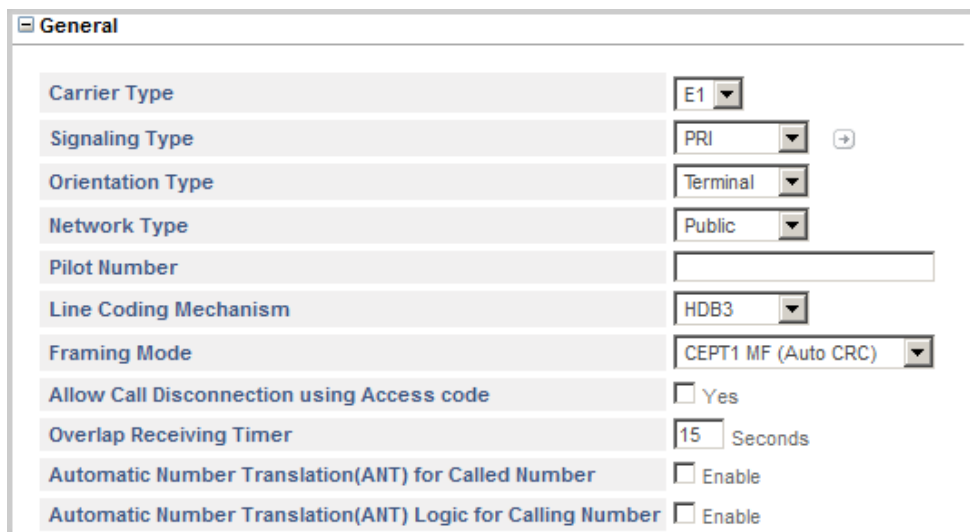


Follow the instructions provided below to configure the port parameters for the E1 connection.

- Keep the **Enable** check box enabled. If you do not want to route calls through this port clear the check box. Default: Enabled.
- You can assign a **Name** to the port. Name can be of maximum 12 characters. Default: Blank.

General

- Click **General** to expand.



- Select **Carrier Type**. Default: E1.
- Select **Signal Type**. Signal Type signifies the type of signaling to be used on E1 line. The E1 signalling supported by SETU VTEP are:
 - PRI
 - CAS
 Default: PRI

If you select **PRI** as the Signal Type, configure the **PRI Parameters**.

If you select **CAS** as the Signal Type, configure the **CAS Parameters**.

PRI Parameters

If you have selected **PRI** as **Signal Type**, click the settings icon.

The screenshot shows the 'General' configuration window. The 'Signaling Type' dropdown is set to 'PRI' and is highlighted with a red rectangle. Other settings include: Carrier Type: E1, Orientation Type: Terminal, Network Type: Public, Line Coding Mechanism: HDB3, Framing Mode: CEPT1 MF (Auto CRC), and checkboxes for 'Allow Call Disconnection using Access code', 'Automatic Number Translation(ANT) for Called Number', and 'Automatic Number Translation(ANT) Logic for Calling Number' are all unchecked.

T1E1-PRI Parameters page opens.

The screenshot shows the 'T1E1 Parameters' configuration window. It contains dropdown menus for 'ISDN Switch Variant' (set to 'ETSI NET5'), 'Caller - Type of Numbering Plan (TON)' (set to 'Unknown'), 'Caller - Numbering Plan Identification (NPI)' (set to 'ISDN Numbering'), 'Called - Type of Numbering Plan (TON)' (set to 'Unknown'), and 'Called - Numbering Plan Identification (NPI)' (set to 'ISDN Numbering'). At the bottom, there are 'Submit' and 'Close' buttons.

- Configure the following parameters:
 - **ISDN Switch Variant:** ISDN supports a variety of service provider switches. Different countries use specific type of ISDN switch. This switch is designed using ISDN standard protocol. The type of switch determines various factors such as how many ISDN devices would be handled, which B-channel will support voice, video, data, etc. SETU VTEP supports **ETSI NET5** as the ISDN PRI Variant.
 - **Caller - Type of Numbering Plan (TON):** Select the appropriate option from the following for sending the type of numbering plan of the calling party:

- Unknown
- International
- National
- Network Specific
- Subscriber
- Abbreviated
- Reserved

Default: Unknown.

- **Caller- Numbering Plan Identification (NPI):** Select the appropriate option from the following for sending the numbering plan identification of the calling party:

- Unknown
- ISDN Numbering
- Data Numbering
- Telex Numbering
- National Numbering
- Private
- Reserved

Default: ISDN Numbering.

- **Called - Type of Numbering Plan (TON):** Select the appropriate option from the following for sending the type of numbering plan of the called party:

- Unknown
- International
- National
- Network Specific
- Subscriber
- Abbreviated
- Reserved

Default: Unknown.

- **Called - Numbering Plan Identification (NPI):** Select the appropriate option from the following for sending the numbering plan identification of the called party:

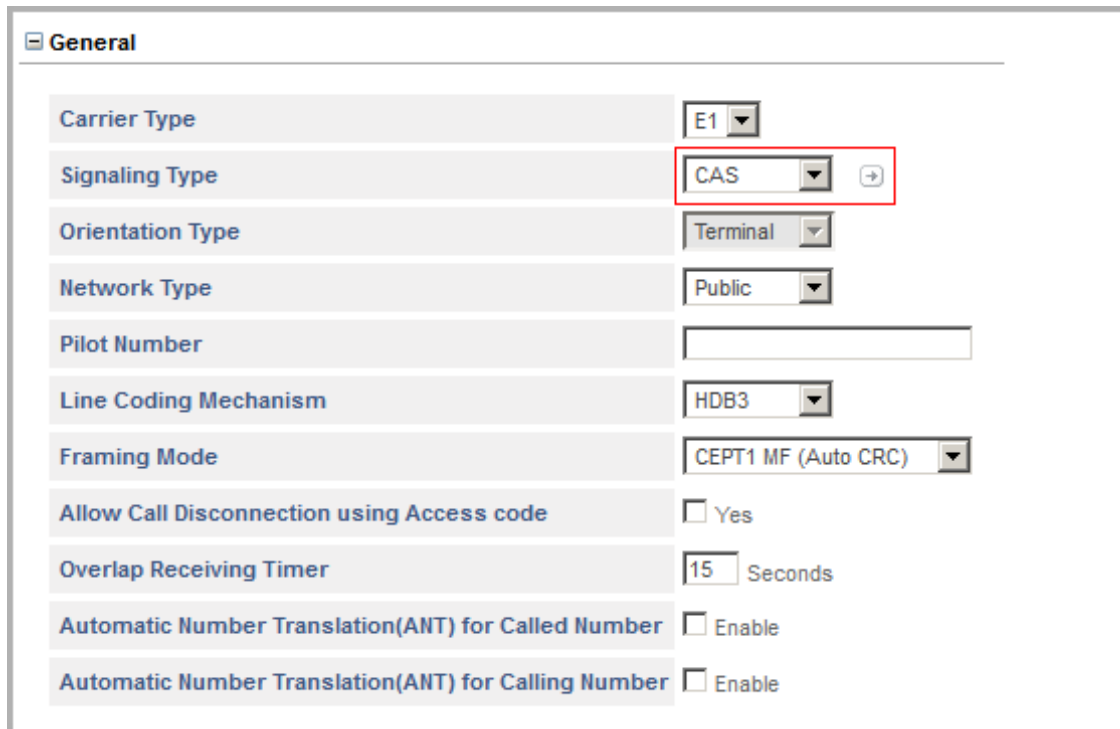
- Unknown
- ISDN Numbering
- Data Numbering
- Telex Numbering
- National Numbering
- Private
- Reserved

Default: ISDN Numbering.


- Click **Submit** to save changes.
- Close the window to return to the main page.

CAS Parameters

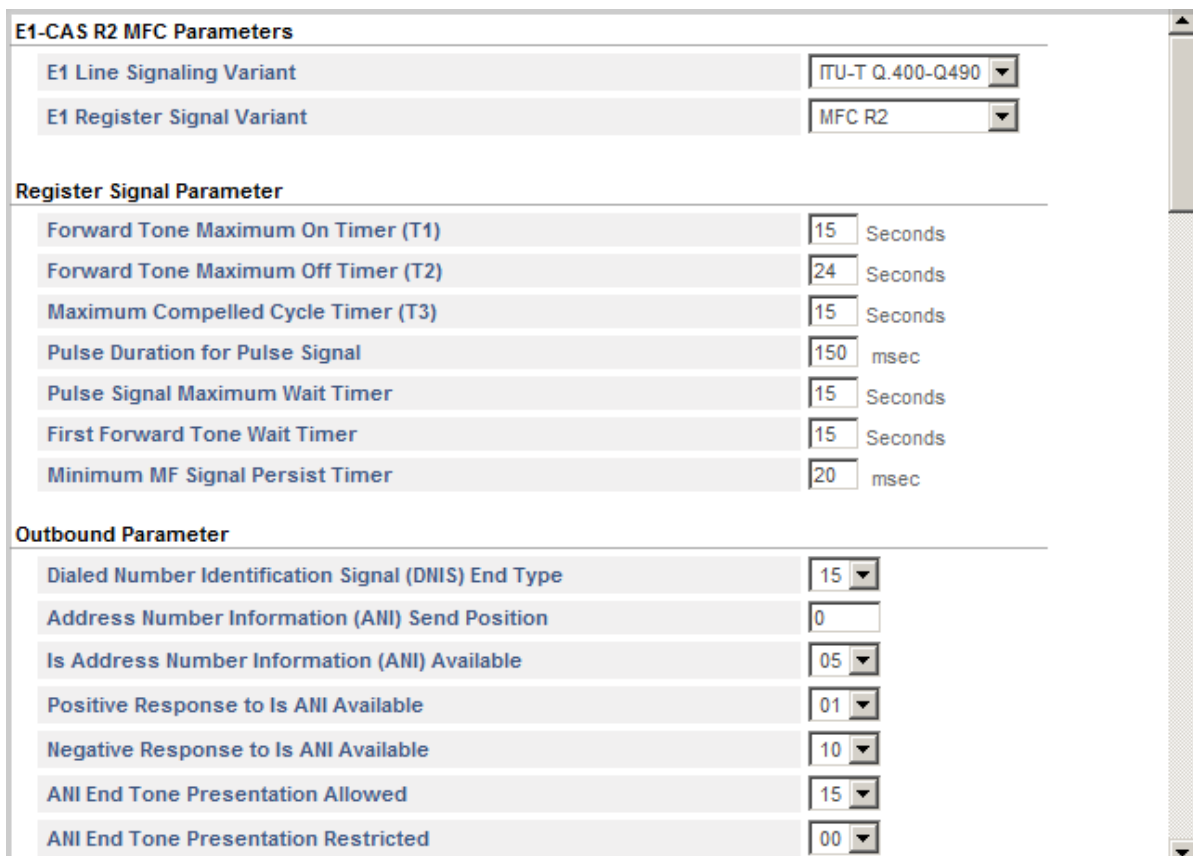
If you have selected **CAS** as **Signal Type**, click the settings icon.



General

Carrier Type	E1
Signaling Type	CAS 
Orientation Type	Terminal
Network Type	Public
Pilot Number	
Line Coding Mechanism	HDB3
Framing Mode	CEPT1 MF (Auto CRC)
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Overlap Receiving Timer	15 Seconds
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Enable
Automatic Number Translation(ANT) for Calling Number	<input type="checkbox"/> Enable

T1E1-CAS Parameters page opens.



E1-CAS R2 MFC Parameters

E1 Line Signaling Variant	ITU-T Q.400-Q490
E1 Register Signal Variant	MFC R2

Register Signal Parameter

Forward Tone Maximum On Timer (T1)	15 Seconds
Forward Tone Maximum Off Timer (T2)	24 Seconds
Maximum Compelled Cycle Timer (T3)	15 Seconds
Pulse Duration for Pulse Signal	150 msec
Pulse Signal Maximum Wait Timer	15 Seconds
First Forward Tone Wait Timer	15 Seconds
Minimum MF Signal Persist Timer	20 msec

Outbound Parameter

Dialed Number Identification Signal (DNIS) End Type	15
Address Number Information (ANI) Send Position	0
Is Address Number Information (ANI) Available	05
Positive Response to Is ANI Available	01
Negative Response to Is ANI Available	10
ANI End Tone Presentation Allowed	15
ANI End Tone Presentation Restricted	00

- Configure the following parameters:
- Keep the **E1 Line Signaling Variant** as **ITU-T Q.400-Q.490**. Default: ITU-T Q.400-Q.490.
- Keep the **E1 Register Signal Variant** as **MFC R2**. Default: MFC R2.

Register Signal Parameters

- **Forward Tone Maximum On Timer (T1) (Seconds):** This timer signifies the maximum time for which the forward signal remains ON, from the outbound end.

The range of Forward Time Maximum ON Timer is from 01 to 99 seconds. Default: 15 seconds.

- **Forward Tone Maximum Off Timer (T2) (Seconds):** This timer signifies the maximum time between two outgoing forward signals. Forward tone remains OFF during this time.

The range of Forward Time Maximum OFF Timer is from 01 to 99 seconds. Default: 24 seconds.

- **Maximum Compelled Cycle Timer (T3) (Seconds):** This timer signifies the maximum time within which one compelled signaling cycle shall end.

The range of Maximum Compelled Cycle Timer is from 01 to 99 seconds. Default: 15 seconds.

- **Pulse Duration for Pulse Signal (Milliseconds):** Backward signals A-3, A-4, A-6 and A-15 are pulsed to the outbound end. Pulse duration of these signals vary from country to country.

The range of Pulse Duration for Pulsed Signals is from 001 to 999 ms. Default: 150 ms.



It is recommended that tolerance be fixed at +/- 25 ms.

- **Pulsed Signal Maximum Wait Timer (Seconds):** This timer signifies the time for which the outbound end waits for the pulsed signal. If the pulsed signal is not received during this time, the compelling signaling is said to be complete.

The range of Pulsed Signal Maximum Wait Timer is from 01 to 99 seconds. Default: 15 seconds.

- **First Forward Tone Wait Timer (Seconds):** This timer signifies the time between receipt of line seizure signal and the first forward signal.

The range of the First Forward Tone Wait Timer is from 08 to 24 seconds. Default: 15 seconds.

- **Minimum MF Signal Persist Timer (Milliseconds):** This timer signifies the minimum time for which the forward/backward signal shall be sustained on the line by the receiving end.

The range of Minimum MF Signal Persist Timer is from 001 to 255 ms. Default: 20 ms.

Outbound Parameters

- **Dialed Number Identification Signal (DNIS) End Type:** This parameter is applicable only when DNIS length is set to 99 (i.e. variable). The outbound end indicates end of DNIS using a group I tone or using time out.

Range of DNIS End Type is from 00, 01 to 15; where 00 indicates End of DNIS as time out. 01 to 15 indicates group I tone to declare End of DNIS. Default: 15.

- **Address Number Information (ANI) Send Position:** This parameter signifies the number of DNIS digits after which address number information is to be sent. Address number information is usually sent on receiving the backward tone Send next digit or Send next ANI digit.

If send next address number information tone is received then this parameter is not applicable. But if same tone is used by the inbound end to request the next ANI digit and the next DNIS digit, ANI is sent after the number of digits as set in this field.

The range of ANI Send Position is from 00 to 99. Default: 00.

- **Is Address Number Information (ANI) Available:** This parameter indicates Group A tone (received from the inbound tone) that is to be interpreted as a question by the inbound end asking the outbound end whether the outbound end has ANI digits to be sent.

The range of Is ANI Available, Group A tone is from 01 to 15. Default: 05.

- **Positive Response to Is ANI Available:** This parameter signifies the Group 1 tone that the outbound end will send to the inbound end as a response to Is ANI Available tone from the inbound end. The tone defined in this parameter indicates the Group 1 tone with which the Outbound end will respond to the inbound end to indicate that it has ANI digits to be sent.

The range of Positive Response to Is ANI Available, Group 1 tone is from 01 to 15. Default: 01.

- **Negative Response to Is ANI Available:** This parameter signifies the Group 1 tone that the outbound end will send to the inbound end as a response to Is ANI Available tone from the inbound end. The tone defined in this parameter indicates the Group 1 tone with which the Outbound end will respond to the inbound end to indicate that it does not have ANI digits to be sent.

The range of Negative Response to Is ANI Available, Group 1 tone is from 01 to 15. Default: 10.

- **ANI End Tone Presentation Allowed:** This parameter signifies the Group 1 tone used to signify end of ANI digits with Presentation Allowed.

The range of End of ANI with Presentation Allowed, Group 1 tone is from 01 to 15. Default: 15.

- **ANI End Tone Presentation Restricted:** This parameter signifies the Group 1 tone used to signify end of ANI digits with Presentation Restricted.

The range of End of ANI with Presentation Restricted, Group 1 tone is from 01 to 15. Default: 00.

Inbound Parameters

- **Dialed Number Identification Signal (DNIS) End Type:** This parameter is applicable only when the DNIS length is set to 99 (i.e. variable). The outbound end indicates end of DNIS using a group I tone or using time out.

The range of DNIS End Type is from 00, 01 to 15; where 00 indicates End of DNIS as time out, 01 to 15 indicates group I tone to declare End of DNIS. Default: 15.

- **Dialed Number Identification Signal (DNIS) Digit Length:** This parameter signifies the number of DNIS digits required by inbound end to indicate the Called party number during MFC R2 signaling.

The range of DNIS Length is from 01 to 99. Default: 99.

- **Address Number Information (ANI) Request Position:** The inbound end may or may not request ANI digits. It may request ANI digits after receiving the first DNIS or after receiving second DNIS or even after receiving all the DNIS digits.

The range of ANI Request Position is as follows:

ANI Request	Meaning
00	Never request ANI digits
01-98	Request ANI digits on receipt of these many DNIS digits
99	Request after receiving all the DNIS digits (complete DNIS)

Default: 99.

- **Address Number Information (ANI) Length:** This parameter signifies the number of ANI digits that would be expected by the inbound side as Calling Party Number during MFC R2 signaling. This parameter at the inbound side guides the inbound register to switch from requesting ANI digits back to requesting DID digits.

The range of ANI Length is from 00 to 99. Default: 99.

- ANI Length = 00, ANI is not sent by the Outbound end.
- ANI Length = 99, ANI Length is variable.

- **Ask Address Number Information (ANI):** This parameter specifies the backward group A tone used to ask the outbound end whether it has ANI digits to be sent. This parameter is also known as **Request ANI Category**.

The range of Ask ANI is from 00 or 01 to 15. If no tone is sent by the inbound end, set this parameter to 00. For India, this parameter is set to 04. Default: 05.

- **Positive Response to Ask ANI:** This parameter specifies that the Group 1 forward tone is to be received by the inbound end from the outbound which in turn indicates that outbound end has ANI digits to be sent. This parameter is also known as ANI category.

The range of Positive Response to Ask ANI is from 01 to 15. Default: 01.

For example, In India I-1 or I-10 is sent by the outbound end. In Kuwait, I-6 is sent. This parameter cannot be zero because; Is ANI Available request will be made by the inbound end only if the country supports this protocol.

- **Negative Response to Ask ANI:** This parameter specifies the Group 1 forward tone to be received by the inbound end from the outbound which would indicate that outbound end has ANI digits to be sent. This parameter is also known as ANI category.

The range of Negative Response to Ask ANI is from 01 to 15. Default: 10.

For example, in India I-1 or I-10 is sent by the outbound end. In Kuwait, I-6 is sent. This parameter cannot be zero because; Is ANI Available request will be made by the inbound end only if the country supports this protocol.

- **ANI End Tone Presentation Allowed:** This parameter specifies the Group I tone that the inbound end should expect from the outbound end to consider End of ANI digits with information that the Presentation of ANI by the outbound end is allowed.

The range of ANI End Tone Presentation Allowed is 00 or from 01 to 15. Default: 15.

If no tone is sent, set this parameter to 00. For India use A-4, for China use A-1.

- **ANI End Tone Presentation Restricted:** This parameter specifies the group I tone that the inbound end shall expect from the outbound end to consider End of ANI digits with an information that the Presentation of ANI by the outbound end is Restricted.

The range of ANI End Tone Presentation Restricted is 00 or from 01 to 15. Default: 00.

If no tone is sent, set this parameter to 00. For India use A-4, for China use A-1.

- **Ask Calling Party Sub Category:** This parameter specifies the group 1 tone that the inbound end shall expect from the outbound end to consider End of ANI digits with an information that the Presentation of ANI by the outbound end is Restricted. Select the check box to enable. Default: Disabled.

Forward Group II

- **Ordinary Subscriber:** This parameter specifies the forward group II tone used to inform the inbound end that the calling party is an Ordinary Subscriber. This signal is sent in response to Calling Party Category signal Request from the inbound end.

Ordinary Subscriber is 00, 01 to 15. Default: 01. If this parameter is not applicable, assign 00.

- **Priority Subscriber:** This parameter specifies the forward group II tone used to inform the inbound end that the calling party is a Priority Subscriber. This signal is sent in response to Calling Party Category signal Request from the inbound end.

Priority Subscriber is 00, 01 to 15. Default: 02. If this parameter is not applicable, assign 00.

- **Maintenance Equipment:** This parameter specifies the forward group II tone used to inform the inbound end that the calling party is Maintenance equipment.

Maintenance Equipment is 00, 01 to 15. Default: 03. If this parameter is not applicable, assign 00.

- **Operator:** This parameter specifies the forward group II tone used to inform the inbound end that the calling party is Operator.

Operator is from 00, 01 to 15. Default: 05. If this parameter is not applicable, assign 00.

- **Pay Phone:** This parameter specifies the forward group II tone used to inform the inbound end that the calling party is Pay Phone (Coin box).

Pay Phone is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

- **Data Transmission:** This parameter specifies the forward group II tone used to inform the inbound end that the call is a Data Call.

Data Transmission is from 00, 01 to 15. Default: 06. If this parameter is not applicable, assign 00.

- **Interception Operator:** This parameter specifies the forward group II tone used to inform the inbound end that the call is from Interception Operator.

Interception Operator is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

Backward Group A

- **Send Next Digit (N+1) (DNIS):** This parameter specifies the backward group A tone used to request next digit. Be it ANI digit or DNIS digit.

Send next Digit range is 00, 01 to 15. Default: 01. If you do not want to use any tone, assign 00.

For India, use A-1 to signify Send DNIS Digit event.

- **Send Last But One Digit (N-1) (DNIS):** This parameter specifies the backward group A tone used to request last but one digit i.e. N-1 digit. Be it ANI digit or DNIS digit.

Send last but one digit range is 00, 01 to 15. Default: 02. If you do not want to use any tone, assign 00.

For India, use A-9 to signify Send last but one digit event.

- **Send Last But Two Digits (N-2) (DNIS):** This parameter specifies the backward group A tone used to request last but two digits i.e. N-2 digit. Be it ANI digit or DNIS digit.

Send last but two digits range is 00, 01 to 15. Default: 07. If you do not want to use any tone, assign 00.

For India, use A-7 to signify Send last but two digits event.

- **Send Last But Three Digits (N-3) (DNIS):** This parameter specifies the backward group A tone used to request last but three digits i.e. N-3 digit. Be it ANI digit or DNIS digit.

Send last but three digits range is 00, 01 to 15. Default: 08. If you do not want to use any tone, assign 00.

For India use A-8 to signify Send last but three digits event.

- **Send Caller Party Category and ANI Digit:** It is to send calling party's category requests transmission of a group II signal. Range is 00 to 15. By Default, it is 05.
- **Address Completed, Change over of Group B:** This parameter specifies the backward group A tone used to inform the inbound end that the incoming register at the inbound end needs no additional address digit and is about to go over to transmission of a group B signal conveying the status of equipment at the subscriber at the inbound end.

Address-Complete, Changeover to reception of Group B signal range is 00, 01 to 15. Default: 03. If you do not want to use any tone, assign 00.

- **Send Calling Party Category and Change to Group C:** This parameter specifies the backward group A tone used by the inbound end to request Calling Party Category from the outbound end. This tone also informs the outbound end to change to reception of Group C signal.

Send Calling Party Category and Change to Group C range is from 00, 01 to 15. Default: 00. If you do not want to use any tone, assign 00.

- **Congestion in the National Network:** This parameter specifies the backward group A tone used to inform the congestion at the inbound end.

Congestion in National Network range is 00, 01 to 15. Default: 04. If you do not want to use any tone, assign 00.

- **Send Calling Party Category:** This parameter specifies the backward group A tone used to request calling party category.

Send calling party's category range is 00, 01 to 15. Default: 05. If you do not want to use any tone, assign 00.

For India, use A-7 to signify 'Send calling party's category' event.

- **Address Completed, Charge, Set Speech Condition:** This parameter specifies the backward group A tone used to inform the inbound end that the incoming register at the inbound end needs no additional address digit, but will not send Group B signals. Also charge the call on answer.

The range of Address-Complete, Charge, Set-up Speech conditions is 00, 01 to 15. Default: 06. If you do not want to use any tone, assign 00.

- **Repeat DNIS Digits from Beginning:** This parameter specifies the backward group A tone used to inform the outbound end to send all the DNIS digits from the beginning.

The range of Repeat DNIS digits from beginning is 00, 01 to 15. Default: 00. If you do not want to use any tone, assign 00.

- **Send Next ANI Digits:** This parameter specifies the backward group A tone used to request next (first) ANI digit.

The range of Send Next ANI Digit is 00 or 01 to 15. Default: 00. If no such tone is sent, set this parameter to 00.

A few countries use different tone to request next ANI digit and next DNIS digits. For example, India uses A-4, China uses A-1.

Backward Group B

- **Send Special Information Tone:** This parameter specifies the backward group B tone used to inform the outbound end that the call cannot be made through because of reasons beyond those which are considered by the Protocol. Hence Special Information tone will be sent to the calling party. SETU VTEP will send only the Group B signal and then disconnect the call.

The range of Send Special Information Tone is from 00, 01 to 15. Default: 02. If you do not want to use any tone, assign 00.

- **Send Special Information Tone and Setup Speech Conditions:** This parameter specifies the backward group B tone used to inform the outbound end that the call cannot be made through because of reasons beyond those which are considered by the Protocol. Hence, Special information tone will be sent to the calling party and request the outbound end to setup speech conditions.

In this case, SETU VTEP shall connect the calling party to the voice message of the system informing the caller that the call cannot be connected.

The range of Send Special Information Tone and setup speech conditions is from 00, 01 to 15. Default: 02. If you do not want to use any tone, assign 00.

- **Subscriber Line Busy:** This parameter specifies the backward group B tone used to inform the outbound end that the called subscriber is busy.

Subscriber Line busy range is from 00, 01 to 15. Default: 03. If you do not want to use any tone, assign 00.

- **Subscriber Line Free, Charge:** This parameter specifies the backward group B tone used to inform the outbound end that the called subscriber is free and the call is to be charged on answer.

The range of Subscriber Line free, Charge is from 00, 01 to 15. Default: 06. If you do not want to use any tone, assign 00.

- **Subscriber Line Free, No charge:** This parameter specifies the backward group B tone used to inform the outbound end that the called subscriber is free, but the call is not to be charged on answer. This signal permits non-chargeable calls without the need for transferring **no charge** information by line signals.

The range of Subscriber Line free, NO Charge is 00, 01 to 15. Default: 07. If you do not want to use any tone, assign 00.

- **Congestion:** This parameter specifies the backward group A tone used to inform that congestion is encountered after changeover from Group-A to Group-B signals.

Congestion range is from 00, 01 to 15. Default: 04. If you do not want to use any tone, assign 00.

- **Unallocated Number:** This parameter specifies the backward group B tone used to inform the outbound end that the number received is not in use.

The range of Unallocated Number is from 00, 01 to 15. Default: 05. If you do not want to use any tone, assign 00.

- **Subscriber Line Out of Order:** This parameter specifies the backward group B tone used to inform the outbound end that the called subscriber's line is out of order.

Range of Subscriber's Line out of order is from 00, 01 to 15. Default: 08. If you do not want to use any tone, assign 00.

- **Call Rejected, No Indication:** This parameter specifies the Group B backward tone used to inform the outbound end that the call is rejected but there is no indication of cause.

Call rejected, No indication range is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

- **Alternative Answer Tone:** This parameter specifies the Group B backward tone used to inform the outbound end that the call is accepted and the speech path is made through.

Alternative Answer Tone range is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

- **Changed Number:** This parameter specifies the Group B backward tone used to inform the outbound end that the number dialed by the calling party is changed. However, this parameter is rarely used.

The range of Changed Number (announcement on line) is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

Backward Group C

- **Send Next ANI Digit:** This parameter specifies the backward group C tone to request next (even first) ANI digit from the outbound end.

The range of Send next ANI digit (Group C) is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

- **Request Transition Back to Group A and Restart from First DNIS (Group C):** This parameter specifies the backward group C tone to restart from the first DNIS and request transition to Group A.

The range of Request transition to Group A and restart from first DNIS is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

- **Address Completed, Change to Reception of Group B:** This parameter specifies the backward group C tone used to signify Address completed, change to reception of Group B signal.

The range of Address completed, change to reception of Group B signal is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

- **Congestion:** This parameter specifies the backward group C tone used to signify Congestion.

The range of Congestion is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

- **Request Transition Back to Group A and Sent Next DNIS:** This parameter specifies the backward group C tone used to signify request transition back to group A, and send next DNIS.

The range of Request transition back to group A, and send next DNIS is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

- **Request Transition Back to Group A and Repeat the Last DNIS:** This parameter specifies the backward group C tone used to signify request transition back to group A, and repeat the last DNIS.

The range of Request transition back to group A, and repeat the last DNIS is from 00, 01 to 15. Default: 00. If this parameter is not applicable, assign 00.

Line Signal Parameters

- **C & D Bits:** This parameter 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

CD Bits	Meaning (Binary Value)
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:** This parameter signifies 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:** This parameter signifies 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:** This parameter signifies 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:** This parameter signifies 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:** This parameter signifies the bit used by the network to signal metering pulses. You can select from the following options:

- None
- Bit-A
- Bit-B
- Bit-C
- Bit-D

Default: Bit-A.

- **E1 Metering Pulse Minimum Timer (Milliseconds):** This timer signifies 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. The range of E1 Metering Pulse Minimum timer is from 20ms to 1000ms. Default: 150ms.

- **Clear Back Signal:** This parameter signifies 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.

- **Release Timer (Milliseconds):** This timer signifies 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.

The range of Release Timer is from 20ms to 1000ms. Default: 400 ms.

- **Line Seizure Acknowledge Wait Timer (Milliseconds):** This timer signifies 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.

The range of Line Seizure acknowledge Wait Timer is from 0001ms to 9999 ms. Default: 200ms.

- **Release Guard Timer (Milliseconds):** This timer signifies 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.

The range of Release Guard Timer is from 0000 ms to 9999 ms. Default: 200ms.

- Click **Submit** to save changes.
- Close the window to return to the main page.
- Select the **Orientation Type** for the port as **Terminal** or **Network**, according to your installation scenario. Default: Terminal.



By default Orientation Type is set to Terminal and is non-programmable, if you select Carrier Type as E1 and Signaling Type as CAS.

If you select **Terminal** as Orientation Type, configure the following:

- Network Type
- Pilot Number
- Line Coding Mechanism
- Framing Mode
- Allow Call Disconnection using Access Code
- Overlap Receiving Timer
- Automatic Number Translation (ANT) for Called Number
- Automatic Number Translation (ANT) for Calling Number
- ["Handling of Incoming Calls"](#)
- ["Handling of Outgoing Calls"](#)

General

Carrier Type

E1

Signaling Type

PRI

Orientation Type

Terminal

Network Type

Public

Pilot Number

Line Coding Mechanism

HDB3

Framing Mode

CEPT1 MF (Auto CRC)

Allow Call Disconnection using Access code

☐ Yes

Overlap Receiving Timer

15

Seconds

Automatic Number Translation(ANT) for Called Number

☐ Enable

Automatic Number Translation(ANT) Logic for Calling Number

☐ Enable

Handling of Incoming Calls

Handling of Outgoing calls

Submit

Default

If you select **Network** as Orientation Type, configure the following:

- Pilot Number
- Line Coding Mechanism
- Framing Mode
- Allow Call Disconnection using Access Code
- Automatic Number Translation (ANT) for Called Number
- Automatic Number Translation (ANT) for Calling Number
- ["Handling of Calls"](#)

General

Carrier Type

E1

Signaling Type

PRI

Orientation Type

Network

Pilot Number

Line Coding Mechanism

HDB3

Framing Mode

CEPT1 MF (Auto CRC)

Allow Call Disconnection using Access code

☐ Yes

Automatic Number Translation(ANT) for Called Number

☐ Enable

Automatic Number Translation(ANT) for Calling Number

☐ Enable

- 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: 0 to 9, #, *. Default: Blank.
- **Line Coding Mechanism:** Line coding is a pattern that data assumes as it is propagated over a communication channel. The Line Coding mechanisms supported in SETU VTEP are:
 - AMI-Basic
 - HDB3
 Default: HDB3.
- **Framing Mode:** Framing means to form a set of 24 or 32, 8 bits time slot that is to be treated as single transmission unit. The Framing Modes supported by SETU VTEP are:
 - CEPT1 MF (No CRC)
 - CEPT1 MF (Forced CRC)
 - CEPT1 MF (Auto CRC)
 Default: CEPT1 MF (Auto CRC).
- Select the **Allow Call Disconnection using Access code**, if you want to enable the feature Disconnect Call using Access Code on the T1/E1 port. See [“Disconnecting a Call using Access Code”](#).
- You can apply Automatic Number Translation (ANT) logic on the outgoing calls made from the E1 Port.
 - To apply ANT logic on the Called Numbers, click the **Automatic Number Translation (ANT) for Called Number** check box. Default: Disabled.

General	
Carrier Type	E1
Signaling Type	PRI
Orientation Type	Terminal
Network Type	Public
Pilot Number	
Line Coding Mechanism	HDB3
Framing Mode	CEPT1 MF (Auto CRC)
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Overlap Receiving Timer	15 Seconds
Automatic Number Translation(ANT) for Called Number	<input checked="" type="checkbox"/> Enable
Use Automatic Number Translation Table	1
Pause Timer	2 Seconds
Automatic Number Translation(ANT) for Calling Number	<input type="checkbox"/> Enable

- In the **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 page will open in a new window.

