SYNC
Software User Manual
Field Level: SYNC1000, 2000, 3000

Version 1.0.0
December 2010

Kalki Communication Technologies Limited

SYNC

Software User Manual

Field Level: SYNC1000, 2000, 3000

Version 1.0.0

December 2010

Kalki Communication Technologies Limited
Anantha Pushpa Building,#147, 5th Main road,HSR lay Out 7th sector,
Bangalore 560 102, India.
Ph: 91 80 40527900
Web Site: www.kalkitech.com

Disclaimer

Note

'KSGL' model names are changed to 'SYNC' from revision 2.16.0 of GPC, (protocol conversion engine). The details of old model name and corresponding change are listed in table under Appendix-C

Document Release Note

The details of the document is given as follows.

Document Release Number	1.0.0
Document Release Date	30 January,2010

Table 1: Document Details

Created By	Tomy
Modified By	First Version
Reviewed By	Midhin, Victoria
Version Number	1.0.0
Project Name	SYNC Software UserManual Field Level: SYNC1000,2000,3000

Table 2: Document Authoring Details

About the Document

Purpose

This manual serves as a guide for using Kalkitech SYNC protocol gateway models including SYNC2000-S6R1, SYNC3000-S4R2, SYNC3000-S12R6, SYNC3000-S8R2, SYNC3000-S16R2, SYNC3000-S16R4,SYNC3000-S16R4I and SYNC3000-S16F2. This manual describes the configuration details of SYNC models and installation of the configuration tool Easy Connect. It contains information on using all aspects of the software support features including redundancy, NERC-CIP and VPN.

Please note that separate user manuals are available for each protocol, which explains the detailed configuration and mapping.

Intended Audience

This user manual is intended for the Kalkitech SYNC protocol gateway users:

- Introduces you to SYNC and EasyConnect
- Familiarizes you with the user interface
- Gives you step-by-step instructions to install and get started with SYNC and EasyConnect
- Gives you step-by-step instructions to configure and map protocols present inside SYNC and EasyConnect

Organization of the Document

This document is organized in to three parts as follows:

Chapter	Chapter Name	Description
Chapter 1	SYNC Field1000,2000,3000	The chapter provides an introduction to the SYNC.
Chapter 2	Getting Started	This chapter provides instructions on getting started with the SYNC.
Chapter 3	Configuring Gateways	This chapter gives you information and instructions for configuring the SYNC Gateways
Chapter 4	Downloading Configuration File	This chapter gives you information and instructions for configuring the master stations
Appendix A to C	Appendix A to C	This section provides references and other information.

Table 3: Organization of the document

Documentation Conventions

The following table shows the conventions used in the document:

Sl. No	Item	Conventions Used
1	Field Name, Screen Name and Button	Arial, Bold face font
2	Note	**Note:**
3	Each step in the task is numbered	Identified by numbered list 1. **First Step** 2. **Second Step**

Table 4: Document Conventions

List of Abbreviations

The following table shows the acronyms/abbreviations used in this document:

Acronyms/Abbreviations	Description
CHAP	Challenge-Handshake Authentication Protocol
DCCP	Diagnostic and Converter Configuration Protocol
DPI	Dots Per Inch
EDGE	Enhanced Data rates for Global Evolution
GPC	Generic Protocol Conversion
GPRS	General Packet Radio Service
HSB	Hot-Standby
IP	Internet Protocol
KSGL	Kalki Substation Gateway Lite
PPP	Point to Point Protocol
RAM	Random Access Memory
UDP	User Datagram Protocol
VPN	Virtual Private Network
XML	Extensible Markup Language

Table 5: List of abbreviations

Table of Contents

List of Figures

List of Tables

1 SYNC Field Level: 1000,2000,3000

This document gives a comprehensive information on our SYNC field level products pertaining to the software installation and its configuration. Please note for hardware installation and mounting, please refer to the Hardware Installation Guide file found in the CD.

1.1 Overview of SYNC

Kalkitech SYNC is the family Hardware protocol-in-a-box solutions that provide any-to-any protocol conversions delivered as a single software solution. SYNC products are available in a range of substation-hardened hardware configurations to suit every requirement from a simple 1 modem-channel and limited I/O to a 16-channel multi-protocol data concentrator/converter. The different product models vary in processing power, storage capabilities, number of channels and types of channels to suit different requirements. However they present a singular front end via the SYNC Configuration tool Easy Connect.

1.2 Easyconnect

The complete configuration of SYNC is done through a configuration utility software called EasyConnect, which includes defining protocol attributes, mapping data and achieving the functionalities like firmware updating, IP setting, diagnostics etc. EasyConnect generates a configuration file in Extensible Markup Language (XML) format as the output. You can download the configuration file using the download function in EasyConnect for configuring the hardware gateway.

EasyConnect can be used for:

- Any communication with the SYNC
- Update firmware
- Upload or download configuration file
- Reset the SYNC
- Configure and map the protocols supported on the SYNC
- Manage different profiles in your hard disk for different conversions when using SYNC. The configuration is simple to carry it out on your own
- Supports packet diagnostics of the various channels

1.3 Environment

This section specifies the software and hardware requirements to install and use EasyConnect configuration utility.

1.3.1 Software Requirements

The software requirements are stated as follows:

Requirement	Description
EasyConnect	The protocol configuration utility
Operating System	Windows 98 (Required) or Higher

Table 6: Software Requirements

1.3.2 Hardware Requirements

The hardware requirements are stated as follows

Requirement	Description
RAM	128 MB or more
HardDisk Space	1.5 GB or more
DPI Setting	96 DPI

Table 7: Hardware Requirements

2 Getting Started

This sections familiarizes you with SYNC and EasyConnect and gives step-by-step instructions to get started with the SYNC and EasyConnect. This section covers the following topics:

- Installing EasyConnect
- Removing EasyConnect
- Starting EasyConnect
- Exiting EasyConnect
- Using the EasyConnect interface

2.1 Installing EasyConnect

EasyConnect uses Microsoft XML engine to manage XML files. You have to install Microsoft XML engine before installing EasyConnect. You can get the EasyConnect installable files from:

- CD supplied along with the SYNC gateway
- Download from the Website – please contact sales@kalkitech.com for the link to download the file

Note: Follow default options for installing EasyConnect

Prerequisites

You have to obtain EasyConnect before you can install it. Please contact support@kalkitech.com for any further information.

To install EasyConnect perform the following steps:

1. Double-click the **EasyConnect** icon.
   The **Welcome window** appears.
2. Click **Next**.
   The **Choose Destination Location** window appears.
3. Click **Next**.
   The **Setup Complete** window appears.

2.2 Removing EasyConnect

You can remove all the installed contents of EasyConnect from your system

To remove EasyConnect perform the following steps:

1. From **Start** menu, choose **Settings,** the corresponding window will get displayed. Choose **Control Panel** from the window, the **Control Panel** window get displayed. Select **Add** or **Remove** program.
2. From the program list in the **Add or Remove Programs** window, choose **EasyConnect**.
3. Click **Change/Remove.**
   The **Confirm File Deletion** window appears.
4. On the **Confirm File Deletion** window, click **Yes**.
   The uninstall shield wizard removes all components from your system.
5. On the uninstall shield wizard, Click **OK**.

2.3 Starting EasyConnect

EasyConnect helps you to configure files. You have to download the configured file to the SYNC before running it. To access EasyConnect, as a first step, you have to start the EasyConnect.

To start EasyConnect perform the following steps:

1. From **Start** menu, choose **Programs,** the corresponding window will get displayed. Choose **Kalkitech,** the corresponding window will get displayed, Choose **EasyConnect**.

   The **EasyConnect** user interface appears

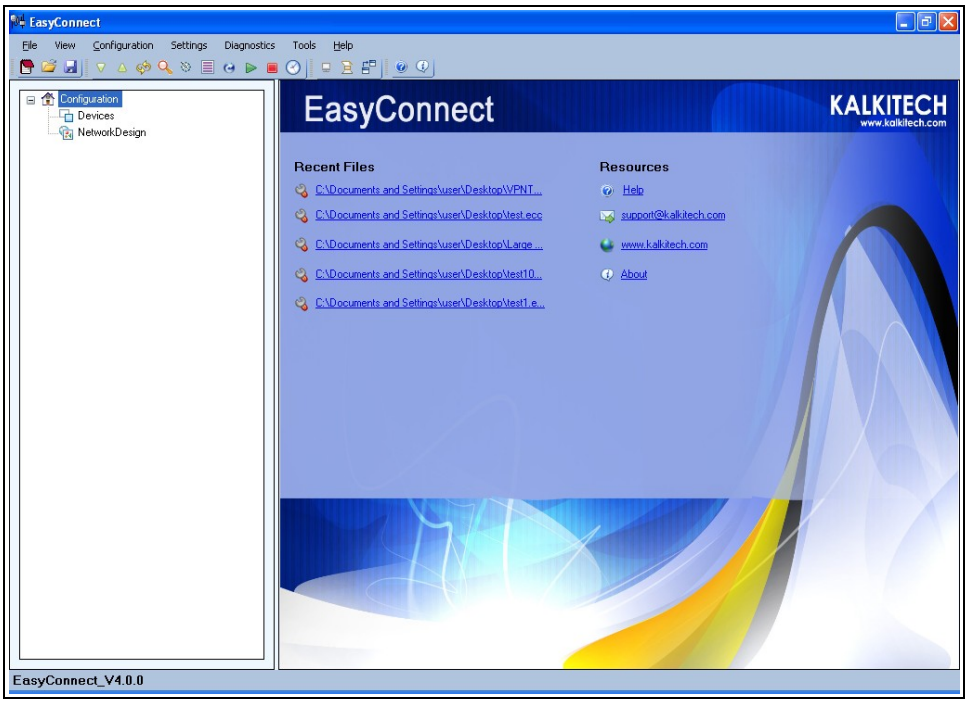


Figure 1: EasyConnect user interface

2.4 Exiting EasyConnect

You can close EasyConnect at any point during the running of the application

To exit EasyConnect perform the following steps:

1. From **File** menu, choose **Exit**. If there is any open configuration, a warning window will appear to confirm whether the user would like to save the configuration before closing EasyConnect.
2. Click **Yes,** to save the configuration at desired location before exiting EasyConnect. Click **No,** not to save the configuration and to continue with exiting EasyConnect. Click **Cancel** to cancel exiting EasyConnect.

2.5 Using the Easyconnect Interface

This section gives you an overview of the elements and menus in the user interface using the graphical user interface diagram. The components in the user interface of EasyConnect are shown in the figure below and each one is described in detail:

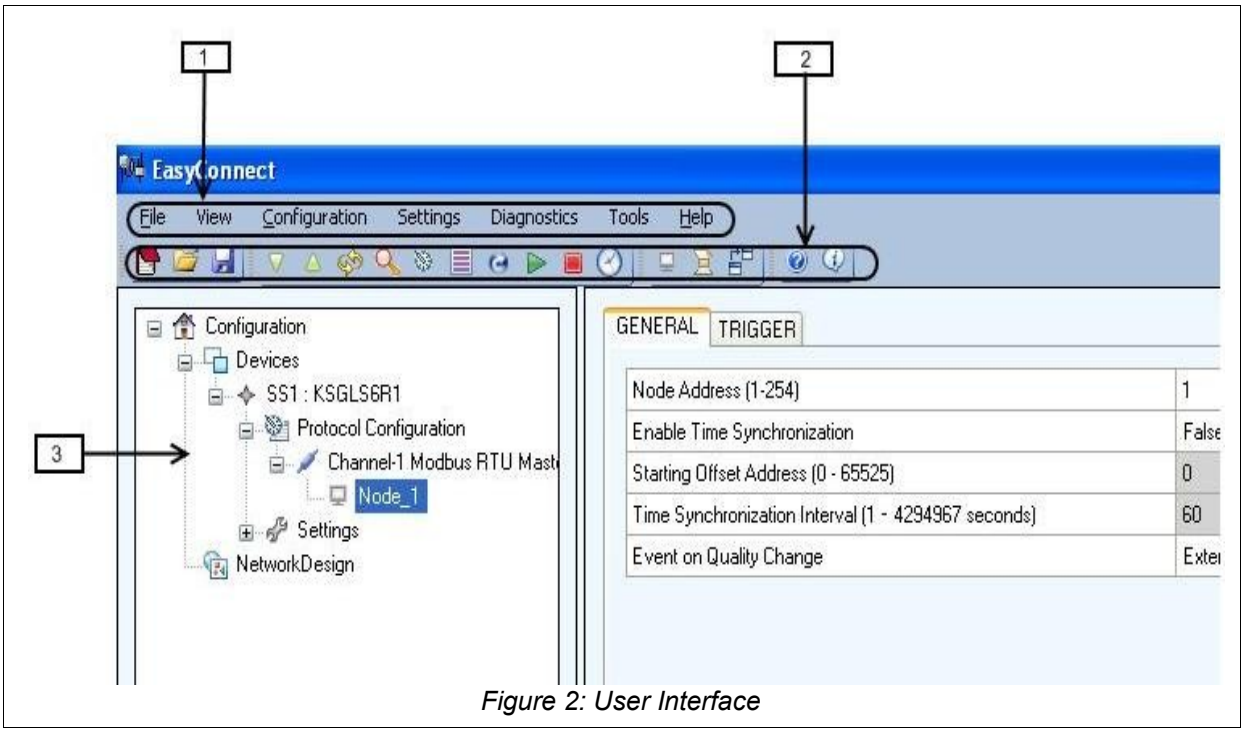


Figure 2: User Interface

The Components are:

1. Menu
2. Toolbar
3. Workspace

2.5.1 Menu

The Menu contains options to execute all the actions that can be done using EasyConnect. The different Menus are:

1. **File Menu**

To start a new configuration, opening a saved configuration file, saving the configuration etc are the options which are available in the menu. A few of these actions are also made available in the toolbar.

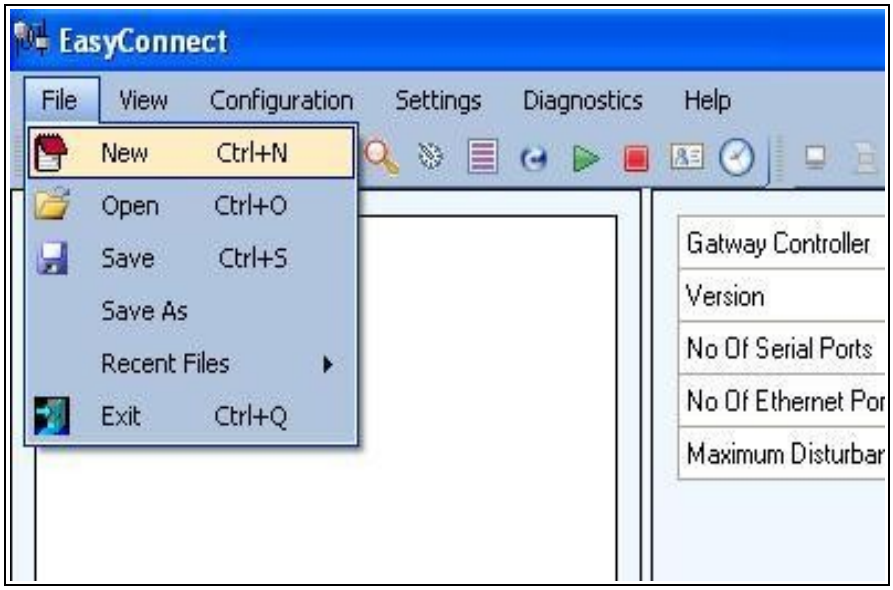


Figure 3: File Menu

2. **View Menu**

The **View Menu** contains the option to enable or disable the toolbar buttons.

3. **Configuration Menu**

The Configuration menu contains options corresponding to the node in the Tree-View that has been selected. Depending on the node selected, the options available in the Configuration menu varies. These actions can also be availed by clicking the right mouse button on the node. This menu is extensively used in configuring the SYNC and is well explained in the respective sections.

4. **Settings Menu**

The Settings menu contains the generic actions such as downloading or uploading configuration, restarting the device, IP configuration, firmware starting and stopping etc.

5. **Diagnostics Menu**

The **Diagnostic menu** contains action items for the diagnostic functionality. The options available in diagnostic menu are **Traffic Monitoring**, **PDC Diagnostics,** and **Gateway Access Log.**

6. **Tools Menu**

Tools menu contains options to set the EasyConnect parameters like Timeout settings.

7. **Help Menu**
8. The **Help menu** contains the options to get EasyConnect Help documentation and Information about EasyConnect.

2.5.2 Toolbar

The toolbar provides easy access buttons to menu options and they are:

1. File
2. Settings
3. Diagnostics
4. Help

These are selected options from the toolbar menus. They can be enabled or disabled in the View Menu. Tool tips are available for each toolbar button, describing the functionality associated with each of them.

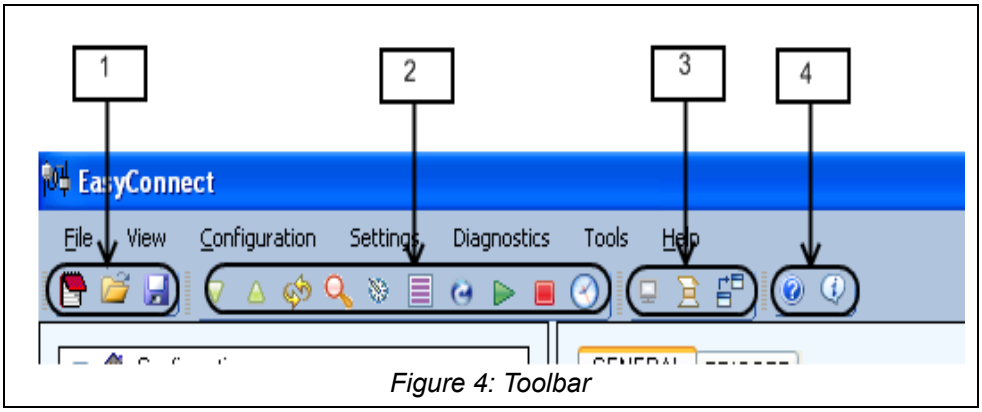


Figure 4: Toolbar

2.5.3 Workspace

The workspace section is the place where all the configurations regarding the different channels, stations etc are done. Depending on the node selected in the Tree-view, the options available in the Workspace may vary. These are described in the configuration of each item in detail.

3 Configuring Gateways

You have to configure the SYNC before it can be run. The configuration of any protocol interface module in SYNC can be done with EasyConnect configuration Utility. The configuration for any protocol conversion function can be divided into a few logical steps. Master protocol configuration will be divided into the following sections namely; Channel, Node, Profile and Row addition. For a slave; Profile, Channel and Node are configured. A master and slave can be mapped by the Add Map option. The following steps explains how to configure protocol modules for any SYNC model.

Steps to configure a gateway:

1. Add Master channels

2. Add Slave Channels

3. Add Master to Slave Map

4.Slave to Slave Mapping

5. Dialup Support

6. VPN Support

7. SNMP Support

Step 1,2 and 3 deals with protocol conversion function of the gateway. Step 4 and 5 deals with additional/optional communication features of the gateway. For normal protocol conversion requirements users can stop at step 3.You may proceed to step 4 or step 5 when you use any of the described features.

3.1 Add Master Channel

1. Add converter either by selecting a converter model from **Device configuration** section or right click on **Devices** in the left hand side pane,as shown in figure below:

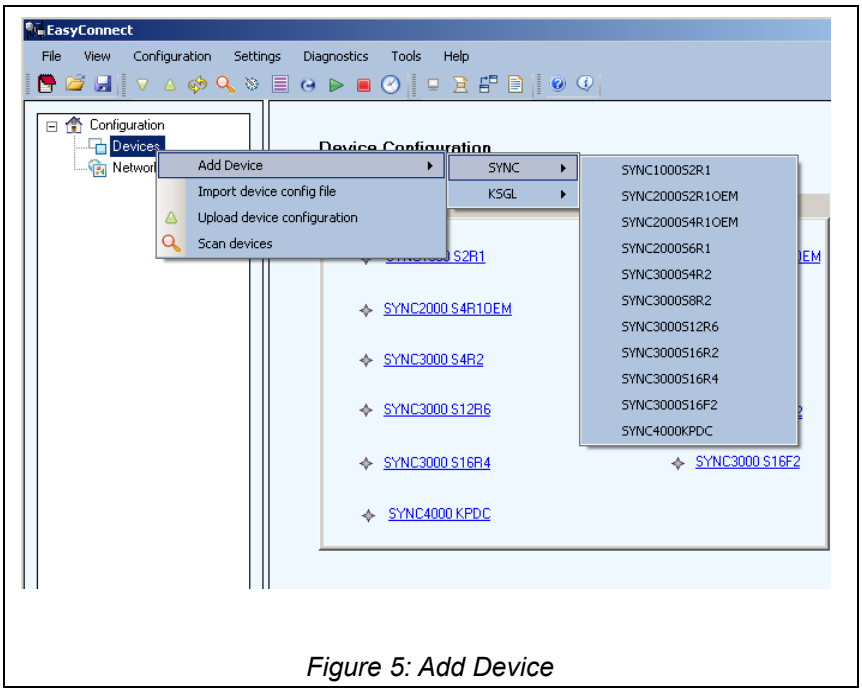


Figure 5: Add Device

If you want to modify an added gateway model, right click the selected gateway model in the left pane of the application, choose gateway model from sub menu of **Modify Gateway.**

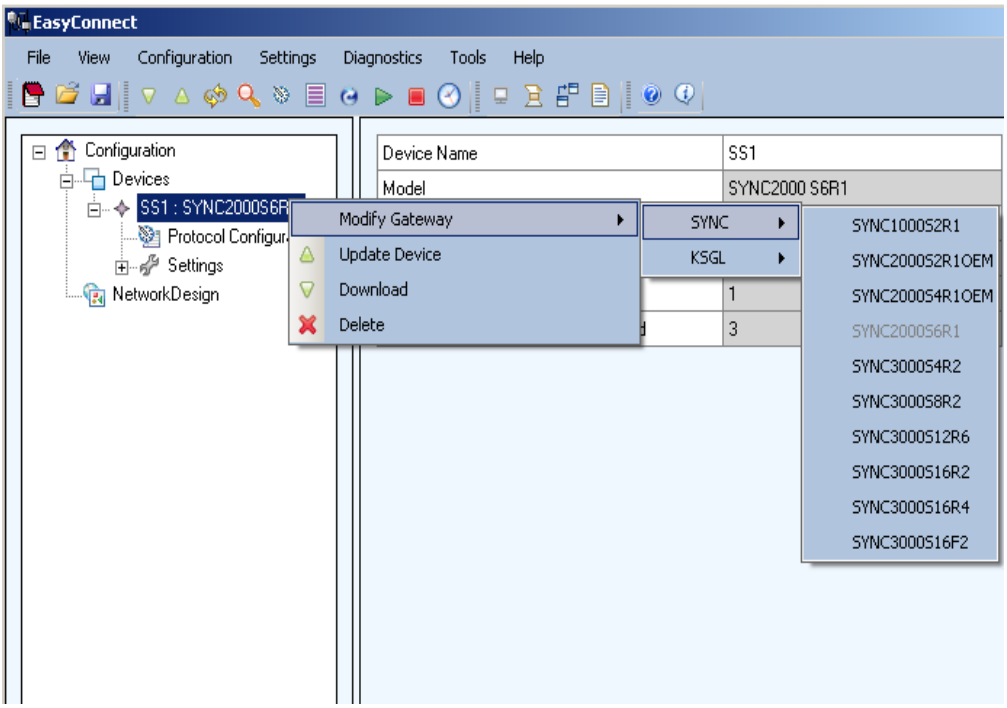


Figure 6: Modify Device

To delete the selected gateway, right click the selected gateway, and choose **Delete**.

