SIEMENS

3G OTU

IP ROUTERS INSTALLATION GUIDE

Jun-19

Issue 4

667/CI/45025/000

Contents

List of Figures

List of Tables

Health and Safety Protection

Installation and Maintenance Personnel

In the interests of health and safety, when installing, using or servicing this equipment the following instructions must be noted and adhered to:

(1) Only skilled or instructed personnel, with relevant technical knowledge and experience, who are also familiar with the safety procedures required when dealing with modern electrical/electronic equipment, are to be allowed to use and/or work on this equipment. All work shall be performed in accordance with the local regulations[1,2].

(2) Such personnel must take heed of all relevant notes, cautions and warnings in this Handbook and any other Document or Handbook associated with the equipment including, but not restricted to, the following:

i. The equipment must be correctly connected to the specified incoming power supply.
ii. Only trained / competent persons should work on this equipment.
iii. Any power tools must be regularly inspected and tested.
iv. Any personnel working on site must wear the appropriate protective clothing, e.g. reflective vests, etc.

Road Users

It is important that all personnel are aware of the dangers to road users that could arise during repair and maintenance of traffic control equipment.

Ensure that the junction area is coned and signed as necessary to warn motorists and pedestrians of any dangers and to help protect the personnel working on the site.

[1] For UK this refers to Electricity at Work Regulations 1989.
[2] For DE this refers to GV A3, DIN EN 50110-1 (VDE 0105-1) and VDE 0832 and the work-safety leaflet ASM 0099-01

Handling Precautions

Handling

- Take care not to 'kink' the cable when installing. The impact may manifest in poor return loss.
- Due to the cable thickness the RF cable the minimum bend radius of 25cm must be observed
- It is recommended that RF connectors exposed to the environment are protected using amalgamating Tape, and electrical tape

1. Introduction

1.1. Purpose

This User Guide gives a general description for the range of IP router used by Siemens ITS. This document either outlines the general procedures for installation, commissioning and maintenance or refers to appropriate and applicable documents.

1.2. Document References

External Document References	
667/HB/31601/000	UTMC OTU/ MOVA Handbook
667/HB/32600/000	GEMINI² Traffic Outstation Handbook
667/AY/45025/000	3G/4G OTU Communications Site Selection Guide
667/DZ/31601/000	Family Tree
667/CI/32630/000	Gemini MK2 3G/4G Conversion GUIDE
667/CI/52251/000	Stratos Outstation 3G/4G Comms Installation QS Guide

Table 1 : External Document References

1.3. Key Terms and Abbreviations

	Key Terms and Abbreviations
PSTN	**P**ublic **S**witching **T**elephone **N**etwork
GSM	**G**lobal **S**ystem for **M**obile communication (This Usually Refers to 2nd Generation, 2G Networks)
GPRS	**G**lobal **P**acket **R**adio **S**ervice, Used on, 2G networks as a packet data service.
2G	Second Generation GSM Networks optimised for Voice Communication
3G	Third Generation GSM Network optimised for Data Communications
4G	**Fourth Generation** GSM Network optimised for Data Communications
EDGE	**E**nhanced **D**ata rates for **G**SM **E**volution (or EGPRS). Used on 2G networks to increase the data rates achievable.
PSU	**P**ower **S**upply **U**nit
I/O	**I**nputs / **O**utputs

	Key Terms and Abbreviations
MOVA	**M**icroprocessor **O**ptimised **V**ehicle **A**ctuated
UTC	**U**rban **T**raffic **C**ontrol
OTU	**O**utstation **T**ransmission **U**nit
SCOOT	**S**plit **C**ycle **O**ffset **O**ptimisation **T**echnique
IPT	**I**ntelligent **P**ortable **T**erminal
RAM	**R**andom **A**ccess **M**emory
PROM	**P**rogrammable **R**ead **O**nly **M**emory
CPU	**C**entral **P**rocessor **U**nit
UTMC OTU	**U**rban **T**raffic **M**anagement and **C**ontrol (**O**utstation **T**ransmission **U**nit)
UTMC VMS	**U**rban **T**raffic **M**anagement and **C**ontrol (**V**ariable **M**essage **S**ign)
NAT	**N**etwork **A**ddress **T**ranslation (sometimes referred to as Port Forwarding)
VPN	**V**irtual **P**rivate **N**etwork
LAN	**L**ocal **A**rea **N**etwork
WAN	**W**ide **A**rea **N**etwork
ADSL	**A**symmetrical **D**igital **S**ubscriber **L**ine
SDSL	**S**ymmetrical **D**igital **S**ubscriber **L**ine

Table 2 : Terms and Abbreviations

2. Routers - General Description

Siemens ITS (Poole) provide and support three types of routers, namely a 3G/4G Router, xDSL Route and Instation Router for use in customer networks.

This chapter outlines these devices and provides an overview on their use.

2.1. MuLogic RSA ADSL

This type of router can be used to connect IP based equipment to a customer network using an ADSL "Broadband" Connection. The ADSL line will allow a connection to the Public Internet, and the router can provide a IPSEC VPN (Virtual Private Network) tunnel to another Router to allow the WAN (Wide Area Network) connection back to the customer LAN (Local Area Network). For details please refer to 667/CI/99107/000.

2.2. PROROUTE 4G Router

The current router is the PROROUTE H685 4G (667/1/99110/000), which can be used to connect IP based equipment to a customer network using a Mobile Phone connection (3G or 4G GSM). Wireless connections of this type are not normally as reliable as using wired communications solutions and are not always suitable in some locations or for certain applications. If in doubt, please contact the Engineering department in Poole for clarification.