1
2
3
4
5
6
7
8

Automatic Number Translation Table - 1

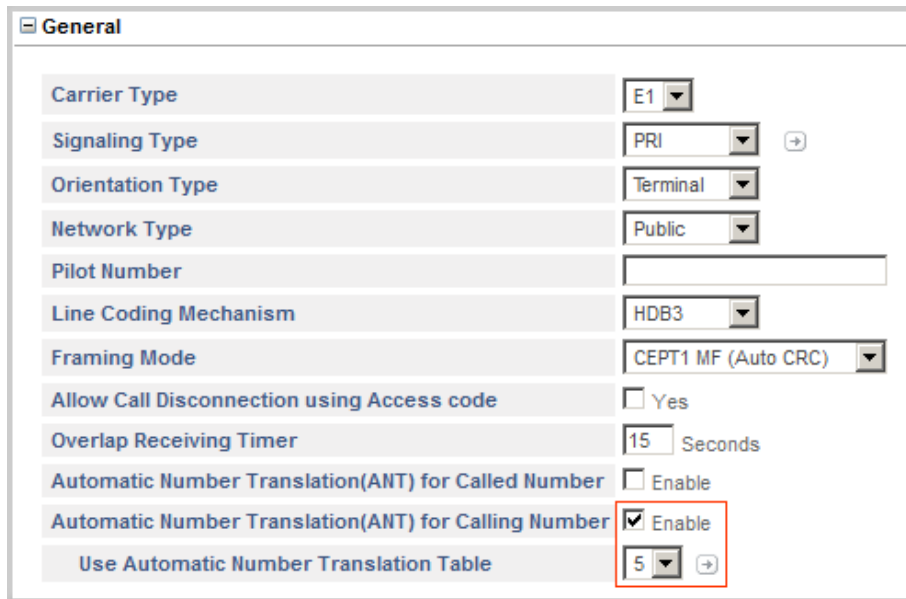
Index	Number	Strip Digit	Add Prefix
01		0	
02		0	
03		0	
04		0	
05		0	
06		0	
07		0	
08		0	
09		0	
10		0	

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 1 or any other Table (2 to 8). 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.
- Configure the **Pause Timer**, if you have configured ^ (Pause) in the Add Prefix column of the ANT Table. The valid range of the Pause Timer 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.



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

Carrier Type	E1
Signaling Type	PRI
Orientation Type	Terminal
Network Type	Public
Pilot Number	
Line Coding Mechanism	HDB3
Framing Mode	CEPT1 MF (Auto CRC)
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Overlap Receiving Timer	15 Seconds
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Enable
Automatic Number Translation(ANT) for Calling Number	<input checked="" type="checkbox"/> 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 page will open in a new window.




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.

Orientation Type - Terminal

If you select Orientation Type as **Terminal**, configure the following:

- If you have selected *Terminal* as Orientation Type, specify the **Network Type**, i.e. whether the E1 line is from a **Public** Network (telephone exchange) or from a **Private** Network (NT port of a PBX). Default: Public.
- Overlap Receiving Timer:** Overlap Receiving Timer is relevant while receiving the called party number information in overlap receiving mode. It is not relevant for the port in overlap sending mode.

Range of Overlap Receiving Timer is from 01 to 99 Seconds. Default: 15 Seconds.

Handling of Incoming Calls

T1E1 1

T1E1 Port 1

T1E1 Port ☒ Enable

Name

General

Handling of Incoming Calls

☒ Port wise

☐ Channel Number Wise

☐ MSN/DDI Number Wise

Handling of Outgoing calls

Select the method to route the incoming calls from the T1/E1 Port. SETU VTEP provides three options for **Handling of Incoming Calls**: i) Port wise, ii) Channel Number wise, iii) MSN Number wise. Default: Port wise.

- **Port wise:** Select this method to apply the call routing method for the entire port, that is on all channels and all called party numbers received.
- **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 of the 30 channels.
- **MSN 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.
 - **MSN Number 1:** Enter the first **MSN Number** (max. 24 digits) provided by your service provider. Valid digits: 0-9, # and *. Default: Blank.
 - **Total DDI Number:** Specify the **Total DDI Numbers** provided by your service provider. Valid range: 1 to 9999. Default: 0100.

For the incoming call routing option you select, click the settings icon and configure the parameters.

Port Wise Routing

Handling of Incoming Calls - Port Wise

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)

Select Destination Port for routing calls

Allowed-Denied Logic ☐ Apply

To configure Handling of Calls Portwise,

- Select the **Block calls received on this port** check box, if you do not want to route calls through this port.

Route all Incoming calls (with 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 DigitsDefault: 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	to the Fixed Destination Number
Route all Incoming calls (without CLI)	on the basis of Calling Party Number
Select Destination Port for routing calls	on the basis of DDI Number
Allowed-Denied Logic	to the Called Party Number
	after Answering the Call and Collecting the Digits

☐ Apply

Route To the Fixed Destination Number

In this method, a call received on the T1/E1 Port is routed to a fixed destination number, which is configured for the T1/E1 Port.

Handling of Incoming Calls - Port Wise

Block calls received on this port	<input type="checkbox"/> Yes
Route all Incoming calls (with CLI)	to the Fixed Destination Number
Block Calls received without CLI on this port	<input type="checkbox"/> 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

If you select this method,

- 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. Default: **Blank**.
- Click **Submit** to save your setting.





Route On the basis of Calling Party Number

In this method, a call received on the T1/E1 Port is routed to a specific number, as per the calling party's number.




If you select this method,



- Click the settings icon and configure the table **Calling Number Based** for the T1/E1 Port.




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 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	<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
First Digit Wait Timer	7 Seconds
Inter Digit Wait Timer	5 Seconds
End Of Dialing Digit	# 
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

 Submit  Default  Close

The Calling Number Based Table page opens in a new window.

The screenshot shows a web-based configuration window titled "T1E1 Port - Destination Number Determination: Calling Number Based". At the top, there are five tabs: "1-100" (selected), "101-200", "201-300", "301-400", and "401-499". Below the tabs is a table with three columns: "Index", "Calling Number", and "Destination Number". The table has 15 rows, indexed from 001 to 015. To the right of the table is a vertical scrollbar. At the bottom of the window are three buttons: "Submit" (with a checkmark icon), "Default All" (with a plus icon), and "Close" (with an X icon).

Index	Calling Number	Destination Number
001		
002		
003		
004		
005		
006		
007		
008		
009		
010		
011		
012		
013		
014		
015		

- Configure following parameters in this table:
 - **Calling Number:** Enter the calling party numbers in the column Calling Numbers. Calling numbers may consist of a maximum of 24 characters. Default: Blank.
 - **Destination Number:** For each calling party number, enter a corresponding destination number in the column Destination Numbers. 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.

When there is an incoming call on the T1/E1 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 port.
- **If no match found in the Calling Party Number Table**, you may select any of the following options for processing the call:
 - to a Fixed Destination Number, see ["Route To the 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, ["Route After Answering the Call and Collecting the Digits"](#)

Default: after Answering the Call and Collecting the Digits

- Click **Submit** to save and close the window to return to the main page.

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



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 selected for IP Dialing. (Refer “IP Dialing” feature for more details).

Route On the basis of DDI Number

In this method, a call is routed to a specific number as per the DDI number received in the SETUP message of the T1/E1 Port.

If you select this option,

- Click the settings icon and configure the table **DDI Number Based** for the T1/E1 Port.

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

The DDI Number Based Table page opens in a new window.

1-100101-200201-300301-400401-500501-600601-700701-800

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"/>	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

☒ Submit

☐ Default All

☐ Close

- Configure the following:
 - DDI Number
 - Destination Number
 - Reverse DDI
- 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*. See [“Destination Number Determination”](#) under *Advanced Settings*.



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

Route 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

In this method, a call received on the T1/E1 port is routed to a specific number depending upon the called party number received in the SETUP Message of the T1/E1 port.

Route After Answering the Call and Collecting the Digits

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
First Digit Wait Timer	7 Seconds
Inter Digit Wait Timer	5 Seconds
End Of Dialing Digit	#
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: ☐ Apply

Submit Default Close

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.

If you select this option, configure the following:

- **First Digit Wait Timer (FDWT):** Define the number of seconds the system should wait for the user to dial the destination number. Default: 7 seconds. You may change this timer, if required. The valid range of this timer is 01 to 99 seconds.
- **If No Digit dialed during First Digit Wait Timer (FDWT)** by the user, you may either **Disconnect the Call** or **Use Fixed Destination Number** to route the call. 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. Default: Blank.

You may configure the following options as end-of-dialing indication:

- **Inter Digit Wait Timer:** Define the number of seconds the system should wait while receiving the dialing digits, to consider it as end-of-dialing. You may change this timer, if required. The valid range is 01 to 99 seconds. Default: 05 seconds.
- **End of Dialing Digit (Termination digits):** Select whether the system should consider # or * as termination digit to detect end of dialing. Default: #
- **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. The 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 you want to enable [“PIN Authentication”](#), select the **Prompt caller to enter PIN** check box.
- Select the **Allow making New Call using Access code**, if you want to enable the feature Making New Call using Access Code on the T1/E1 port. See [“Making a New Call using Access Code”](#).
- Click **Submit** to save settings.
- Select the **Block calls received without CLI on this port** check box, if you do not want to route calls received without CLI through this port. Default: Disabled.

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 checked="" type="checkbox"/> Yes
Select Destination Port for routing calls	Fixed
Allowed-Denied Logic	<input type="checkbox"/> Apply

Submit
 Default
 Close

Route all Incoming calls (without CLI)

- To **Route all Incoming calls (without CLI)**, you may select from any of the following methods. 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	to a Fixed Destination Number on the basis of DDI Number
Allowed-Denied Logic	to the Called Party Number after Answering the Call and Collecting the Digits

Submit Default Close

- to a Fixed Destination Number, see [“Route To the 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, [“Route After Answering the Call and Collecting the Digits”](#).

Destination Port for routing calls

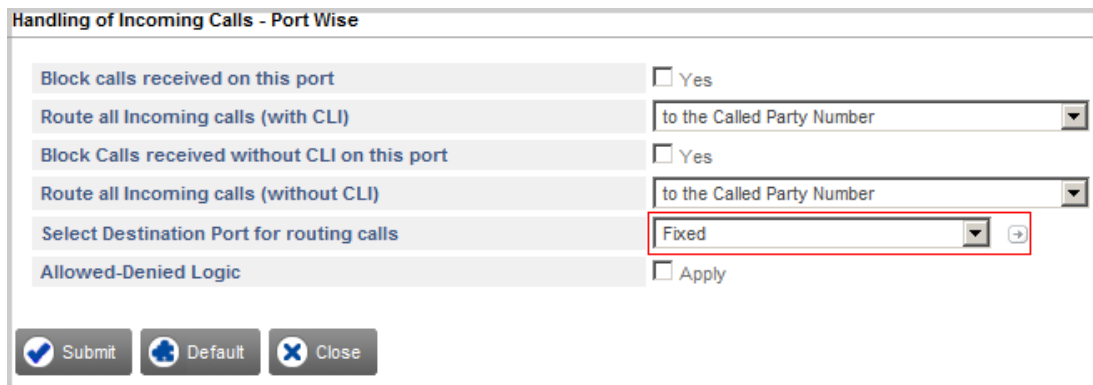
- You must select the Destination Port for routing calls for the port/channel/MSN Number. You may select from any of the following options:
 - Fixed
 - On the basis of Destination Number
 - On the basis of Calling Party Number
- Default: Fixed

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	Fixed

Submit Default Close

Fixed



Handling of Incoming Calls - Port Wise

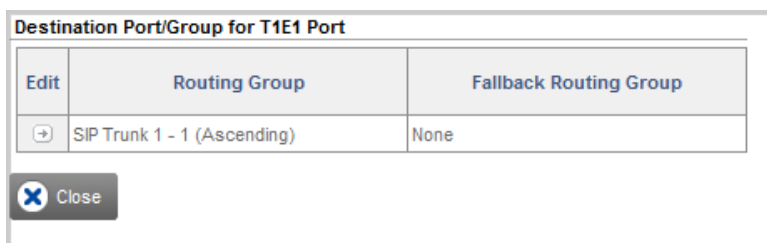
Block calls received on this port	<input type="checkbox"/> Yes
Route all Incoming calls (with CLI)	to the Called Party Number
Block Calls received without CLI on this port	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number
Select Destination Port for routing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

Submit Default Close

In this method, calls received on the T1/E1 Port are routed to a fixed destination port, irrespective of the number dialed on the source port.

If you select this option,

- Click the settings icon. A new window opens.



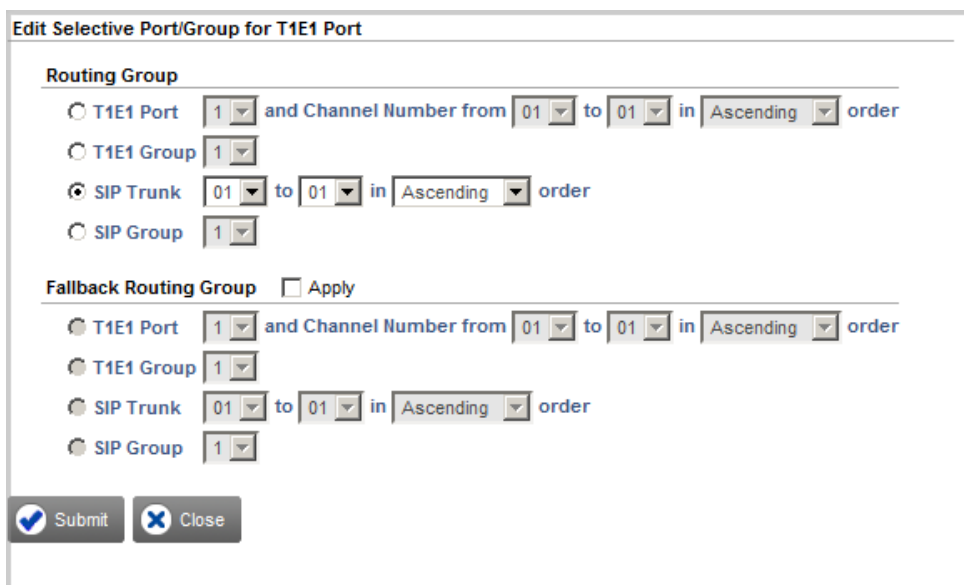
Destination Port/Group for T1E1 Port

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

Close

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

- Click **Edit**, if you want to change the default Routing Group options. A new 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 01 to 01 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 01 to 01 in Ascending order

☐ SIP Group 1

Submit Close

- Create the **Routing Group**.

- To create a routing group of *sequential* E1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* E1 channels as members, select a **T1E1 Group** Number.

Click the settings icon and create the E1 Group. See [“Group”](#) for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group** Number.

Click the settings icon and create the SIP Group. See [“Group”](#) for further instructions.

- To create the **Fallback Routing** Group,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and the SIP Trunks.
- Click **Submit** to save changes. The **Edit** window closes.
- The Routing and Fallback Groups you created appear. Close the window to return to the main page.

On the basis of Destination 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

On the basis of Destination Number

Allowed-Denied Logic

☐ Apply

✓ Submit



⚙ Default

✕ Close

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.


If you select this option, you must configure the **Destination Number Based** table.


- Click the settings icon. A new window opens.


T1E1 Port - Destination Port Determination - Destination Number Based						
	Edit	Destination Number	Minimum Digits	Maximum Digits	Routing Group	Fallback Routing Group
		No Match Found	3	16	SIP Trunk 1 - 1 (Ascending)	None

Total Records : 1

1

 Add

 Delete

 Close

- Click **Add** to add an entry. A new window opens.

Add Entry

Destination Number:

Minimum Digits:

Maximum Digits:

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 the **Destination Number** field, enter the number (max. 24 characters) you expect callers to dial. Valid digits: 0 to 9, *, #, (dot). Default: blank.
- In the **Minimum Digits** field, enter the minimum digits for the system to consider the destination number as a valid number. Range: 01 to 24. Default: 03.

If the dialed number string is less than the configured minimum length, the call will be rejected.

- In the **Maximum Digits** field, enter the maximum number of digits of the destination number the caller must dial for the system to route the call.

If the number string dialed by the caller exceeds the maximum length configured, the system will strip off the extra digits, and route the call. Maximum length range: 01 to 24. Default: 16.

- Create the **Routing Group**.
 - To create a routing group of *sequential* E1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* E1 channels as members, select a **T1E1 Group Number**.

Click the settings icon and create the E1 Group. See [“Group”](#) for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group Number**.

Click the settings icon and create the SIP Group. See [“Group”](#) for further instructions.

- To create the **Fallback Routing** Group,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and SIP Trunks.
- Click **Submit** to save changes and close the window.
- The Routing and Fallback Groups you created appear.
- To edit an entry, click **Edit**, a new window opens. Make the changes as per your requirement and click **Submit**.
- To delete an entry, select the check box and click **Delete**.
- Close the window to return to the main page.

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

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)

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

In this method, Incoming calls on the source port will be routed to the destination port on the basis of the calling party's number.




If you select this option, you must configure the **Calling Number Based** table.

- Click the settings icon. A new window opens.

T1E1 Port - Destination Port Determination - Calling Number Based				
	Edit	Calling Number	Routing Group	Fallback Routing Group
		No Match Found	SIP Trunk 1 - 1 (Ascending)	None

Total Records : 1

1

 Add
  Delete
  Close

- Click **Add** to add an entry. A new window opens.

Add Entry

Calling Number

Routing Group

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

☐ T1E1 Group 1

☐ SIP Trunk 01 to 01 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 01 to 01 in Ascending order

☐ SIP Group 1

- In the **Calling Number** field, enter numbers (max. 24 characters) from which you expect calls to be received. Valid digits: 0 to 9, *, #, (dot). Default: blank.
- Create the **Routing Group**.
 - To create a routing group of *sequential* E1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* E1 channels as members, select a **T1E1 Group** Number.

Click the settings icon and create the E1 Group. See [“Group”](#) for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group** Number.

Click the settings icon and create the SIP Group. See [“Group”](#) for further instructions.

- To create the **Fallback Routing** Group,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and SIP Trunks.
- Click **Submit** to save changes and close the window.
- The Routing and Fallback Groups you created appear.
- To edit an entry, click **Edit**, a new window opens. Make the changes as per your requirement and click **Submit**.
- To delete an entry, select the check box and click **Delete**.
- Close the window to return to the main page.

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

Allowed - Denied Logic (Toll-Control)

With the Allowed-Denied Numbers feature you can permit and restrict the dialing of particular numbers from the T1/E1 Port.

Allowed Denied Number Logic makes use of two predefined Number lists:

- **Allowed Numbers List:** This is the list of numbers that can be dialed out from T1/E1 Port. By default, List Number 1 is assigned to the T1/E1 Port.
- **Denied Numbers List:** This list contains the numbers that are to be restricted from being dialed out from the T1/E1 Port. By default, List Number 2 is assigned to the T1/E1 Port.

Both lists must be programmed first and then applied on the T1/E1 Port. For instructions see [“Number Lists”](#).

To apply Allowed - Denied Logic on the T1/E1 Port,

- Click the Allowed - Denied Logic **Enable** check box.

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 Calling Party Number
Allowed-Denied Logic	<input checked="" type="checkbox"/> Apply
Allowed Numbers List	01
Denied Numbers List	02

Submit Default Close

- As **Allowed Numbers List**, select the number of the Number List, which you have programmed as Allowed Number List. If you retained the default Number List 1, select the same list number.

If you have not configured the Allowed Numbers List,

- Click the settings icon.

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

Submit Default Close

- The Number List page will open in a new window.
- You may configure the default Number List 1 or any other Number List as Allowed Number List.
- Click **Submit** to save Number List and close the window.
- Return to Allowed - Denied Logic parameter and assign the Number List you configured.
- Denied Number List:** Select the number of the Number List, which you have programmed as Denied Number List. If you retained the default Number List 2, select the same list number. If you have not configured the Denied Number List,

- Click the settings icon.
 - The Number List page will open in a new window.
 - You may configure the default Number List 2 or any other Number List as Denied Number List.
 - Click **Submit** to save Number List and close the window.
 - Return to Allowed - Denied Logic parameter and assign the Number List you configured.
- Click **Submit** to apply the changes. See [“Allowed - Denied Logic”](#) under [“Number Lists”](#).

Channel Number Wise Routing

Channel 1 Channel 2 Channel 3 Channel 4 Channel 5 Channel 6 Channel 7 Channel 8 Channel 9

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 Close

If you have selected Channel Number Wise method for Handling of Incoming Calls, you must configure the following parameters for each channel:

- Block calls received on this channel
- Route all Incoming calls (with CLI), see [“Route all Incoming calls \(with CLI\)”](#) under [“Port Wise Routing”](#).
- Block calls received without CLI on this channel.
- Route all Incoming calls (without CLI) see [“Route all Incoming calls \(without CLI\)”](#) under [“Port Wise Routing”](#).
- Select Destination Port for routing calls, see [“Destination Port for routing calls”](#).
- Allowed-Denied Logic, see [“Allowed - Denied Logic \(Toll-Control\)”](#).

MSN Number Wise Routing

MSN 1 MSN 2 MSN 3 MSN 4 MSN 5 MSN 6 MSN 7 MSN 8

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 Close

If you have selected MSN Number Wise method for Handling of Incoming Calls, you must configure the following parameters for each MSN Number:

- MSN Number 1
- Total DDI Numbers
- Block calls received on this MSN number
- Route all Incoming calls (with CLI), see [“Route all Incoming calls \(with CLI\)”](#) under [“Port Wise Routing”](#).
- Block Calls received without CLI on this MSN number.
- Route all Incoming calls (without CLI), see [“Route all Incoming calls \(without CLI\)”](#) under [“Port Wise Routing”](#).
- Select Destination Port for routing calls, see [“Destination Port for routing calls”](#).
- Allowed-Denied Logic, see [“Allowed - Denied Logic \(Toll-Control\)”](#).

Handling of Outgoing Calls

T1E1 1

T1E1 Port 1

T1E1 Port ☒ Enable

Name

General

Handling of Incoming Calls

Handling of Outgoing calls

Block calls through this port ☐ Yes

Route Return calls of unconnected calls to Original Caller ☐ Yes

Connect Source Port when number is outdialed ☐ Yes

Connect Source Port when Progress Indicator is received on T1E1 Port ☐ Yes

☒ Submit ☐ Default

When **T1E1 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 though 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, this incoming call is placed to the original calling party. You can change the duration of this timer and delete records of such calls. 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 feature [“Making a New Call using Access Code”](#) to users.*

- Click **Submit** to save settings.

Orientation Type - Network

If you select **Network** as Orientation Type, configure the following:

Handling of Calls

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

The screenshot shows a configuration window for 'T1E1 1'. Under 'T1E1 Port 1', there is a 'T1E1 Port' checkbox which is checked, and an 'Enable' checkbox which is also checked. Below these is a 'Name' input field. The 'Handling of Calls' section has two radio button options: 'Port wise' (which is selected) and 'Channel Number Wise'. At the bottom of the window are two buttons: 'Submit' (with a checkmark icon) and 'Default' (with a plus icon).

SETU VTEP provides two options for **Handling of Calls**, when the port is configured as Network:

- **Port wise:** Select this method to apply the call routing method for the entire port. See [“Port Wise Routing”](#).

Handling of Calls - Portwise

Block calls received on this port	<input type="checkbox"/> Yes
Dial Tone Timer	<input type="text" value="7"/> Seconds
Inter Digit Wait Timer	<input type="text" value="5"/> Seconds
End Of Dialing Digit	# <input type="button" value="v"/>
Maximum Number of digits that can be dialed by the caller	24 <input type="button" value="v"/>
Select Destination Port for routing calls	Fixed <input type="button" value="v"/> <input type="button" value="➔"/>
Allowed-Denied Logic	<input type="checkbox"/> Apply

- **Channel Number wise:** Select this method to apply a different call routing method for each of the 30 channels. See [“Channel Number Wise Routing”](#).

Channel 2
Channel 3
Channel 4
Channel 5
Channel 6
Channel 7
Channel 8

Handling of Calls - Channel Numberwise

Block calls received on this channel	<input type="checkbox"/> Yes
Dial Tone Timer	<input type="text" value="7"/> Seconds
Inter Digit Wait Timer	<input type="text" value="5"/> Seconds
End Of Dialing Digit	# <input type="button" value="v"/>
Maximum Number of digits that can be dialed by the caller	24 <input type="button" value="v"/>
Select Destination Port for routing calls	Fixed <input type="button" value="v"/> <input type="button" value="➔"/>
Allowed-Denied Logic	<input type="checkbox"/> Apply

- For the method you select, **Portwise** or **Channel Numberwise**, configure the following parameters:
 - **Block calls received on this port/channel:** Select this check box, if you do not want to route calls through this port/channel.
 - **Dial Tone Timer:** This is the time for which SETU VTEP will play Dial Tone to the caller. Default:7 seconds. At the end of this timer, the system plays error tone to the caller.
 - **Inter Digit Wait Timer:** Define the number of seconds the system should wait while receiving the dialing digits, to consider it as end-of-dialing. You may change this timer, if required.The valid range is 01 to 99 seconds. Default: 5 seconds.
 - **End of Dialing Digit (Termination digits):** Select whether the system should consider # or * as termination digit to detect end of dialing. Default: #
 - **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. The valid range is 01 to 24 digits. Default: 24 digits.

- **Select Destination Port for routing calls:** Select the desired method for destination port determination - Fixed, on the basis of Calling Party Number, on the basis of Destination Number. See [“Destination Port for routing calls”](#).
- **Allowed - Denied Logic:** To permit and restrict the dialing of particular numbers from the T1/E1 Port, enable Allowed-Denied Logic and configure the Allowed and Denied Number Lists. See [“Allowed - Denied Logic \(Toll-Control\)”](#).
- Click **Submit** to save your changes.

T1 Port

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

If you have connected SETU VTEP to a T1-PRI network,

- Under Basic Settings, click **T1E1 Port** link.

The screenshot shows the MATRIX SETU VTEP configuration interface. On the left is a sidebar with a menu under 'Basic Settings' including Region, Network, SIP Trunk, T1E1 Port (selected), Login Password, and Date-Time Settings. Below this are sections for Advanced Settings, Maintenance, and Status. The main panel on the right is titled 'T1E1 1' and 'T1E1 Port 1'. It contains a 'T1E1 Port' label, an 'Enable' checkbox which is checked, and a 'Name' text input field. Below these are expandable sections for 'General' and 'Handling of Calls'. At the bottom are 'Submit' and 'Default' buttons.

Follow the instructions provided below to configure the port parameters for the T1 connection.

- Keep the **Enable** check box enabled. If you do not want to route call through this port clear the check box. Default: Enabled.
- You can assign a **Name** to the port. Name can be of maximum 12 characters. Default: Blank.

General

- Click **General** to expand.

The screenshot shows a configuration window titled "General". It contains the following fields and options:

Carrier Type	T1
Signaling Type	PRI
Orientation Type	Terminal
Line Buildout Parameter	0-133 ft
Network Type	Public
Pilot Number	
Line Coding Mechanism	AMI Basic
Framing Mode	SF (D4)
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Overlap Receiving Timer	15 Seconds
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Enable
Automatic Number Translation(ANT) for Calling Number	<input type="checkbox"/> Enable

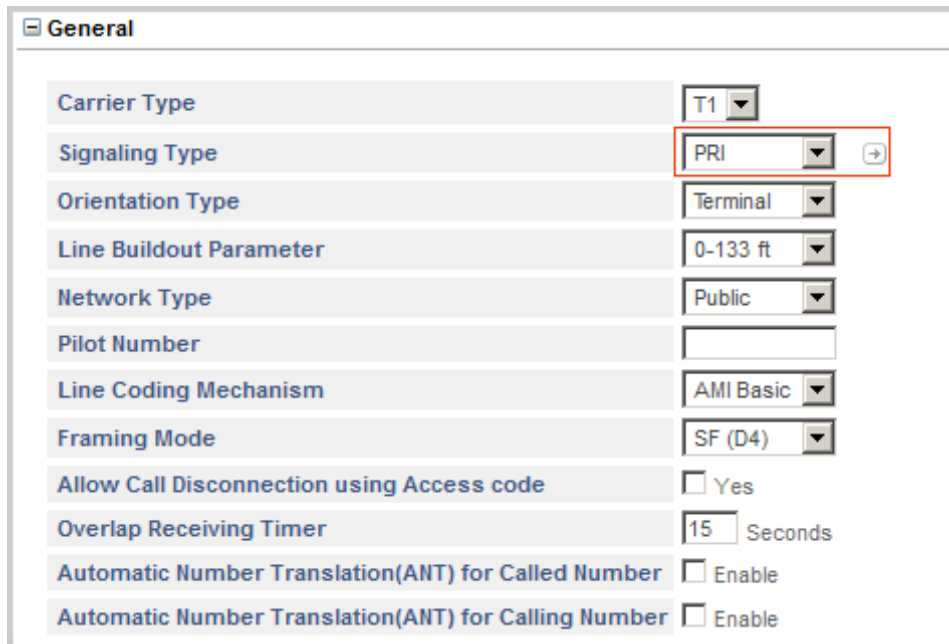
- Select **T1** as the **Carrier Type**. Default: E1.
- Select **Signaling Type**. Signal Type signifies the type of signaling to be used on the T1 line. SETU VTEP supports the following types of signaling:
 - PRI
 - RBSDefault: PRI

If you select **PRI** as the Signal Type, configure the **PRI Parameters**.

If you select **RBS** as the Signal Type, configure the **RBS Parameters**.

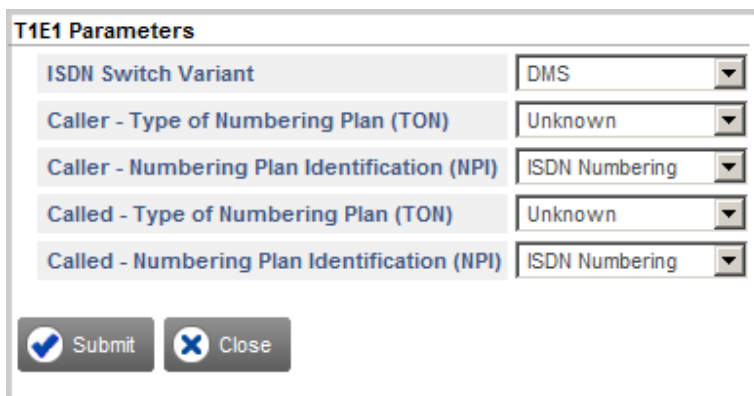
PRI Parameters

If you have selected **PRI** as **Signal Type**, click the settings icon.



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

Parameter	Value
Carrier Type	T1
Signaling Type	PRI
Orientation Type	Terminal
Line Buildout Parameter	0-133 ft
Network Type	Public
Pilot Number	
Line Coding Mechanism	AMI Basic
Framing Mode	SF (D4)
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Overlap Receiving Timer	15 Seconds
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Enable
Automatic Number Translation(ANT) for Calling Number	<input type="checkbox"/> Enable



The screenshot shows a 'T1E1 Parameters' configuration window with the following fields and values:

Parameter	Value
ISDN Switch Variant	DMS
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

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

- Configure the PRI parameters:
 - **ISDN Switch Variant:** ISDN supports a variety of service provider switches. Different countries use specific type of ISDN switch. This switch is designed using ISDN standard protocol. The type of switch determines various factors such as how many ISDN devices would be handled, which B-channel will support voice, video, data etc. SETU VTEP supports the following as the ISDN Switch Variant.
 - DMS
 - US NI2
 - ATT 5ESSDefault: DMS.
 - **Send Calling Party Name as FACILITY IE in SETUP message:** Select this check box, if you want the system to send the Calling party name received from the source port in the FACILITY header of the SETUP message. Default: Disabled.

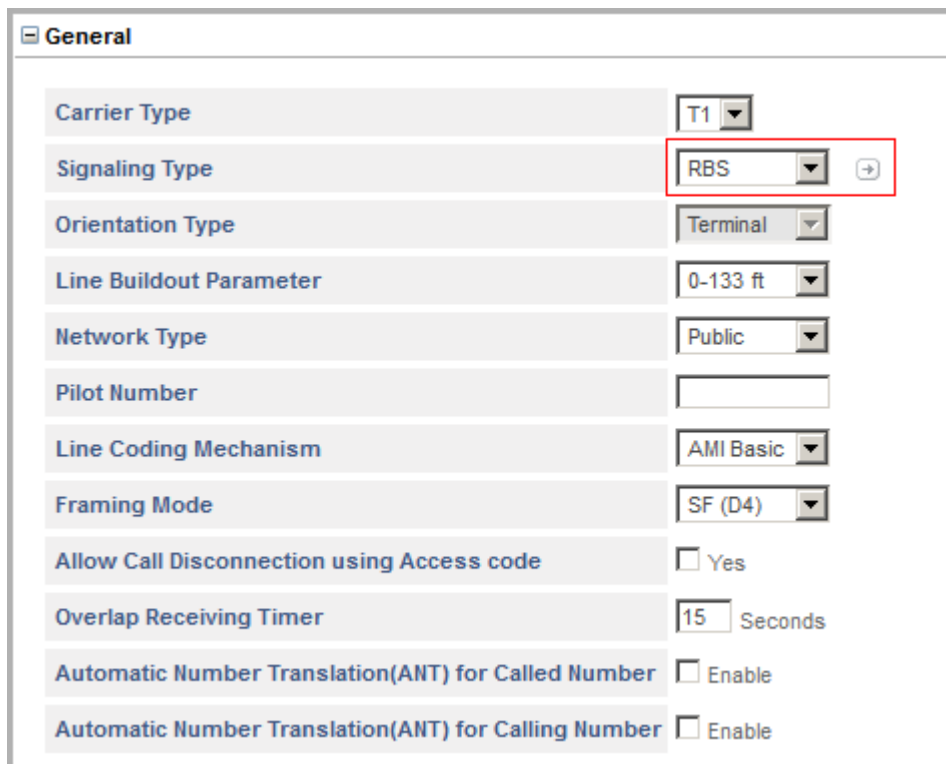


Send Calling Party Name as FACILITY IE in SETUP message parameter is applicable only if you select US NI2 as ISDN Switch Variant.

- **Caller - Type of Numbering Plan (TON):** Select the appropriate option from the following for sending the type of numbering plan of the calling party:
 - Unknown
 - International
 - National
 - Network Specific
 - Subscriber
 - Abbreviated
 - ReservedDefault: Unknown.
- **Caller- Numbering Plan Identification (NPI):** Select the appropriate option from the following for sending the numbering plan identification of the calling party:
 - Unknown
 - ISDN Numbering
 - Data Numbering
 - Telex Numbering
 - National Numbering
 - Private
 - ReservedDefault: ISDN Numbering.
- **Called - Type of Numbering Plan (TON):** Select the appropriate option from the following for sending the type of numbering plan of the called party:
 - Unknown
 - International
 - National
 - Network Specific
 - Subscriber
 - Abbreviated
 - ReservedDefault: Unknown.
- **Called - Numbering Plan Identification (NPI):** Select the appropriate option from the following for sending the numbering plan identification of the called party:
 - Unknown
 - ISDN Numbering
 - Data Numbering
 - Telex Numbering
 - National Numbering
 - Private
 - ReservedDefault: ISDN Numbering.
- Click **Submit** to save changes.
- Close the window to return to the main page.