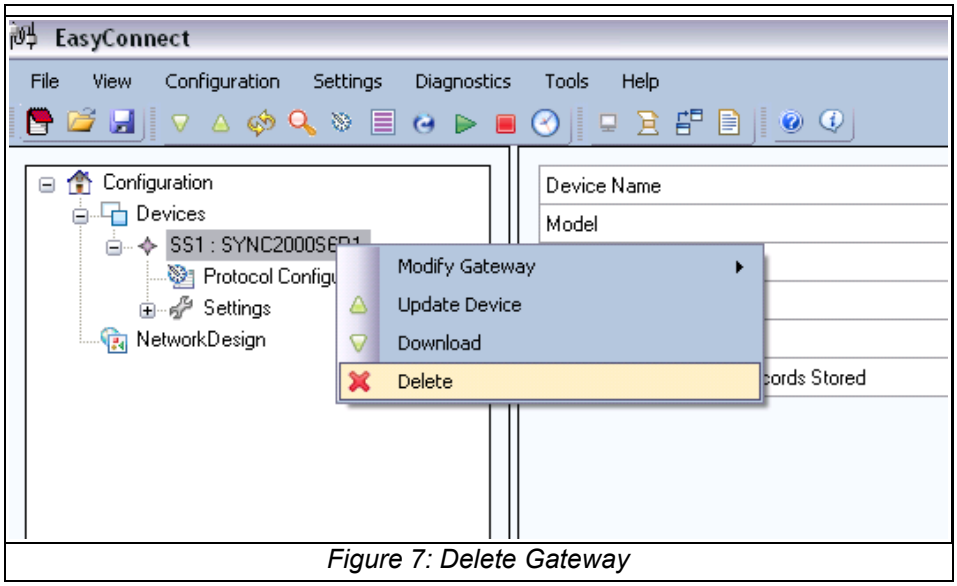


Figure 7: Delete Gateway

2 .Add **Master channels** to the converter model as shown in figure below:

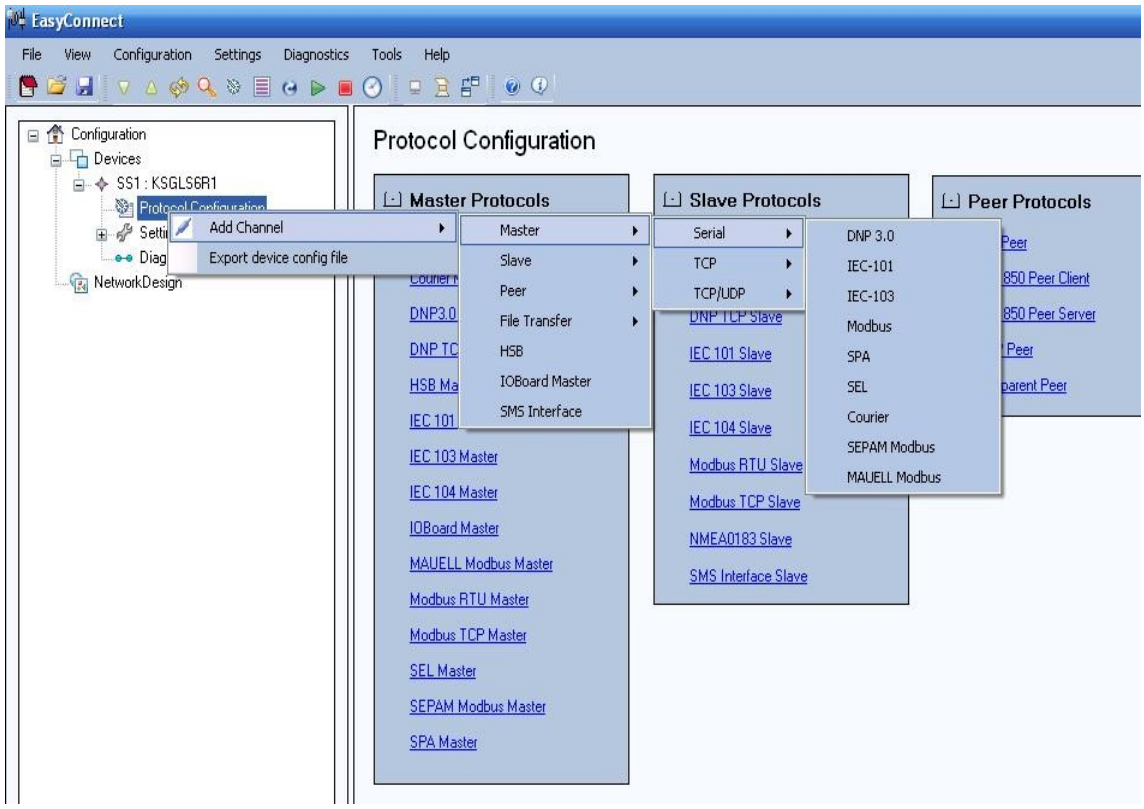


Figure 8: Add Master Protocol

You can delete a protocol specific communication channel by selecting Delete option from menu on right clicking on the selected channel as shown below:

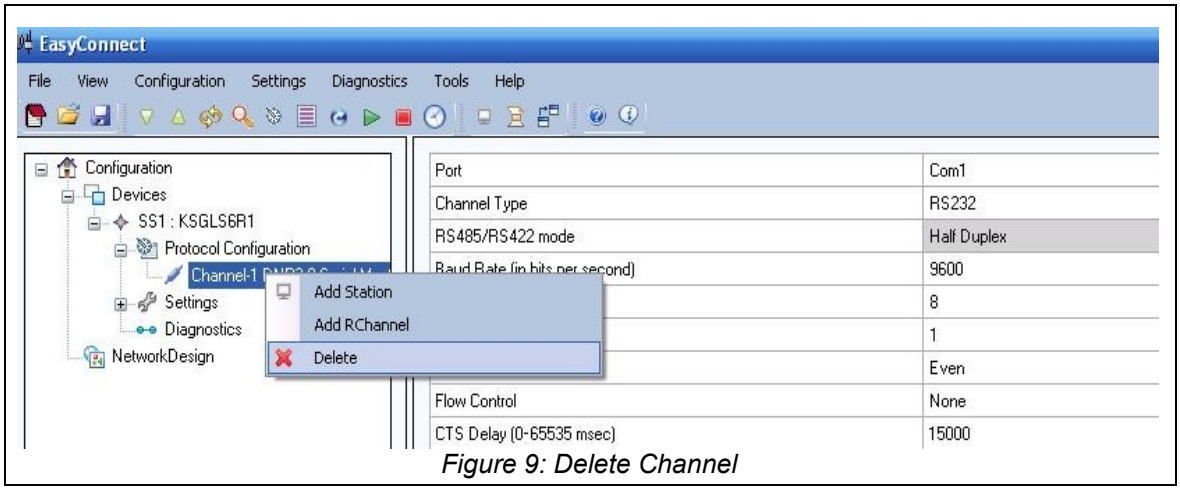


Figure 9: Delete Channel

3. Add **Node** or **Station** as shown in the figure below.

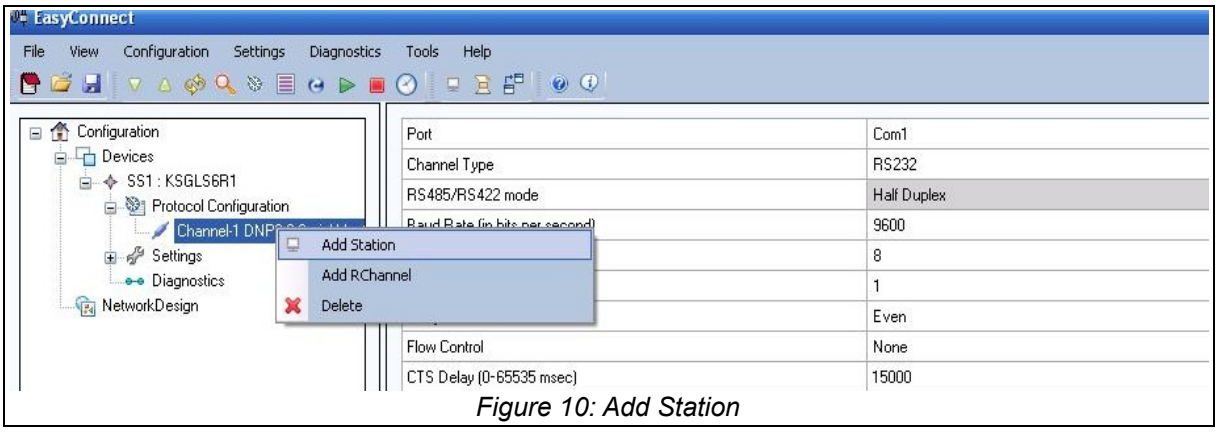


Figure 10: Add Station

4. Delete a station by selecting **Delete** from menu displayed on right click of selected station.

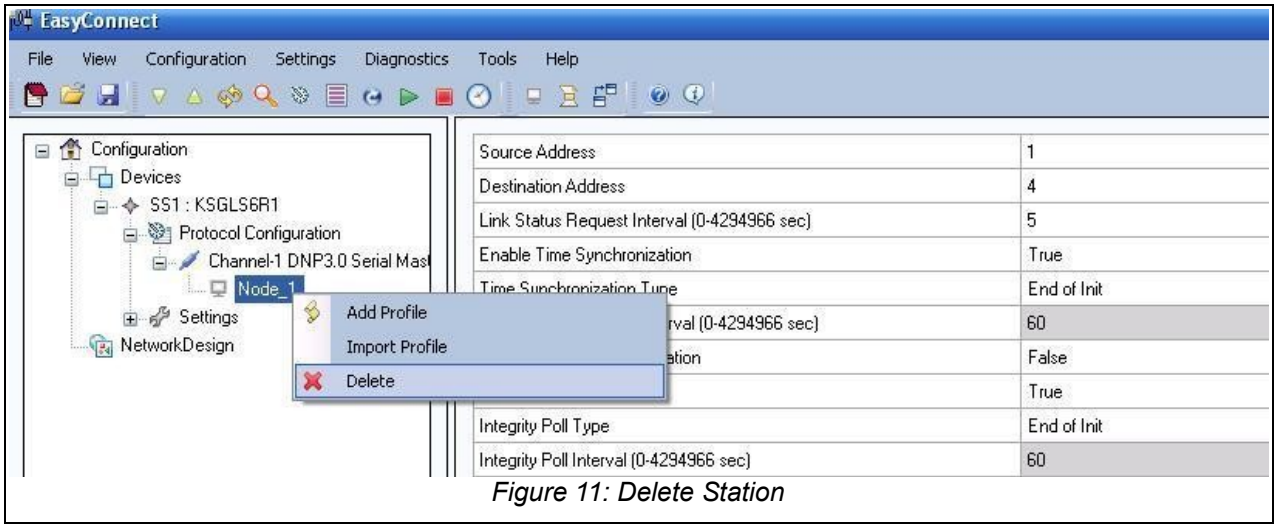


Figure 11: Delete Station

5. To add **Master Profile** right click on **Node** and select **Add Profile.**

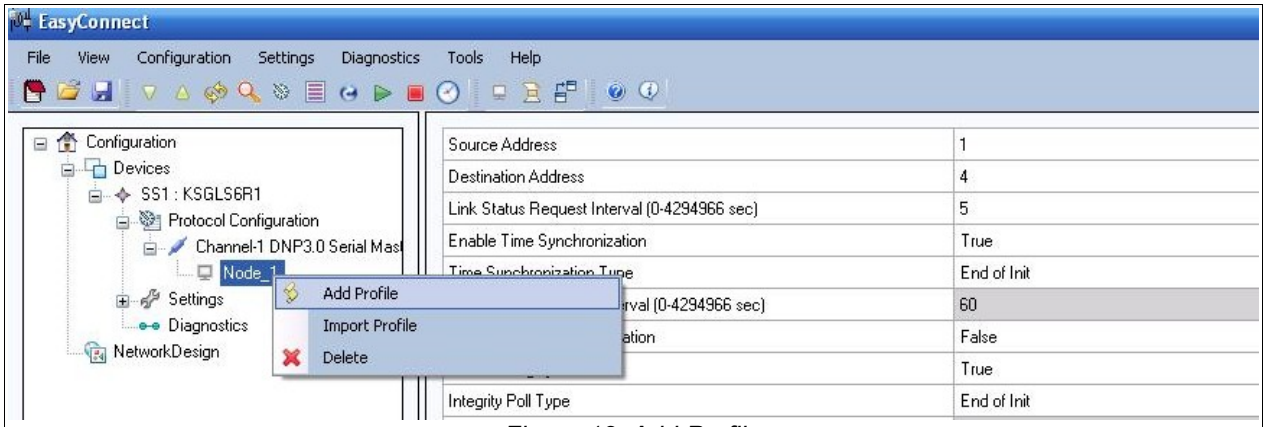


Figure 12: Add Profile

Profiles can be saved for reusing the same address configuration for different masters. Right click a **Profile** tree node and select **Export Profile**, a Save File window will pop up. Save the profile in desired name in desired location.

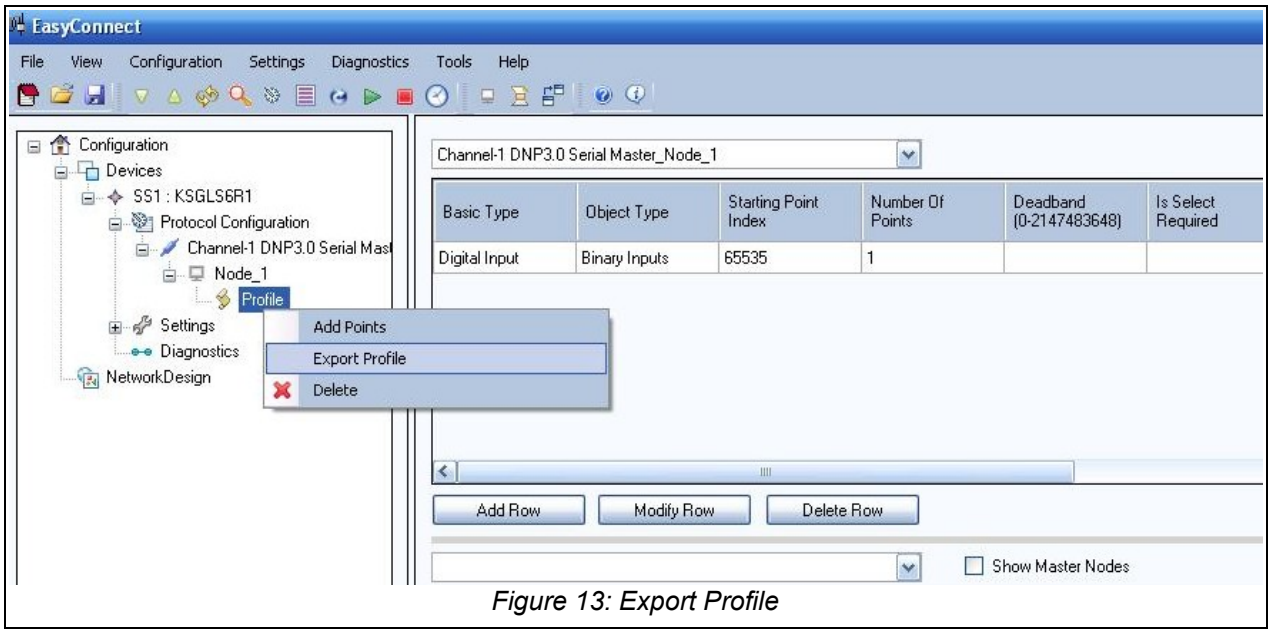


Figure 13: Export Profile

Instead of adding a new profile you can also import previously saved profile data. Right click on a **master station** and select **Import Profile** option, an Open File window will pop up. Open a saved profile file. Refer figure below:

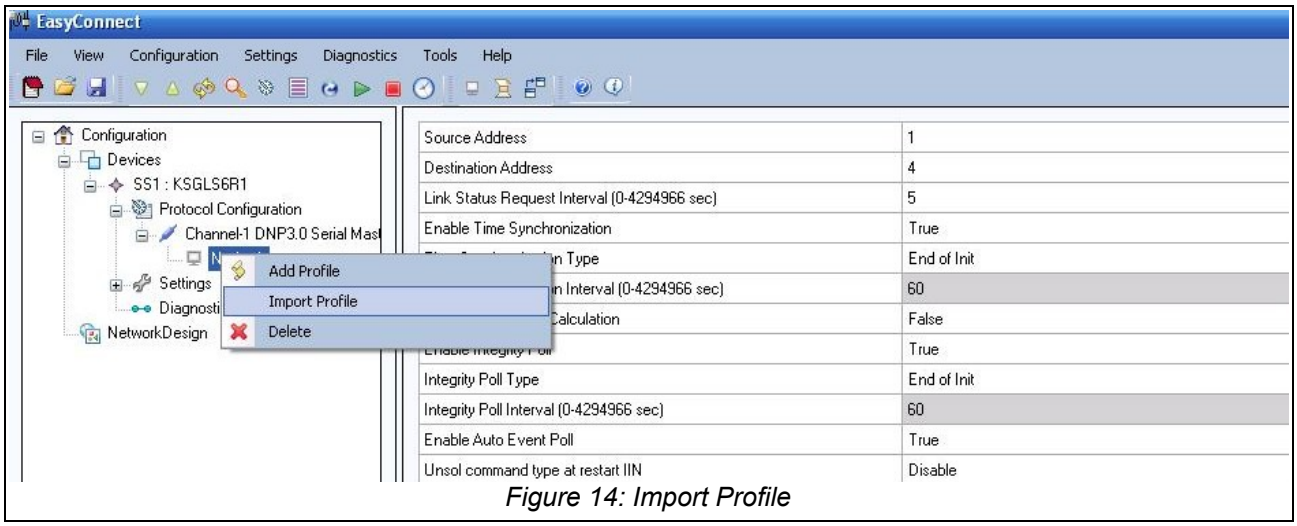


Figure 14: Import Profile

To delete a **Profile**, right click on added **profile** and select **Delete** .

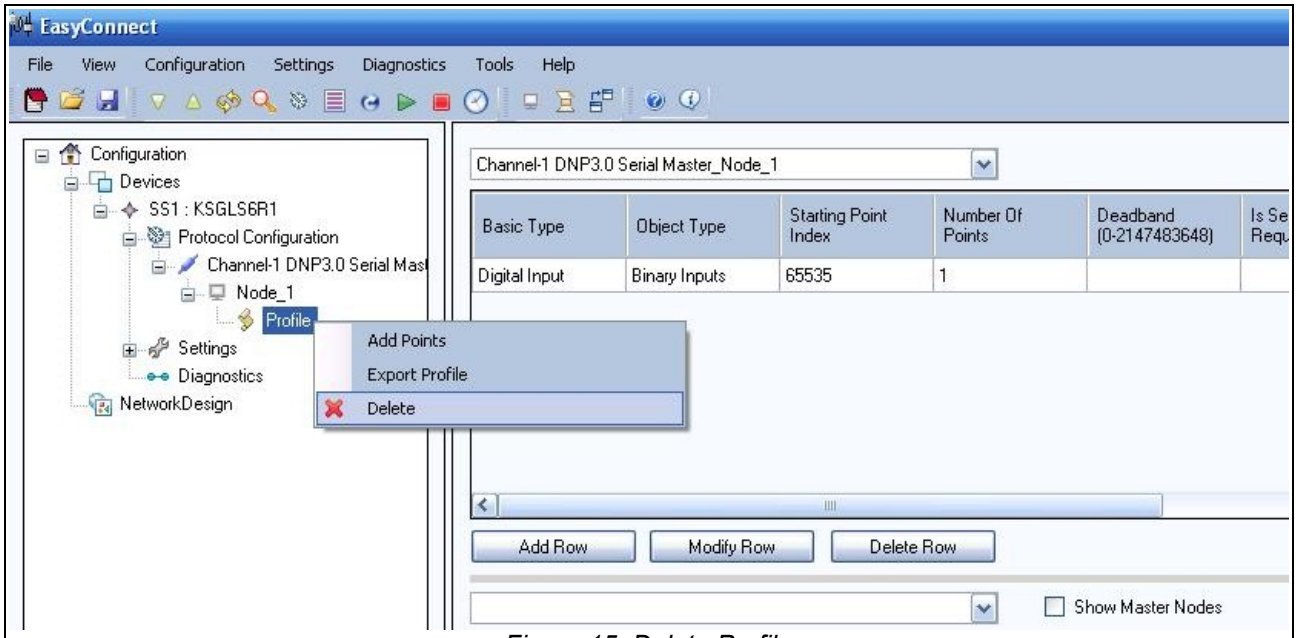


Figure 15: Delete Profile

6. To add Master Row right click on **Profile** and select **Add Points** as shown in the figure below

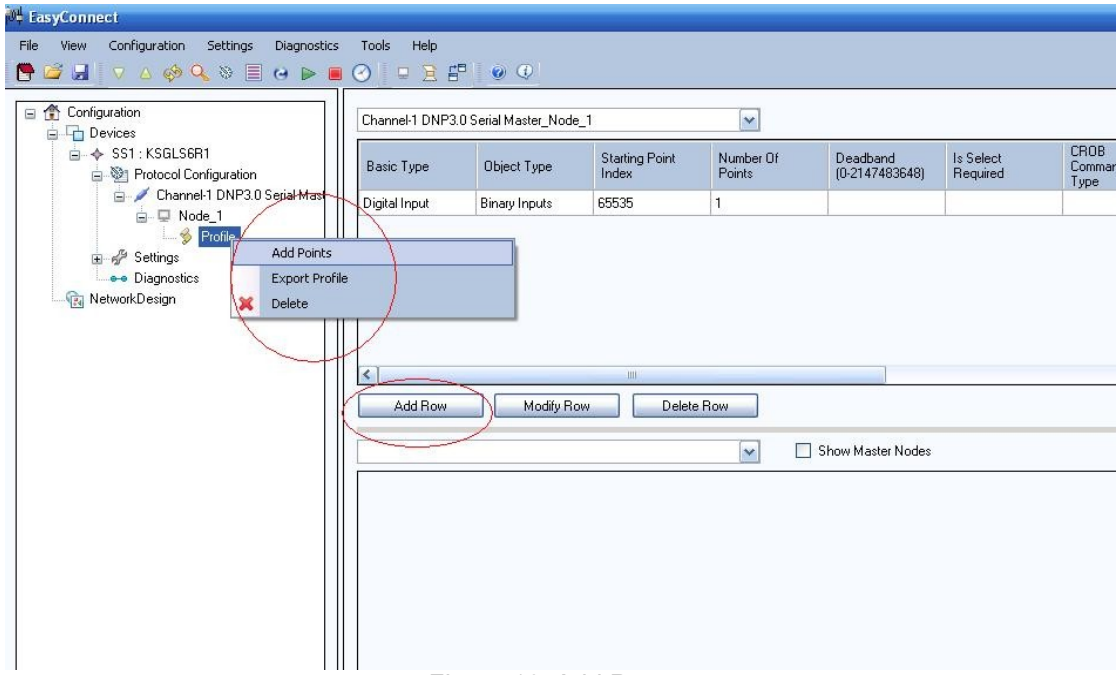


Figure 16: Add Row

Select a row from the profile grid. Click on **Modify Row** button. A new window will pop up with values of selected row.

