San Telequip Private Limited.
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27273455, 9764027070, 8390069393
email : info@santelequip.com

Connecting. Converting. Leading!

User Manual for Modbus Gateway Model: SC10E4IM S

Table of Contents

San Telequip Private Limited.
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27273455, 9764027070, 8390069393
email : info@santelequip.com

Introduction

The SC10E4IM S Modbus Gateway is an industrial network device in between Modbus over Serieal Line devices and computer hosts running Modbus/TCP on Ethernet network. Figure 2.1 illustrates a possible network configuration of the SC10 Series Modbus Gateway. Fully compliant with Modbus/TCP protocol, the Modbus gateway offers a convenient solution to connect existing devices or controllers running Modbus serial protocol (Modbus/ASCII or Modbus/RTU) to an Ethernet network. The SC10E4 MS Series are standard Modbus gateways that convert packets between Modbus TCP and Modbus RTU/ASCII protocols.

Each RS-232/422/485 serial port can be individually configured for Modbus/RTU or Modbus/ASCII operation with different baud rate, allowing both types of networks to be fully integrated with Modbus/TCP within one package.

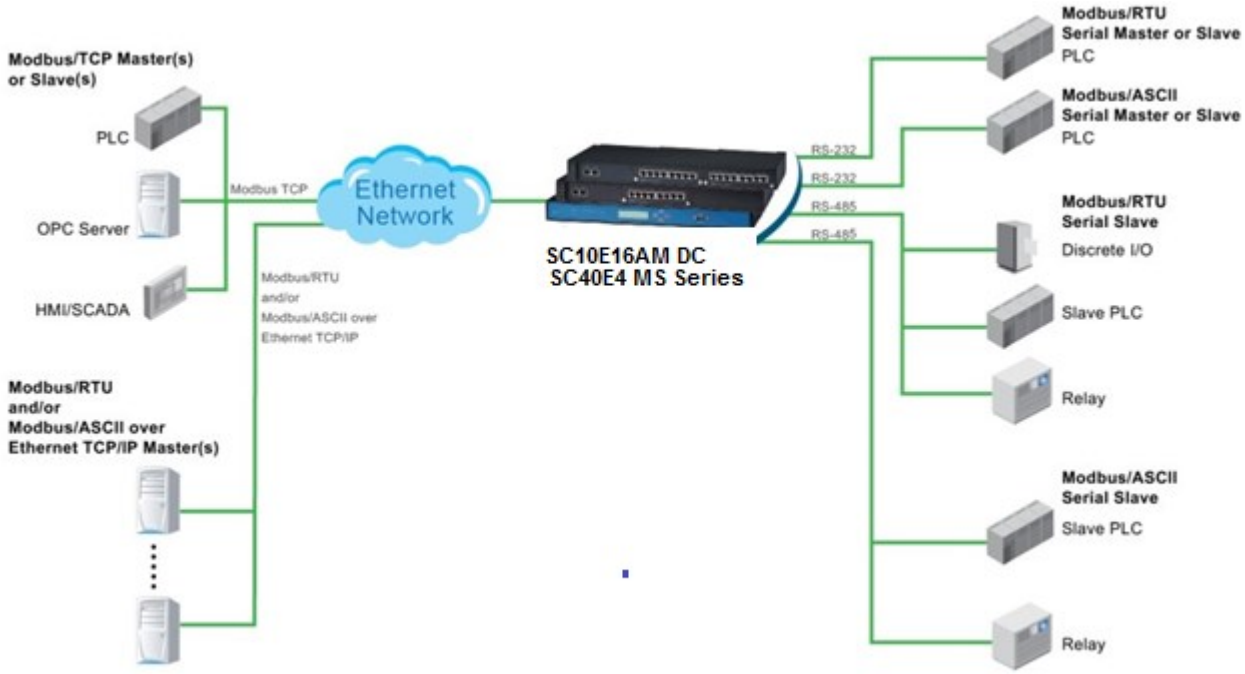


Figure 2.1 Possible Network Configuration of SC10E4 MS Series Modbus Gateway

Figure 2.2 shows three different use cases of the SC10E4 MS Series Modbus Gateway:

1) The interface between Modbus RTU/ASCII serial host to Modbus RTU/ASCII serial devices
2) The interface between Modbus/TCP over Ethernet network to Modbus RTU/ASCII serial devices
3) The interface between Modbus RTU/ASCII host connected through Serial IP over Ethernet (virtual communication port (VCOM)) to Modbus RTU/ASCII serial devices.

San Telequip Private Limited.
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27273455, 9764027070, 8390069393
email : info@santelequip.com

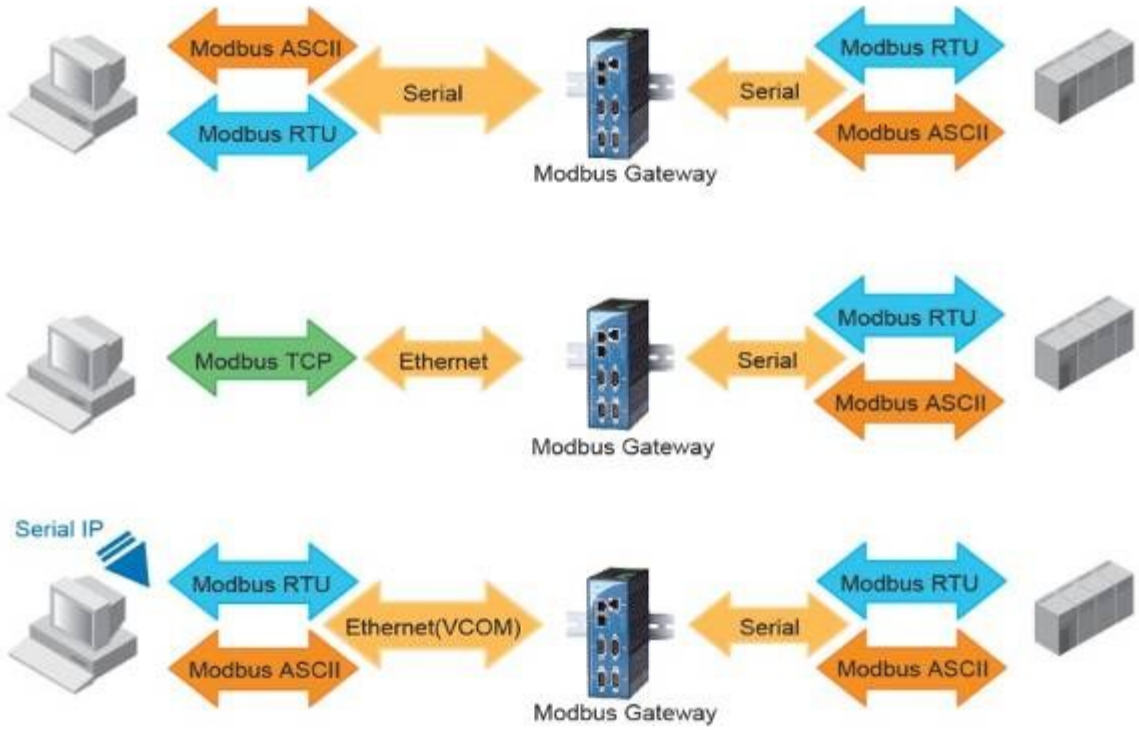


Figure 2.2 Use Cases of the SC10E4 MS Series Modbus Gateway

,

1.1 Factory Default Setting

1.1.1 Network Default Settings

The SC10E4 MS Modbus Gateway comes with one IP address specifically for redundant Ethernet interfaces.

Interface	Device IP	Subnet Mask	Gateway IP
LAN 1	10.0.50.100	255.255.0.0	10.0.0.254
LAN 2	192.168.1.1	255.255.255.0	192.168.1.254

Remarks: Default DNS 1 setting is 168.95.1.1 and DNS 2 setting is 0.0.0.0.

1.1.2 Modbus Default Settings

The SC10E4 MS Modbus Gateway comes with the following default Modbus settings.

Table 2.1 Modbus Default Settings

Parameter	Default Values
Modbus Master	
TCP Settings	TCP Master Mode: TCP Master Port: 502
Modbus Slave	
SC10E4IMS	Mode: RTU Slave Serial Configuration: RS-232, 9600 bps, 8 data bits, No parity bit, 1 stop bit, No Flow Control, Buffer Disable

Other default settings are shown in the following table.

Table 2.2 Other Default Settings

Parameter	Default Values
Security	
User Name	admin
Password	default
SNMP	
Sys Name of SNMP	SAN TELEQUIP
Sys Location of SNMP	location
Sys Contact of SNMP	Contact
SNMP	Disable (Unchecked)
Read Community	Public
Write Community	Private
SNMP Trap Server	0.0.0.0

Note: Press the “Reset” button on the front panel for 5 seconds to restore the SC10E4 MS Series Modbus Gateway to the factory default settings.

2. Configuration and Setup

It is strongly recommended for the user to set the Network Parameters through **Serial Manager**

1.2 Configuration of Network Parameters through Device Management Utility

First, please install Serial manager config utility from our website www.santelequip.com/download. After you start **Serial Manager Utility**, if the Modbus Gateway is already connected to the same subnet as your PC, the device can be accessed via broadcast packets. Serial Manager **Utility** will automatically detect your Modbus Gateway and list it on Serial Manager Utility's window. Alternatively, if you did not see your Modbus Gateway on your network, press "**Rescan**" icon, a list of devices, including your Modbus Gateway device currently connected to the network will be shown in the window of **Serial Manager Utility** as shown in Figure 2.3.

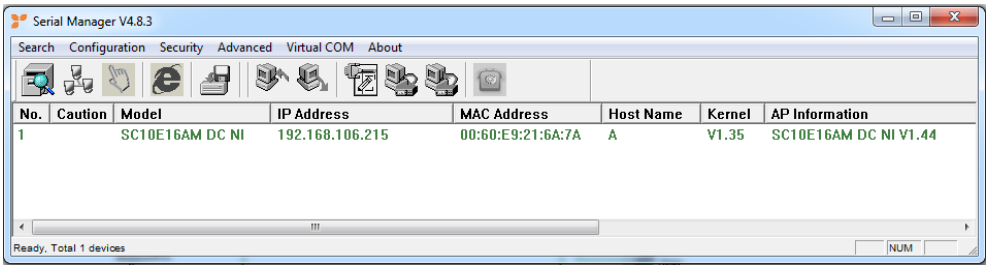


Figure 2.3 Serial Manager Utility

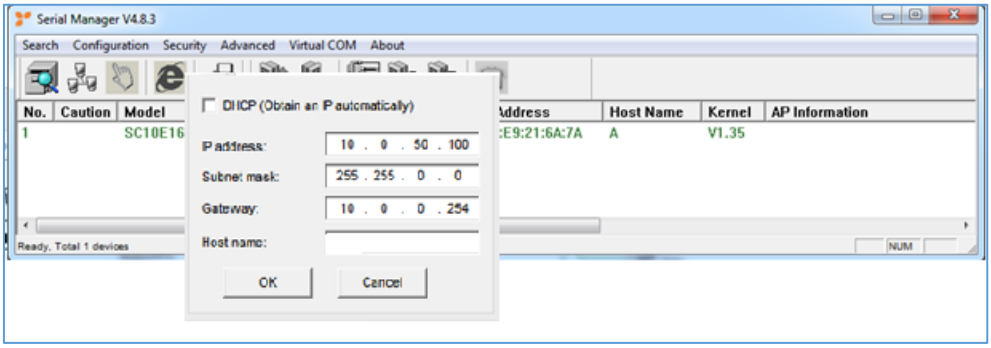


Figure 2.2 Window of Network Setting

You may proceed then to change the IP address to avoid any IP address conflict with other hosts on your LAN or to connect the device to your existing LAN as shown in Figure 2.2. The system will prompt you for a credential to authorize the changes. It will ask you for the **Username** and the **Password** as shown in Figure 2.3. The default username is "**admin**", while the default password "**default**". After clicking on the **Authorize** button, a notification window will pop-up as shown in Figure 2.4 and some device may be restarted. After the device is restarted , it will beep twice to indicate that the unit is running normally. Then, the Modbus Gateway can be found on a new IP address. It may be listed automatically by the **Serial Manager Utility** or it can be found by clicking on the "**Rescan"** icon.

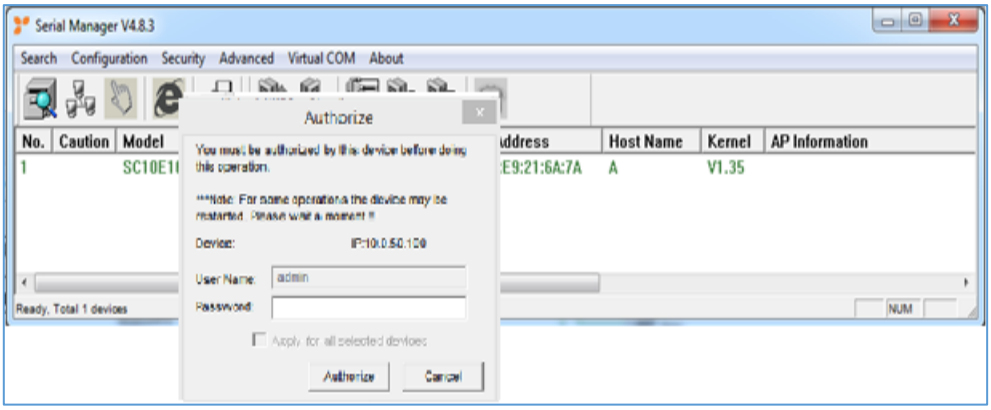


Figure 2.3 Authorization for Changes of Network Setting

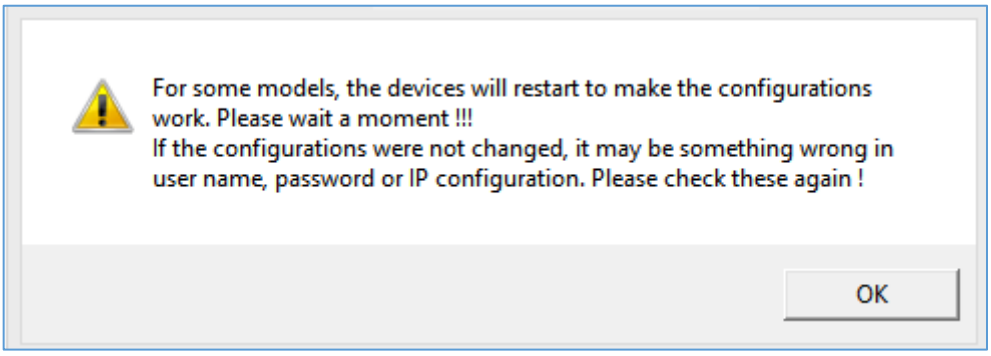


Figure 2.4 Pop-up Notification Window after Authorization

Please consult your system administrator if you do not know your network's subnet mask and gateway address.
Note: If your LAN address begins with 192.168.X.X, please use the LAN2 interface for configuration.

1.3 Configuring through Web Interface

SC10E4 MS Modbus Gateway device is equipped with a built-in web server in the firmware. Therefore, the device can be accessed by using a web browser for configuring by entering the device's IP address (default IP address is 10.0.50.100) in the URL field of your web browser. Figure 2.5-overview page of the web interface.

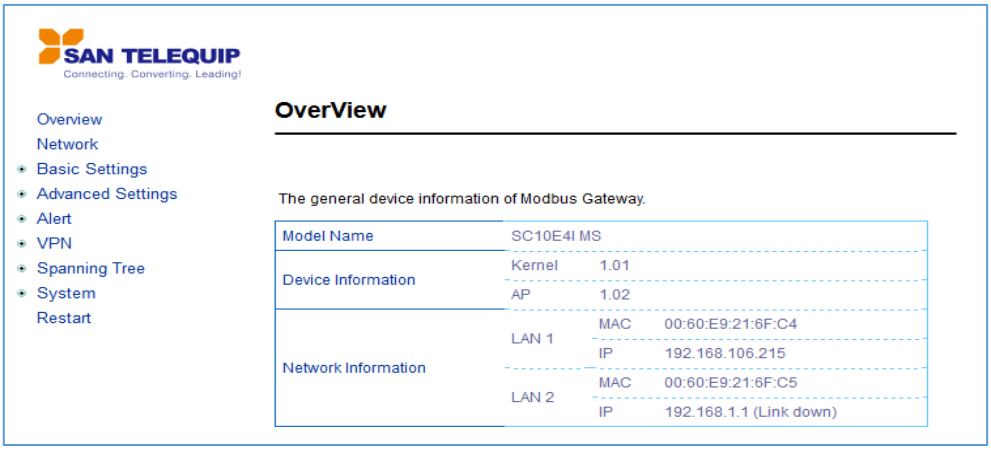


Figure 2.5 Overview Web Page of Modbus Gateway

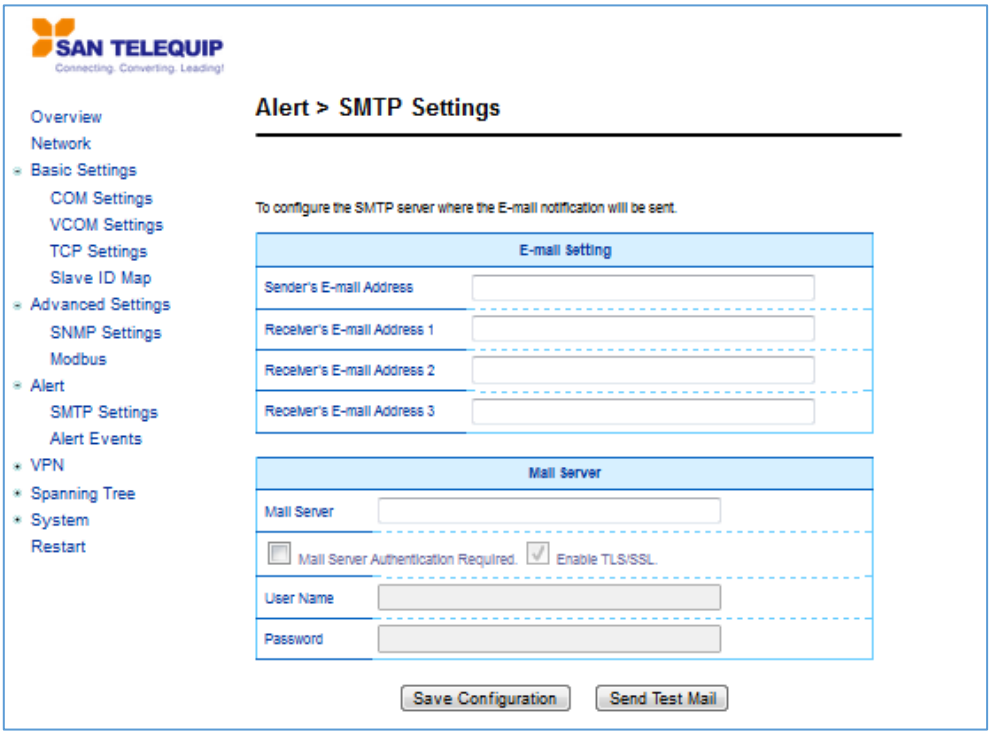


Figure 2.6 Configuring Web Page on Modbus Gateway

This approach for configuring your device is the most user-friendly. It is the most recommended and the most common method used for SC10E4 MS Series Modbus Gateway. Please go to its corresponding section for a detailed explanation.

1.4 Configuring Automatic IP Assignment with DHCP

A DHCP server can automatically assign IP addresses, Subnet Mask and Network Gateway to LAN1 or LAN2 interface. You can simply check the **"DHCP (Obtain an IP Automatically)"** checkbox in the Network Setting dialog as shown in Figure 2.2 using **Serial Manager Utility** and then restart the device. Once restarted, the IP address will be configured automatically.

1.5 Web Overview

In this section, current information on the device's status and settings will be displayed. An example of SC10E4IM S overview page is shown in Figure 2.7.

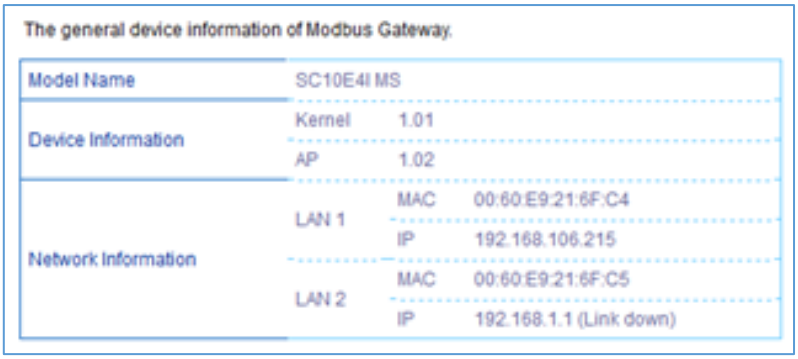


Figure 2.7 Overview Web Page

In detail, the following information is given:

- **Model Name**, shows the device's model
- **Device Information** displays information on the Kernel version as well as the AP version of your Modbus Gateway device.
- **Network Information** shows the Mode in which the Modbus Gateway device is currently operating on (Dual Subnet Mode or Redundancy Mode), both LANs corresponding MAC and IP addresses for Dual Subnet mode.
    - **Dual Subnet Mode:** Two Ethernet ports have separate IP addresses and subnets.
    - **Redundancy Mode:** The system will use only one port for data transfer. If the port is disconnected, the whole system will change to another port automatically.

1.6 Network Configuration

In this section, IP address, Subnet Mask, Default **(**Network**)** Gateway, Domain Name System (DNS) and overall connectivity settings of Modbus Gateway device can be accessed as shown in Figure 2.. For any LAN Interface Settings (i.e. LAN1 or LAN2), you can check the corresponding DHCP box to obtain an IP address, Subnet Mask, and Default **(**Network**)** Gateway automatically. The Default Gateway Select box is the next option after the LAN Interface Settings. In this box, you will have option to select (either one of the two radio buttons) which LAN interface (LAN1 or LAN2) will be the default interface in the Default Gateway Select box.