RBS Parameters

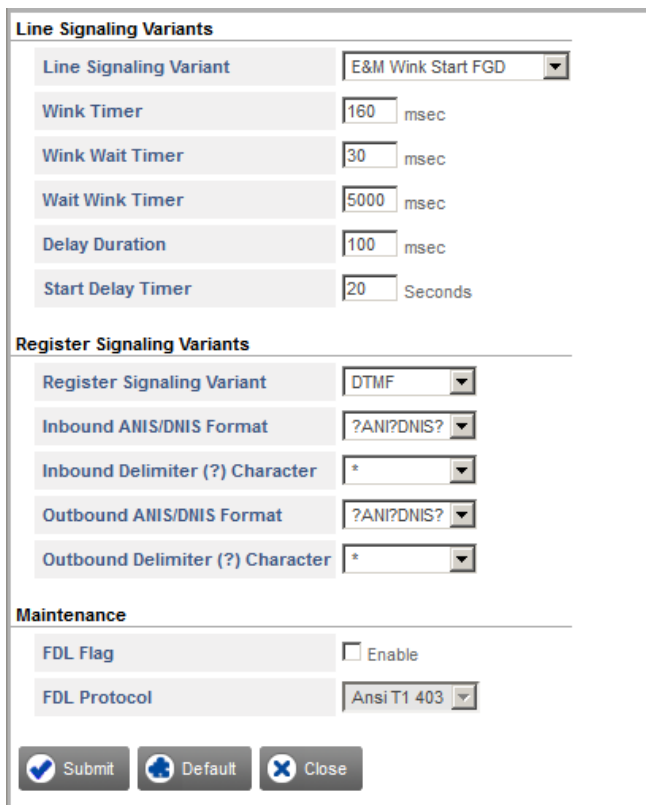
If you have selected **RBS** as **Signaling Type**, click the settings icon and configure the RBS parameters.



The screenshot shows a configuration window titled "General". It contains several settings for RBS parameters. The "Signaling Type" dropdown is highlighted with a red box and shows "RBS" selected. Other settings include "Carrier Type" (T1), "Orientation Type" (Terminal), "Line Buildout Parameter" (0-133 ft), "Network Type" (Public), "Pilot Number" (empty), "Line Coding Mechanism" (AMI Basic), "Framing Mode" (SF (D4)), "Allow Call Disconnection using Access code" (checkbox), "Overlap Receiving Timer" (15 Seconds), "Automatic Number Translation(ANT) for Called Number" (checkbox), and "Automatic Number Translation(ANT) for Calling Number" (checkbox).

Carrier Type	T1
Signaling Type	RBS
Orientation Type	Terminal
Line Buildout Parameter	0-133 ft
Network Type	Public
Pilot Number	
Line Coding Mechanism	AMI Basic
Framing Mode	SF (D4)
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Overlap Receiving Timer	15 Seconds
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Enable
Automatic Number Translation(ANT) for Calling Number	<input type="checkbox"/> Enable

T1E1-RBS Parameters page opens.



The screenshot shows a configuration window titled "Line Signaling Variants". It contains settings for "Line Signaling Variant" (E&M Wink Start FGD), "Wink Timer" (160 msec), "Wink Wait Timer" (30 msec), "Wait Wink Timer" (5000 msec), "Delay Duration" (100 msec), and "Start Delay Timer" (20 Seconds). Below this is a section for "Register Signaling Variants" with settings for "Register Signaling Variant" (DTMF), "Inbound ANIS/DNIS Format" (?ANI?DNIS?), "Inbound Delimiter (?) Character" (*), "Outbound ANIS/DNIS Format" (?ANI?DNIS?), and "Outbound Delimiter (?) Character" (*). At the bottom is a "Maintenance" section with "FDL Flag" (checkbox) and "FDL Protocol" (Ansi T1 403). The window ends with "Submit", "Default", and "Close" buttons.

Line Signaling Variant	E&M Wink Start FGD
Wink Timer	160 msec
Wink Wait Timer	30 msec
Wait Wink Timer	5000 msec
Delay Duration	100 msec
Start Delay Timer	20 Seconds

Register Signaling Variant	DTMF
Inbound ANIS/DNIS Format	?ANI?DNIS?
Inbound Delimiter (?) Character	*
Outbound ANIS/DNIS Format	?ANI?DNIS?
Outbound Delimiter (?) Character	*

Maintenance	
FDL Flag	<input type="checkbox"/> Enable
FDL Protocol	Ansi T1 403

Submit Default Close

Line Signaling Variants

- **Line Signaling Variant:** Select the T1 Line Signaling Variant from following options:
 - FXS Loop Start
 - FXO Loop Start
 - FXS Ground Start
 - FXO Ground Start
 - E&M Immediate Dial/Start
 - E&M Wink Start
 - E&M Wink Start FGDDefault: E&M Wink Start FGD.
- **Wink Timer:** Wink timer refers to the momentary Off-Hook condition to acknowledge end of making an outgoing call. The Wink Timer ranges from 001 ms to 999 ms. Default: 160 msec.
- **Wink Wait Timer:** Wink Wait Timer signifies the maximum time the system should wait before sending a wink start signal after an incoming seizure is detected. Wink Wait Timer ranges from 0001 to 9999 msec. Default: 30msec.



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

- **Wait Wink Timer:** Wait Wink Timer signifies the time for which SETU VTEP will wait for receiving the DNIS after sending the outgoing seizure signal. Wait Wink Timer ranges from 001 to 999 msec. Default: 5000 msec.



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

- **Delay Duration:** This duration signifies the time after which the DNIS information is to be sent while making an outgoing call. Range of the Delay Duration is from 0001 to 9999 msec. Default: 100 msec.
- **Start Delay Timer:** Start Delay Timer 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). The Start Delay Timer ranges from 0001 to 9999 ms. Default: 20 msec.

Register Signaling Variant

- **Register Signaling Variant:** Select the Register Signaling Variant for T1/E1 Ports from the following options:
 - DTMF
 - Decadic
 - MFC R2
 - MFC R1Default: DTMF.
- **Inbound ANI/DNIS Format:** Select the Inbound ANI/DNIS Format for T1/E1 Ports from the following options:
 - ANI
 - DNIS
 - ?ANI?
 - ?DNIS?
 - ?ANI?DNIS?
 - ?DNIS?ANI?Default: ?ANI?DNIS?.

- **Inbound Delimiter (?) Character:** Define the Inbound Delimiter Character in this field. Characters supported in this field are 0-9, #, *, A, B, C and D. Default: *
- **Outbound ANI/DNIS Format:** Select the Outbound ANI/DNIS Format for T1/E1 Port from the following options:
 - ANI
 - DNIS
 - ?ANI?
 - ?DNIS?
 - ?ANI?DNIS?
 - ?DNIS?ANI?
 Default: ?ANI?DNIS?.
- **Outbound Delimiter (?) Character:** Define the Outbound Delimiter Character in this field. 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.

If the Network (Public or Private) to which SETU VTEP is connected supports FDL, select the **FDL Flag** check box to enable. By default, the FDL flag is disabled.

- If you have enabled FDL Flag, select the **FDL Protocol**. SETU VTEP supports **ANSI T1 403** and **AT&T 54016** protocols for reporting the performance monitoring. Default: ANSI T1 403.
- Click **Submit** to save changes.
- Close the window to return to the main page.
- Select the **Orientation Type** for the port as **Terminal** or **Network**, according to your installation scenario. Default: Terminal.



By default Orientation Type is set to Terminal and is non-programmable, if you select CarrierType as T1 and Signaling Type as RBS.

If you select **Terminal** as Orientation Type, configure the following:

- Line Buildout Parameter
- Network Type
- Pilot Number
- Line Coding Mechanism
- Framing Mode
- Allow Call Disconnection using Access Code
- Overlap Receiving Timer
- Automatic Number Translation (ANT) for Called Number
- Automatic Number Translation (ANT) for Calling Number
- ["Handling of Incoming Calls"](#)
- ["Handling of Outgoing Calls"](#)

General	
Carrier Type	T1
Signaling Type	PRI
Orientation Type	Terminal
Line Buildout Parameter	0-133 ft
Network Type	Public
Pilot Number	
Line Coding Mechanism	AMI Basic
Framing Mode	SF (D4)
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Overlap Receiving Timer	15 Seconds
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Enable
Automatic Number Translation(ANT) for Calling Number	<input type="checkbox"/> Enable
<div> <div>Handling of Incoming Calls</div> <div>Handling of Outgoing calls</div> </div>	

If you select **Network** as Orientation Type, configure the following:

- Line Buildout Parameter
- Pilot Number
- Line Coding Mechanism
- Framing Mode
- Allow Call Disconnection using Access Code
- Automatic Number Translation (ANT) for Called Number
- Automatic Number Translation (ANT) for Calling Number
- ["Handling of Calls"](#)

General	
Carrier Type	T1
Signaling Type	PRI
Orientation Type	Network
Line Buildout Parameter	0-133 ft
Pilot Number	
Line Coding Mechanism	AMI Basic
Framing Mode	SF (D4)
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Enable
Automatic Number Translation(ANT) for Calling Number	<input type="checkbox"/> Enable
<div> <div>Handling of Calls</div> </div>	

- Select the **T1 Line Buildout Parameter** for T1/E1 Port from the options:
 - 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
- 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: 0 to 9, #, *. Default: Blank.
- **Line Coding Mechanism:** Line coding is a pattern that data assumes as it is propagated over a communication channel. The Line Coding mechanisms are supported in SETU VTEP:
 - AMI Basic
 - B8ZS
 Default: AMI Basic.
- **Framing Mode:** Framing means to form a set of 24 or 32, 8 bits time slot that is to be treated as single transmission unit. The Framing Modes supported by SETU VTEP are:
 - SF (D4)
 - ESF
 Default: SF (D4).
- Select the **Allow Call Disconnection using Access code** check box, if you want to enable the feature Disconnect Call using Access Code on the T1/E1 port. See [“Disconnecting a Call using Access Code”](#).
- You can apply Automatic Number Translation (ANT) logic on the outgoing calls made from the T1 Port.

- To apply ANT logic on the Called Numbers, click the **Automatic Number Translation (ANT) for Called Number** check box. Default: Disabled.

General

Carrier Type	T1
Signaling Type	PRI
Orientation Type	Terminal
Line Buildout Parameter	0-133 ft
Network Type	Public
Pilot Number	
Line Coding Mechanism	AMI Basic
Framing Mode	SF (D4)
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Overlap Receiving Timer	15 Seconds
Automatic Number Translation(ANT) for Called Number	<input checked="" type="checkbox"/> Enable
Use Automatic Number Translation Table	1
Pause Timer	2 Seconds
Automatic Number Translation(ANT) for Calling Number	<input type="checkbox"/> Enable

- In the **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 page will open in a new window.

1
2
3
4
5
6
7
8

Automatic Number Translation Table - 1

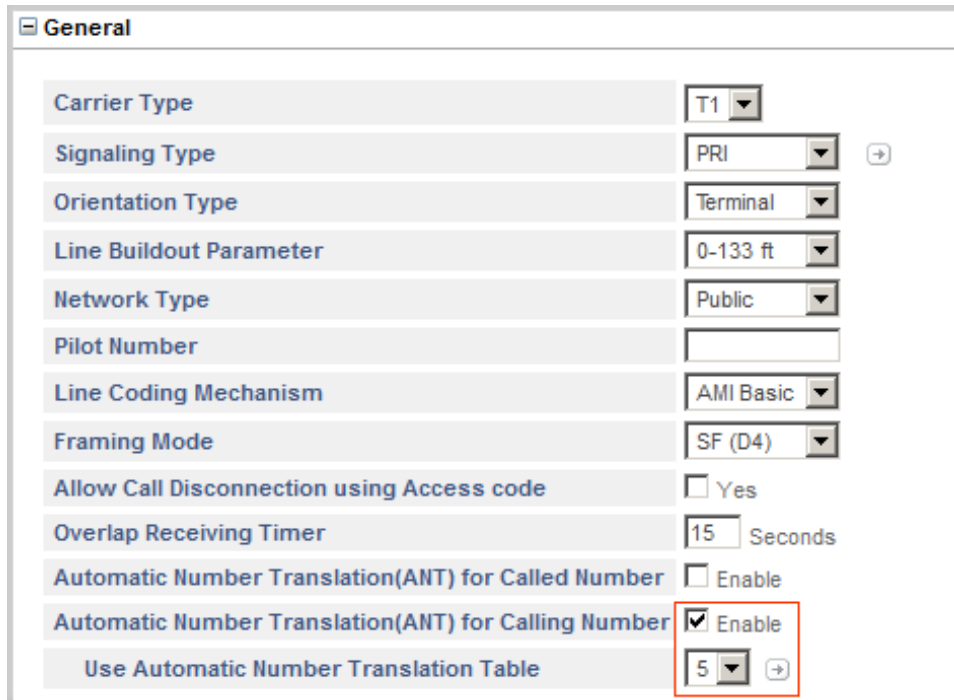
Index	Number	Strip Digit	Add Prefix
01		0	
02		0	
03		0	
04		0	
05		0	
06		0	
07		0	
08		0	
09		0	
10		0	

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 1 or any other Table (2 to 8). 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.
- Configure the **Pause Timer**, if you have configured ^ (Pause) in the Add Prefix column of the ANT Table. The valid range of the Pause Timer 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.



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

Carrier Type	T1
Signaling Type	PRI
Orientation Type	Terminal
Line Buildout Parameter	0-133 ft
Network Type	Public
Pilot Number	
Line Coding Mechanism	AMI Basic
Framing Mode	SF (D4)
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Overlap Receiving Timer	15 Seconds
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Enable
Automatic Number Translation(ANT) for Calling Number	<input checked="" type="checkbox"/> 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 page will open in a new window.




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	
13		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

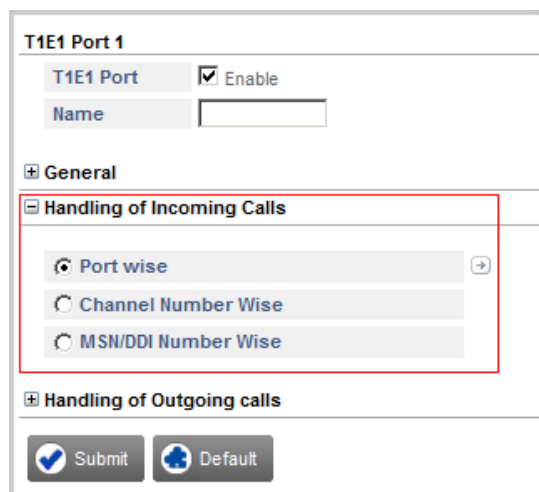
- You may configure the default Automatic Number Translation Table 5 or any other Table. See [“Automatic Number Translation \(ANT\)”](#) to configure the ANT Table.
- Click **Submit** to save the ANT Table and close the window.
- Return to ANT parameter and assign the ANT Table you configured.
- Click **Submit** to apply List.

Orientation Type - Terminal

- If you have selected *Terminal* as Orientation Type, specify the **Network Type**, i.e. whether the T1 line is from a **Public** Network (telephone exchange) or from a **Private** Network (to the NT port of a PBX). Default: Public.
- Overlap Receiving Timer:** Overlap Receiving Timer is relevant while receiving the called party number information in overlap receiving mode. It is not relevant for the port in overlap sending mode.

Range of Overlap Receiving Timer is from 01 to 99 Seconds. Default: 15 Seconds.

Handling of Incoming Calls




T1E1 Port 1

T1E1 Port ☒ Enable

Name

General

Handling of Incoming Calls

☒ Port wise 

☐ Channel Number Wise

☐ MSN/DDI Number Wise

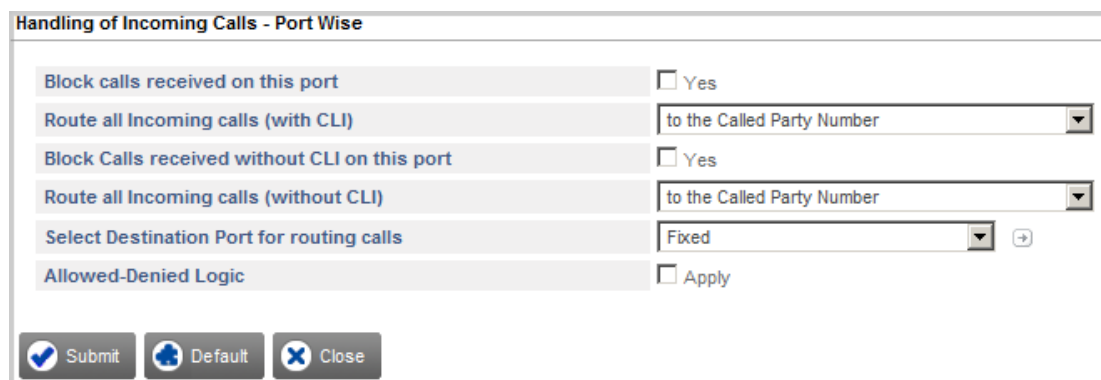
Handling of Outgoing calls

Select the method to route the incoming calls from the T1/E1 Port. SETU VTEP provides three options for **Handling of Incoming Calls**: i) Port wise, ii) Channel Number wise, iii) MSN Number wise. Default: Port wise.

- **Port wise**: Select this method to apply the call routing method for the entire port, that is on all channels and all called party numbers received.
- **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 of the 30 channels.
- **MSN 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.
 - **MSN Number 1**: Enter the first **MSN Number** (max. 24 digits) provided by your service provider. Valid digits: 0-9, # and *. Default: Blank.
 - **Total DDI Number**: Specify the **Total DDI Numbers** provided by your service provider. Valid range: 1 to 9999. Default: 0100.

For the incoming call routing option you select, click the settings icon and configure the parameters.

Port wise Routing




Handling of Incoming Calls - Port Wise

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)

Select Destination Port for routing calls 

Allowed-Denied Logic ☐ Apply

To configure Handling of Calls Portwise,

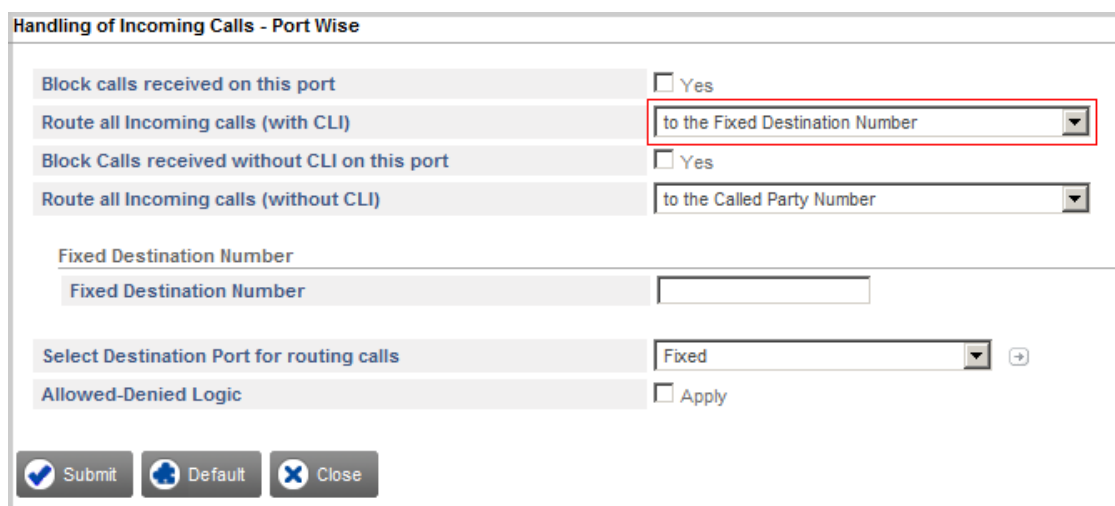
- Select the **Block calls received on this port for further routing** check box, if you do not want to route calls through this port.

Route all Incoming calls (with 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.

Route To the Fixed Destination Number

In this method, a call received on the T1/E1 Port is routed to a fixed destination number, which is configured for the T1/E1 Port.



If you select this method,

- 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. Default: Blank.
- Click **Submit** to save your setting.

Route On the basis of Calling Party Number


In this method, a call received on the T1/E1 Port is routed to a specific number, as per the calling party's number.


If you select this method,

- Click the settings icon and configure the table **Calling Number Based** for the T1/E1 Port.


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

First Digit Wait Timer 7 Seconds


Inter Digit Wait Timer 5 Seconds

End Of Dialing Digit # 




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

The Calling Number Based Table page opens in a new window.

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		

 Submit  Default All  Close

- Configure the following parameters in this table:

- **Calling Number:** Enter the calling party numbers in the column Calling Numbers. Calling numbers may consist of a maximum of 24 characters. Default: Blank.
- **Destination Number:** For each calling party number, enter a corresponding destination number in the column Destination Numbers. 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.

When there is an incoming call on the T1/E1 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 port.
- **If no match found in the Calling Party Number Table**, you may select any of 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
- Click **Submit** to save and close the window to return to the main page.

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



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 configured/selected for IP Dialing. (Refer [“IP Dialing”](#) feature for more details).

Route On the basis of DDI Number

In this method, a call is routed to a specific number as per the DDI number received in the SETUP message of the T1/E1 Port.

If you select this option,

- Click the settings icon and configure the table **DDI Number Based** for the T1/E1 Port.

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

The DDI Number Based Table page opens in a new window.

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

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"/>	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

- Configure the following:
 - DDI Number
 - Destination Number
 - Reverse DDI
- 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*. See [“Destination Number Determination”](#) under *Advanced Settings* for instructions.



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

Route 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

In this method, a call received on the T1/E1 port is routed to a specific number depending upon the called party number received in the SETUP Message of the T1/E1 port.

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 the destination number.

If you select this option, configure the following:

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
First Digit Wait Timer	7 Seconds
Inter Digit Wait Timer	5 Seconds
End Of Dialing Digit	#
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

- **First Digit Wait Timer (FDWT):** Define the number of seconds the system should wait for the user to dial the destination number. Default: 7 seconds. You may change this timer, if required. The valid range of this timer is 01 to 99 seconds.
- **If No Digit dialed during First Digit Wait Timer (FDWT)** by the user, you may either **Disconnect the Call** or **Use Fixed Destination Number** to route the call. 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. Default: Blank.

You may configure the following options as end-of-dialing indication:

- **Inter Digit Wait Timer:** Define the number of seconds the system should wait while receiving the dialing digits, to consider it as end-of-dialing. You may change this timer, if required. The valid range is 01 to 99 seconds. Default: 05 seconds.
- **End of Dialing Digit (Termination digits):** Select whether the system should consider # or * as termination digit to detect end of dialing. Default: #.
- **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. The 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 you want to enable “[PIN Authentication](#)”, select the **Prompt caller to enter PIN** check box.
- Select the **Allow making New Call using Access code**, if you want to enable the feature Making New Call using Access Code on the T1/E1 Port. See “[Making a New Call using Access Code](#)”.
- Click **Submit** to save settings.
- Select the **Block calls received without CLI on this port** check box, if you do not want to route calls received without CLI through this port. Default: Disabled.

Route all Incoming calls (without CLI)

- To **Route all Incoming calls (without CLI)**, you may select from any of the following methods.
 - to a Fixed Destination Number, see “[Route To the 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.

Destination Port for routing calls

Select the Destination Port for routing calls for the port/channel/MSN Number. You may select from any of the following options:

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

Default: Fixed

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 (selected)
Allowed-Denied Logic	

Submit Default Close

Fixed

In this method, calls received on the T1/E1 Port are routed to a fixed destination port, irrespective of the number dialed on the source port.

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

If you select this option,

- Click the settings icon. A new 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 Group** appear.

- Click **Edit**, if you want to change the default Routing Group options. A new window opens.

Edit Selective Port/Group for T1E1 Port		
Routing Group		
<input type="radio"/> T1E1 Port	1 and Channel Number from 01 to 01 in Ascending order	
<input type="radio"/> T1E1 Group	1	
<input checked="" type="radio"/> SIP Trunk	01 to 01 in Ascending order	
<input type="radio"/> SIP Group	1	
Fallback Routing Group <input type="checkbox"/> Apply		
<input type="radio"/> T1E1 Port	1 and Channel Number from 01 to 01 in Ascending order	
<input type="radio"/> T1E1 Group	1	
<input type="radio"/> SIP Trunk	01 to 01 in Ascending order	
<input type="radio"/> SIP Group	1	

Submit Close

- Create the **Routing Group**.
 - To create a routing group of *sequential* T1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* T1 channels as members, select a **T1E1 Group** Number.

Click the settings icon and create the T1 Group. See “[Group](#)” for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,

- Select the **SIP Trunk** numbers as members.
- In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

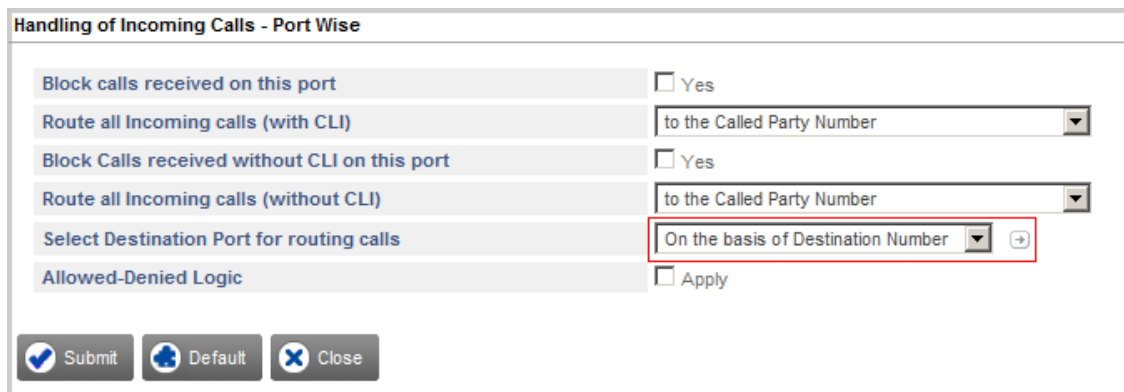
Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group Number**.

Click the settings icon and create the SIP Group. See “[Group](#)” for further instructions.

- To create the **Fallback Routing Group**,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and the SIP Trunks.
- Click **Submit** to save changes. The **Edit** window closes.
- The Routing and Fallback Groups you created appear. Close the 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.

If you select this option, you must configure the **Destination Number Based** table.

- Click the settings icon. A new window opens.

T1E1 Port - Destination Port Determination - Destination Number Based						
	Edit	Destination Number	Minimum Digits	Maximum Digits	Routing Group	Fallback Routing Group
		No Match Found	3	16	SIP Trunk 1 - 1 (Ascending)	None
Total Records : 1		1				
<div><div> Add</div><div> Delete</div><div> Close</div></div>						

- Click **Add** to add an entry. A new window opens.

Add Entry

Destination Number

Minimum Digits

Maximum Digits

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 the **Destination Number** field, enter the number (max. 24 characters) you expect callers to dial. Valid digits: 0 to 9, *, #, (dot). Default: blank.

- In the **Minimum Digits** field, enter the minimum digits for the system to consider the destination number as a valid number. Range: 01 to 24. Default: 03.

If the dialed number string is less than the configured minimum length, the call will be rejected.

- In the **Maximum Digits** field, enter the maximum number of digits of the destination number the caller must dial for the system to route the call.

If the number string dialed by the caller exceeds the maximum length configured, the system will strip off the extra digits, and route the call. Maximum length range: 01 to 24. Default: 16.

- Create the **Routing Group**.

- To create a routing group of *sequential* T1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* T1 channels as members, select a **T1E1 Group Number**.

Click the settings icon and create the T1 Group. See [“Group”](#) for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group Number**.

Click the settings icon and create the SIP Group. See [“Group”](#) for further instructions.

- To create the **Fallback Routing** Group,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and SIP Trunks.
- Click **Submit** to save changes and close the window.
- The Routing and Fallback Groups you created appear.
- To edit an entry, click **Edit**, a new window opens. Make the changes as per your requirement and click **Submit**.
- To delete an entry, select the check box and click **Delete**.
- Close the window to return to the main page.

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

On the basis of Calling 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	On the basis of Calling Party Number
Allowed-Denied Logic	<input type="checkbox"/> Apply

In this method, Incoming calls on the source port will be routed to the destination port on the basis of the calling party's number.

If you select this option, you must configure the **Calling Number Based** table.

- Click the settings icon. A new window opens.

T1E1 Port - Destination Port Determination - Calling Number Based

	Edit	Calling Number	Routing Group	Fallback Routing Group
		No Match Found	SIP Trunk 1 - 1 (Ascending)	None

Total Records : 1 1

- Click **Add** to add an entry. A new window opens.

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 the **Calling Number** field, enter numbers (max. 24 characters) from which you expect calls to be received. Valid digits: 0 to 9, *, #, (dot). Default: blank.
- Create the **Routing Group**.

- To create a routing group of *sequential* T1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* T1 channels as members, select a **T1E1 Group Number**.

Click the settings icon and create the T1 Group. See [“Group”](#) for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group Number**.

Click the settings icon and create the SIP Group. See [“Group”](#) for further instructions.

- To create the **Fallback Routing Group**,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and SIP Trunks.
- Click **Submit** to save changes and close the window.
- The Routing and Fallback Groups you created appear.
- To edit an entry, click **Edit**, a new window opens. Make the changes as per your requirement and click **Submit**.
- To delete an entry, select the check box and click **Delete**.

- Close the window to return to the main page.

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

Allowed - Denied Logic (Toll-Control)

With the Allowed-Denied Numbers feature you can permit and restrict the dialing of particular numbers from the T1/E1 Port.

Allowed Denied Number Logic makes use of two predefined Number lists:

- **Allowed Numbers List:** This is the list of numbers that can be dialed out from T1/E1 Port. By default, List Number 1 is assigned to the T1/E1 Port.
- **Denied Numbers List:** This list contains the numbers that are to be restricted from being dialed out from the T1/E1 Port. By default, List Number 2 is assigned to the T1/E1 Port.

Both lists must be programmed first and then applied on the T1/E1 Port. For instructions see [“Number Lists”](#).

To apply Allowed - Denied Logic on the T1/E1 Port,

- Click the Allowed - Denied Logic **Enable** check box.

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 Calling Party Number
Allowed-Denied Logic	<input checked="" type="checkbox"/> Apply
Allowed Numbers List	01
Denied Numbers List	02

Submit Default Close

- As **Allowed Numbers List**, select the number of the Number List, which you have programmed as Allowed Number List. If you retained the default Number List 1, select the same list number.

If you have not configured the Allowed Numbers List,

- Click the settings icon.

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

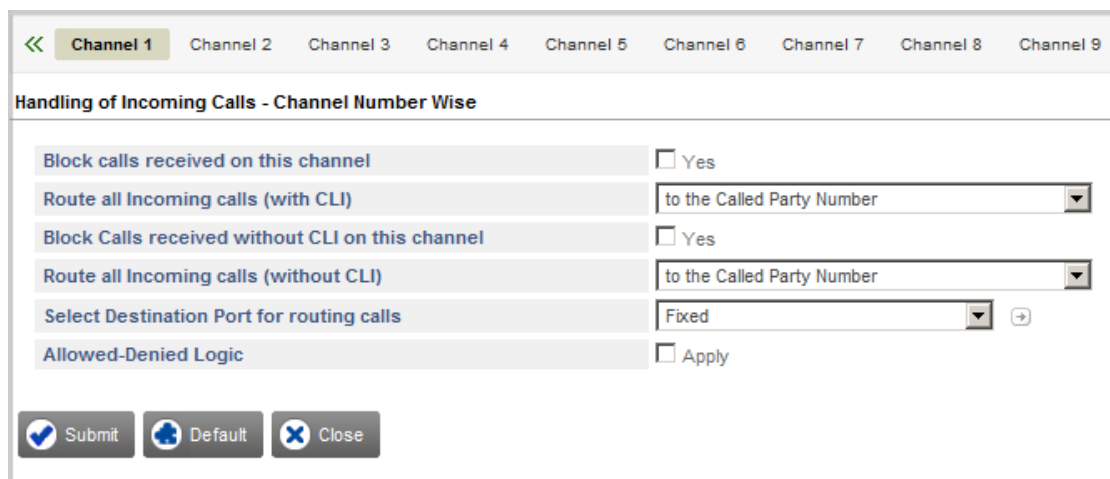
Submit
 Default
 Close

- The Number List page will open in a new window.
 - You may configure the default Number List 1 or any other Number List as Allowed Number List.
 - Click **Submit** to save Number List and close the window.
 - Return to Allowed - Denied Logic parameter and assign the Number List you configured.
- **Denied Number List:** Select the number of the Number List, which you have programmed as Denied Number List. If you retained the default Number List 2, select the same list number.

If you have not configured the Denied Number List,

- Click the settings icon.
 - The Number List page will open in a new window.
 - You may configure the default Number List 2 or any other Number List as Denied Number List.
 - Click **Submit** to save Number List and close the window.
 - Return to Allowed - Denied Logic parameter and assign the Number List you configured.
- Click **Submit** to apply the changes. See [“Allowed - Denied Logic”](#) under [“Number Lists”](#).

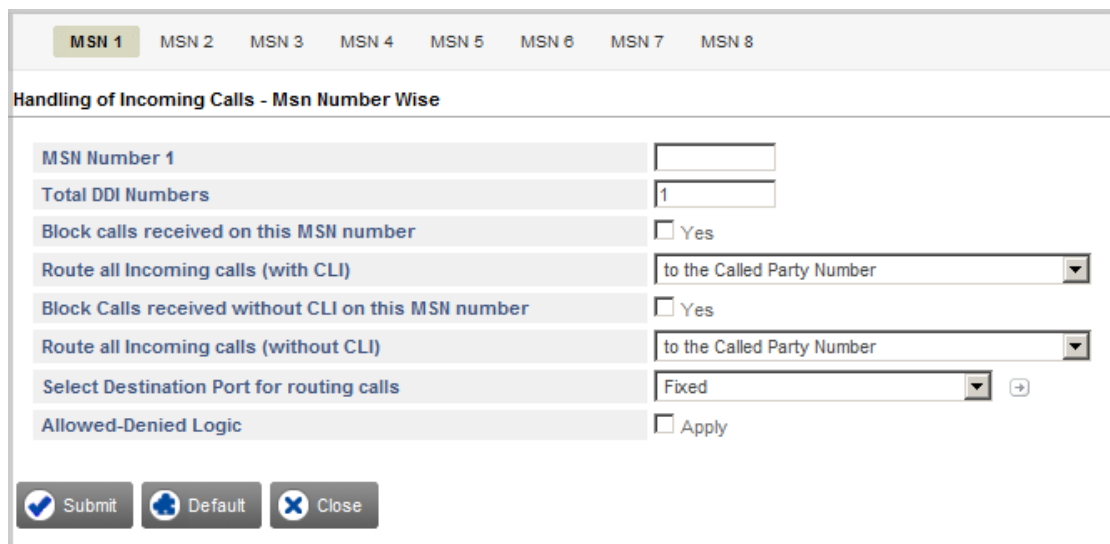
Channel Number Wise Routing



If you have selected Channel Number Wise method for Handling of Incoming Calls, you must configure the following parameters for each channel:

- Block calls received on this channel
- Route all Incoming calls (with CLI), see [“Route all Incoming calls \(with CLI\)”](#) under [“Port wise Routing”](#).
- Block Calls received without CLI on this channel.
- Route all Incoming calls (without CLI), see [“Route all Incoming calls \(without CLI\)”](#) under [“Port wise Routing”](#).
- Select Destination Port for routing calls, see [“Destination Port for routing calls”](#) under [“Port wise Routing”](#).
- Allowed-Denied Logic, see [“Allowed - Denied Logic \(Toll-Control\)”](#) under [“Port wise Routing”](#).