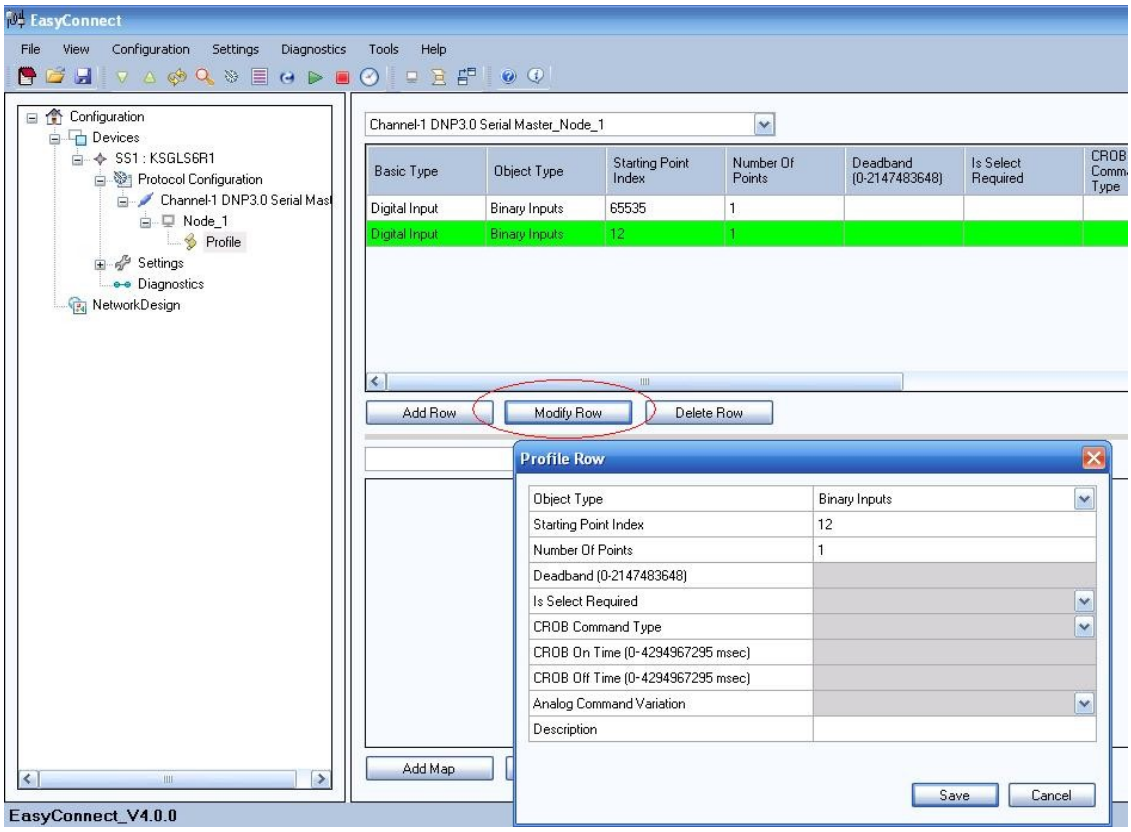


Figure 17Modify Row

For deleting added rows, select rows from profile grid and click **Delete Row** on the right pane.

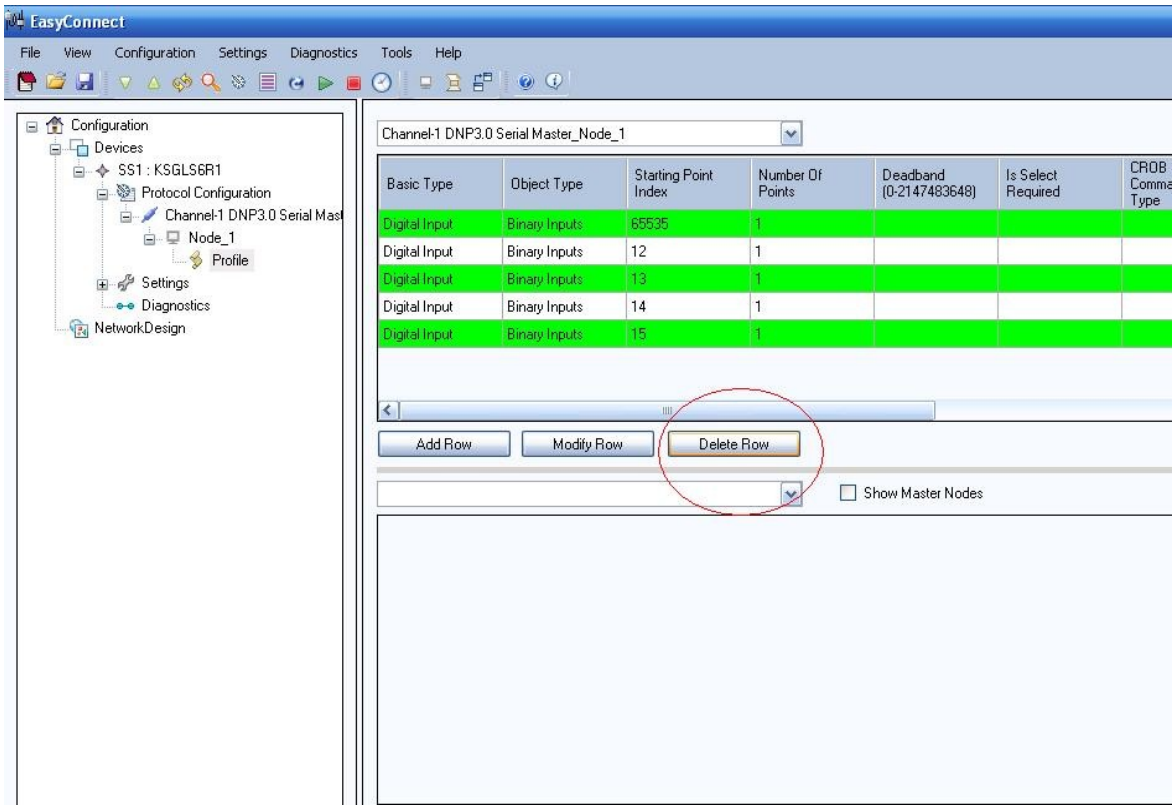


Figure 18: Delete Row

Adding large number of points in a profile using Easy Connect Add Row button can be time consuming. Easy Connect Configuration Utility provides facility to export profile rows to an excel worksheet and import the points form an excel worksheet to the profile rows. User can configure the required points in an excel worksheet and it can be imported to the required profile.

After adding required rows in the profile, select **Excel Export** from the context menu as shown in figure below:

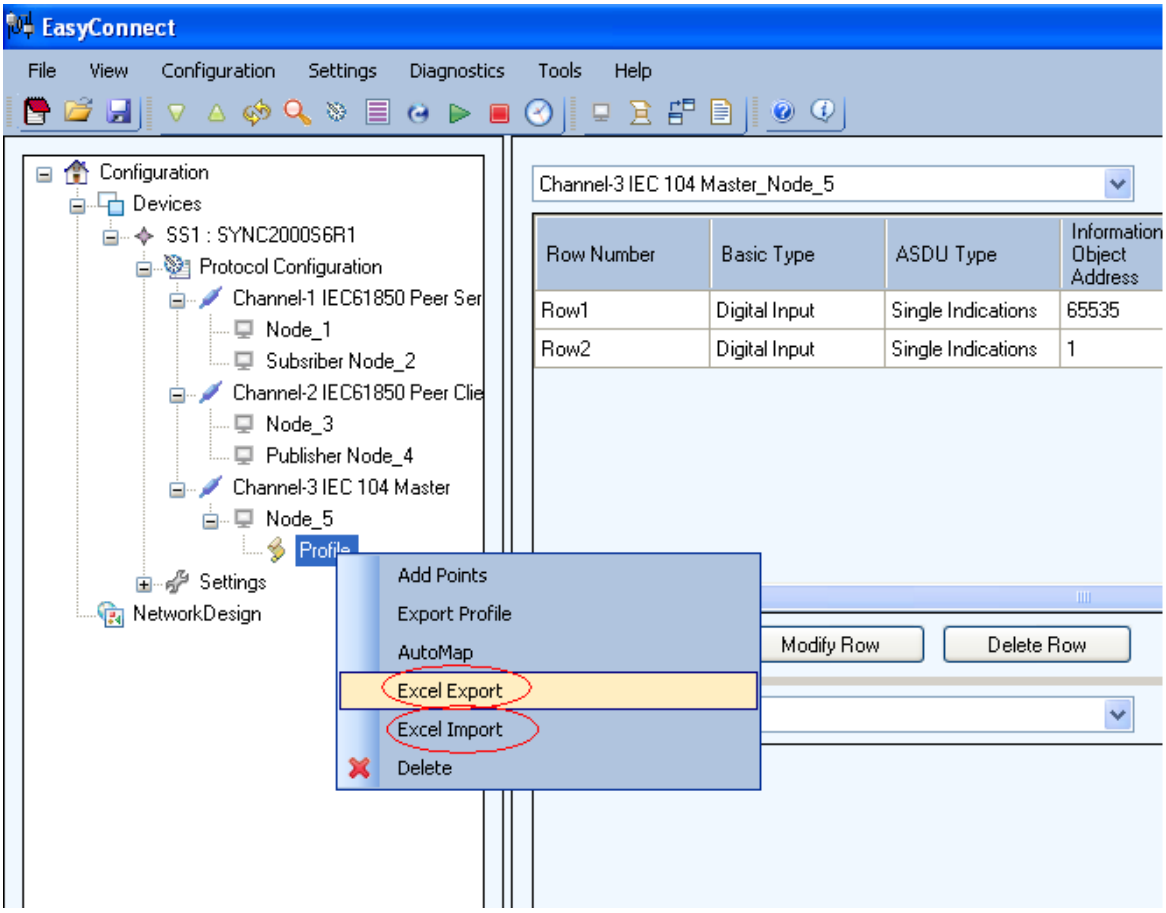


Figure 19: Excel Export & Import

Exported excel worksheet format is shown in figure above. The worksheet will contain the protocol Name. All the configurable parameters in the Profile Row window of the specified protocol form individual columns. All the available options for a parameter will be available in the combo box independent of the type of point selected.

Note: Communication diagnostic point will not be imported to the excel worksheet.

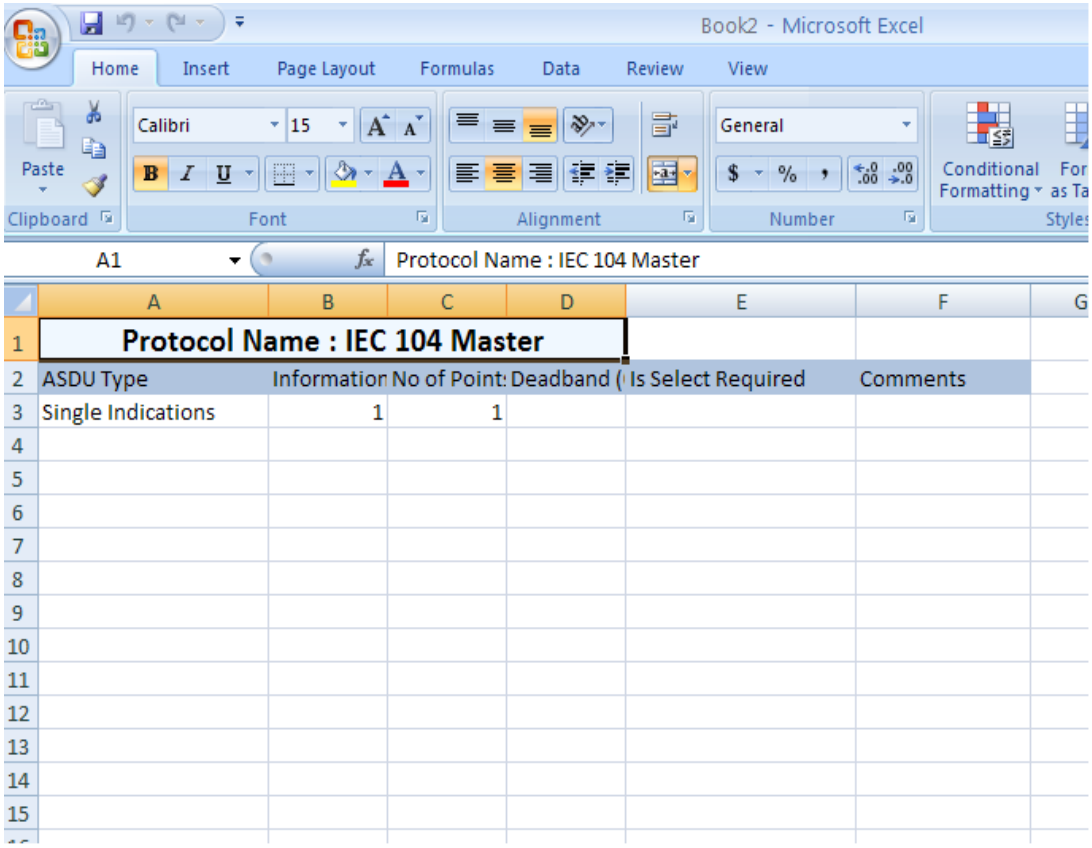


Figure 20: Excel Profile

Excel Import:

Select Excel Import from the context menu of profile and choose the excel worksheet prepared to import. See figure . Certain conditions are applicable for the Excel Import functionality.

- Only worksheets previously exported from Easy connect can be imported. User should add at least one point (other than communication diagnostic point) in the profile and use **Excel Export** to generate an excel worksheet template. Configure required points in this file and save. Note that Easy Connect expects a specific format for the worksheet. So the user should refrain from modifying the format of the sheet in any manner. Only the contents may be changed.

- The protocol name in the Excel worksheet should match with the protocol of the profile to which it is imported. For example an excel worksheet exported from IEC104 Master can only be imported to a profile under an IEC104 Master Channel.

- Easy Connect validates all the parameters configured in the excel worksheet before importing and will push an error message if the validation fails. All the available options for a parameter will be available in the worksheet cells independent of the type of point selected. For example in Modbus Master, Function Type 'Read Coil status' is not applicable for object type 'Analog Input'. But this option will be available in the excel worksheet cell. User should select the valid options while editing the worksheet. Any failure in validation will terminate excel import.

- After validation, all the existing profile rows will be replace by the points configured in the worksheet.
- For points that are already mapped to a destination protocol;
- For all the rows where the address parameters are not modified, the other parameter values are read in from the worksheet.
- If the address parameters are changed in the worksheet, Easy connect will pop up a message as shown in figure below. On selecting yes the mapping will be deleted and the points in worksheet will be imported. On selecting No the excel worksheet will not be imported.

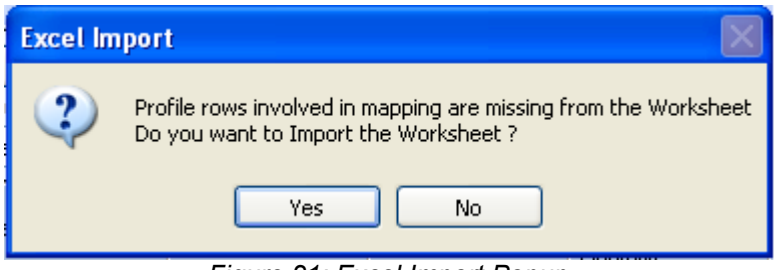


Figure 21: Excel Import Popup

To delete a Profile, right click on added **profile** and select **Delete** .

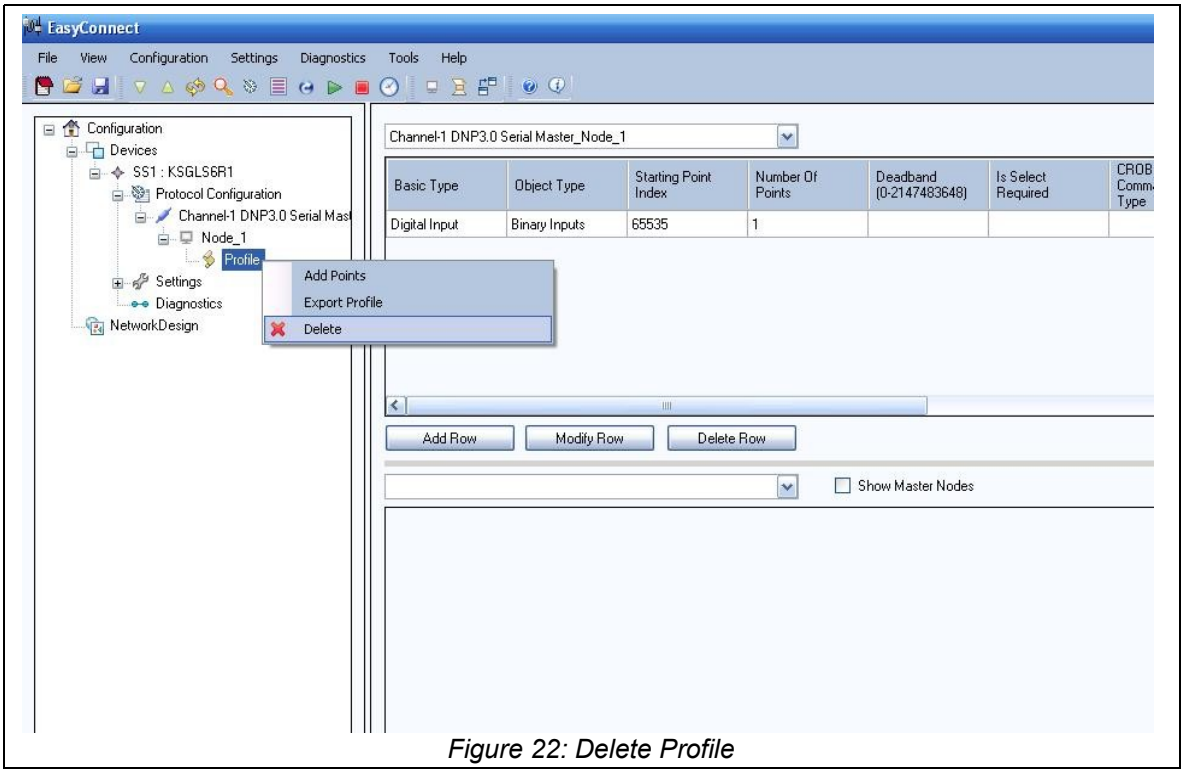


Figure 22: Delete Profile

3.2 Add Slave Channel

To add a slave channel and node follow the procedures mentioned above.

3.3 Add Master to Slave Map

To add a Map, select the required Row and the desired slave node,then click on **Add Map**.

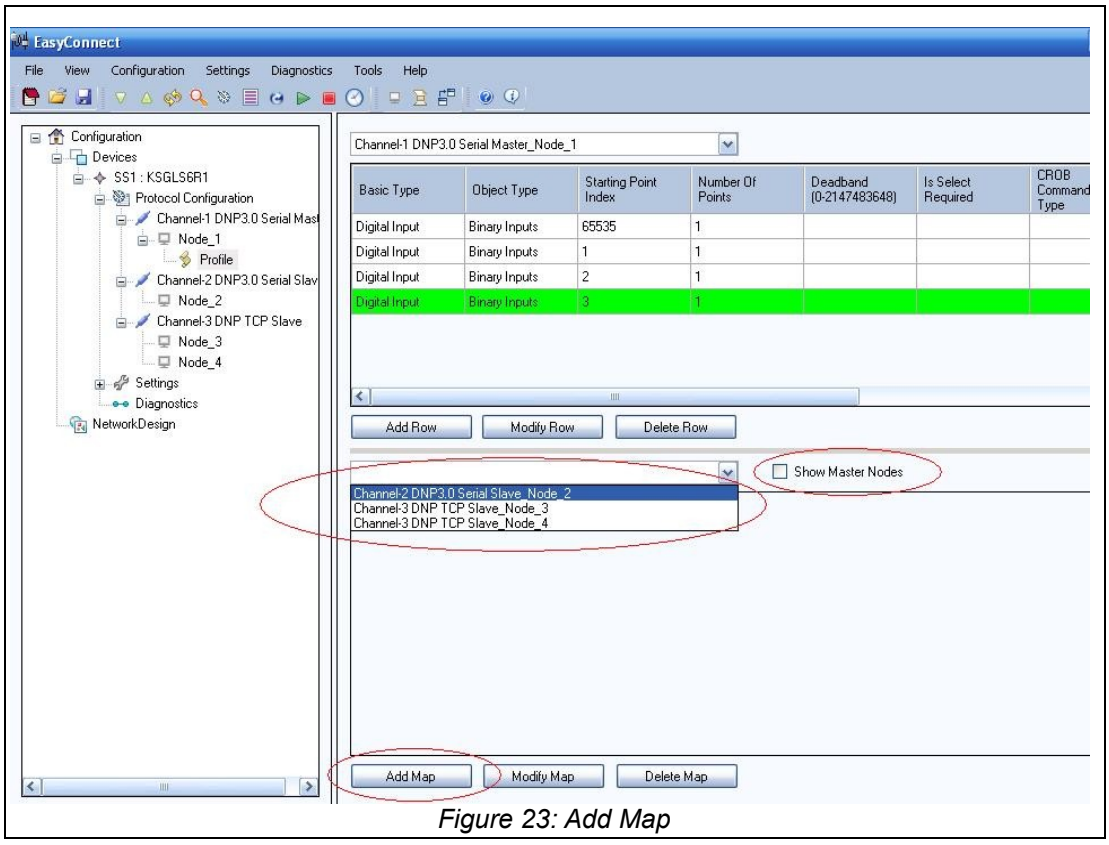


Figure 23: Add Map

Note: To Enable Master to Master mapping select Show Master Nodes.(Master to Master mapping is used when input data from an external device is translated to a command/output and sent to an external device.)