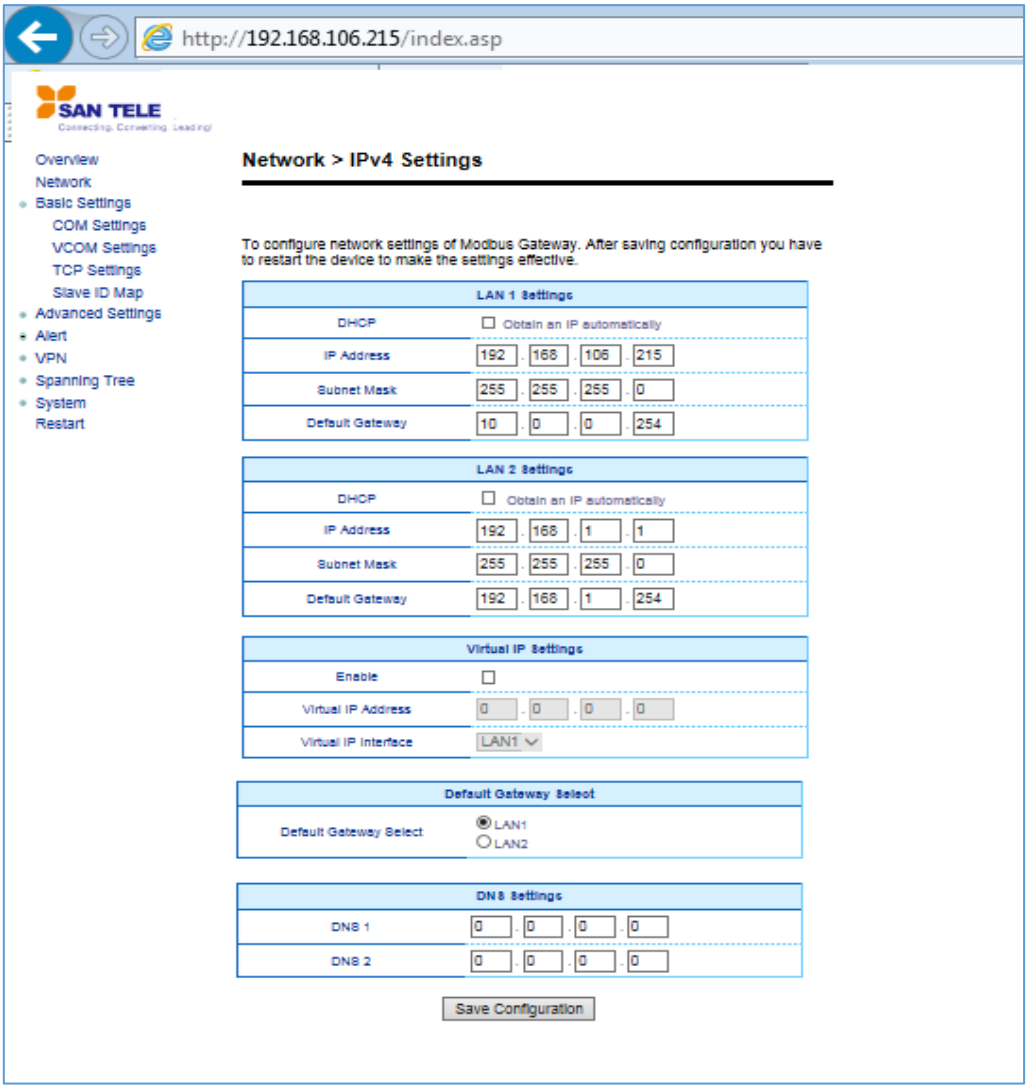


Figure 2.8 Network Web Page

At the lowest box in Figure 2., you will have the **DNS Settings** box which allows you to set the **IP addresses** of Domain Name Server 1 (**DNS 1**) and Domain Name Server 2 (**DNS 2**) for redundancy. If the device is connected to the Internet and should connect to other servers over the Internet to get some services such as Network Time Protocol (NTP) server, the user will need to configure the DNS server in order to be able to resolve the host name of the NTP server. Please consult your network administrator or internet service provider (ISP) to obtain local DNS's IP addresses.

1.7 Spanning Tree

Spanning tree functionality is supported SC10E4 MS Industrial Device Server series. However, SC10E4 MS is only an end device in a network; therefore, it only has the receiving function of spanning tree. Generally, the **S**panning **T**ree **P**rotocol (**STP**) provides a function to prevent switching loops and broadcast radiation at the OSI layer 2. A switching loop occurs in a network when there are multiple connections or redundant paths between two network switches or at least two ports are connected on both sides of the two network switches. The switching loop can create a broadcast radiation, which is the accumulation of broadcast and multicast traffics in a computer network. As broadcast and multicast

messages are forwarded by bridges/switches to every port, the bridges/switches will repeatedly rebroadcast the broadcast messages, and this accumulation of traffic can flood the network. STP creates a spanning tree topology and disables those links of the network that are not part of the spanning tree, which leaves only a single active path between two nodes. This function can avoid flooding and increase network efficiency. Therefore, SC10E4 MS deploys spanning tree as a tool when the users set up connection or port redundancy or fault-tolerance in their network.

RSTP (**R**apid **S**panning **T**ree **P**rotocol), IEEE 802.1W, is the only mode of spanning tree supported in SC10E4 MS. It is an evolution of the STP (IEEE 802.1D standard), but it is still backwards compatible with standard STP. RSTP has the advantage over the STP. When there is a topology change such as link failure in the network, the RSTP will converge significantly faster to a new spanning tree topology. RSTP improves convergence on point-to-point links by reducing the Max-Age time to 3 times Hello interval, removing the STP listening state, and exchanging a handshake between two switches to quickly transition the port to forwarding state.

The **Spanning Tree** menu and its sub-menus can be found on left frame of the web interface of SC10E4 MS. The list of **Spanning Tree** menu is shown in 3.9. The sub-menus und the **Spanning Tree** are **Setting**, **Bridge Info**, and **Port Setting**. Each of this sub-menu will be described in the following subsections.

Figure 2.9 Spanning Tree Menu

1.7.1 Spanning Tree's Setting

Figure 2.40 shows an example of **Setting** web page of **Spanning Tree** menu. The **Spanning Tree Setting** page is divided into three parts which are **Mode Setting**, **Main Setting**, and **Port Setting**. For SC10E4 MS, the user can only select one spanning tree mode, which is the **RSTP** (Rapid Spanning Tree Protocol) under the **Mode Setting**. The user can enable or disable spanning tree protocol under the **Main Setting** by checking the box behind the **Enabled** option. Note that when Enabled option is checked, the rest of the fields will become active. Then, the user can configure the **Prioirty**, **Maximum Age**, **Hello Time**, and **Forward Delay** or can leave the default setting values for each of these options. Under the **Port Setting** part, the user can select two different ports for **Primary Port** and **Secondary Port** options from the drop-down list. After configuring the spanning tree's parameters, please click **Update** button at the end of the page to allow the change to take effect. The description of each parameter is summarized in Table.

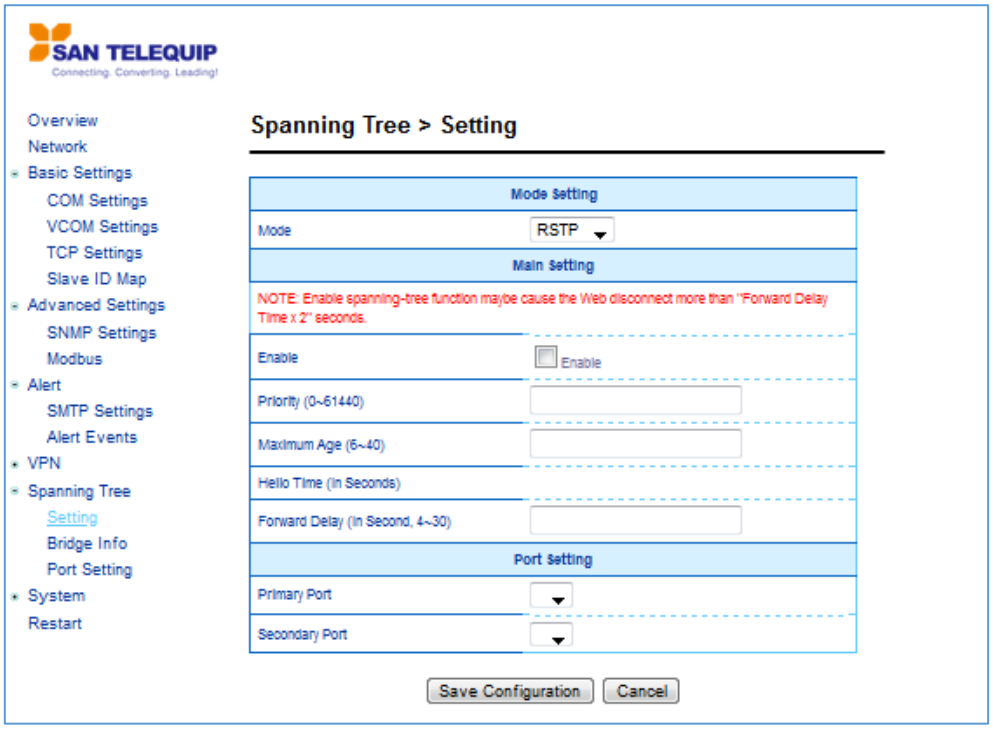


Figure 2.40 Setting Web Page of Spanning Tree

Table 2.3 Descriptions of Spanning Tree Parameters

Label	Description	Default Factory
Mode	Mode of Spanning Tree Protocol to be enabled on SC10E4 MS	RSTP
Enabled	Check the box to enable spanning tree functionality.	Disable
Priority	Enter a number to set the device priority. The value is in between 0 and 61440. The lower number gives higher priority.	32768
Maximum Age	Maximum expected arrival time for a hello message. It should be longer than Hello Time.	20
Hello Time	Hello time interval is given in seconds. The value is in between 1 to 10.	2
Forward Delay	Specify the time spent in the listening and learning states in seconds. The value is in between 4 to 30.	15
Primary Port	Spanning tree's primary port	LAN1
Secondary Port	Spanning tree's secondary port	LAN2

Note: To disable spanning tree function on SC10E4 MS, the user can uncheck the **Enable** option and then click **Update** butoon.

1.7.2 Spanning Tree's Bridge Info

Bridge Info (information) provides the current configured parameters of spanning tree protocol as shown in Figure 2.51. Note that this page will not display any data on all fields if the RSTP was not enabled in the Spanning Tree's **Setting** web page. The information is further divided into two parts: **Root Information** and **Topology Information**. To check the latest information, please click on the

Refresh button at the end of the page. Table 2.4 and Table 2.5 summarize the descriptions of each entry in the root information table and topology information table, respectively.

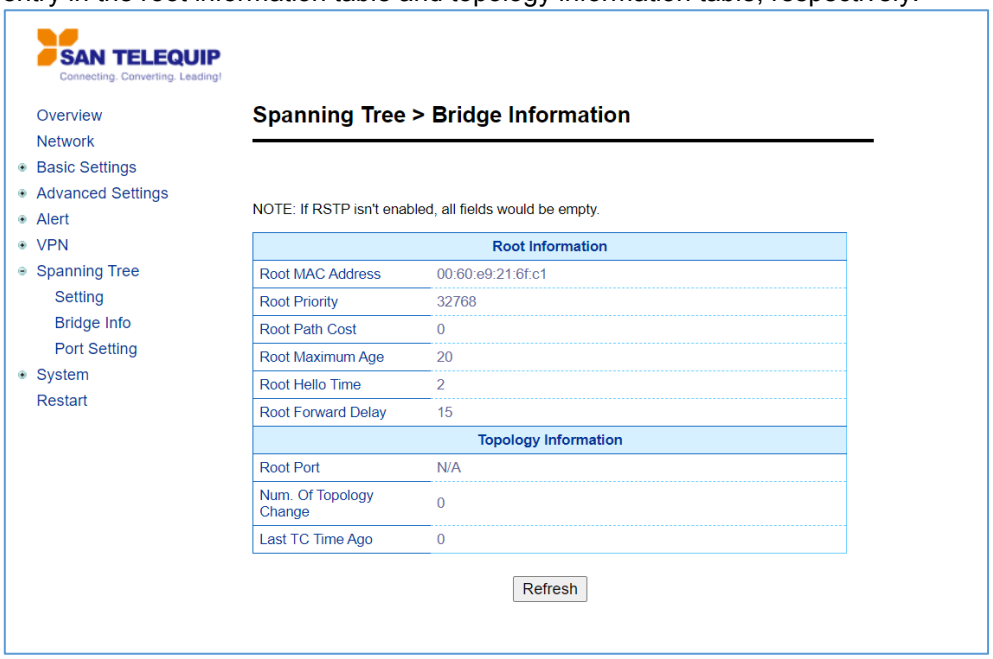


Figure 2.5 Bridge Info Web Page of Spanning Tree

Table 2.4 Bridge's Root Information

Label	Description	Factory Default
Root MAC Address	MAC address of the root of the spanning tree	-
Root Priority	Root's priority value: The device with highest priority has the lowest priority value and it will be elected as the root of the spanning tree.	0
Root Path Cost	Root's path cost is calculated from the data rate of the device's port.	0
Root Maximum Age	Root's maximum age is the maximum amount of time that the device will maintain protocol information received on a link.	0
Root Hello Time	Root's hello time which is the time interval for RSTP to send out a hello message to the neighboring nodes to detect any change in the topology.	0
Root Forward Delay	Root's forward delay is the duration that the switch will be in learning and listening states before a link begins forwarding.	0

Table 2.5 Bridge's Topology Information

Label	Description	Factory Default
Root Port	A forwarding port that is the best port from non-root bridge/switch (SC10E4 MS) to root bridge/switch. Note that for a root switch there is no root port.	-

Num. of Topology Change	The total number of spanning topology change over time.	0
Last TC time ago	The duration of time since last spanning topology change.	-

1.7.3 Spanning Tree's Port Setting

Spanning Tree's **Port Setting** shows the configured value of spanning tree protocol for each port, as shown in Figure 2.6 and Figure 2.7. The configured information for each port is **state**, **role**, **path cost**, **path priority**, **link type**, **edge**, **cost**, and **designated information**. To check the latest update on the statistics, please click on the **Refresh** button. Table 2.6 summarizes the descriptions of spanning three port setting. If **Spanning Tree** is enabled, the table of **Spanning Tree Port Stting** becomes editable and four parameters (**Path Cost** (**Config**), path priority (**Pri**), **Link Type** (**Config**) and **Edge** (**Config**)) can be adjusted on this page. The user can use the **Update** button to save the settings.

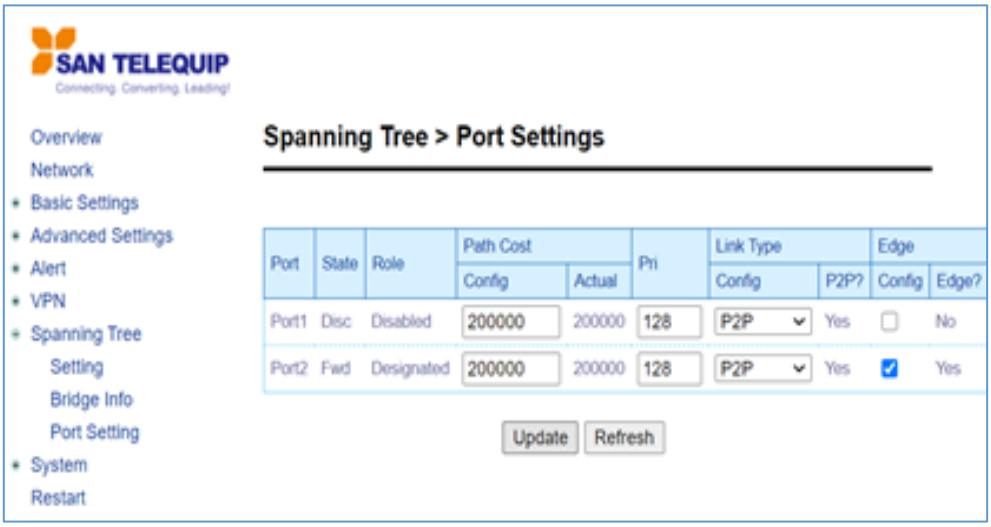


Figure 2.6 Spanning Tree Port Setting (Part 1)

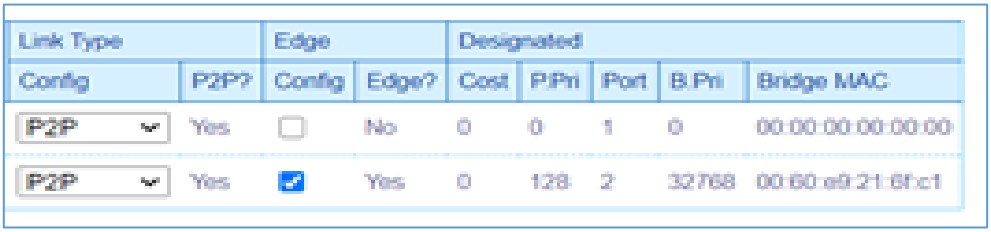


Figure 2.73 Spanning Tree Port Setting (Part 2)

Table 2.6 Descriptions of Spanning Tree Port Setting

Label	Description	Factory Default
Port	The name of the SC10E4 MS port	-
State	State of the port: **'Disc':** Discarding - No user data is sent over the port. **'Lrn':** Learning - The port is not forwarding frames yet, but it is populating its MAC Address Table. **'Fwd':** Forwarding - The port is fully operational.	N/A
Role	Non-STP or STP RSTP bridge port roles:	Non-STP

		'Root' - A forwarding port that is the best port from non-root bridge to root bridge. **'Designated'** - A forwarding port for every LAN segment. **'Alternate'** - An alternate path to the root bridge. This path is different from using the root port. **'Backup'** - A backup/redundant path to a segment whose another bridge port already connects. **'Disabled'** - Note strictly part of STP, a network administrator can manually disable a port.	
Path Cost		Setting the path cost for each switch port	
	Config	Setting path cost (default: 0, meaning that using the system default value (depending on link speed))	0
	Actual	The actual value path cost (For RSTP, please see Note 1 below and table.)	0
Pri		Setting the port priority, used in the Port ID field of BPDU packet, value = 16 x N, (N:0~15) See Note 2 below.	128
Link Type		The connection between two or more switches (for RSTP)	
	Config	Setting of the Link Type **P2P:** A port that operates in full-duplex mode is assumed to be point-to-pint link. **Non-P2P:** A half-duplex port (through a hub) **Auto:** Detect link type automatically	Auto
	P2P?	**Yes:** This port is a Point-to-Point (P2P). **No:** This port is not Point-to-Point (Non-P2P).	No
Edge		Edge port is a port which no other STP/RSTP switch connect to (for RSTP). An edge port can be set to forwarding state directly.	
	Config	Edge functional is set: **Yes** or **No**	No
	Edge?	**Yes:** This port is an edge port. **No:** This port is not an edge port.	No
Designated		This shows some information of the best BPDU packet through this port.	
	Cost	Root path cost	0
	P. Pri. (Port Priority)	Port priority (high 4 bits of the Port ID), Value = 16 x N, (N: 0~15)	128
	Port	Interface number (lower 12 bits of the Port ID)	-
	Bri. Pri. (Bridge Priority)	Bridge priority, (value = 4096 x N, (N: 0~15)	32768
	Bridge MAC	The MAC address of the switch which sent this BPDU	-

Note: In general, the path cost is dependent on the link speed. Table 2.7 lists the default values of path cost for RSTP.

Table 2.7 Default Path Cost for RSTP

Data Rate	RSTP Cost (802.1W-2004)
4 Mbits/s	5,000,000
10 Mbits/s	2,000,000
16 Mbits/s	1,250,000

San Telequip Private Limited.
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27273455, 9764027070, 8390069393
email : info@santelequip.com

Data Rate	RSTP Cost (802.1W-2004)
100 Mbits/s	200,000
1 Gbits/s	20,000
2 Gbits/s	10,000
10 Gbits/s	2,000

2. The sequence of events to determine the best received BPDU (which is the best path to the root).
   - Lowest root bridge ID determines the root bridge.
   - Lowest cost to the root bridge favors the upstream switch with the least cost to root.
   - Lowest sender bridge ID serves as a tie breaker if multiple upstream switches have equal cost to root.
   - Lowest sender port ID serves as a tie breaker if a switch has multiple (non-Ether channel) links to a single upstream switch.

   Bridge ID = priority (4 bits) + locally assigned system ID extension (12 bits) + ID [MAC Address] 48 bits
   The default bridge priority is 32768.
   Port ID = priority (4 bits) + ID (Interface number) (12 bits)
   The default port priority is 128.

1.8 Basic Settings

In this section, the term **"**Modbus Gateway device**"** will be used to refer to the SC10E4 MS series and the term **"**serial device**"** to refer to any Modbus device that connect to Modbus Gateway via COM, VCOM, or TCP connections. In any Modbus network, there are two types of Modbus devices: Modbus Master and Modbus Slave. The Modbus Master will send a request message to a Modbus Slave. Then, the Modbus Slave will respond to the Modbus Master's request. A Modbus device (serial device) that is connected to the SC10E4 MS series Modbus Gateway device will either assume a role of Modbus Master or Modbus Slave. The basic settings in this section will address how to configure the role of the serial device in your Modbus Gateway device and its serial communication parameters. The term **"**Operation Mode**"** will be used to refer to the combination of role (Master or Slave) and the message or data transfer types (RTU/ASCII/TCP) of the Modbus protocol used by the serial device.

1.8.1 COM Settings

This section shows how to set up the physical ports of the Modbus Gateway device (COM ports or serial ports that serial devices are connected to). The available number of COM ports may vary according to the chosen Modbus Gateway model. Figure 2.7 shows the COM Settings web page in which COM1 port is shown with its Operation Mode under Modbus Setting and Serial Configuration settings. These settings will configure the role of the serial device through the Operation Mode and the serial communication parameters of that serial device through the Serial Configuration settings.

