

# SINAUT ST7 Telecontrol Configuration in a Secure EGPRS Environment with MD741-1/ SCALANCE S612

SINAUT ST7 Telecontrol – Configuration 8 – Volume 2

[Application Description • August 2011](#)

## Applications & Tools

Answers for industry.

**SIEMENS**

**Note**

The Application Examples are not binding and do not claim to be complete with regard to configuration, equipment or any contingencies. The application examples do not represent customer-specific solutions; they are only intended to provide support for typical applications. You are solely responsible for the correct operation of the described products. These application examples do not relieve you of your responsibility to use sound practices in application, installation, operation and maintenance. When using these application examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these application examples at any time without prior notice. If there are any deviations between the recommendations provided in these application examples and other Siemens publications – e.g. catalogs – the contents of the other documents have priority

## Warranty, Liability and Support

We do not accept any liability for the information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of Siemens Industry Sector.

If you have any questions concerning this document please e-mail us to the following address:

[online-support.automation@siemens.com](mailto:online-support.automation@siemens.com)

## Preface

### Objective of this application

This volume is aimed at making you familiar with the internet/GPRS communication in the world of automation.

For this purpose, the Ethernet connection between the control center and other stations set forth in Volume 1 shall be replaced by a secured internet/GPRS connection. The example project is used as a basis to describe, step-by-step, the configuration of the entire chain of transmission (EGPRS, DSL, Security), as well as the necessary changes to the SINAUT project of Volume 1.

#### Note

This document is based on the example application described in Volume 1 for SINAUT Configuration 8. Volume 1 is available as a separate document on the HTML page.

### Main contents of this application

This volume focuses on the following topics:

- basic terms related to the EGPRS/GPRS technology and security aspects
- a detailed description of all configuration settings required to set up a VPN tunnel between the EGPRS router type MD741-1 and the SCALANCE S612 security module.

#### Note

For basic information and further details on configuration with STEP 7, TIM 3V-IE, TIM 4R-IE and the control center with ST7cc WinCC, please refer to Volume 1.

### Topics not covered by this application

This example project contains no technologically relevant program for the control or coordination of drives. It is only intended to demonstrate how data exchange between the stations and the control center is effected. It has intentionally been kept simple and programmed bit-by-bit, so as to illustrate the correlation between data in the CPUs and the control center.

### Structure of this document

The documentation of this application is divided into the following main parts.

Section	Description
Application description	This section provides a general overview of the contents and informs you about the components used (standard hardware and software components and specially programmed user software).
Function principle and program structures	This part describes in detail the functional processes of the integrated hardware and software components, the solution structures and – where useful – the specific implementation of this application. In this section you will learn how the individual components of the solution interact, so as to use them as a basis for your own developments, for example.

Section	Description
Structure, configuration and operation of the application	This section leads you step-by-step through the structure, important configuration steps, commissioning and operation of the application.
Appendix	Here you will find some further sources of information, such as links and literature, glossaries, etc.

**Reference to Automation and Drives Service & Support**

This article is taken from the Internet application portal of Automation and Drives Service & Support. The following link takes you directly to the download page of this document.

<http://support.automation.siemens.com/WW/view/en/23810112>

# Table of Contents

<b>Warranty, Liability and Support.....</b>	<b>3</b>
<b>Table of Contents.....</b>	<b>6</b>
<b>Application Description.....</b>	<b>8</b>
<b>1 Automation Task.....</b>	<b>8</b>
1.1 Overview .....	8
1.2 Requirements .....	8
<b>2 Automation Solution .....</b>	<b>9</b>
2.1 Overview of the overall solution .....	9
2.2 Description of the core functionality .....	11
2.3 Required hardware and software components .....	12
<b>Function Principles and Program Structures .....</b>	<b>15</b>
<b>3 Functional Mechanisms .....</b>	<b>15</b>
3.1 Radio communication.....	15
3.2 Components/infrastructure of the EGPRS/GSM transmission chain.....	18
3.3 EGPRS-router MD741-1 .....	19
3.4 DSL / internet connection .....	21
3.5 SCALANCE S.....	22
3.6 Security .....	23
3.6.1 VPN tunnel .....	23
3.6.2 IPsec.....	25
3.7 Cross-communication via EGPRS .....	27
<b>4 Explanations on the Example Program.....</b>	<b>28</b>
4.1 Setting the IP addresses for the ST7cc and TIMs .....	28
4.1.1 ST7cc control center .....	29
4.1.2 TIM 4R-IE in the control center .....	29
4.1.3 Stations 2 and 3 .....	31
<b>Structure, Configuration and Operation of the Application .....</b>	<b>32</b>
<b>5 Installation and Commissioning .....</b>	<b>32</b>
5.1 Hardware / structural layout and software installation .....	32
5.2 Installation of the example project.....	33
5.3 Commissioning the example project .....	34
5.3.1 Configuring the DSL router .....	34
5.3.2 Configuring the control center .....	35
5.3.3 Downloading the master TIM and the stations 2 and 3.....	37
5.3.4 Configuring SCALANCE S and the VPN tunnel.....	38
5.3.5 Configuring MD741-1 .....	45
5.3.6 MD741-1 of 02_Station .....	45
5.3.7 Additional settings recommended for the MD741-1 .....	55
5.3.8 New features available for MD741-1 V 1.0.38 or higher .....	59
5.3.9 MD741-1 of 03_Station .....	60
<b>6 Operation of the Application .....</b>	<b>61</b>
6.1 Final configuration .....	61
6.2 Commissioning of the ST7cc control center and function test.....	61

<b>7</b>	<b>Diagnostics .....</b>	<b>62</b>
7.1	Diagnostic options .....	62
7.2	What can I do, if .....	65
	<b>Appendix – Links &amp; Literature .....</b>	<b>66</b>
<b>8</b>	<b>Literature .....</b>	<b>66</b>
8.1	Literature .....	66
8.2	Internet links .....	66
<b>9</b>	<b>History.....</b>	<b>67</b>

# Application Description

## Contents

This section provides you with an overview of the automation task and its solution. Furthermore, you will become acquainted with the individual components used (standard hardware and software components).

## 1 Automation Task

### 1.1 Overview

Two waste water processing stations shall be controlled and monitored from one control center.

### 1.2 Requirements

In addition to the conditions stated in Volume 1, the following requirements shall be met:

- The transmission of process data shall be performed via a secured internet connection.
- The outstations cannot be accessed over the internet via a landline or DSL connection.



## 2 Automation Solution

### 2.1 Overview of the overall solution

The main SIMATIC components deployed for this solution are the EGPRS router type SINAUT MD741-1 in the stations, and the SCALANCE S612 security module in the control center.

These two components are used to establish IPsec-based tunnel connections (virtual private network, VPN) between

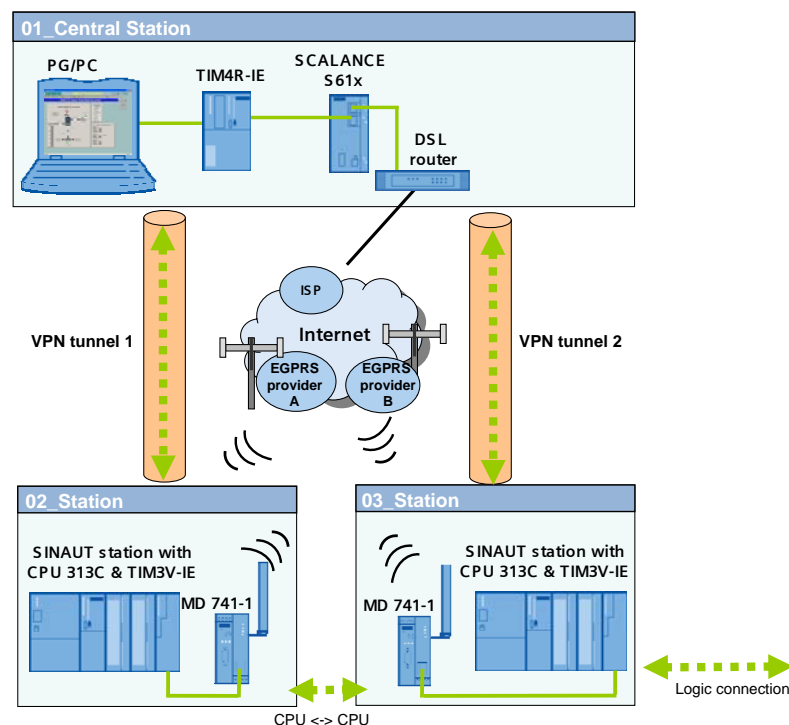
- the WinCC/ST7cc control center which is connected to the internet via DSL and
- several SINAUT stations which are connected to the internet via EGPRS or GPRS.

This configuration enables the exchange of process data between a station and the control center or between individual stations (bidirectional transmission is possible).

#### Schematic layout

The illustration below provides an overview of how the solution has been realized in this configuration:

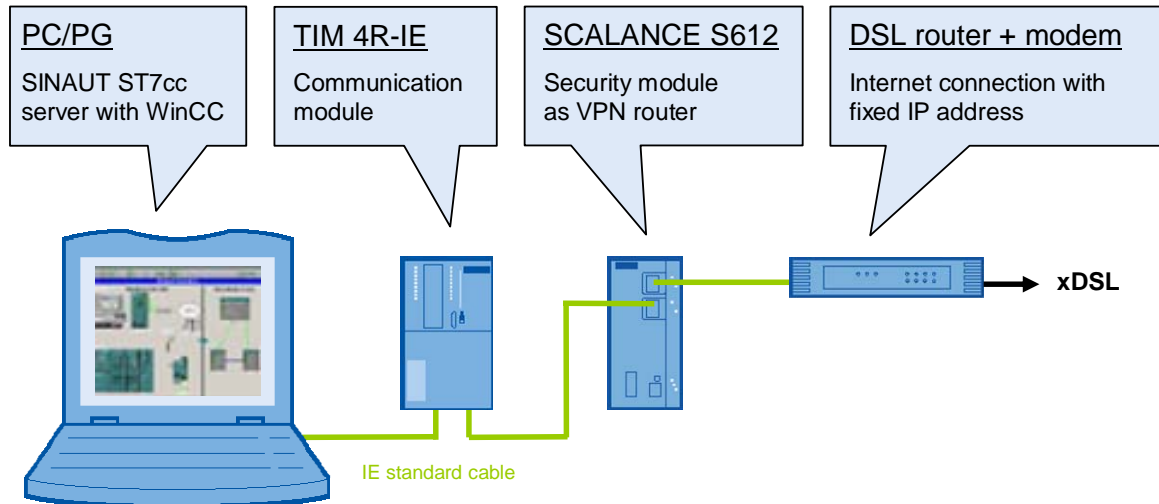
Figure 2-1



#### Structure

#### Setup of the control center

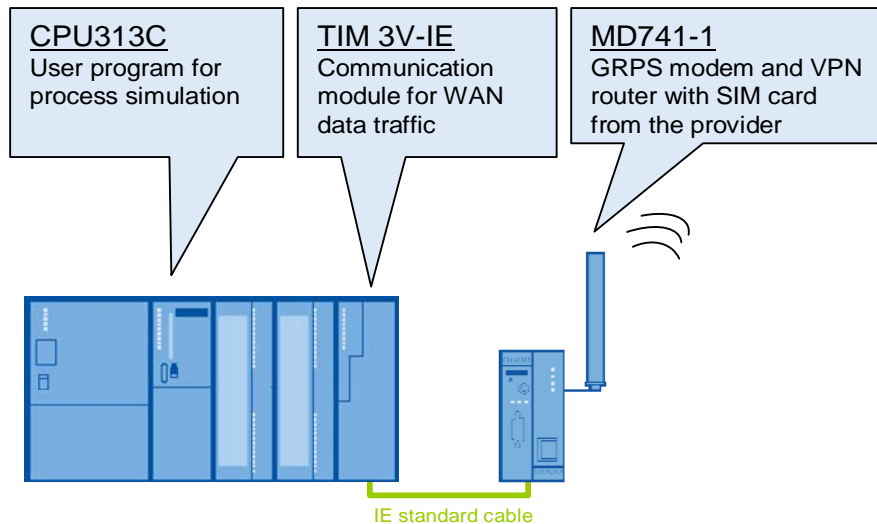
Figure 2-2



The control center consists of a standard Windows PC/PG. The PC is connected to a port of the TIM4R-IE module via an integrated Ethernet interface. The second Ethernet port is used to connect the TIM4R-IE with the internal (secure) port of the SCALANCE S612 module. The DSL router is connected to the external (unsecure) port of the SCALANCE S612 module.