To modify a mapped row, select a row from the destination unit and click on Modify button. A new window will open with added mapped values. Edit the parameter values. Click on **Save** to update the modified mapped point. Refer the figure below:

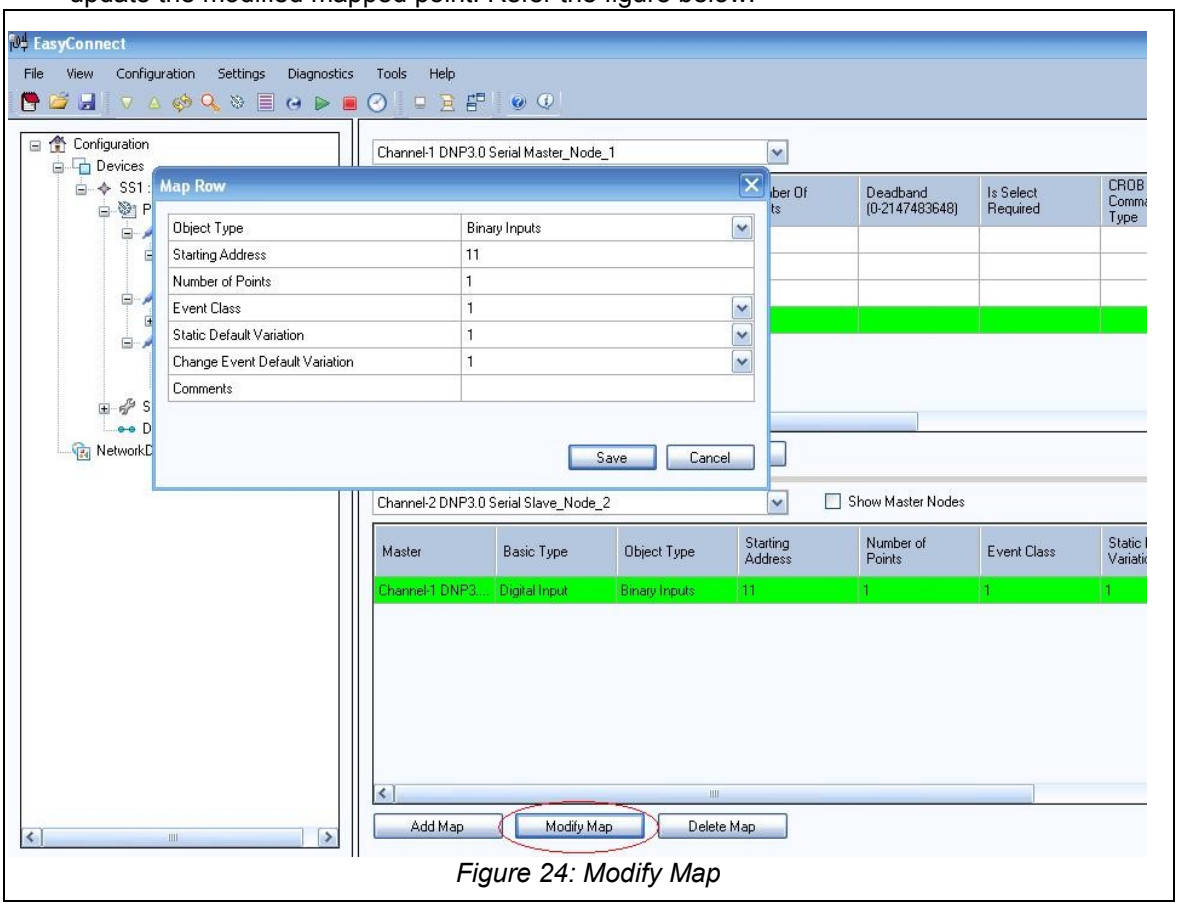


Figure 24: Modify Map

To delete a mapped row or group of rows from the conversion, select mapped row from the destination unit and click **Delete Map**. To delete destination unit profile, right click on **Mapping** tree node under destination unit, select **Delete**. Refer Figure below.

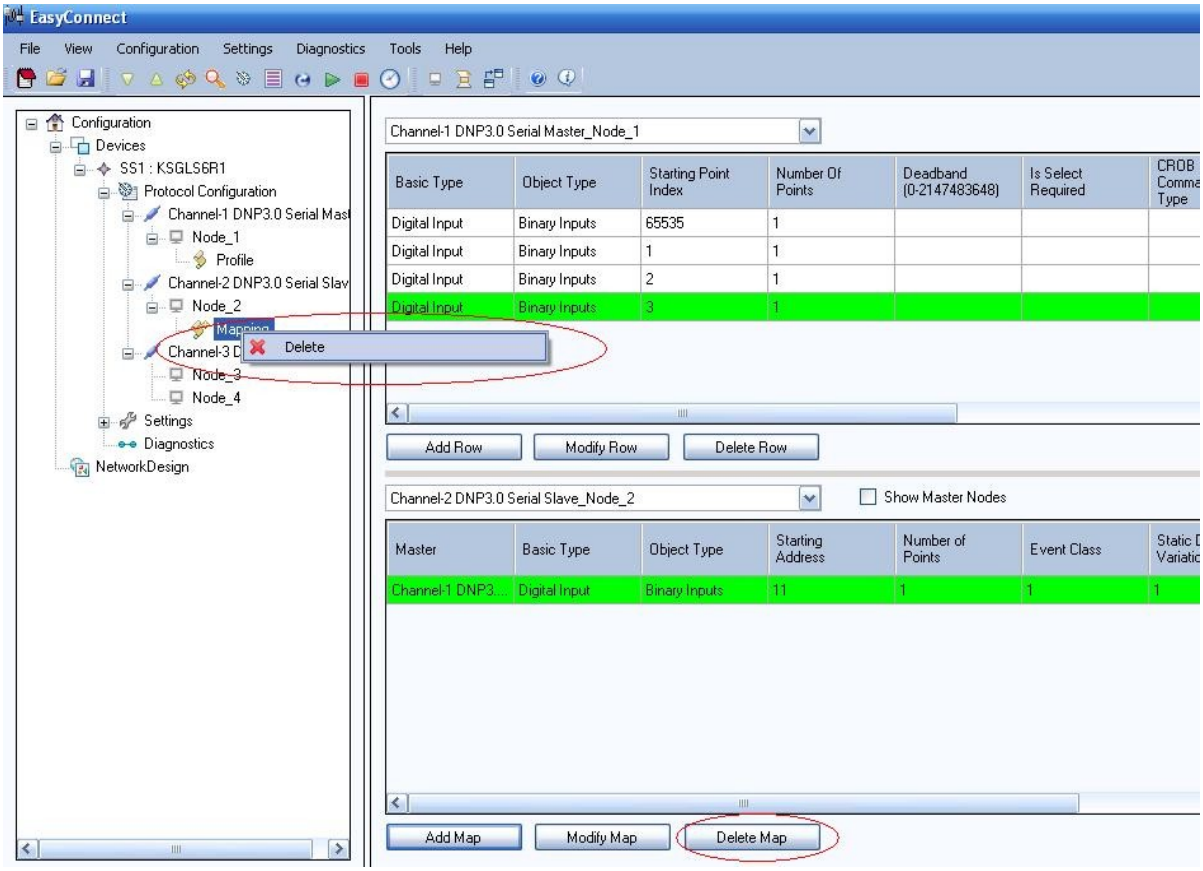


Figure 25: Delete Map

3.3.1 Auto Mapping - Master to Slave

EasyConnect Provides Options for mapping the master points automatically to a selected slave node. User can either auto map the entire row configured in the master profile or some selected rows.

1 Select the slave protocol to which the points are to be mapped.

2 For mapping the entire rows in a profile, Right click on the corresponding profile and click the option **Auto Map** as shown in figure below

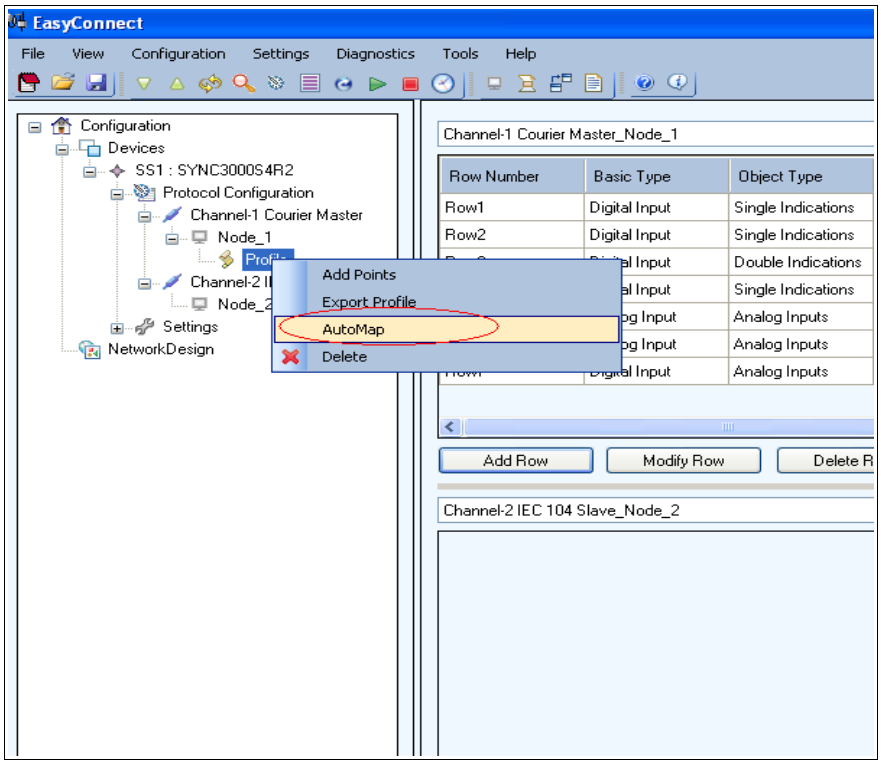


Figure 26: Auto map entire profile points

1. For mapping the selected rows in a profile, select the needed rows in the profile for which the automatic mapping needs to be done. Click on **Auto Map** (slave/destination mapping part) as shown in the figure below:

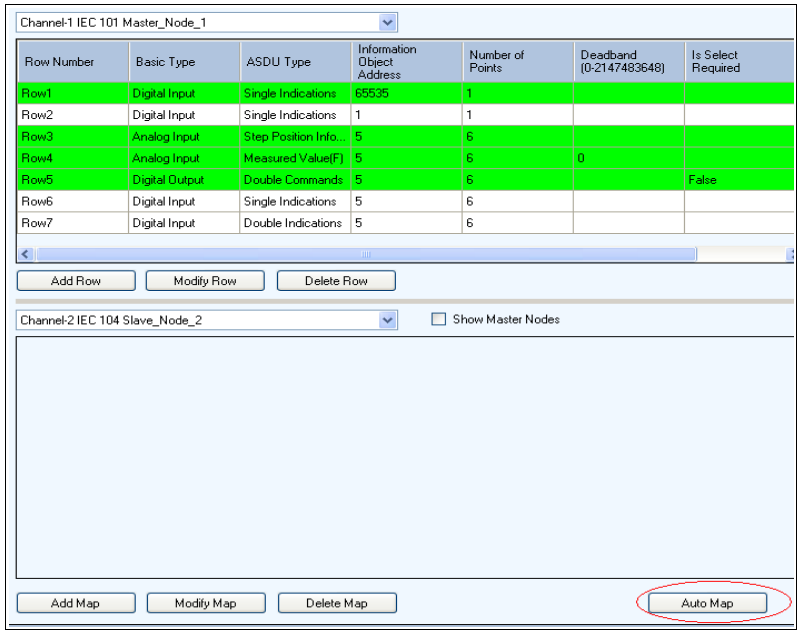


Figure 27: Auto map selected profile points

2. Step 2 or 3 will pop up the **Auto Map** window as shown in the figure below. User can configure the details in the Auto map window and generate auto mapping.

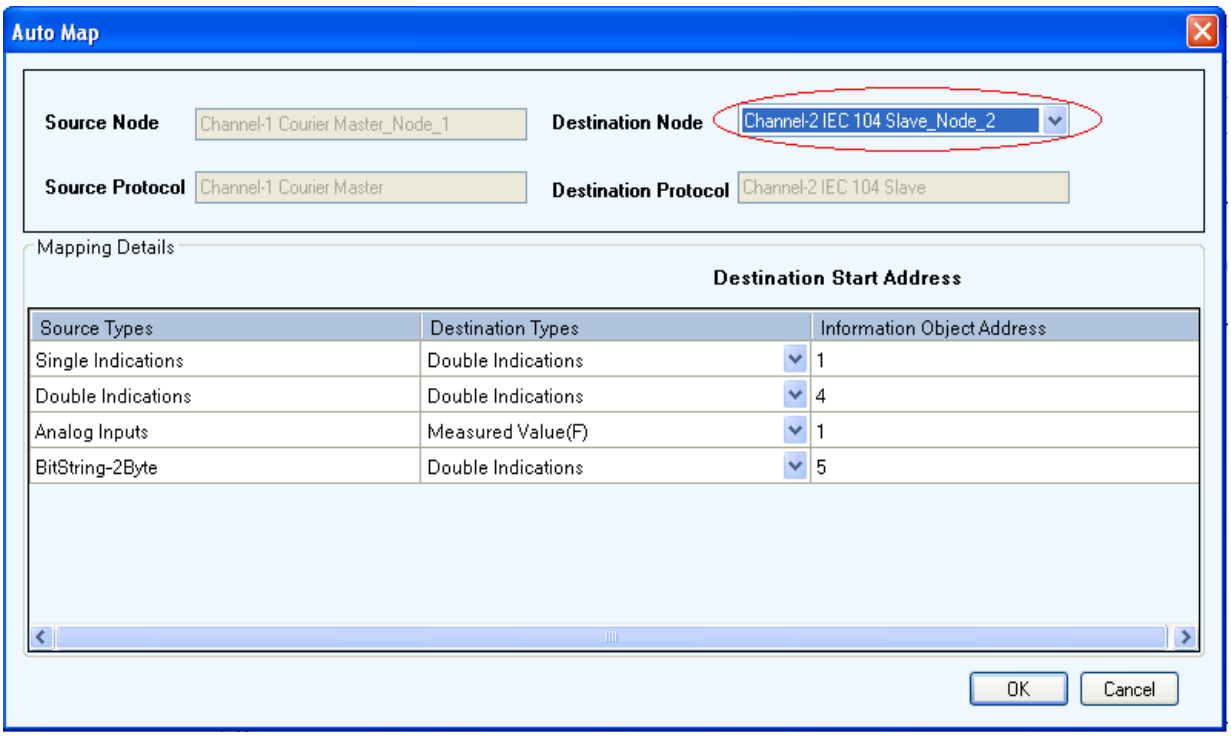


Figure 28: Auto map window

3.3.1.1 Auto Map Window

Auto Map window shows the master (source) types that are considered for automatic mapping, corresponding slave types automatically considered as mapping type (user can change using combo options) and corresponding start address in the slave. The parameter details of Auto Map window are given in table.

Sl No	Parameter	Details
1	Source Node	Indicates the node number whose profile needs to be mapped. This parameter is not editable.
2	Destination Node	Indicates the node to which the mapping needs to be done. The default will be the node selected in the mapping window. User will able to change the same to any other nodes which is available in the configuration system.
3	Source Protocol	Protocol of the source node. This parameter is not editable.
4	Destination Protocol	Protocol of the destination node. This parameter is not editable.
5	Source Types	Indicates source data types from which mapping is carried out.
6	Destination Types	Indicates suggested destination data type for the specific source type to which mapping is carried out. This indicates default suggestion and user can even change the same from the allowed types available in combo box.

7	Destination Start Address	This indicates the destination start address for the specific destination type. This is generated after evaluating all the existing address and last address + 1 of the already existing address is considered as default. User can change the start address but it will again undergo evaluation. There will be multiple address parameters based on the protocol used. If it is IEC101/104 the same will only have IOA, if it is IEC 103 it ftype will have & I number.

Table 8: Document Revision History

The following points will be applicable to the Auto mapping window.

1. Only data types which has at least a point available for mapping to the current slave shall be displayed in the auto-mapping window.
2. Similar source types will be grouped and displayed as a single row in the Auto Map window. In each protocol the grouping of source types differ.
3. All the types coming under the *Basic type* of the source type will be available in the combo box options of *Destination Types*.
4. In cases, where destination address range is not sufficient to map all the points, an error message would be displayed in the validation stage after clicking the '**OK**' button.
5. Points will not be split and mapped for numerical address based protocols. A continuous address space large enough to hold the points in a single row (source) is found and the points are mapped to those range.
6. Auto-map shall be provided for all Master protocols except 'HSB Master' and 'Logic Master'.
7. On pressing **OK** from Auto-map window, points that can be successfully mapped are processed and for those which could not be mapped,an error message is displayed.

   Note: All the other profile parameters will be default when auto mapped. User can modify the row if required

3.4 Slave to Slave Mapping Feature

Introduction

The Slave to Slave mapping provides the facility to transfer some critical information between two master stations.

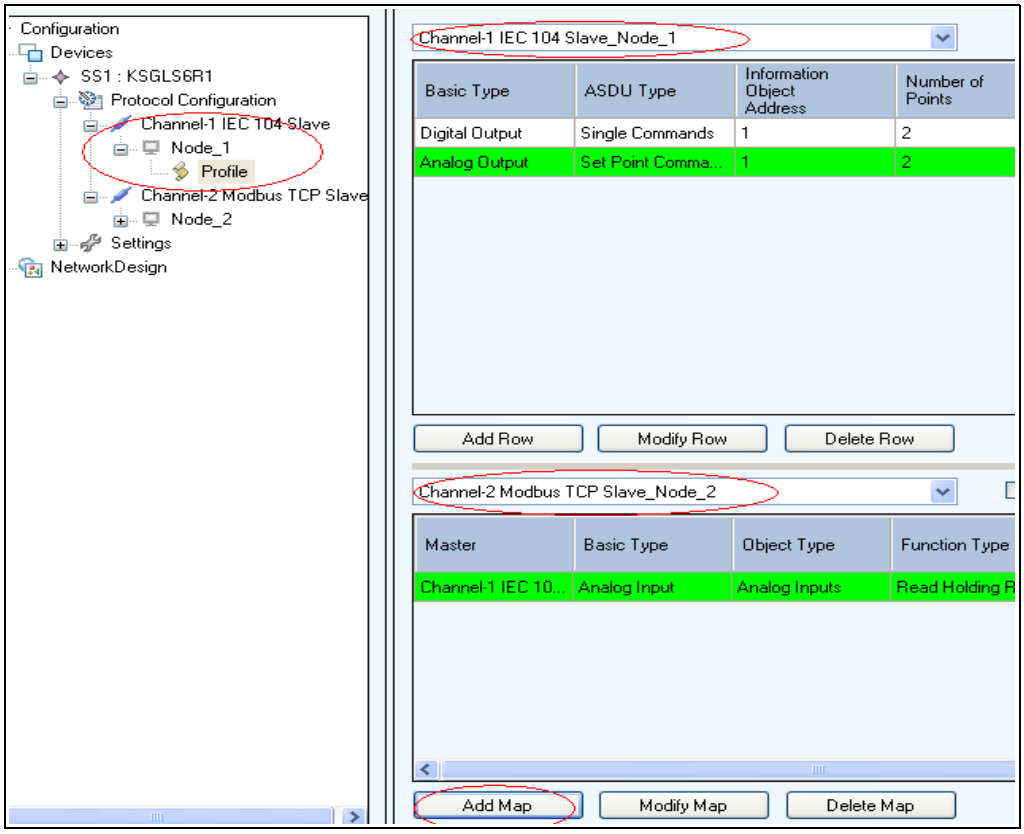
For provisioning communication between masters,the corresponding source slave should be mapped to the destination slave. The source slave is the 'slave which transacts with the master from which data has to be transferred' and the 'destination slave is the slave which transacts with the master to which the data has to be transferred'. User can add profile and configure command points under the source slave nodes. These command points can be mapped to input points. A command received on the source slave will be sent as an event to the mapped destination slave.

Depending on the command type and protocol a positive acknowledgment will be sent back to the source slave after sending the event notification. If the command point is not mapped, a negative acknowledgment will be sent back. For the protocols and particular data types which do not support event intimations,the data can be retrieved by polling.

Note: Slave to Slave Mapping does not allow multiple mapping. Also a single row can only be mapped to a single node. For example consider a row with three points. Each of these three points should be mapped to a single node. Splitting and mapping to different nodes is not permissible. Also,the quality of the points configured will always be good. And the time stamp of the event will be the time taken from the converter when the command is processed.

Configuration Details

1. Add slave channels and nodes (source and destination).
2. Add Profile under source Slave and configure Points as shown in figure below



Select destination Slave and click on AddMap to add the mapping as shown in figure above. Modify mapping and Delete mapping functions identically to the master to slave mapping counterparts

3.5 Dialup Support

SYNC series gateways can be configured to work with a dialup modems.SYNC series with a built in modem can be ordered separately. SYNC series can be also be used with external modems .

Configuring Dialup/Modem:

We can configure Dialup/Modem settings for a converter whose configuration has been uploaded in the configuration window.

1. Right-click on the **Settings** node to get the option **Add Dialup** settings.

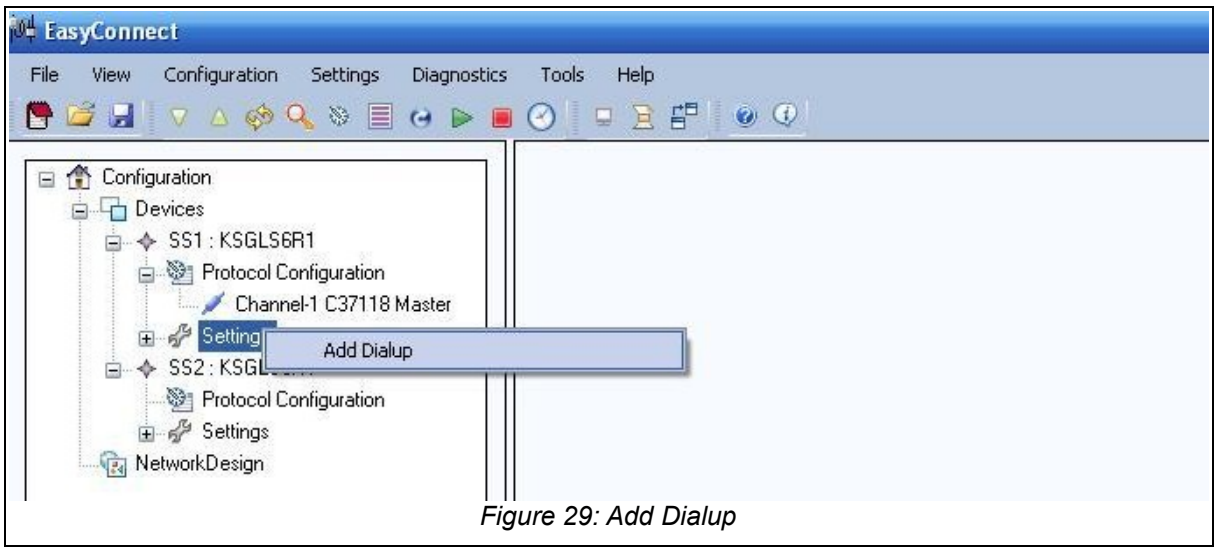


Figure 29: Add Dialup

2. Click on **Add Dialup.** Add Dialup window will be displayed. Enter the relevant changes. Refer Dialup parameters table for its parameter name and its description.