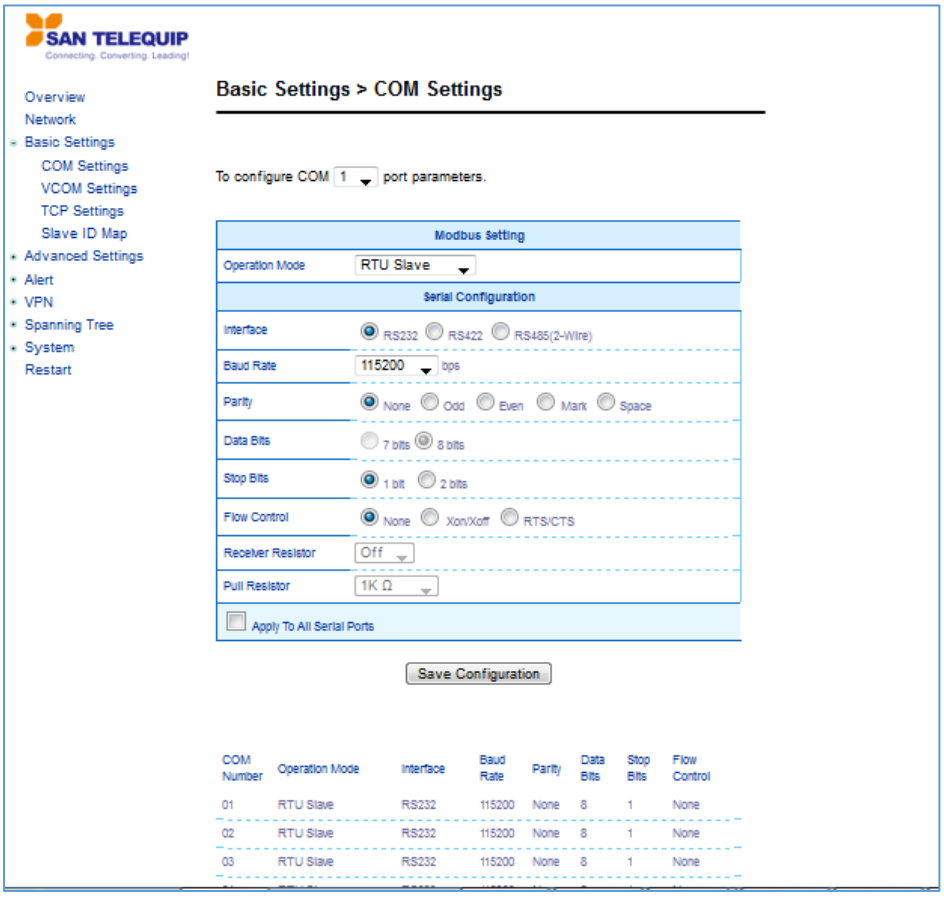


Figure 2.7 COM Settings Web Page

1.8.2 Operation Mode

To set the Operation Mode of the serial device that is connected to the Modbus Gateway through a COM port, use the pull-down menu to select among the following modes under Modbus Setting.

- **RTU Slave:** The serial device is working as a Modbus Slave node: the serial device will wait, accept request from, and response to its Modbus Master node. Data transfer is done in RTU format.
- **RTU Master:** The serial device is working as a Modbus Master node: the serial device will issue commands to or query Modbus slave nodes. Data transfer is done in RTU format.
- **ASCII Slave:** The serial device is working as a Modbus Slave node: the serial device will wait, accept request from, and response to its Modbus Master node. Data transfer is done in ASCII format.
- **ASCII Master:** The serial device is working as a Modbus Master node: the serial device will issue commands to or query Modbus Slave nodes. Data transfer is done in ASCII format.

1.8.3 Serial Settings

This section summarizes the options of serial communication parameters used between the serial device and the Modbus Gateway device over the selected COM port.

- RS-232/RS-422/RS-485 (2-wire) Software Selectable
- Baud-rate: 110 bps ~ 921600 bps Software Selectable
- Parity: None, Odd, Even, Mark, or Space
- Data Bits: 5, 6,7 or 8
- Stop Bits: 1 or 2 Software Selectable
- Flow Control: None, Software Xon/Xoff, Hardware RTS/CTS
- Receiver Resistor: On or Off
- Pull Resistor: 1K Ω or 100K Ω

Apply to all Serial Ports **(**check box**):** The settings can be chosen to apply to all serial ports if needed by checking the last checkbox on the options.

After finish the COM Settings configuration, click the Save Configuration button to save all changes that have been made. A Save Successfully message will show up as shown in Figure 2.8 and after a short period of time the web browser will be redirected back to COM Settings page (Figure 2.7).

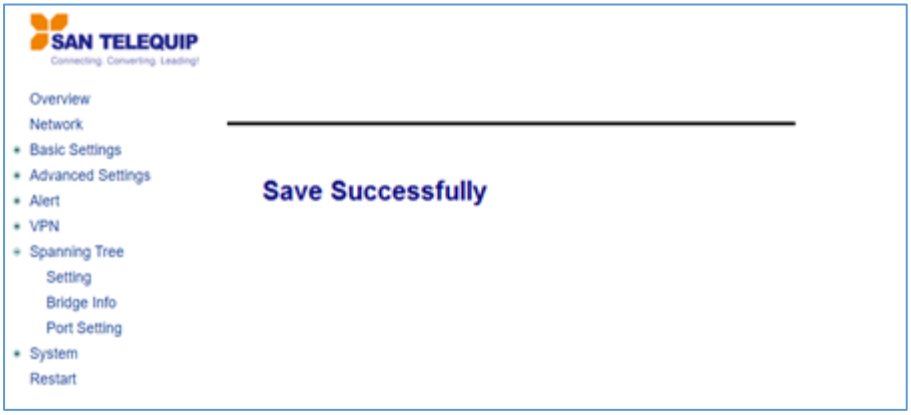


Figure 2.8 Save Successfully Message

1.8.4 VCOM Settings

These settings will generate a virtual Serial (VCOM) port within the Modbus Gateway device based on a TCP network connection. VCOM is a **TCP connection** which is encoded in an SAN Technologies' exclusive private protocol. SC10E4 MS series Modbus Gateway can only run as a TCP server which will be waiting for a connection request from a TCP client (a serial device).

Figure 2. shows the page of VCOM Settings in which the VCOM number 1 is set as an RTU Slave. This means that a device that is connected to this VCOM port on the Modbus Gateway will be a Modbus Slave node and communicate with a Modbus Master node using Modbus/RTU protocol. It is an interface concept that allows Modbus Slave devices to be connected via TCP connection by using VCOM from a PC (for example). If a VCOM setting is needed, proceed to select **Basic Settings → VCOM Settings** and check the VCOM's **"Enable"** box to allow configuration on the selected TCP's port of the Modbus Gateway device.

- **VCOM Port:** Using a TCP connection, the Modbus Gateway device (TCP server) listens to any TCP Clients (VCOM Clients) connecting (using Serial-IP) to its ports. The VCOM Port or the port of the TCP connection can be configured as a number between 1 and 65535. The default VCOM Port number is 4660.

Note: For Windows operating system, a Serial/IP software is required to use this feature. A restrictive **Serial/IP Redirector** software is installed along with **Serial Manager Utility**. The user can access the Serial/IP software through **Virtual COM → Serial/IP Tools** menu.

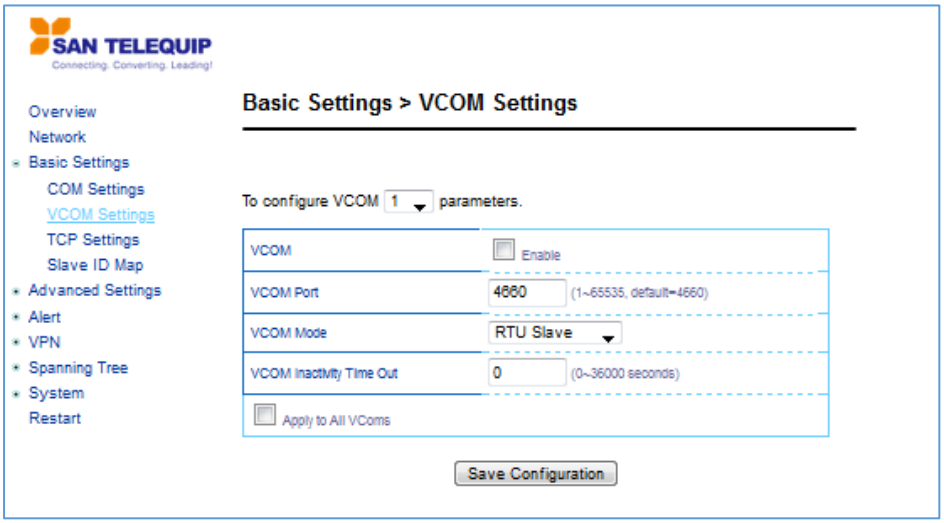


Figure 2.9 VCOM Settings Web Page

- **VCOM Mode:** This setting is a pull-down menu in which the user can select the **Operation Mode** of the devices connected through this VCOM port as shown in Figure 2.8. Its definition is the same to the one given in Section 1.8.2. Here the user can choose whether device conforms to a RTU or an ASCII message format and can select whether the device is either Modbus Slave node or Modbus Master Node. Figure 2. depicts the **RTU Slave** mode. So, the devices connected through VCOM 1 port will assume Modbus Slave role and communicate using Modbus/RTU protocol. If a Master mode (either RTU or ASCII) is selected, the options for the Master mode will be the same as the Slave mode. The only difference is the device's function.

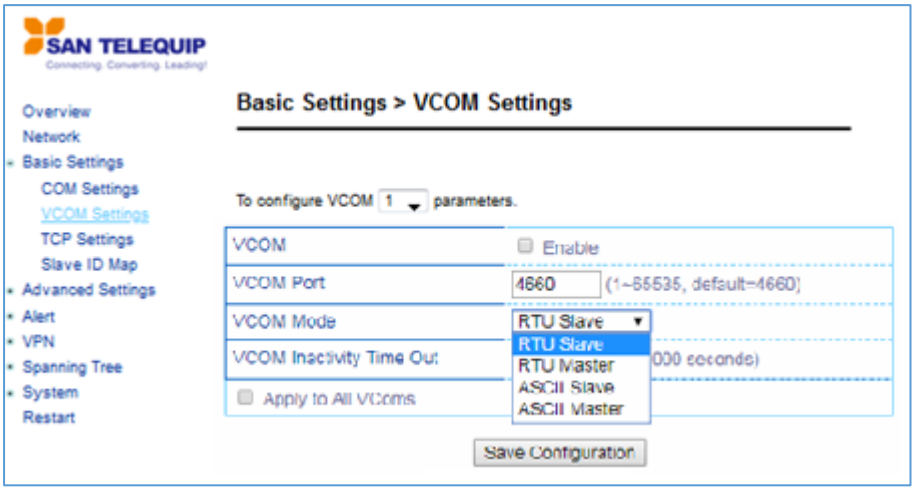


Figure 2.8 Pull-down Menu of VCOM Mode

- **VCOM inactivity Time Out:** This is a period of time allowed between actions. This setting can be set with a maximum of 600 minutes (36000 seconds) or 10 hours. If there is no activity within this period, the VCOM connection (TCP connection) will be automatically closed by the Modbus Gateway.

These settings can be applied to All VCOMs if needed by checking the last checkbox on the options. Figure 2.9 highlights the checkbox for applying the settings to all VCOMs.

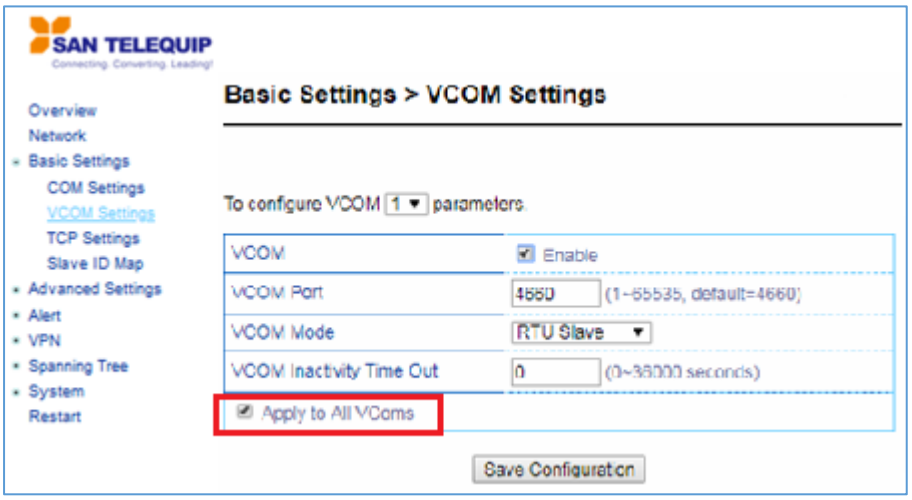


Figure 2.9 Check Box for Applying the Settings to All VCOMSs

After finishing configuring the **VCOM Settings**, click on **Save Configuration** button to save all changes that have been made. A **Save Successfully** message will show up, then the web browser will be redirected back to the **VCOM Settings** page**.**

1.8.5 TCP Settings

A device using Modbus/TCP connection, which communicates over the internet, can be set in this section. If a Modbus/TCP connection is needed, navigate to **Basic Settings → TCP Settings**, then choose whether or not to enable TCP by checking on the "**Enable**" check box. Figure 2.2 shows the Modbus TCP Settings page in which a device connected to this Modbus Gateway device is chosen to be run in **TCP Slave Operation Mode**. The device will take the Modbus Slave role and communicate using Modbus/TCP protocol.

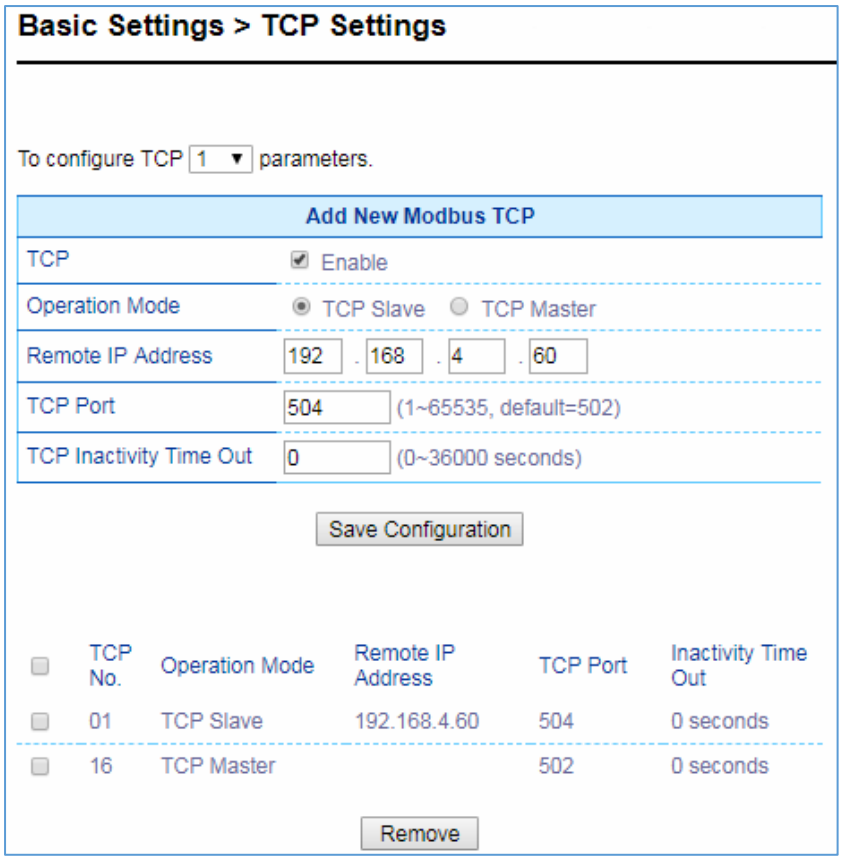


Figure 2.12 Modbus TCP Settings Web Page with TCP Slave Mode

- **Operation Mode:** There are two radio buttons in this setting: TCP Slave and TCP Master. When running on TCP Slave mode (the TCP Slave radio button is checked) as shown in Figure 2., the device will wait to receive Modbus requests from a Modbus Master. The data transmission is done under a Modbus/TCP protocol format. This means that the device will operate as a TCP Server that opens its TCP port to accept connections. The TCP Master option will be described at the end of this section.
- **Remote IP Address:** This setting shows the IP address of the device which is a Modbus slave node. This address refers to the IP address that belongs to the device that is going to be controlled from the SC10E4 MS Series Modbus Gateway device. This device can also be considered as a TCP server of whom it is needed to know its IP address. This option will disappear when the operation mode as TCP Master is selected, because in that mode the device will be running as a TCP Client which does not require to publish its IP address.
- **TCP Port:** This setting shows the TCP port number of the device (or Modbus Slave node in Figure 2.) which can be a number in between 1 and 65535. The default port number is 502.

- **TCP inactivity Time Out:** A time out period, which is the maximum period of time allowed between actions, can be set as well. This setting has a maximum duration of 600 minutes (36000 seconds) or 10 hours. If no activity has occurred within this period, the Modbus/TCP connection will be automatically terminated by the Modbus Gateway.

At the end of the TCP Settings page shown in Figure 2., a list of all configured Modbus/TCP connections with TCP No., Operation Mode, Remote IP Address, TCP Port and TCP Inactivity Time Out information will appear. The user will have the ability to remove any Modbus/TCP connection settings by checking on box in front of the record of the desired TCP settings and clicking on the Remove button. To remove all TCP connections, simply check the box on the header row of the list to select all items and click remove.

Alternatively, the Modbus/TCP connection can be configured to run in TCP Master Operation Mode. This means that the device will be a Modbus Master node and communicate using Modbus/TCP protocol. Figure 2.103 shows the TCP Master Settings. When TCP Master Operation Mode is selected, the Remote IP address setting will disappear because the device will be running as a TCP Client. Next, the TCP Port is the port through which the signal is going to be relayed upon by the Modbus Gateway. Once again, there is a TCP Inactivity Time Out with the same maximum value of 10 hours as stated in the previous mode.

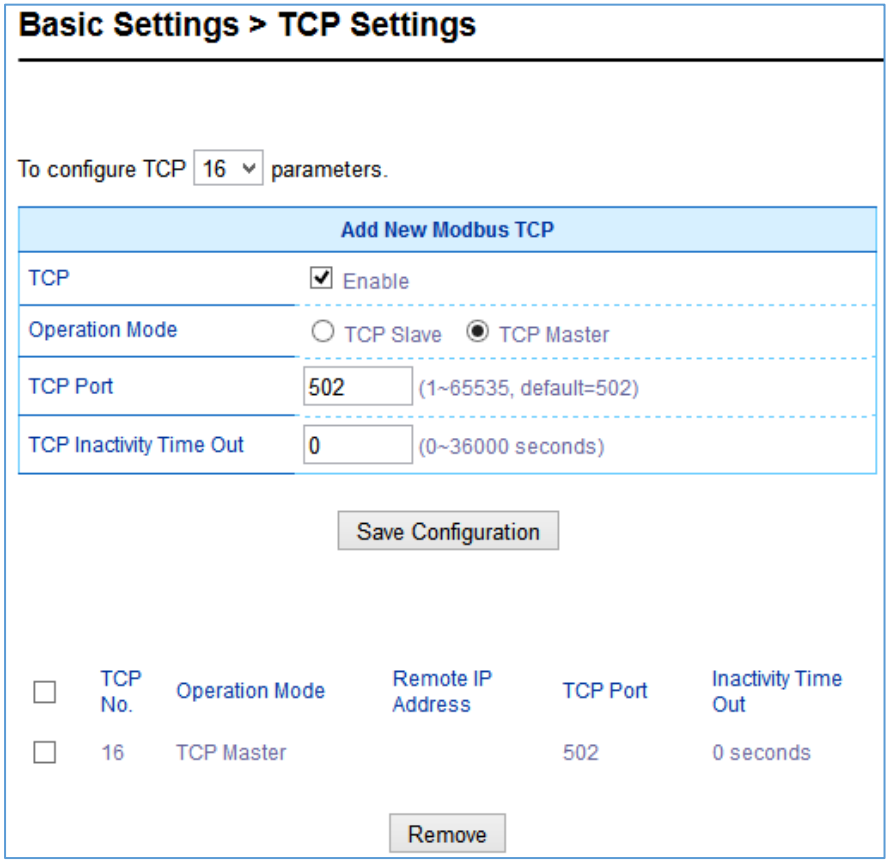


Figure 2.103 Modbus TCP Setting Page with TCP Master Operation Mode Selection

After TCP Settings configuration is finished, click on Save Configuration button to save all changes that have been made. A Save Successfully message will show up, and the web browser will be redirected back to the TCP Settings page.

1.8.6 Slave ID Map

The system uses the Modbus ID to route Modbus' request commands from a Modbus master node to the related Modbus Slave node. It is important to define ID mapping for each Modbus Slave node. For every Modbus Slave node, there should be a correct Virtual ID (Alias ID) and Real ID defined in the mapping. Figure 2.11 shows the Slave ID Map settings. To configure Slave 2's parameters, check the **Enable** box to enable Slave. Then, select the corresponding Slave interface.

- **Slave Interface:** When a port is set to Modbus slave mode, a slave interface will be created. Select a radio button of a port number behind the **Slave Interface,** which can be any one of the listed **COM/VCOM/TCP ports**.
- **Slave ID Setting Mode**: Next, select the mapping between real slave ID and Virtual ID to modify the slave ID setting as needed.

Slave ID Virtual maps a virtual ID to a real ID by the **Slave ID Count**. Figure 2.114 depicts Slave ID settings of COM02 to have real slave ID from 1 to 16 mapped from virtual ID 17 to 32.

- **Slave ID Virtual** refers to a Virtual ID for the reading Master node.
- **Slave ID Real** is the starting real ID within this interface (COM02 in Figure 2.114).
- **Slave ID Count** is the number of slave devices in this interface that are mapped.

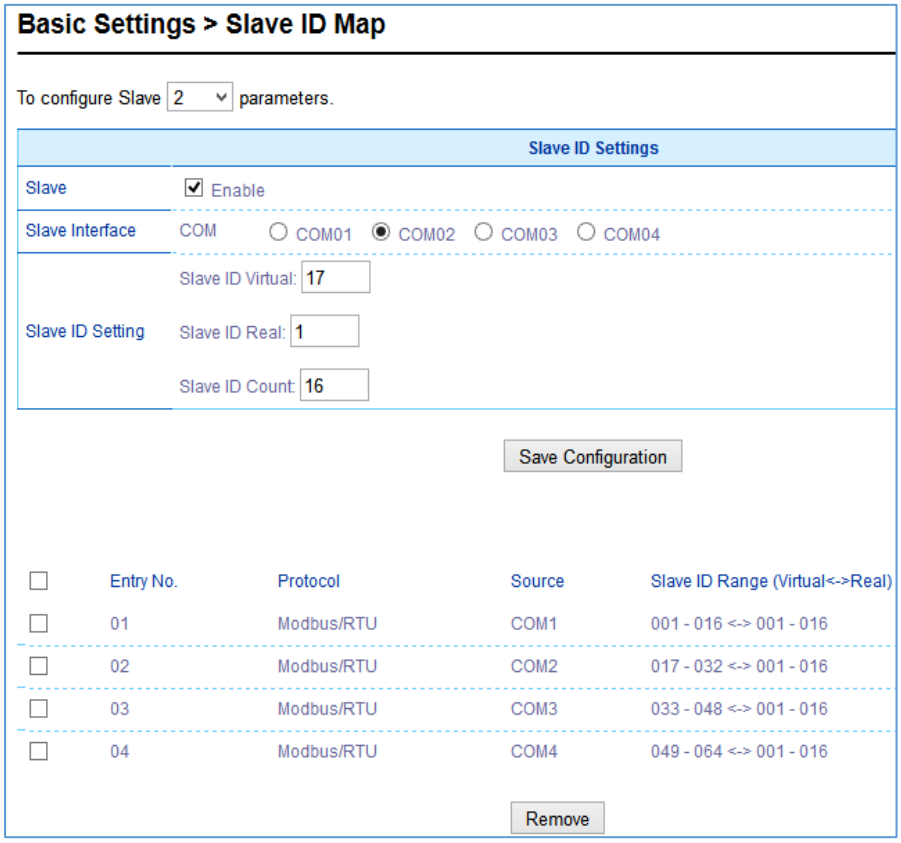
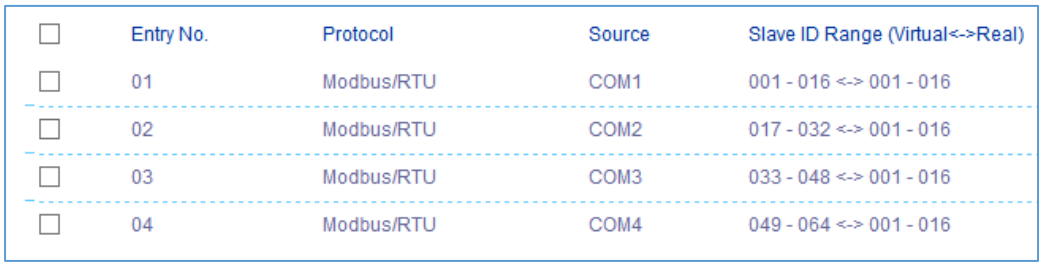


Figure 2.11 Slave ID Map Page with Slave ID Setting in Alias Mode

Note: Master and Slave IDs can be set on COM, VCOM, and TCP. However, COM works only with serial ports while TCP and VCOM operate via Ethernet ports.