MSN Number Wise Routing



If you have selected MSN Number Wise method for Handling of Incoming Calls, you must configure the following parameters for each MSN Number:

- MSN Number 1
- Total DDI Numbers
- Block calls received on this MSN number
- Route all Incoming calls (with CLI), see [“Route all Incoming calls \(with CLI\)”](#) under [“Port wise Routing”](#).
- Block Calls received without CLI on this MSN number.

- Route all Incoming calls (without CLI), see [“Route all Incoming calls \(without CLI\)”](#) under [“Port wise Routing”](#).
- Select Destination Port for routing calls, see [“Destination Port for routing calls”](#) under [“Port wise Routing”](#).
- Allowed-Denied Logic, see [“Allowed - Denied Logic \(Toll-Control\)”](#) under [“Port wise Routing”](#).

Handling of Outgoing Calls

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 though 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, this incoming call is placed to the original calling party. You can change the duration of this timer and delete records of such calls. 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 feature *"Making a New Call using Access Code"* to users.

- Click **Submit** to save settings.

Orientation Type - Network

Handling of Calls

If you have selected **Network** as Orientation Type,

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

SETU VTEP provides two options for **Handling of Calls** when the Port is set in Network mode.

- **Port wise:** Select this method to apply the call routing method for the entire port. See [“Port wise Routing”](#).

Handling of Calls - Portwise

Block calls received on this port ☐ Yes

Dial Tone Timer 7 Seconds

Inter Digit Wait Timer 5 Seconds

End Of Dialing Digit #

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

Select Destination Port for routing calls Fixed

Allowed-Denied Logic ☐ Apply

Submit Default Close

- **Channel Number wise:** Select this method to apply a different call routing method for each of the 30 channels. See [“Channel Number Wise Routing”](#).

Handling of Calls - Channel Numberwise

Channel 1 Channel 2 Channel 3 Channel 4 Channel 5 Channel 6 Channel 7 Channel 8

Block calls received on this channel ☐ Yes

Dial Tone Timer 7 Seconds

Inter Digit Wait Timer 5 Seconds

End Of Dialing Digit #

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

Select Destination Port for routing calls Fixed

Allowed-Denied Logic ☐ Apply

Submit Default Close

- For the method you select, Portwise or Channel Number wise, configure the following parameters:
 - **Block calls received on this port/channel:** Select this check box, if you do not want to route calls through this port/channel.
 - **Dial Tone Timer:** This is the time for which SETU VTEP will play Dial Tone to the caller. Default:7 seconds. At the end of this timer, the system plays error tone to the caller.
 - **Inter Digit Wait Timer:** Define the number of seconds the system should wait while receiving the dialing digits, to consider it as end-of-dialing. You may change this timer, if required.The valid range is 01 to 99 seconds. Default: 5 seconds.
 - **End of Dialing Digit (Termination digits):** Select whether the system should consider # or * as termination digit to detect end of dialing. Default: #

- **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. The valid range is 01 to 24 digits. Default: 24 digits.
- **Select Destination Port for routing calls:** Select the desired method for destination port determination - Fixed, on the basis of Calling Party Number, on the basis of Destination Number. See [“Destination Port for routing calls”](#).
- **Allowed - Denied Logic:** To permit and restrict the dialing of particular numbers from the T1/E1 Port, enable Allowed-Denied Logic and configure the Allowed and Denied Number Lists. See [“Allowed - Denied Logic \(Toll-Control\)”](#).
- Click **Submit** to save your changes.

Login Password

To configure the system, you must log into the Jeeves using the Jeeves Password. The default Jeeves Password is 1234. However, you must change it for security reasons.

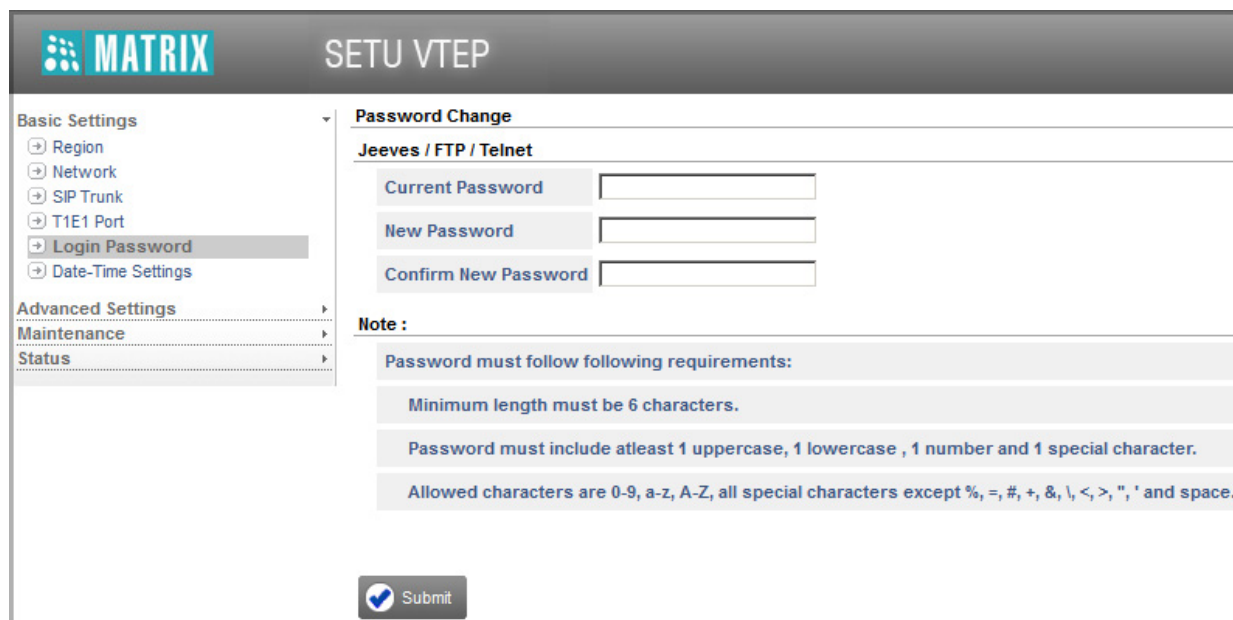
The Jeeves Password must fulfill the following requirements.

- It must not be less than 6 characters and can be of upto 16 characters.
- 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.
- 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:

- Log into Jeeves.
- Click the **Basic Settings** link to expand.
- Click **Login Password**.



The screenshot displays the MATRIX SETU VTEP web interface. On the left, a sidebar menu shows 'Basic Settings' expanded, with 'Login Password' selected. The main content area is titled 'Password Change' and contains a section for 'Jeeves / FTP / Telnet'. This section has three input fields: 'Current Password', 'New Password', and 'Confirm New Password'. Below these fields is a 'Note' section with the following requirements: '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.', and 'Allowed characters are 0-9, a-z, A-Z, all special characters except %, =, #, +, &, \, <, >, ', ' and space.' At the bottom of the form is a 'Submit' button with a checkmark icon.

Under **Jeeves/FTP/Telnet**,

- Enter **Current Password**.
- **Enter 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** 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 Login Password (1234) and are unable to recall or locate it, you must restore the default login password.

Restoring Default Login Password

Restoring the Default Login Password requires you to change the Jumper Settings 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 **J4** from **BC** to **AB**.
- Switch ON the system and wait for 15 seconds.
- Switch OFF the system.
- Change the Jumper position from **AB** to the original position **BC**.
- Replace the enclosure cover.
- Switch ON the system.
- The default login password will be restored to 1234.



When you change the jumper positions to restore default Jeeves Password (1234), a few other parameters will also be set to default. See [“Restoring Default Settings by changing the Jumper Position”](#) for details.

Date-Time Settings

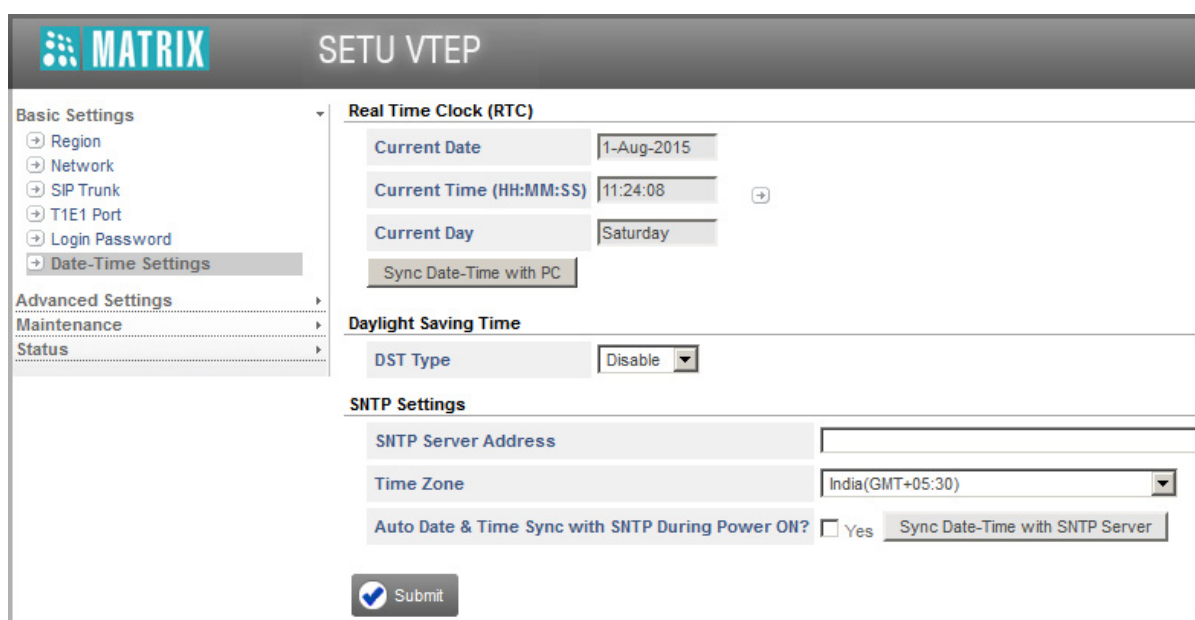
Real Time Clock

SETU VTEP has its own Real Time Clock (RTC) to store the date and time. When you select the Region, the RTC will be set automatically.

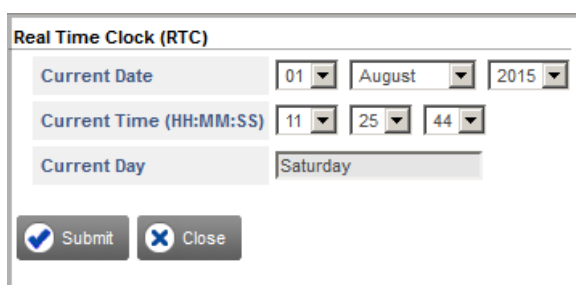
However, the RTC can drift over a long period. So, you may check and reset the RTC values at regular intervals to correct this drift.

To set the Real Time Clock,

- Under Basic Settings, click **Date-Time Settings** link.
- The Real Time Clock parameters appears on the screen.



- Click the settings icon beside the **Current Time**.
- A new window opens.



- Set the Current Date in date, month and year format.
- Set the Current Time in 24 hours, minutes and seconds format.

The current day is displayed automatically for the date and time you set.

- Close the window.
- Click **Submit**.
- Click **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 world² use it, though the start and end dates of DST vary with location and year.

SETU VTEP supports Daylight Saving Time adjustment to set the Date and Time³ 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**.

Configuring DST

To configure DST parameters,

- Under Basic Settings, click the **Date and Time Settings** link.

Real Time Clock (RTC)

Current Date: 1-Aug-2015

Current Time (HH:MM:SS): 11:24:08

Current Day: Saturday

Sync Date-Time with PC

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

- Scroll to **Daylight Saving Time**.
- Select the **DST Type**. You may select **Auto** or **Custom**. If you do not want to apply DST, select Disable. Default: Disable.

2. In most countries in Asia and Africa, and in certain countries of South America, DST is not observed.

3. 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"](#).

- If you select **Auto**, you must select the **Region**.

Daylight Saving Time

DST Type: Auto

Region: United Kingdom

SNTP Settings

SNTP Server Address:

Time Zone:

Auto Date & Time Sync with:

☒ Submit

The DST will be set automatically as per the region selected.

- If you select **Custom**,

Daylight Saving Time

DST Type: Custom

Time Offset (Minutes): 61

Type: Day-Month wise

	Ordinal	Day	Month	Time	
				Hours	Minutes
DST Start	2nd	Sunday	March	01	59
DST End	1st	Sunday	November	01	59

- Enter the **Time Offset**. This is the time which the system will 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**. Select this option 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**. Select this option 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 selected the **Day-Month Wise** option, 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. The time mode is 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. The time mode is 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 example 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. The time mode is 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. The time mode is 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.

1. Select the **DST Type** as **Custom**.
2. Set the **Time Offset** as 60 minutes.
3. Select the option **Day-Month Wise** as **Type**.
4. Configure the **DST Start** as follows:
 - Select **5th** as the **Ordinal**.
 - Select **Sunday** as the **Day**.
 - Select **March** as the **Month**.
 - Set Time to 01 Hours and 00 Minutes.

5. Now, go to the option **DST End**, and configure as follows.
 - Select **5th** as the **Ordinal**.
 - Select **Sunday** as the **Day**.
 - Select **October** as the Month.
 - Set Time to 01 Hours and 00 Minutes.

6. Click **Submit** to save DST settings.

SNTP Settings

To use SNTP for synchronizing the time of SETU VTEP with the Real Time Clock,

- Under Basic Settings, click the **Date and Time Settings** link and configure the following parameters:



- **SNTP Server Address:** Enter the Time Server Address. SNTP Server address can be of maximum 40 characters. Default: Blank.
- **Time Zone:** 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. Default: India (GMT+05:30).
- **Auto Date and Time Sync with SNTP during Power ON?:** If you want to synchronize date and time with the SNTP server automatically at Power On, select Yes.

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 set to No.

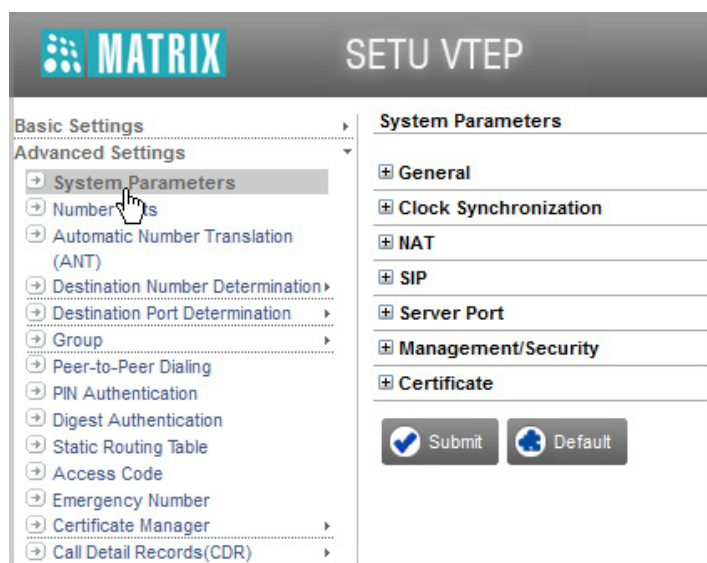
- **Sync Date and Time Server with SNTP:** Click this button to synchronize date and time of SETU VTEP with the SNTP server, whenever required.
- Click **Submit** to save the changes.

System Parameters

System Parameters are general parameters, related to features and facilities that are applied system-wide, such as system name, clock synchronization, NAT and SIP related parameters.

To change the settings of System Parameters,

- Click the **Advanced Settings** link to expand.
- Click the **System Parameters** link to open the page.



- Configure the following System Parameters, as required.

General Parameters

- Click **General** to expand options and configure the following.

General	
System Name	<input type="text"/>
SIP Trunk for IP Dialing	SIP Group <input type="text" value="1"/>
SIP LED	SIP Trunk 1 <input type="text"/>
Play Routing Tone	<input type="checkbox"/> Yes
Call Release Timer	999 Minutes
VoIP Silence Disconnect Timer	999 Seconds
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 <button>Clear Unconnected Call Records</button>
Remove Country Code from CLI received	<input type="checkbox"/> Yes

- System Name:** You can assign a name to SETU VTEP as 'System Name'. This name can serve as an identifier, when there are more than one SETU VTEP connected in the same LAN network.

System Name can be of maximum 40 characters. Default: Blank.

- SIP Trunk for IP Dialing:** To use the IP Dialing feature (to directly dial IP Addresses), you must select a **SIP Trunk** or **SIP Group** for routing the call to the IP Address. For example, if you configured SIP Trunk Group 3 for IP Dialing, you must select 3. See ["IP Dialing"](#) to know more about this feature.

The valid range for the SIP Trunk is 1 to 32 and 1 to 9 for SIP Group. Default: SIP Group 1.

When you assign a SIP Trunk, make sure it is enabled and has the necessary configuration done. See ["SIP Trunks"](#) under *Basic Settings* for instructions.

When you assign a SIP Group, you must configure the SIP Group first. See ["Group"](#) for instructions.

- SIP LED:** You can select the SIP trunk whose status you want to monitor on the LED. The system will display the status of the SIP Trunk number you select on the SIP LED. Default: SIP Trunk 1.
- Play Routing Tone:** Routing Tone is played at the time of routing the call to the destination port. During an outgoing call, the routing tone indicates that the call is in progress. Select this check box, to enable the routing tone. Default: Disabled.
- Call Release Timer:** This is the timer used to release the ports involved in a call after a definite period of time if not released due to any reason. This timer is loaded as soon as a call gets matured. This timer is stopped if one of the ports involved in a call is released. The valid range of Call Release Timer is 001 to 999 minutes. Default: 999 minutes.
- VoIP Silence Disconnect Timer:** It is the duration (in seconds) after which SIP call is disconnected, if continuous silence (no RTP Packets) is detected for the set time period. The VoIP Silence Disconnect Timer is loaded as soon as silence is detected during an IP call. The IP call is disconnected if continuous silence is detected after the expiry of this timer. This timer is applicable for all types of calls received or made through the SIP Trunks.

The valid range of the VoIP Silence Disconnect Timer is 001 to 999 seconds. Default: 999 seconds.

- **Routing Group Busy Wait Timer:** It is the duration for which SETU VTEP searches for a free destination port in the Routing Group and the Fallback Routing Group to route and place the call. The Routing Group Busy Wait Timer is loaded when no destination port is free in both the Routing Group and the Fallback Routing Group.

The valid range of the Routing Group Busy Wait Timer is 01 to 99 seconds. Default: 01 second.

- **Error Tone Timer:** The time for which the system plays the Error Tone. The valid range of the Error Tone Timer is 0 to 9. Default: 7 seconds.
- **Error Tone Delay Timer:** It is the duration after which the system will play the Error Tone, if the call is disconnected during speech. The valid range of the Error Tone Delay Timer is 00 to 99 seconds. Default: 00 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.

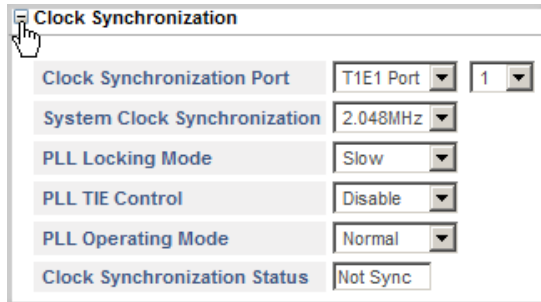
You can also delete the records of unconnected calls any time, without waiting for this timer, by clicking the **Clear Unconnected Call Records** button.

- **Remove Country Code from CLI received:** You may remove country code from the CLI received on the source port, before presenting it on the destination port, if required.

If you want the system to remove country code from the CLI received, select this check box. Default: Disabled. Make sure you configure **Country Code** under *Region* in Basic Settings.

Clock Synchronization

- Click **Clock Synchronization** to expand options and configure the following.



- Clock Synchronization Port:** Select the Port that the system should use as the clock source for clock synchronization. You may select:
 - None
 - T1E1 Port
 - SYNC IN

Default: T1E1 Port.



If you select None, SETU VTEP will use the internal clock for Clock Synchronization.

- System Clock Synchronization:** Select appropriate Clock Synchronization option in this field. You may select:
 - 2.048 MHz
 - 1.54 MHz

By default, System Clock Synchronization is set to 2.048 MHz for India and other countries except USA. For USA, it is set to 1.54 MHz.



The system will restart when the frequency is changed.

- PLL Locking Mode:** Depending upon the speed required for clock synchronization, select the speed for PLL Locking in SETU VTEP. You can select either Slow or Fast. Default: Slow.
- PLL TIE Control:** You can enable or disable PLL TIE Control. By default, it is disabled.
- PLL Operating Mode:** Select the PLL Operating Mode in this field. You can select from the following options:
 - Normal
 - Hold Over
 - Free Run

Default: Normal.

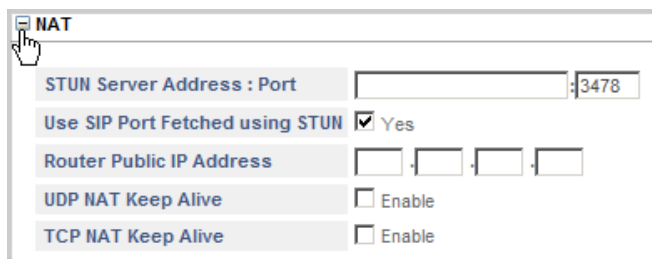
- Clock Synchronization Status:** This field displays the status of Clock Synchronization.



Clock Synchronization Status will be displayed only when PLL Operating Mode is set to Normal.

NAT

- Click **NAT** to expand options and configure the following.



- STUN Server Address: Port:** STUN (Simple Traversal of UDP through NAT) server facilitates traversing through most NATs, except symmetric NATs. So, if your router has Symmetric NAT, do not configure STUN. If your SETU VTEP is located behind a NAT router that is other than symmetric, use STUN.

In the **STUN Server Address: Port** field, enter the STUN Server Address and the Listening Port of the STUN Server.

The STUN Server Address can have a maximum of 40 characters.

The valid range of the STUN Server Port is from 1024–65535. Default: 3478.

- Use SIP Port Fetched using STUN:** Clear this check box, if your 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 configure the **NAT Type** on the SIP Trunk as **STUN**. See “[SIP Trunks](#)”.*

- Router Public IP Address:** The Router’s public IP address specifies the public IP address of the NAT router behind which system is located. Default: Blank.

You need to configure this field only if the system is located behind the NAT router and a Static IP Address is assigned as Public IP Address of the Router.



*Make sure you configure the **NAT Type** on the SIP Trunk as **Router’s IP Address**. See “[SIP Trunks](#)”.*

- UDP NAT Keep Alive:** When SETU VTEP is connected behind a NAT router and SIP messages are transported over UDP, NAT Keep Alive messages must be sent to refresh the binding in the NAT router.

Select the **UDP NAT Keep Alive** check box to enable. Default: Disabled.

- Keep Alive Message:** Select the type of **Keep Alive Message** to be sent. You may select either REGISTER or NOTIFY. Default: NOTIFY.

As **Interval**, set the time period after which the system should send Keep Alive messages. This time period should be less than the NAT binding timer of the router. The valid range for the UDP NAT Keep Alive Interval is 001–999 seconds. Default: 120 seconds.

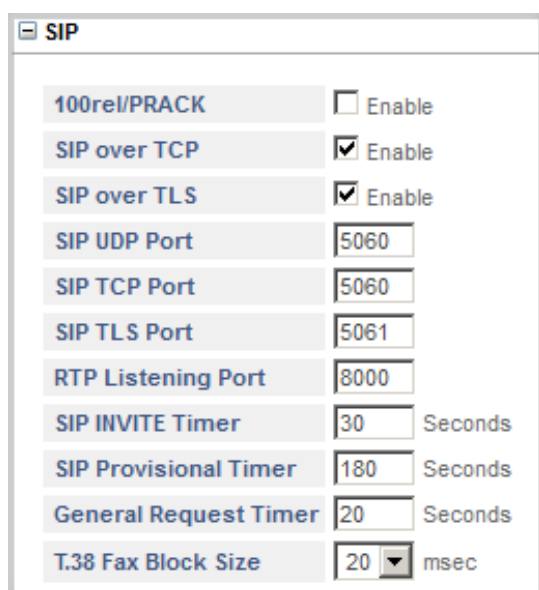
- **TCP NAT Keep Alive:** When SETU VTEP is connected behind a NAT router, and SIP messages are transported over TCP, NAT Keep Alive messages must be sent to refresh the binding in the NAT router.

Select the **TCP NAT Keep Alive** check box, if you want the system to send Keep Alive messages periodically to refresh the binding in the NAT router. Default: disabled.

As **Interval**, set the time period after which the system should send Keep Alive messages. This time period should be less than the NAT binding timer of the router. The valid range for the TCP NAT Keep Alive Interval is 001–999 seconds. Default: 120 seconds.

SIP

- Click **SIP** to expand options and configure the following.



SIP	
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
RTP Listening Port	8000
SIP INVITE Timer	30 Seconds
SIP Provisional Timer	180 Seconds
General Request Timer	20 Seconds
T.38 Fax Block Size	20 msec

- **100rel/PRACK:** This parameter is to be configured if you want to support reliable transmission of (SIP) provisional responses.

Select the **100rel/PRACK Enable** check box, if you want the SETU VTEP to use 100rel SIP extension for reliable transmission of SIP provisional responses and to use PRACK (Provisional Acknowledgement). Default: Disabled.

- **SIP Over TCP:** 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 SIP messages.

By default, SIP over TCP is enabled. If you want to receive SIP messages over TCP keep this option enabled.

You must also enable 'TCP' or 'TCP (Fallback to UDP)' on the SIP Trunk.

- **SIP Over TLS:** SETU VTEP supports transporting of SIP messages over TLS. TLS protects SIP signaling against loss of integrity, confidentiality and against replay.

By default, SIP over TLS is enabled. If you want to receive SIP messages over TLS keep this option enabled.

You must also enable 'TLS' on the SIP Trunk.

- **SIP UDP Port:** This is the port on which the 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. The valid range for this port is 1031–65534. Default: 5060.
- **SIP TCP Port:** This is the port on which the 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. The valid range for this port is 1031–65534. Default: 5060.
- **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. The valid range for this port is 1031–65534. Default: 5061.
- **RTP Listening Port:** This 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. The valid range for this port is 1032–65535. Default: 08000.
- **SIP INVITE Timer:** This is the time in seconds for which SETU VTEP waits for a response from the called party after sending INVITE message. This timer starts after sending INVITE message to the called party and stops on receipt of the provisional response or the final response or when the user disconnects the call. On expiry of the timer, the SETU VTEP terminates the call process and gives an error tone to the user. The range of the SIP INVITE TIMER is 10–200 seconds. Default: 30 seconds.
- **SIP Provisional Timer:** This is the time in seconds for which SETU VTEP waits for final response after receiving the provisional response from the called party. This timer starts on the receipt of the provisional response from the called party and stops on receipt of the final response from the called party or when the user disconnects the call. On expiry of the timer, the SETU VTEP terminates the call process and gives error tone to the user. The range of SIP Provisional Timer is 10–200 seconds. Default: 180 seconds.
- **General Request Timer:** This is the time in seconds for which the SETU VTEP waits for response of a transaction request. This timer starts on initiating a transaction and stops on the receipt of a response for the request. On expiry of the timer, the SETU VTEP clears the transaction. This timer is used for Registration request, etc. The range of the General Request Timer is 10–60 seconds. Default: 20 seconds.
- **T.38 Fax Block Size:** For T.38 negotiation, select an appropriate T.38 Fax Block Size in this field. You may select from the following options:
 - 10 msec
 - 20 msec
 - 30 msec

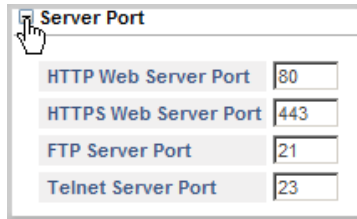
Default: 30 msec.



If you have made any changes in the NAT or SIP Parameters, all the current ongoing calls will be disconnected.

Server Port

- Click **Server Port** to expand and configure the following.

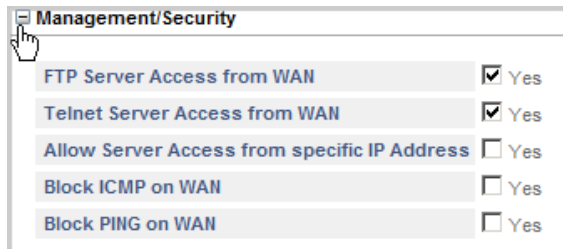


Server Port	
HTTP Web Server Port	80
HTTPS Web Server Port	443
FTP Server Port	21
Telnet Server Port	23

- HTTP Web Server Port:** SETU VTEP has an embedded web server called *Jeeves*, for system configuration. You can access *Jeeves* using HTTP. By default, HTTP Web Server Port is 80. You can change it as per your requirement. Valid range of the port is: 80, 1031-65535.
- HTTPS Web Server Port:** You can access *Jeeves* of SETU VTEP using HTTPS. By default, HTTPS Web Server Port is 443. You can change it as per your requirement. Valid range of the port is: 443, 1031-65535.
- FTP Server Port:** SETU VTEP has an embedded FTP server for Software Upgrade. By default, FTP Server Port is 21. You can change it as per your requirement. Valid range of the port is: 21, 1031-65535.
- Telnet Server Port:** You can access SETU VTEP using Telnet. By default, Telnet Server Port is 23. You can change it as per your requirement. Valid range of the port is: 23, 1031-65535.

Management/Security

- Click **Management/Security** to expand and configure the following.




Management/Security	
FTP Server Access from WAN	<input checked="" type="checkbox"/> Yes
Telnet Server Access from WAN	<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

- FTP Server Access from WAN:** Keep this check box enabled, if you want to allow users to access the system's FTP Server from the WAN Port.

You may clear this check box, if required. Default: Enabled.
- Telnet Server Access from WAN:** Keep this check box enabled, if you want to allow users to access the system using Telnet from the WAN Port.

You may clear this check box, if required. Default: Enabled.
- Allow Server access from specific IP Address:** Enable this check box, if you want to allow users to access system from specific IP Addresses only. Default: Disabled.

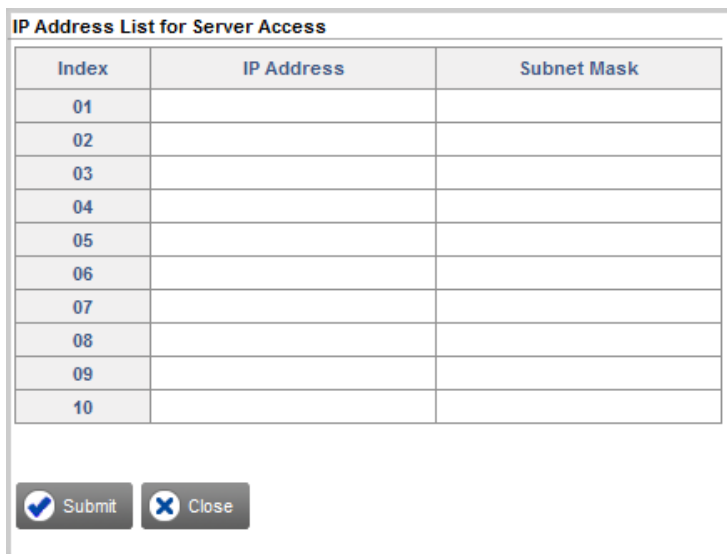
If you enable this parameter, you must configure the IP Address table for Server Access. To configure the IP Address table, Click **Settings** .



The image shows a 'Management/Security' settings window. It contains five rows of settings, each with a label and a checkbox. The third row, 'Allow Server Access from specific IP Address', has its checkbox checked and is highlighted with a red rectangle. A small arrow icon is visible next to the checked checkbox.


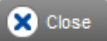
Management/Security	
FTP Server Access from WAN	<input checked="" type="checkbox"/> Yes
Telnet Server Access from WAN	<input checked="" type="checkbox"/> Yes
Allow Server Access from specific IP Address	<input checked="" type="checkbox"/> Yes 
Block ICMP on WAN	<input type="checkbox"/> Yes
Block PING on WAN	<input type="checkbox"/> Yes

The **IP Address List for Server Access** opens in a new window. You can store 10 entries in this table.



The image shows a window titled 'IP Address List for Server Access'. It contains a table with 10 rows and 3 columns: Index, IP Address, and Subnet Mask. The 'Index' column contains numbers 01 through 10. Below the table are two buttons: 'Submit' (with a checkmark icon) and 'Close' (with an 'X' icon).

Index	IP Address	Subnet Mask
01		
02		
03		
04		
05		
06		
07		
08		
09		
10		

- 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.



When you change the Jumper position (J3) to restore the default IP Address or to restore default Jeeves/Command Password, the following Server Access parameters will also be set to default.

- *FTP Server Access from WAN*
- *Telnet Server Access from WAN*
- **Block ICMP on WAN:** Enable this check box, if you want the system to discard the ICMP packets received on WAN. Default: Disabled.
- **Block PING on WAN:** Enable this 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 and acquire your IP Address.



Block PING on WAN will not be applicable, if you have enabled **Block ICMP on WAN**.

Certificate

- Click **Certificate** to expand and select the certificate for each of the following.

The screenshot shows a window titled "Certificate" with a list of five certificate selection options, each with a dropdown menu. A mouse cursor is pointing at the first option.

Local Certificate for	Selected Certificate
TLS	DefaultServerCert_Setu
WebServer	DefaultServerCert_Setu
Firmware Upgrade	DefaultServerCert_Setu
Configuration Upgrade	DefaultServerCert_Setu
TR069	DefaultServerCert_Setu

- In **Local Certificate for TLS**, select the certificate to be used by the system for TLS.
- In **Local Certificate for WebServer**, select the certificate to be used by the system for accessing the WebServer.
- In **Local Certificate for Firmware Upgrade**, select the certificate to be used by the system for Firmware Upgrade.
- In **Local Certificate for Configuration Upgrade**, select the certificate to be used by the system for Configuration Upgrade.
- In **Local Certificate for TR069**, select the desired certificate to be used by the system for TR069.