#### Setup of the SINAUT substations

Figure 2-3



Each distributed station consists of a compact CPU and a TIM3V-IE module. The TIM3V-IE module is connected to the EGPRS router MD741-1 via the integrated Ethernet interface.

## 2.2 Description of the core functionality

The MD741-1 router in the station sets up a VPN tunnel over the internet for connection to the SCALANCE S612 security module in the control center. Over this tunnel, the station can communicate with the control center.

Communication between the individual stations ("cross-communication") is effected via the TIM4R-IR module in the control center.

### Advantages of this solution

- The SINAUT outstations are independent of the location and can be connected wirelessly at almost any place (worldwide).
- High communication availability due to standardized mobile radio and internet technology.
- EGPRS and internet ensure short transmission times and permanent online availability.
- Cost-effective data transmission by pay per data volume.
- VPN functionality enables secure, protected and encrypted data connection based on the IPSec standard.
- High degree of security by means of an integrated firewall.
- Simple and user-friendly configuration of the VPN tunnel with the Security Configuration Tool.
- Communication between GPRS stations is also possible.

### Note

This document refers only to the advantages if an EGPRS router is used in combination with a SCALANCE S612 module.

## 2.3 Required hardware and software components

### SINAUT ST7

Table 2-1

Component	Qty.	MLFB / order number	Notes
TIM 4R-IE Firmware <b>V2.1.0</b>	1	6NH7800-4BA00	You may update your TIM 4R-IE to version 2.1.0. See <a href="#">3</a>
TIM 3V-IE Firmware <b>V2.1.0</b>	2	6NH7800-3BA00	You may update your TIM 3V-IE to version 2.1.0. See <a href="#">4</a>
SINAUT ST7 <b>V5.0 SP1</b>	1	6NH7997-0CA15-0AA0	You may upgrade the SINAUT ST7 Tool V5.0 with SP1. See <a href="#">5</a>
SINAUT ST7cc V2.7	1	6NH7997-7CA15-0AA1	License for max.6 SINAUT stations
EGPRS Router MD741-1	2	6NH9741-1AA00	
ANT 794-4MR	2	6NH9860-1AA00	Quadband antenna, omnidirectional, including a 5m cable

### Security

Table 2-2

Component	Qty.	MLFB / order number	Notes
SCALANCE S612 Firmware <b>V2.3</b>	1	6GK5612-0BA00-2AA3	As an option, you may update an existing SCALANCE S V2.1 to version 2.3. See <a href="#">6</a>
Security Configuration Tool	1		<b>Version 3</b> SCALANCE S is included in the SCT delivery.

#### Note

You can obtain the update version V3 for the Security Configuration Tool via you local contact person.

SCALANCE S V2.3 can be configured with the Security Configuration Tool V 2.2 or a higher version. We recommend to use the Security Configuration Tool V3.

**SIMATIC S7**

Table 2-3

Component	Qty.	MLFB / order number	Notes
PG	1	6ES7712-	<a href="#">Configurator</a>
STEP 7 V5.4 SP4	1	6ES7 810-4CC08-0YA5	Or higher
SIMATIC NET PC Software Edition 2006	1	6GK1704-1LW64-3AA0	
SIMATIC WinCC V6.2 & SP2	1	6AV6381-1BM06-2AX0	The "Service & Support News" (see <a href="#">1</a> in the appendix) provides further information about the latest releases.
Power supply unit PS307 5A	3	6ES7 307-1EA00-0AA0	
S7-CPU 313C	2	6ES7313-5BF03-0AB0	
Micro Memory Card	2	6ES7953-8LF11-0AA0	At least 64 kB
Front connector for signaling modules	2	6ES7392-1BM01-0AA0	

**LAN components**

Table 2-4

Component	Qty.	MLFB / order number	Notes
IE FC TP STANDARD CABLE	1	6XV1840-2AH10	IE connecting line, minimum order quantity: 20m
IE TP XP CORD CABLE	1	6XV1870-3RH20	Crossed IE connecting line, min. order quantity: 2m
RJ45 plug-in connector	10	6GK1901-1BB10-2AA0	Easy to adjust

**Infrastructure**

Table 2-5

Component	Qty.	MLFB / order number	Notes
DSL router + modem with VPN passthrough function (port forwarding)	1		Router optionally with integrated modem or separately, e.g. with Netgear RP614GR, Gigaset SE 515
Internet provider	1		
Fixed IP address	1		Contract with your Internet provider
SIM card	2		Subscriber contract with a GSM network provider; released for EGPRS

**Example files and projects**

The following list contains all files and projects used in this example.

Table 2-6

Component	Notes
23810112_SINAUT_INTERNET_DOKU_V21.pdf	This document
23810112_SINAUT_INTERNET_CODE_V20.zip	This ZIP file includes:
• STEP7_ INTERNET.zip	STEP 7& SINAUT ST7 project
• WinCC_ INTERNET.zip	WinCC & ST7cc project

# Function Principles and Program Structures

## Content

This section goes into some background information with regard to GSM, GPRS, EGPRS and Security. It additionally describes the required settings in NETPRO, so that the project of Volume 1 can also be used for (E)GPRS.

## 3 Functional Mechanisms

This chapter briefly discusses the underlying technologies and principles that take effect here.

### 3.1 Radio communication

In this SINAUT example, part of the transmission path is realized with the GSM/GPRS radio service.

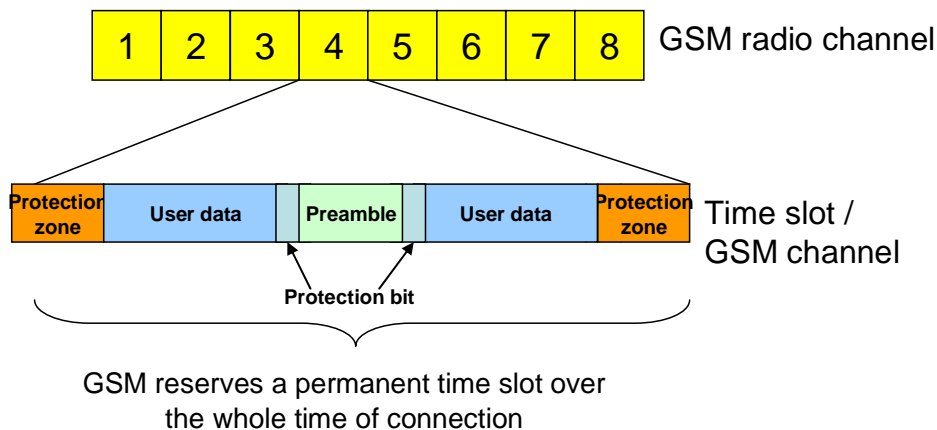
#### GSM

The **G**lobal **S**ystem for **M**obile Communications (GSM) is a standardized and fully digital mobile radio network. This network is used for mobile phones, the transmission of circuit switched data (CSD) and short messages (SMS).

The GSM radio channels are divided into eight time slots, each of which has a data transmission rate of 9.6 kbit/s.

Line transmission means that a GSM channel (time slot) is permanently reserved over the entire time of connection, and that the data to be transmitted to the receiver is always sent through the same channel.

Figure 3-1



If circuit switched data transmission (CSD) is used, the network provider will charge the entire connection time, independently of the data volumes transmitted.

## 3 Functional Mechanisms

### 3.1 Radio communication

#### Availability

The following table shows a list of the frequency bands and their national and international availability.

Table 3-1

GSM standard	Transmission range	Availability	Mobile service providers in Germany
GSM 850	850 MHz band	North America	
GSM 900	900 MHz band	Global	T-Mobile, Vodafone, D networks
GSM 1800	1800 MHz band	Global	T-Mobile, Vodafone, o2, E-Plus
GSM 1900	1900 MHz band	North America	
GSM-R		For trains	

#### GSM 900

GSM works with different frequencies for uplink (mobile phone → network) and downlink (network → mobile phone). This shall be explained by the example of GSM 900.

Table 3-2

Criterion	Parameter
Uplink	890 - 915 MHz
Downlink	935 - 960 MHz
Number of frequency channels	124
Channel bandwidth	200 kHz
Number of time slots (GSM channel) per channel	8 at 577 µs each

#### GPRS

The **General Packet Radio Service** (GPRS) is a method for packet-switched data transmission via the GSM networks. It offers a higher data rate than circuit-switched GSM services.

'Packet-switched' means that no GSM channel is permanently reserved. At the sender, the message is broken down into individual packages which are provided with additional information. This information tells the network how the individual packages relate to each other and where the message shall be received. The GPRS system allows to send the packages through different time slots of the network and thus enables the use of free capacities. Then, the receiving unit compiles the packages in their correct order.

GPRS enables data traffic without establishing a connection beforehand and only the data volume actually transmitted will be charged.

Packet switching is enabled by the IP (Internet Protocol) technology. GPRS is mainly used for access in IP-based networks (e.g. internet).

#### Data rate for GPRS

In order to obtain higher data rates for transmission, several time slots can be combined. In the highest multislot class (class 12) a maximum of five time slots can be bundled up for one device. This means that a total of five channels at the maximum can be used simultaneously for uplink and downlink (e.g. 3 channels for uplink and 2 for downlink, or 1 for uplink and 4 for downlink, see table 4-1).



In each direction, however, a maximum of four channels can be bundled.

Table 3-3

Downlink	Uplink
1	4
2	3
3	2
4	1

Depending on the error protection mechanisms used, up to 21.4kbit/s can be transmitted per time slot. This results in a theoretical data rate of 85.6 kbit/s (4 x 21.4 kbit/s) at the maximum. In practice, however, this theoretical value is very rarely reached.

On the one hand, this is owed to the fact that the number GSM channels that can be used in parallel varies, depending on the network load and the capability of the mobile device. On the other hand, the data rate is adjusted to the quality of the radio network through channel coding (Coding Schemes/CS). For GPRS the data rate in the individual GSM channel is fixed to 13.4 kbit/s (CS2).

The MD741-1 router supports the highest multislot class (class 12). This results in a maximum practical data rate of **53.6 kbit/s** for uplink (4 GSM channels with CS2) or **53.6 kbit/s** for downlink (4 GSM channels with CS2).

## EGPRS

The **E**nhanced **G**eneral **P**acket **R**adio **S**ervice (also referred to as **EDGE**, **E**nhanced **D**ata **R**ates for **G**SM **E**volution) is an expansion of GPRS. EGPRS uses a different modulation method (8-PSK) than GPRS, which is more efficient. With EGPRS the data rate can be accelerated up to four times.

### Data rate for EGPRS

Like GPRS, EGPRS also allows the combination of up to five time slots at a time. The maximum data rate per time slot is 59.2 kbit/s. If four time slots are used for uplink or downlink, the maximum data rate is 236.8 kbit/s (4 x 59.2 kbit/s) in theory.

In practice, however, this theoretical value is rarely reached. In Germany, most providers use the modulation and coding scheme MCS8 for EGPRS. The MCS8 scheme has a fixed data rate of 54.4kbits/s per channel.