After finishing configuring the **Slave ID Settings**, click the **Save Configuration** button to save all changes that have been made. A **Save Successfully** message will show up, then the web browser will be redirected back to the **Slave ID Settings** page.

Below the **Slave ID Settings** box, there is a list of mapping entries as shown in Figure 2.125 in which each line will summarize an **Entry No.**, a Modbus **Protocol**, a **Source**, a Slave ID Setting **Mode**, and the **Slave ID Range (Virtual <-> Real)**. Check the box in front of each entry to select that entry. Then, click **Remove** button to remove that particular entry from the **Slave ID Map**. To remove all entries, check on the box in front of the header line and click **Remove** button.



	Entry No.	Protocol	Source	Slave ID Range (Virtual<->Real)
☐	01	Modbus/RTU	COM1	001 - 016 <-> 001 - 016
☐	02	Modbus/RTU	COM2	017 - 032 <-> 001 - 016
☐	03	Modbus/RTU	COM3	033 - 048 <-> 001 - 016
☐	04	Modbus/RTU	COM4	049 - 064 <-> 001 - 016

Figure 2.125 Slave ID Map Web Page with Slave ID Setting in in Offset Mode

1.9 Advanced Settings

1.9.1 SNMP Settings

SNMP (Simple Network Management Protocol) Settings determine whether the device settings can be viewed with a standard SNMP software. By default, it is disabled. Figure 2.13 shows the **SNMP Settings** page with SNMP disabled. The first group of options on this web page is called **Basic Data Objects**:

- **System Contact** is the device administrator's contact information. The default value is "contact".
- **System Name,** which is by default, is the MAC address of the Modbus Gateway. The default value is "SAN TELEQUIP".
- **System Location** is the device's physical location. The default value is "location".

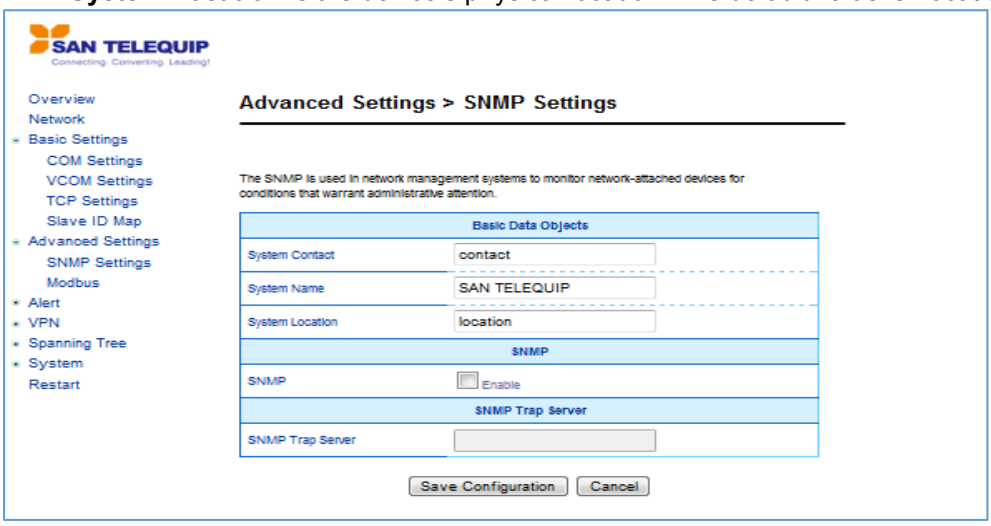


Figure 2.16 SNMP Settings Web Page with SNMP disabled

San Telequip Private Limited.
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27273455, 9764027070, 8390069393
email : info@santelequip.com

The second group of options is called **SNMP:**

- **SNMP** is followed by a "**Enable**" check box in which to enable the SNMP feature on the Modbus Gateway. If this box is not checked, it means that SNMP is disabled. Then, the rest of the options will be disappeared as shown in Figure 2. If the SNMP option is enabled, there can be three different views for SNMP options as shown in Figure 2.13, , and Figure 2.19.
- **SNMP Version** is a drop-down box, which allows the user to choose version of supported SNMP protocol. This can be **v1/v2c** or **v1/v2c/v3** or **only v3**. Note that if this option is set as v1/v2c/v3, the SNMP options will be shown as in Figure 2.13.
    - SNMP v1 and v2c support simple community string based authentication protocol for their security mechanism. If this option is selected as v1/v2c, the SNMP options will be shown as in .
    - SNMP v3 is improved with additional authentication and cryptography security. If this option is selected as Only v3, the SNMP options will be shown as in Figure 2.19.

- **Read Community** is the field that you can specify the **SNMP Read Community String** which is a user ID or plaintext password string for simple authentication in SNMP v1 and v2c. In order to make the SNMP information available for public viewing, simply flag the **"Enable SNMP"** checkbox and fill in your desired password string (the default string is **"public"**) in the **Read Community** field.
- **Write Community** is the field that you can specify the **SNMP Write Community String** which is a user ID or plaintext password string for simple authentication in SNMP v1 and v2c. In order to allow a group of people to change the SNMP information, enter your desired password string (the default string is **"private"**) in the **Write Community** field**.**
- **User Name** is the user name for SNMP account for SNMP v3.
- **Password** is the password for SNMP account for SNMP v3.
- **Encrypt** is a drop-down box which allows the user to choose the encryption scheme for SNMP v3. The available options are None, DES, or AES. The default is "None".
- **Encrypt Key** is where you can specify the encryption key for the SNMP v3 access.

The last group of option is **SNMP Trap Server**. In order to allow a trap server to collect device information, fill in **SNMP Trap Server** with its corresponding IP address (a trap server is designed to collect all alarm information from the Modbus Gateway). An example in Figure 2.13 is 192.168.106.92.

After **SNMP Settings** configuration is finished, click the **Save Configuration** button to save all changes that have been made or click **Cancel** button to discard your changes.

San Telequip Private Limited.
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27273455, 9764027070, 8390069393
email : info@santelequip.com

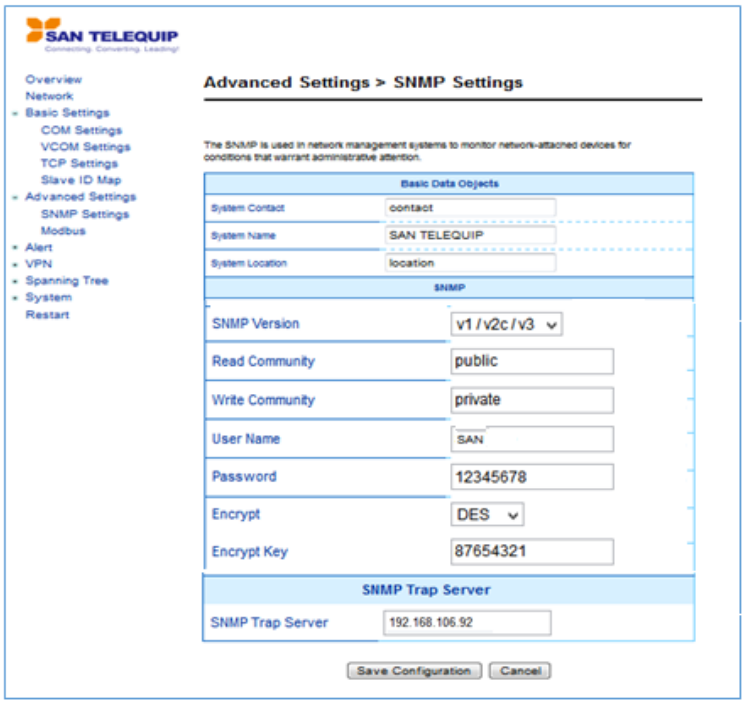


Figure 2.13 SNMP Settings Web Page with SNMP Enabled and Version v1/v2c/v3

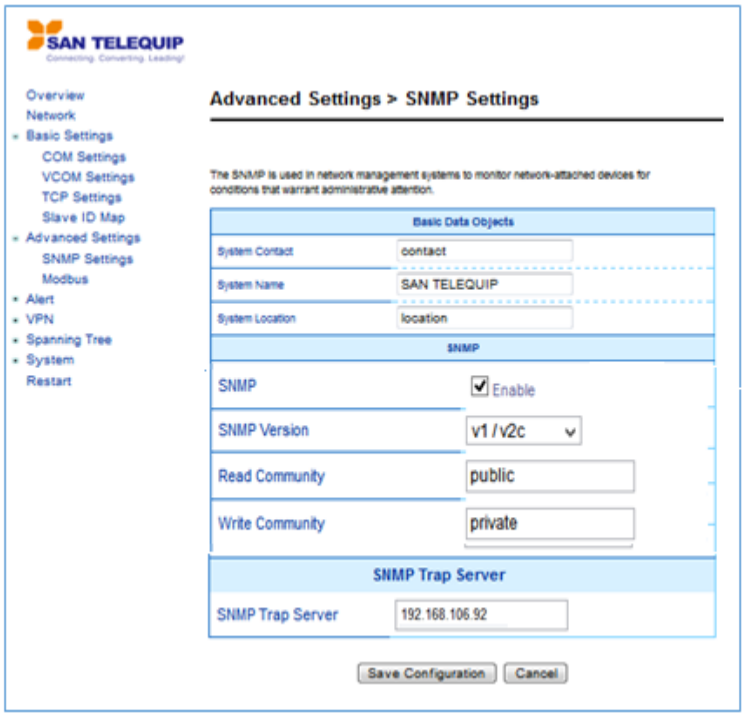


Figure 2.18 SNMP Settings Web Page with SNMP Enabled and Version v1/v2c

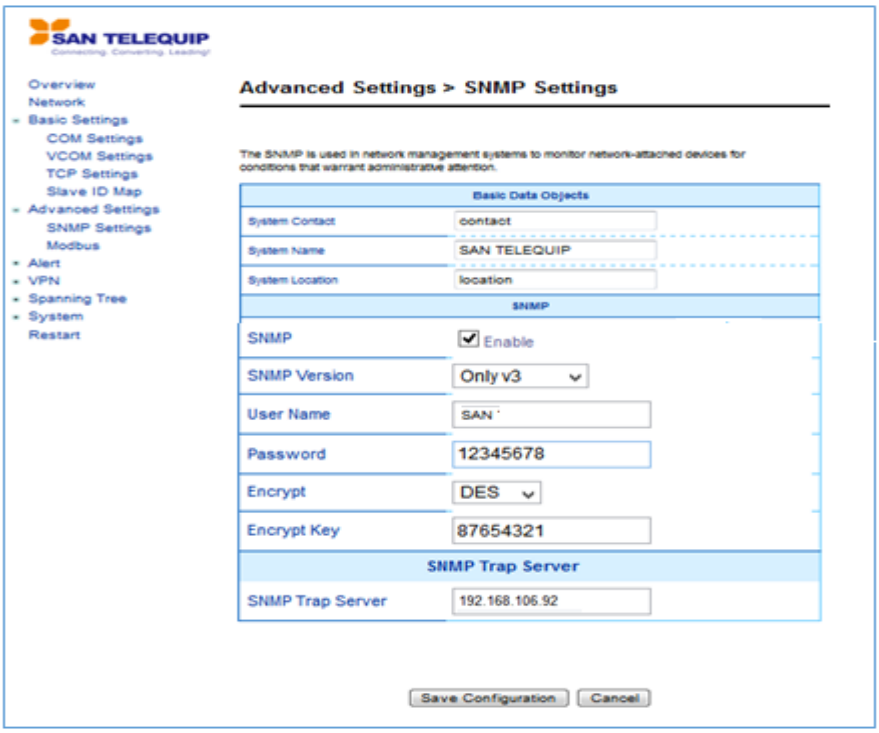


Figure 2.19 SNMP Settings Web Page with SNMP Enabled and Version Only v3

1.9.2 Modbus

In **Modbus** settings, it is possible select whether to enable **Modbus Exception** by flagging the **Enable** checkbox as shown in
Figure 2.14. If the Modbus slave returns no response and timeout occurs, it may then be necessary for the gateway to return an exception. To set **Response Timeout** for COM and TCP/VCOM, fill in the timeout periods in the fields as shown in
Figure 2.14. Note that the timeout setting can be applied to all COM ports by checking the **Apply to All Coms** box.

- Configure timeout for each COM port between 10ms to 120000ms with a default value of 1000ms.
- Configure timeout for TCP/VCOM port between 10ms to 120000ms with a default value of 1000ms.

After finishing the Advanced Modbus Settings configuration, click on the **Save Configuration** button to save all changes that have been made. A **Save Successfully** message will show up, and the web browser will be redirected back to the **Modbus** page**.**

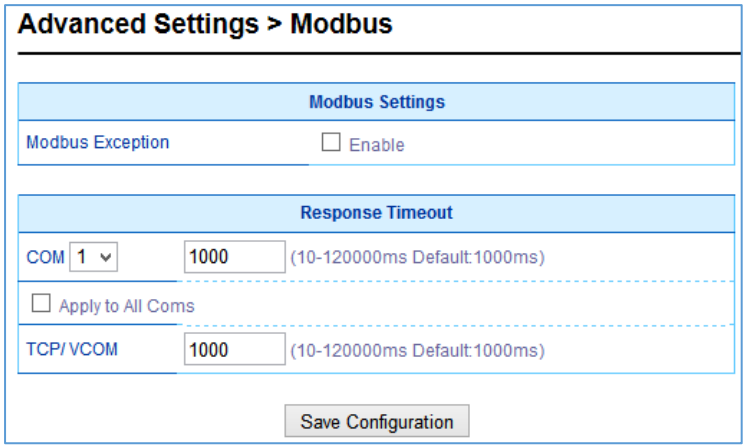


Figure 2.140 Advanced Modbus Settings of Response Timeout for Modbus Exception

1.10 Alert

1.10.1 Settings

When enabled, an E-mail alert will be sent to the designated E-mail addresses in the **SMTP** (Simple Mail Transfer Protocol) **Settings.** To setup an email alert function, the user needs to configure the **sender's E-mail address**, the **receiver's E-mail addresses** (up to three receivers), and the mail server configuration as shown in Figure 2.15. Under **Mail Server** settings, fill in the IP address or host name of a **Mail Server**. Make sure that the Modbus Gateway device is able to resolve the host name properly. This require the DNS server to be configured first as explained in Section o. If a mail server authentication is required, check on the **Mail Server Authentication Required** box and fill in the **User Name** and the **Password** fields.

After configuration of the SMTP Settings is complete, click **Save Configuration** to save all changes that have been made. A **Save Successfully** message will show up, and the web browser will be redirected back to the **SMTP Settings** page**.** The user can also send a test E-mail from the Modbus Gateway by clicking on the **Send Test Mail** button. A pop-up window will notify the user of the result of test mail. If there is a problem, please re-check the information of **Mail Server**, **User Name** and **Password** or check the network connection to the **Mail Server**.

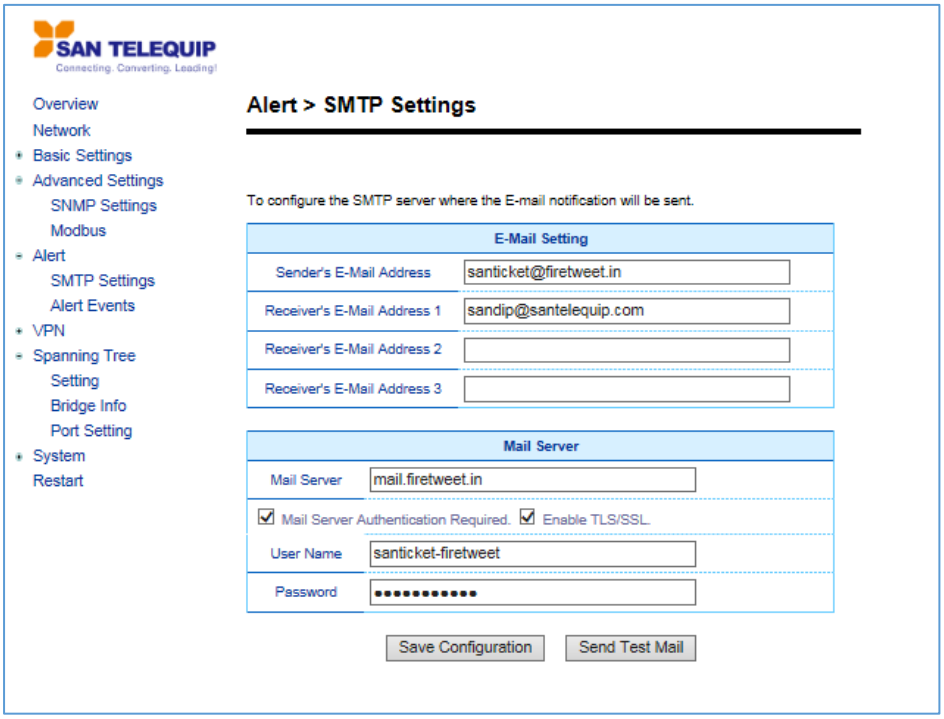


Figure 2.15 SMTP Settings Web Page

1.10.2 Alert Events

In **Alert Events** settings**,** the user can configure options to have the Modbus Gateway sending out device information to alert users, administrators, or responsible personnel as shown in Figure 2.16. They can be sent out automatically. There are seven anomalies defined on this page that can trigger alert functions (by checking the corresponding **E-mail** boxes), which are:

- **Cold Start** is an event when power supply is interrupted,
- **Warm Start** is an event when the device Restart function is used either by pressing a button or by its interface,
- **Authentication Fail** is an event when incorrect username and password are entered,
- **IP address change** is an event when the device's IP address is changed,
- **Password Changed** is an event when the authentication password is changed,
- **Watchdog Reset** is an event when the system reboots because of a hardware failure or a software crash,
- **Power Failure** : devices equipped with redundant (dual) power input are set as they expect to have power available from both sources at the same time. In the event one of the two power inputs is missing, the Relay output is triggered.

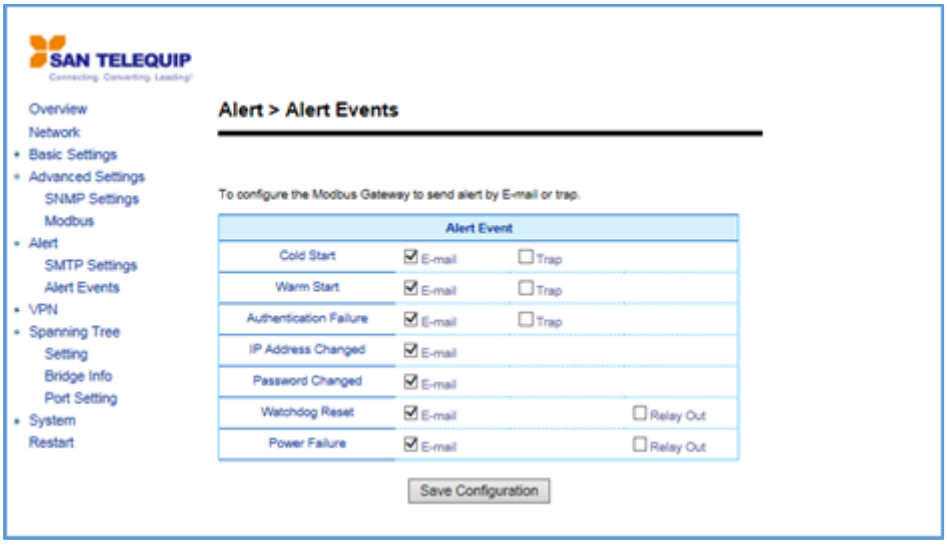


Figure 2.16 Alert Events Web Page

The user can also set an SNMP trap by checking the **Trap** checkbox for each of the first three anomalies above. This will send out alerts to an SNMP Trap Server. Note that to configure **SNMP Trap Server**.

The user can enable **Watchdog Reset** and **Power Failure** events to trigger the Relay Output alarm digital output. In order to do so, check the corresponding checkbox in front of the "**Relay Out**".

After the **Alert Events** setting is complete, click on **Save Configuration** button to save all changes that have been made. A **Save Successfully** message will show up, and the web browser will be redirected back to the **Alert Events** page**.**

1.11 VPN

A virtual private network(VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private networks, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.
See below VPN scenario of SC10E4I MS for your reference.

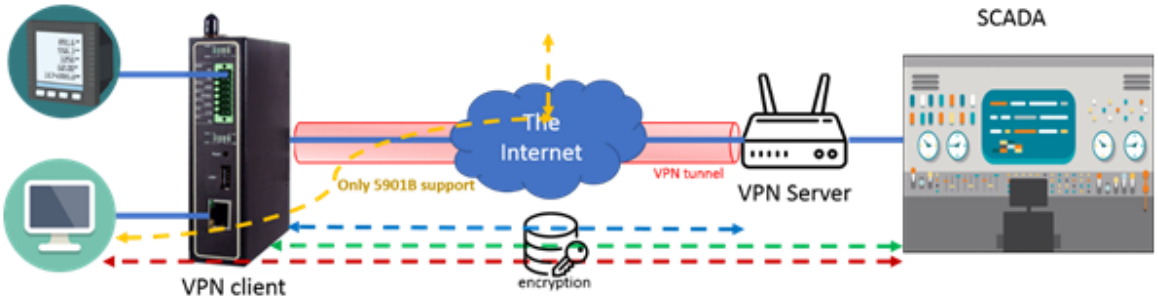


Figure 2.173 VPN Scenario of SC10E4I MS

SC10E4I MS supports several VPN protocols: PPTP (Point-to-Point-Tunneling-Protocol), IPsec (Internet Protocol Security), and OpenVPN. In order to configure VPN, please click on the related item in the dedicated VPN sub-menu on the left-hand side of the screen, as shown in 24 below.