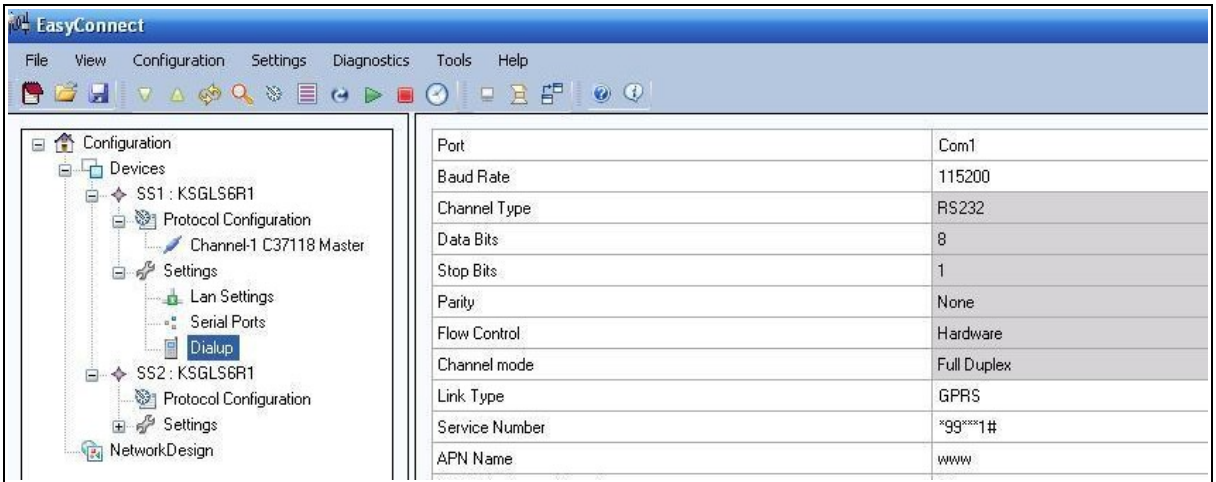


Figure 30: Add DialUp

Parameter name	Range/Optional values	Default value	Description
Port	Com1-Com16	Com1	Gives the valid com port to which the modem will be connected
Baud Rate	200,600,1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200	115200	To set the baud rate according to the modem baud rate
Channel Type	NA	RS -232	Not Editable. Type of channel used
Data Bits	NA	8	Not Editable. Number of data bits
Stop Bits	NA	1	Not Editable. Number of stop bits
Parity	NA	None	Not Editable. Number of parity bits
Flow Control	NA	Hardware	Not Editable. To prevent overflow of modem buffer
Channel Mode	NA	Full-Duplex	Not Editable.
Link Type	NA	GPRS	Specifies the link type to be used
Service Number	*99#, *99***1#	*99***1#	Universal dialing Number for the given link type
APN Name	Depends upon service provider	www	Access Point Name for a given service provider
LCP Echo Interval	Depends upon service provider	20	Depends upon support from service provider
LCP Echo Failure	Depends upon service provider	3	Depends upon support from service provider
Packet Compression	Enable/Disable	Disable	Depends upon support from service provider
Authentication type	PAP, CHAP, None	PAP	Type of authentication protocol used
Client Name			Configure if provided by service provider. Else use default values.
Server Name			Configure if provided by service provider. Else use default values.
Password			Configure if provided by service provider. Else use default values.

Table 9: Dialup Parameters

Download the settings via File Download option and check the option **Dialup Settings**.

Figure 31: Download

To delete the dialup settings from the configuration window, right click on the Dialup node to get the Delete option as shown in figure below. Click on option **Delete**.

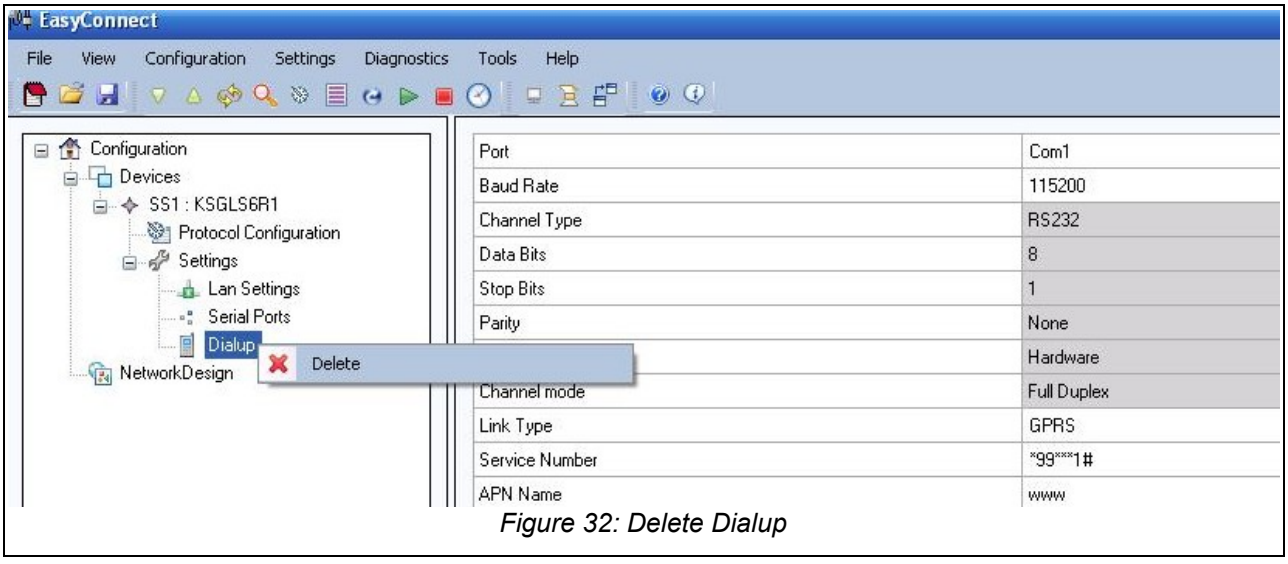


Figure 32: Delete Dialup

To delete the dialup settings from the converter, delete the dialup settings from the configuration window as explained above. Then check the option Dialup settings box in the **Download** command window as shown below and click on **Download.**

Figure 33: Delete converter dialup

3.6 VPN Support

SYNC2000-S6R1 series have option of loading GPRS/ EDGE units (needs to be ordered separately) which allows the users to extend the Ethernet over wireless networks. This allows users to connect and integrate the gateways to remote locations without any distance limitations. Kalkitech M2M gateways can be used with the SYNC2000-S6R1 series to enable secure communication and data transfer via public networks using a virtual private network formed by the SYNC gateways. Virtual Private Network (VPN), provides secure communication between SYNC2000-S6R1 gateways present at different site locations to the single M2M gateway present on the control-center. Data between two ends are encrypted before transmission, making it highly secure.

The SYNC2000-S6R1 will act as VPN clients and connects to the VPN server (M2M Gateway) using its public IP. The client and server uses secret keys and encryption to establish a secure connection. Both client and server will validate the supplied credentials before accepting a connection. After the successful connection establishment, the M2M Gateway will assign an IP addresses to each client gateway. The IP address given to the client Gateways can be pre-configured using the Easy Connect configuration utility. The client can securely communicate with the server using this IP address. A typical network configuration is shown below:

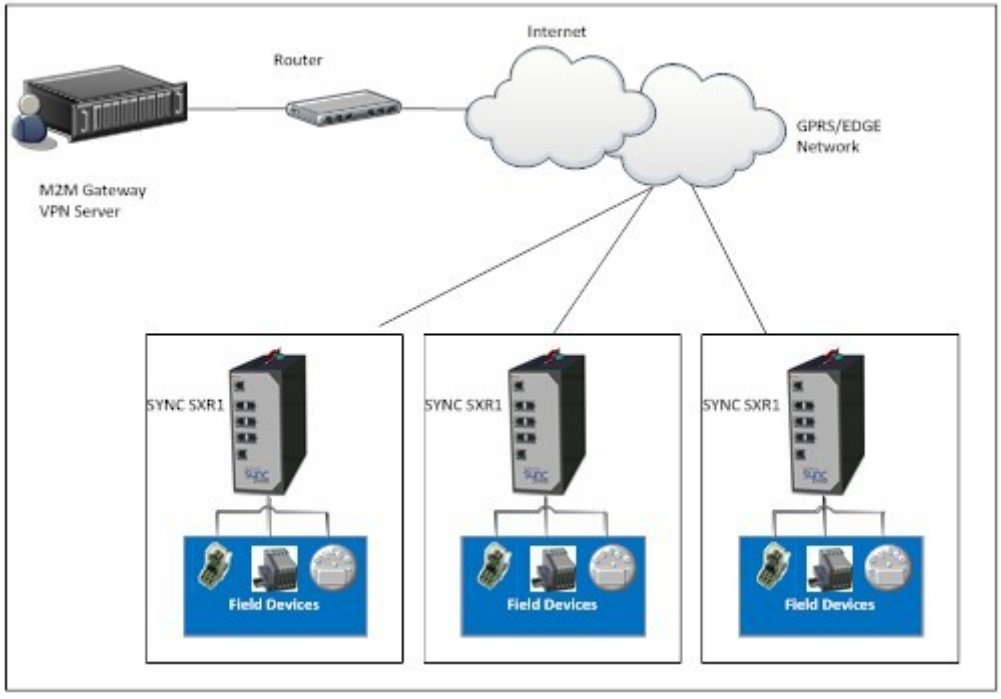


Figure 34: VPN / GPRS network with Kalki Gateways

Configuring VPN:

We can configure VPN (Virtual Private Network) settings for a converter whose configuration has been uploaded in the configuration window.

1. Right-click on the **Network Design** node to get the option **Add VPN** settings.

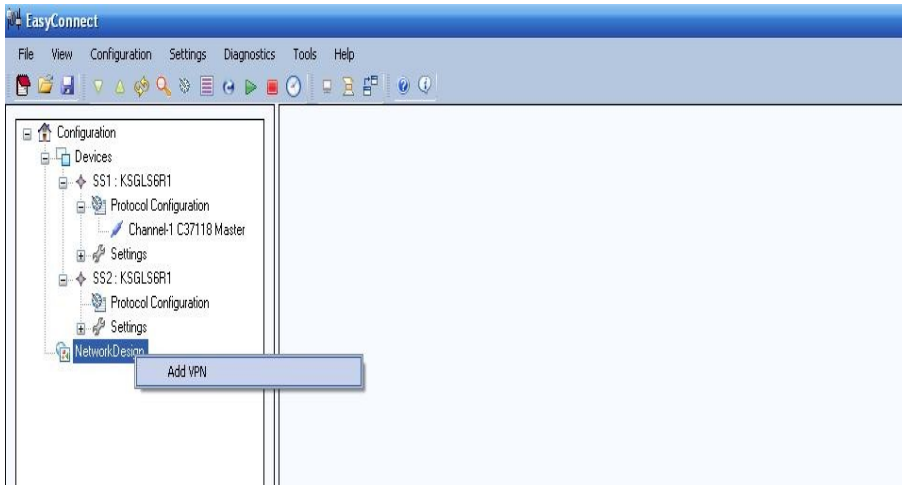


Figure 35: Add VPN

2. Click on **Add VPN** link. A new dialog box will appear as in figure below. Refer VPN Pop-Up Details table for parameter details.

Figure 36: VPN Pop-Up

Parameter name	Range/Optional values	Default value	Description
Country Code	AU, BH ,BR, CA, CN, IN, JP, PK, US	IN	A drop down menu gives an option to set various country codes. Select the required country code
State/Province		Karnataka	This field is for entering the state.
City		Bangalore	This field is for entering the city location.
Organization		Kalkitech	This field is for entering the name of the organization.
E-mail ID		support@kalkitech.com	This field is for entering the e-mail ID

Table 10: VPN Pop-Up Details

These are used for certificate generation purposes only and has no other function.

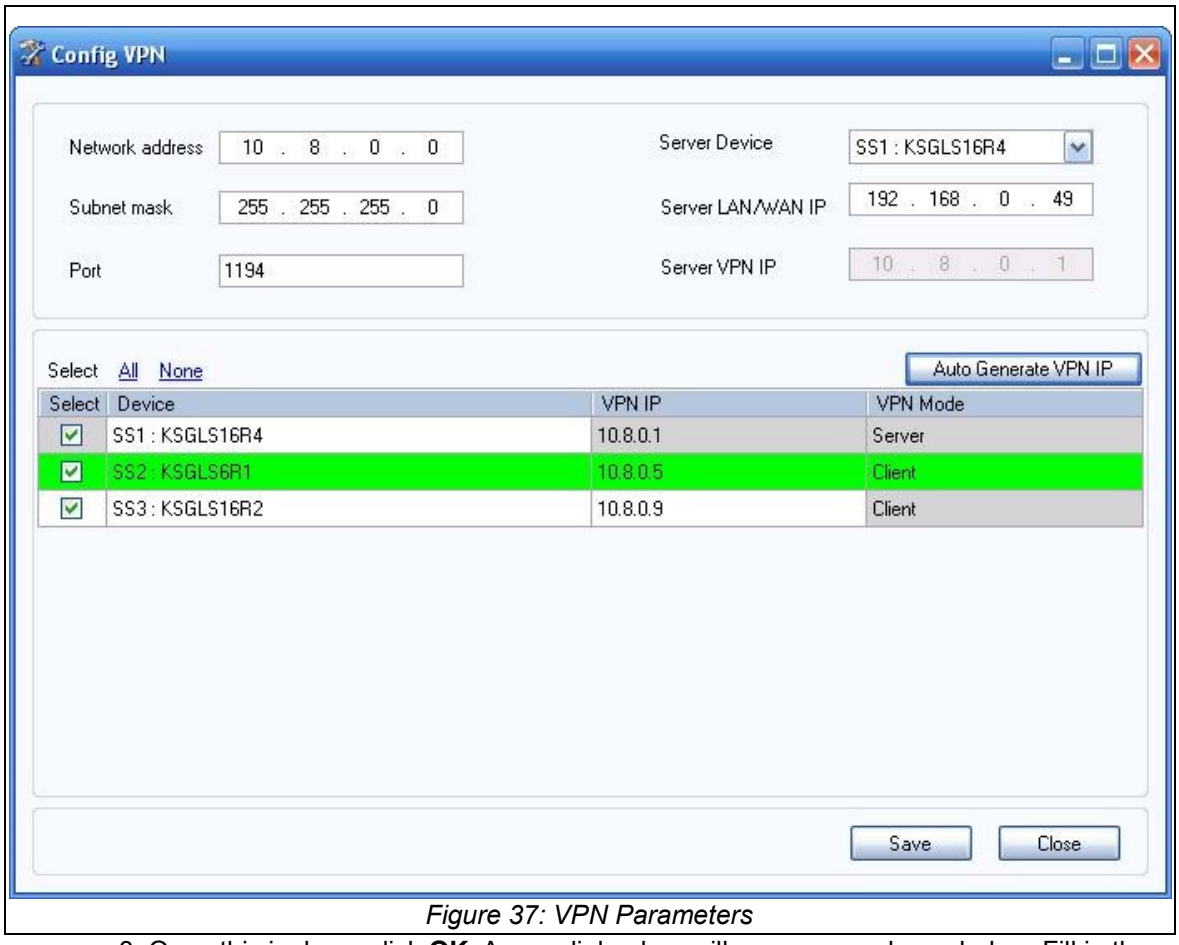


Figure 37: VPN Parameters

3. Once this is done, click **OK.** A new dialog box will appears as shown below. Fill in the

required parameters and click **Save**.

Note: For any VPN configuration one of the devices is configured as server and the rest of the devices operates in client mode.

Parameter name	Range/Optional values	Default value	Description
Network Address:		10.8.0.0	It signifies the IP address template/range over which the VPN IPs can be configured
Subnet Mask		255.255.255.0	A valid subnet address
Port	NA	1194	The UDP port used to establish the VPN connection
.Server Device		SS1 Device	Choose the device you want to set as the VPN Server Device
Server LAN/WAN IP		0.0.0.0	Give the LAN/WAN IP of the VPN server chosen above
Server VPN IP	NA	10.8.0.1	The VPN IP of the server allocated by the system.
Client VPN IP		NA	IP Address address of the VPN clients. This can be generated by clicking the button ' Auto Generate VPN IP'.

Table 11: VPN Parameters

4. The VPN settings are saved to the configuration. To download, right-click the **VPN** node and click the **Download** link that appears as shown below.

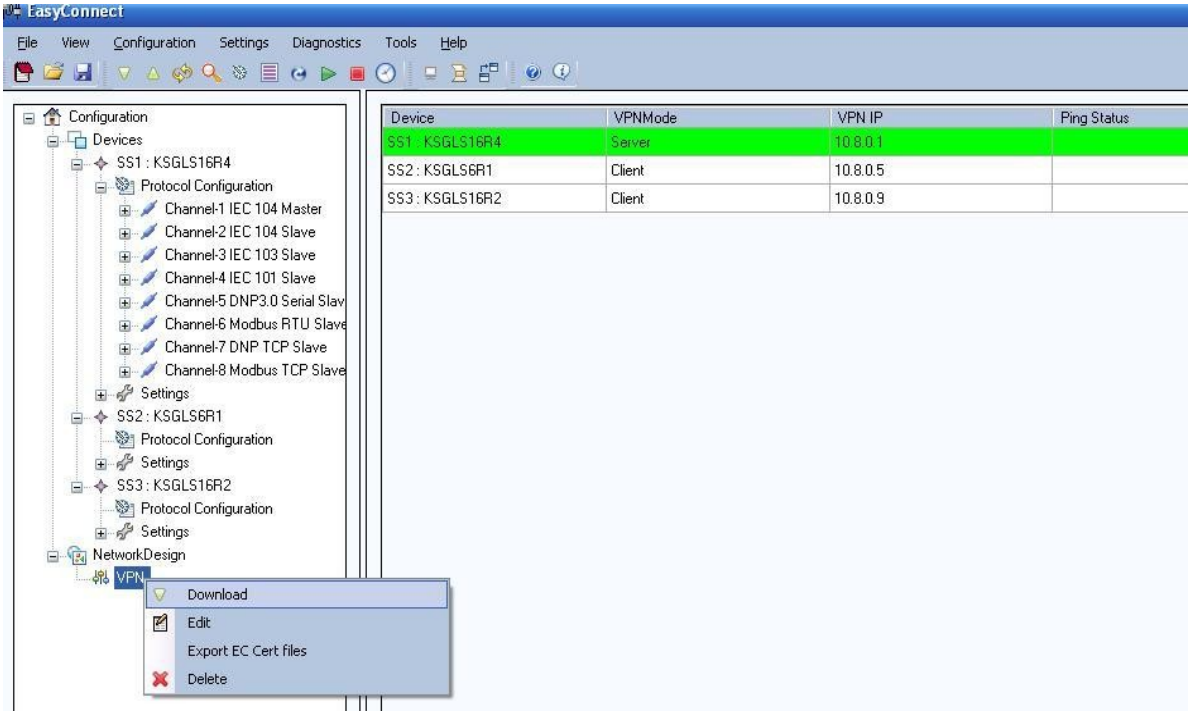


Figure 38: Download VPN

To edit the VPN settings from the configuration window, right click on the **VPN**' node to get the **Edit** link as shown below. Click on **Edit.**.

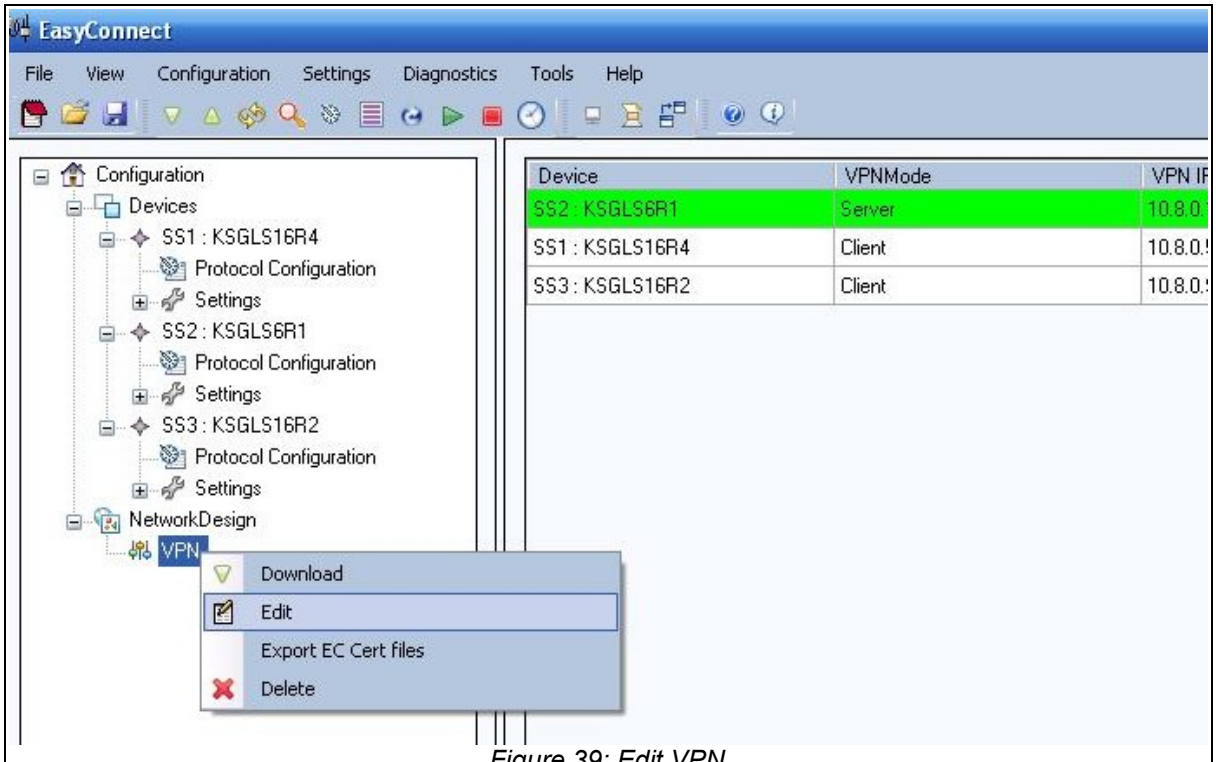


Figure 39: Edit VPN

The following **Config VPN** window will pop up. Make the required changes and click **Save** button at the bottom of the window.