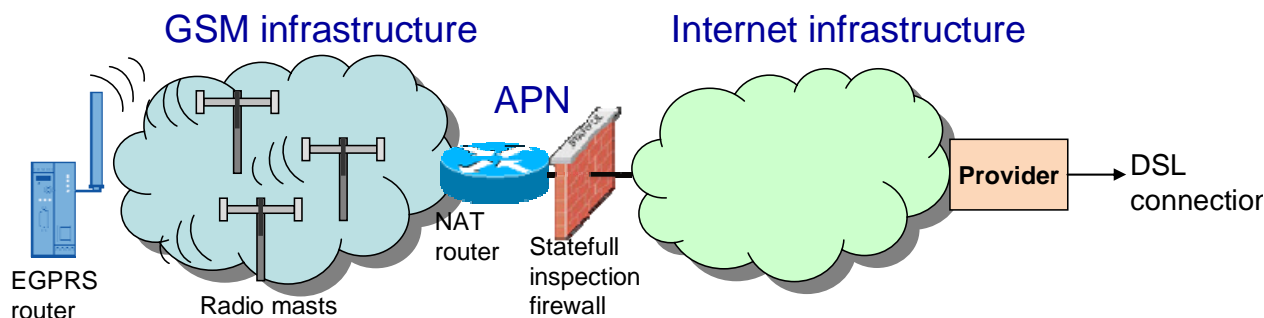
Of course, the data rate also depends on the network load and the capacity of the mobile device. The MD741-1 supports the highest multislot class (class 12) which offers a maximum of four channels for uplink or four for downlink. This results in a maximum practical data rate of **217.6 kbit/s** for uplink (4 GSM channels with MCS8) or **217.6 kbit/s** for downlink. (4 GSM channels with MCS8).

## 3.2 Components/infrastructure of the EGPRS/GSM transmission chain

### EGPRS/GSM transmission chain

The following graphic illustrates the transmission path along the EGPRS chain.

Figure 3-2



The illustration shows all components required for a GPRS connection via internet.

Table 3-4

Component	Function	Notes
EGPRS router	EGPRS-/GPRS client; can send data via the EGPRS/GPRS radio network;	Receives an IP address assigned by APN
APN	<b>Access Point Name</b> ; address of the mobile service provider which defines the node from the EGPRS/GPRS network to the internet. Assigns an IP address to the client (private or public IP address, depending on the APN).	APN for Vodafone: <b>web.vodafone.de</b> APN for D1: <b>internet.t-mobile</b> APN for E-Plus: <b>internet.eplus.de</b>
NAT router	Uses NAT to switch between internal, private networks and the public internet	<b>Network Address Translation</b> maps private IP addresses to public ones.
Statefull inspection firewall	Protection wall; only allows response packages after requests.	Any packages from outside which do not respond to a request triggered by the client will be rejected.
Provider	Local internet provider	

### Transmission requirements

The transmission of data packages in this example is subject to certain requirements:

- **Security:** The transmission path must be saved and protected against unauthorized access. In this example, an IPsec tunnel (VPN) is used for this purpose.
- **Stability:** The transmission path must be stable. Requires regular monitoring by means of keepalive protocols (NAT-T Keep Alive, Dead Peer Detection, Rx/Tx Delay Trigger, TCP-IP Keep Alive).

- Bi-directionality: Point-to-point data transmission in both directions.
- Accessibility: The DSL router in the control center must have a fixed public IP address.

#### Connection setup procedure

Because of the involvement of the internet service provider, the setup of a connection between MD741-1 and SCALANCE S requires several steps as explained in the following.

Table 3-5

Step	Description
1	The MD741-1 router establishes an EGPRS data connection via the mobile service provider (APN). The mobile service provider forwards the GRPS data traffic to the internet.
2	The MD741-1 router sends data packages with the target address (IP address of the router) to the internet.
3	Provided, that a DSL connection between the control center and the internet has been established, the data packages are forwarded to the S612 unit via the DSL router.
4	The VPN tunnel between MD741-1 and SCALANCE S is being established.
5	Package-oriented data traffic can be effected.

### 3.3 EGPRS-router MD741-1

The MD741-1 router uses EGPRS or GPRS to establish a secured IP data connection between the remote stations and the service center.

#### Basic requirements for operation

Operation of the MD741-1 router requires the use of a SIM card for EGPRS/GPRS services which must be inserted into the router.

#### Note

SIM cards released for GPRS services also support EGPRS. Whether the router logs in into an EGPRS or GPRS network depends on the network coverage of the provider. Information on the network coverage of the provider is usually available on the provider's internet site.

In combination with a quad band antenna type ANT 794-4MR, the EGPRS router MD741-1 covers all four band widths of the GSM networks and can therefore be used almost worldwide.

- 850 MHz
- 900 MHz
- 1800 MHz
- 1900 MHz

#### Note

Please take note of the country approvals for the MD741-1 router.

Link [2](#)

##### Properties of the MD741-1 router

The router provides the following core functions for secure radio data connection:

- VPN router: supports safe data connection via an IPSec-secured VPN tunnel (Virtual Private Network)
- 3DES data encryption, AES encryption
- Firewall for protection against unauthorized access. The dynamic packet filter searches data packages on the basis of their source and target address (statefull packet inspection) and blocks any undesired data traffic (anti-spoofing)
- EGPRS modem for a data communication in packets via GSM
- Bidirectional data connection
- Cyclic processing of protocol data to keep up and monitor the connection (NAT-T Keep Alive, Dead Peer Detection, Rx-Tx-Delay)

##### Modem configuration

The router is configured with the help of a standard browser using the integrated web page with web-based management.

##### Explanation of important terms

This section provides a brief explanation of the most important features of the MD741-1 router.

##### Note

For further information, please refer to the MD741-1 manual (see [/2/](#) in the appendix)

Table 3-6

Feature	Explanation
Virtual Private Network (VPN)	A VPN is used to connect computers or networks via the internet and to ensure secure data transmission. This so-called tunnel is encrypted. The use of passwords, public keys or a digital certificate guarantees authentication of the VPN end product.
IPSec	IPsec is an advancement of the internet protocol (IP) and includes extensive security functions: <ul style="list-style-type: none"> <li>• an AH mechanism (Authentication Header) manages the authentication and identification of the source.</li> <li>• ESP (Encapsulation Security Payload) transmits the encrypted data via the UDP port 4500</li> <li>• IKE (Internet Key Exchange ) is used for the key exchange via the UDP port 500</li> </ul>
Anti-spoofing	The anti-spoofing function prevents the misuse of IP addresses and obscures one's own identity.
NAT-T Keep Alive	The MD741-1 sends UDP packets through tunnel port 4500 within a fixed time frame (in this example, at 90-second intervals), so as to maintain the connection at the APN. The period after which the provider disconnects a connection without data transfer activities is not defined and must be adapted accordingly. When NAT-T Keep Alive is used, no response from the peer station is expected and thus the existence of the VPN tunnel cannot be checked in this way.

Feature	Explanation
Dead Peer Detection (DPD)	If no packets have been sent or received through the tunnel for a certain period of time (in this example after 150 seconds at the latest), the MD741-1 will send an UDP packet through port 4500. A response from the peer is expected and hence the status of the VPN tunnel will be monitored. If a failure of the VPN tunnel is identified, the MD741-1 will attempt to reconnect.

## 3.4 DSL / internet connection

The internet connection is the access point to the SINAUT control center. In this example setup, a DSL connection (Digital Subscriber Line) is used which enables the sending or receiving of data at high transmission rates. The speed of transmission differs depending on the specific DSL rate and service provider.

### Technology for DSL via telephone

Data transmission to the internet is mostly effected via a two-core copper cable connected to the telephone. It does not matter whether an analog or an ISDN telephone connection is used. This method allows to use the telephone line for voice calls and internet surfing at the same time, since the DSL data is transmitted in a different frequency range than the telephone data. A splitter separates the signals received at the telephone jack into voice and data signals. The splitter is connected to a modem which compiles the DSL-compliant data signals into computer data and vice versa. The PC can then be connected with the modem either directly or via a router.

### Requirements for the router

One advantage of a secured EGPRS connection via the internet is that the router has a **fixed IP address**. This means that the router is provided with a permanent IP address under which it is always accessible. This IP address is defined in the configuration of the MD 741-1 as a default value.

If the VPN tunnel is established via a DSL router, the router must offer the features **port forwarding** and **IPSec pass-through**. Port forwarding means that the router waits for data packages at a specified port and forwards them to a specific port in the internal network. When IPSec-based VPN tunnels are used, the ports 500 and 4500 must be forwarded to the VPN peer. Key exchange and authentication are effected via port 500, whereas port 4500 is used for NAT-T Keep-Alive, Dead Peer Detection and the ESP packets packed into UDP packages.

## 3.5 SCALANCE S

The SCALANCE S product family supports automation cells / networks from unauthorized access. The models S612/613 can be used as VPN-capable peers for the MD741-1.

### Properties of the SCALANCE S612/613 modules

SCALANCE S61x modules have the following core properties:

- Support of a secure data connection via an IPSec-secured VPN tunnel.
- VPN-Server/ Client; supports up to 64 (S612) or 128 (S613) VPN tunnels simultaneously.
- Firewall for protection against unauthorized access. The features of the firewall are:
  - Check of the data packets based on the source and target address (statefull packet inspection)
  - Support of "Non-IP" Ethernet messages
  - Band width limitation
- Router mode to operate SCALANCE S module as an NAT/NAPT router. The internal network can be used as individual subnet.
- Bridge mode to operate the SCALANCE S module in a flat network. The internal and external networks are located in a subnet.

### Configuration of the SCALANCE S module

The Security Configuration Tool (SCT) is used as a configuration tool for SCALANCE S modules and for the generation of configuration files for MD741-1. All stations can be combined to groups. The relevant assignments define which modules are allowed to communicate with each other via a VPN tunnel.

### Advantages of the interaction with MD741-1

- Both modules can be configured with the Security Configuration Tool.
- Very simple configuration process.

#### Note

For further information, please refer to the SCALANCE S manual.

See Appendix [/3/](#)

## 3.6 Security

### Security requirements

- Data confidentiality: All user data must be encrypted and protected against unauthorized access.
- Station authorization: Data communication must be allowed only for defined stations. Authentication is required.
- Packet identification: It must be ensured, that data packets arrive at their target address unchanged.
- Secrecy: Any networks behind the VPN Gateways should be concealed from third parties.

### 3.6.1 VPN tunnel

A VPN tunnel is a “virtual private network” (comparable with a LAN) via an unsecured network (Internet). This is made possible by using encrypted data packages and authentication of the stations. Authentication (proof of one's own identity or check of the peer's identity) is effected by means of a key (pre-shared key) or certificates (X.509v3 certificates).

#### Pre-shared key

The use of a pre-shared key is a symmetrical crypto-system. Each station has only one secret key for the encryption and decryption of data packets. Authentication is effected with the help of a joint password.

#### Certificates

The use of certificates is an asymmetrical crypto-system, whereby each station has one pair of keys – one secret, private key and one public key of the peer. The private key is used for the decoding of data, the generation of digital signatures and authentication. The public key enables the encryption of data packets for the peer.

The authenticity of the peer's public key (authentication) is checked by means of an additional certificate which is issued by a certification authority. For SCALANCE S modules, the CA is the group from the configuration tool SCT in which all nodes of a VPN tunnel are located. This group issues certificates to the group members and certifies them with the group certificate (CA certificate).