The PROROUTE H685 4G (667/1/99110/000) Router also allows IPSEC VPN tunnels to be configured for secure connections across the public Internet, these settings would be provided by the Customer or Poole Engineering department.

2.3. Connection Types

There are two types of equipment connections used in Siemens ITS. The first is the 'transparent' connection and the second is the 'VPN' connection.

2.3.1. Transparent Connection

In this type of connection the STRATOS Outstation, or ST950 controller, will be the VPN client. Therefore any communications interface only needs to act as a transparent 'pipe' to and from the STRATOS Outstation/ST950 Controller.

Licences

The STRATOS Outstation/ST950 Controller needs to be supplied with the appropriate certificates in order to enable connection through to the STRATOS Instation.

Security

Although the 3G/4G router modem does not handle the STRATOS Outstation to Instation security explicitly, it is nevertheless incumbent on the installers to secure the router. Having a secure router may discourage accidental or intentional re-configuration that could end up providing third parties with access to customers' internet bandwidth.

The process for securing the 3G/4G router is as follows;

1 Generate a random password. It is recommended that KeePass (www.keepass.com) is used for such a purpose.

2 Configure the router such that the spare Ethernet port is not active.

3 Confirm and configure the modem such that the WiFi device is in-operable.

4 Update the modem with the password generated above.

5 Export the router configuration

6 Store the password for the router along with router configuration in the STRATOS Outstation site-log or the ST950 Site Log.

7 Delete local copies of the configuration and password.

2.3.2. VPN Connection

This type of connection relies on the router to become the VPN client. Product applications such as RMS over IP (Gemini Mk2), OMU, Saphire JTM will use this methodology.

Security

It should be noted that this method of connection is not considered as secure as the 'Transparent' connection method.

3. Installation and Configuration Guidance

3.1. Site Selection Guide

In order to assist in appropriate site selection for 3G/4G installation, the user is referred to the 3G/4G Communications Site Selection Guide (667/AY/45025/002).

3.2. Antenna Selection Guide

Siemens provide two types of antenna. The first is the Omni antenna which is normally mounted on a traffic pole. Due to the mounting height the Omni installation is most likely to provide the 'best' performance.

The second type, is a case (controller cabinet or VMS sign) mounted antenna. This antenna is unlikely to perform as well as a pole mounted Omni due to the mounting height (<2m in the case of a controller cabinet) and its antenna technology (patch antenna), which has a lower gain (typically 0dBi as opposed to 3dBi for an Omni).

To assist installers in deciding the type of antenna to select, the sample signal strength; that has been ascertained by working through the Site Selection Guide (see above), can be used.

Signal Guide			Antenna Guide	
Strength	Quality	Condition	Omni Antenna	Case Antenna
RSSI dBm	CSQ			
-109	2	Marginal		
-107	3	Marginal		
-105	4	Marginal		
-103	5	Marginal		
-101	6	Marginal		
-99	7	Marginal		
-97	8	Marginal		
-95	9	Marginal		
-93	10	OK		
-91	11	OK		
-89	12	OK		
-87	13	OK		
-85	14	OK		
-83	15	Good		
-81	16	Good		
-79	17	Good		
-77	18	Good		
-75	19	Good		
-73	20	Excellent		
-71	21	Excellent		
-69	22	Excellent		
-67	23	Excellent		

-65	24	Excellent		
-63	25	Excellent		
-61	26	Excellent		
-59	27	Excellent		
-57	28	Excellent		
-55	29	Excellent		
-53	30	Excellent		

3.3. Installation of the Antenna Cable

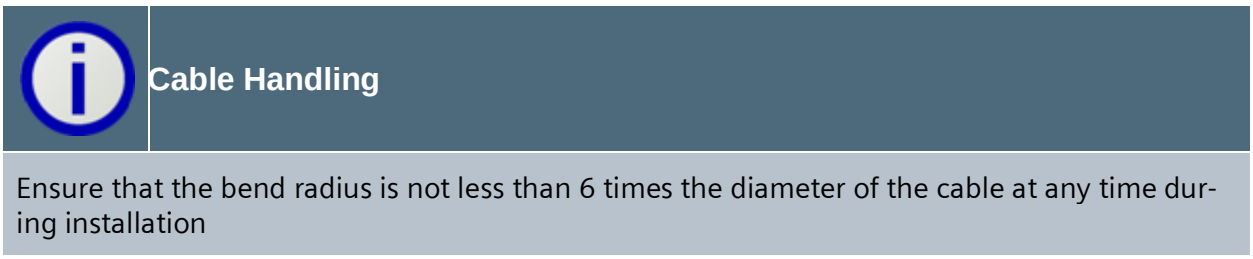
The Cable kits (667/1/46193/150 and /300) comes with:

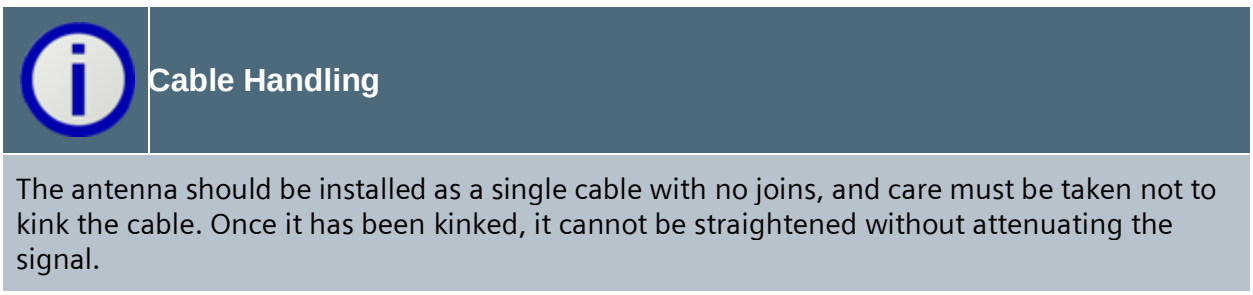
- 15M or 30M lengths of reinforced coaxial antenna cable (998/4/25011/400)
- PIB Self Amalgamating Tape (992/4/07906/000)
- Female N-Type Connector (For termination in the controller Cabinet)
- Male N-Type Connector (For Pole Top Termination)
- Adapter SMA plug to ReSMA socket
- ReSMA plug to N type plug pigtail cable.
- N-Type Cable Termination Guide (667/CI/46193/ETC)

The reader is to refer to N-Type Cable Termination Guide (667/CI/46193/ETC) for details;

1 Install the cable between the Roadside Cabinet and traffic signal pole.

2 Terminate the antenna cable using a Male N-Type connector (See Terminating N-Type Connectors).





Cable Handling

Use some PIB Self Amalgamating Tape (992/4/07906/000) (supplied) and some electrical tape to protect the N-Type connectors.

3.3.1. Installation of Pole Mounted Antenna Kit

The pole mounted 3G/4G Omni Antenna kit (667/1/46190/100) comes with:

- 3G/4G Omni Antenna
- Bracket and fittings to mount the Antenna at the pole top
- Installation drawing (667/CI/46190/ETC)

The reader is to refer to Installation drawing (667/CI/46190/ETC) for details;

1 Install the antenna in the supplied plastic bracket.

2 Attach the plastic bracket to the metal Pole mounting bracket using the supplied bolts.

3 Bolt the pole spacer kit to the pole using U Bolt provided.

4 Attach the Pole mounting bracket to the spacer kit and pull the antenna cable out through the hole.

5 Plug terminated antenna cable directly into the Antenna

6 The N-Type connector needs to be protected using self-amalgamating tape sealing against the bottom of the antenna housing and extending 1-2cm past the barrel of the connector onto the cable.

7 Complete the protection by neatly covering the self-amalgamating tape with black electrical tape, ensuring that the tape finishes with a cut off end (do not snap tape).

8 At the cabinet, bring the cable into the cabinet and terminate using appropriate connector, dependent on the router provided.

Cable Handling

Use some PIB Self Amalgamating Tape (992/4/07906/000) (supplied) and some electrical tape to protect the N-Type connectors.

3.4. Configuration and Installation of the 3G/4G Router

3.4.1. RMS over IP Gemini Mk2

For details the reader is referred to document 667/CI/32630/000 which is supplied as part of the Gemini Mk2 3G/4G Router Kit (667/1/32630/000).

3.4.2. STRATOS Outstation Connection

For details the reader is to refer to the STRATOS Outstation 3G Communications Installation Quickstart Guide (667/CI/52251/000), which is supplied as part of the STRATOS OUTSTATION 3G/4G ROUTER KIT (667/1/32630/100).

The STRATOS Outstation will be the VPN client. Any communications interface only needs to act as a transparent 'pipe' to and from the STRATOS Outstation. The STRATOS Outstation needs to be supplied with the appropriate certificates in order to enable connection through to the STRATOS Instation.

The 4G router needs to be setup as follows:

1 Ensure the router SIM card has been installed. Remove the panel at the back of the router and slide the SIM card into the slot.