To create and Upload /Download Certificates, see ["Certificate Manager"](#).

- Click **Submit** to save changes.

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 listed below.

SETU VTEP offers as many as 24 number lists. Each number list can store up to 64 entries of a maximum of 24 characters each.

You need to configure number lists for the following features. 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 Trunks and T1/E1 port—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 list contains the numbers that are to be restricted from being dialed out from the source port.

Both lists must be programmed separately for each port first 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.

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 the method for Handling Incoming Calls is:
 - on the basis of Calling Party Number
 - to a Fixed Destination Number
 - on the basis of DDI 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, for Allowed Denied Logic for the T1/E1 port, Number list 1 is assigned for Allowed Numbers, Number List 2 for Denied Numbers. For Allowed Denied Logic for the SIP Trunk, Number list 7 is assigned

for Allowed Numbers and Number list 8 for Denied Numbers. You may retain these lists or configure any other Number list from 1 to 24.

- enable **Allowed-Denied Logic** on the SIP Trunks, on which you want to apply this feature, and the T1/E1 Port.
- assign the **Allowed Number List** and the **Denied Number List** you configured.

See “[Handling of Incoming Calls](#)” under “[SIP Trunks](#)”, “[Handling of Incoming Calls](#)” under “[T1 Port](#)”, “[Handling of Incoming Calls](#)” under “[E1 Port](#)” for instructions.

Black Listed Callers

The Black Listed Callers feature enables you to block incoming calls from specific numbers and addresses on the SIP Trunks. You can apply this feature on a 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 Caller** check box on the SIP Trunk on which you want to apply this feature.
- select the Number List you configured as **Black Listed Callers List**.

See “[Handling of Incoming Calls](#)” under “[SIP Trunks](#)” for instructions.

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 11 is assigned as the Black Listed Callers List. You may retain this list or configure another Number list from 1 to 24.



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 1 is assigned for both Called Party and Calling Party numbers. Since you cannot configure the same list for both, you may retain this list for one type of numbers and configure another Number list for the other type of numbers. You can configure any Number list from 1 to 24.

- 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**.

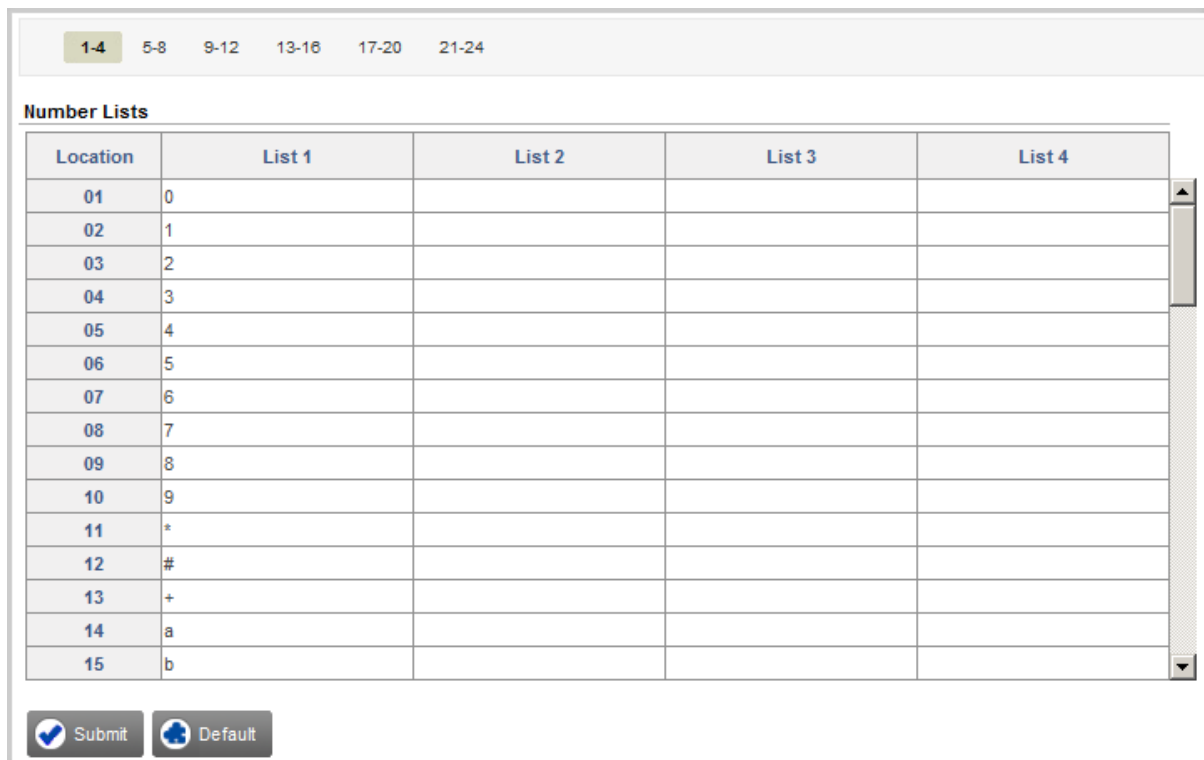
See [“Call Detail Record”](#) for instructions.

Configuring Number Lists

You must determine the purpose for which the list is required and accordingly prepare them.

To configure Number lists,

- Under Advanced Settings, click the **Number List** link.



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			
02	1			
03	2			
04	3			
05	4			
06	5			
07	6			
08	7			
09	8			
10	9			
11	*			
12	#			
13	+			
14	a			
15	b			

☒ Submit ☐ Default

- List 1 to 4 appear 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.

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 the T1/E1 Port.

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 need 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 trunks, on which you want to apply this feature.
- assign the **Automatic Number Translation Table** you configured.
- configure the **Pause Timer**, if applicable.

See [“Handling of Outgoing Calls”](#) under [“SIP Trunks”](#), [“General”](#) under [“T1 Port”](#) and [“General”](#) under [“E1 Port”](#).

Now, whenever there is a call on/from the SIP Trunk or the T1/E1 Port on 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

- Under Advanced Settings, click the **Automatic Number Translation (ANT)** link.

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	

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.

The Automatic Number Translation Table page will open. In this table, you can store as many as 24 Numbers at Index Numbers 01 to 24.

- In the **Number** column, 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 the **Strip Digit** column, enter the number of digits you want the system to strip off from the Called/Calling Number. You can configure from 00-24. Default: 00.

- In the **Add Prefix** column, 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.

Destination Number Determination

The process of routing calls originated on T1/E1 Port and SIP Trunks 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 number for the calls originated on SIP Trunks and on the T1/E1 port.

Destination Number Determination on SIP Trunks

For SIP Trunks, the system supports the following methods for Destination Number Determination:

- 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

To apply Destination Number Determination **on the basis of Calling Party Number**, you must configure the **Destination Number Determination: SIP-Calling 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 port.

To apply Destination Number Determination **on the basis of DDI Number**, you must configure the **Destination Number Determination: SIP-DDI Number Based** table.

When there is an incoming call on the SIP Trunk, SETU VTEP will match the DDI Number received in the SIP INVITE message with the entries of the DDI Number Based Table. If a match is found, the call is routed to the destination port.

Destination Number Determination on T1/E1 Port

For **T1/E1 Port with Orientation Type - Terminal**, the system allows you to configure the following destination number determination methods by Port, Channel and MSN 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 Digits

To apply Destination Number Determination **on the basis of Calling Party Number**, you must configure the **Destination Number Determination: T1E1-Calling Number Based** table.

When there is an incoming call on the T1/E1 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 port.

To apply Destination Number Determination **on the basis of DDI Number**, you must configure the **Destination Number Determination: T1E1-DDI Number Based** table.



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 configured for IP Dialing. (Refer “[IP Dialing](#)” feature for more details).

Configuring SIP-Calling Number Based Table

- Under Advanced Settings, click the **Destination Number Determination** link.
- Click the **SIP-Calling Number Based** link.

The Calling Number Based Table page opens. You can configure as many as 500 entries.

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		

- Configure following parameters in this table:
 - Enter the calling party numbers in the column **Calling Numbers**. Calling numbers may consist of a maximum of 24 characters. All ASCII characters are allowed. Default: Blank.
 - For each calling party number, enter a corresponding destination number in the column **Destination Numbers**. Destination numbers may consist of a maximum of 24 characters. Characters 0-9, *, # and dot (.) are allowed. Default: Blank.
- Click **Submit** to save your entries.
- Click **Default All** to clear all the entries.

Configuring SIP-DDI Number Based Table

To configure the DDI Number Based Table,

- Under Advanced Settings, click the **Destination Number Determination** link.
- Click the **SIP-DDI Number Based** link.

The DDI Number Based Table page opens. You can configure as many as 100 entries.

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

☒ Submit
 ☒ Default All

- There are two ways to generate the DDI Numbers:
 - Using the **DDI Number Generation** Button to automatically generate the DDI Number Table.
 - OR**
 - Entering each DDI Number manually.
- If you want to generate DDI Numbers automatically, click the **DDI Number Generation** button and configure the following parameters:

DDI Numbers Generation

Total DDI Numbers

Enter Start Index Number

Enter Start DDI Number

Enter Start Destination Number

Apply Reverse DDI (for all DDI Numbers) ☐

Enter Reverse DDI Reference ID (for all DDI Numbers)

☒ Apply
 ☒ Close

- **Total DDI Numbers:** The DDI numbers are allotted by the service provider. You must enter the total number of DDI numbers you want to generate in the DDI Number Based table. You can generate upto 100 numbers. Default: 10

- **Enter Start Index Number:** Enter the desired Index Number from where you want to start the DDI Number generation. Default: 1
- **Enter Start DDI Number:** Enter the start DDI Number. DDI Number can be of maximum 24 characters. Characters 0-9, +, * and # are allowed in this field.
- **Enter Start Destination Number:** Each DDI Number can be assigned a corresponding destination number. Enter the Start Destination Number corresponding to the Start DDI Number. Destination Number can be 24 characters long. Characters 0 to 9, # and * are allowed.
- **Apply Reverse DDI (for all DDI Numbers):** When the user makes a call from the assigned DDI number, this number will be displayed to the called party. Select the check box to apply Reverse DDI logic on all DDI Numbers.
- Click **Apply** button to generate the table. The DDI numbers generated will appear in the DDI Number Based Table.

DDI Number Generation

SIP Trunk - Destination Number Determination: DDI Number Based

Index	DDI Number	Destination Number	Reverse DDI	
			Apply	Reference ID
001	2630550	2001	<input checked="" type="checkbox"/>	1
002	2630551	2002	<input checked="" type="checkbox"/>	1
003	2630552	2003	<input checked="" type="checkbox"/>	1
004	2630553	2004	<input checked="" type="checkbox"/>	1
005	2630554	2005	<input checked="" type="checkbox"/>	1
006	2630555	2006	<input checked="" type="checkbox"/>	1
007	2630556	2007	<input checked="" type="checkbox"/>	1
008	2630557	2008	<input checked="" type="checkbox"/>	1
009	2630558	2009	<input checked="" type="checkbox"/>	1
010	2630559	2010	<input checked="" type="checkbox"/>	1

☒ Submit
 ☐ Default All

- You can also edit the generated numbers, if required.
- If you want to generate DDI Numbers manually,
 - Enter each DDI Number and its corresponding Destination Number against the desired Index in the table.
 - To apply **Reverse DDI** logic on the DDI Number, select the **Apply Reverse DDI?** check box.

The Reverse DDI **Reference ID** for the DDI Number, will be applied on the DDI Number.

For detailed instruction for generating DDI Numbers manually, see [“Route on the basis of DDI Number”](#) under SIP Trunks.

- Click **Submit** to save your entries.
- Click **Default All** to clear all the entries.

Configuring T1E1-Calling Number Based Table

- Click the **T1E1-Calling Number Based** link.

The Calling Number Based Table page opens. You can configure as many as 500 entries.

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		

- Configure following parameters in this table:
 - Enter the calling party numbers in the column **Calling Numbers**. Calling numbers may consist of a maximum of 24 characters. All ASCII characters are allowed. Default: Blank.
 - For each calling party number, enter a corresponding destination number in the column **Destination Numbers**. Destination numbers may consist of a maximum of 24 characters. Characters 0 to 9, *, # and (.) dot are allowed. Default: Blank.
- Click **Submit** to save your entries.
- Click **Default All** to clear all the entries.

Configuring T1E1-DDI Number Based Table

- Click the **T1E1-DDI Number Based** link.

The DDI Number Based Table page opens. You can configure as many as 1000 entries.

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

- There are two ways to generate the DDI Numbers:
 - Using the **DDI Number Generation** Button to automatically generate the DDI Number Table.
OR
 - Entering each DDI Number manually.
- If you want to generate DDI Numbers automatically, click the **DDI Number Generation** button and configure the following parameters:

- **Total DDI Numbers:** The DDI numbers are allotted by the service provider. You must enter the total number of DDI numbers you want to generate in the DDI Number Based table. You can generate upto 1000 numbers. Default: 10
- **Enter Start Index Number:** Enter the desired Index Number from where you want to start the DDI Number generation. Default: 1

- **Enter Start DDI Number:** Enter the start DDI Number. DDI Number can be of maximum 24 digits. Digits 0 to 9 are allowed in this field.
- **Enter Start Destination Number:** Each DDI Number can be assigned a corresponding destination number. Enter the Start Destination Number corresponding to the Start DDI Number. Destination Number can be 24 digits long. Digits 0 to 9, #, * and dot (.) are allowed.
- **Apply Reverse DDI (for all DDI Numbers):** When the user makes a call from the assigned DDI number, this number will be displayed to the called party. Select the check box to apply Reverse DDI logic on all DDI Numbers.
- Click **Apply** button to generate the table. The DDI numbers generated will appear in the DDI Number Based Table.

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

DDI Number Generation

T1E1 Port - Destination Number Determination: DDI Number Based

Index	DDI Number	Destination Number	Reverse DDI	
			Apply	Reference ID
001	2630555	2001	<input checked="" type="checkbox"/>	1
002	2630556	2002	<input checked="" type="checkbox"/>	1
003	2630557	2003	<input checked="" type="checkbox"/>	1
004	2630558	2004	<input checked="" type="checkbox"/>	1
005	2630559	2005	<input checked="" type="checkbox"/>	1
006	2630560	2006	<input checked="" type="checkbox"/>	1
007	2630561	2007	<input checked="" type="checkbox"/>	1
008	2630562	2008	<input checked="" type="checkbox"/>	1
009	2630563	2009	<input checked="" type="checkbox"/>	1
010	2630564	2010	<input checked="" type="checkbox"/>	1

☒ Submit

☐ Default All

- You can also edit the generated numbers, if required.
- If you want to generate DDI Numbers manually,
 - Enter each DDI Number and its corresponding Destination Number against the desired Index in the table.
 - To apply **Reverse DDI logic** on the DDI Number, select the **Apply** check box.

The Reverse DDI Reference ID for the DDI Number, will be applied on the DDI Number.

- Click **Submit** to save the entries.
- Click **Default All** to clear all the entries.

Destination Port Determination

The process of routing calls originated on T1/E1 Port and SIP Trunks 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 on the T1/E1 port.

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 **Destination Port Determination: SIP-Calling Number Based** table.

To apply Destination Port Determination **On the basis of Destination Number**, you must configure the **Destination Number Determination: SIP-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 **Destination Port Determination: T1E1-Calling Number Based** table.

To apply Destination Port Determination **On the basis of Destination Number**, you must configure the **Destination Number Determination: T1E1-Destination Number Based** table.

Configuring Destination Number Based Table

- Click the **Advanced Settings** link.
- Click the **Destination Port Determination** link.
- To configure the table for the SIP Trunk, click the **SIP-Destination Number Based** link. You can configure as many as 100 entries.

- To configure the table for the T1/E1 Port, click the **T1E1-Destination Number Based** link. You can configure as many as 1000 entries.

The Destination Number Based Table page opens.

SIP Trunk - Destination Port Determination - Destination Number Based

	Edit	Destination Number	Minimum Digits	Maximum Digits	Routing Group	Fallback Routing Group
		No Match Found	3	16	T1E1 Group 1	None

Total Records : 11

Add

Delete

- Click **Add** to add an entry. A new window opens.

Add Entry

Destination Number

Minimum Digits

Maximum Digits

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

- Configure the following parameters:
 - In the **Destination Number** field, enter the number (max. 24 characters) you expect callers to dial. Valid characters: 0 to 9, +, * and #. Default: blank.
 - In the **Minimum Digits** field, enter the minimum digits for the system to consider the destination number as a valid number. Range: 01 to 24. Default: 03.

If the dialed number string is less than the configured minimum length, the call will be rejected.
 - In the **Maximum Digits** field, enter the maximum number of digits of the destination number the caller must dial for the system to route the call.

If the number string dialed by the caller exceeds the maximum length configured, the system will strip off the extra digits, and route the call. Maximum length range: 01 to 24. Default: 16.

- Create the **Routing Group**.
 - To create a routing group of *sequential* T1/E1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* T1/E1 channels as members, select a **T1E1 Group Number**.

Click the settings icon and create the T1/E1 Group. See ["Group"](#) for further instructions.
 - To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.
 - To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group Number**.

Click the settings icon and create the SIP Group. See ["Group"](#) for further instructions.
- To create the **Fallback Routing Group**,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and the SIP Trunks.
- Click **Submit** to save changes. The **Edit** window closes.
- The Routing and Fallback Groups you created appear.
- To edit an entry, click **Edit**, a new window opens. Make the changes as per your requirement and click **Submit**.
- To delete an entry, select the check box and click **Delete**.
- Close the window to return to the main page.

Configuring Calling Number Based Table

- Click the **Advanced Settings** link.
- Click the **Destination Port Determination** link.
- To configure the table for the SIP Trunk, click the **SIP-Calling Number Based** link. You can configure as many as 500 entries.
- To configure the table for the T1/E1 Port, click the **T1E1- Calling Number Based** link. You can configure as many as 500 entries.

The Calling Number Based Table page 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

- Click **Add** to add an entry. A new window opens.

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 the **Calling Number** field, enter numbers (max. 24 characters) from which you expect calls to be received. All ASCII characters are allowed. Default: blank.
- Create the **Routing Group**.
 - To create a routing group of *sequential* T1/E1 channels as members,
 - Select the **T1E1 Port** number.

- In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
- 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 routing group of *not-sequential* T1/E1 channels as members, select a **T1E1 Group Number**.

Click the settings icon and create the T1/E1 Group. See [“Group”](#) for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group Number**.

Click the settings icon and create the SIP Group. See [“Group”](#) for further instructions.

- To create the **Fallback Routing** Group,
 - Select the **Apply** check box.
 - Follow the same instructions for creating *sequential* and *not-sequential* groups, for T1/E1 port and the SIP Trunks.
- Click **Submit** to save changes. The **Edit** window closes.
- The Routing and Fallback Groups you created appear.
- To edit an entry, click **Edit**, a new window opens. Make the changes as per your requirement and click **Submit**.
- To delete an entry, select the check box and click **Delete**.
- Close the window to return to the main page.

Group

SETU VTEP supports the following methods of determining the destination port for the calls originated on SIP Trunks and on the T1/E1 port.

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

For any of these methods that you select, you need to configure **Routing Group** and **Fallback Routing Group**.

A Routing Group may have *sequential* or *not-sequential* ports as members.

A Routing Group of *sequential* ports is to be formed when you select **SIP Trunk** or **T1/E1 Port** as the destination port.

A Routing Group of *not-sequential* ports is to be 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. A SIP Group can have only SIP Trunks as members. Similarly, a T1E1 Group can have only T1E1 channels as members.

SIP Group

You can create as many as 9 SIP Groups with maximum 9 SIP Trunks as members in each group. Decide which group number you want to assign as Routing Group and Fallback Routing Group.

To create a SIP Group,

- Under Advanced Settings, click the **Group** link.
- Click **SIP Group**.

SIP Trunk - Groups										
SIP Group Number	Member Selection Method	Member 1	Member 2	Member 3	Member 4	Member 5	Member 6	Member 7	Member 8	Member 9
1	First Free	01	02	03	04	05	06	07	08	09
2	First Free	01	None	None	None	None	None	None	None	None
3	First Free	02	None	None	None	None	None	None	None	None
4	First Free	03	None	None	None	None	None	None	None	None
5	First Free	04	None	None	None	None	None	None	None	None
6	First Free	05	None	None	None	None	None	None	None	None
7	First Free	06	None	None	None	None	None	None	None	None
8	First Free	07	None	None	None	None	None	None	None	None
9	First Free	08	None	None	None	None	None	None	None	None

- Select a SIP Group Number from **1 to 9**.
- Configure member ports - **Member 1 to Member 9**.
 - For each Member, select a SIP Trunk number from **01 to 32** from the combo box.

- If you do not want any more members in a group, select **None**. 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, 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 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, SIP Group Number 2 has four members SIP Trunk 7 (Member 1), 8 (Member 2), 9 (Member 3) and 10 (Member 4). For the first incoming call, SETU VTEP will check the status of Member 1 (SIP Trunk 7). If free, the call will be routed using this port else system will check status of Member 2 (SIP Trunk 8) and so on. For the next call, system will check status of Member 2 (SIP Trunk 8). If free, call will be routed using this port else Member 3 (SIP Trunk 9) will be checked. Similarly, for the subsequent call the system will check the next member port in the group.

Default: **First Free**.

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

T1E1 Group

You can create as many as 8 T1E1 Groups with maximum 4 members in each group.

To create T1E1 Group,

- Click **T1E1 Group**.

T1E1 Port - Groups															
T1E1 Group Number	Member Selection Method	Member 1				Member 2				Member 3					
		Port Number	Start Channel Number	Total Channels	Channel Selection Method	Port Number	Start Channel Number	Total Channels	Channel Selection Method	Port Number	Start Channel Number	Total Channels	Channel Selection Method		
1	First Free	1	01	30	Ascending	None	01	30	Ascending	None	01	30	Ascending		
2	First Free	1	01	30	Ascending	None	01	30	Ascending	None	01	30	Ascending		
3	First Free	1	01	30	Ascending	None	01	30	Ascending	None	01	30	Ascending		
4	First Free	1	01	30	Ascending	None	01	30	Ascending	None	01	30	Ascending		
5	First Free	1	01	30	Ascending	None	01	30	Ascending	None	01	30	Ascending		
6	First Free	1	01	30	Ascending	None	01	30	Ascending	None	01	30	Ascending		
7	First Free	1	01	30	Ascending	None	01	30	Ascending	None	01	30	Ascending		
8	First Free	1	01	30	Ascending	None	01	30	Ascending	None	01	30	Ascending		

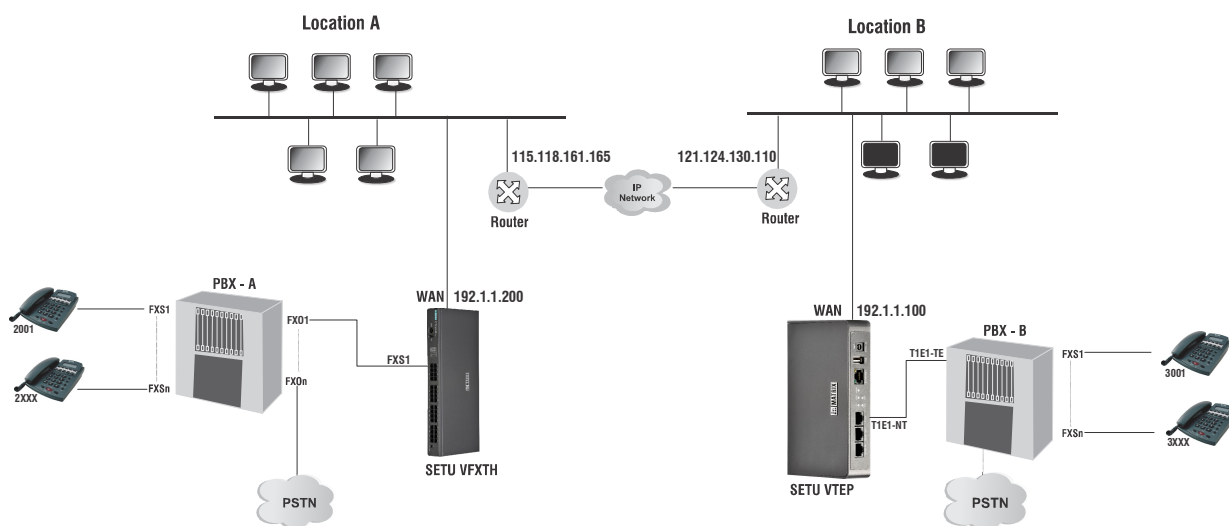
- Select a T1E1 Group Number from **1 to 8**.
- Configure members of the Group - **Member 1 to Member 4**. Each Member can have multiple channels.

- For each Member,
 - Select 1 as **Port Number**. If you do not want any more members in a group, select **None** as Port Number. E.g.: 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** from the combo box. While determining the destination port, SETU VTEP will select this channel first for routing the calls originated on the T1/E1 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. For the next call, system will check the second channel; if found busy the call will be routed to the third channel. For the third call the call will be routed to the third channel and so forth.
- Click **Submit** to save the groups.

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 VFXTTH 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 Trunks](#)” 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	Minimum Digits	Maximum Digits	Destination Address	Name
		No Match Found	3	16		
<input type="checkbox"/>		2001	3	16	115.118.161.165	Location A

Total Records : 21

Add

Delete

- 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 VFXTH at Location A routes this call through the FXS Port of the SETU VFXTH 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 Trunks](#)”.



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.


Peer-to-Peer Dialing

	Edit	Destination Number	Minimum Digits	Maximum Digits	Destination Address	Name
		No Match Found	3	16	192.168.1.100	

Total Records : 11

 Add

 Delete

 Close

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

Minimum Digits

Maximum Digits

Destination Address

Name

- In the **Destination Number** field, enter the peer-to-peer number string—prefix or entire number—that will be dialed. The number string must not exceed 24 characters. 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.

- As **Minimum Digits**, define the minimum length of the number string that must be dialed for the system to consider it as a valid number. Default: 03.
- As **Maximum Digits**, define the maximum length of the number string that must be dialed out for the system to consider it the complete number string. Default: 16.
- 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 of up 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.

PIN Authentication

PIN Authentication is a necessary security feature to restrict access to the system and prevent possible misuse of 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 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 up to 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 a feature 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 attempts, the system disconnects the call.

Configuring PIN Authentication

You can enable PIN Authentication and configure the PIN Authentication Table on the desired ports on the SIP Trunk page and T1E1 Port page under *Basic Settings*.

If you have not already configured the PIN Authentication on the T1/E1 Port or SIP Trunk page, you may configure the PIN Authentication table now.

To configure PIN Authentication table,

- Under Advanced Settings, click the **PIN Authentication** link and configure the PIN Authentication table.

1-100
101-200
201-300
301-400
401-500

PIN Authenticaon

Index	PIN Number	PIN Password
001		
002		
003		
004		
005		
006		
007		
008		
009		
010		
011		
012		
013		
014		
015		

✓ Submit
+ Default All

- In the **PIN Number** column, 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 the **PIN Password** field. 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 T1/E1 port or SIP Trunk(s) under [“Basic Settings”](#).

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 authorised 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, namely the User Name and Passwords 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**.

When you enable this feature on a SIP trunk, for all incoming calls (SIP requests),

- SETU VTEP will challenge the identity of the calling party, i.e. 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, make sure you have enabled **Digest Authentication** on the desired SIP Trunk and configure the Digest Authentication Table.

If you have not already configured the Digest Authentication Table on the SIP Trunk parameters page, you may do so now.

- Under Advanced Settings, click the **Digest Authentication** link.

The Digest Authentication Table page opens. You can configure upto 500 entries in this table. This Table is common for all SIP Trunks.

Digest Authentication

Index	User ID	User Password
001		
002		
003		
004		
005		
006		
007		
008		
009		
010		
011		
012		
013		
014		
015		

Submit Default All

- Enter the user name assigned to the caller/calling device in the **User ID** field. 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 can be up to 40 characters long. Default: Blank.

- Enter the password to authenticate the user ID in the **User Password** field. 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.

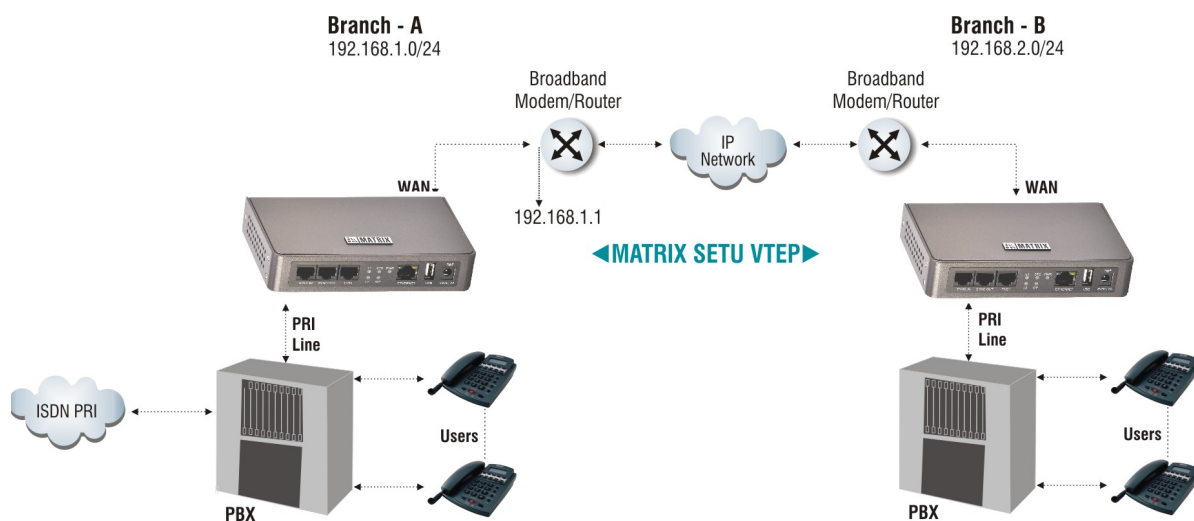
You can configure the Digest Authentication Table from the SIP Trunk parameters page of Jeeves also. See [“SIP Trunks”](#) under *Basic Settings* for instructions.

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 “[Network Parameters](#)” the page.



The Static Routing Table is common for all SIP Trunks.

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,

- Under Advanced Settings, click the **Static Routing Table** link. The Static Routing Table page opens.

Index	Destination Address	Subnet Mask	Gateway Address
1			
2			
3			
4			
5			
6			
7			
8			

The Static Routing Table allows you to configure up to 8 entries.

For each entry, you must configure the following fields:

- Destination Address:** This is the address of the final destination where the call is to be made. This can be a device IP Address or Network Address.
- Subnet Mask:** This is the mask to be applied on the destination address.
- Gateway Address:** This is 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.

- Click **Submit** to save your entries.

To take the above example further, 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			
:			

Index	Destination Address	Subnet Mask	Gateway Address
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 in location A.

With the Static Routing Table configured thus, 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 address 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 Codes

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 assigned to them from a phone.

- Making a New Call (**#91**)
- Disconnect Call (**#92**)
- Knowing the current IP Address (**#51**), Subnet Mask (**#52**), Gateway Address (**#53**) and DNS Address (**#54**) of the system.



The access codes for knowing the IP Address, Subnet Mask, Gateway Address and DNS Address of the system are applicable on the T1/E1 port only.

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,

- Under Advanced Settings, click the **Access Code** link.

Access Codes	
Making a New Call	#91
Disconnect Call	#92
Ip Address	#51
Subnet Mask	#52
Gateway Ip Address	#53
DNS Address	#54

☒ Submit ☐ Default

- Change the default access code for the feature/facility, as required.



Do not configure Access Codes that may conflict with the Emergency Numbers.

- Click **Submit** to save changes.

Emergency Numbers

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,

- Under Advanced Settings, click the **Emergency Numbers** link.

	Emergency Number	Routing Group
<input type="checkbox"/> Edit		

- To **Add** an Emergency Number to the table, click the **Add** button.

- To **Edit** an Emergency Number and or assign a Routing Group, click the settings icon of that number.

A new window opens, allowing you to add/edit the entry.

- In the **Emergency Number**, enter the emergency numbers used in your country/region.



Make sure that Access Codes you have configured do not conflict with the Emergency Numbers.

- Create the **Routing Group**.
 - To create a routing group of *sequential* T1/E1 channels as members,
 - Select the **T1E1 Port** number.
 - In the Channel Number **From - to** options, select the **Start Channel Number** and the **End Channel Number**.
 - 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 routing group of *not-sequential* T1/E1 channels as members, select a **T1E1 Group Number**.

Click the settings icon and create the T1E1 Group. See [“Group”](#) for further instructions.

- To create a routing group of *sequential* SIP Trunks as members,
 - Select the **SIP Trunk** numbers as members.
 - In the **in - order** field, select the order in which the system should check for a free member SIP Trunk to route the call.

Select **Ascending** to start checking from the first to the last member SIP Trunk. Select **Descending** to start checking from the last to the first member SIP Trunk. Default: Ascending.

- To create a routing group of *not-sequential* SIP Trunks as members, select a **SIP Group Number**.

Click the settings icon and create the SIP Group. See [“Group”](#) for further instructions.

- Click **Submit** to save changes you made. Close the **Add Entry/Edit Entry** window.

Certificate Manager

SETU VTEP supports certification for TLS, Web Server, Firmware Upgrade, Configuration Upgrade and TR-069.

SETU VTEP supports two types of Certificates: **Self-signed Certificate** and **CA Signed Certificate**.

Self-Signed Certificate

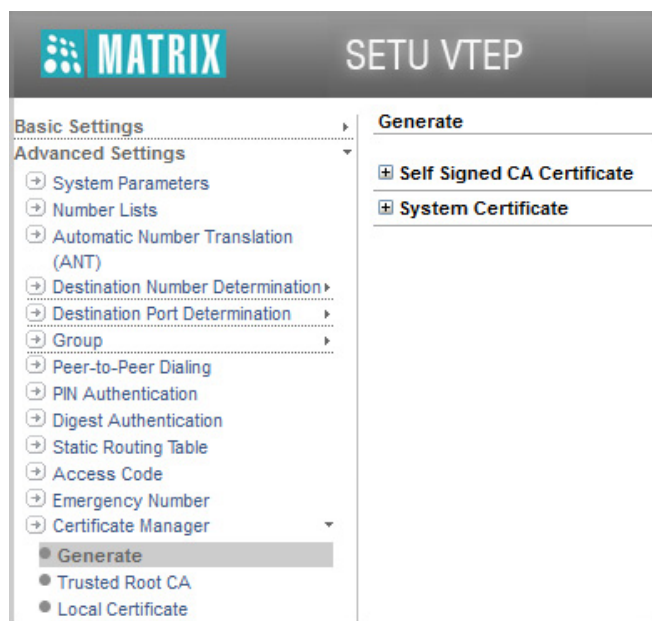
A self-signed certificate is created by the clients themselves or by the Servers and then given to their clients. It means that you yourself become the Certificate Authority (CA), create a CA Certificate and sign it. The self-signed certificate is faster to create but is not signed by a trusted CA Organization. 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' trusted 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

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Certificate Manager** link.
- Click the **Generate** link.