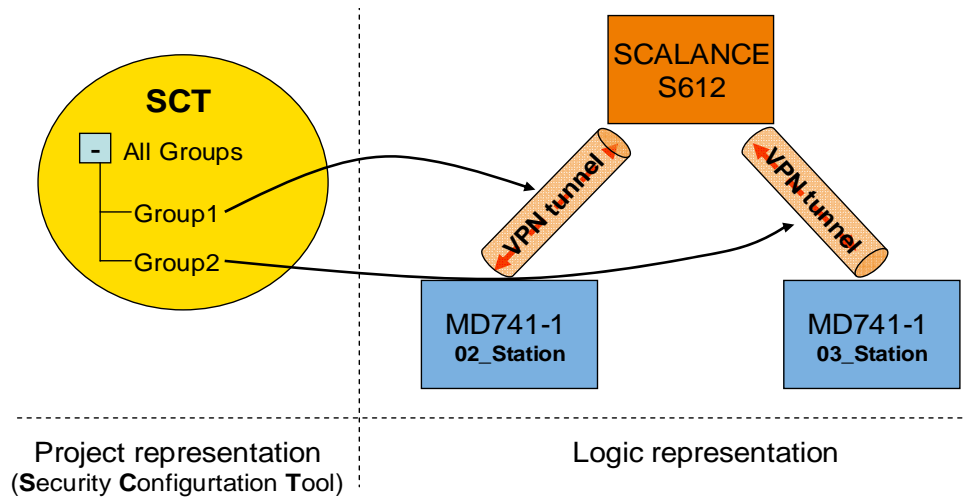
#### Note

In this example, authentication is effected by means of certificates.

**Illustration of the logic of VPN connections**

The figure below shows the logical end points of the VPN connection:

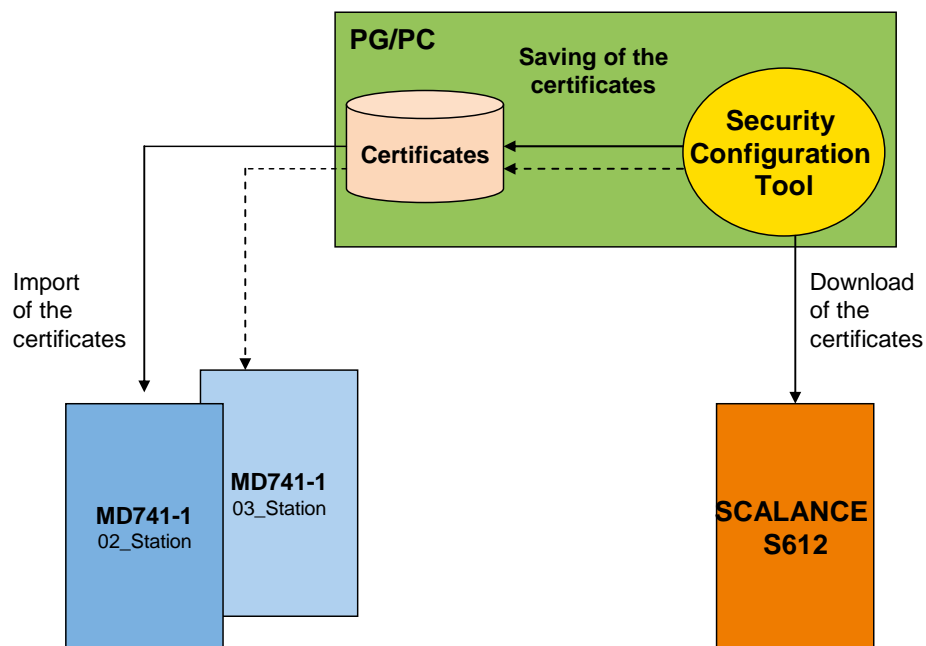
Figure 3-3



The exact correlations during configuration are explained in chapter 5 ff.

**Allocation of certificates**

Figure 3-4



**Certificates= \*.p12-file (public & private key) and \*.cer-file (CA certificate)**



### 3.6.2 IPSec

IPSec stands for IP security protocol and works on layer 3 of the OSI reference model. It is a tunneling method used in the internet for safe data transmission.

#### Targets

IPSec is aimed at:

- Station authentication
- Protection against unauthorized and unnoticed changes to the data packets (data integrity)
- Secrecy of the transmitted data packets.
- Protection against replay attacks; prevents repeated receipt of the same data package
- Key management

#### Protocols

IPSec is a standard which uses various protocols for security. The safety functions are realized with the help of the following mechanisms:

- The IP authentication header is used to manage source authentication and identification, so as to ensure data integrity.
- ESP (Encapsulation Security Payload) is used for data encryption and protects from unauthorized access.
- Security Association (SA) is an agreement between the stations regarding the live of the key, the encryption algorithm, the period valid for a new authentication.
- The Internet Key Exchange Protocol (IKE) is based on the Internet Security Association and Key Management Protocol (ISAKMP). It manages the key exchange in two phases and enables communication between the individual stations.
  - Phase 1 comprises an agreement on a key and on how the public keys of the peer can be exchanged safely (ISAKMP-SA). Then the public keys are exchanged (authentication). The CA certificate is used to check the authenticity of the key (authentication). If the life of the key has elapsed, a new key will be generated so as to ensure safe transmission of the public key.
  - Phase 2 is the encrypted data transmission with the help of the p12 certificate. If the life of the p12 certificate has elapsed, a new certificate will be generated (IPSec-SA). Phase 1 starts again.

#### Operating modes

IPSec offers two operating modes. These operating modes define how the IP data packages must be extended, so as to meet the targets of IPSec.

- The **transport mode** is used, if the cryptographic endpoints also communication send points (computer-computer connections).
- The **tunnel mode** is selected, if the cryptographic endpoints are only used as security gateways and if remote subnets are coupled via an unsecured network.

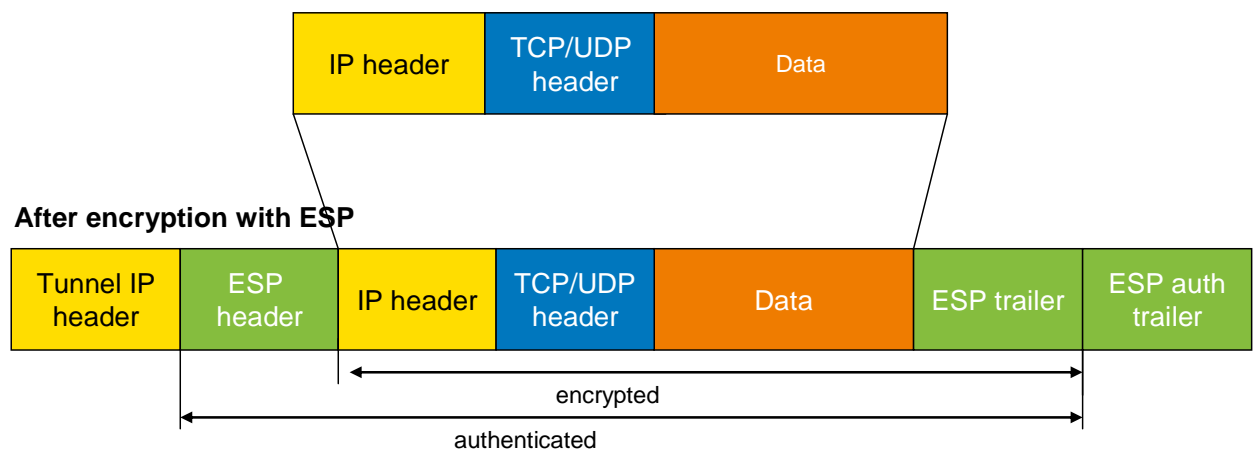
**IPSec data package**

Between the SCALANCE S612 and MD741-1 VPN connection, the data packages are transferred in tunnel mode. The VPN endpoints decode the data packages and forward them to the intended recipient.

The data packages may also be secured by using ESP and/or an authentication header (AH). The MD741-1 uses only encryption via ESP.

In tunnel mode, the entire IP data package is embedded into a new IP package. The original IP address cannot be spotted from outside anymore.

Figure 3-5

**Data package before encryption**

The following table provides a brief overview of the meaning and function of the individual headers.

Table 3-7

Header	Function
Tunnel IP header	This IP header contains the address of the cryptographic endpoint (VPN gateway).
ESP header	ESP is used to encrypt the original IP data package and the ESP trailer. The ESP header provides protection against replay attacks and contains the SPI (Security Parameters Index).
ESP trailer	If the user data volume to be transferred is smaller than the block size, the ESP trailer fills up the missing quantity and stores the number of bits added.
ESP authentication trailer	Contains the integrity test value for authentication and integrity of the message.

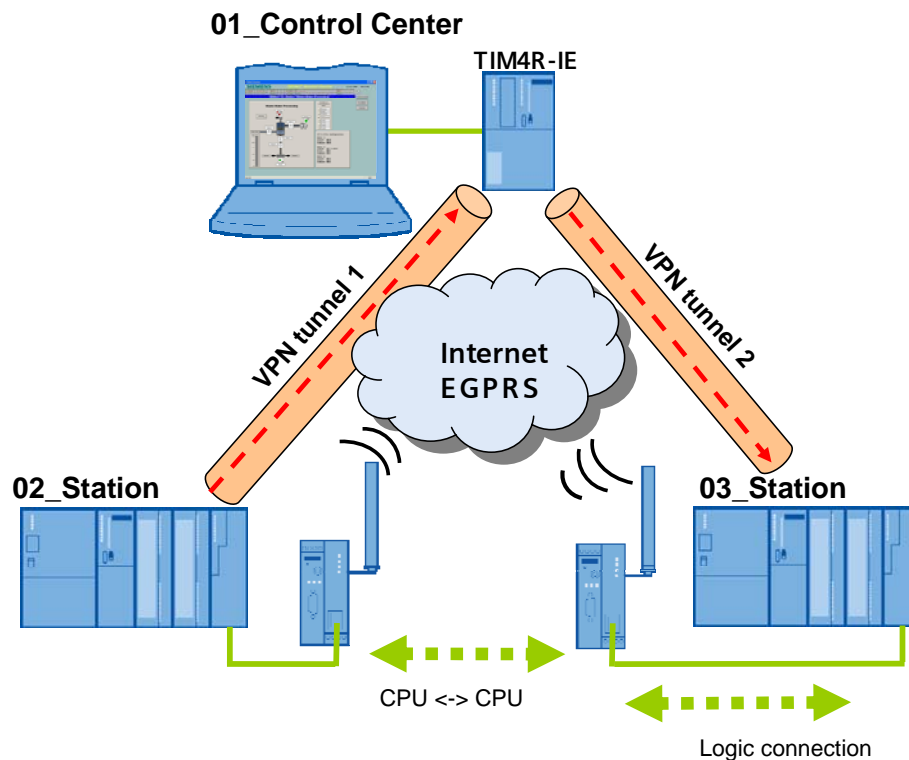
### 3.7 Cross-communication via EGPRS

Communication between the outstations (GPRS stations) is made possible with the help of a TIM4R-IE in the control center.

The GPRS stations, the 02\_Station and the 03\_Station can send and receive data between each other via the TIM4R-IE in the control center. For this purpose, the TIM4R-IE has been configured as a GPRS master.

The function principle is as follows: Station 2 sends data to station 3, for example. The telegrams are forwarded to the central TIM through VPN tunnel 1. The TIM uses VPN tunnel 2 to forward the telegrams to station 3.