Figure 1 : SIM Card Slot

2 Connect to the 3G/4G router, using the default IP address 192.168.8.1. Login using username **siemens_field.**

3 APN setup (including username and password)

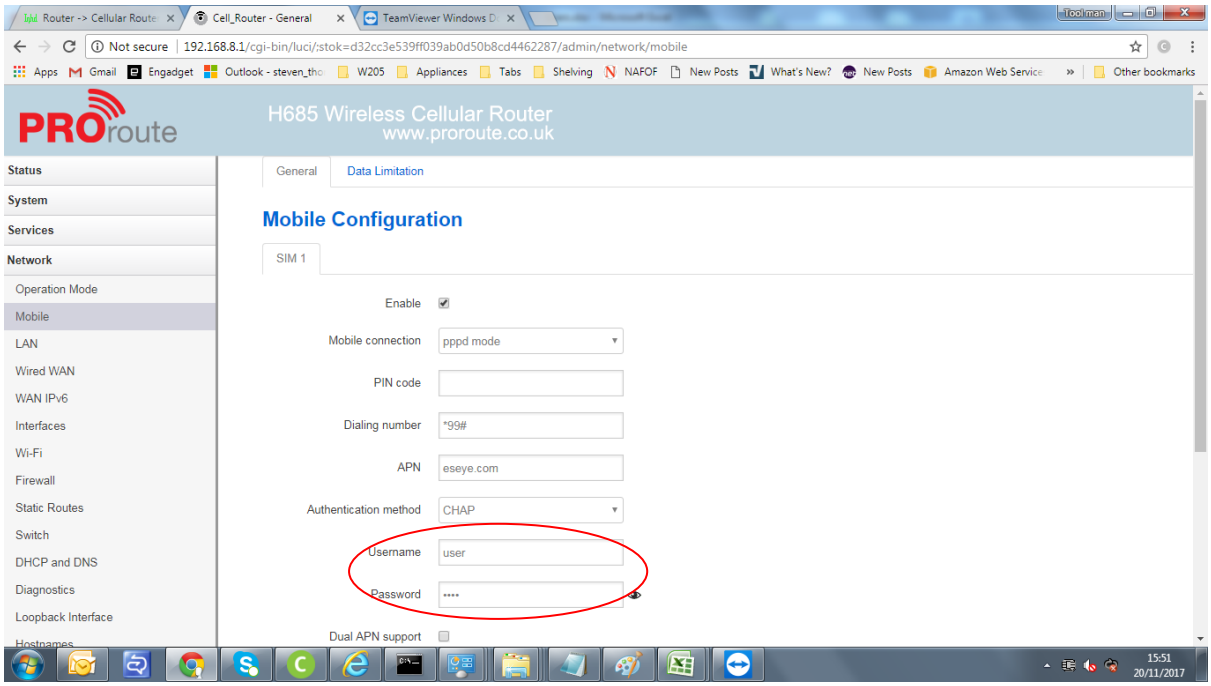


Figure 2 : 3G/4G Router Settings (WAN)

4 Setup ICMP check settings. This provides the 3G/4G router the ability to monitor the backhaul link and if down will reboots to ensure there are no router issues. Any 'pingable' IP address can be used but the STRATOS Instation would be a reasonable option.

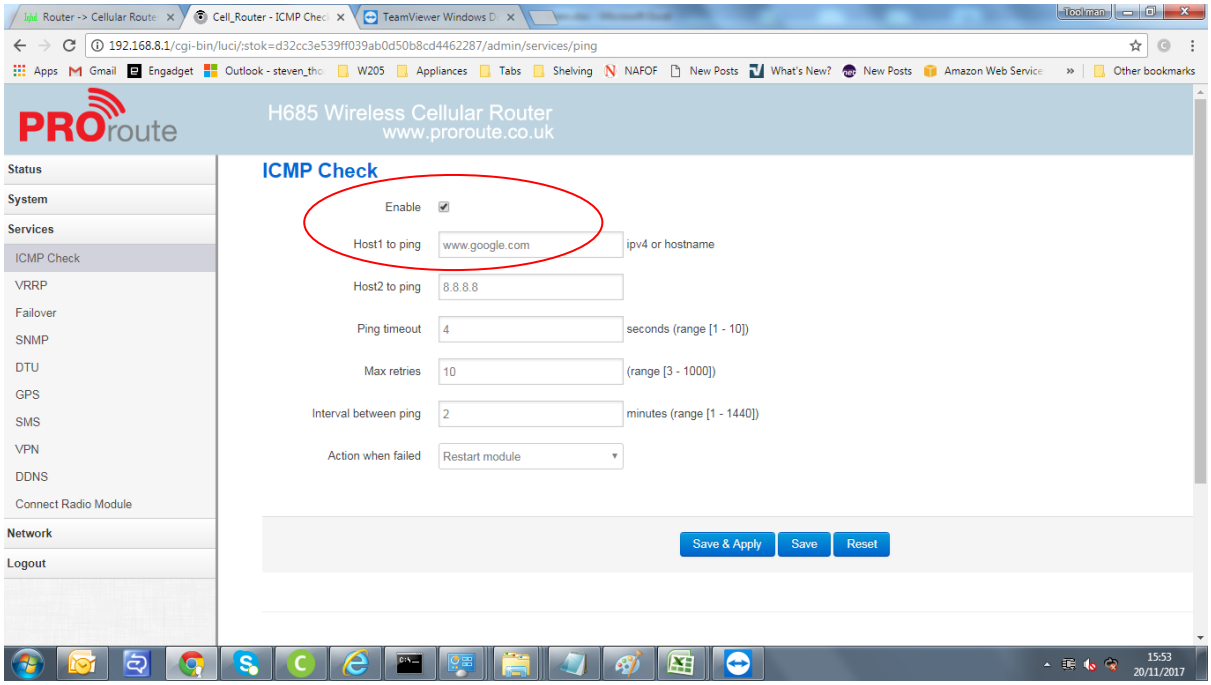


Figure 3 : 3G/4G Router Settings (ICMP)

3.4.3. UTC Connection via 3G/4G router

In these applications the 3G/4G router provides the secure connection to the Instation, where there will be an Instation router configured to accept the VPN connections.

VPN Prerequisites

- This section assumes that the PROROUTE is already configured to allow traffic out to the internet.
- It is also assumed that the router has been updated to the latest firmware (v3.2.133 as of 12th October 2017) available here:

http://www.proroute.co.uk/support/firmware/proroute-h820wrt-h685wrt-firmware/

1 The following instructions are used to ensure the 3G/4G router is configured for appropriate VPN connection;

2 Log on to the PROROUTE router(s) and navigate to **Services > VPN > IPSec**

3 Enter a memorable name in the **New instance name** box (*spaces not allowed*), select a method of **Client** and click the **Add** button:

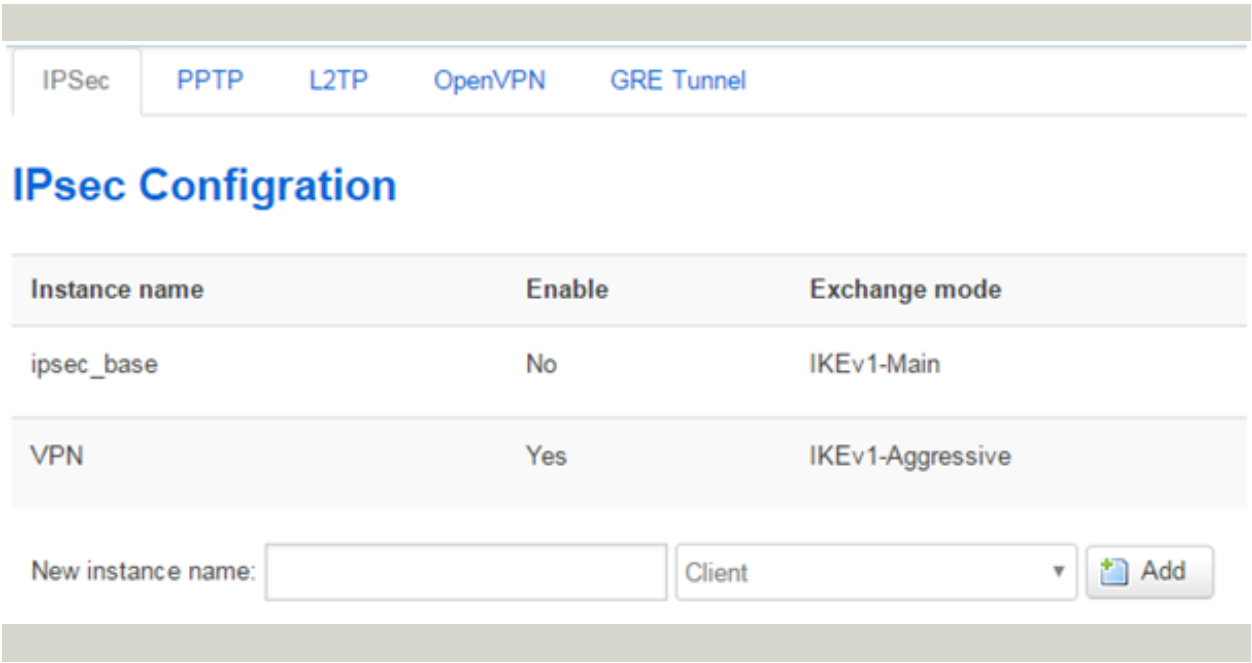


Figure 4 : IPSec Configuration

4 Once created, select **Edit** beside the newly created instance.

5 On the new page you will be required to enter the information as follows;

Setting	Value
Enable	*Tick this box to enable the tunnel*
Exchange mode	***IKEv1-Aggressive*** *or* ***IKEv1-Main***
Operation Level	***Main***
Authentication Method	***Client***
Remote VPN endpoint	*Change to* 'custom' *then enter the* ***public IP address for the VPNC***
Local endpoint	***Any***
Local IKE identifier	[SCN]@[customer].com ***(must match VPNC)***
Remote IKE identifier	Instation_[SCN]@[customer].com ***(must match VPNC)***
Preshared Keys	*Preshared key for this tunnel (refer to the ipsec.secrets file on VPNC)*
Perfect Forward Secrecy	***Enable***
DPD action	***Clear***
DPD delay	***30*** seconds ***(must match VPNC)***
DPD timeout	***120*** seconds ***(must match VPNC)***
NAT traversal	***Enable***
Local LAN bypass	*Tick this box if the local network range is contained within the remote range*
Local subnet	*Internal IP Address and subnet Mask (including any static routes) of the outstation*
Remote subnet	*Internal IP Address and subnet Mask of cloud-hosted environment*
Phase 1	
Encryption algorithm	This is the AES value e.g. AES 256 ***(must match VPNC)***
Hash algorithm	*This is the 3DES/SHA value e.g.* HMAC_SHA1 ***(must match VPNC)***
DH group	*Set the Diffie Hellman Group e.g. MODP4096/16* ***(must match VPNC)***
Life time	28800 *(refer to lifetime details within ipsec.conf on VPNC)*
Phase 2	
Encryption algorithm	This is the AES value e.g. AES 256 ***(must match VPNC)***
PFS group	*Set the Diffie Hellman Group e.g. MODP4096/16* ***(must match VPNC)***
Authentication	*This is the 3DES/SHA value e.g.* HMAC_SHA1 ***(must match VPNC)***
Life time	3600 *(refer to lifetime details within ipsec.conf on VPNC)*