- Click **Self Signed CA Certificate** to expand and configure the following parameters.

Self Signed CA Certificate

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.)	
Email Address (eg. me@myhost.mydomain)	

Generate

Download

- In **Country Name - 2 letter code (eg. 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 (eg. city)**, enter the name of your city.
- In **Organization Name (eg. company)**, enter the name of your organization where SETU VTEP is installed.
- In **Organizational Unit Name (eg. section)**, enter the name of the unit or section or domain of your organization, where SETU VTEP is installed.
- In **Common Name (eg. 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 (eg. me@myhost.mydomain)**, enter your host's e-mail address.
- 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.
- Under **Certificate Manager**, click the **Trusted Root CA** link. The CA Certificate you created appears in the **Root CA Certificate** table.

Trusted Root CA

Upload CA Certificate

Browse...

(Valid format .cer, .crt & .pem)

Upload

Root CA Certificates

	Issued To	Issued By	Expiration Date	Friendly Name
<input type="checkbox"/>	www.MatrixComSec.com	www.MatrixComSec.com	Dec 31 2036	SelfSignedCaCertificate

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 under:

```
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: Aug 13 13:13:18 2013 GMT
      Not After : Dec 31 13:13:18 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
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:da:9e:27:ae:64:58:1d:88:d1:58:10:96:1d:42:
          cf:7a:cc:ef:07:ef:66:8c:93:1e:66:3b:15:07:60:
          ea:87:f0:72:a2:93:de:31:05:64:97:92:14:e9:31:
          47:3e:d2:dd:13:d3:06:d0:19:d4:f9:d6:b9:b6:f3:
          9a:0c:ec:bb:bd:eb:1e:b5:24:1a:30:a5:53:2f:d5:
          74:54:a9:10:fa:da:f1:39:05:3d:7d:09:cd:d6:d6:
          23:37:d1:c4:d7:a4:a7:34:22:70:66:4d:b0:65:f9:
          3b:bf:06:d0:1a:e8:97:e0:ef:c0:9e:ef:40:f1:c4:
          c9:e2:a7:7e:03:b6:72:00:fd:8c:02:c5:57:9c:57:
          fc:99:8c:36:22:9f:e9:7a:32:49:27:a5:11:21:3d:
          f9:e9:6f:d2:1f:88:65:a9:45:5a:99:e2:1a:51:cb:
          69:31:b1:dc:06:7b:ef:94:24:2e:c0:f9:f0:bd:25:
          67:6a:e5:e9:46:f7:e8:d7:6c:f5:5c:ed:dc:cd:7c:
          82:02:0f:7d:f7:fd:0b:66:d0:ee:24:e1:2b:64:97:
          58:27:3b:96:bd:dd:b4:ea:3f:51:f7:a5:2c:dd:c7:
          22:72:b9:3c:09:75:04:df:56:5b:af:f8:3d:fe:f0:
          50:3f:01:c9:8e:2a:3e:36:66:1f:fe:dd:87:84:99:
          11:7b
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      Netscape Comment:
        OpenSSL Generated Certificate
      X509v3 Subject Key Identifier:
```

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 your 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 **Certificate Manager** link.
- Click the **Generate** link.
- Click **System Certificate** to expand and configure the following parameters.

- 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 (eg. 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 (eg. city)**, enter the name of your city.
- In **Organization Name (eg. company)**, enter the name of your organization where SETU VTEP is installed.
- In **Organizational Unit Name (eg. section)**, enter the name of the unit or section or domain of your organization, where SETU VTEP is installed.
- In **Common Name (eg. 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 (eg. 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.
- 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

Browse...

(Valid format .cer, .crt & .pem)


Upload Private Key

Browse...

(Valid format .pem & .key)

Upload


Local Certificates

	Issued To	Issued By	Expiration Date	Friendly Name	Download
<input type="checkbox"/>	www.MatrixComSec.com	www.MatrixComSec.com	Dec 31 2036	DefaultServerCert_Setu	

Delete

- 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 Self-Signed System Certificate is as under:

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: Aug 13 13:14:57 2013 GMT

Not After : Dec 31 13:14:57 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

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:b5:29:61:26:35:db:d7:a8:fd:05:4d:ac:2d:6c:
65:70:4d:42:fb:f6:1e:c8:18:bd:1c:c7:5a:92:b3:
28:52:48:66:7c:0f:c8:35:6f:13:46:62:1e:23:44:
b3:27:28:f5:8e:43:1a:e3:f6:7e:d5:8f:a9:73:8a:
2c:34:1e:35:d0:c8:0c:b2:68:12:dc:1a:23:da:fe:
02:af:88:4e:a1:7a:7f:a0:2b:ca:b9:72:5d:ac:3a:
e3:9b:fd:0d:ab:0f:c3:57:a9:99:cd:2e:be:02:9c:
60:0e:83:e8:69:2d:0f:95:79:52:87:66:9f:4a:10:
09:db:4e:41:e2:f2:b4:86:cd:42:a9:55:6d:33:a3:
60:67:fd:1d:3d:0e:8d:6a:53:77:e0:07:78:c9:c8:
34:23:df:3d:94:02:41:e9:c4:2b:c8:04:10:ba:69:
dc:d3:4c:85:39:09:a6:df:c4:1d:2d:80:2b:d8:f6:
88:0a:c6:98:3f:85:34:19:c0:a5:fe:d9:f8:96:39:
ec:cb:b7:c5:fa:84:e1:93:6d:82:7c:12:70:cf:67:
5d:95:15:e9:1a:71:18:ad:f7:3f:09:1b:f5:0f:80:
fb:9e:e9:96:54:91:59:39:6b:dd:5f:02:22:b9:c6:
2a:60:e8:76:61:88:84:fl:e1:74:a1:17:12:66:98:
6a:93

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

In the above Self-Signed System 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 contains 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

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Certificate Manager** link.
- Click the **Generate** 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)

☒ 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 (eg. 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 (eg. city)**, enter the name of your city.
- In **Organization Name (eg. company)**, enter the name of your organization where SETU VTEP is installed.