Figure 3-6



## 4 Explanations on the Example Program

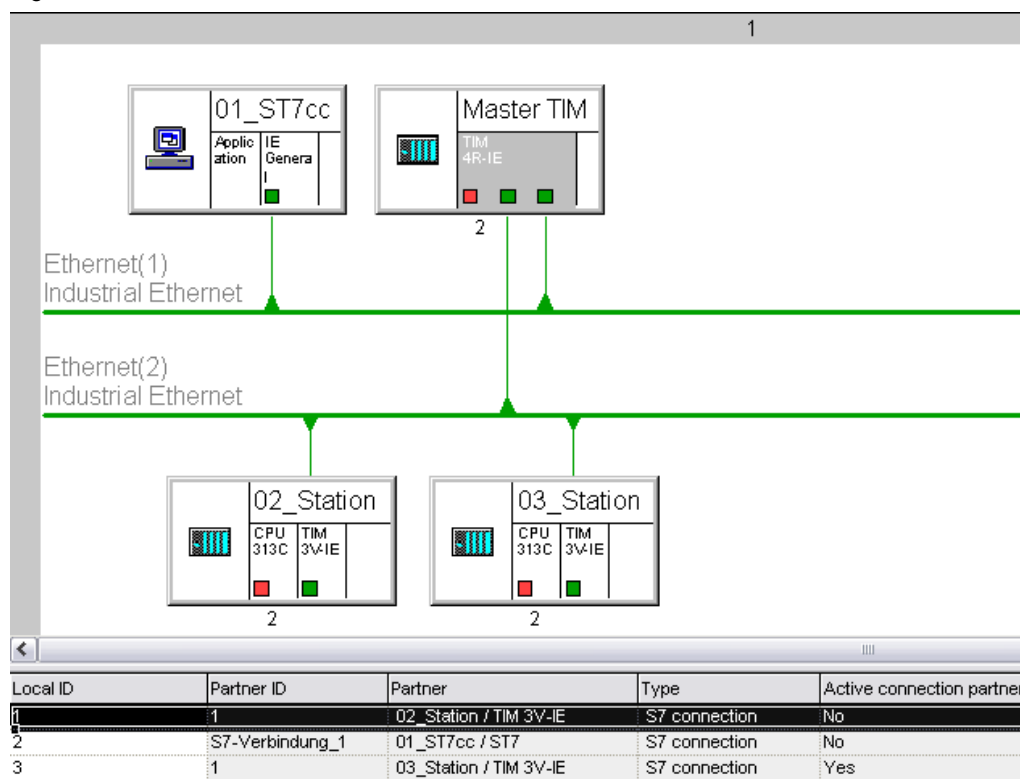
This chapter describes the required settings in NETPRO, so that the project of Volume 1 can also be used with EGPRS. These settings have already been integrated in the STEP7 project for Volume 2 and need not be defined by the user for the example project.

### 4.1 Setting the IP addresses for the ST7cc and TIMs

#### NetPro

The connection between the S7 stations and the master TIM through the VPN tunnel is a plain point-to-point Ethernet connection. The following figure shows an extract from NetPro:

Figure 4-1



#### Default router

In reality, the connection via EGRPS and internet involves several subnets. Consequently, the SIMATIC stations, the master TIM and the ST7cc control center must be informed about their default router.

#### 4.1.1 ST7cc control center

The ST7cc control center is configured as follows:

IP address: **192.168.4.2**

Subnet mask: **255.255.255.0**.

#### 4.1.2 TIM 4R-IE in the control center

The TIM4R-IE in the control center uses the SCALANCE S module as a router. For this reason, the Ethernet port of the TIM connected to the SCALANCE S module is configured as follows:

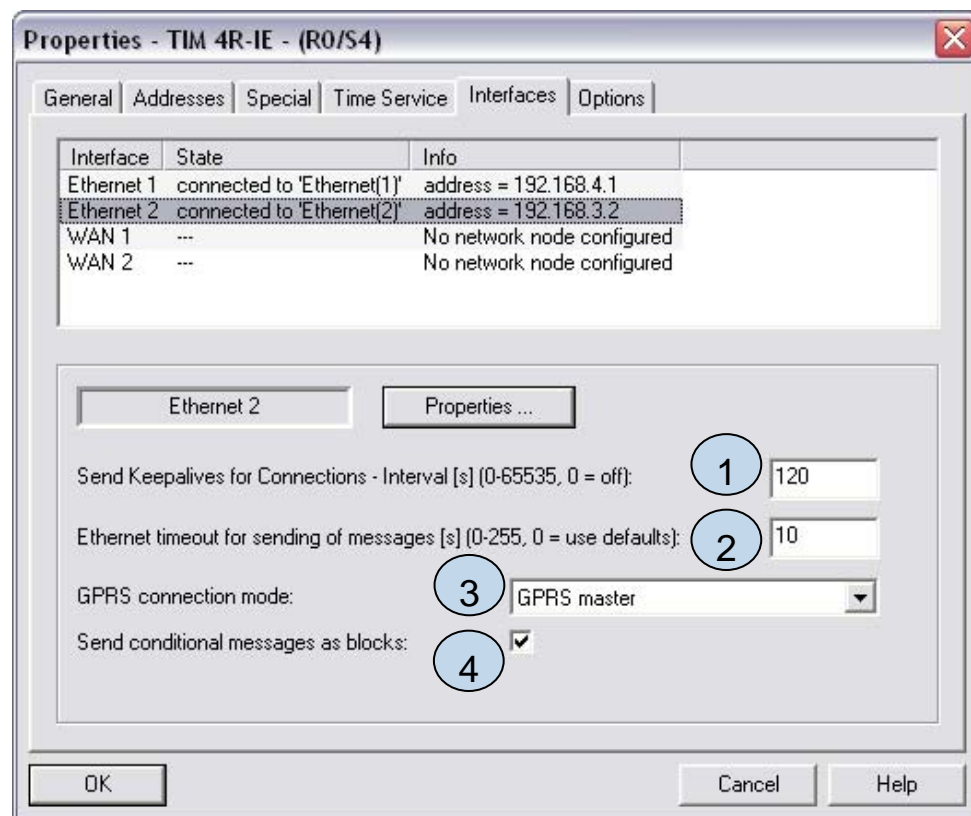
IP address: **192.168.3.2**

Subnet mask: **255.255.255.0**

Gateway: **192.168.3.1** (IP address of the secure SCALANCE S port)

The figure below shows additional settings for the master TIM, so that this TIM module will be used as GPRS master.

Figure 4-2



## 4 Explanations on the Example Program

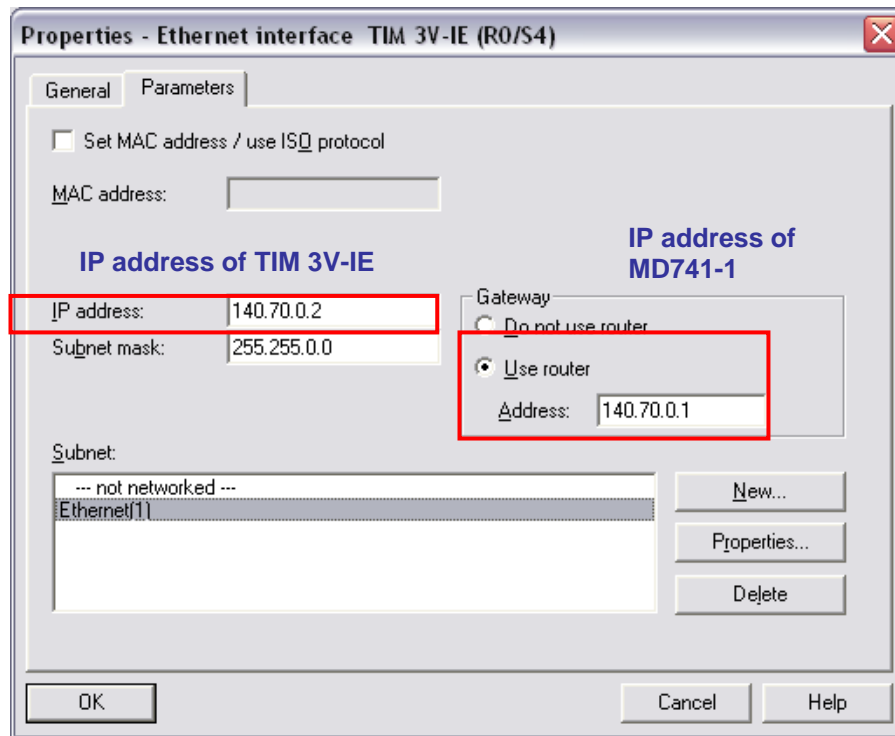
### 4.1 Setting the IP addresses for the ST7cc and TIMs

Table 4-1

No.	Property	Description
1	Send Keepalives for Connections- Interval [s]	This parameter is used to set the <b>TCP/ IP Keep Alive Interval</b> of the TIM. The period indicated should be shorter than the <b>Dead Peer Detection</b> time of the MD741-1 (150 sec). Recommended are 120 sec.
2	Ethernet timeout for sending of messages [s] (Ethernet Timeout für das Senden von Telegrammen)	Normally, a send message in the EGPRS/GPRS network is acknowledged within 1-2 seconds. During high network load this procedure may take longer. In practice, a value of 10 seconds has proven reasonable.
3	GPRS connection mode	EGPRS/GPRS is a point-to-point connection between station and control center. Cross-connections from station to station are only possible via an additional TIM 4V-IE in the control center which takes over the routing of data messages. Each TIM in the SINAUT project must give its connection node at the GPRS network: " <b>GPRS station</b> " (for all TIMs in the stations) or " <b>GPRS control center</b> " (for the TIM in the control center).
4	Send conditional messages as blocks	The activation of conditional messages enables the collection of smaller data packages in the intermediate memory of the TIM and to transmit them in larger blocks. The collected data are transmitted by the TIM: <ul style="list-style-type: none"> <li>• When they have reached 202 bytes in size.</li> <li>• If an important message must be transmitted immediately, all messages in the intermediate memory will also be transmitted.</li> <li>• If the TCP/IP Keep Alive interval has elapsed, the stored messages will be transmitted instead of the Keep Alive.</li> </ul>

### 4.1.3 Stations 2 and 3

Stations 2 and 3 use their MD741-1 routers as a gateway. The TIM module in station 2 is configured as shown in the following figure:



In addition, the TIM3V-IE module in station 2 has been configured as “**GPRS Station**” (see table 5-9 point 3). Station 3 has been configured in the same way.

## Structure, Configuration and Operation of the Application

For the startup we offer you a complete STEP 7 / SINAUT example project for download. This software example will assist you in your first steps and tests with this configuration. It offers a quick function test of the hardware and software interfaces between the products described in this document.

The software example is always assigned to the components used in this configuration and shows their basic principle of interaction. However, it is not a real application in the sense of a technological problem solution with definable properties.

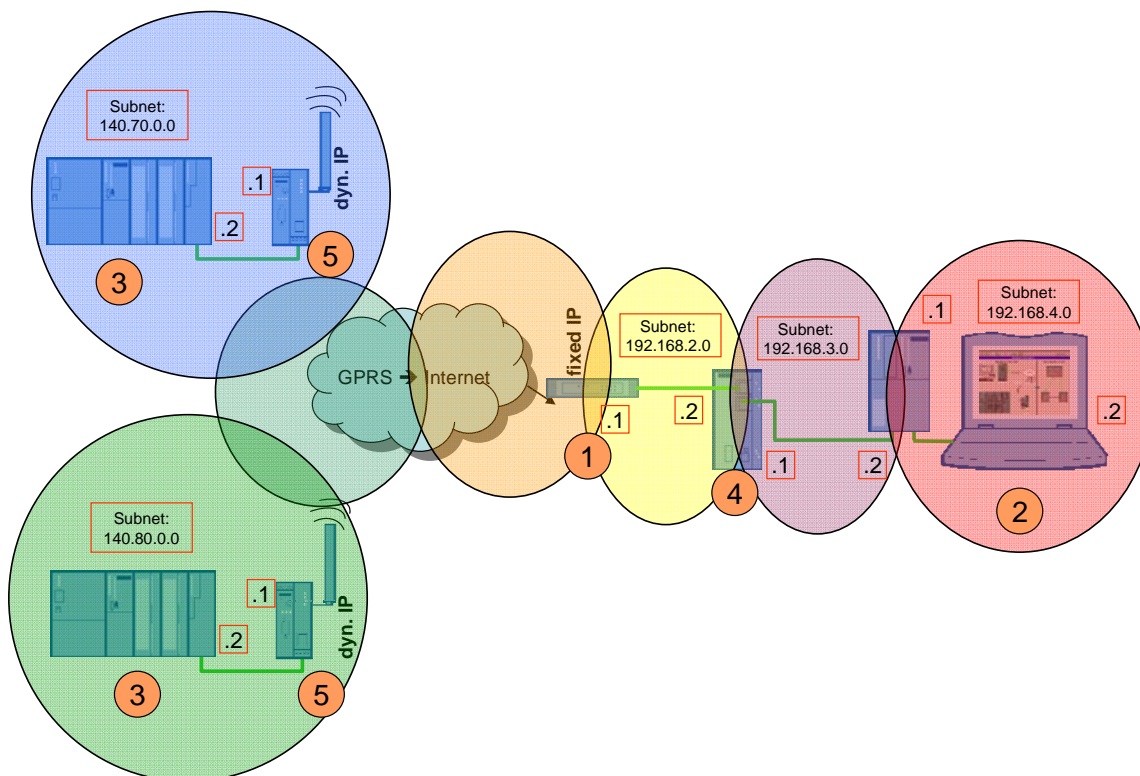
The following chapters will take you, step by step, through the necessary configuration settings.