Table 3 : IPSec Settings Table

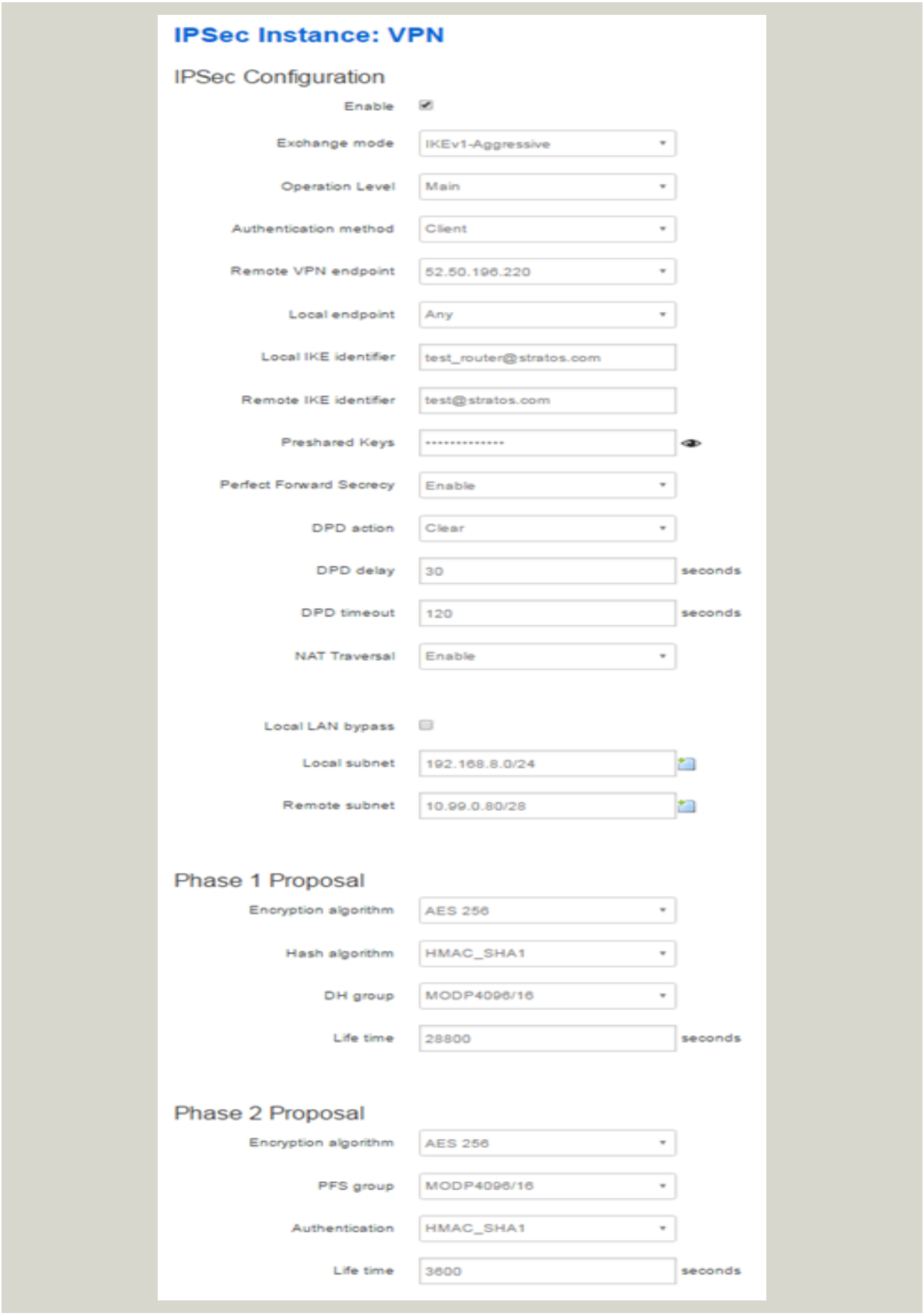


Figure 5 : Example IPSec Instance

6 Click **Save & Apply** to save this new tunnel.

7 Once the settings have saved you will return to the main list and a connection will be attempted.

8 You can check the status of the tunnel by navigating to **Status > VPN > IPSec** and identify any issues by selecting **IPSec Log** above the status

Figure 6 : Example IPSec Status

3.5. Installation and Configuration of xDSL Routers

For details the reader is to refer to the Field Document Installation of the MuLogic RSA-4222 667/CI/99107/000). This document also includes the details relevant to VPN connections.

In addition, the Installation of the MuLogic RSA-4222 Base Configuration (667/CR/99107/000) document is supplied as part of the CONFIGURED MULOGIC ROUTER RSA-4222/VR2 (667/1/99107/000).

3.6. 2U Mounting Kits

When installing an xDSL router and/or a wireless router, which isn't mounted to a STRATOS Outstation, the use of a 19 INCH 2U Mounting Kit is recommended.

There are a few options available, with the main ones listed below;

Part Number	Description
667/1/31625/019	19 INCH 2U Rack with UTMC 13A Socket Kit
667/1/31625/119	19 INCH 2U Rack
667/1/31625/219	19 INCH 2U Rack with STRATOS O/S 13A Socket Kit

4. Maintenance

4.1. Modifications

There are no approved modifications for these products.

Modifications

Use of components, other than those permitted in this document, or modifications or enhancements that have not been authorised by Siemens, will invalidate Type Approval of this product.

4.2. Routine Maintenance Visits

The interval between visits are dependent on local conditions.

The periodic inspection should include the following:

1 Checking the detector securing screws are tight.

4.3. First Line Maintenance

First line maintenance will be achieved on a modular replacement basis.

1 Check which type of router is fitted.

2 Note the router configuration (assuming correct install this may be available in the STRATOS Outstation/ST950 Controller Site Log.

3 Fit a replacement router of the same type.

4 Configure the replacement router in the same way as the router that was removed – or upload the configuration provided/downloaded.

4.4. Second Line Maintenance

The faulty parts being returned must always be sent back in the original packaging if available or in an approved Anti-Static packaging, along with a fully completed Fault Label to the following address:

Logistics Spares Returns Centre
Siemens Mobility
Traffic Solutions
Coalfield Way
Ashby Park
Ashby de la Zouch
LE65 1JD

For UK users, any queries should be directed to the Service Logistics Manager on:
(01530) 258181

A InHand Router (End of Life)

A.1 Installation

1 Before installing the router in the rack, the SIM card needs to be installed. Remove the panel at the top of the router and slide the SIM card into the slot.