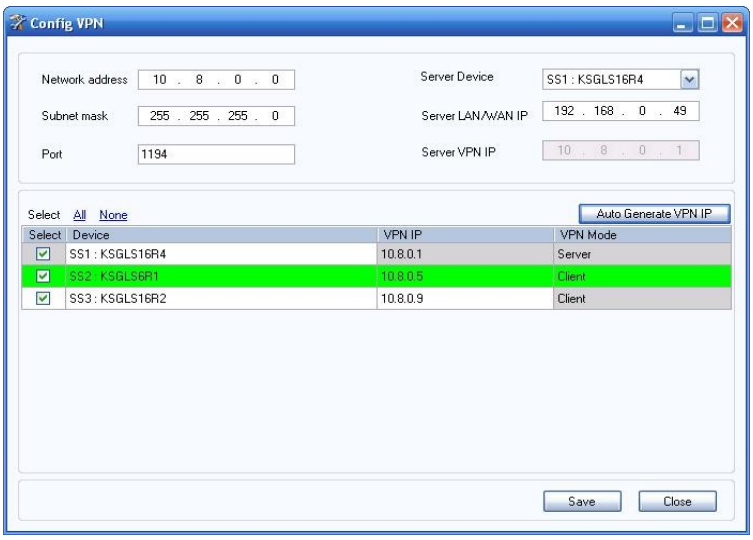


Figure 40: Edit VPN Pop-Up

To delete the VPN settings from the configuration window, right click on the **VPN** node to get the Delete link and then click the **Delete** button.

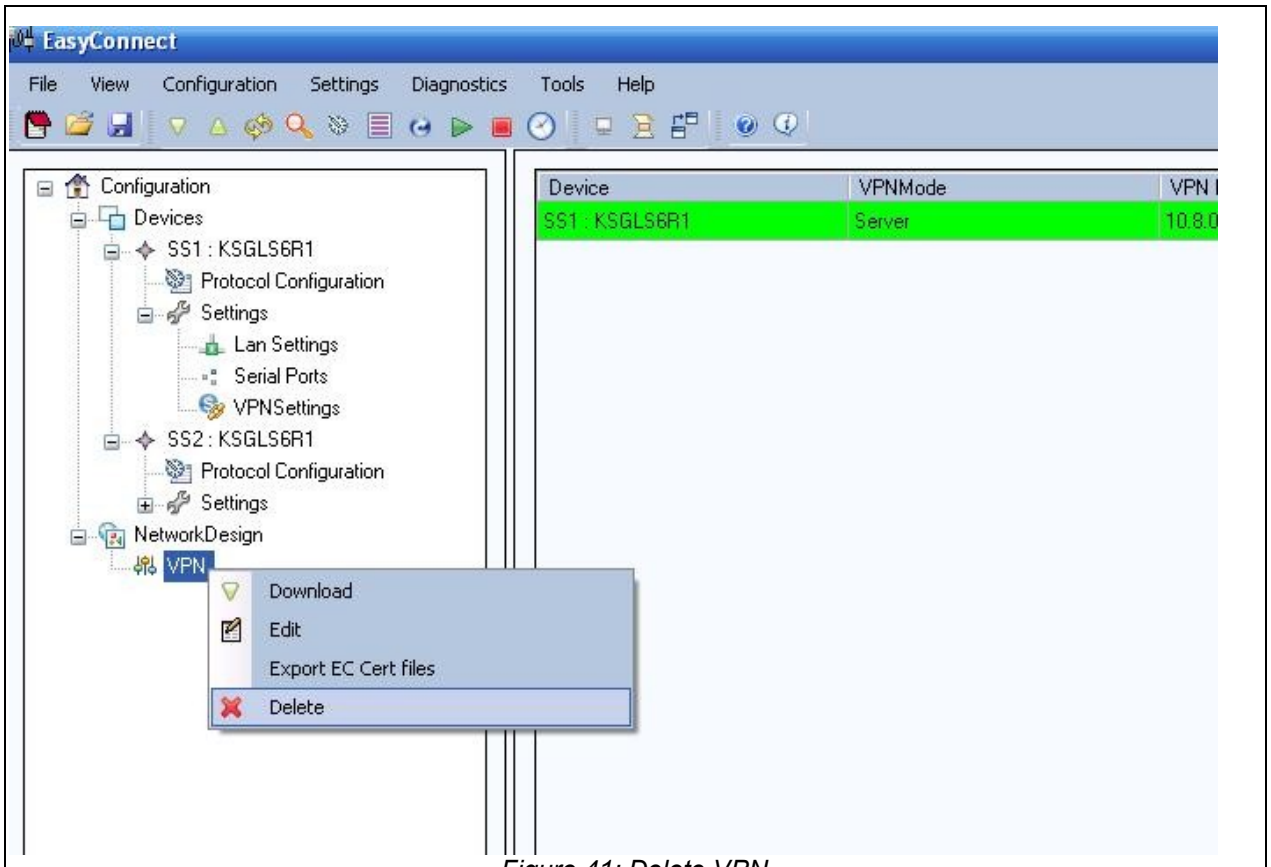


Figure 41: Delete VPN

To delete the VPN settings from the converter, delete the VPN settings from the configuration window as explained above. Then check the **VPN settings** box in the Download command window as shown below and click **Download.**

Figure 42: Delete converter VPN

If necessary, repeat for each converter configured for the VPN network in the project

The SYNC gateways configured in the VPN network becomes part of a private encrypted network. Access to the network is restricted .Under normal circumstances access to the VPN network from the workstation in which EasyConnect is installed is not necessary. So the steps mentioned below are not necessary for normal operation.

To access gateways that are part of a VPN network,requires certain system setup procedures to be completed. To make EasyConnect a part of the VPN network, install OpenVPN on the workstation in which EasyConnect is installed. Now right click on the VPN node to get the Export EC cert files link' as shown below. Click on the link and save the files. Use these files to connect to the VPN network.* Refer to the OpenVPN documentation for information

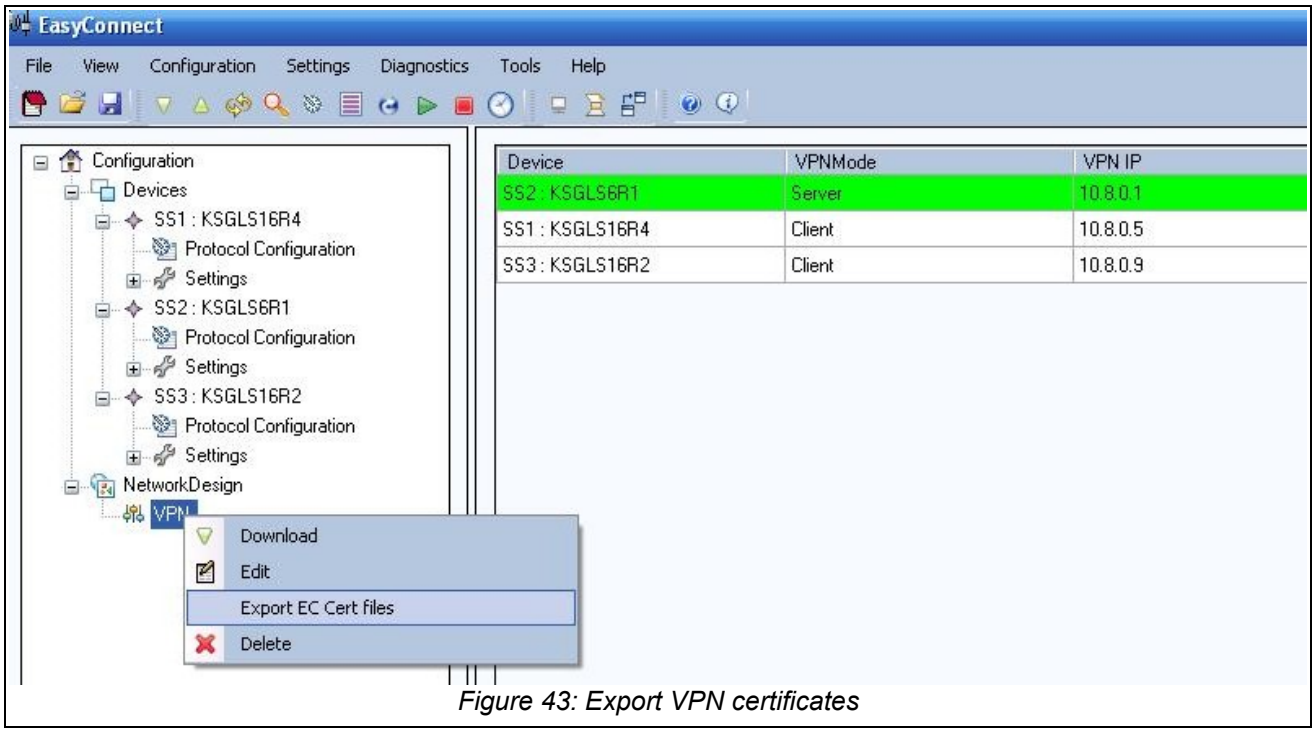


Figure 43: Export VPN certificates

*The set of Easy Connect certificates can be used to configure only one instance of OpenVPN client at a time. Also make sure that the Easy Connect workstation and the protocol gateway are time-synchronized.

Once Easy Connect is a part of the VPN network, we can get the ping status of the converters in VPN mode using the 'Get Device Status' button as shown below.

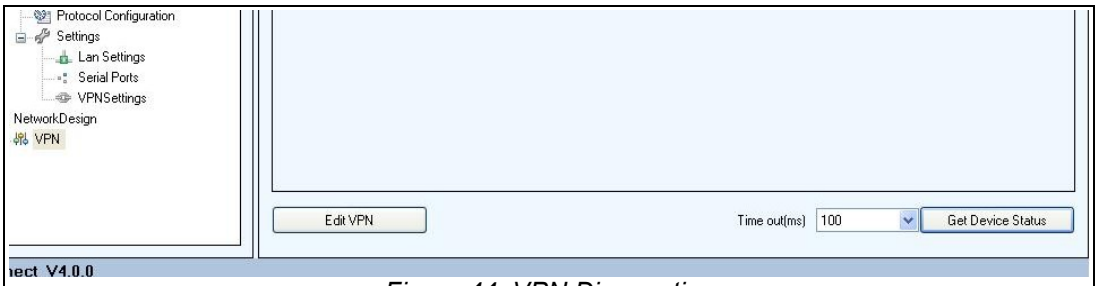


Figure 44: VPN Diagnostics

3.7 SNMP Support

Simple Network Management Protocol (SNMP) is a UDP based network protocol. It helps to manage network-attached devices and make sure they are not only up and running but also performing optimally. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried or set by managing applications.

SYNC specific objects managed by SNMP are Model Name, Hardware Informations, such as Ethernet Interfaces Details, Serial Port Details, Memory Usage etc and Software Informations such as GPC health, DCCP health etc.

3.7.1 ADD SNMP Details

To configure SNMP settings for a gateway

1. Right click on the **Settings** and choose **Add SNMP'** .

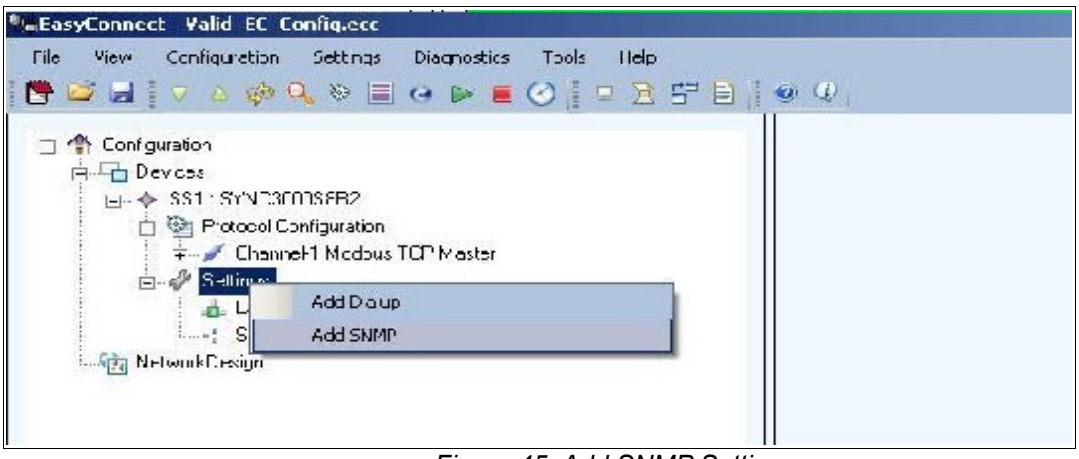


Figure 45: Add SNMP Settings

Fill the common configurable parameters. The parameters are explained below

Parameter Name	Range / Optional Values	Default Value	Description
System Name	255 characters	Depending on the gateway selected.	Name of the managed device being monitored. **Note :** Field is not editable
System Description		Protocol Gateway	Description about the device being monitored. **Note :** Field is not editable
System Location	255 characters	kalkitech	The physical location for the device being monitored.
System Contact		support@kalkitech.com	The interface to be contacted,it can be a mail id .
Read-Write Access		private	Community strings for read-

Community String			write access
Read-Only Access Community String		public	Community strings for read-only access

Table 12: SNMP Parameters

1. To Add User,click **Add User** and Click **Save** button. For details refer figure below

   Fill the common configurable parameters. The parameters are explained below

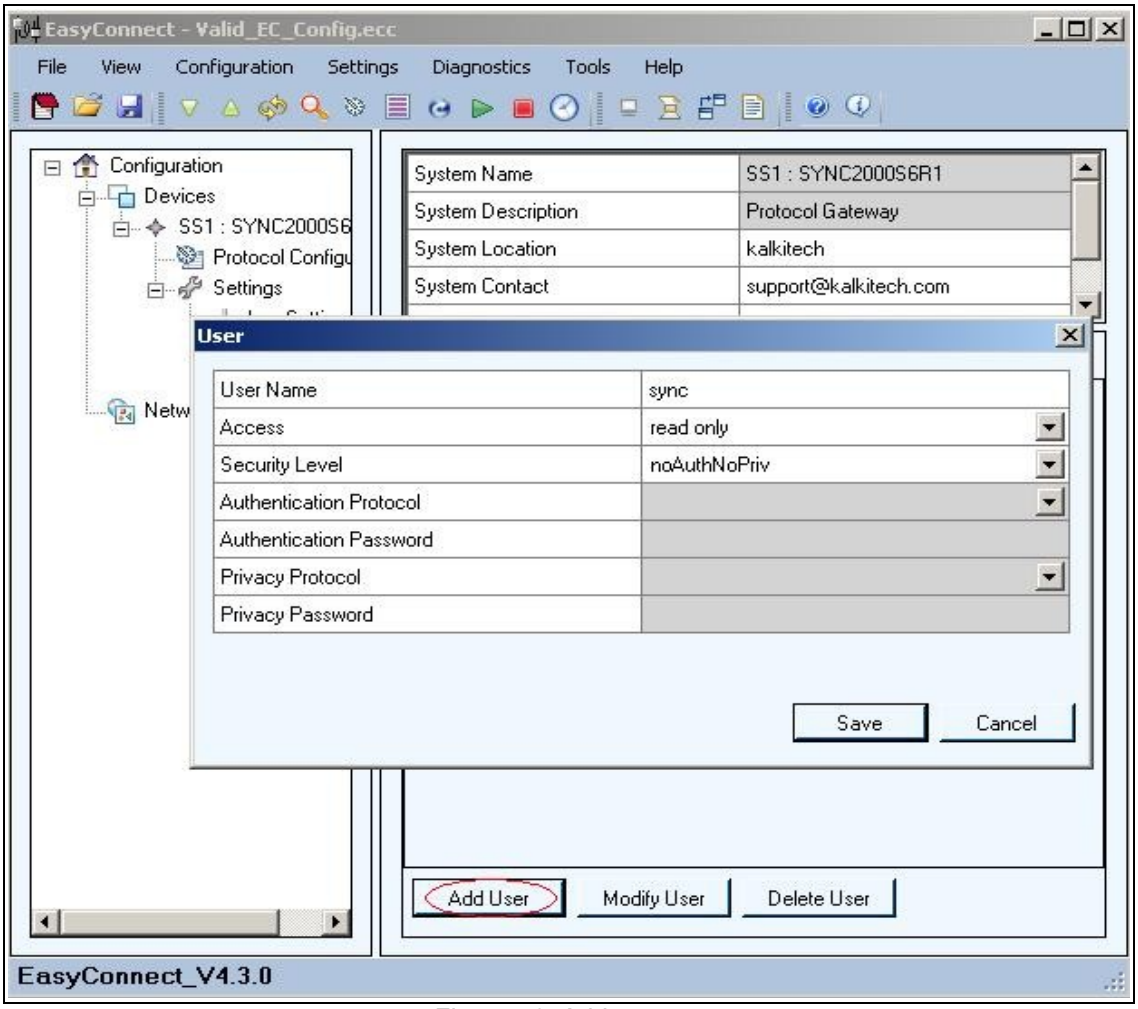


Figure 46: Add user

The parameters in the user window are explained below

Parameter Name	Range / Optional Values	Default Value	Description
User Name	-	sync	This is the textual description of the person responsible for the SNMP entity that is to be managed.
Access	read only / read write	read only	Specifies access level applicable for the user.
Security Level	noAuthNopriv , authNopriv, authpriv	noAuthNopriv	Specifies the security level applicable for the user added. NoAuthNoPriv means no authentication and no privacy, authNoPriv means authentication and no privacy, authPriv means authentication and privacy
Authentication Protocol	MD5 / SHA	MD5	The protocol used for authentication. **Note :** Applicable only when selected 'Security Level' is either authNopriv or authpriv.
Authentication Password	-	passkalkitech	The password used in conjunction with the authentication protocol.
Privacy Protocol	DES / AES	DES	The protocol used for privacy, that is, to encrypt the data portion of the SNMP packet. **Note :** Applicable only when selected 'Security Level' is authpriv.
Privacy Password	-	passkalkitech	The password used in conjunction with the Privacy protocol.

Table 13: SNMP - User Parameters

2. Check the **SNMP settings** box in the Download command window as shown in the figure below and click **Download.**

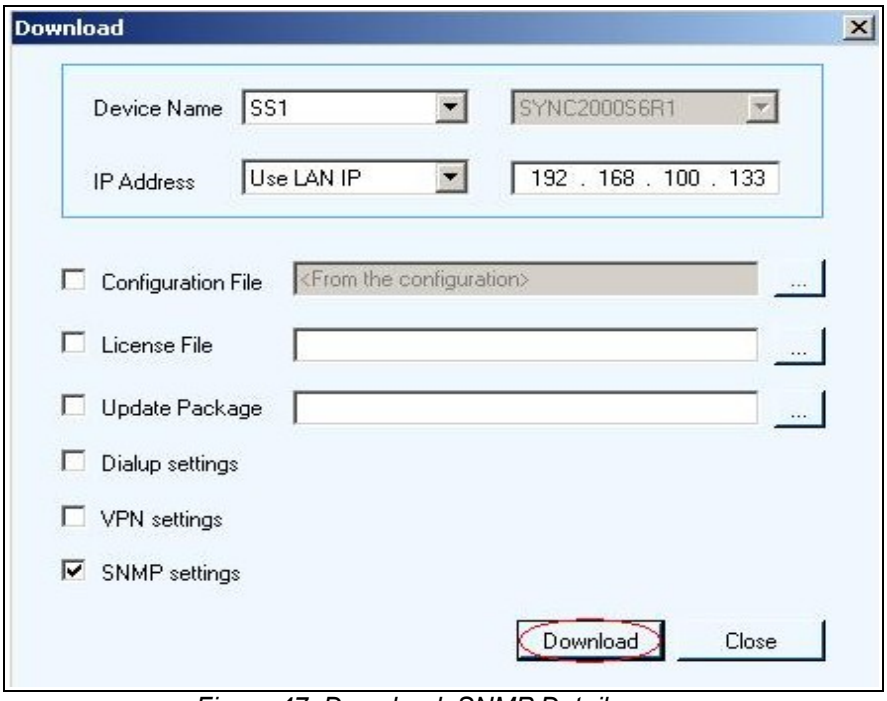


Figure 47: Download SNMP Details

Note : Restart is required after downloading the settings for the changes to take effect.

3.7.2 Delete SNMP Details

To delete the **SNMP** settings from the gateway .

1. Right click on the **SNMP** node and choose **Delete**.

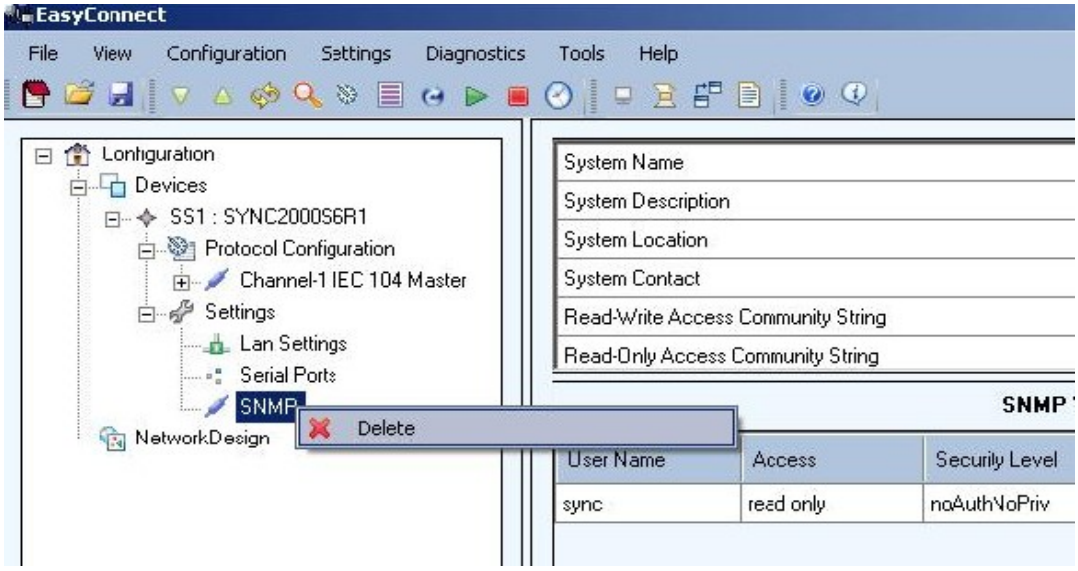


Figure 48: Delete SNMP Configuration

2. Check the **SNMP settings** box in the Download command window and click **Download**.

Note : Restart is required after downloading the settings for the changes to take effect.