## 5 Installation and Commissioning

### 5.1 Hardware / structural layout and software installation

The figure below shows the various subnets and configuration points relevant in this context.

Figure 5-1



The following table provides an overview of the IP addresses used. Cells of the same color belong to one subnet. Modules with two addresses (internal/external) are used as routers for the respective other subnet.



Table 5-1

Module		IP address	
		Internal	External
STATION 2	TIM 3V-IE	140.70.0.2	
	MD741-1	140.70.0.1	Dynamic from APN
STATION 3	TIM 3V-IE	140.80.0.12	
	MD741-1	140.80.0.11	Dynamic from APN
Control center	DSL router	192.168.2.1	Fixed IP from provider
	SCALANCE S612	192.168.3.1	192.168.2.2
	TIM 4R-IE	192.168.4.1	192.168.3.2
	PC/ PG	192.168.4.2	

### Installation of the standard software

The following software packages are required for this configuration:

- STEP 7
- SIMATIC NET
- SINAUT ST7
- WinCC
- SINAUT ST7cc
- Security Configuration Tool

#### Note

For the order of software installation, please refer to Volume 1.

In addition to software of Volume 1, the Security Configuration Tool is installed. Please follow the instructions of the installation program.

## 5.2 Installation of the example project

Table 5-2

No.	Action	Comment/Display
1.	Unzip the file 23810112_SINAUT_INTERNET_Code_V20.zip	In the following, the directory <b>D:\SINAUT_Configuration8</b> will be used as project directory.
2.	Unzip the file WinCC_INTERNET.zip	The WinnCC project can be found under <b>D:\SINAUT_Configuration8\WinCC_Internet\ DemoTIM3V-IE\ DemoTIM3V-IE.MCP</b>
3.	Start STEP 7 and retrieve STEP 7_INTERNET.zip to <b>D:\SINAUT_Configuration8</b>	The STEP 7 project is now filed at <b>D:\SINAUT_Configuration8\ Demo_INTERNET</b>

## 5.3 Commissioning the example project

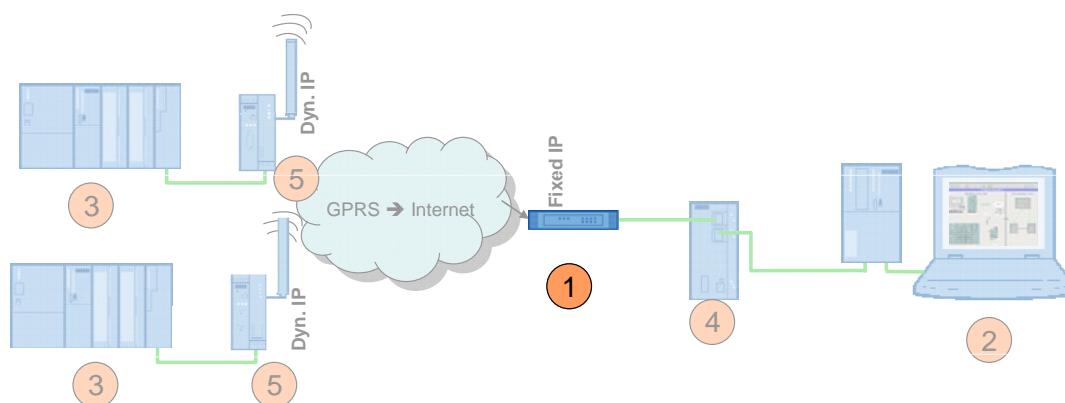
The following chapters describe the configuration steps required for the individual components.

Table 5-3

Number	Step of configuration	Chapter
1	Configuring the DSL router	5.3.1
2	Configuring the control center	5.3.2
3	Downloading the master TIM and stations 2 and 3	5.3.3
4	Configuring SCALANCE S and the VPN tunnel	5.3.4
5	Configuring MD741-1	5.3.5

### 5.3.1 Configuring the DSL router

Figure 5-2



Configuration does not refer to a specific router, since the operating displays are different for each type of router.

For most routers, a web page for configuration is available.

#### Required PC/PG IP address

Before starting configuration of the router, you must assign an IP address to your PG/PC which is located in the same network as your router.

#### Configuration

Table 5-4

No.	Action	Remarks/Notes
1.	Open the user interface for router configuration.	This may be either an additional software, "Telnet" or a web site.
2.	Enter the connection data for your internet connection.	The login, password, etc. you have received from your provider.

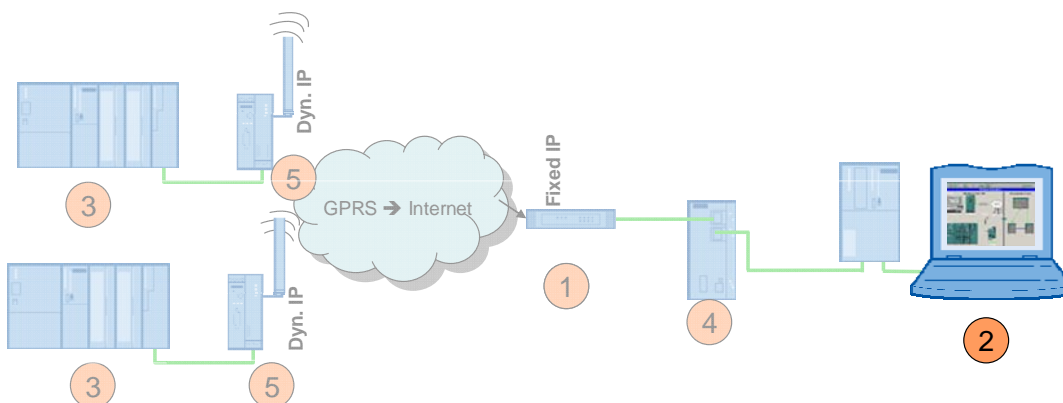
No.	Action	Remarks/Notes
3.	Switch off the DynDNS server.	Your internet access has a fixed IP address.
4.	Enter your DNS server.	You have received this address with your access data.
5.	Specify a LAN IP address for the router.	192.168.2.1
6.	Switch off the DHCP server.	SCALANCE S and the PC are assigned to a fixed address.
7.	Allocate the <b>UDP ports 500 and 4500</b> to the same ports as SCALANCE S.	UDP port 500 to UDP port 500 of 192.168.2.2 UDP port 4500 to UDP port 4500 of 192.168.2.2

**Note**

Some routers are provided with an “IPSec Pass through” function. Activate this function (if explicitly available at your router) so as to support IPSec.

### 5.3.2 Configuring the control center

Figure 5-3



The following settings are to be made:

- assign an IP address
- change the computer name to CONTROLROOM
- initial startup of the PC station:
  - setting the Components Configurator
  - setting the access point

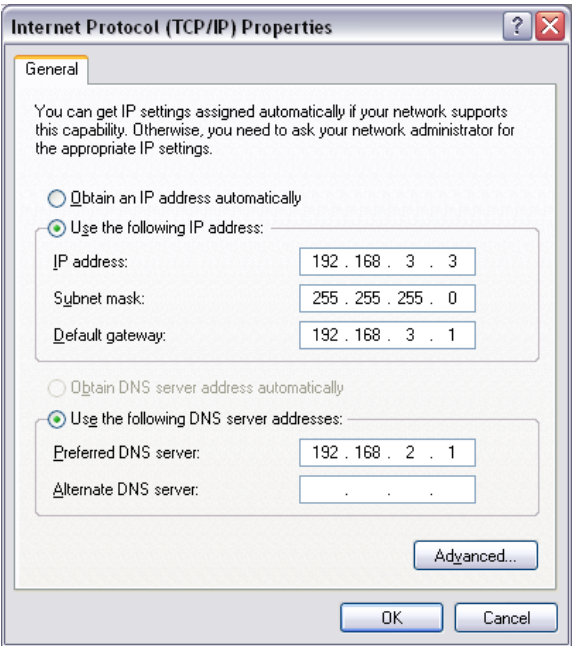
#### Changing the IP address

Because of the various module downloads (SCALANCE S, MD741-1, TIM) the IP address of the PCs/PGs needs to be changed several times. This section describes the steps required for this procedure. The figure below shows the network settings of the PG/PC to be defined at the end of the configuration procedure (after chapter 5.3.7)!

## 5 Installation and Commissioning

### 5.3 Commissioning the example project

Table 5-5

No.	Action	Remarks/Notes
1.	<p>Open the Internet Protocol (TCP/IP) Properties by selecting</p> <p>“Start &gt; Settings &gt; Network Connection &gt; Local Connections”.</p> <p>Select the options field</p> <p>“Use following IP-address”</p> <p>and fill in the fields as shown in the screenshot on the right.</p> <p>Select the options field “Use the following DNS Server” and enter the DNS server as shown in the screenshot.</p> <p>Click “OK” to close this dialog.</p>	
2.	If your PG is provided with an IWLAN interface, switch it off.	

#### Computer name and PC station

Volume 1 includes a detailed step-by-step description of how to rename the computer and how to configure the PC station for initial operation. (See chapter 6.3.1 and 6.3.4 of Volume 1.)

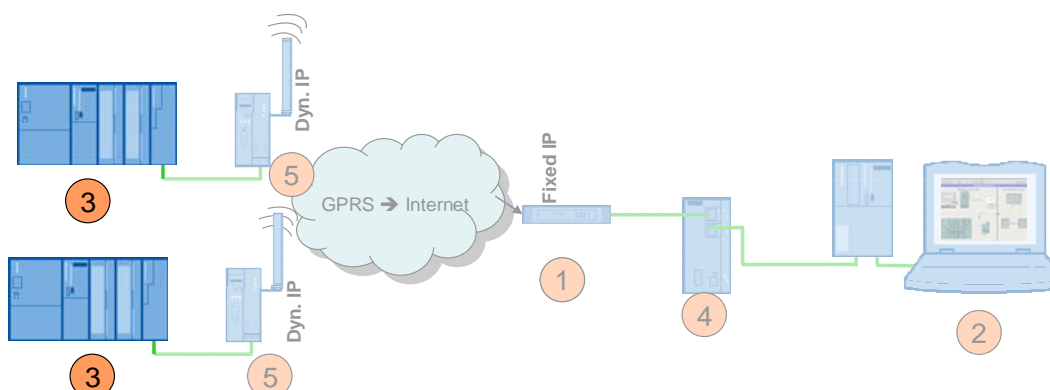
#### Note

The STEP 7 project for this Volume 2 is included in the delivery and will be used as a basis for the configuration of the PC station.