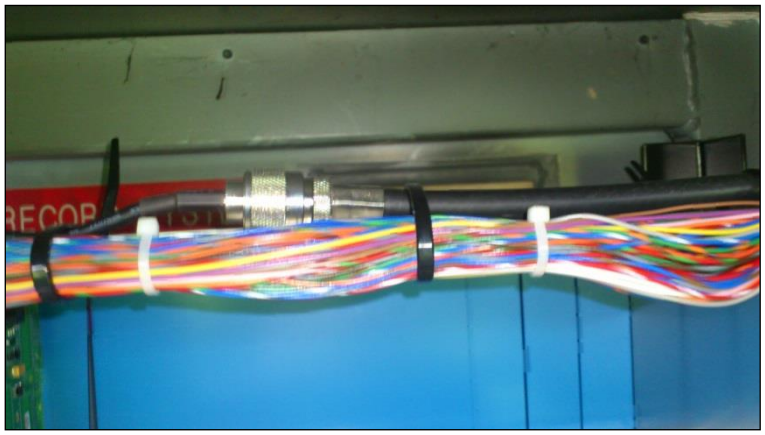
2 The Router should be installed on a suitable rack-mounted shelf and held in position using the clamp provided (not shown). (Usually part of Rack mounted UTMC OTU). This router needs to be installed on its side to fit into the rack.

3 Cable tie the provided PSU to the shelf alongside the Router and wire the DC connections directly onto the terminations of the router.

4 Wire the supplied plug onto the mains lead and plug into the socket on the Modem Rack (do NOT use the maintenance socket).

5 Terminate the Antenna Cable in the controller where the supplied Antenna Adaptor cable (SMA to N-Type) will reach between the router and the end of the cable. (See **Error! Reference source not found.**)

6 Install the Antenna Adaptor cable between the Antenna cable and the Routers “Primary Cellular” SMA connector.



7 Plug the Ethernet cable (supplied separately) into the Ethernet port on the Router and into the Laptops Ethernet port.

8 Set up the communications on the router (see below)

The settings for each router will change between sites and customer systems.

Before trying to set up a router, you should have received all configuration information, or a configuration file for the router, or both. This would normally be provided by the Poole Engineering Department.

Profile

The UTC instation should be configured to use a communications profile that is compatible with the physical network layer (ADSL, wireless, 3G etc). This should be checked with the in-station operator.

A.2 Inhand 3G Router Commissioning

Instation should use the 3G communications profile.

This type of 3G router would normally be set up using a Private APN, this would be requested by the customer and the information supplied.

You would normally expect to be provided with the following information:

- Mobile APN and Password
- Local (LAN) IP address for the Router (Also the Gateway for other devices on the LAN)
- LAN Subnet Mask/ Netmask
- LAN IP address for the Outstation Device (e.g. UTMC OTU)
- LAN IP address for the Engineers Laptop
- Port Forwarding details (NAT)
- VPN (IPSEC) settings (usually instead of NAT above)

This information may also be delivered as a complete configuration file from Poole engineering.

After connecting to the router using a laptop, you should be able to browse to its web page by typing its private IP address into a browsers address bar.

Default Settings to connect to this router:

Router IP Address: 192.168.2.1 (Gateway)

Subnet Mask: 255.255.255.0

Laptop: 192.168.2.5

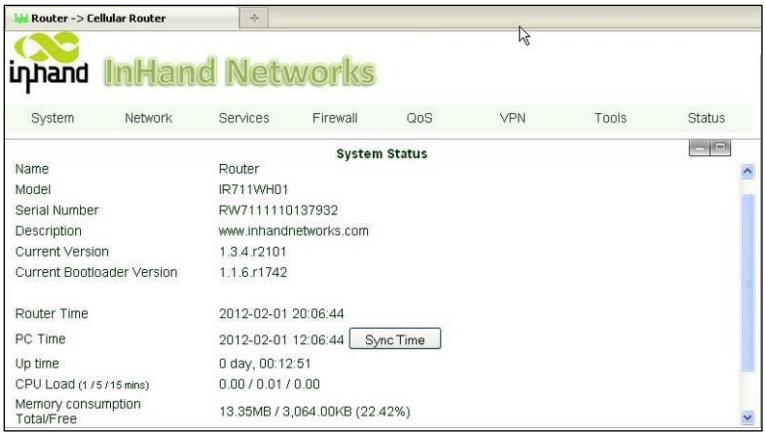
The default Username and password for the Inhand routers are:

Username: adm

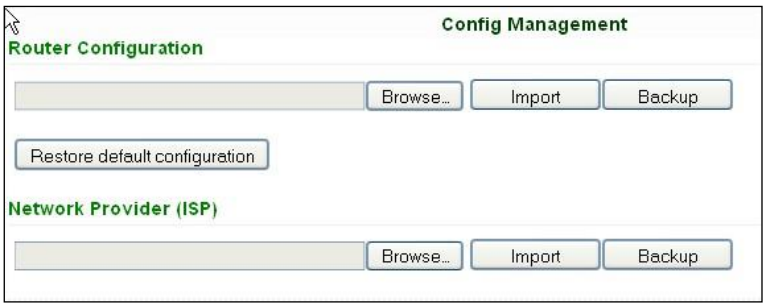
Password: 123456

Once logged onto the router the home screen should appear, this shows you the current state of the router and the signal strength. At this point you would expect the router to have logged onto the network and be showing the signal strength.