4 Downloading Configuration File

You have to download the configured file to SYNC after creation or editing. In case of editing you have to stop and start the firmware for the changes to take effect.

To download the configured and mapped file perform the following steps:

1. On the user interface, click **Download**
   The **EasyConnect-Download** window appears.

2. Click **Download**. The file is downloaded to the SYNC and a corresponding success message is displayed.

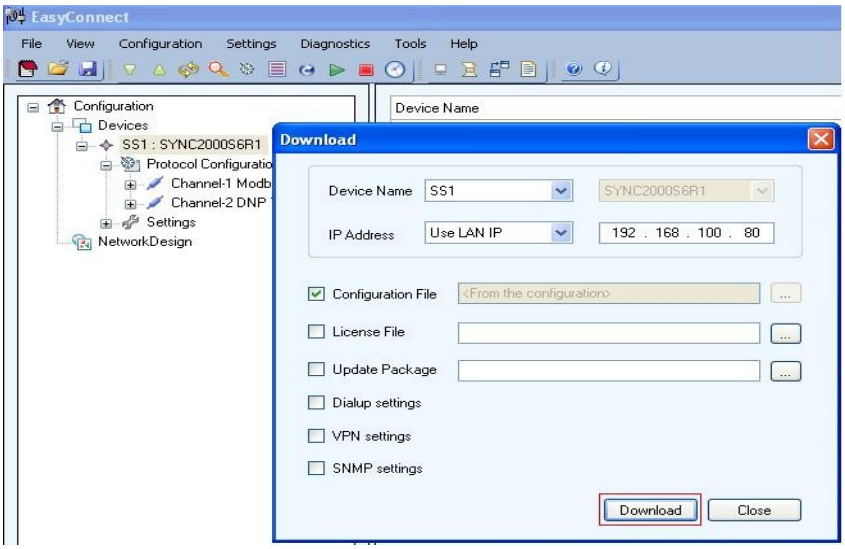


Figure 49: Download Configuration File

5 Redundancy Support

This part of the document describes the implementation of redundancy using SYNC series of protocol gateways.

5.1 Introduction

KALKI Substation Gatewaylite offers several options to create redundant solutions. This section outlines the redundant options one by one. The usage will be described with diagrams and at the end, use cases will be presented to show how combinations of redundant options can be used to create reliable communication systems.

The redundancy mechanism consists of a hot gateway and a warm gateway. The hot gateway is polling the devices and communicates with the control center as it was a stand-alone system. The hot and warm gateways are communicating with each other through an integrated link. Integrated link options supported by SYNC gateways include Serial, TCP, Serial/TCP and Dual TCP links. Out of these integrated link mechanisms, the latter two provide a redundancy for the integrated link also.

5.2 Types of Switchover

SYNC gateways supports the following types of switchover:

5.2.1 External Trigger Switchover

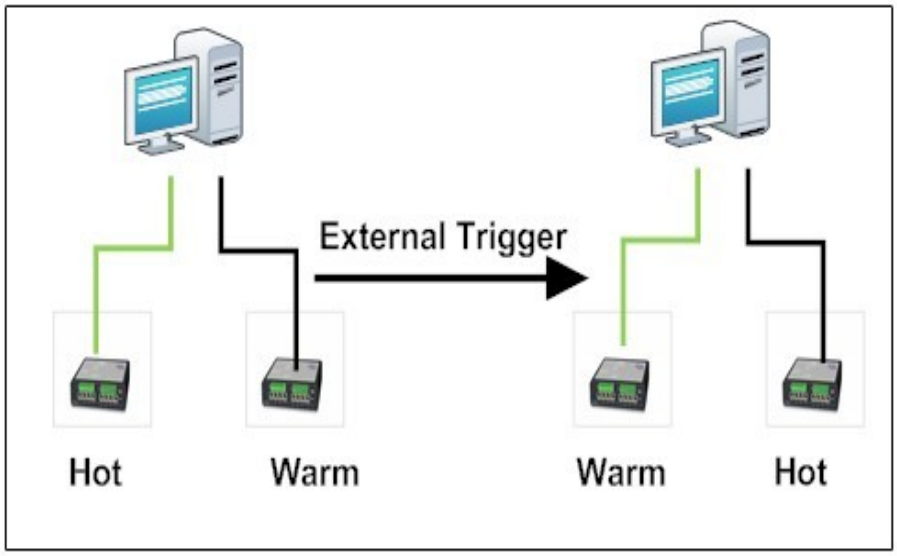


Figure 50: Switchover due to external trigger

In this mode, the gateway will not take a switchover decision on it's own. The switchover is triggered by an explicit command received from external master. To assist in making a decision, the external master can monitor the gateway status via some default status points. Based on this information, the external master can change the gateway state.

5.2.2 Self Switchover

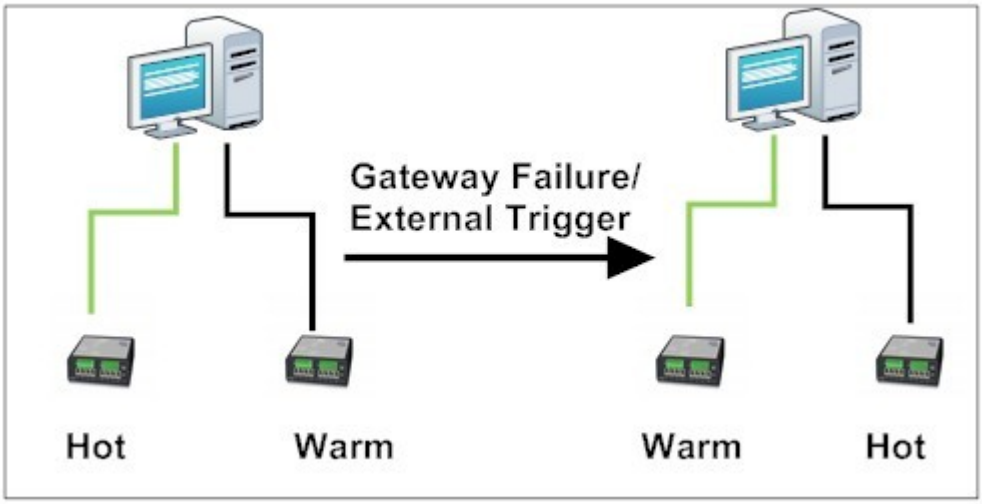


Figure 51: Self Switchover

Self switchover mechanisms extend the functionality of external trigger switchover, by providing provision for making switchover decision from the gateway itself. The gateway monitors the status of all the connected channels, as well as the status of the other gateway (via an integrated link). In this mode, when the warm gateway detects a failure of hot, it changes it's state to hot. Also, a communication failure in active channels of the hot gateway will result in the warm gateway switching to hot.

5.2.3 Redundant Configuration with IP Swapping

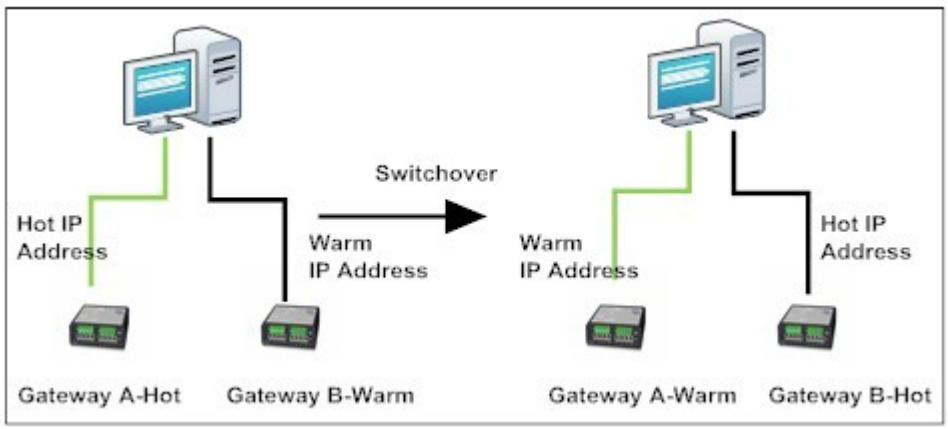


Figure 52: Redundant configuration with IP Swapping

In this mode, the hot and warm gateways share two public IP addresses. Each gateway uses any of them, depending on the state of the gateway. Because of this, the control center can connect to the hot gateway using a fixed address. This ensures that no special network configuration is needed at the control center; in fact when the control center connects to the known IP-address it has no indication which gateway is hot and which one is warm. The warm gateway can also be accessed with it's public IP address, for maintenance purposes.

5.2.4 Redundant Configuration with Alias IP sharing

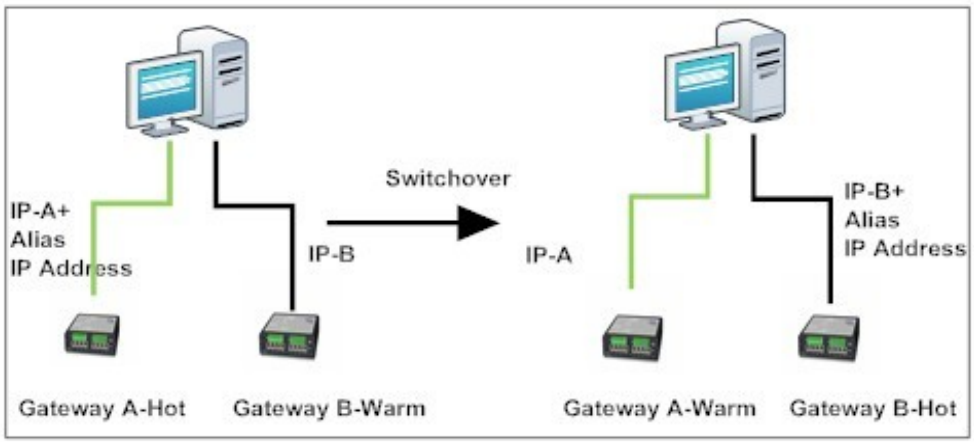


Figure 53: Redundant configuration with Alias IP sharing

In this mode, each gateway has it's own private IP address. Also, both gateways share a public IP address to which the control center can connect. This IP address is set as an Alias IP address for the interface. This ensures that no special network configuration is needed at the control center. When the control center connects to the alias IP-address, it will always connect to the hot gateway. The hot and warm gateways can be accessed with their private IP addresses also, for maintenance purposes.

5.2.5 Redundant Configuration with No IP Switching

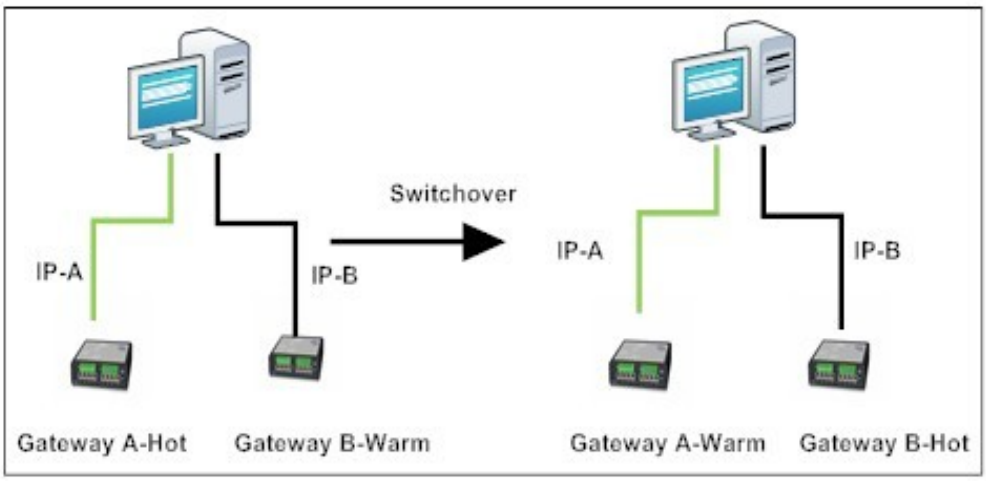


Figure 54: Redundant configuration with No IP Switching

In this configuration, each gateway has it's own private IP address only. This will require special network configuration on the part of the control center. The control center needs to detect the hot gateway, and it should ensure that the correct gateway is being connected after a switchover.

5.3 Redundancy Requirements

One of the gateways should be configured to have the higher priority. This will make the gateway with the higher priority hot when

a. There are no error conditions
b. Both the gateways have the same channel healthiness.

In all other cases, the hot gateway is determined based on the healthiness of each gateways.

- Basic switchover condition is when the hot gateway has a hardware/software failure.
- All serial links are made through Y-cables.
- It is possible to force a switchover.
- Both gateways should have the same hardware configuration. And also Software configuration should be the same, with minor changes in configuration file.
- It is mandatory to have a dedicated link between the two gateways involved in redundant configuration. Also, it is preferable to select an Ethernet link as the dedicated link between two gateways, because of the speed offered by the medium.

5.4 Gateway Redundancy Information and Control

When SYNC are placed in redundant configuration, status information is added to the device database. This information can be accessed by the control center.

The following indications are supported by the gateways.

- Gateway ID: this indication gives the Gateway ID of the connected gateway. This shows whether the gateway is configured as main or standby.
- Gateway Status: this indication gives the Gateway Status of the connected gateway. This shows whether the gateway is currently working as hot or standby.
- IL Communication Status: this indication shows the current communication status of the integrated link. It shows whether the remote gateway is communicating via the integrated link.
- Gateway Healthiness: this indication shows the healthiness information of different channels of the gateway.
- Remote status indication: this indication gives the Gateway Status of the remote gateway. This shows whether the remote gateway is currently working as hot or standby. This information is only valid if the IL communication status indicates that the gateway is on-line.

Apart from this, the SYNC protocol gateway with redundancy support has the following command point for triggering switchover from an external Master.

- External Trigger Point : this command point is used to give the switchover command to the gateway from an external Master.

5.5 Hot-Standby Protocol

The Hot-standby (HSB) protocol is used to maintain a complete up-to-date database on the warm gateway. This feature will copy the internal database of the hot gateway to the warm gateway. Also, all the events received by the hot gateway are mirrored in the warm gateway.

The following points should be noted while implementing a redundant configuration of SYNC using HSB protocol:

- Not all masters support this feature at the moment.
- Not all slaves support this feature at the moment.
- Not all automation functions support this feature at the moment.

5.5.1 Configuration of Hot-Standby

Redundancy can be configured for SYNC by adding an “HSB Master” channel to the EasyConnect. One of the gateways is configured as **Main**, and the other as **Standby**. Details of configuration in EasyConnect is given in table Channel configuration parameters for achieving redundancy.

5.5.2 Channel Configuration

When the user adds a new HSB channel to the configuration, the following window will be shown when the user clicks on “**Channel-n HSB Master**”. This corresponds to the channel parameters of HSB Master.

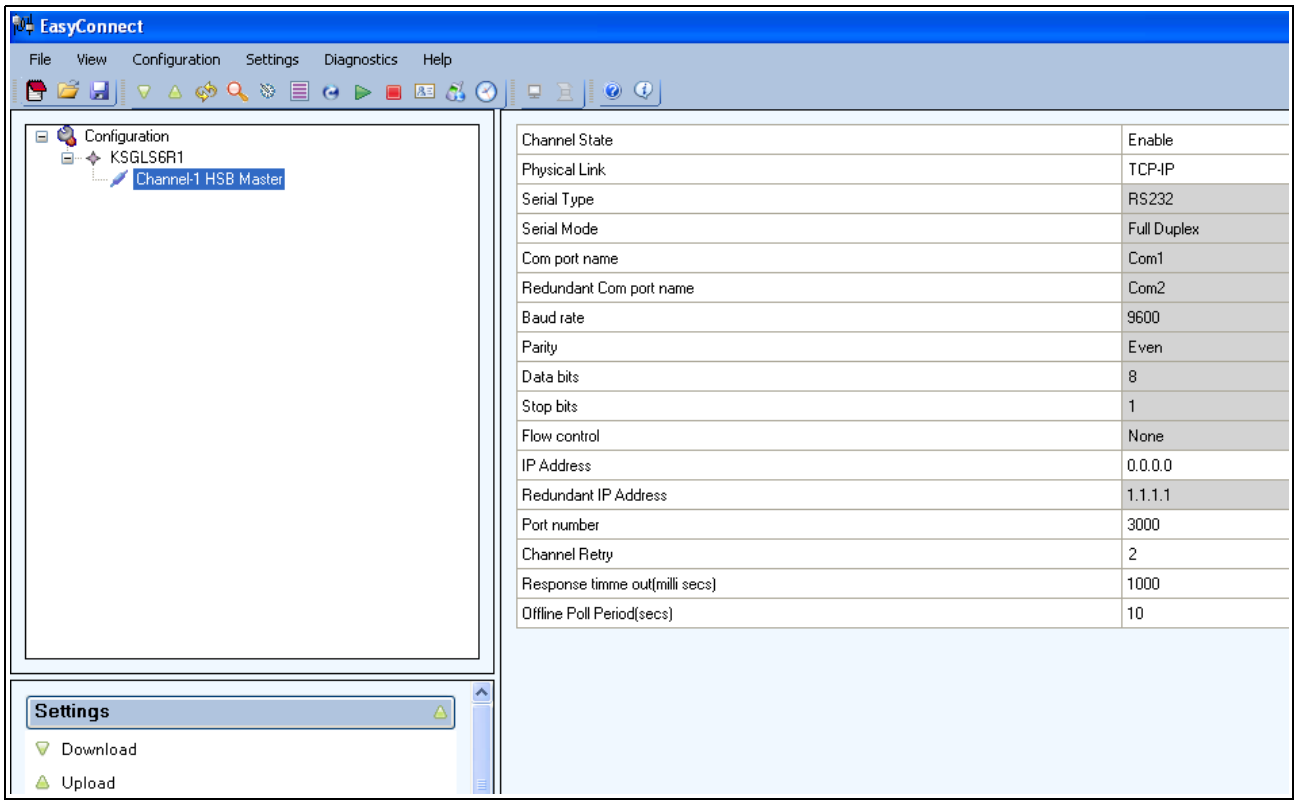


Figure 55: Channel configuration for achieving redundancy

The following tables describes each of the configurable options inside the Channel parameters.

Sl No:	Name	Description	Range	Required Value
1	Channel State	Used to enable or disable the channel	Enable / Disable	Should be configured as “Enable”
2	Physical Link	Used to configure the type of link used for integrated link.	Serial / TCP-IP / Dual / Dual Ethernet / Dual Serial	Dual Serial mode is currently not supported.
3	Serial Type	Serial port type	RS232 / RS485 / RS422	
4	Serial Mode	Mode in which the serial port communicates	Full Duplex / Half Duplex	
5	COM Port Name	Name of the port through which serial communication happens	COM1 - COM10	
6	Redundant COM Port Name	Name of the port which provides a redundant link to #5	COM1-COM10	Should have a different value from #5
7	Baud Rate	Serial communication parameter	An integral value should be provided as baud rate	Should be kept one of the following recommended values: 9600/19200/38400/ 115200
8	Parity	“	Odd / Even / None	
9	Data Bits	“	7 or 8	
10	Stop Bits	“	1 or 2	
11	Flow Control	“	None / Software/ Hardware	
12	IP Address	IP address of the other gateway for TCP-IP/Dual/Dual-Ethernet links	Any valid class-A/B/C IP address	
13	Redundant IP Address	IP address of the redundant TCP link of other gateway for Dual-Ethernet link	Any valid class-A/B/C IP address	
14	Port Number	Port number used for accepting incoming TCP connections on **Main** gateway	Any valid port number	Recommended value is 3000

15	Channel Retry	Number of times an HSB link packet is resend, in case of failure to get an ack.	An integral value	Default value 2
16	Response Timeout	Response timeout in milliseconds, for HSB messages with acknowledgment.	“	Recommended to be kept as multiples of 1000
17	Offline Poll Period	Time interval in seconds, in which a non-communicating gateway is probed to check whether it is alive or not	“	

Table 14: Channel configuration parameters for achieving redundancy

5.5.3 Node Configuration

After the configuration of an HSB channel, we need to add a node under that. The following window will be shown when the user clicks on “**Node_1**”. This corresponds to the node parameters of HSB Master.