- In **Organizational Unit Name (eg. section)**, enter the name of the unit or section or domain of your organization, where your SETU VTEP is installed.
- In **Common Name (eg. 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 (eg. 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 (eg. me@myhost.mydomain)**, enter your host's e-mail address.
- 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-----
MIIDLDCCAQCAQAwgaoxCzAJBgNVBAYTAklOMRAwDgYDVQQIEwdHdWphcmFOMREw
DwYDVQQHEWhWYWRvZGFyYTEgMB4GA1UEChMXTUUFUUK1YIENPTVNFQyBQV1QuIExU
RC4xDDAKBgNVBAsUA1ImRDEdMBsGA1UEAxMUd3d3Lk1hdHJpeENvbVNiYy5jb20x
JzAlBgkqhkiG9w0BCQEWGfN1cHBvcnRATWF0cm14Q29tU2VjLmNvbTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAPutA1/cZcz/qZe3soIITiVpPI8PIZ6d
9RvInx4haqVob7Ml10dYWvN2rLmFod3ZtEu9dX645crC4NXn9pxKXmkp5iNdBVca
rm1qed263S1cR3m4YhL2dUc7DQ9T1GNTPbXLr1A4sQk+nVwO+C+XU/jPlpqiR0sn
Idh2/eLWVOauRgY3qdGjPaN8ndq8xVieY+v1/XpLQa4Oyd6aP+xn+z4pSWK4YLeP
36/CRh5q4f3vfMpuQTfegxGA+UB1V3qPMSqI0jBr7r1jptDxlmwzXkwz5w1rovh8
ZNP+1sIYPyZ9zrZm+eyhxpSX8o09jCcEm/R816x6GHEER7UGdZR1HvUCAwEAAaA8
MDoGCSqGSIb3DQEJDDjEtcMscwCQYDVROTBAlwADALBgNVHQ8EBAMCBwAwEQYDVRO
BAowCIIGTWF0cm14MA0GCSqGSIb3DQEBBQUAA4IBAQCQtMjN13HAWYa9w1JGbKW
Yjoc/gbrhSUwgbR4Jh+13guInViTyJ5YDt9pLc8xzJe23MV2XDv4ImSSUSkRojcg
IpVTqNPgf91k50WmJHTIT0JJGEUXvzKE71V0kuf0XTelW0o81QYpjGn8GaSQQCDV
q746F0i84zwsejY+/jL+pDMpczxvbn0tWg+wCkMXwdkAk0InqL+DuSTEnuBecW82
UF0rqoMdt90XpS9YZpjIsotRYgTRNIFaBFF4LxQa1bYQ15p279MxWJIZQ2TnqHf
MbwSosS/QM7ZjE147b13m9Lk69jdzfSAPmCW4AdulBe7PENGGI+MMzfAVyYSwdkw
-----END CERTIFICATE REQUEST-----
```

Enrolling the Certificate Signing Request with CA

Enrollment is a process of obtaining a certificate from any trusted third party (CA). After you have generated the Certificate Signing Request (CSR), you must contact any authorized third party that issues TLS Certificates to companies or web owners, such as Thawte, VeriSign, etc. and enroll the Certificate Signing Request (CSR) with them. These third parties Certificate Authorities (CA) have their charges to sign and validate the Certificate Signing Request (CSR) for a year. After the Certificate Signing Request (CSR) has been validated and signed by the CA, it becomes the CA Signed Certificate.

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:

- Log into Jeeves.

- Click the **Certificate Manager** link.
- Click the **Local Certificate** link.

Local Certificates

Upload Certificate

Browse...

(Valid format .cer, .crt & .pem)


Upload Private Key

Browse...

(Valid format .pem & .key)

Upload

Local Certificates

<input type="checkbox"/>	Issued To	Issued By	Expiration Date	Friendly Name	Download
<input type="checkbox"/>	www.MatrixComSec.com	www.MatrixComSec.com	Dec 31 2036	DefaultServerCert_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 Record

SETU VTEP enables you to generate reports of Call Detail Records of calls using various filters such as:

- The port from which the calls originated (Source Port)
- The port on which the calls terminated (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 those 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 maximum 2000 call record entries and these entries are stored using the First In First Out (FIFO) method.

Call records remain stored,

- when the system is set to default.
- when the firmware version is changed.

Call records can be cleared manually at any time.

Configuring Call Detail Record Filters

- Under Advanced Settings, click the **Call Detail Record (CDR)** link.

Setting Filters

- To set filters, click the **Filters** link under Call Detail Record.

Call Details Record (CDR) Filters			
Filter	Apply Filter	From	To
Calls originated from SIP Trunks	<input checked="" type="checkbox"/>	01	32
Calls originated from T1E1 Ports	<input checked="" type="checkbox"/>	1	1
Calls originated from T1E1 Channels	<input checked="" type="checkbox"/>	01	30
Calls terminated on SIP Trunks	<input checked="" type="checkbox"/>	01	32
Calls terminated from T1E1 Ports	<input checked="" type="checkbox"/>	1	1
Calls terminated on T1E1 Channels	<input checked="" type="checkbox"/>	01	30
Calls Made From	<input checked="" type="checkbox"/>	01 - Jul - 2010	05 - Jan - 2009
Calls Made Between	<input checked="" type="checkbox"/>	00 : 00	23 : 59
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"/>			
<input checked="" type="button" value="Submit"/> <input type="button" value="Default"/>			

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, without filters.

- Calls originated from SIP Trunks:** The system will generate report of calls that originated from SIP Trunks, i.e. 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, set 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 Port:** The system will generate report of calls that originated from the T1/E1 port.
- 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 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 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 Port:** The system will generate report of calls that terminated on the T1/E1 port.
- **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 channels in the **From** and **To** fields.

To generate report for calls terminated on a single channel, set the same channel number in both 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 a 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 the details 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.

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.

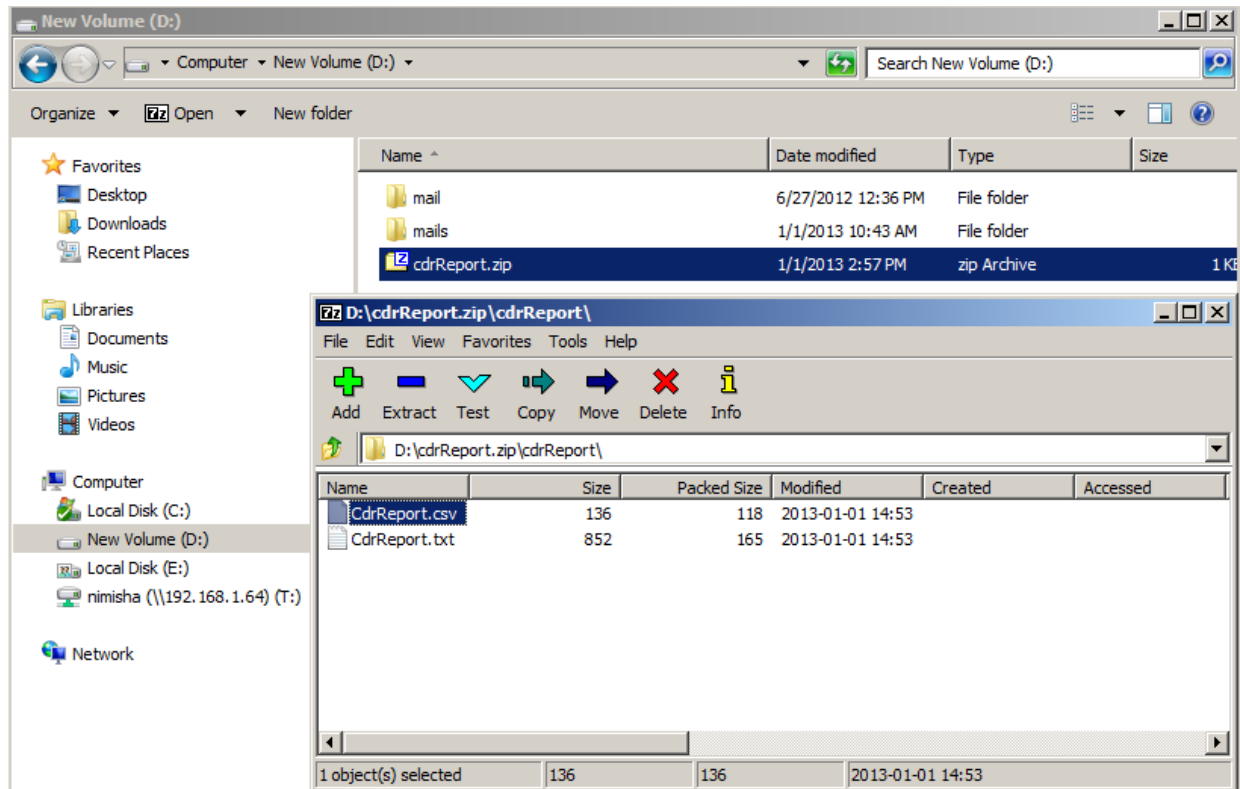
The screenshot shows the 'Call Details Record (CDR) Filters' window. It contains a table with filter categories, an 'Apply Filter' checkbox, and 'From' and 'To' date pickers. A Firefox download prompt is overlaid on the window, asking 'What should Firefox do with this file?' for 'cdrReport.zip'. The prompt offers options to 'Open with WinRAR archiver (default)' or 'Save File', and a checkbox for 'Do this automatically for files like this from now on.'.

Filter	Apply Filter	From	To
Calls originated from SIP Trunks	<input checked="" type="checkbox"/>	01	32
Calls originated from T1E1 Ports	<input type="checkbox"/>		1
Calls originated from T1E1 Channels	<input type="checkbox"/>		30
Calls terminated on SIP Trunks	<input type="checkbox"/>		32
Calls terminated from T1E1 Ports	<input type="checkbox"/>		1
Calls terminated on T1E1 Channels	<input type="checkbox"/>		30
Calls Made From	<input type="checkbox"/>		- Jan - 2009
Calls Made Between	<input type="checkbox"/>		23 : 59
Called Party Numbers Matching with	<input type="checkbox"/>		
Calling Party Numbers Matching with	<input type="checkbox"/>		
Call Duration equal to and greater than	<input type="checkbox"/>		0
Calls without PIN Number	<input type="checkbox"/>		
Calls with PIN Number	<input type="checkbox"/>		9999

Buttons: Clear Call Records, Download Call Records

Buttons: Submit, Default

- 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

- To view the report generated by the system for the filters you set, click the **Report** link under Call Detail Record.

Sr. No.	Date	Start Time	Calling Number	Called Number	Duration (sec)	Source Port	Destination Port
0001	21-May-2012	17:59	192.168.1.137	1234	00:00:15	SIP-01	SP-01
0002	21-May-2012	18:00	192.168.1.137	1234	00:00:09	SIP-01	SP-01
0003	21-May-2012	18:06	192.168.1.137	5678	00:00:05	SIP-01	SP-01
0004	21-May-2012	18:25	192.168.1.137	3698	00:00:15	SIP-01	SP-01
0005	22-May-2012	11:06	192.168.1.137	2001	00:00:00	SIP-01	SP-01
0006	22-May-2012	16:03	3001	192.168.201.7	00:00:36	T1E1-1-01	SP-01
0007	22-May-2012	16:09	3001	192.168.201.7	00:00:28	T1E1-1-01	SP-01
0008	22-May-2012	17:09	3001	658	00:00:00	T1E1-1-01	SP-01
0009							
0010							
0011							
0012							
0013							
0014							
0015							
Total Records : 8 1							

- 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 between 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/T1/E1 Ports/T1E1 Channels.
 - Destination Port:** Calls terminated on the SIP Trunks/T1/E1 Ports/T1E1 Channels.
 - Disconnected By:** The port/channel 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-Normal.

The total number of 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 T1E1 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 Trunks”](#), [“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 Trunks”](#), [“E1 Port”](#) and [“T1 Port”](#) under *Basic Settings* for instructions.

To Disconnect a Call using Access Code, dial **#92**.

IP Dialing

SETU VTEP supports direct dialing of IP Addresses from the source port. To provide IP Dialing facility to the users, you must configure a SIP Trunk or a SIP Group for IP Dialing.

When a number is dialed out from the source port, SETU VTEP routes the call to the desired destination as per the routing mechanism configured for that port. However, when an IP Address is dialed from the source port of SETU VTEP, the system does not check the Destination Port Determination method you have configured for that port, instead it routes the dialed IP Address through the SIP Trunk or SIP Group you configured for IP Dialing.

When dialing an IP Address, users must press * key (star/asterisk) in place of. (dot/period) in the IP Address.

For example, to call the IP Address **192.167.100.1**, users must dial **192*167*100*1** or **192*167*100*001**

SETU VTEP interprets the * you dialed as a '.' (dot/period).

To provide this feature to users,

- you need to select a **SIP Trunk** or a **SIP Group** through which the dialed IP Addresses are to be routed.

If you want to use a SIP trunk group for IP Dialing, you must configure a SIP Group first. This Group is common for all port types. See the topic [“Group”](#) for instructions.

When you assign a SIP Trunk, make sure it is enabled and has the necessary configuration done. See [“SIP Trunks”](#) under *Basic Settings* for instructions.

- assign the SIP Trunk you want or the SIP Group you configured to **SIP Trunk for IP Dialing** in the System Parameters. See [“System Parameters”](#) under *Advanced Settings* for instructions. By default, SIP Group 1 is selected for IP Dialing in the System Parameters.

Knowing Network Information using Access Codes

You can know the current IP Address, Subnet Mask, Gateway Address and DNS Address of SETU VTEP by dialing the specific access codes on the T1/E1 port.

To do this,

- Call the ISDN Number of the T1/E1 Port.
- To know the current IP Address, dial **#51**
- To know the current Subnet Mask, dial **#52**
- To know the current Gateway Address, dial **#53**
- To know the current DNS Address, dial **#54**
- The system will announce the IP Address, Subnet Mask, Gateway Address and DNS Address according to the access code you dial.

Firmware Upgrade

You can upgrade Firmware of SETU VTEP:

1. From a Provisioning Server
2. From a Personal Computer

Firmware Upgrade from Provisioning Server

Auto Firmware Upgrade

Using Auto-Firmware Upgrade, SETU VTEP can automatically upgrade its firmware by downloading the firmware files stored at a central location: HTTP Server or HTTPS Server or Provisioning Server.

This feature is useful for ITSPs that have Provisioning Servers to store the firmware files. ITSPs can update the firmware of SETU VTEP provided to their customers from a centralized location without physically visiting the customer premises.



*For the **Auto Firmware Upgrade File** contact Matrix Support Team.*

To perform Auto-Firmware Upgrade,

1. ITSPs must store the following Auto firmware upgrade files of SETU VTEP on the Provisioning Server.
 - matrix_firmware.html file
 - SETU VTEP_VxRy.Zip file
2. The following parameters must be configured in the SETU VTEP.
 - IP Address of the Provisioning Server.
 - Path of the Folder (containing the firmware files) on the Provisioning Server.
 - The protocol to be used: HTTP, HTTPS.
3. When SETU VTEP installed at a customer site gets connected to the ITSP network, it will automatically compare its current firmware with the firmware files stored on the Provisioning Server.

The matrix_firmware.html file helps SETU VTEP decide which firmware it should upgrade to.

- After SETU VTEP decides the Firmware Version/Revision to upgrade to, it will send the request for the firmware files to the Provisioning Server. Once the respective firmware files are received, SETU VTEP will upgrade its current firmware with the new firmware without the intervention or assistance of a technician.

The table below describes a few possible cases and the corresponding action taken by SETU VTEP.

Version-Revision of your SETU VTEP	Version- Revision in the matrix_firmware.html file received from the Provisioning Server	Action Taken by SETU VTEP
V1R5	V1R4	SETU VTEP will accept and upgrade its current firmware with V1R4.
	V1R5	SETU VTEP will discard the upgrade process.
	V1R6 and V1R6.1	SETU VTEP will accept and upgrade its current firmware with V1R6.1.
	V1R4, V1R5 and V1R6	SETU VTEP will accept and upgrade its current firmware to the highest version, V1R6.
	V2R2_V2R1, V2R1, V1R8	Highest Version available is V2R2, however, V2R2 has a benchmark of V2R1. Therefore, SETU VTEP will first upgrade with V2R1 and then with V2R2.

To configure Auto Firmware Upgrade parameters,

- Under Maintenance, click the **Firmware** link.

- Select the **Auto Firmware Upgrade** check box. Default: Disabled.
- Select the **Protocol for Auto Firmware Upgrade** to be used by the Provisioning Server to upgrade the firmware of SETU VTEP. SETU VTEP generates file transfer request to the server according to the protocol you select. You may select **HTTP** or **HTTPS**. Default: HTTP.
- Server Address: Port:** Enter the IP Address/Domain and Port of the Provisioning Server on which the firmware files of SETU VTEP are stored.

The Provisioning Server Address can also be obtained by SETU VTEP using DHCP (using Option 224). To fetch Provisioning Server Address using DHCP, keep the Server Address: Port field blank.

If you want SETU VTEP to get the Server Address from the DHCP server, keep this field blank. Make sure that you also set the *Connection Type* on the “[Network Parameters](#)” page to *DHCP*.

The default Port differs as per the protocol you select. For HTTP, the Default Port is 80 and for HTTPS, the Default Port is 443. You can also change the port as per your requirement. Valid Port Range: 80, 443, 1031 to 65534.

- **Firmware Folder Path:** Specify the path of the folder on the Provisioning Server where the firmware files are stored. Default: Blank.
- **Upgrade Firmware Automatically at Every Power ON:** Enable this check box, if you want SETU VTEP to check for updates in the firmware at each power ON.



- *At Power ON, if both Auto-Firmware upgrade and Auto-Configuration upgrade is enabled, Auto-Firmware upgrade has priority over Auto-Configuration upgrade.*
- *While upgrading itself, if SETU VTEP has to upgrade itself with the benchmark firmware first then it is recommended that you select **Upgrade Firmware Automatically at Every Power ON**.*
- **Upgrade Firmware Automatically at Scheduled Time:** Enable this check box, if you want SETU VTEP to check for updates in the firmware at a scheduled time. You may select any one of the following schedule options:
 - **Every XX minutes:** The minutes after which SETU VTEP should check for firmware updates.
 - **Everyday at HH:MM:** The time in **Hours (00-23)** and **Minutes (00-59)** when SETU VTEP should check for firmware updates everyday.
 - **Every Month on DD at HH:MM:** The **Date (01-31)** and Time in **Hours (00-23)** and **Minutes(00-59)** when SETU VTEP should check for firmware updates every month.



*If SETU VTEP has to upgrade itself with the benchmark firmware and you have selected **Upgrade Firmware Automatically at Scheduled Time**, SETU VTEP will first upgrade itself with the benchmark firmware. At the next scheduled time, it will upgrade itself with the final firmware.*

- **Request Timeout:** Request Timeout is used when SETU VTEP tries to connect to the Provisioning Server for TCP/TLS binding. 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 Provisioning Server, it will make 10 attempts at a regular interval of 10 seconds between each attempt to establish the binding. Even then, if it is unable to establish the binding, it will abort the Auto upgrade process.

- Click **Submit** to save.
- To view the status of Auto-Firmware Upgrade from Jeeves, see “[Firmware](#)” under “[Status](#)” Chapter.

Manual Firmware Upgrade

You can manually upgrade Firmware of SETU VTEP, whenever you want.

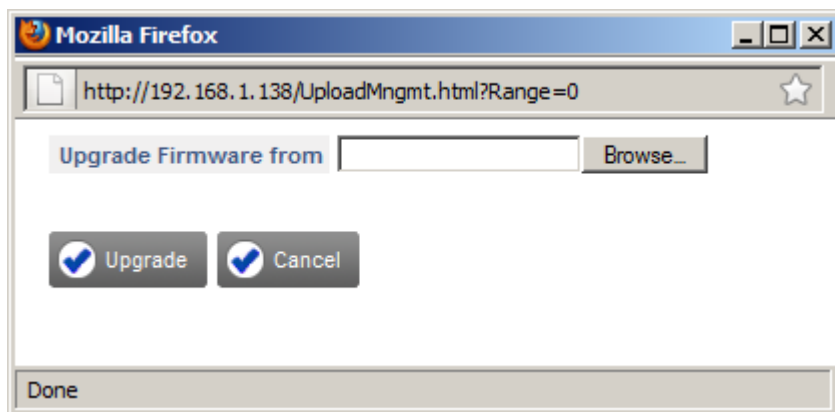
To manually upgrade firmware of SETU VTEP from server,

- Click the **Upgrade Firmware from Server** button on the Firmware page. SETU VTEP will automatically upgrade its firmware with the latest firmware available on the server.

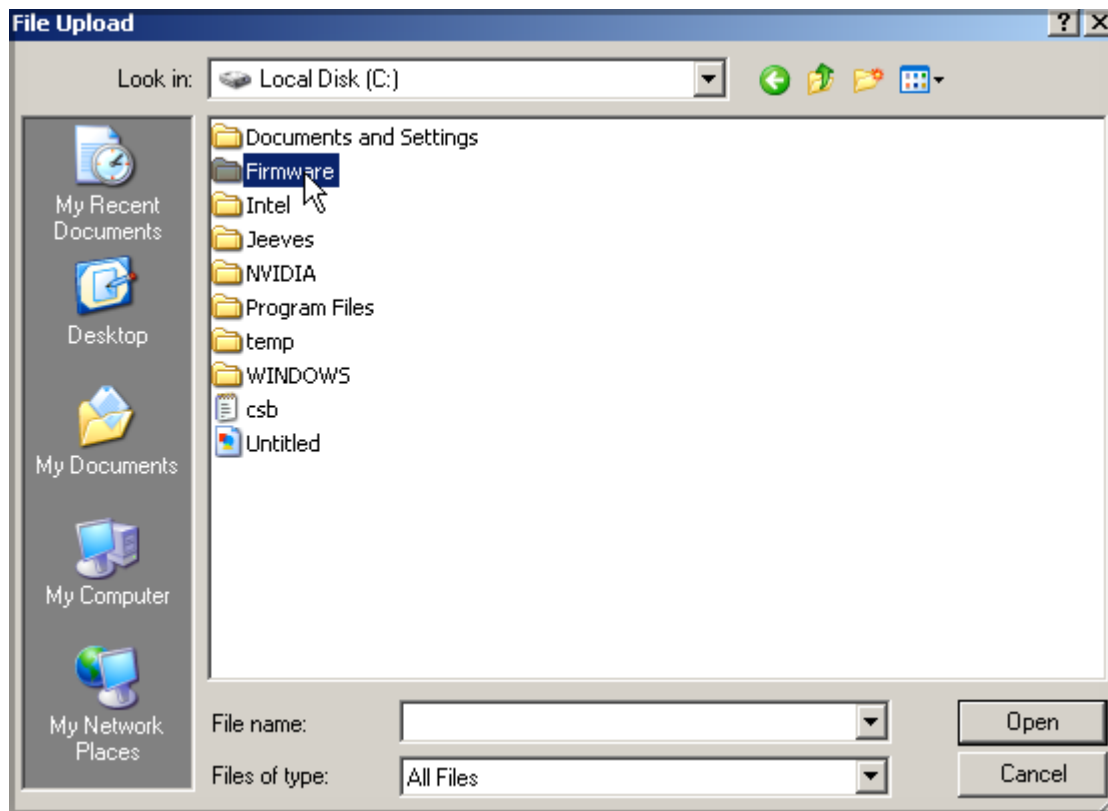
Firmware Upgrade from Personal Computer

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 **Browse** 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.

Checking Firmware Availability

You can check the firmware files available on the server and then decide whether you want to upgrade SETU VTEP. Before upgrading Firmware from server, you can also choose the firmware with which you want to upgrade your SETU VTEP.

- To view the firmware files available on the Server, click the **Check Firmware Available on Server** button.

- A list of Firmware files available on the server appears in a new window.

The screenshot shows a Mozilla Firefox browser window with the address bar displaying `http://192.168.1.139/AutoFirmwareManually.html?Range=3`. The main content area contains a form with the following elements:

- Current Firmware of the system:** A text input field containing `SetuVTEP_V1R5`.
- Status of Last Synchronization:** A text input field containing `Waiting for Firmware File Name`.
- Firmware available on the server:** A list of four radio button options:
 - ☐ SetuVTEP_V1R6_V1R5
 - ☐ SetuVTEP_V1R16_V1R5
 - ☐ SetuVTEP_V2R1_V1R16
 - ☐ SetuVTEP_V2R6_V2R1
- Buttons:** Two buttons labeled **Submit** and **Cancel**, each with a blue checkmark icon.

At the bottom of the browser window, a status bar shows the word **Done**.

- If you want to upgrade SETU VTEP with the desired Firmware, select the Firmware and click the **Submit** button.
- SETU VTEP will upgrade itself with the firmware you select.

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,

- Under **Maintenance**, click the **Configuration** link.

The screenshot shows a web interface titled "Configuration". It contains several settings for the "Auto Configuration Upgrade" feature. The "Enable" checkbox is checked. The "Protocol for Auto Configuration Upgrade" is set to "HTTP" (selected with a radio button). The "Server Address:Port" field is empty, followed by a colon and the port number "80". The "Configuration Folder Path" field is empty. There are two checkboxes for automatic upgrades: "Upgrade Configuration Automatically at every Power ON" (unchecked) and "Upgrade Configuration Automatically at Scheduled time" (unchecked). Under the scheduled time section, there are three radio button options: "Every" (selected) with a value of "1440" minutes, "Everyday at time" with a time of "00 : 00", and "Every Month on Date" with a date of "01" and a time of "00 : 00". The "Request Timeout" is set to "60" seconds. The "Password to Decrypt Configuration File" field is empty. At the bottom, there are three buttons: "Upgrade Configuration from Server", "Upgrade Configuration from PC", and "Backup Configuration". Below these are two more buttons: "Submit" (with a checkmark icon) and "Default" (with a reset icon).

- By default, **Auto Configuration Upgrade** check box is enabled. You may clear this check box, if required.
- **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.
- **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.

If you want SETU VTEP to get the Server Address from the DHCP server, keep this field blank. Make sure that you also set the *Connection Type* on the "[Network Parameters](#)" page to *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 Port Range: 69, 80, 443, 1031 to 65534.

- **Configuration Folder Path:** Specify the path of the folder on the Auto Configuration Server where the configuration file is stored. Default: Blank.
- **Upgrade Configuration Automatically at Every Power ON:** Enable this 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 is enabled, Auto-Firmware upgrade has priority over Auto-Configuration upgrade.

- **Upgrade Configuration Automatically at Scheduled Time:** Enable this 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:
 - **Every XX minutes:** The minutes after which SETU VTEP should check for configuration updates.
 - **Everyday at HH:MM:** The time in Hours(00-23) and Minutes(00-59) when SETU VTEP should check for configuration updates everyday.
 - **Every Month on DD at HH:MM:** The **Date (01-31)** and Time in **Hours (00-23)** and **Minutes(00-59)** when SETU VTEP should check for configuration updates every month.
- **Request Timeout:** 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 retry and wait for next event of Auto-Configuration upgrade.

- **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 [“Configuration”](#) under [“Status”](#) Chapter.

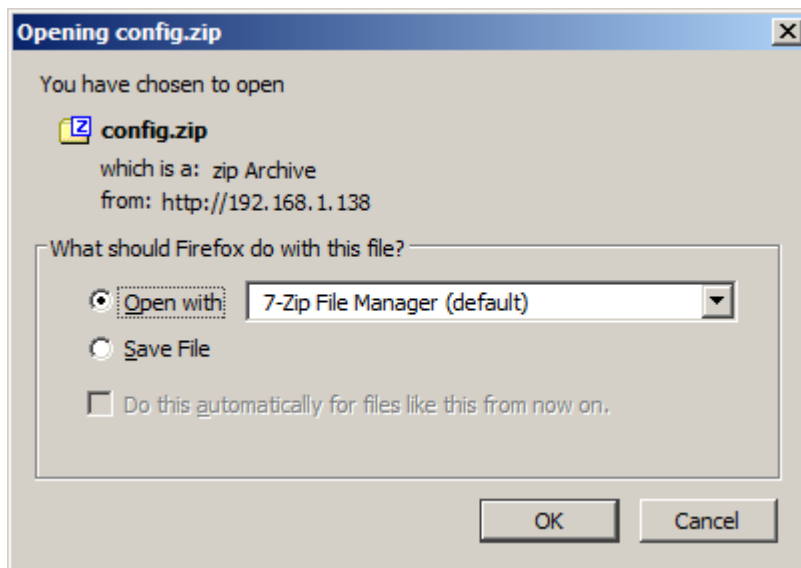
Manual Configuration Upgrade

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.

A **Opening config.zip** window will open.

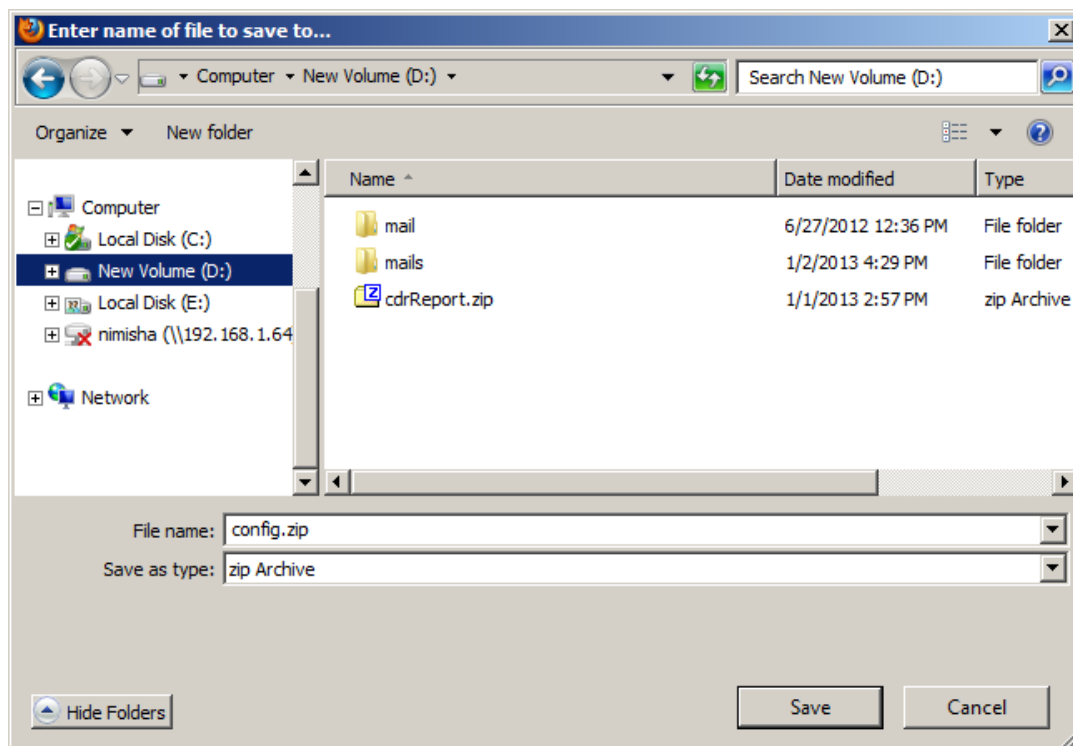


- You can either open the **config.zip** file or save the file to a location.



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 the files**.

- Save the file on the local disk.



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.

- Open the configuration file (.zip) from the location you saved. The zip file contains all the system configuration files.

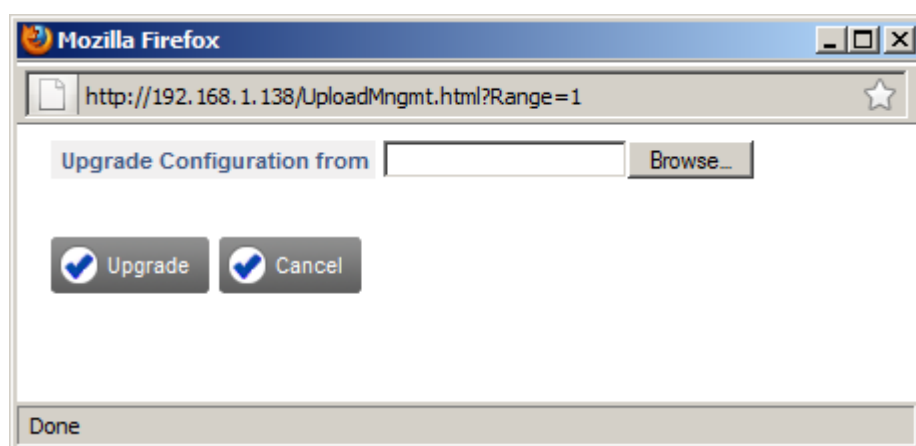
Name	Size	Packed	Type	Modified	CRC32
..			Folder		
websport	3	3	File	5/21/2011 2:06...	EAAAB2D7
SysTimers.cfg	54	44	Microsoft Office Ou...	5/21/2011 2:06...	78DA9D0C
SysPara.cfg	144	81	Microsoft Office Ou...	5/21/2011 2:06...	222434DE
StaticRouting.cfg	122	25	Microsoft Office Ou...	5/21/2011 2:06...	EB4662D2
Sntp.cfg	74	27	Microsoft Office Ou...	5/21/2011 2:06...	4B072D78
SipPara.cfg	11,100	498	Microsoft Office Ou...	5/21/2011 2:06...	9EC62E68
SipHuntGrp.cfg	4,186	175	Microsoft Office Ou...	5/21/2011 2:06...	AE0B9362
SipGlobalPara.cfg	676	179	Microsoft Office Ou...	5/21/2011 2:06...	D49D6C66
SipDestNumTable.cfg	56,050	261	Microsoft Office Ou...	5/21/2011 2:06...	5F36F201
SipCallingNumTable.cfg	28,038	169	Microsoft Office Ou...	5/21/2011 2:06...	B262EB58
SipCalling_FixDestNum.cfg	34,026	92	Microsoft Office Ou...	5/21/2011 2:06...	FC065C7F
RingCad.cfg	15	14	Microsoft Office Ou...	5/21/2011 2:06...	19F6B9CB
Rcoc.info	40,802	57	File info	5/21/2011 2:06...	98C66821
PrefixToDomainTable.cfg	3,092	38	Microsoft Office Ou...	5/21/2011 2:06...	73395587
PinAuthTable.cfg	6,020	39	Microsoft Office Ou...	5/21/2011 2:06...	71909F03
P2PTable.cfg	42,038	239	Microsoft Office Ou...	5/21/2011 2:06...	187F24E9
NwInterface.cfg	338	130	Microsoft Office Ou...	5/21/2011 2:06...	EB0DB8E6
NumList.cfg	160,014	282	Microsoft Office Ou...	5/21/2011 2:06...	BF6A26BD
Mm.cfg	24	24	Microsoft Office Ou...	5/21/2011 2:06...	78571013
T-DialPlan.cfg	24	18	Microsoft Office Ou...	5/21/2011 2:06...	2E81EEFB

- 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.

Upgrading Configuration from a Personal Computer

You can upgrade configuration of SETU VTEP with the configuration files—.cfg format or xml format— stored on your computer. To do so,

- Click the **Upgrade Configuration from PC** button. A new window - **Upgrade Configuration From** opens.



- Click the **Browse** 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 or manually from a Personal Computer.

System Debug

Debugs are logs of actions and events that take place on any computer system. These logs are useful for troubleshooting and system security.

SETU VTEP supports Syslog⁴ Client for debugging. Syslog Client enables the system to send debug messages in syslog format to the remote 'Syslog Server' on IP network. You can view the system debug messages on the remote server.

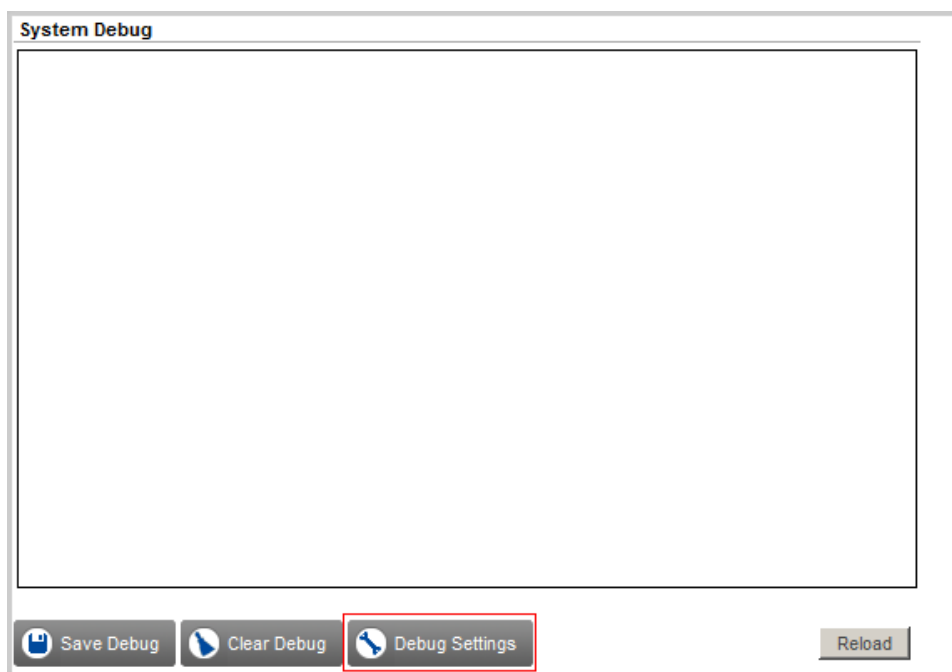
Each debug message includes the MAC Address of SETU VTEP which is sending debug messages to the 'syslog server'.

To be able to use this feature, you must Enable Debug, configure the Syslog Server Address and define the Server Port on which Syslog will listen for debug messages.

Syslog uses the UDP as transport protocol and listens on port 514 (the default listening port).

Configuring System Debug

- Under Maintenance, click the **System Debug** link.



4. Syslog is one of the protocols used extensively for sending debug messages, and is defined in RFC 3164.

- To configure the debug settings, click the **Debug Settings** button. The Debug Settings window will open.

Debug Settings

Debug Enable ☒

Save Debug In File ☐

Syslog Server IP Address . . .

Server Port

Miscellaneous

Call ☒

Config ☐

Media Channel ☐

Time ☐

Webjееves ☐

SNMP ☐

TR069 ☐

Network ☐

SIP

SIP ☐ Message ☐ STUN / NAT ☐

T1E1 Global Parameters

Level 1 ☐ Level 2 ☐

T1E1 Port

Select All ☐

Port 1 Debug Enable ☐ Level 1 ☐ Level 2 ☐

- Select the **Debug Enable** check box to enable system debug. Default: Disabled.
- Select the **Save Debug In File** check box, if you want to save the debug in the system. Default: Disabled.
- In the **Syslog Server IP Address**, enter the remote Syslog Server IP Address. Default: Blank.
- In the Syslog **Server Port**, enter the port number. The range of the server port is 514, 1024 to 65535. Default: 514.
- For **System Debug**, select the desired debug level:
 - Call
 - Config
 - Media Channel
 - Time
 - Webjееves
 - SNMP

Default: All debug levels, are enabled. To disable a debug level, clear the respective check box.
- For **SIP Port**, select the desired debug level:
 - SIP
 - SIP message
 - STUN/ NAT

Default: All debug levels, are enabled. To disable a debug level, clear the respective check box.

- For **T1E1 Global Parameters**, select the desired debug level:
 - Debug Level 1
 - Debug Level 2

Default: Both Debug levels are disabled.

- For **T1E1 Port**, select the **Debug Enable** check box, and then select the desired level:
 - Debug Level 1
 - Debug Level 2

To enable all the parameters of the T1E1 Port debug, you may also select the **Select All** check box.

Default: Both Debug levels are disabled.

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



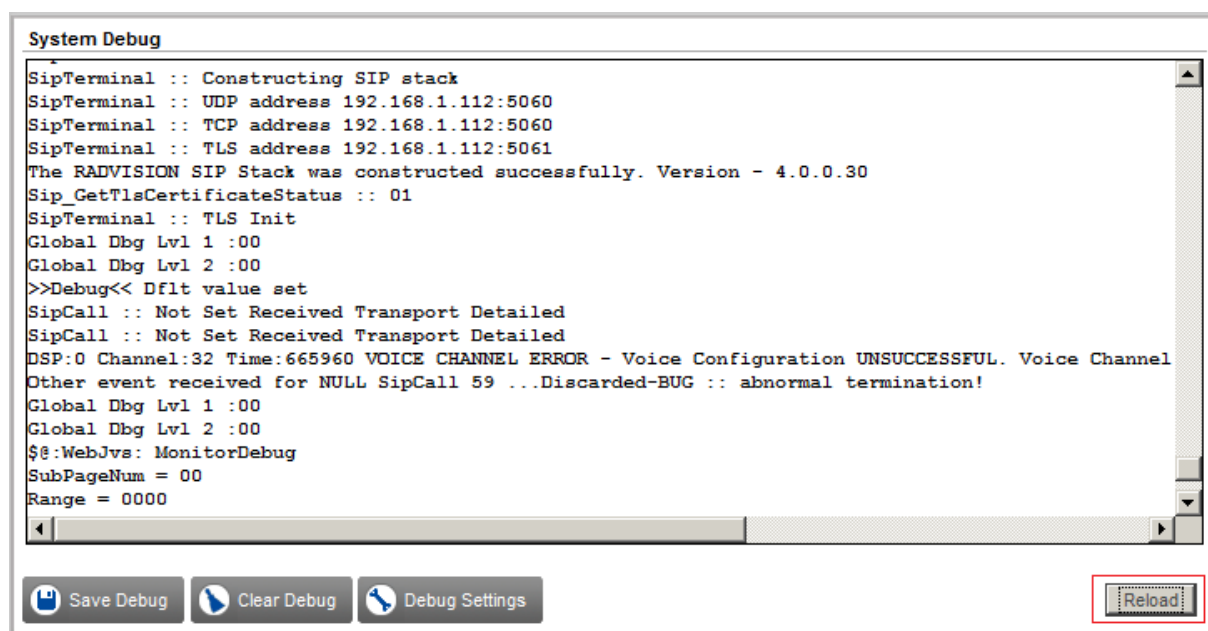
If debug is enabled, at least one debug level should be selected. If no debug level is selected, SETU VTEP will give following error message "Please select the Debug level".

- The window closes, and you return to the System Debug page.
- All the Debug events appear on the screen.



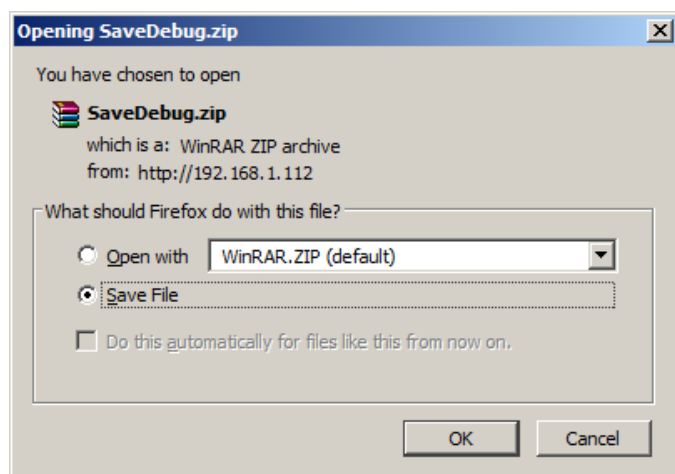
Events will be displayed only if you enable Debug.

- Whenever you want the system to fetch an updated debug report, click the **Reload** button on the System Debug page.

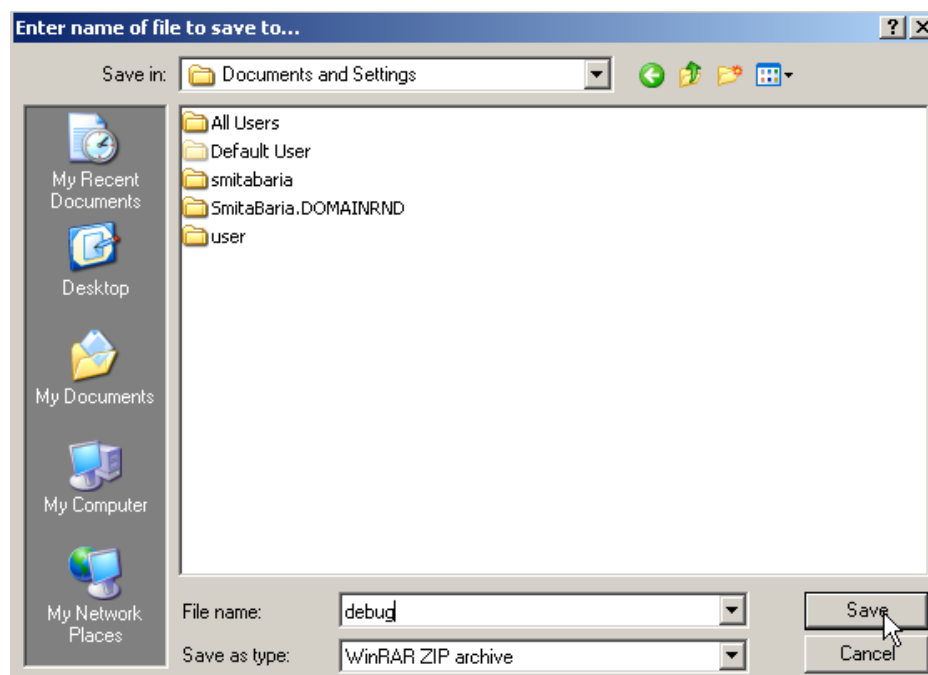


- If you want to delete all the events, click the **Clear Debug** button.

- If you want to Save the Debug events, click the **Save Debug** button.
- You will get a prompt with the option to open the **debug.zip** file or save the file to a location.



- Save the file on the local disk.



- Open the **debug.zip** file from the location you saved. The zip file contains the system debug file **debug.txt**.
- Once you have enabled Debug and set the filters, you can view the debug event log at any time on the **System Debug** page.

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,

- Under **Maintenance**, click the **SNMP** link.

A screenshot of a web-based configuration interface for SNMP. The title bar reads "SNMP (Simple Network Management Protocol)". Below the title bar, there are three expandable sections: "SNMP Settings", "Notification Settings", and "Notification Filters", each preceded by a plus icon. At the bottom of the interface, there are two buttons: "Submit" with a checkmark icon and "Default" with a circular arrow icon.

SNMP Settings

- Click **SNMP Settings** to expand.

SNMP (Simple Network Management Protocol)

SNMP Settings

SNMP ☐ Enable

SNMP Listening Port

SNMP Version

System Name

System Contact

System Location

Listen from specific Manager ☐ Enable

Community Name

Notification Settings

Notification Filters

- Select the **Enable SNMP?** check box. Default: Disabled.
- Configure the **SNMP Listening Port**. Valid Range:161, 1031-65535. Default: 161.
- Select the **SNMP Version** as supported by your SNMP Manager. You can select from:
 - 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.

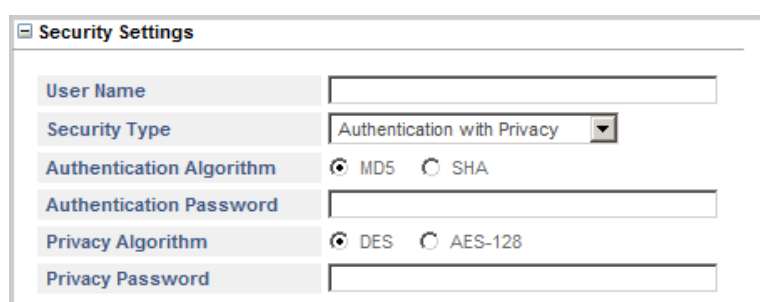
- If SNMP version is set as **SNMPv1** or **SNMPv2c**, configure **Community Name**.

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.

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.

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 up to 24 characters. Default: Blank.

Notification Settings

- Click **Notification Settings** to expand.

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 **Enable Trap?** check box. Default: Disabled.
- You must configure the **Notification Destination**, if you have enabled **Trap**. 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 of the port is 0-65535. Default port is 162.

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

If SNMP version is set as **SNMPv2c** or **SNMPv3**, configure the following parameters.

- Select **Notification Enable** check box, 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.

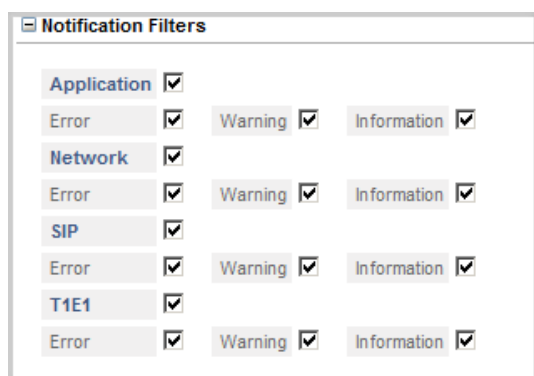
The Notification Destination can be an IP Address or a Domain Name and the Port of the Manager or of any other device where you want to receive the trap messages. IP Address/Domain Name can be a maximum of 64 characters. Valid range of the port is 0-65535. Default port is 162.

- 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** link 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.



You must upload MIB file shipped with the documents of SETU VTEP in your SNMP Manager to get the status and notifications for SNMP.

The List of Events for which you will receive notification is presented in the following table.

Application

Error	Warning	Information
	System Reboot/Gateway Restarted	System boot/initialized
	Web Login - Authentication failure	Web JEEVES Login/Logout status
	CDR Buffer full	Password change
	Sync Out	System Config set to default
	SE Login blocked for IP = IP Address	Page config set to default
		Sync In

Network

Error	Warning	Information
	LAN Link Down	LAN Link Up
	WAN Link Down	WAN Link UP
		IP Address of the Gateway
		New IP Address of Gateway
		MAC Address of Gateway
		DNS address of Gateway
		DynDNS status

SIP

Error	Warning	Information
SIP Stack construction error	DHCP Error	SIP Trunk registering to registrar/ OB Proxy
VOPP Download failed	PPPoE Error	SIP Trunk gets active.
SIP Trunk Registration failed	STUN Error	
	SIP Trunk disabled	

T1E1

Error	Warning	Information
	T1E1 - Layer 1 Status - Red Alarm (When no incoming framing signal is detected on the line)	T1E1 - Layer 1 Status - Alarm Cleared (When recovered from any of the alarm conditions)
	T1E1 - Layer 1 Status - Yellow Alarm (When the far end receives an invalid signal and has reported a red alarm)	T1E1 - Layer 1 up/down status
	T1E1 - Layer 1 Status - AIS Alarm (When some disruption occurs in the communication path)	T1E1 - Layer 2 up/down status

System Port Activity

You can view the state and activity of each Port of SETU VTEP.

- Under Maintenance, click the **System Port Activity** link.
- The port states and activity on each Port appear on this page.

Port	Name	Status	State
T1E1 Port 1		Channel 1 - Active Channel 2 - Active	Channel 1 - Speech Channel 2 - Dial
SIP Trunk 1		Call 1 - Active	Call 1 - Remote Held
SIP Trunk 2		Call 1 - Active	Call 1 - Incoming Call Proceeding
SIP Trunk 3		Disable	
SIP Trunk 4		Disable	
SIP Trunk 5		Disable	
SIP Trunk 6		Disable	
SIP Trunk 7		Disable	
SIP Trunk 8		Disable	
SIP Trunk 9		Disable	
SIP Trunk 10		Disable	
SIP Trunk 11		Disable	
SIP Trunk 12		Disable	
SIP Trunk 13		Disable	
SIP Trunk 14		Disable	
SIP Trunk 15		Disable	
SIP Trunk 16		Disable	
SIP Trunk 17		Disable	
SIP Trunk 18		Disable	
SIP Trunk 19		Disable	
SIP Trunk 20		Disable	

- The **Port** column displays all the Ports present in the system.
- In the **Name** column, the names assigned to the ports on their respective Port Parameters page appear.
- In the **Status** column, the port status is displayed as:
 - **Disable**, when the port is disabled.
 - **Inactive**, when the port is enabled, but is unable to route calls or accept calls due to any reason.
 - **Idle**, when the port is enabled and is currently in use, but there is no call present currently on this port.
 - **Active**, when the port is enabled, is in use, and a call is present on the port.
- In the **State** column, the state of **Active** ports is displayed as:
 - **Dial**, when the port is in Dial state, that is, the call has been answered by the system but no called party number is received.

- **Call in Progress**, when the destination Number is outdialed on the destination port.
- **Speech**, when source port and destination port are in speech.
- **Incoming Call Proceeding**, when Ring event is detected on T1E1 Port or SIP Trunk.
- **Remote Held**, when Hold message is received on SIP Trunk.
- **Error**, when the other party disconnects the call.

As multiple calls are supported on T1E1 Port/ SIP Trunks, the status and state of each call will appear.

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 Trunk is not getting registered, or any 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 PC and open these trace files using a graphical packet capture and protocol analysis tool such as Wireshark or Ethereal.

A maximum of 2 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,

- Under Maintenance, click the **PCAP Trace** link.

PCAP

Filter Setting

Enable Promiscuous mode

☐

Last Status

Packets captured

0

Total Bytes

0

Status

mpcap_init : done : net = 192.168.1.0, mask = 255.255.255.0

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 <i>port number</i>	src port 5060	Capture packets if the packet has a source port value of 5060.
dst port <i>port number</i>	dst port 80	Capture packets if the packet has a destination port value of 80.
port <i>port number</i>	port 5060	Capture packets if the packet has either source or destination port value of 5060
src host <i>ip address</i>	src host 192.168.1.176	Capture packets if the source field of packet is 192.168.1.176
dst host <i>ip address</i>	dst host 192.168.1.176	Capture packets if the destination field of packet is 192.168.1.176
host <i>ip address</i>	host 192.168.1.176	Capture packets if either source or destination field of packet is 192.168.1.176

- Decide the type of packets to be captured and set the Filter accordingly. The Filter Settings parameter should be maximum 60 characters in length. By default, this field is blank. So, all packets will be captured.

You may view examples of Filter Settings on this page.



It is not mandatory to set Filters. When the Filter Settings field is left blank, the system will capture all packets.

- You may select the check box to enable **Promiscuous Mode** if you want. 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.

- Click the **Start** button to begin the capturing of the packets.
- Click the **Stop** button to stop packet capture.

OR

Wait for the system to stop packet capturing. The system stops packet capturing once the maximum allotted memory of 2 MB (RAM) is utilized.

Number of Packets and bytes captured as per the filter setting will be displayed as **Packets Captured** and **Total Bytes**.

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 open. 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.

- You may log out of Jeeves.
- Now, you can open the trace files using Wireshark/Ethereal or any other similar 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,

- Under **Maintenance**, click the **Manual Call Test** link.

The screenshot shows a web interface titled "Manual Call Test". It features two identical rows for configuring a test call. The first row is labeled "Source Port" and the second is labeled "Destination Port". Each row contains three dropdown menus: the first is set to "T1E1", the second to "01", and the third to "CH-01". To the right of these dropdowns is a text input field for a phone number. At the bottom left of the form is a button labeled "Call".

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** you want to test from the list, if you have selected T1E1 as the Port Type.
- 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** you want to test from the list, if you have selected T1E1 as the Port Type.
 - Enter the **Phone Number** in the corresponding field. The phone number must be a valid number that the system can outdial. 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 SETU VTEP

You can restore the system configuration to default values:

- using the Web Jeeves.
- by changing the Jumper position.

Restoring Default Settings using Web Jeeves

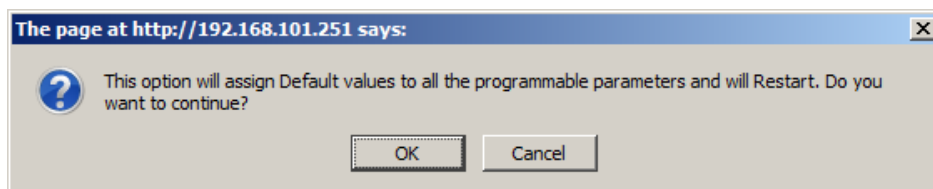
When you restore default settings using the Web Jeeves, all the parameters will be assigned default values **except** the following:

- Region
- Real Time Clock
- Call Detail Records
- Network Parameters
 - Connection Type
 - DNS Settings
 - Dynamic DNS (DynDNS.org)
- System Parameters - NAT
 - STUN Server Address: Port
 - Router Public IP Address
- System Parameters - Server Ports
 - HTTP Web Server Port
 - HTTPS Web Server Port
 - FTP Server Port
 - Telnet Server Port
- Firmware Parameters
- Configuration Parameters
- Login Password

To restore the default settings using the Web Jeeves,

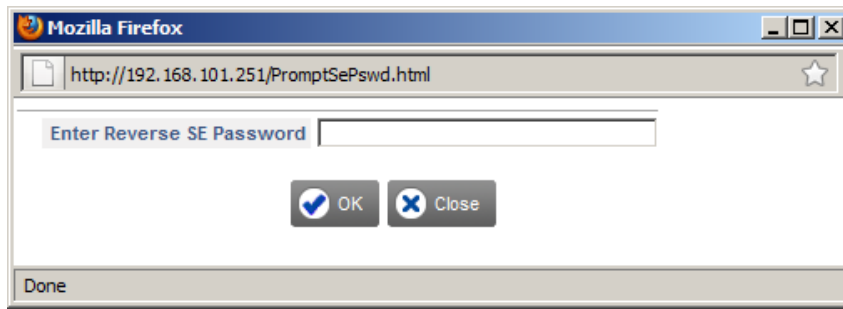
- Under Maintenance, click the **Default System** link.

An alert message, "**This option will assign Default values to all the programmable parameters and will Restart. Do you want to continue?**" will appear as shown under.



- Click the **OK** button.

- You will be prompted to enter the reverse SE password.