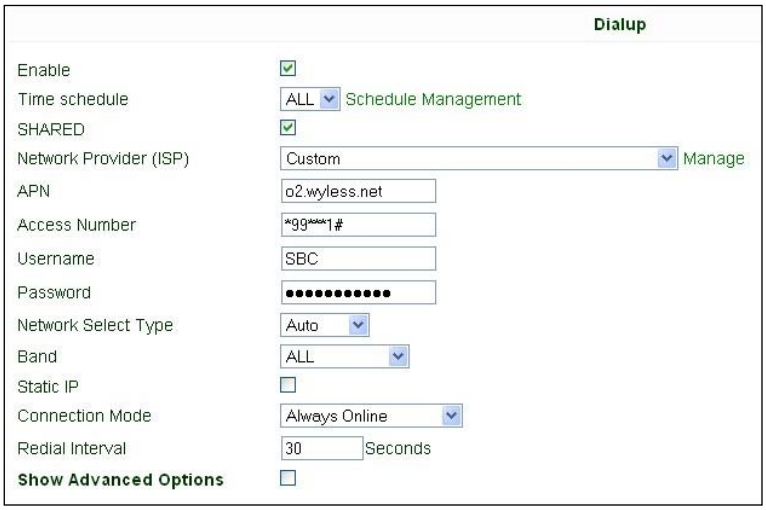
You would also expect the PPP link to show an IP address for the WAN (mobile) side of the router if it connected to the service provider's network. (Usually a class A 10.xxx.xxx.xxx address). This will not appear until the APN and password are entered later in this section.



If you have been supplied a configuration file for the router, or if you are using the Siemens Default Configuration (See Section **Error! Reference source not found.**) this can be uploaded on the "System" – "Config Management" page. Press the browse button under Router Configuration, browse to the file on your laptop and select the import button. (This page can also be used to save a copy of a working configuration).



The APN (or Private APN) and password for the mobile network needs to be entered to allow the router to connect to the mobile data network.

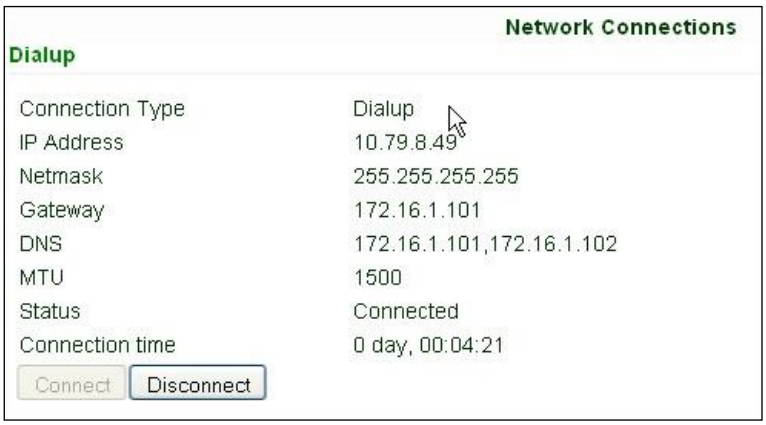


Choose the "Status – Modem" Page, this shows you the current state of the modem and the signal strength. At this point, you would expect the router to have logged onto the network and be showing the signal strength.

The modem should have "Registered" on the network.

You would also expect the PPP link to show an IP address for the WAN (mobile) side of the router if it connected to the service provider's network. (Usually a class A 10.xxx.xxx.xxx address).

The WAN connectivity can be viewed on the “Status” – “Network Connections” – “Dialup” section. It should look similar to the screen below, with the WAN IP (set from the Mobile Network) being listed and the Status being set to connected.



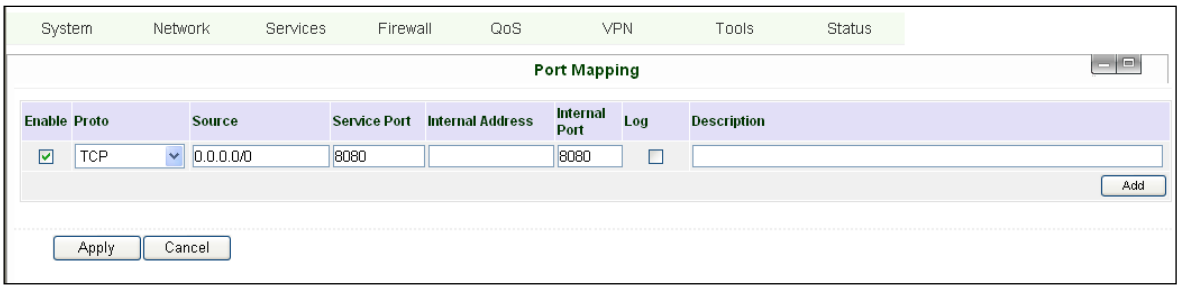
If the site is using the default configuration or a configuration file has been provided by the Poole Engineering Department, no further action would be required. The next section is for information only, and would only require configuring if the information has been specified by the Engineering Department.

A.3 Optional Configuration Parameters

This section is for information only, and would only require configuring if the information has been specified by the Engineering Department.

The private network (Local Area Network) may need to be configured to the given settings, this can be done under “Network” – “LAN”. If you make any changes to the form press the “Apply” Button to save them.

Port forwarding may need to be configured to forward traffic received on the routers WAN side, to the outstation device on the LAN side. These settings can be changed in the “Services” – “Port Mapping” form, these details will be provided if they are necessary.



The Inhand 3G router can also be configured to connect a VPN across public networks using IPSEC, these details are entered on the “Service” – “IPSEC” page, and the “Network” – “IPSEC Tunnels” page. These settings would be provided by Poole Engineering if they were required.

More information

Siemens Traffic
www.siemens.co.uk/traffic

Siemens Mobility
http://www.mobility.siemens.com/mobility

Siemens Plc
Sopers Lane
Poole
BH17 7ER
United Kingdom

Order No. 667/CI/45025/000 /

For more information on ITS products scan the QR code

www.siemens.co.uk/traffic