A better description of PPTP is available in Chapter 1.12 below
A better description of OpenVPN is available in Chapter 1.13 below.
A better description of IPsec related settings is available in Chapter 1.14 below.

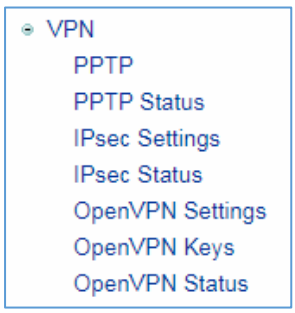


Figure 2.18 VPN menu structure

1.12 PPTP Settings

PPTP (Point-to-Point Tunnelling Protocol) is a method for implementing virtual private networks. PPTP uses a TCP control channel and a GRE tunnel to encapsulate PPP packets. Select the PPTP item in the menu to configure a PPTP tunnel. Figure 2.25 shows the PPTP configuration page under PPTP web setting. Currently SC10E4 MS series only supports PPTP client. After settings are completed, click "**Save**" to save the configuration.

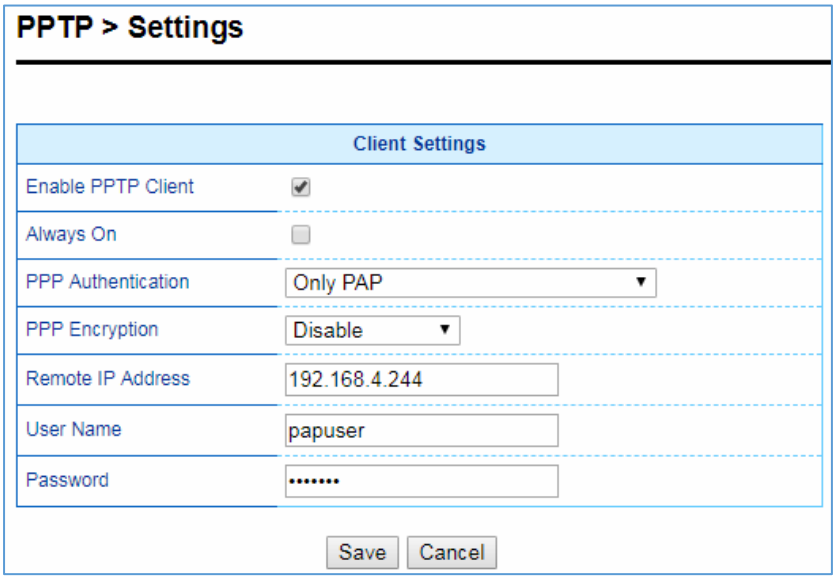


Figure 2.25 PPTP configuration page.

- Enable PPTP client: Check this to enable the PPTP client on SC10E4 MS series.
- Always on: Check this to have SC10E4 MS to automatically reconnect in event of disconnection.
- PPP Authentication: Specify here the authentication algorithm – should be same as server
- PPP Encryption: Specify here the encryption – should be same as server
- Remote IP address: Specify here the IP address of PPTP server.
- User Name: Specify here the User name for authentication.
- Password: Specify here Password for authentication.

Figure 2.26 below shows the PPTP Link status.

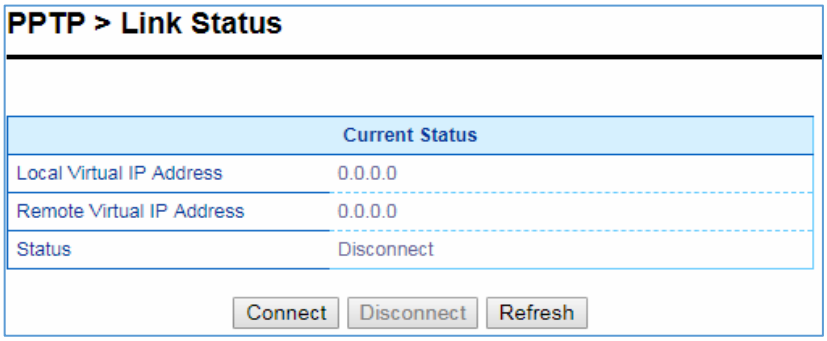


Figure 2.26 PPTP Link Status

- Local Virtual IP Address: The virtual IP address assigned by PPTP server.
- Remote Virtual IP Address: The virtual IP address of PPTP server.
- Status: It shows the PPTP tunnel connection status. It will show Disconnect, Connect and Connecting.
- Disconnect: No tunnel is established.
- Connect: PPTP Tunnel is established.
- Connecting: PPTP Tunnel is establishing.
- Connect Click this button to connect to PPTP server.
- Disconnect Click this button to disconnect PPTP tunnel.
- Refresh Click this button to refresh the PPTP tunnel status.

1.13 OpenVPN Settings

OpenVPN is an application that implements VPN for creating secure point-to-point or site-to-site connections in routed or burdged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.
OpenVPN allows peers to authenticate each other using a Static Key (pre-shared key) or certificates. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and certificate authority.
There are two OpenVPN connection scenarios. They are the TAP and TUN scenario. The product can create ether a layer-3 based IP tunnel(TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. In addition to configuring the device as a Server or Client, you have to specify which type of OpenPVN connection scenario is to be adopted. Currently SC10E4 MS series only support TUN mode.

1.13.1 OpenVPN Setting

In order to configure OpenVPN, click on the VPN tab in the left hand side of the menu and then **OpenVPN Settings**. The user interface is shown in below Figure 2.19.

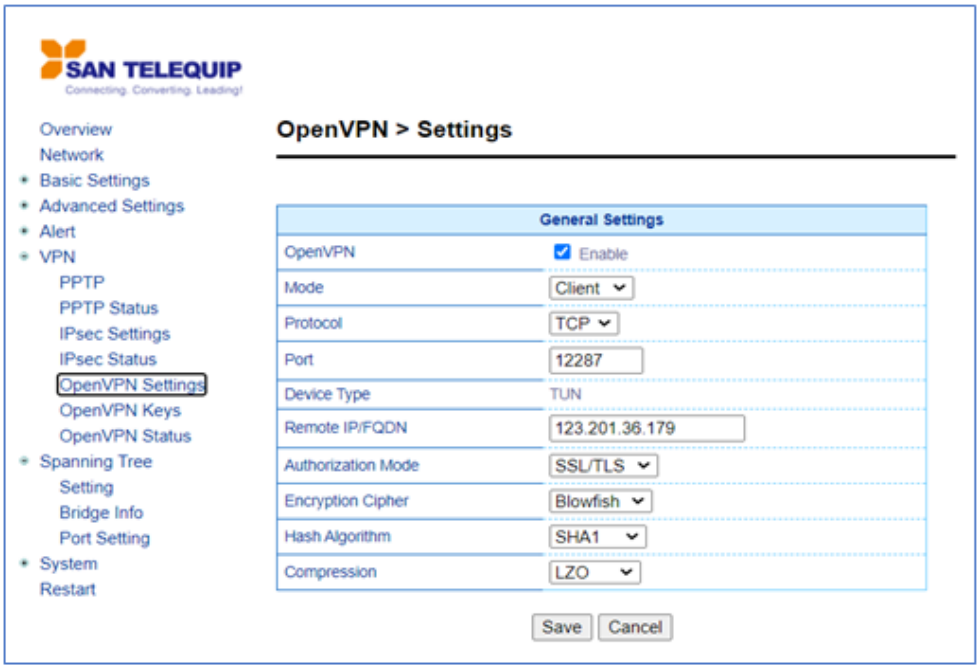


Figure 2.19 OpenVPN Setting

The OpenVPN parameters are described as below:

- **OpenVPN**: Check this to enable OpenVPN.
- **Mode**: Specifies what the scenario of this device, server or client. When choosing server mode, the device will play as server role and will standby for client connection.
- **Protocol**: Selects the transport layer protocol to be used for VPN (TCP or UDP).
- **Port**: Defines the port number for TCP/UDP connection.
- **Device Type**: OpenVPN tunnel connection by TUN (Tunnel) mode or TAP mode. Currently SC10E4 MS series only supports TUN (Tunnel) mode.
- **Virtual IP** (only when “OpenVPN Server” mode is selected): Specify the server’s virtual IP. Virtual IP will only be available when SSL/TLS is chosen as the Authentication Mode. The Server’s virtual IP address will be 10.8.0.1/24 and client virtual IP address will be 10.8.0.x/24.
- **Local/Remote endpoint IP** (only when “OpenVPN Client” mode is selected): Specifies the local and remote endpoint virtual IP address of this OpenPVN gateway. Local/Remote endpoint IP only be available when static key is chosen in Authentication Mode.
- **Authentication Mode**: Specify the authorization mode the OpenVPN server. There are 2 options available:
    - SSL/TLS: OpenVPN will use TLS authorization mode, and the following items CA cert, Server Cert and DH PEM will be used. See section 1.13.2 below for mode details.
    - Static Key: OpenVPN will use static key authorization, and the static key will be used. See section 1.13.2 below for mode details.
- **Encryption Cipher**: Specify the Encryption cipher. There are 5 options available: blowfish, AES 256, AES 192, AES 128 and Disable. When Disable is selected, no encryption will be used.

- **Hash Algorithm**: Specify the Hash algorithm. There are 5 options available: SHA1, MD5, SHA 256, SHA 512 and Disable.When Disable is selected, no Hash algorithm will be used.
- **Compression**: Specify whether or not the tunnel packets will be compressed. There are three options available: LZ4, LZO and Disable. When Disable is chosen, the packet won't be compressed.

1.13.2 OpenVPN Keys

OpenVPN requires encryption keys (unless Encryption Cipher is disabled). In order to key-in, import or generate encryption keys, please select "OpenVPN Keys" from the VPN menu on the left-hand side of the user interface.

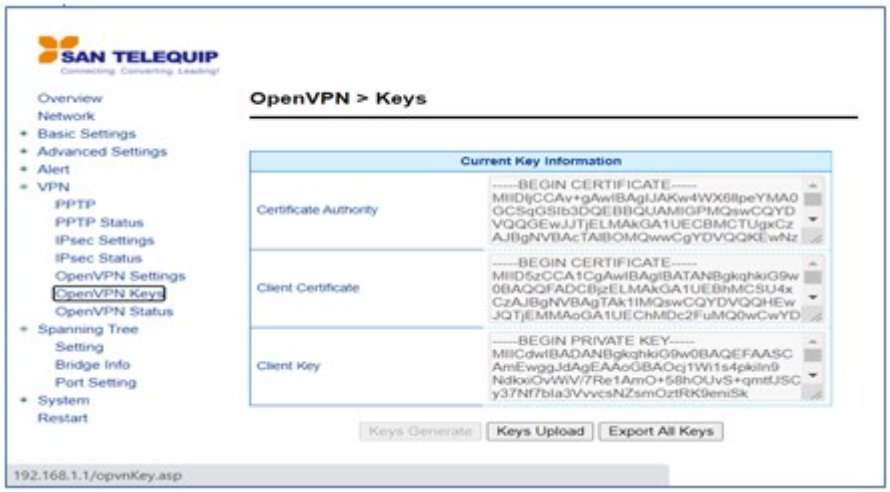


Figure 2.28 OpenVPN Keys

- **Certificate Authority**: A certificate authority(CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. A CA acts as a trusted third party, trusted both by the owner and by the party relying upon the certificate.
- **Server/Client Certificate**: It shows the information of server certificate. You can check the information if you use upload server certificate file.
- **Server/Client Key**: It shows the information of server key. You can check the information if you use upload server key file.
- **Diffie Hellman parameters (Server only)**: It shows the information of Diffie Hellman paramaters.

When SC10E4 MS acts as OpenVPN server, the user could define his own certification information by clicking on the **Secret generate** button. Otherwise, the certificate can be imported. When generating a new key, a Pop-up window will open. Fill in the parameters and click on "**Generation Keys & Apply**" button.

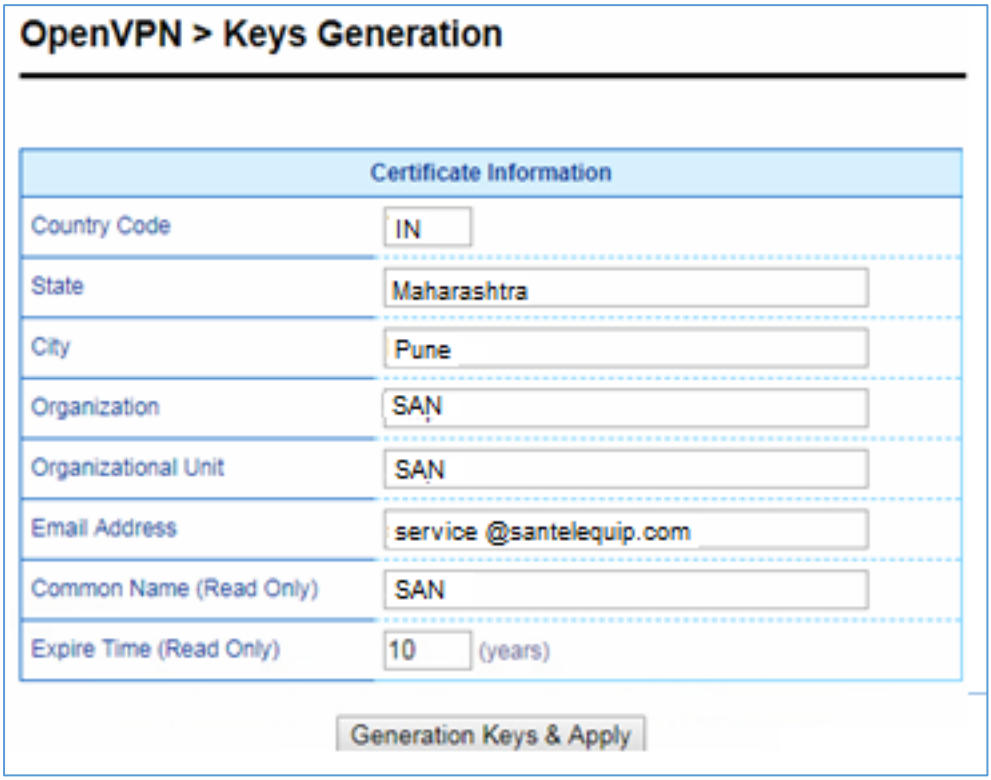


Figure 2.20 Certification information

- **Country Code**: Enter the country ISO code.
- **State**: Enter the state (if applicable)
- **City**: Enter the city
- **Organization**: Enter the name of organization.
- **Organization Unit**: Enter the unit or section in the organization.
- **Email Address**: Enter an email address.
- **Common Name**: The server name. (Read only)
- **Expire time**: The number of years the certificate is valid for. (Read only)

When clicking on the **Keys Upload** button instead, a pop-up window shown in Figure 2.210 will show up and will allow you to import the related server or client certificates.

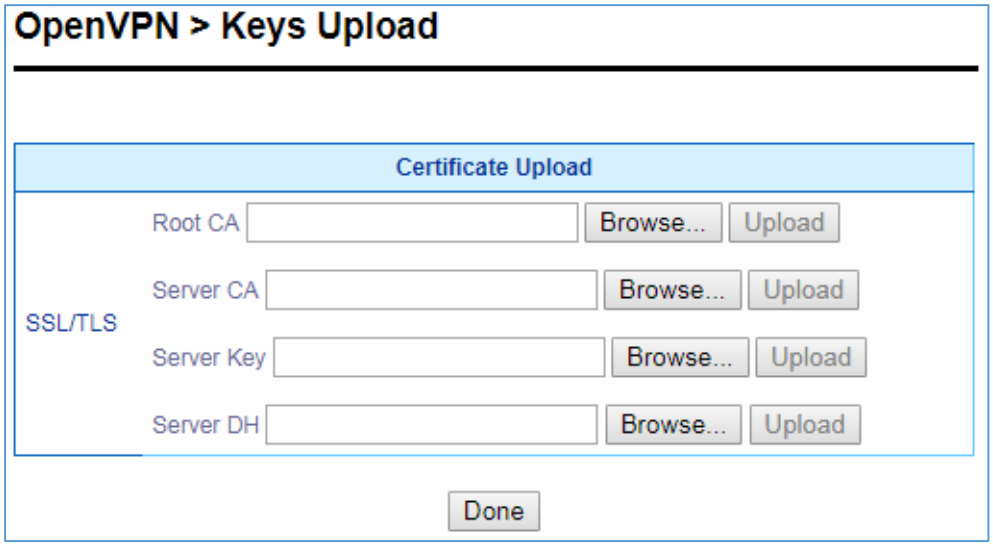


Figure 2.21 Certificate Upload

Click the **Browse** button to select your own server or client certificate and click on the **Upload** button. When SC10E4I MS acts as an OpenVPN server, use **Export All Keys** button to download all the necessary certificates include CA.crt, CA.key and the certificate and key for client side.

1.13.3 OpenVPN Status

In order to check the current OpenVPN connection status, click “OpenVPN status” in the VPN menu on the left-hand side of the screen. A page like below Figure 2.221 will show up when OpenVPN is in Server mode. It will look similar when set in Client mode.

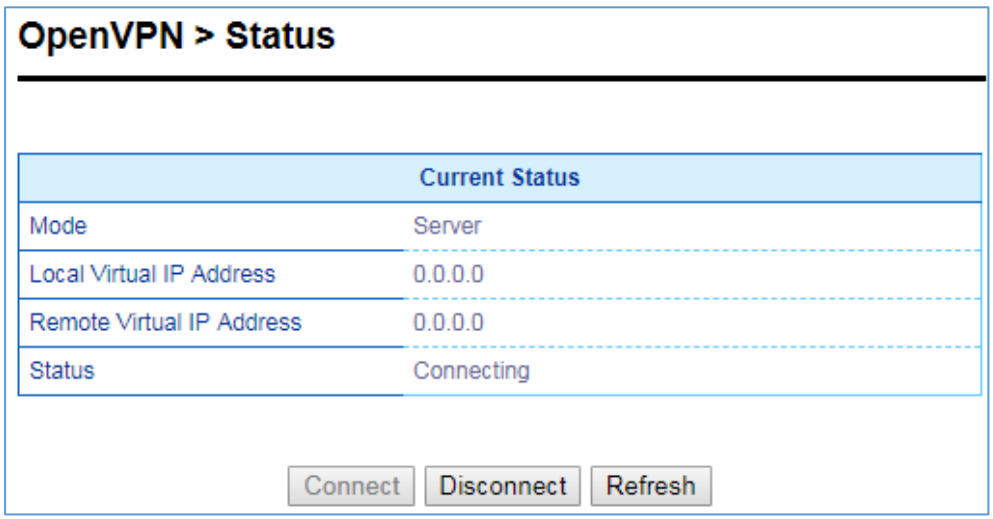


Figure 2.22 OpenVPN server status

San Telequip Private Limited.
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27273455, 9764027070, 8390069393
email : info@santelequip.com

Client Mode Description:

- **Mode**: Displays the OpenVPN mode SC10E4 MS is currently running as.
- **Local Virtual IP address**: Displays the Local virtual IP address.
- **Remote Virtual Status**: Displays the Remote virtual IP address.
- **Status**: Displays the current status of OpvnVPN connection. It will include Disconnected, Connecting and Connected.

Server Mode Description:

- **Mode**: Displays the OpenVPN modeSC10E4 MS is currently running as.
- **Local Virtual IP address**: Displays the Local virtual IP address.
- **Status**: Displays the current status of OpvnVPN connection. It will be either be Deactivated, Activating, Disconnected, Connecting and Connected.

1.14 IPsec Settings

IPsec (or Internet Protocol Security) which is a network protocol suit that can establish secure and reliable communications for different application scenarios. IPsec enables data confidentiality, data integrity, data origin authentication, and antireplay. For example, a corporate headquarter and its branch offices in the fields do not need to apply for dedicated communication lines for sharing their network resources securely. To securely communicate and shared company's resources over the Internet, IPsec connections can be employed to secure all applications at the IP layer. In another case, when employees are on a business trip, they can establish IPsec connections with their company over their mobile devices or the public network to access the internal network resources in their company.

SC10E4 MS has an IPsec connection function to establish a secure communication link between **host-to-host**, **host-to-subnet** (or host-to-network), and **subnet-to-subnet** (or network-to-network). Note that at the other endpoint of the Internet, a router or gateway with full IPsec capability is required to successfully establish the secure communication. There are two types of IPsec connection modes or types supported by SC10E4 MS which are **Tunnel mode** and **Transport mode.**

- In **Tunnel mode**, the entire IP packet is encrypted and authenticated. The IP packet is then encapsulated into a new IP packet with a new IP header. The **Tunnel mode** which is used to create Virtual Private Network (VPN) can be applied to the **host-to-host**, the **host-to-subnet**, and the **subnet-to-subnet** communications. The packet (datagram) format for **Tunnel mode** is as follow:

New IP Header	IPsec Header	Original IP Packet	Optional IPsec Trailer

- In **Transport mode**, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact because the IP header is not modified and not encrypted. However, when the authentication header is used, the IP addresses cannot be modified by Network Address Translation (NAT). The **Transport mode** can only be applied in the **host-to-host** communication. The packet (datagram) format for **Transport mode** is as follow:

Original IP Header	IPsec Header	Original IP Packet	Optional IPsec Trailer

A **host-to-host** connection is typically used in a simple point-to-point communication. It is useful for a direct communication with a server or between the device (SC10E4 MS) and a peer device (such as another SC10E4 MS). Note that this type of connection cannot be use for accessing entire sub-network resources.

Figure 2.23 illustrates an example of host-to-host connection. This configuration can be set in both **Tunnel mode** and **Transport mode.**

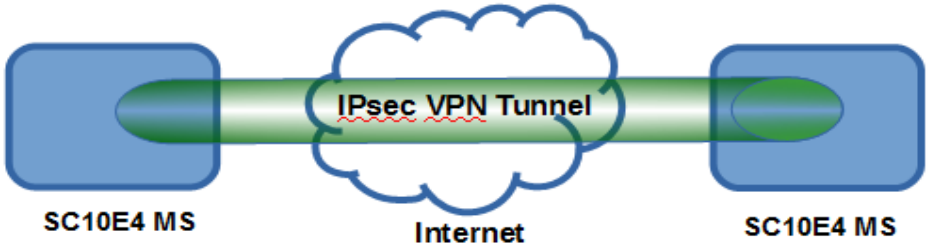


Figure 2.232 An example of Host-to-Host Connection on SC10E4 MS.