- Enter the current SE password backwards. For example, if your password is 5699, enter 9965.
- Click the **OK** button.

The system will restart and all the programmable parameters—except those mentioned above—will be assigned their default values.

Restoring Default Settings by changing the Jumper Position

By changing the position of **Jumper J4** on the PCB, you can restore the following parameters to default values:

- SE Password
- Network Parameters
 - Connection Type
 - FTP Server Access from WAN
 - Telnet Server Access from WAN
 - Allow Server Access from specific IP Address
 - IP Address table for Server Access
 - VLAN
- System Parameters - Server Ports
 - HTTP Web Server Port
 - HTTPS Web Server Port
 - FTP Server Port
 - Telnet Server Port

To restore the default settings by changing the position of **Jumper J4** on the PCB,

- 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 **J4** from **BC** to **AB**.
- Switch ON the system and wait for 15 seconds.
- Switch OFF the system.
- Change the Jumper position from **AB** to the original position **BC**.
- Replace the enclosure cover.
- Switch ON the system.

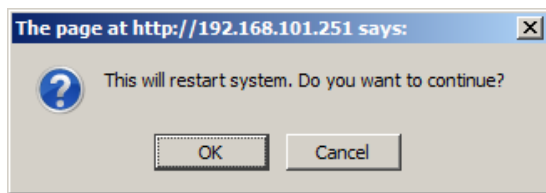
Soft Restart

If you need to restart SETU VTEP, you may do it using Jeeves, instead of switching OFF and switching ON the system again.

When you restart the system, all active calls will be disconnected and the ports in use will be released. The system configuration however, will not be affected.

To restart the system using Jeeves,

- Under Maintenance, click **Soft Restart** link.
- An alert message, "**This will restart system. Do you want to continue?**" will appear as shown below.



- Click **OK** to restart the system.

T1E1 Port Alarms and 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 ms interval. AIS is cleared if the above condition does not exist for 3 ms. This interval of 3 ms can extend upto maximum of 75 ms.
- 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.

Whenever any of the above alarms is detected by the system, it is indicated on the LEDs L1 and L2. See [“Interpreting LEDs”](#) under Connecting SETU VTEP for LED indication. You can also view the status of these alarms on the Jeeves.

To view the Alarms on Jeeves,

- Under Maintenance, click the **T1E1 Port Alarms/Performance Monitoring** link.

T1E1 1

Alarms

Loss of Signal (LoS)	0	Absent
Remote Alarm Indication (RAI)	0	Absent
Alarm Indication Signal (AIS)	0	Absent

Performance Monitoring Counter

CRC-4 Error Counter	0
FAS/NFAS Bit/Pattern Error Counter	12
Far End Block Error Counter	42
Line Code Violation	469
Positive Slip Counter	1
Negative Slip Counter	0

Clear Alarms/Counters

- 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 found 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.



This page is refreshed automatically after every 10 seconds to display the new status.

Performance Monitoring

All errors does 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.
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 ms 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 ms 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 ms 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 on the Jeeves for monitoring the performance of T1E1 Port.

- Under Maintenance, click the **T1E1 Port Alarms/Performance Monitoring** link.

T1E1 1

Alarms

Loss of Signal (LoS)	0	Absent
Remote Alarm Indication (RAI)	0	Absent
Alarm Indication Signal (AIS)	0	Absent

Performance Monitoring Counter

CRC-4 Error Counter	0
FAS/NFAS Bit/Pattern Error Counter	12
Far End Block Error Counter	42
Line Code Violation	469
Positive Slip Counter	1
Negative Slip Counter	0

☒ Clear Alarms/Counters

- 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.



This page is refreshed automatically after every 10 seconds to display the new status.

TR-069

TR-069, also known as CPE WAN Management Protocol (CWMP), is a remote management protocol used for secure communication between the Customer Premises Equipment (CPE) and an Auto-Configuration Server (ACS) for various functionalities such as:

- Auto-configuration and dynamic service provisioning
- Firmware Management
- Status and performance monitoring
- Diagnostics

SETU VTEP supports TR-069. Using TR-069, service providers can manage SETU VTEP remotely for the functions described above.

To configure TR-069 parameters,

- Log into Jeeves.
- Click the **Maintenance** link.
- Click the **TR-069** link.

TR-069

TR-069	<input type="checkbox"/> Enable
ACS URL	<input type="text"/>
ACS User Name	<input type="text"/>
ACS Password	<input type="password"/>
UDP Connection Request Port	<input type="text" value="54320"/>
TCP Connection Request Port	<input type="text" value="7547"/>
Connection Request User Name	<input type="text"/>
Connection Request Password	<input type="password"/>
Periodic Inform	<input checked="" type="checkbox"/> Enable
Periodic Inform Interval	<input type="text" value="1800"/>
STUN	<input checked="" type="checkbox"/> Enable
STUN Server Address:Port	<input type="text"/> : <input type="text" value="3478"/>
STUN Server Username	<input type="text"/>
STUN Server Password	<input type="password"/>

- Select the **TR-069 Enable** check box to use TR-069. Default: Disabled.
- In the **ACS URL** field, enter the URL of the ACS. SETU VTEP will connect and send message to this server address. Default: Blank.
- In the **ACS Username** field, enter the username used by SETU VTEP for HTTP authentication. Default: Blank.
- In the **ACS Password** field, enter the password used by SETU VTEP for HTTP authentication. Default: Blank.

- In the **UDP Connection Request Port** field, enter the port on which the ACS will make a connection request to SETU VTEP using UDP connection. The valid Port range is from 1031-65535. Default: 54320.
- In the **TCP Connection Request Port** field, enter the port on which the ACS will make a connection request to SETU VTEP using TCP connection. The valid Port range is from 1031-65535. Default: 7547.
- In the **Connection Request Username** field, enter the username used by SETU VTEP to authenticate the incoming connection request made by ACS. Default: Blank.
- In the **Connection Request Password** field, enter the password used by SETU VTEP to authenticate the incoming connection request made by ACS. Default: Blank.
- Select the **Periodic Inform** check box, if you want SETU VTEP to check updates available on ACS periodically. Default: Disabled.
- In the **Periodic Inform Interval** field, enter the time in seconds after which SETU VTEP must attempt to connect with the ACS to check for updates. Default: 1800.
- Select the **STUN Enable** check box, if your SETU VTEP is located behind the NAT Router and SIP messages need to be forwarded to the public network. Default: Disabled.

STUN specifies the mechanism required for NAT traversal in SIP messages.



STUN server facilitates traversing through most NATs, except symmetric NATs. If your router has symmetric NAT, do not enable STUN.

- In the **STUN Server Address: Port** field, enter the STUN Server Address and the Listening Port of the STUN Server.

The STUN Server Address can be a maximum of 256 characters. All ASCII characters are allowed. The valid range of the STUN Server Port is from 1025–65535. Default: 3478.

- In the **STUN Server Username** field, enter the username provided by the STUN server to authenticate the STUN Request. Default: Blank.
- In the **STUN Server Password** field, enter the password provided by the STUN Server to authenticate the STUN Request. Default: Blank.
- Click **Submit** to save changes.
- You may log out of Jeeves.

You can view the System Details and the status of Auto-Firmware upgrade, Auto-Configuration upgrade, the Ethernet Port, the SIP Trunks, the T1E1 Port on Jeeves. To do so,

- Click the **Status** link.

System Details

- Click the **System Detail** link.

System Detail	
Product Name	SETU VTEP
WAN Port	1
T1E1 Port	1
VoIP DSP Module	1
Software Version-Revision	V1R7_QARun1
Kernel Date	#1 Fri Nov 29 15:38:33 EST 2013
Stack Status	Constructed
CPLD Version-Revision	V1R2
WAN Port MAC Address	00:1b:09:00:c6:f5
Serial Number of the Product	
Hardware Design of Main Board	
Hardware Design of DSP Module	
VoIP DSP Module (Surf DSP)	No

The following System Details will be displayed on this page.

- **Product Name:** This field displays the name of the product.
- **WAN Port:** This field displays the number of WAN (Ethernet) Port in the system.
- **T1E1 Port:** This field displays the number of T1E1 Port in the system.
- **VoIP DSP Module:** This field displays the number of VoIP DSP Modules present in the system.

- **System Software Version-Revision:** This field displays the current version and revision of the firmware of SETU VTEP.
- **Kernel Date:** This field displays the Kernel compilation date.
- **Stack Status:** This field displays the SIP Stack Status.
- **CPLD Version Revision:** This field displays the CPLD version revision.
- **WAN Port MAC Address:** This field displays the factory set MAC Address of the WAN (Ethernet) Port.



If you have cloned the MAC Address of the WAN (Ethernet) Port, you can view it in Network Status.

- **Serial Number of the Product:** This field displays the Serial Number of the product.
- **Hardware Design of Main Board:** This field displays the Hardware Design of the Main Board.
- **Hardware Design of DSP Module:** This field displays the Hardware Design of the DSP Module.
- **VoIP DSP Module (Surf DSP):** This field displays the VoIP DSP Module present in the system.

Firmware

- Click the **Firmware** link.

Firmware Status	
Last Upgraded On	<input type="text"/>
Next Upgrade On	Schedule Not Available
Last time when Synchronized with Server	<input type="text"/>
Status of Last Synchronization	Disable

The following information related to Auto-Firmware upgrade will appear on your screen.

- **Last Upgraded On:** This field displays the firmware with which SETU VTEP last upgraded itself through the provisioning server, along with the date (DD:MM:YYYY) and time (HH:MM) of the upgradation.
- **Next Upgrade On:** This field displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VTEP will again check for new firmware updates on the server.
- **Last time when Synchronized with Server:** This field displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VTEP last synchronized with the server for new firmware updates.
- **Status of Last Synchronization:** This field 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.

Possible Responses	Event
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 Connection Failed	When no response is received for TCP 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 Firmware Index File	When the system is retrieving Firmware Index file.
Downloading Firmware	When the system is retrieving Firmware zip file.
File Not Found	When the remote file is not found.
Waiting for Firmware File Name	When <i>Check Firmware Available on Server</i> button is clicked manually and the list of available firmware is presented.
No File Found for Up-gradation	When selected firmware benchmark is not found.
	When user does not select the firmware name manually.
	When matrix_firmware.html file is received but current product name is not found from this file.
	Single firmware name is received in matrix_firmware.html but this benchmark file does not match with current firmware benchmark.
	Multiple firmware names are received but all files are below the current firmware.
Firmware Version Below	When the received firmware version is below the current firmware version.
Firmware Version Same	When the received firmware version is same as the current firmware version.

Possible Responses	Event
Firmware Decryption Failed	When the firmware zip file decryption has failed. When the firmware file name does not match or benchmark is less than the current firmware version-revision in the text file.
Auto Upgrade stop due to parameter change	When Auto Upgrade is in process and the Firmware parameters are changed.
Auto Upgrade stop by system	When Auto Upgrade process is stopped due to network restart.
Auto Upgrade Stop on User request	When Firmware upgrade process is started manually but user clicks Cancel button after display of list of firmware files.
Successfully Updated	When firmware is updated successfully.

Configuration

- Click the **Configuration** link.

Configuration Status

Last Upgraded On	
Next Upgrade On	Schedule Not Available
Last time when Synchronized with Server	
Status of Last Synchronization	Disable

The following information related to Auto-Configuration upgrade will appear on your screen.

- Last Upgraded On:** This field displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VTEP last upgraded its configuration through the server.
- Next Upgrade On:** This field 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 field 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 field 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

Possible Responses	Event
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 Status

- Under Status, click the **Network** link.

Ethernet Port

IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
DNS Address	192.168.101.123
System MAC Address	00:1b:09:00:c7:7d
Dynamic DNS Status	Dynamic DNS update is disabled
Stack Status	Constructed

NAT

NAT Type	Unknown - STUN server address is not programmed
Router's Public IP Address	
IP Address fetched using STUN	
SIP Port fetched using STUN	

The current values of the following parameters will appear on your screen:

Ethernet Port

- **IP Address:** This field displays the current IP address of the Ethernet Port of SETU VTEP.
- **Subnet Mask:** This field displays the current Subnet Mask assigned to the Ethernet Port of SETU VTEP.
- **Gateway IP Address:** This field displays the Gateway Address assigned to the Ethernet Port of SETU VTEP.
- **DNS Address:** This field displays the DNS address.
- **System MAC Address:** This field displays the MAC Address assigned to the Ethernet Port of SETU VTEP.



If you have cloned the MAC Address, this field will display the cloned MAC Address. You can view the factory set MAC Address in System Detail.

- **Dynamic DNS Status:** This field displays the response received from DDNS server while sending the IP Address update request to the server. Different responses that can appear in this field are shown below:

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 field.	

- **Stack Status:** In this field, strings such as Idle, DHCP Response wait, PPPoE response wait, NAT checking response wait, construct and error are displayed.

NAT

- **NAT Type:** This field displays the NAT Type, if STUN is enabled in SETU VTEP. Commonly used NAT types are:
 - Unknown
 - Open

- Conenat
 - Restrictednat
 - Portrestrictednat
 - Symmetricnat
 - Symmetricfirewall
 - Blocked
- **Router's Public IP Address:** This field displays Router's Public IP address programmed in the System Parameters. See ["NAT"](#) under *System Parameters*.
 - **IP Address fetched using STUN:** This field displays the IP address fetched using STUN, if STUN server address is programmed.
 - **SIP Port fetched using STUN:** This field displays the SIP Port fetched using STUN, if STUN server address is programmed.

SIP Trunk

- Click the **SIP Trunk** link.

SIP Trunk Number	Status	Registration Time	Registration Retry Count	Failed Reason
1	Active	0	0	
2	Active	0	0	
3	Active	0	0	
4	Disabled	0	0	
5	Disabled	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	

The Status of the SIP Trunks will be displayed as under.

- **SIP Trunk Number:** This non-editable field displays the number of the SIP Trunk.
- **Status:** The possible status indications that can appear in this column are described in the table below.

Status	Description
Disable	Shows that SIP Trunk is disabled.
Registering	Shows that SIP Trunk is enabled and is waiting for response from the SIP server.

Status	Description
Active	Shows that SIP Trunk is registered with the SIP server.
Failed	Shows that some error has occurred in the SIP Trunk and no calls can be made using it (applicable only in case of Proxy Account).
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 field displays the total number of register messages which are sent to the registrar server for registering SIP Trunk.
- **Failed Reason:** This field displays the reason for failure of SIP Trunk registration with the registrar server. The different reasons for registration failure that may appear in this field are:

Reason for Failure	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 constraint/ resource limitation/ 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 error response code.
No contact header in 2xx	This reason is displayed when no contact address is received in 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.
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.



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.

SIP Trunk Status				
SIP Trunk Number	Status	Registration Time	Registration Retry Count	Failed Reason
1	Registering	0	1	Response timeout
	Registering	0	2	Local Failure
	Registering	0	2	Local Failure
2	Active	0	0	
3	Disabled	0	0	
4	Disabled	0	0	
5	Disabled	0	0	
6	Disabled	0	0	
7	Disabled	0	0	
8	Disabled	0	0	
9	Disabled	0	0	

T1E1 Port

- Click the **T1E1 Port** link.

T1E1 Port Status		
T1E1 Port Number	Layer 1	Layer 2
1	UP	UP

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

ANT	Automatic Number Translation
CAS	Channel Associate Signaling
CDR	Call Detail Record
CLI	Caller Line Identification
CLIP	Caller Line Identification and Presentation
CPT	Call Progress Tone
DDI	Direct Dialing In
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Service
DTMF	Dual Tone Multi-Frequency
FoIP	Fax over IP
GMT	Greenwich Mean Time
IP	Internet Protocol
ISDN	Integrated Service Digital Network
ITSP	Internet Telephony Service Provider
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diodes
MAC	Media Access Control
MSN	Multiple Subscribers Numbers
NAT	Network Address Translation
NPI	Numbering Plan Identification
NT	Network Terminal
PBX	Private Branch Exchange
PIN	Personal Identification Number
PPPoE	Point-to-Point Protocol over Ethernet

PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
RBS	Robbed Bit Signaling
RCOC	Returned Call to Original Caller
RTC	Real Time Clock
RTP	Real Time Protocol
SE	System Engineer
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TE	Terminal Equipment / Device
TON	Type of Numbering Plan
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VoIP	Voice over IP
WAN	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	2	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+03:00	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		

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+02:00	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+03:00	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+06:00				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+03:00	1	28	11	7			
92	Russia (Novosibirsk)	English	GMT+06:00	1	28	11	7			
93	Russia (Vladivostok)	English	GMT+10:00	1	28	11	7			
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		
110	United Kingdom	English	GMT	7	36	8	44	A-law		
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	1.54MHz
116	United States (Hawaii)	English	GMT-10:00		37	7	1	U-law	T1	1.54MHz
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			
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	Dial tone		Ring Back Tone		Busy Tone	
		Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)
1	Type1	440	Continuous	350+440	0.4on 0.2off 0.4on 2.0off	440	0.75on 0.75off
2	Type2	400	Continuous	400	0.6on 0.2off 0.2on 2.0off	400	0.5on 0.5off
3	Type3	350+440	Continuous	440+480	2.0on 4.0off	480+620	0.5on 0.5off
4	Argentina	425	Continuous	425	1.0on 4.0 off	425	0.3on 0.2off
5	Australia	425*25	Continuous	400*25	.4on .2off .4on 2.0off	425	0.375on 0.375off
6	Brazil	425	Continuous	425	1.0on 4.0 off	425	0.25on 0.25off

CPTG Type	Country	Dial tone		Ring Back Tone		Busy Tone	
		Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)
7	Canada	350+440	Continuous	440+480	2.0on 4.0off	480+620	0.5on 0.5off
8	China	450	Continuous	450	1.0on 4.0off	450	0.35 on 0.36off
9	Egypt	425*50	Continuous	425*50	2.0on 1.0off	425*50	1.0on 4.0off
10	France	440	Continuous	440	1.5on 3.5off	440	0.5on 0.5off
11	Germany	425	Continuous	425	1.0on 4.0off	425	0.48on 0.48off
12	Greece	425	0.2on 0.3off 0.7on 0.8off	425	1.0on 4.0off	425	0.3on 0.3off
13	India	400*25	Continuous	400*25	.4on .2off .4on 2.0off	400	0.75on 0.75off
14	Indonesia	425	Continuous	425	1.0on 4.0off	425	0.5on 0.5off
15	Iran	425	Continuous	425	1.0on 4.0off	425	0.5on 0.5off
16	Iraq	400	0.4on 0.2off 0.4on 1.5off	400	Continuous	400	1.0on 1.0off
17	Israel	400	Continuous	400	1.0on 3.0off	400	0.5on 0.5off
18	Italy	425	Continuous	425	1.0on 4.0off	425	0.5on 0.5off
19	Japan	400	Continuous	400*25	1.0on 2.0off	400	.5on .5off
20	Kenya	425	Continuous	425	0.67on 3.0off 1.5on 5.0off	425	0.2on 0.6off 0.2on 0.6off
21	Korea	350+440	Continuous	440+480	1.0on 2.0off	480+620	0.5on 0.5off
22	Malaysia	425	Continuous	425	0.4on 0.2off 0.4on 2.0off	425	0.5on 0.5off
23	Mexico	425	Continuous	425	1.0on 4.0off	425	0.25on 0.25off
24	New Zealand	400	Continuous	400+450	0.4on 0.2off 0.4on 2.0off	400	0.5on 0.5off
25	Phillippines	425	Continuous	425+480	1.0on 4.0off	480+620	0.5on 0.5off
26	Poland	425	Continuous	425	1.0on 4.0off	425	0.5on 0.5off
27	Portugal	425	Continuous	425	1.0on 5.0off	425	0.5on 0.5off
28	Russia	425	Continuous	425	0.8on 3.2off	425	0.4on 0.4off
29	Saudi Arabia	425	Continuous	425	1.2on 4.6off	425	0.5on 0.5off
30	Singapore	425	Continuous	425*24	0.4on 0.2off 0.4on 2.0off	425	.75on .75off
31	South Africa	400*33	Continuous	400*33	0.4on 0.2off 0.4on 2.0off	400	.5on .5off

CPTG Type	Country	Dial tone		Ring Back Tone		Busy Tone	
		Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)
32	Spain	425	Continuous	425	1.5on 3.0off	425	0.2on 0.2off
33	Thailand	400*50	Continuous	400	1.0on 4.0off	400	0.5on 0.5off
34	Turkey	450	Continuous	450	2.0on 4.0off	450	0.5on 0.5off
35	UAE	350+440	Continuous	400+450	0.4on 0.2off 0.4on 2.0off	400	0.375on 0.375off
36	UK	350+440	Continuous	400+450	0.4on 0.2off 0.4on 2.0off	400	0.375on 0.375off
37	USA	350+440	Continuous	440+480	2.0on 4.0off	480+620	0.5on 0.5off
38	Type4	400	Continuous	400	1.0on 2.0off	400	0.5on 0.5off
39	Belgium	425	Continuous	425	1.0on 3.0off	425	0.5on 0.5off
40	Type5	350+440	Continuous	350+440	0.4on 0.2off 0.4on 2.0off	400	0.75on 0.75off

CPTG Type	Country	Error Tone 1		Error Tone 2		Confirmation Tone	
		Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)
1	Type1	440	0.25on 0.25 off	440	1on 1off	350+440	0.1on 0.1off
2	Type2	400	0.25on 0.25 off	400	1on 1off	400	0.1on 0.1off
3	Type3	440	0.25on 0.25 off	440	1on 1off	350+440	0.1on 0.1off
4	Argentina	425	0.3on 0.4off	425	1on 1off	425	0.1on 0.1off
5	Australia	425	0.375on 0.375off	425	1on 1off	425*25	0.1on 0.1off
6	Brazil	425	0.25on 0.25 off	425	1on 1off	425	0.1on 0.1off
7	Canada	480+620	0.25on 0.25off	480+620	1on 1off	350+440	0.1on 0.1off
8	China	450	0.7on 0.7off	450	1on 1off	450	0.1on 0.1off
9	Egypt	450	0.5on 0.5off	450	1on 1off	425*50	0.1on 0.1off
10	France	440	0.25on 0.25off	440	1on 1off	440	0.1on 0.1off
11	Germany	440	0.20on 0.48off	425	1on 1off	425	0.1on 0.1off
12	Greece	425	0.15on 0.15off	425	1on 1off	425	0.1on 0.1off

CPTG Type	Country	Error Tone 1		Error Tone 2		Confirmation Tone	
		Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)
13	India	400	0.25on 0.25off	400	1on 1off	400	0.1on 0.1off
14	Indonesia	425	0.25on 0.25off	425	1on 1off	425	0.1on 0.1off
15	Iran	425	0.25on 0.25off	425	1on 1off	425	0.1on 0.1off
16	Iraq	400	0.25on 0.25off	400	1on 1off	400	0.1on 0.1off
17	Israel	400	0.25on 0.25off	400	1on 1off	400	0.1on 0.1off
18	Italy	425	0.2on 0.2off	425	1on 1off	425	0.1on 0.1off
19	Japan	400	0.25on 0.25off	400	1on 1off	400	0.1on 0.1off
20	Kenya	425	0.2on 0.6off	425	1on 1off	425	0.1on 0.1off
21	Korea	480+620	0.3on 0.2off	480+620	1on 1off	350+440	0.1on 0.1off
22	Malaysia	425	2.5on 0.5off	425	1on 1off	425	0.1on 0.1off
23	Mexico	425	0.25on 0.25off	425	1on 1off	425	0.1on 0.1off
24	New Zealand	400	0.25on 0.25off	400	1on 1off	400	0.1on 0.1off
25	Phillippines	480+620	0.25on 0.25off	480+620	1on 1off	425	0.1on 0.1off
26	Poland	425	0.5on 0.5off	425	1on 1off	425	0.1on 0.1off
27	Portugal	450	0.33on 1.0off	450	1on 1off	425	0.1on 0.1off
28	Russia	425	0.25on 0.25off	425	1on 1off	425	0.1on 0.1off
29	Saudi Arabia	425	0.25on 0.25off	425	1on 1off	425	0.1on 0.1off
30	Singapore	425	0.25on 0.25off	425	1on 1off	425	0.1on 0.1off
31	South Africa	400	0.25on 0.25off	400	1on 1off	400*33	0.1on 0.1off
32	Spain	425	0.25on 0.25off	425	1on 1off	425	0.1on 0.1off
33	Thailand	400	0.3on 0.3off	400	1on 1off	400*50	0.1on 0.1off
34	Turkey	450	0.2on 0.2off .6on .2off	450	1on 1off	450	0.1on 0.1off

CPTG Type	Country	Error Tone 1		Error Tone 2		Confirmation Tone	
		Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)
35	UAE	400	0.4on 0.35off 0.225on 0.525off	400	1on 1off	350+440	0.1on 0.1off
36	UK	400	0.4on 0.35off 0.225on 0.525off	400	1on 1off	350+440	0.1on 0.1off
37	USA	480+620	0.25on 0.25off	480+620	1on 1off	350+440	0.1on 0.1off
38	Type4	400	0.25on 0.25 off	400	1on 1off	400	0.1on 0.1off
39	Belgium	425	0.167on 0.167 off	425	1on 1off	425	0.1on 0.1off
40	Type5	400	0.25on 0.25 off	400	1on 1off	350+440	0.1on 0.1off

CPTG Type	Country	Feature / Programming / Prompt Tone		Routing Tone		IntrusionTone	
		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	0.2on 4.8off
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	Continuous
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	480+620	0.5on 0.5off
8	China	450	0.1on 0.9off	450	0.1on 1.9off	450	0.2on 0.2off 0.2on 0.6off
9	Egypt	425*50	0.1on 0.9off	425*50	0.1on 1.9off	450	0.5on 0.5off
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	0.15on 0.25off 0.15on 1.45off
13	India	400*25	0.1on 0.9off	400*25	0.1on 1.9off	400	0.15on 4.85off

CPTG Type	Country	Feature / Programming / Prompt Tone		Routing Tone		IntrusionTone	
		Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)
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*25	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	440	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	0.2on 1.4off
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	0.25on 2.0off
31	South Africa	400*33	0.1on 0.9off	400*33	0.1on 1.9off	400	0.15on 0.25off 0.15on 1.45off
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	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	400	0.2on 4.8off
37	USA	350+440	0.1on 0.9off	350+440	0.1on 1.9off	480+620	0.5on 0.5off
38	Type4	400	1.75on 0.1off	400	0.1on 1.9off	400	0.2on 0.2off 0.2on 2.5off
39	Belgium	425	0.1on 0.9off	425	0.1on 1.9off	440	0.1on 2.9off
40	Type5	350+440	0.1on 0.9off	350+440	0.1on 1.9off	350+440	0.5on 0.5off 1.0on 5.0off

Product Specifications

System Resources

System Resources	Maximum Capacity
VoIP Calls	32
SIP Accounts	32
T1/E1/PRI Main Port	1
T1/E1/PRI Sync-in Port	1
T1/E1/PRI Sync-out Port	1
WAN / Ethernet Port	1

Technical Specifications

VoIP

VoIP Protocols	SIP v2, SDP, RTP (RFC 2883)
Network Protocol	IPv4, TCP, UDP, DHCP, SNTP, STUN, HTTP
SIP	32 SIP Accounts Out Bound Proxy Support
NAT	STUN and NAT Keep Alive
Voice CODECS	G.723, G.729, iLBC 30ms & 20ms, GSM-FR, G.711 A-Law & μ -Law, GSM-EFR
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 and Pass-Through
Quality of Service	Layer 3 DiffServe and ToS
Data Network	1 WAN Port RJ45 Auto MDIX 10/100 BaseT
Security	Password Protection Administration

Maximum Simultaneous Calls supported by Vcoders

Vocoder	Maximum Simultaneous calls
G.729	16
G.723	30
GSM FR	30
iLBC 30ms	30

Vocoder	Maximum Simultaneous calls
iLBC 20ms	26
GSM EFR	24
G.711 (m-Law)	30
G.711 (A-Law)	30

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	5V DC, 2A
Power Consumption	5W (Maximum)

Mechanical

Dimensions (WxHxD)	161.50 x 101.25 x 30.30 mm (without side clamps)
	483.50 x 101.25 x 30.30 mm (with side clamps)
Mounting	Wall, Rack and Table-Top

Weight

Unit Weight	550 grams (without side clamps)
	610 grams (with side clamps)

Environmental

Operating Temperature	0°C to 40°C (32°F to 104°F)
Operating Humidity	5-95% RH, Non-Condensing
Storage Temperature	-40°C to +85°C (-40°F to +185°F)
Storage Humidity	0-92% RH, Non Condensing

System Commands

Description	Commands
Making a New Call	#91
Disconnect Call	#92
To know IP Address	#51
To know Subnet Mask	#52
To know Gateway Address	#53
To know DNS Address	#54

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"

Regulatory Information

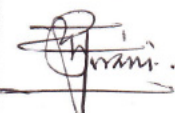


Federal Communications Commission Statement

Part 15: Class A Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE and ROHS Certificate



Declaration of Conformity	
Manufacturer's Name	: Matrix Comsec Pvt. Ltd.
Manufacturer's Address	: 15 & 19-GIDC, Waghodia, Dist: Vadodara 391760 Gujarat, India
Declares that the product/s Product	: VoIP to T1/ E1 PRI Gateway
Model/ Type	: SETU VTEP
Trade Name	: MATRIX
The designated products are in conformity with the below mentioned European directive ;	
EMI/EMC:	
CISPR 22 : 2006 Edition 5.0 (with Am 1: 2007 and Am 2 : 2010)	
IEC 61000-3-2 : 2005 Edition 2.2 (with Am 1: 2008 and Am 2 : 2009)	
IEC 61000-3-3 : 2005 (with Am 1: 2001 and Am 2 : 2005-06 modified in 2008)	
CISPR 24 : 2010	
IEC 61000-4-2 : 2001 (with Am 1: 1998 and Am 2 : 2000)	
IEC 61000-4-3 : 2006 (with Am 1: 2007 and Am 2 : 2010)	
IEC 61000-4-4 : 2004 (with Am 1: 2010)	
IEC 61000-4-5 : 2005 (with Am 1: 2000)	
IEC 61000-4-6 : 2004 (with Am 1: 2004 and Am 2: 2006)	
IEC 61000-4-8 : 2002 Edition 1.1	
IEC 61000-4-11 : 2004 Edition 2.0	
SAFETY:	
IEC 60950-1: 2005 (Second Edition)	
Supplementary information:	
The Product herewith complies with the following directives :	
EMC	2004/108/EC
Low Voltage Directive	2006/95/EC
RoHS Recast (RoHS 2)	2011/65/EU (as per standard EN 50581:2012)
 Mr. Ganesh Jivani Director Date: 15.06.2015 Vadodara	
	
	

MATRIX COMSEC PVT. LTD.

Head Office: 394-GIDC, Makarpura, Vadodara-390 010, India. Ph: +91 265 2630555, Email: Inquiry@MatrixComSec.com • www.MatrixComSec.com

Factory: 19-GIDC, Waghodia, Dist. Vadodara-391 760, India. Ph: +91 2668 263172/73

Registered Office: C-1/394, GIDC, Makarpura, Vadodara-390 010, India. • CIN: U72200GJ1998PTC034047

Open Source Licensing Terms and Condition

- The firmware of this product also includes some of the Open-Source software released under GNU General Public License (GPL) Version 2 and SNMP License. Terms of these licenses are 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.

GPL Version 2

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.

The SNMP License

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

----- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

----- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright B) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written

permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
 oss@fabasoft.com
 Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

----- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS
OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

Index

A

Access Codes 200
After Answering the Call and Collecting the Digits 97
Allow Server access from specific IP Address 162
Allowed - Denied Logic 57, 141
Allowed IP Address for Incoming SIP Message 35, 41
Allowed-Denied Logic 165
Applications 6
Authentication ID 35, 39
Authentication Password 35, 39, 241, 242
Auto Firmware Upgrade 223
Auto-Configuration Upgrade 229
Automatic Number Translation 62, 87, 110, 122
Automatic Number Translation (ANT) 169

B

Battery 8
Black Listed Callers 59, 166
Block ICMP on WAN 163
Block PING on WAN 163

C

CA Signed Certificate 210
Call Details
 Filters 213
 Report 218
Call Disconnection using Access code 68, 122
Call Hold Method 68
Call Hold using Inactive 68
Call Progress Tone 25, 26
Call Release Timer 156
Called party 3
Called Party Number 97
Callee 3
Caller 3
Calling party 3
Calling Party Number 93
Certificate 164
Certificate Manager 204
Check Proxy Address for Incoming SIP Message 36

Check Proxy Port for Incoming SIP Message 36
Check SIP ID for Incoming SIP Message 36
Checking Firmware Availability 227
Clear Call Records 216
CLIR 61
Clock Synchronization Port 158
Comfort Noise (CN) 43, 44
Configuration Upgrade 229
Connect Source Port when 183(Session Progress) is received on SIP 65
Connect Source Port when number is outdialed 111, 144
Connecting SETU VTEP
 Computer 17
 ISDN Network 11
 Power Supply 13
 SYNC Ports 13
 VoIP Network 10
Connection Type 28
 DHCP 29
 PPPoE 29
 Static 29
Country Code 27

D

Daylight Saving Time 151
Default Login Password 149
Default Region Table 271
Default SETU VTEP 250
 Restoring Default Settings by changing the Jumper Position 251
Default System
 Restoring Default Settings using Web Jeeves 250
Destination Number Determination
 After Answering the Call and Collecting the Digits 49, 97, 132
 Called Party Number 49, 97, 132, 46, 93, 128
 DDI Number 95, 130
 Fixed Destination Number 92, 128
 on the basis of DDI Number 47
 SIP Trunks 173
 T1/E1 Port 173

- Destination Port 3
- Destination Port Determination 180
 - Calling Party Number 55, 105, 139
 - Destination Number 53, 102, 136
 - Fixed 51, 100, 134
 - SIP Trunks 180
 - T1/E1 Port 180
- Destination Port for routing calls 51, 134
- Digest Authentication 36, 42, 195
- Disconnecting a Call using Access Code 221
- DNS Setting
 - DNS Address 29
 - Static DNS 29
- DNS Settings 29
- DNS SRV 37
- Download Call Records 216
- Dynamic DNS 29

E

- E1
 - CAS Parameters 75
 - PRI Parameters 73
- E1 Network 111
- E1 Terminal 85
- Emergency Numbers 201
- End of Dialing Digit 50, 133
- Enrolling the Certificate Signing Request with CA 211
- Error Tone Delay Timer 157
- Error Tone Timer 157
- Ethernet Port 3, 264

F

- Fallback Event 38
- Fallback Outbound Proxy Server Address 1
 - Port 37
- Fallback Outbound Proxy Server Address 2
 - Port 37
- Fallback Registrar Server Address 1
 - Port 37
- Fallback Registrar Server Address 2
 - Port 37
- Fallback Server 37
- Firmware Upgrade 223
- First Digit Wait Timer 49, 133
- Fixed Destination Number 45, 92
- FTP Server Access from WAN 162
- FTP Server Port 162

G

- General Request Timer 161
- Group
 - SIP Group 185
 - T1E1 Group 186

H

- Heartbeat Interval 37
- HTTP Web Server Port 162
- HTTPS Web Server Port 162

I

- Incoming Call Routing
 - Channel Number Wise 109
 - MSN Number Wise 109, 143
 - Port wise 127, 91
- Incoming calls (with CLI) 44, 92, 128
- Incoming calls (without CLI) 50, 99, 133
- Inter Digit Wait Timer 50, 133
- IP Dialing 222

J

- Jitter Buffer Setting for Passthrough 69
- Jitter Buffer Setting for Speech 68

L

- Language Selection 24
- LEDs

- SIP Trunk 14, 15
 - T1E1 Port 14

- Load Balancing 38

- Local Certificate for Configuration Upgrade 164

- Local Certificate for Firmware Upgrade 164

- Local Certificate for TLS 164

- Local Certificate for TR069 164

- Local Certificate for WebServer 164

M

- MAC Cloning 31
- Making a New Call using Access Code 221
- Making New Call using Access code 50, 133
- Managed device 239
- Management Information Base 239
- Management/Security 162
- Manual Call Test 249
- Manual Configuration Upgrade 231
- Manual Firmware Upgrade 226
- Maximum number of dialed digits 50
- Multi-Stage Dialing 170

N

- NAT 159
- NAT Type 67
- Network Information using Access Codes 222
- Network Port 3
- Network Status 260, 262
- Network Type 90
- No Response Timer 38
- Number Lists 165

O

- Open Source Licensing Terms and Condition 288
- Orientation Type 85
- Originating Port 3
- Outbound Proxy 35
- Outgoing Calls E1 Port 110
- Outgoing Calls SIP Trunks 60
- Outgoing Calls T1 Port 144
- Overview of SETU VTEP 5

P

- Package Contents 9
- Passthrough FAX Codec 68
- Pause 170
- Pause Timer 63, 88, 124
- PCAP Trace 247
- Peer-to-Peer Dialing 188
- Peer-to-Peer SIP Trunk 34
- PIN Authentication 193
- Play Routing Tone 156
- Printing Call Detail Record Report 217
- Prioritization of traffic 30
- Protecting SETU VTEP 7
- Proxy SIP Trunk 34

Q

- QoS
 - RTP DiffServe/ToS 31
 - SIP DiffServe/ToS 31

R

- Real Time Clock 150
- Region 24
 - Call Progress Tones 25, 27
 - Language 25
 - PCM Companding Type 25
- Register with all Servers 38
- Register with only one Server 38
- Registration Behavior 38
- Registration Retry Timer 37
- Remove Country Code from CLI received 157
- Re-registration Timer 37
- Reset Cycle 13
- Restoring Default Settings by changing the Jumper Position 251
- Restoring Default Settings using Web Jeeves 250
- Route calls returned unconnected to original caller 65, 110, 144
- Router's Public IP Address 160
- Routing Group 52, 100, 135, 185
- Routing Group Busy Wait Timer 157
- Routing Tone 156
- RTP Listening Port 161
- RTP QoS 31

S

- Self-Signed Certificate 204
- Send "user=phone" in SIP URI 68
- Send OPTIONS message as Heartbeat 36
- Simple Network Management Protocol (SNMP) 239
- SIP 160
- SIP ID 34, 39
- SIP INVITE Timer 161
- SIP LED 156
- SIP Over TCP 160
- SIP Provisional Timer 161
- SIP Registration 35
- SIP TCP Port 161
- SIP TLS Port 161

- SIP Transport 66, 69, 70

- SIP Trunk

 - Peer-to-Peer 34

- SIP Trunk for IP Dialing 156

- SIP Trunk Mode 34

 - Peer-to-Peer 39, 34

- SIP UDP Port 161

- SIP/RTP Port

 - RTP Listening Port 161

 - SIP TCP Port 161

- SIP-DDI Number Based Table 174

- SNMP 239

- SNMP Agent 239

- SNMP Manager 239

- SNTF Settings 154

- Source 3

- Static Routing 197

- Status

 - Firmware 259

 - NAT 264, 263

 - SIP Trunk 265

 - T1E1 Port 267

- STUN 159

- Switch Registration to Alternate Server on Fallback 38

- Symmetric RTP 67

- Sync Date-Time with PC 151

- Syslog Server Settings 236

- System Certificate 207

- System Debug 235, 236

- System Default 250

- System Engineers 1

- System Parameters 155

- System Port Activity 245, 249

- System Restart 252

T

- TCP NAT Keep Alive 160

- Telnet Server Access from WAN 162

- Telnet Server Port 162

- Terminating Port 3

- Time Offset 152

- Time Zone 154

- TR-069 257

- Type of DST 152

U

- UDP NAT Keep Alive 159

- Unconnected Calls Record Delete Timer 157

- Users 1

V

- VLAN header 30

- VLAN/CoS 30

 - RTP CoS 31

 - SIP CoS 30

 - VLAN ID 30

- VMS Debug 285

- Vocoders 42

- VoIP Silence Disconnect Timer 156

W

Wait for Answer 170

Web Server Access from WAN 162

Wizard 22



MATRIX COMSEC

Head Office

394-GIDC, Makarpura, Vadodara - 390010, India.

M:+91 85111 73344

E-mail: Customer.Care@MatrixComSec.com

www.MatrixTeleSol.com