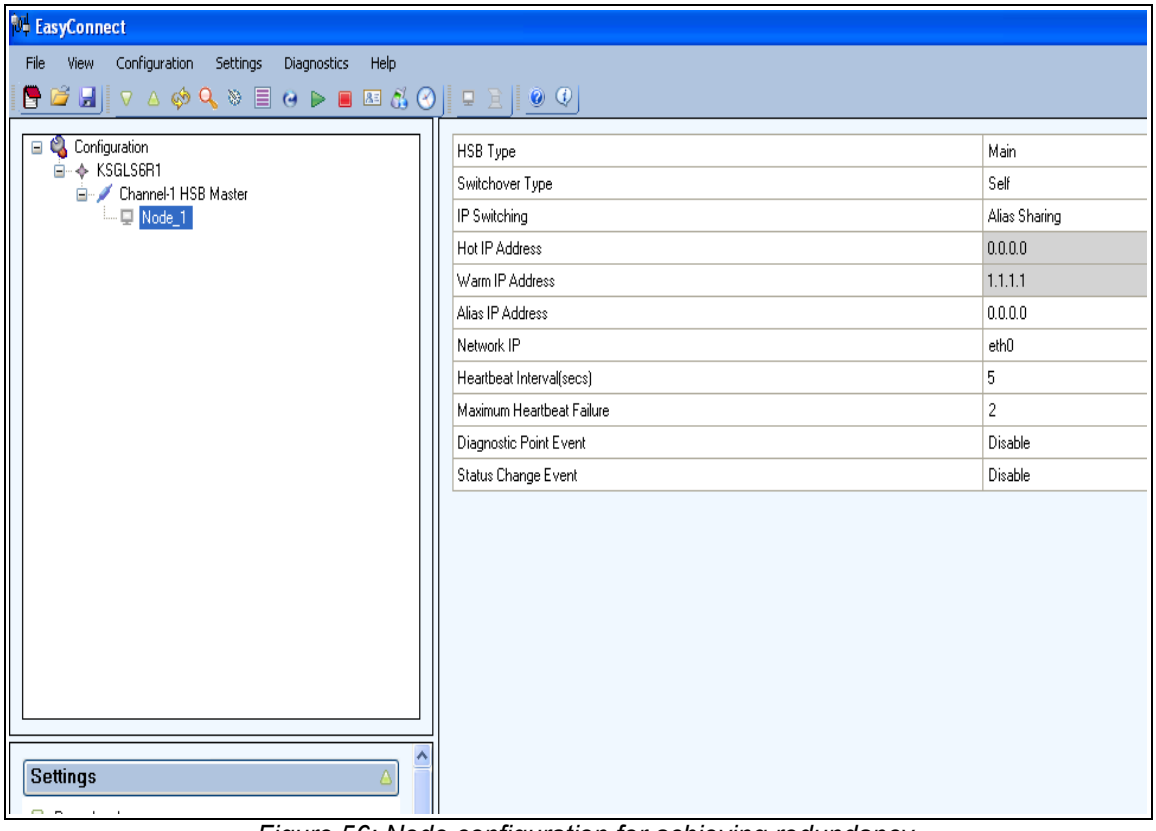


Figure 56: Node configuration for achieving redundancy

The following tables describes each of the configurable options inside the Node parameters

Sl No:	Name	Description	Range	Required Value
1	HSB Type	Used to determine whether the gateway is main or standby	Main / Standby	One gateway should be main and other gateway should be standby always. Failure to do the same will result in redundancy not working properly.
2	Switchover Type	Switchover type for the gateway	External triggered / Self	
3	IP Switching	Used to configure the IP switching mechanism for the gateways	None / Swapping / Alias Sharing	
4	Hot IP Address	IP address of the hot gateway. The IP would be applied to the Network interface specified below	Any valid class-A/B/C IP address	
5	Warm IP Address	IP address of the warm gateway. The IP would be applied to the Network interface specified below	“	
6	Alias IP Address	IP address of the alias interface on gateway. The alias interface would be made on the Network interface specified below	“	
7	Network IP	Used to select the interface to which the IP switching mechanisms are applied	Eth0 / Eth1	
8	Heartbeat Interval	Time interval in seconds, in which each gateway sends a keep-alive message to other one.	An integer value	The switchover time in case of an integrated link failure is determined by (Heartbeat Interval * (Maximum Heartbeat Failure + 1)). So, these values should be designed optimally to suit the application.
9	Maximum Heartbeat Failure	The maximum number of heartbeat failures which are tolerated by each gateway, before changing the other gateway's status as offline	“	This parameter is recommended to have the following values: TCP-IP/Serial – 1 Dual links – 2
10	Diagnostic Point Event	Enable diagnostic point events	Enable / Disable	

11	Status Point Event	Enable status point events	Enable / Disable	

Table 15: Node ParametersProfile Configuration

The following table lists the status points and command point supported by HSB master. With these points, the user can monitor the status of both gateways, and issue external switchover commands to the gateway.

Sl No:	Name	Description	Type	Required Value
1	Gateway ID	Used to determine whether the gateway is main or standby	Binary Input / Analog Input	0 → Main Gateway 1 → Standby Gateway
2	Gateway State	Used to determine whether the gateway is currently Hot or Warm	Binary Input / Analog Input	0 → Warm 1 → Hot
3	External Trigger Point	Used to give Switchover command to the gateway	Binary Output / Analog Output	0 → Switch to Warm 1 → Switch to Hot
4	IL Communication Status	Status point showing whether the other gateway is Online or Offline	Binary Input / Analog Input	0 → Offline 1 → Online
5	Gateway Healthiness	Shows the health of the channels running inside the gateway.	Analog Input	Bit 0 → Unused Bit 1 → Channel 1 …. …. Bit 15 → Channel 15
6	Gateway State	Used to determine whether the other gateway is currently Hot or Warm	Binary Input / Analog Input	0 → Warm 1 → Hot

Table 16: Profile configuration details for redundancy

Redundancy Switchover Details:

S.No	Failure	G/w Action	G/w A	G/w B	DCS Alarm Annunciation
	Normal operation	-	Hot	Warm	
1	Gateway A Power fails	Change over at Gateway level	Power Off	Hot	Gateway A Failure...!
2	Downstream communication fails in Gateway A	Change over at Gateway level	Warm	Hot	
3	Upstream communication fails in Gateway A due to Ethernet link removal	Change over at Gateway level	Warm	Hot	
4	Upstream communication fails in Gateway A, not caused by Ethernet link removal	-	Hot	Warm	
5	Partial failure of integrated links between the gateways (relevant only for Dual integrated links)	-	Hot	Warm	
6	Complete failure of integrated link between the gateways	Both gateways become hot	Hot	Hot	Gateway Failure...! Critical alarm
7	Issuing changeover request from the master to Gateway A	Change over at Gateway level to the requested state	Warm	Hot	

Table 17: Redundancy switchover details

6 NERC-CIP Support

SYNC2000-S6R1, SYNC3000-S8R2, SYNC3000-S16R2, SYNC3000-S16R4 gateways provide NERC-CIP standard compliance as an optional purchase. In gateways having NERC-CIP compliance, only the ports and services essential for normal and emergency operations of the device are enabled by default. Event logging is provided in gateways for all user actions through EasyConnect and web-server. These logs are kept for at least 90 days. Older logs will be automatically erased from the device. Users can retrieve this log using EasyConnect.

Retrieving Gateway Access Log

The gateway access log can be retrieved for a selected period. Steps to upload the log are as follows:

- Choose **Gateway Access Log** from **Diagnostics** menu, A pop-up window named **Gateway Access Log** appears

Figure 57: Retrieve Gateway Log

- Choose the device name, model and type the IP address of the device in the corresponding fields.
- Choose the start date and end date between which you want to take the log.
- Type the file name to save the log and click the button **Get Log**
- Now the Log will be saved to your PC and it will show a message that the log is successfully saved.

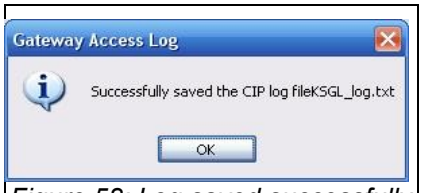


Figure 58: Log saved successfully

7 File Transfer Support

Kalkitech protocol gateway models SYNC2000-S6R1, SYNC3000-S8R2, SYNC3000-S16R2 and SYNC3000-S16R4 have support for uploading and downloading all kinds of files through the File Transfer channel, if they are supported in the firmware. File transfer is done by configuring a File Transfer Master/Slave channel through EasyConnect.

File transfer master channel is able to connect with FTP/SFTP server programs running on a given remote system and upload/download files and folders. File transfer master configuration includes a schedule and file/folder details. File transfer slave will setup FTP/SFTP sever inside the gateway to which FTP/SFTP clients can connect. There is a folder size limiting functionality implemented for these protocols, which helps in keeping the given folders within a maximum size.

Following is a brief description of the steps involved in configuring a File Transfer master/slave channel in EasyConnect.:

7.1 Configuring File Transfer Master Channel

The steps for configuring File Transfer Master channel are as follows:

- Choose **File Transfer Master** from **Add Channel** menu in **Protocol Configuration**
- Type **Remote IP Address** in which FTP/SFTP server is running
- Select **Protocol Supported** and type **Port No** in the corresponding fields.
- Now right click on the **File Transfer Master** channel and choose the option **Add Station**.
- In the **General** tab of node parameters, select **Authentication Scheme**, type **user name**, **password** and type the **Connection Timeout.**
- In **Scheduled Transfer** tab, add a schedule by specifying the time period for the scheduled transfer to run. You can add as many schedules as required.

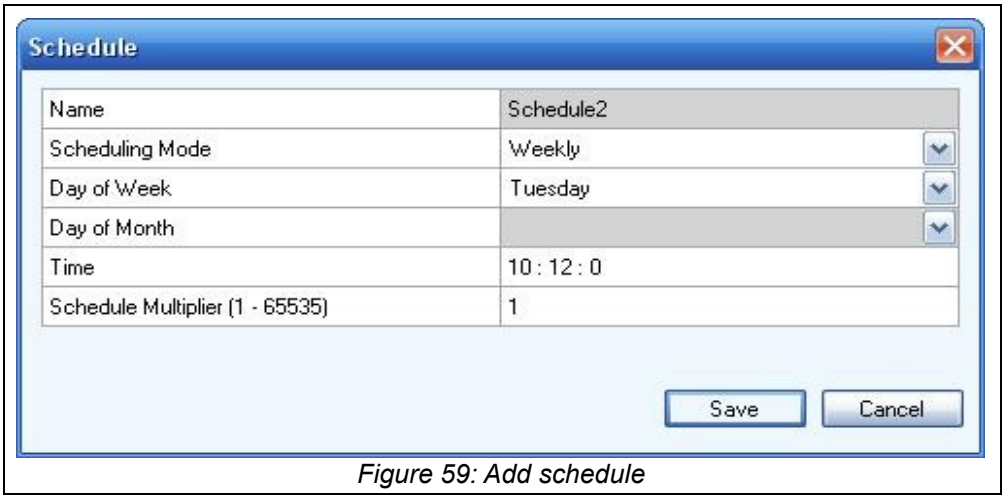


Figure 59: Add schedule

- Now click on the schedule under which you want to add a transfer task. Add a new transfer by specifying the transfer details.

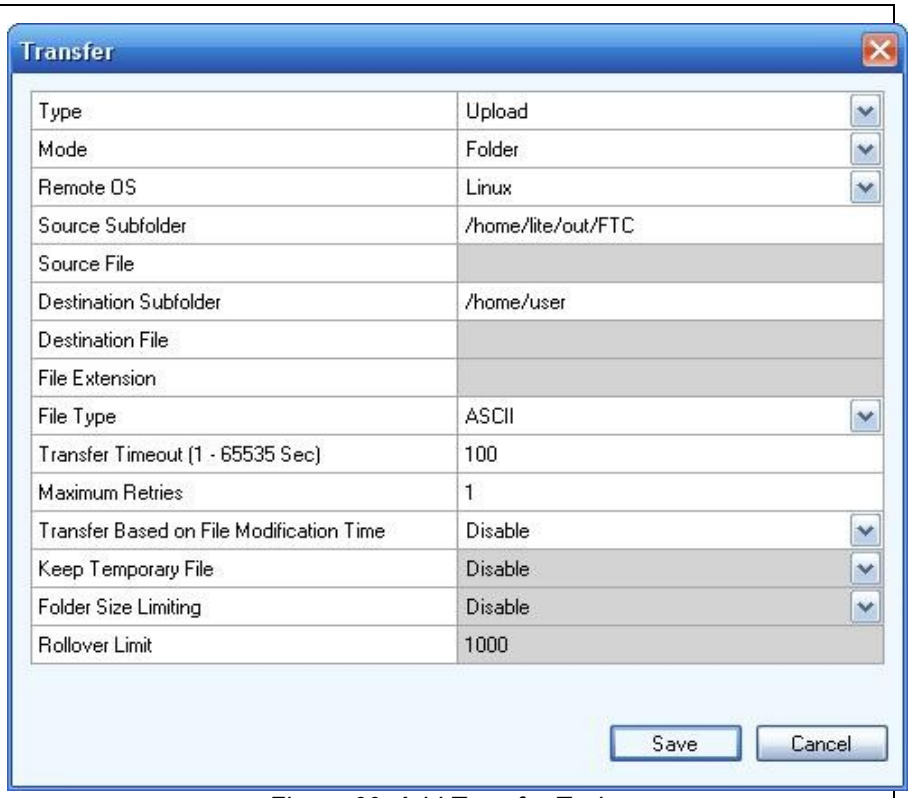


Figure 60: Add Transfer Task

7.2 Configuring File Transfer Slave Channel

Steps for configuring file transfer slave are as follows:

- Choose **File Transfer Slave** from **Add Channel** menu in **Protocol Configuration**
- Select Protocol Supported, type **Listen Port** and **Inactivity Time Period** in the corresponding fields.
- Now right click on the **File Transfer Slave** channel and choose the option **Add Station**.
- In the **General** tab of node parameters select **Authentication Scheme**.
- In the **Users List** tab, add users by specifying **User name** and **Password**. The remote clients can use them for password authentication.

Figure 61: Add User

- In **Size Limit** tab add a schedule for running size limiter by specifying the time period. You can add as many schedules as required.

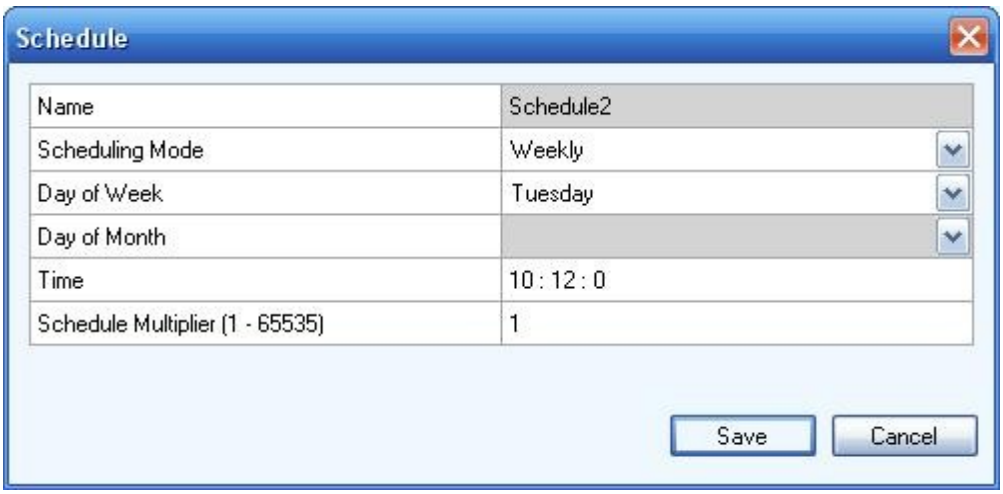


Figure 62: Add Schedule

- Now click on the schedule and add folder by specifying the **Folder Name** and **Rollover Limit**. The size of the specified folder will be checked and limited to the rollover limit in the scheduled interval.

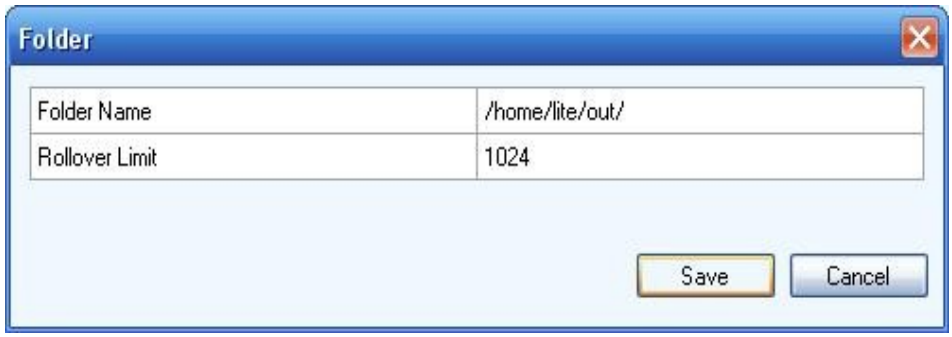


Figure 63: Add Folder

8 Parametrization through Pass-Through (Transparent) Channel

This module in the SYNC protocol converters enables to parametrize the relays or IEDs with the particular configuration software for the relay/IED. The transparent channel(pass-through) routes the frames directly from the input(server) port to the output(client) port and in the reverse direction. The Transparent Peer protocol can be associated to either any of the serial communication port of the SYNC or a TCP/IP client por. The SYNC models must be loaded with the license and firmware supporting Transparent Peer interface module, and the configuration file containing all the specific information for the communication. The detailed block diagram is shown in the figure below:

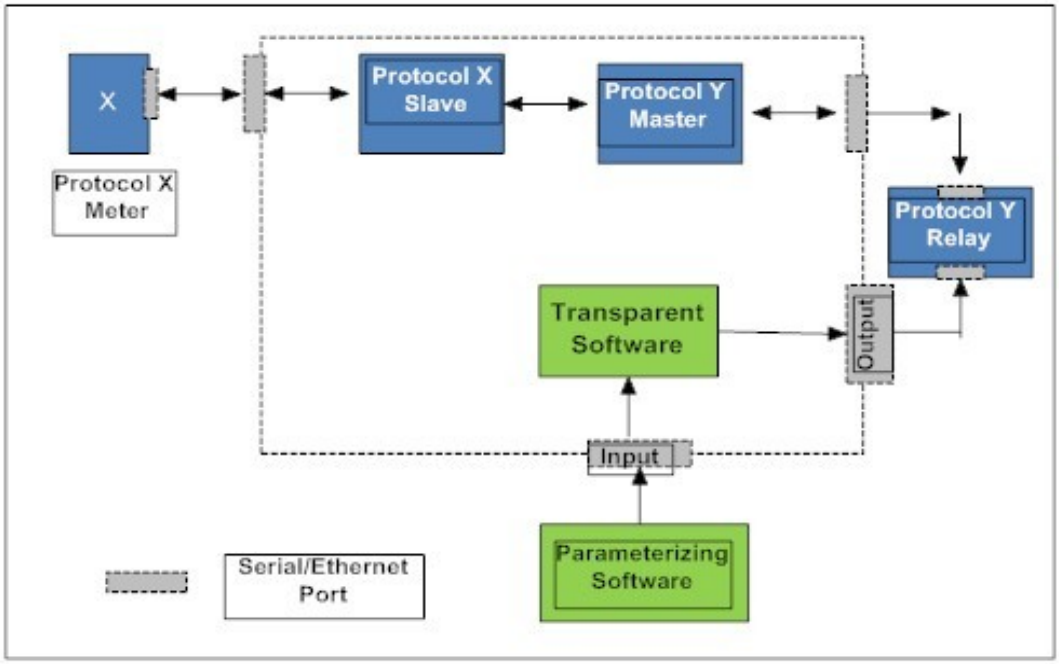


Figure 64: Parametrization through transparent channel

9 Advanced User Configurations

SYNC supports login to the unit over telnet. The “login” and “password” is preset before shipment and is available from support@kalkitech.com on request and through fax.

Using the root login, advanced administration and trouble-shooting can be carried out. The root user can set the SYNC to a predefined IP address manually. You can also set-up predefined routing for the IP address in a LAN/WAN scenario as well as setup DHCP connection if required.

The root login also permits for starting and stopping the protocol engine inside the SYNC. Please contact support@kalkitech.com for detailed information.

Appendix A - Special Case: Configuring PPP, IEC 61850 Server and ICCP peer

PPP is supported on our converters, but the customer has to specify separately in the order. The PPP configuration files are provided separately, which can be downloaded after modification into the converter at the specified locations.

Configuration of IEC61850 Server in EasyConnect has got some variation from configuration of other channels. The following procedure has to be done for the same.

1. Add IEC61850 server channel in EasyConnect.
2. The ICD file is created using SCL Manager and is saved in a file location.
3. You can select the configured ICD file from EasyConnect and add it to the profile.
4. Generate MMS tags for mapping.
5. Add stations and channels as described in the document.
6. Download the configured file to SYNC.

Configuration of ICCP Peer in EasyConnect has also got some variation from configuration of other channels. The following procedure has to be done for the same.

1. Add ICCP Peer channel in EasyConnect.
2. To configure ICCP, right-click and select Configure ICCP Utility.
3. The ICCP configuration file with local control center and remote control center with its association and bilateral table information is created using *ICCP Configuration utility* and is saved in a file location.
4. You can select the configured iccp file from EasyConnect and add it to the profile.
5. To generate Nodes, right-click the channel will create the client and server nodes automatically by reading the ICCP Configuration file.
6. Download the configured file to SYNC.

Appendix B – Flag conversion in SYNC

When a protocol conversion is achieved using SYNC, the quality flag conversion between the protocols has to be defined. The table below is used to explain the quality flag translation between protocols inside SYNC. The flags received in any of the SYNC-Master Protocol (SYNC Master) will be translated to the specific flag of SYNC-Slave Protocol (SYNC Slave) as in the table given below:

KSGL-Slave Protocol		IEC 101/104							DNP 3.0									IEC 103			Modbus	IEC 61850										
		OV	BL	SB	NT	IV	EI	On link failure (Not protocol flag)	Roll-over (Counter)/Over-range (Analog)	Local forced data	Communication lost	On-line = 0	Restart	Remote forced data	Chatter filter	Reference check	On link failure (Not protocol flag)	OV	ER (MVAL Invalid)	On link failure (Not protocol flag)	On link failure (Not protocol flag)	Validity = Questionable & Detail quality = Old data	Validity = Invalid & Detail quality = Oscillatory	Validity = Invalid & Detail quality = Failure	Validity = Invalid & Detail quality = Bad Reference	Validity = Questionable & Detail quality = Inaccurate	Validity = Questionable & Detail quality = Inconsistent	Source = Substituted	Blocked	Validity = Invalid & Detail quality = Overflow	Validity = Invalid & Detail quality = Out of Range	On link failure (Not protocol flag)
IEC 101/104	OV	X							X									X												X	X	
	BL		X																										X			
	SB			X						X				X														X				
	NT				X			X			X						X			X	X	X										X
	IV					X		X				X					X		X	X	X		X									X
	EI						X																									
DNP 3.0	Roll-over (Counter)/Over-range (Analog)	X							X									X												X	X	
	Local forced data			X						X																		X				
	Communication lost				X			X			X									X	X	X										X
	On-line = 0					X		X				X							X	X	X			X								X
	Restart												X																			
	Remote forced data													X																		
	Chatter filter																						X									
	Reference check															X									X							
IEC 103	OV	X							X									X														
	ER (MVAL Invalid)				X	X		X			X	X	X				X		X	X	X	X		X						X	X	X
IEC 61850	Validity = Questionable & Detail quality = Old data				X			X			X						X			X	X	X										X
	Validity= Invalid & Detail quality = Oscillatory														X								X									
	Validity= Invalid & Detail quality = Failure					X		X				X					X		X	X	X			X								X
	Validity = Invalid & Detail quality = Bad Reference															X									X							
	Validity = Questionable & Detail quality = Inaccurate												X													X						
	Validity = Questionable & Detail quality = Inconsistent																										X					
	Source = Substituted			X						X				X														X				
	Blocked		X																										X			
	Validity= Invalid & Detail quality = Out of Range	X							X									X												X	X	

All fags described in the table are considered to be set and the following translation is applicable, unless specified otherwise

1 See quality description details in section 7.2.6.3 and 7.2.6.4 of IEC 60870-5-101.
2 See DNP V3.00 Data Object Library – FLAG details given in each objects
3 See details in section 7.2.6.8 of IEC 60870-5-103
4 See details in section 6.2 of IEC 61850-7-3.

Appendix C – Model Mapping Details

The following table contains the details of old models of Kalki protocol gateways and corresponding new model names.

Old Model name	New Model name
KSGL-S2R1, S4R1, S6R1	SYNC2000-S6R1
KSGL-S4R2	SYNC3000-S4R2
KSGL-S8R2	SYNC3000-S8R2
KSGL-S16R2	SYNC3000-S16R2
KSGL-S16R4, R4I	SYNC3000-S16R4