A **host-to-subnet** (or host-to-network) connection is mainly applied when one endpoint needs to access the other side's sub-networks. Typical applications are employees who are travelling on business and would like to connect back to their corporate headquarters via mobile devices. They can establish IPsec connections to access the internal corporate network resources. Figure 2.24 illustrates a road-warrior application in which SC10E4 MS can access a remote sub-network resource via a peer gateway. Figure 2.25 illustrates a gateway application in which SC10E4 MS can passively accept connection requests from remote sides and provide access to the SC10E4 MS sub-network resources. Note that both of these configurations must set the connection type to **Tunnel mode** only.

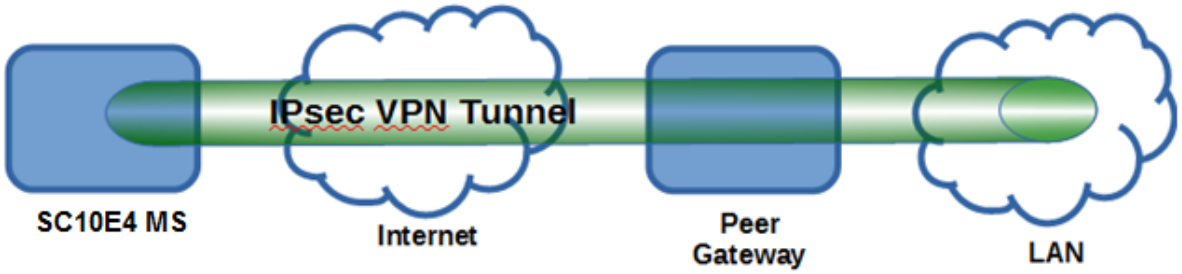


Figure 2.243 Road warrior Application using Host-to-Subnet Connection

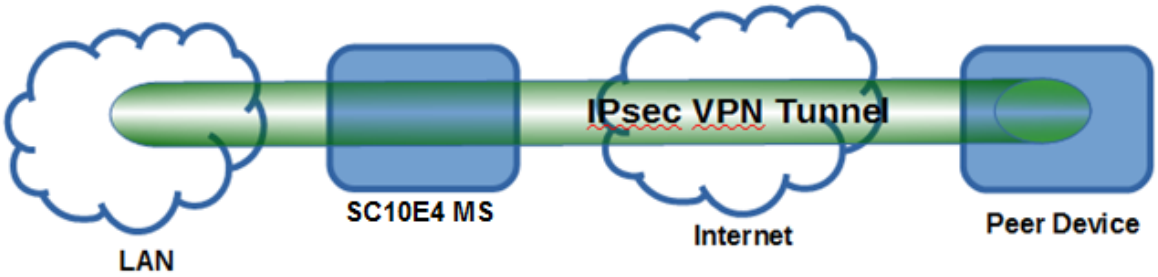


Figure 2.25 Gateway Application using Host-to-Subnet Connection

A **subnet-to-subnet** connection is mainly used to connect two subnets from different sides together. Typically, applications are corporate headquarters and branch offices that share internal network resources. A specific application can also be set up as one side's subnet to establish IPsec VPN tunnels for accessing a device in the other side's subnet or as a device in one's side subnet to establish IPsec VPN tunnels for accessing another device in the other side's subnet.
Figure 2.2635 illustrates an example of the subnet-to-subnet connection with a network application. A host inside the remote subnet can also connect to a local subnet (host-network application) based on

this subnet-to-subnet connection as shown in Figure 2.. On the other hand, two different devices on two different subnets (host-host application) can be connected via a IPsec VPN tunnel based on this subnet-to-subnet connection as shown in Figure 2.37. Note that all subnet-to-subnet configurations must set the connection type to **Tunnel mode** only.

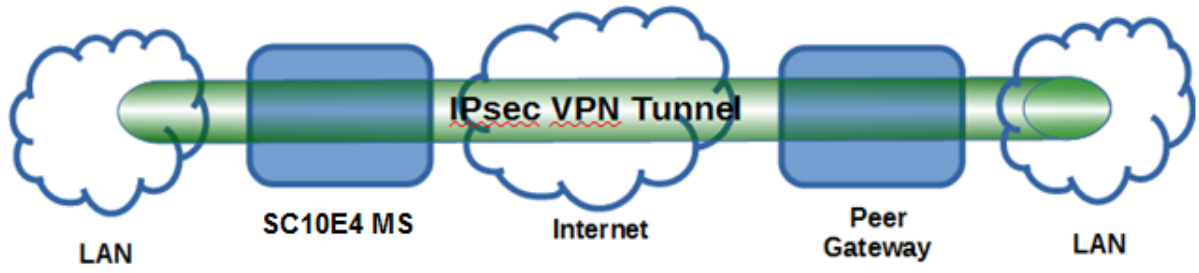


Figure 2.26 Example of network application using subnet-2-subnet connection via SC10E4 MS and a peer device

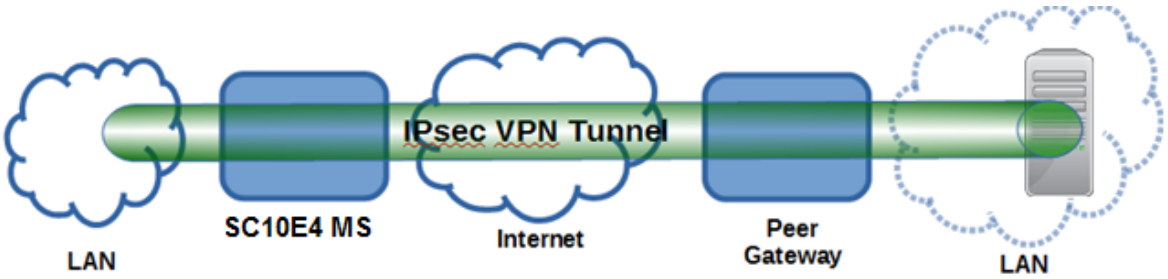


Figure 2.36 An example of host-network application via the subnet-to-subnet connection

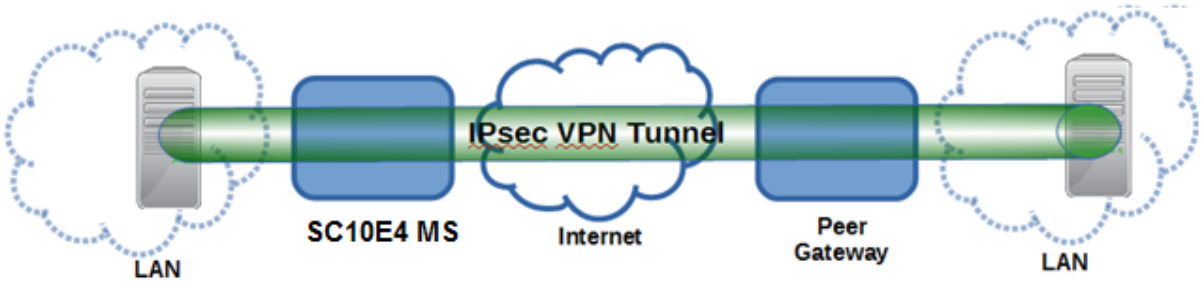


Figure 2.37 An example of host-host application via the subnet-to-subnet connection

In some network configuration, there is an implementation of network address translation (NAT) on its gateway/routers. NAT is typically used to allow private IP addresses on private networks behind gateways/routers with a single public IP address connecting to the public Internet. The internal network devices can communication with hosts on the external network by changing the source address of outgoing requests to that of the NAT device (gateway/router) and relaying replies back to the originating device. IPsec virtual private network (VPN) clients use network address translation (NAT) traversal in order to have Encapsulating Security Payload (ESP) packets traverse NAT. IPsec uses several

protocols in its operation, which must be enabled to traverse firewalls and network address translators (NATs), such as

- Internet Key Exchange (IKE) protocol uses User Datagram Protocol (UDP) port number 500.
- Encapsulating Security Payload (ESP) uses IP protocol number 50.
- Authentication Header (AH) uses IP protocol number 51.
- IPsec NAT traversal uses UDP port number 4500 when NAT traversal is in use.

SC10E4 MS also has a feature called NAT traversal (NAT-T) that allows the IPsec tunnel to pass through the NAT in its network. SC10E4 MS will activate this option automatically and encapsulate the IPsec packets inside UDP port 4500 to be able to pass through a NAT router.

To provide security service for all types of tunnel connections and applications described above, SC10E4 MS utilizes the Internet Key Exchange (IKE) protocol to set up a security association (SA) in the IPsec protocol suite. Note that IKE builds upon the Oakley protocol and ISAKMP (Internet Security Association and Key Management Protocol). IKE uses X.509 certificates for authentication either pre-shared or distributed using DNS (preferably with DNSSEC). IKE also uses a Diffie-Hellman key (DH) key exchange to set up a shared session secret from which cryptographic keys are derived. The IPsec security associations (SA) is divided into two phases. In phase one, IKE creates an authenticated secure channel between SC10E4 MS and its peer device, which is called the IKE Security Association. The Diffie-Hellman (DH) key agreement is always performed in this phase to create a shared secret key or DH key. In phase two, IKE negotiates the IPsec security associations and generates the required key material for IPsec. This IPsec key which is a symmetrical key will be used for bulk data transfer inside the IPsec tunnel. A new Diffie-Hellman agreement can be done in phase two, or the keys can be derived from the phase one shared secret.

1.14.1 IPsec Settings

Figure 2.27 shows the IPsec Settings web page under the IPsec Settings menu. There are four sections on this page: General Settings, Authentication Settings, IKE Settings, and Dead Peer Detection Settings.

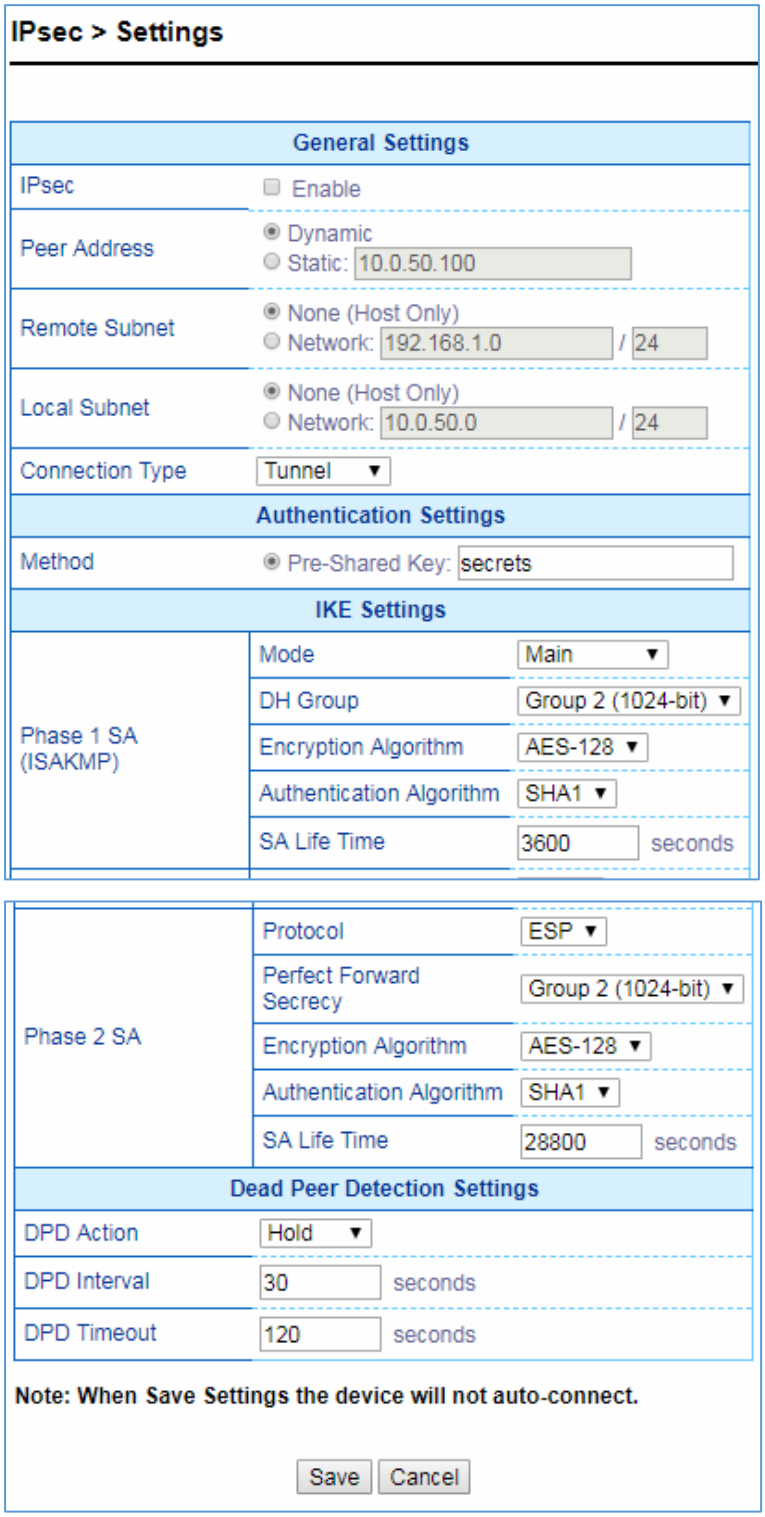


Figure 2.27 IPsec Tunnels Web Page under IPsec Setting Menu

San Telequip Private Limited.
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27273455, 9764027070, 8390069393
email : info@santelequip.com

To configure IPsec Settings, first you need to configure the General Settings section under the IPsec Settings menu. Under the General Settings, there are five parameters that need to be set as follows:

- **IPsec**: By checking the box for this option, you enable the IPsec feature for SC10E4 MS.
- **Peer Address:** This option is to specify the IP address of a remote host or peer host or remote gateway. There are two choices for the Peer Address which are Dynamic and Statics.
  - **Dynamic:** When you selected the Dynamic by choosing the Dynamic radio button, the Peer Address or the remote device IP address is not fixed or unknown. Note that when Peer Address is set to dynamic mode, the SC10E4 MS can accept remote connection request or will be the responder.
  - **Static:** On the other hand, if you know the IP address of the remote device, you can choose the ratio button for **Static** option and enter the IP address in the text box behind it. The SC10E4 MS will be the initiator/responder.
- **Remote Subnet:** This option is to indicate whether you want to create an IPsec connection to the remote subnetwork. There are also two choices for Remote Subnet access:
  - **None)Host only(:** This option is to specify that the remote subnet is not supported or no remote subnet and only host access is supported. That is the remote end of the IPsec tunnel is a host or peer device only.
  - **Network:** This option is to specify the Remote Subnet by entering the Subnet IP Address and the number of Subnet Masking Bits or associated routing prefix. This option supports the Classless Inter-Domain Routing (CIDR) notation. For example, Subnet IP Address is 192.168.11.0 and Subnet mask are 24 bits (from 255.255.255.0).
- **Local Subnet:** This option is to enable an IPsec connection to the local subnetwork. There are two choices for Local Subnet access:
  - **None (Host only):** This option is to specify that the local subnet is not supported or no local subnet and only local host access is supported. That is the local end of the IPsec tunnel is a host or peer device only.
  - **Network:** This option is to specify the Local Subnet by entering the Subnet IP Address and the number of Subnet Masking Bits or associated routing prefix. This option supports the Classless Inter-Domain Routing (CIDR) notation. For example, Subnet IP Address is 192.168.11.0 and Subnet mask are 24 bits (from 255.255.255.0).
- **Connection Type:** This option is to specify the IPsec connection type which can be either Tunnel mode or Transport mode. Please select the corresponding connection type from the drop-down list. Note that the Tunnel mode can be applied to the host-to-host, the host-to-subnet, and the subnet-to-subnet communications. The Transport mode can only be applied in the host-to-host communication.

The second part of IPsec Settings is the Authentication Settings. Here you have an authentication's Method which already selected as the Pre-Shared Key. Then, you must enter in a secret key or a pass-phrase in the textbox behind it. Both ends of the the VPN tunnel must use the same secret key or password. The pre-shared key can be 1 to 60 case-sensitive ASCII characters and special symbols.

The third part of IPsec Settings is the IKE (Internet Key Exchange) Settings. Internet Key Exchange (IKE) that SC10E4 MS supports is the IKE version 1 or IKEv1. Within the Phase 1 SA (ISAKMP), there are five security options to be configured. In phase 1, the two VPN gateway exchange information about the encryption algorithms that they support and then establish a temporary secure connection to exchange authentication information.

- First option is the Mode of IKE session which defines how many steps or packets will be used or exchanged during the IKE SA negotiation. You can choose either Main Mode or Aggressive Mode. The Main Mode will send SA proposals, Diffie-Hellman public key, and ISAKMP session authentication in three exchange packets, while the Aggressive Mode will put all SA proposals, DH public key, and ISAKMP session authentication in to one exchange packet. Aggressive Mode makes the IKE negotiation quicker than Main Mode. The difference between Main Mode and Aggressive Mode is that the "identity protection" is used in the Main Mode. The identity is transferred encrypted in the Main Mode but it is not encrypted in Aggressive Mode. Typically, the Main Mode is recommended.
- Second option is the selection of Diffie-Hellman's group (DH Group) of standardized global unique prime numbers and generators that will be used to provide secure asymmetric key exchange. The DH Group is used to encrypt this IKE communication. **SC10E4 MS** supports two DH groups which are DH Group 2, which is a 1024-bit modular exponentiation group (MODP), and DH Group 5, which is a 1536-bit MODP group.
- Third option is the selection of Encryption Algorithm which can be either AES-128 or 3DES. This option will select the key size and encryption algorithm to be used in the IKEv1 Phase 1. The default value is AES-128.
- Fourth option is the selection of Authentication Algorithm which can be either SHA1 or MD5. This option will select which hash algorithm will be used to authenticate packet data in the IKEv1 Phase 1. The default value is SHA1.
- Fifth option is the SA Life Time which must be set in unit of seconds. This value represents the lifetime of the IKE key which is dedicated at Phase 1 between both end host or network. The default SA Life Time is 10800 seconds. The configurable range for SA Life Time is between 300 to 86400 seconds.

Within the Phase 2 SA, there are five security options to be configured. Similar to Phase 1 SA, SC10E4 MS and its peer device will negotiate or exchange proposals to determine which security parameters will be used in this Phase 2 SA. A Phase 2 proposal also includes a security Protocol (first option), which you can choose either Encapsulating Security Payload (ESP) or Authentication Header (AH). The second option is the Perfect Forward Secrecy which is a property of key-agreement protocol to ensure that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. In Phase 2 SA, SC10E4 MS also supports two DH groups which are DH Group 2 (1024-bit) and DH Group 5 (1536-bit).

Then you can proceed to select encryption and authentication algorithms. Third option is the selection of Encryption Algorithm which can be either AES-128 or 3DES. This encryption algorithm will be used in the IPsec tunnel. The default setting is the AES128. Fourth option is the selection of Authentication Algorithm which can be either SHA1 or MD5. This is the hash algorithm that will be used to authenticate packet data in the IPsec tunnel. The default selection is the SHA1. Finally, the last option is the SA Life Time for phase 2 which must be set in unit of seconds. The range of this setting can be from 180 to 86400 seconds. The default SA Life Time is 3,600 seconds.

The final part of the IPsec Settings is the Dead Peer Detection Settings. Dead peer detection (DPD) is a mechanism that SC10E4 MS use to verify the existence of a remote Internet Key Exchange (IKE) gateway or the peer device of SC10E4 MS. To detect the peer device, SC10E4 MS will sent encrypted IKE Phase 1 notification payloads (or hello message) to its peer device and wait for DPD acknowledgement from the peer device. If SC10E4 MS does not receive an acknowledge message during a specific time interval (DPD timeout), it will consider that the peer device is dead. Then, SC10E4 MS will remove the Phase 1 Security Association and all Phase 2 Security Association of that dead peer device. Under the Dead Peer Detection Settings, you will have to choose the DPD Action that the SC10E4 MS will perform if it found that the peer device is dead. You can choose either Hold to still hold the security association for the peer device and wait for the peer device to return or Restart to restart the security association process again. The DPD Interval is the period of time for sending the hello message to the peer device or the interval that SC10E4 MS will repeatly check the endpoint with keep-

alive message. The DPD interval can be ranged from 1 to 65535 seconds. The default value for DPD Interval is 30 seconds. The DPD Timeout will be the time that SC10E4 MS declares the peer device dead if it did not receive any reply or traffic from the peer device. If the keep-alive check fails before this time period expires, the SC10E4 MS will take the PDP action. The DPD Timeout value range from 1 to 65535 seconds. The default value of DPD Timeout is 120 seconds. Description of each parameters in the IPsec Tunnels web page is summarized in Table 2.8

Table 2.8 Description of Parameters in IPsec Tunnels Web Page

Field Name		Description	Default Value
General Settings			
IPsec		Enable the IPsec Tunnel	Disable
NAT Traversal		Enable the NAT Traversal mechanism	Enable
Peer Address		IP address of the remote device which can be dynamic (any address) or static (fixed address)	Dynamic
Remote Subnet		Remote subnet can be either None (Host only) or Network (IP and Netmask)	None (Host Only)
Local Subnet		Local subnet can be either None (Host Only) or Network (IP and Netmask)	None (Host Only)
Connection type		Tunnel mode or Transport mode	Tunnel
Authentication Settings			
Method		Pre-Shared Key	secrets
IKE Settings			
Phase 1 SA	**Mode**	Choose how IKE negotiation is performed between Main Mode and Aggressive Mode	Main Mode
	DH Group	Diffie-Hellman groups, determine the strength of the key used in the key exchange process: DH Group 2 (1024-bit) or DH Group 5 (1536-bit)	Group 2 (1024-bit)
	Encryption Algorithm	Encryption algorithm used in the key exchange process: Either 3DES or AES	AES128
	Authentication Algorithm	Hash algorithm used to authenticate packet data in the key exchange process of IKEv1 phase 1: Either MD5 or SHA1	SHA1
	SA Life Time	How long a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiry. The value can be from 300 to 86,400 seconds.	3600
Phase 2 SA	**Protocol**	Choose how IP packet will be encrypted and verify: either Encapsulate Security Payload (ESP) or IP Authentication Header (AH)	ESP
	Perfect Forward Secrecy	Diffie-Hellman groups for Perfect Forward Secrecy of keys, determine the strength of the key used in the key exchange process: DH Group 2 (1024-bit) or DH Group 5 (1536-bit)	Group 2 (1024-bit)
	Encryption Algorithm	Select which key size and encryption algorithm will be used in IPsec tunnel: either 3DES or AES128	AES128
	Authentication Algorithm	Section of hash algorithm to be used to authenticate packet data in the IPsec tunnel: either MD5 or SHA1	SHA1
	SA Life Time	Value that represents the lifetime of the IKE key which is dedicated in Phase 2 between both end	28800

Field Name		Description	Default Value
		host or network. The available setting ranges is from 180 to 86,400 seconds.	
Dead Peer Detection Settings			
DPD Action		Select either Hold or Restart the tunnel's security association for the peer**.** Note that Hold is suitable for a statistically defined tunnel**.**	Hold
DPD Interval		Duration of time for sending hello message to the peer device: value from 1 to 65535 seconds.	30 seconds
DPD Timeout		Duration of time to declare that the peer is dead: value from 1 to 65535 seconds.	120 seconds

After finishing the **IPsec settings** configuration, please click the **Save** button to save all changes that have been made. If you would like to discard any setting, please click the **Cancel** button.