Please make sure to use the IP address and xdb-file defined for Volume 2. (See Table 5-1)

### 5.3.3 Downloading the master TIM and the stations 2 and 3

Figure 5-4



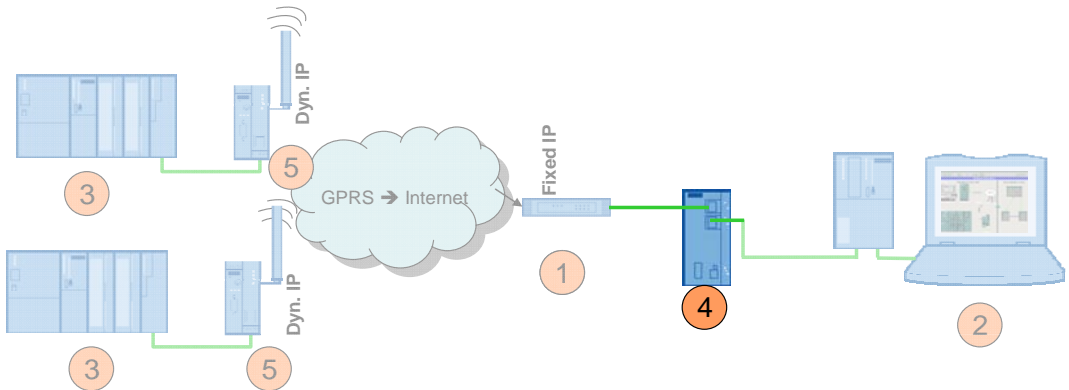
Configuration of the stations and the master TIM is based on the STEP 7 project, which is included in the delivery and already preconfigured with the correct IP addresses for Volume 2.

Table 5-6

No.	Action	Remarks/Display
3.	When downloading the SINAUT <b>02_Station</b> , please change the IP address of your PC/PG as follows: IP address: <b>140.70.0.20</b> Subnet mask: <b>255.255.0.0</b>	
4.	Before the STEP 7 project can be downloaded to the CPU, the IP address of the TIM module must be changed as shown in Table 5-1.	How to configure the IP address in the TIM is described in Volume 1, chapter 6.3.2.
5.	Use the cross-connection cable to connect the PC/PG with the TIM for downloading.	Make sure that the TIM 3V-IE is assigned to the IP address <b>140.70.0.2</b> and the subnet mask to 255.255.0.0.
6.	Repeat this procedure for station 3 and for the master TIM.	Use an uncrossed patch cable for the master TIM.
7.	Then set the IP address of the PC as shown in Table 5-1.	

5.3.4 Configuring SCALANCE S and the VPN tunnel

Figure 5-5



This section shows all steps necessary in the Security Configuration Tool for the setup of two VPN tunnels to the MD741-1 routers in the stations.

**Note** Before you start configuration, reset the SCALANCE S612 to factory settings. This ensures that no other certificates / VPN connections will be saved in the SCALANCE S module and that the IP address of SCALANCE S is set to 0.0.0.0.

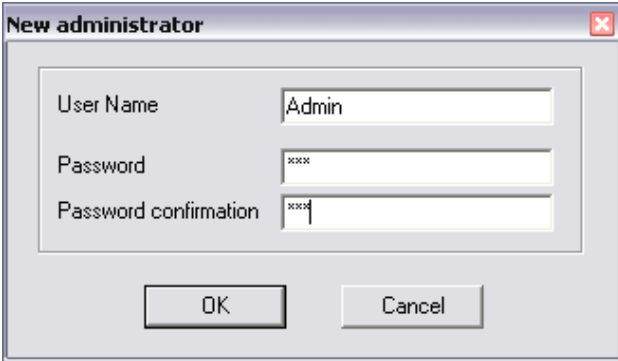

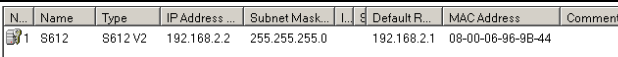
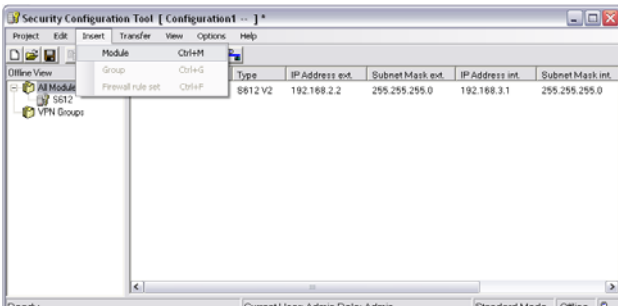
The SCALANCE S manual, chapter 2.1.7 /3/, includes an instruction for the reset of configuration to factory settings.

For SCALANCE S configuration, enter the IP address **192.168.2.3** for your PC/PG (subnet mask 255.255.255.0).

VPN tunnel configuration for stations 2/3 – SCALANCE S in the control center

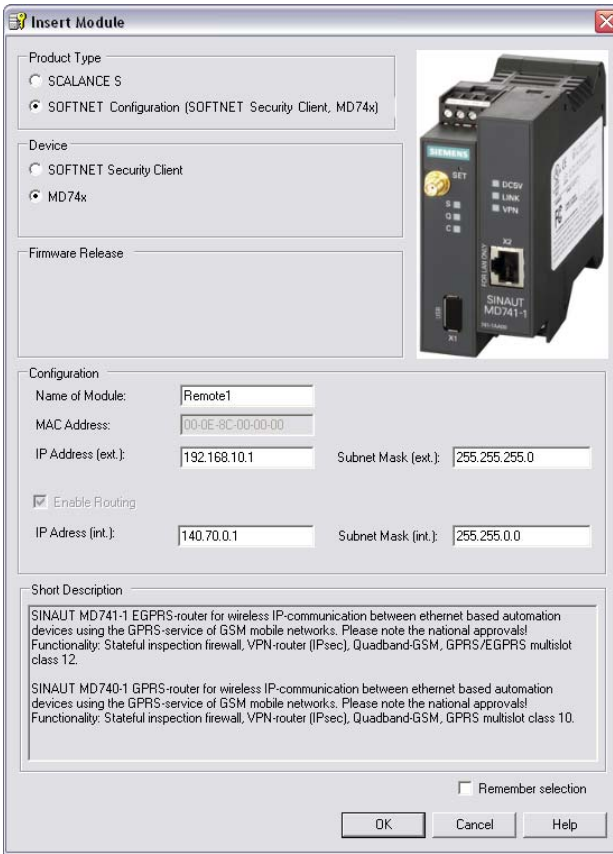
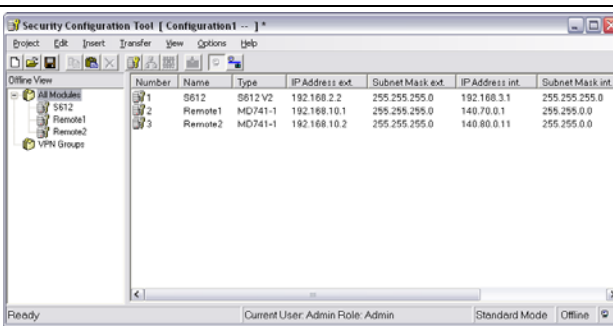
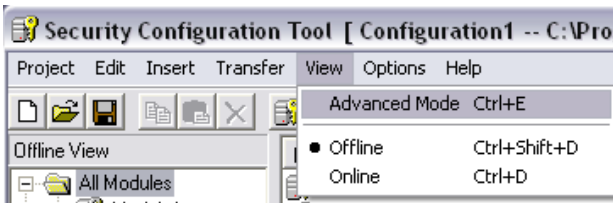
Table 5-7

No-	Action	Remarks / Notes
1.	Select “Start > SIMATIC > SCALANCE > Security > Security Configuration Tool” to open the Security Configuration Tool (SCT).	

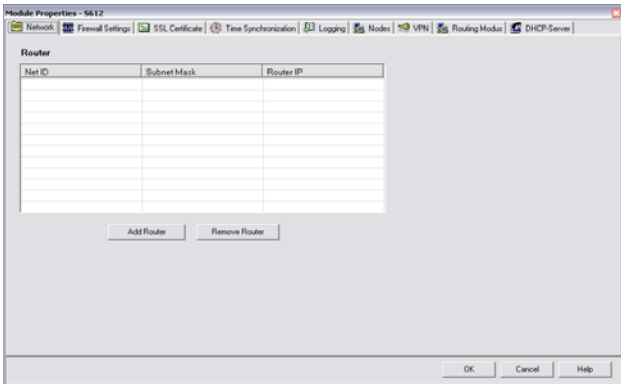
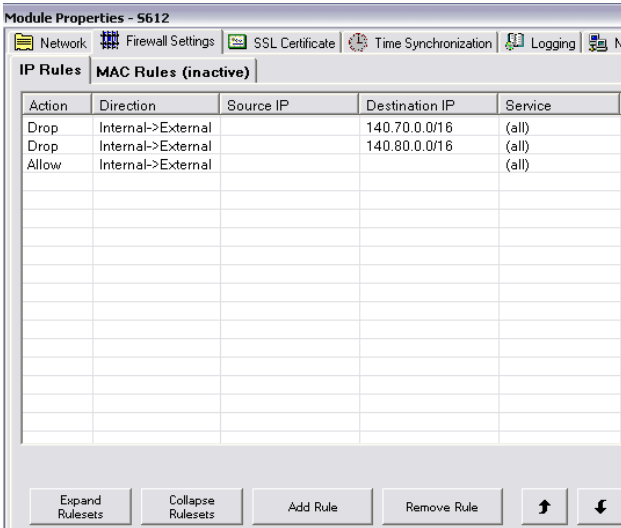
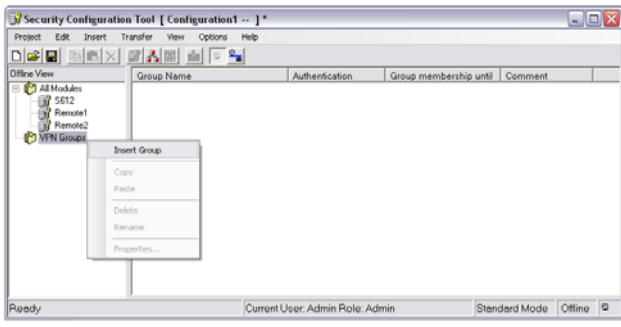
No-	Action	Remarks / Notes
2.	Select "Project > New" to create a new project. You will be prompted to enter a user name and password for the new project. Fill in this dialog (e.g. User Name: Admin, Password: VPN), then click <b>OK</b> to close this box.	 The "New administrator" dialog box is shown. It has three input fields: "User Name" with the text "Admin", "Password" with "xxxx", and "Password confirmation" with "xxxx". There are "OK" and "Cancel" buttons at the bottom.
3.	The <b>Insert Module</b> dialog opens. Configure the SCALANCE S module first. In this example, the type S612, V2 is used. Enter a name and the MAC address for this module.  The <b>MAC address</b> is printed on the front casing of your SCALANCE S.  In this example, the external address as shown in the screenshot is used. Activate the option " <b>Enable Routing</b> " and enter the internal IP address. Click OK to confirm your settings.	 The "Insert Module" dialog box is shown. It has several sections: "Product Type" with radio buttons for "SCALANCE S" (selected) and "SOFTNET Configuration"; "Device" with radio buttons for "S602", "S612" (selected), and "S613"; "Firmware Release" with radio buttons for "V2" (selected) and "V1"; "Configuration" with fields for "Name of Module:" (S612), "MAC Address:" (08-00-06-96-97-E3), "IP Address (ext.):" (192.168.2.2), "Subnet Mask (ext.):" (255.255.255.0), a checked "Enable Routing" checkbox, "IP Address (int.):" (192.168.3.1), and "Subnet Mask (int.):" (255.255.255.0); and "Short Description" with a text area. There are "OK", "Cancel", and "Help" buttons at the bottom right. A small image of the SCALANCE S module is shown on the right.
4.	Define the internal IP address of your DSL router as <b>Default Router</b> in the module line. In this example, the address is 192.168.2.1.	 A table showing the configuration of modules. The table has columns: N., Name, Type, IP Address, Subnet Mask, I., Default R., MAC Address, and Comment. The first row shows: 1, S612, S612 V2, 192.168.2.2, 255.255.255.0, I., 192.168.2.1, 08-00-06-96-9B-44, and an empty comment.
5.	Select "Insert > Module" to add a new module.	 The "Security Configuration Tool" interface is shown. It has a menu bar with "Project", "Edit", "Insert", "Transfer", "View", "Options", and "Help". Below the menu bar is a toolbar with icons for "Module", "Group", "Ctrl+M", "Ctrl+G", and "Ctrl+F". The main area shows a tree view with "All Modules" and "VPN Groups". A table at the bottom shows the configuration of modules, similar to the one in the previous step.