1.14.2 IPsec Status

On this web page, you can check the status of your IPsec connection between SC10E4 MS and its peer device in different connection types and modes. The first information is the Peer Address which is the IP address of the other device that is connected to SC10E4 MS. The second information is the VPN Tunnel's status. The third information is the Status of the IPsec connection which can be Disabled, Listening, or Connected. shows the IPsec Status web page under the IPsec Settings menu. There are three buttons at the end of the web page which are Connect, Disconnect, and Refresh. The Connect and Disconnect buttons allow you to establish or tear down the IPsec connection. The Refresh button enable you to check the latest status of the connection.

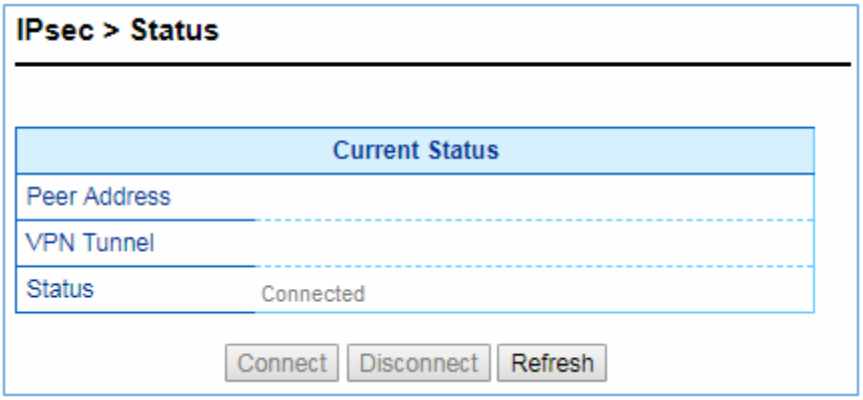


Figure 2.28 IPsec Status Web Page

1.14.3 Examples of IPsec Settings

The following subsections provide examples of IPsec settings. However, each example will be focused only on the General Settings part. The other parts of the IPsec Settings can be configured according to the user's preference. Please consult previous section on the details of Authentication Settings, IKE Settings, and Dead Peer Detection Settings. Note that the network-to-network (or subnet-to-subnet) connections are now supported in new firmware of SC10E4 MS.

1.14.4 Host-to-Host Connections

Two scenarios can be configured for host-to-host connections: with static peer and with dynamic peer. A host-to-host topology for both scenarios is illustrated in Figure 2.29. Please follow the steps provided next for each scenario to set the General Settings.

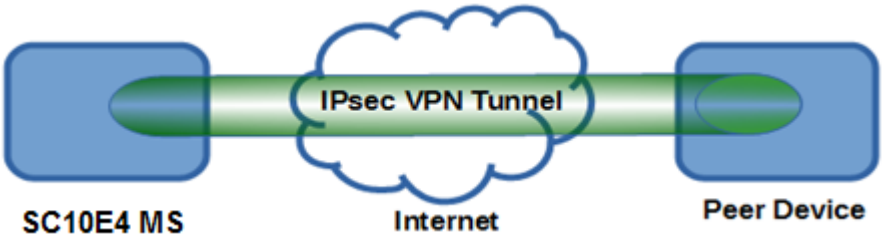


Figure 2.290 IPsec VPN Tunnel with Host-to-Host Topology

Scenario: host-to-host with static peer as shown in Figure 2.30

- Check the Enable box for IPsec.
- In the Peer Address field, select the Static option and enter the peer IPv4 address.
  Note: When peer address is entered as the static address, the SC10E4 MS acts as an initiator which takes the initiative and establishes a connection. SC10E4 MS also acts as a responder and passively accepts the connection initiated by the remote gateway.
- Select the radio button for None (Host Only) in the Remote Subnet field.
- Since this VPN connection is established on two hosts, the Connection Type option can be either Transport or Tunnel.

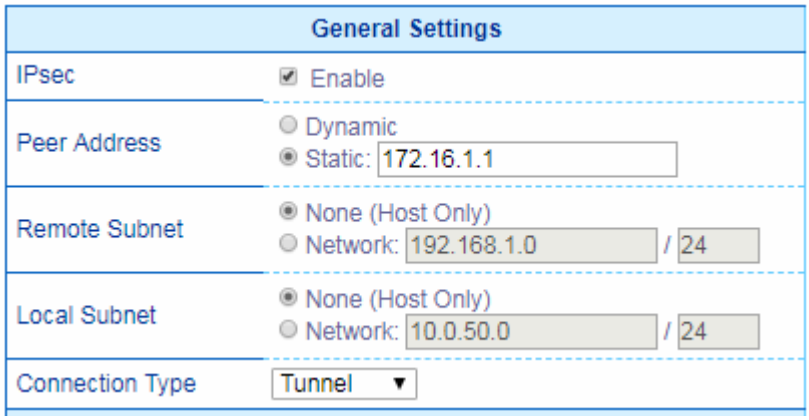


Figure 2.30 General Settings for Host-to-Host with Static Peer

Scenario: host-to-host with dynamic peer as shown in Figure 2.31

- Check the Enable box for IPsec.
- In the Peer Address field, select the Dynamic option.
  Note: When VPN connects to a peer with dynamic IP address, the SC10E4 MS acts as a responder and passively accepts the connection initiated by the remote gateway.
- The remaining settings are the same as the host-to-host with static peer scenario described above.

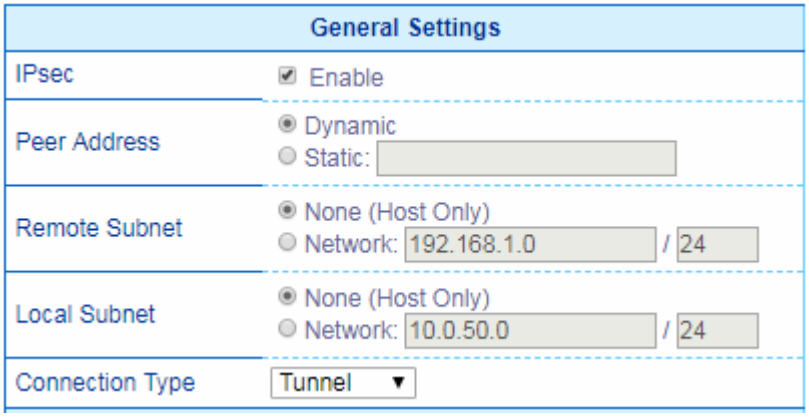


Figure 2.31 General Settings for Host-to-Host with Dynamic Peer

1.14.5 Host-to-Network Connections

Two scenarios can also be configured for host-to-network (or host-to-subnet or host-to-site) connections: with static peer and with dynamic peer. Note that the SC10E4 MS is the host in these scenarios. A host-to-network topology for both scenarios is illustrated in Figure 2.32. Please follow the steps provided next for each scenario to set the **General Settings**.

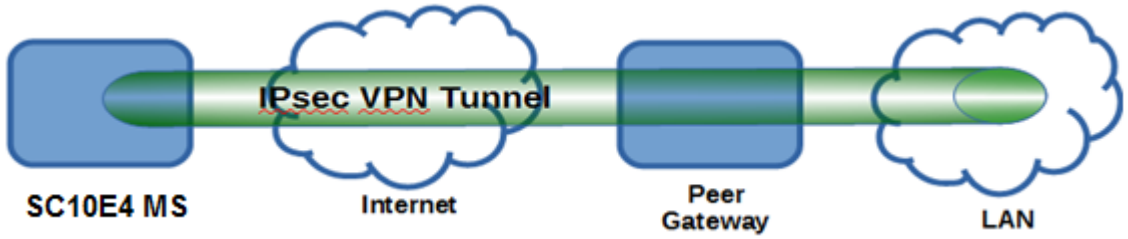


Figure 2.32 IPsec VPN Tunnel with Host-to-Network Topology

Scenario: host-to-network with static peer as shown in Figure 2.44

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
  Note: When peer address is entered as a static address, SC10E4 MS is an **initiator** which takes the initiative and establish a connection, or can be a **responder** waiting for connection. SC10E4 MS also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in "address prefix length" or behind the "*/*" symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.

General Settings	
IPsec	☑ Enable
Peer Address	○ Dynamic ◉ Static: 172.16.1.1
Remote Subnet	○ None (Host Only) ◉ Network: 192.168.1.0 / 24
Local Subnet	◉ None (Host Only) ○ Network: 10.0.50.0 / 24
Connection Type	Tunnel ▼

Figure 2.44 General Settings for Host-to-Network with Static Peer

Scenario: host-to-network with dynamic peer as shown in Figure 2.3345

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
  Note: When VPN connection is set to a peer with dynamic IP address, SC10E4 MS will act as a **responder** and will passively accept the connection initiated by the remote gateway.

- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “/” symbol.
- Because this IPsec VPN connection has a subnet at one end, the **Connection Type** option must be set to **Tunnel** only.

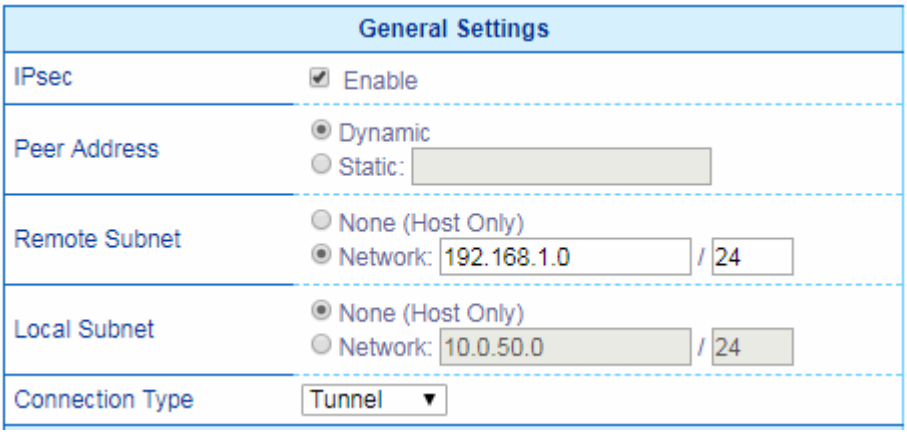


Figure 2.33 General Settings for Host-to-Network with Dynamic Peer

1.14.6 Network-to-Network (Subnet-to-Subnet) Connections

Two scenarios can also be configured for network-to-network (or subnet-to-subnet) connections: with static peer or with dynamic peer. A VPN tunnel will be created between two separate private sub-networks. Note that the SC10E4 MS is the gateway to a local network in these scenarios. A network-to-network topology for both scenarios is illustrated in 6. Please follow the steps provided next for each scenario to set the **General Settings**.

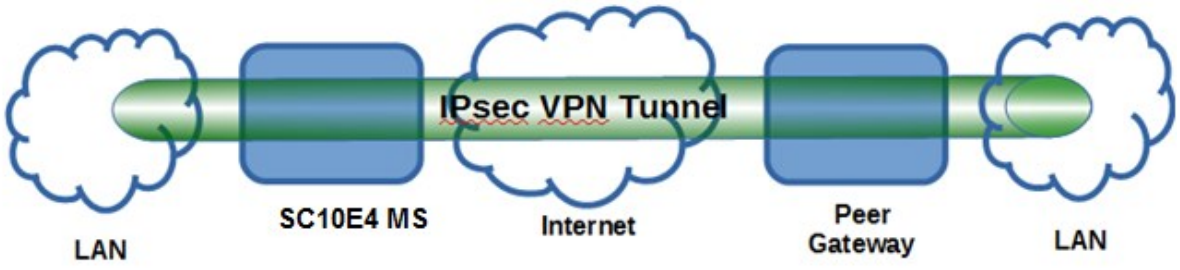


Figure 2.46 IPsec VPN Tunnel with Network-to-Network Topology

Scenario: network-to-network with static peer as shown in Figure 2.

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Static** option and enter the peer IPv4 address.
  Note: When peer address is entered as a static address, SC10E4 MS is an **initiator**, which takes the initiative and establish a connection, or can be a **responder** waiting for connection. SC10E4 MS also acts as a **responder** and passively accepts the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “*/*” symbol.
- Set the network IPv4 address in the **Local Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “*/*” symbol.

- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.

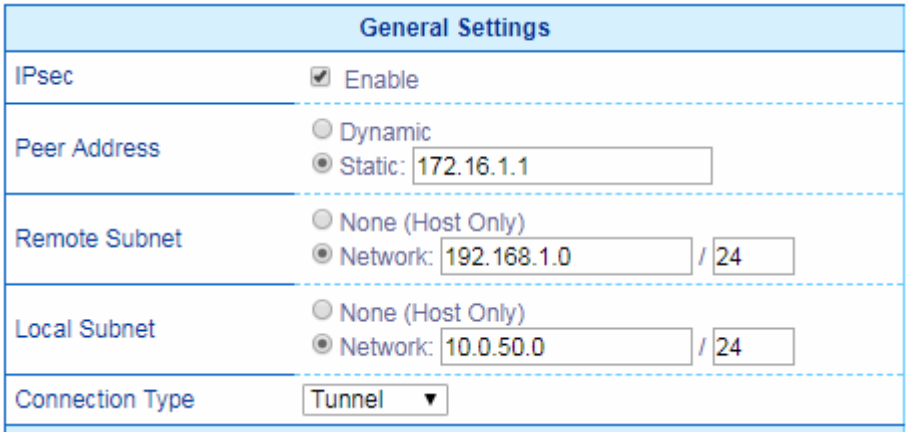


Figure 2.47 General Settings for Network-to-Network with Static Peer

Scenario: network-to-network with dynamic peer as shown in Figure 2.8

- Check the **Enable** box for **IPsec**.
- In the **Peer Address** field, select the **Dynamic** option.
  Note: When VPN connection is set to a peer with dynamic IP address, SC10E4 MS will act as a **responder** and will passively accept the connection initiated by the remote gateway.
- Set the network IPv4 address in the **Remote Subnet** with the number of bits for subnet mask in “address prefix length” or behind the “*/*” symbol.
- Set the network IPv4 address in the **Local Subnet** with the number of bits for sub netmask in “address prefix length” or behind the “*/*” symbol.
- Because this IPsec VPN connection has subnets at both ends, the **Connection Type** option must be set to **Tunnel** only.

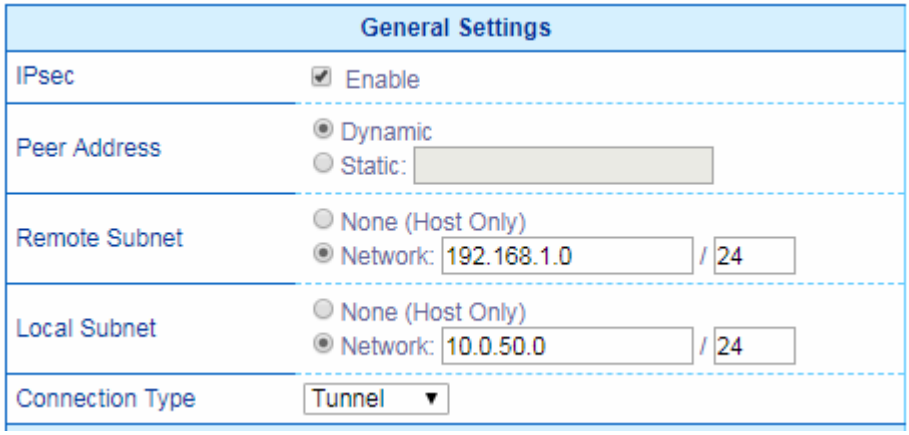


Figure 2.48 General Settings for Network-to-Network with Dynamic Peer

1.15 System

1.15.1 Log Settings

This section allows the user to change the way to report the Log. The user can save his Log Event to the flash memory of the Modbus Gateway by checking the Enable Log Event to Flash box. To specify the contents of the Log, select different Log Level by changing the pull-down menu of the Log Level. There are two log levels available on the menu: Level 3**: (**LOG_ERR**)** and Level 4**: (**LOG_WARNING**)**. Figure 2. shows a selection of Log Level 4 which will keep LOG_WARNING.

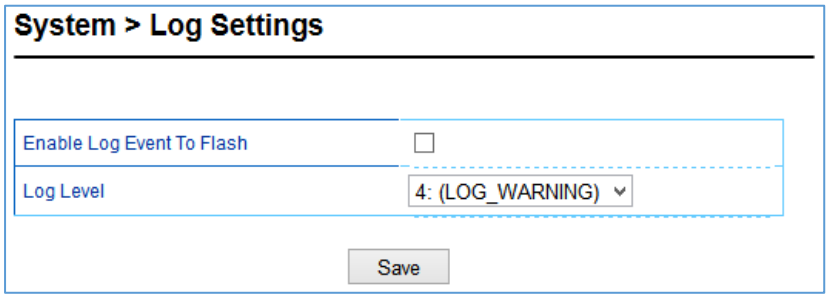


Figure 2.49 Log Settings Web Page

1.15.2 System Log

This section lists current system events aside its properties (Date, Time, Startup Time, Level, and Event). Figure 2.34 shows an empty System Log page. The user can navigate through the system log by using Last Page or Next Page buttons. The user will have the option to show all events by clicking the Show All Event button and the option to clear them all by clicking on Clear All Event button.

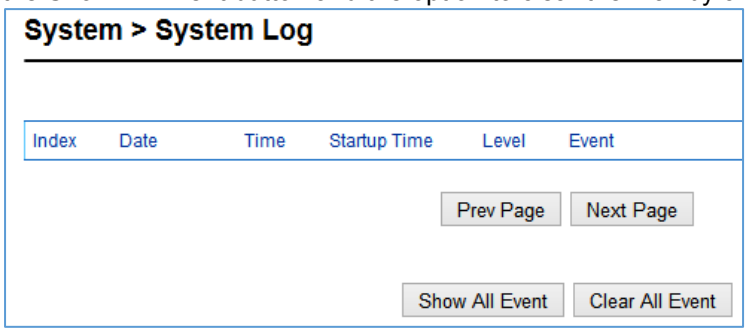


Figure 2.34 System Log Web Page

1.15.3 Data Log

The log of Modbus's exchanged messages will be shown in the **Data Log** section and listed in Figure 2.351. This can be very useful for debugging and testing. The user can filter the data based on the **Interface** by using the drop-down box. All available interface will be listed in the box such as COM1, COM2, COM3, COM4, and TCP_Link*XX*. Then click on the **Query** button to list the data log based on the chosen interface. Traffic analysis in the system can be done here as well. Click the **Start** button to enable continuous data log collection or click **Stop** to end it. All data log can be cleared by clicking the **Clear** button. The user will be able to browse through the list of message by clicking on the **Last Page** or the **Next Page** buttons at the bottom of the log table. Finally, if the user would like to save the data log to a file on the local PC, please click on the **Export** button.

Figure 2.35 Data Log Web Page

1.15.4 Modbus Statistic

Modbus's interface statistics are reported in this section as shown in Figure 2.36. For each interface, there is a **Net_Connection** or socket which is an IP address bundled with its port number (only for TCP and VCOM interfaces), a **DataType** of the interface (**ASCII**, **RTU**, or **TCP**), a **Mode** of the Interface (either **MASTER** or **SLAVE**), the count of received messages (**RxCnt**), the received bytes (**RxByte**), the count of transmitted message (**TxCnt**), and the transmitted bytes (**TxByte**). Click on the **Refresh** button to obtain the latest statistics of the Modbus's interfaces.

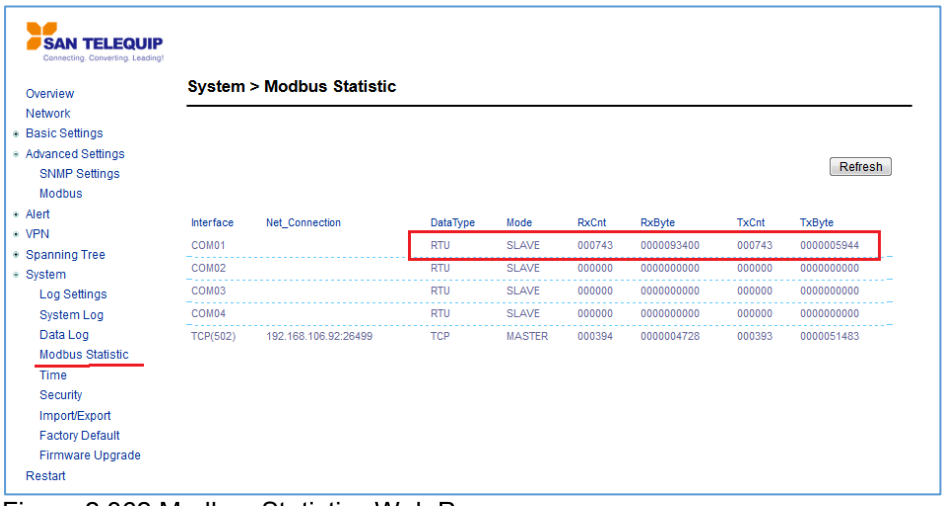


Figure 2.362 Modbus Statistics Web Page

1.15.5 Time

Date and time can be set manually or through **N**etwork **T**ime **P**rotocol (NTP) to automatically synchronize date and time of the Modbus Gateway with a **Time Server.** Figure 2.3 shows the **Time** setting page. The user can obtain the **Current System Time** by clicking on the **Refresh** button. Under the **System Time Setting** box, the user can set the **Time Zone** by selecting the proper time zone from the pull-down menu. Then, in order to choose the options of time setting, select either **NTP** or **Manual**. For auto-synchronization, check the radio button in front of **NTP** option. Then, proceed to fill in the IP address or hostname of the preferred time server such as time.nist.gov which is the default setting. If a hostname is entered, the DNS server should be configured properly following the procedure explained in Section o. Other options will be disabled if the **NTP** option is selected.

If the **Manual** option is selected, select the current **Date (Year, Month, Day)** and **Time (Hour, Minute, and Second)** from their corresponding pull-down menus under the **Manual Setting** box. In certain

region, the daylight time saving is practiced. In order to enable it, check the **Enable Daylight Saving Time** checkbox and specify the **Start Date**, **End Date**, and **Offset** in the fields under **Daylight Save Setting** box as shown in the greyed out area of Figure 2.3.

After Time Setting is complete, click **Save Configuration** to save all changes that have been done. A **Save Successful** message will show up with a hyperlink to **restart** the device as shown in **Error! R eference source not found.** Click the **restart** hyperlink to apply the changes**.** Then, a message indicating **System Restarting** status with a counting down number will show up as shown in Figure 2**..** After a successful device's restart, the web browser will be redirected to the Overview page as shown in Figure 2**..**

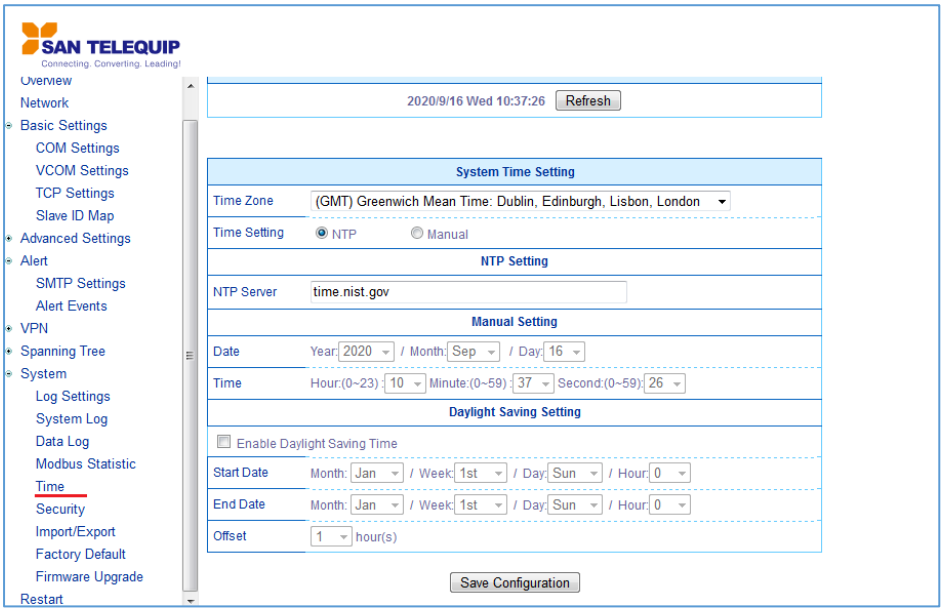


Figure 2.53 Time Web Page

1.15.6 Security

The default security setting for the password is a standard password (default). To change security, enter the Security web page as shown in Figure 2., enter a password in the **Change Password** box. The user should enter the **Old Password** (enter nothing in case of a null password), the **New Password**, and the **Verified Password** (same as the New Password). The password is case sensitive and limited to a maximum of 8 characters. After entering all required fields, click **Save Password** button to save the change. After the **Save Successfully** message showed up, the user will be prompted with a pop-up window to enter the **User name** and the **New Password** again for verification, as shown in Figure 2..

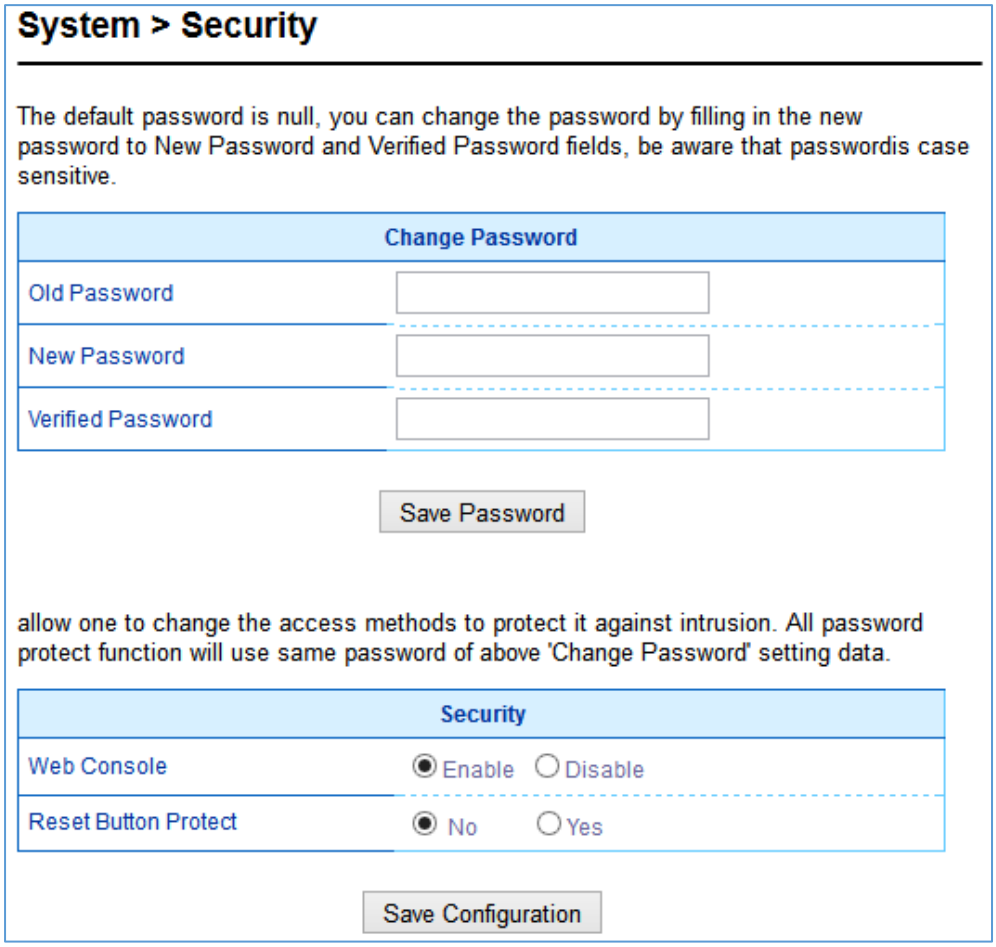


Figure 2.54 Security Web Page

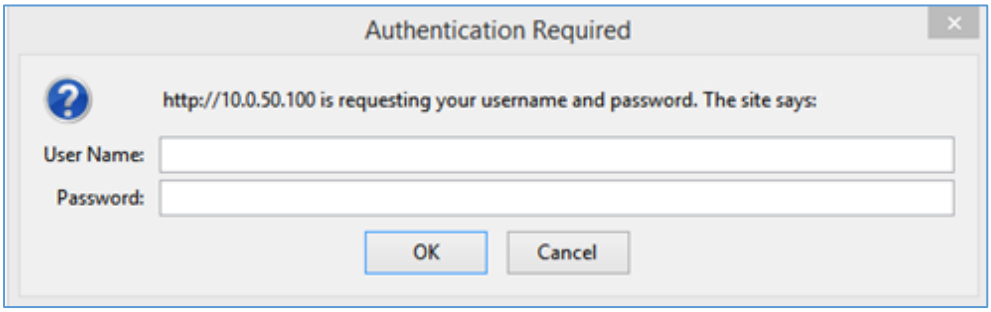


Figure 2.55 Authentication Required after a Password Change

The user can limit how the Modbus Gateway is accessed and controlled by changing the settings under the **Security** . All password-protected features will use the same password whose setting is described in the previous paragraph. The user can enable or disable **Web Console** by clicking on the corresponding radio button. Additionally, the user can protect how the user accesses the device with a **Reset Button Protect** option by checking on either **No** or **Yes** radio buttons.

After Security Settings are set, click **Save Configuration** to save all changes that have been made. A **Save Successful** message will appear with a hyperlink asking to **restart.** Please click the **restart**

hyperlink to apply the changes**.** Then, a message indicating **System Restarting** status with a countdown will show up**.** After a successful restart, the web browser will be redirected to the Overview page.

1.15.7 Import/Export

Once all configurations are set and the device is working properly, the user may want to backup **(Export)** the configuration to a file. A backup configuration file can be used when a new firmware is uploaded and the device is reset to a factory default settings, or simply to prevent accidental loading of incompatible old settings. The backup file could also be used to efficiently deploy multiple Modbus Gateways of similar settings by restoring the settings to the devices by **importing** the corresponding file. Figure 2.56 depicts the Import/Export web page.

Figure 2.56 Import/Export Web Page

To import a configuration file from the computer, click on the **Browse…** button. Then, a pop-up window will ask the user to choose a configuration file (with .DAT extension). After selection, click **Open button** Then, click on the **Import Configuration** button to start the importing process.

After importing is complete, the system will show a **Save Successful** message with a hyperlink to **restart** the device**.** Click the **restart** hyperlink to apply the changes**.** Then, a message indicating **System Restarting** status with a countdown will show up**.** After a successful device's restart, the web browser will be redirected to the Overview page.

In order to export the current configuration of the Modbus Gateway to a file for backup purposes, click the **Export Configuration** button as shown in Figure 2.56. Then, a pop-up window will ask to either **Open** the configuration file for viewing with a default application such as Notepad or to simply **Save** the configuration file to the preferred name and destination path.

1.15.8 Factory Default

A return to **Factory Default** function is available in SC10E4 MS Series. To restore all parameters of the Modbus Gateway to the original factory default setting, click **Set to Default and Restart** button as shown in Figure 2.37. After a short moment, a message indicating **System Restarting** status with a countdown number will show up**.** After a successful device's restart, the web browser will be redirected to the Overview page.

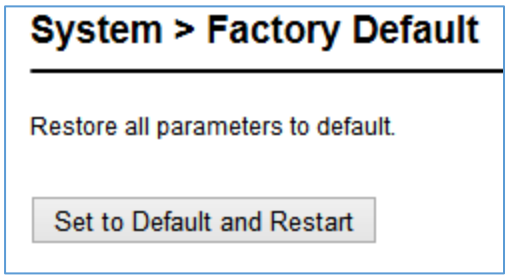


Figure 2.37 Factory Default Web Page

1.16 Restart

For some unexpected circumstances, the Modbus Gateway system may stop responding correctly**.** The user has the option to restart the device by clicking the **Restart** button The device's RUN LED will start blinking when the restart process is completed. Then, a message indicating **System Restarting** status with a countdown will show up**.** After a successful device**'**s restart, the web browser will be redirected to the Overview page.

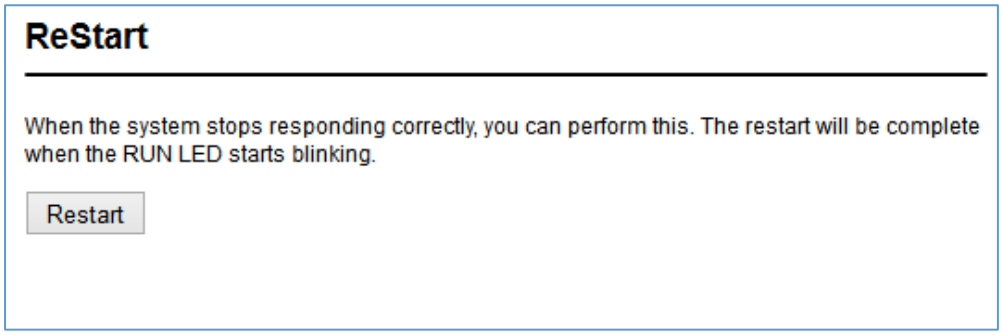


Figure 2.58 Restart Web Page

2 Applications and Examples

On the device two different Slave ID mapping definitions are available, which represent the alias mode and the offset mode. Both Modbus ID definitions can be used to route the request command (from the Master) to the Slave node. Please see details of Slave ID setting mode in Section 1.8.6.

2.1 Using ID offset range mapping

SC10E Slave ID is continuous as shown in Figure 2.1, it is recommended to use the Offset mode in your configuration setting of ID mapping as shown in Figure 2.2.

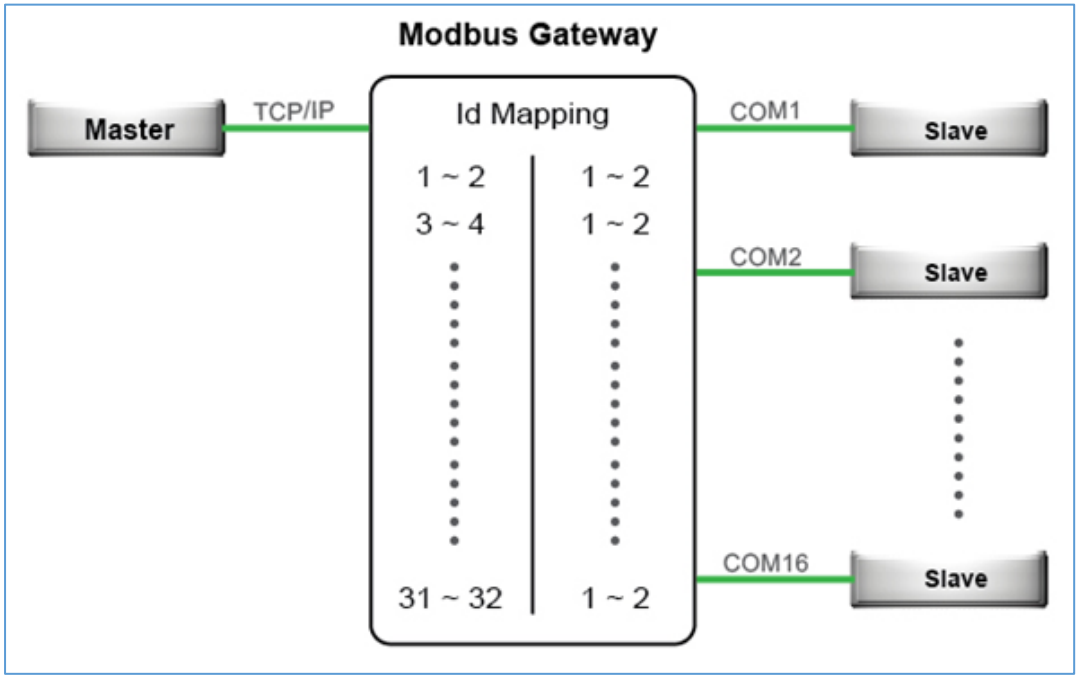
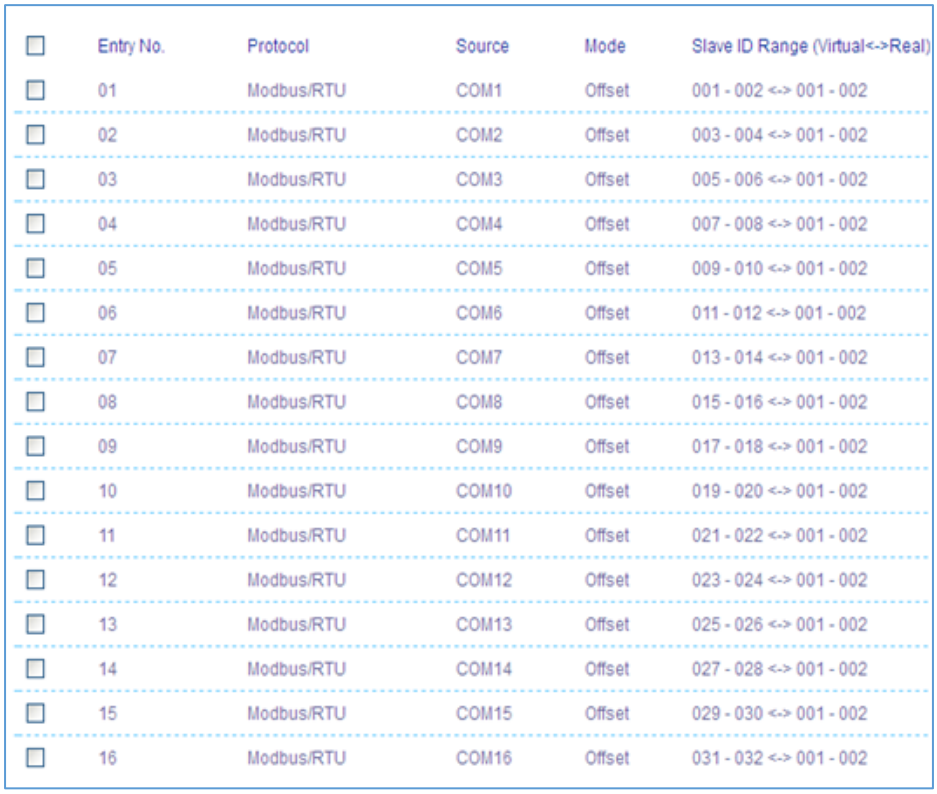


Figure 2.1 Continuous Slave ID Mapping Example



	Entry No.	Protocol	Source	Mode	Slave ID Range (Virtual<->Real)
☐	01	Modbus/RTU	COM1	Offset	001 - 002 <-> 001 - 002
☐	02	Modbus/RTU	COM2	Offset	003 - 004 <-> 001 - 002
☐	03	Modbus/RTU	COM3	Offset	005 - 006 <-> 001 - 002
☐	04	Modbus/RTU	COM4	Offset	007 - 008 <-> 001 - 002
☐	05	Modbus/RTU	COM5	Offset	009 - 010 <-> 001 - 002
☐	06	Modbus/RTU	COM6	Offset	011 - 012 <-> 001 - 002
☐	07	Modbus/RTU	COM7	Offset	013 - 014 <-> 001 - 002
☐	08	Modbus/RTU	COM8	Offset	015 - 016 <-> 001 - 002
☐	09	Modbus/RTU	COM9	Offset	017 - 018 <-> 001 - 002
☐	10	Modbus/RTU	COM10	Offset	019 - 020 <-> 001 - 002
☐	11	Modbus/RTU	COM11	Offset	021 - 022 <-> 001 - 002
☐	12	Modbus/RTU	COM12	Offset	023 - 024 <-> 001 - 002
☐	13	Modbus/RTU	COM13	Offset	025 - 026 <-> 001 - 002
☐	14	Modbus/RTU	COM14	Offset	027 - 028 <-> 001 - 002
☐	15	Modbus/RTU	COM15	Offset	029 - 030 <-> 001 - 002
☐	16	Modbus/RTU	COM16	Offset	031 - 032 <-> 001 - 002

Figure 2.2 Entries of Slave ID Mapping in Offset Mode

San Telequip Private Limited.
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27273455, 9764027070, 8390069393
email : info@santelequip.com

3 Specifications

3.1 Hardware

Table 3.1 Hardware Specification

System			
CPU	32-bit ARM Based TI CPU AM3354 800MHz		
Flash Memory	32MB		
RAM	DDR3 256MB		
EEPROM	8 KB		
Reset	Built-in Recessed Key (Restore to Factory Defaults)		
Watchdog	Hardware built-in		
Network			
Ethernet Interface	IEEE 802.3 10BaseT IEEE 802.3u 100BaseT(X)		
Protocol	ICMP TCP UDP IPv4 HTTP Syslog	DNS DHCP Client SNMPv1,v2c,v3 Modbus TCP/ASCII/RTU	SMTP NTP ARP Telnet RFC2217
Serial			
Serial Interface	RS-232/RS-422/RS-485 Software Selectable (Default: RS-232)		
Serial Connector	4 Serial Ports (TB-5 or DB-9)		
Serial Port Communication	Baud-rate: 1200 bps ~ 921600 bps Parity: None, Even, Odd, Mark, or Space Data Bits: 5, 6, 7, 8 Stop Bits: 1, 2 Software Selectable Flow Control: RTS/CTS (RS-232 only), XON/XOFF, None		
LED Indicator			
LED indication	P1,P2 RUN,ALM,COM1 - 4		
Power Requirement & EMC			
Input	Redundant 9~48 VDC		
Mechanical			
Dimensions (W x H x D, mm)	55 mm x 145 mm x 113mm (2.17 x 5.17 x 4.45 in)		
Enclosure	IP30 protection, metal housing		
Environmental			
Temperature	-40°C ~ 85°C (-40°F ~ 185°F)		
	Storage -40°C ~ 85°C (-40°F ~ 185°F)		
Humidity	5% ~ 95%, 55°C Non-condensing		

3.2 Serial port Pin Assignments

3.2.1 Pin Assignments

DB9 to RS-232/RS-485/RS-422 connectors

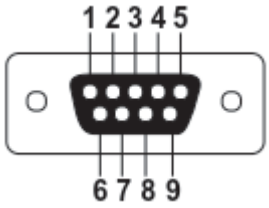


Figure 3.1 DB9 Pin Number

Table 3.2 Pin Assignment for DB9 to RS-232/RS422/RS-485 Connectors

Pin#	RS-232 Full Duplex	RS-422 Full Duplex	RS-485 Half Duplex
1	DCD	N/A	N/A
2	RxD	TxD+	Data+
3	TxD	RxD+	N/A
4	DTR	N/A	N/A
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)
6	DSR	N/A	N/A
7	RTS	RxD-	N/A
8	CTS	TxD-	Data-
9	RI	N/A	N/A

5-Pin Terminal Block to RS-485/RS-422 connectors

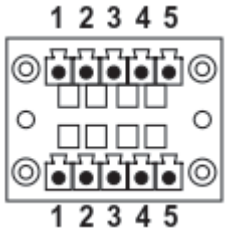


Figure 3.2 Terminal Block (TB-5) Pin Number

Table 3.3 Pin Assignment for 5-Pin Terminal Block to RS-232/RS-422/RS-485 Connectors

Pin#	RS-232	RS485-4 Wire	RS485- 2Wire
1	RxD	TxD+	Data+
2	CTS	TxD-	Data-
3	TxD	RxD+	N/A
4	RTS	RxD-	N/A
5	SG (Signal Ground)	SG (Signal Ground)	SG (Signal Ground)

3.3 LED Indicators

Table 3.4 Color Interpretation of LED Indicators

Name	Color	Message
PWR (Power)	(Steady Green)	Power ON
RUN (Ready)	(Steady On/Off Green)	System is not ready or halt
	(Blinking Green)	AP firmware is running normally
ALM (Alarm)	(Steady Red)	Alarm is triggered by user defined events
	(Light Off)	Alarm is not triggered by user defined events
COM	(Blinking Green)	COM port is transmitting data
	(Light Off)	COM port is not transmitting data
LAN	(Steady Amber)	Data is transmitting at 10Mbps
	(Light Off Green)	Ethernet is disconnected
	(Blinking Green)	Data is transmitting at 100Mbps