## 5 Installation and Commissioning

### 5.3 Commissioning the example project

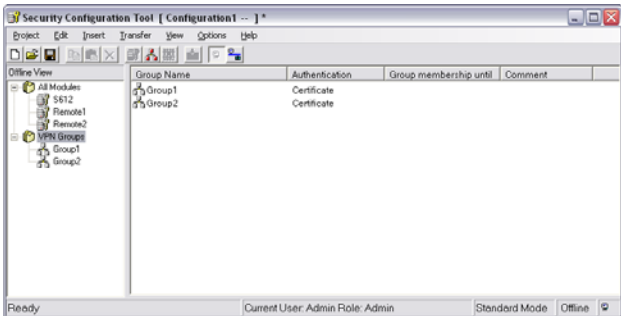
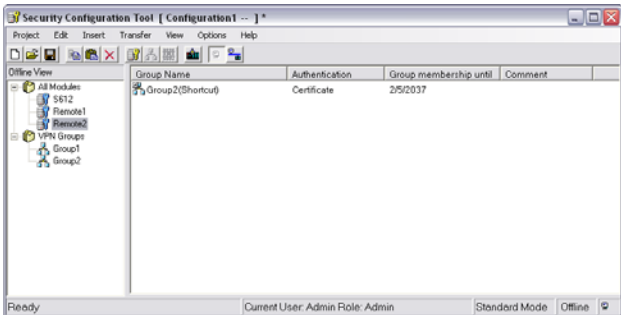
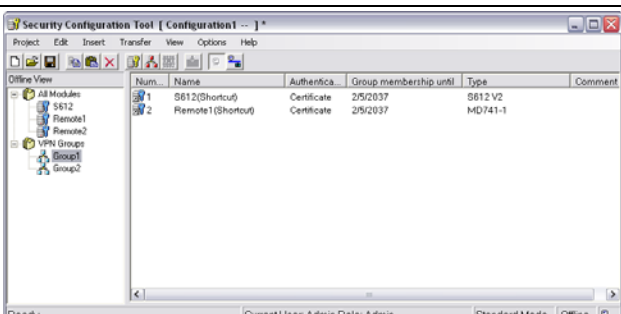
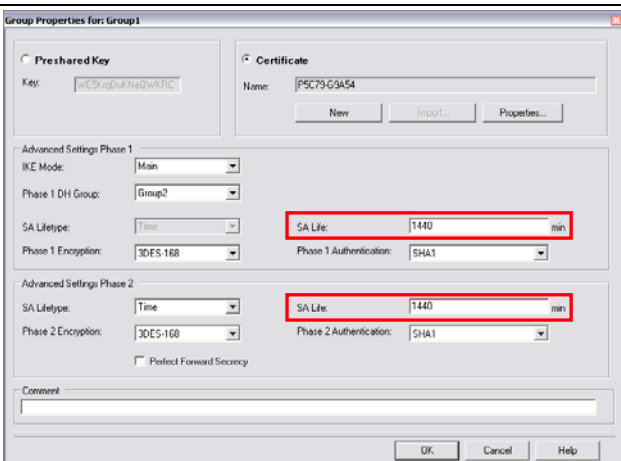
No-	Action	Remarks / Notes
6.	<p>Select <b>SOFTNET Configuration</b> and then <b>MD74X</b>.</p> <p>Configure the MD741-1 as shown in the screenshot.</p> <p><b>Note:</b> The SCT requires an external IP address for the MD741-1 router. Since this IP address is assigned dynamically by the mobile service provider, it cannot be entered here. For this reason, just use the default IP address of the SCT (here: 192.168.10.1).</p>	
7.	Select "Insert > Module" to add a new module.	
8.	<p>Specify the second MD741-1 as follows.</p> <p><b>Name:</b> Remote2</p> <p><b>Type:</b> MD741-1</p> <p><b>IP Address ext.:</b> leave the default settings unchanged</p> <p><b>Subnet Mask ext.:</b> leave the default settings unchanged</p> <p><b>IP Address int.:</b> 140.80.0.11</p> <p><b>Subnet Mask int.:</b> 255.255.0.0</p> <p>Save your project.</p>	
9.	<p>Select "View &gt; Advanced Mode" to change over to the SCT advanced mode menu.</p> <p>Confirm the next dialog with <b>Yes</b>. The advanced mode offers extended setting options.</p>	

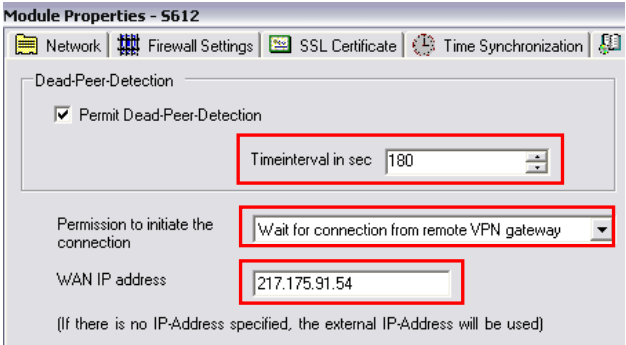
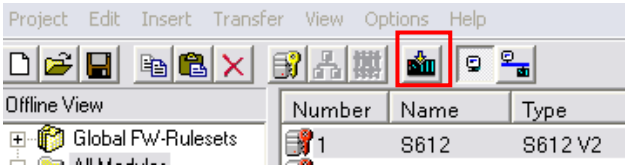
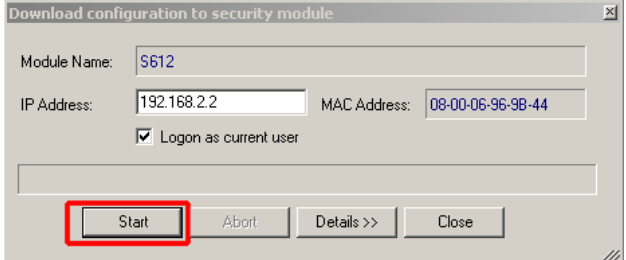
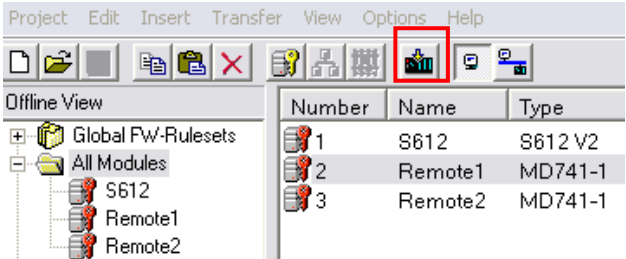


No-	Action	Remarks / Notes
10.	Select the first module line (SCALANCE S module). Doubleclick to open the Properties dialog.	
11.	<p>If you have used the function <b>NAT active</b> in step 10, proceed as follows:</p> <p>Open the <b>Firewall Settings</b> tab. Click the <b>Add Rule</b> button to add a new drop rule. Enter the IP address of the remote subnet as <b>Destination IP</b>.</p> <p>Remote1: 140.70.0.0/16 (MD741-1 in Station_02) Proceed in the same way for the second router. Remote2: 140.80.0.0/16 (MD741-1 in Station_03)</p> <p>Finally, add an Allow Rule for internet access from your local network (SCALANCE local network) via the SCALANCE and DSL router. Click <b>OK</b> to confirm your settings.</p>	 <p>A drop rule should be defined for each target subnet. If no VPN tunnel has been established yet, all packages addressed to the MD741-1 will be rejected.</p> <p>The last firewall rule allows all remaining packages destined to other stations. This rule causes that the firewall will be open from internal to external for all packages which have not been rejected.</p>
12.	Select the <b>VPN Groups (All Modules)</b> in <b>Offline View</b> and click your right mouse button. Select "Insert Group" to create a new group. Repeat this procedure once again.	 <p><b>Note:</b></p> <p>As an alternative, you may configure all modules of the same group. In this case, the VPN properties and the certificates will be identical for all MD741-1 routers.</p>

## 5 Installation and Commissioning

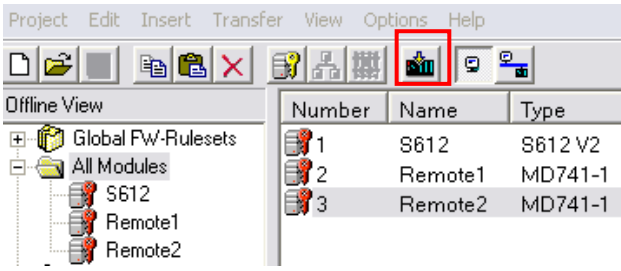
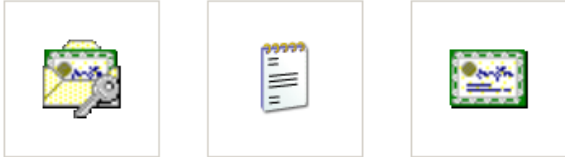
### 5.3 Commissioning the example project

No-	Action	Remarks / Notes
13.	<b>Group1</b> shall include <b>S612</b> and <b>MD741-1 Remote1</b> . Select the modules <b>S612</b> and <b>Remote1</b> separately in the same column and move them to <b>Group1</b> by drag&drop.	
14.	<b>Group2</b> shall include <b>S612</b> and <b>MD741-1 Remote2</b> . Select the modules <b>S612</b> and <b>Remote2</b> separately in the same column and move them to <b>Group2</b> by drag&drop.	 <b>Note:</b> A group represents a VPN connection. Only stations included in this group can communicate via the VPN tunnel.
15.	Select <b>Group1</b> , for example. All stations of this group, and thus of a VPN connection, will be listed.	
16.	The group properties of each group are to be edited. Double click the group to open the relevant Properties dialog.	
17.	Change the SA Lifetimes settings to 1440 minutes. Click OK to close the dialog.  Proceed in the same way for the other group!	

No-	Action	Remarks / Notes
18.	Return to the module lines and select the first module line (SCALANCE S).	
19.	Open the Properties dialog for the SCALANCE S module with a double-click. Select the <b>VPN</b> tab. Set the <b>Dead-Peer-Detection</b> interval to 180 seconds. This function prevents the display of obsolete VPN tunnels in online view. The SCALANCE S <b>waits for connection</b> of the MD741-1. Change the permission to initiate connection accordingly. Specify the <b>WAN IP address</b> by entering the <b>fixed IP address</b> of your DSL router. Click <b>OK</b> to close this dialog.	 <p><b>Module Properties - S612</b></p> <p>Dead-Peer-Detection</p> <p><input checked="" type="checkbox"/> Permit Dead-Peer-Detection</p> <p>Timeinterval in sec: 180</p> <p>Permission to initiate the connection: Wait for connection from remote VPN gateway</p> <p>WAN IP address: 217.175.91.54</p> <p>(If there is no IP-Address specified, the external IP-Address will be used)</p> <p>Note:</p> <ul style="list-style-type: none"> <li>The Dead-Peer-Detection function for SCALANCE S must be set to a higher value than that of the MD741-1. (The MD741-1 is set to 150 seconds by default)</li> <li>DynDNS is not supported by SCALANCE S.</li> </ul>
20.	Connect your PC/PG with the external port of the SCALANCE S.	The factory settings do not include an IP address for the SCALANCE S. For download, the indicated MAC address is used.
21.	Load the configuration into the SCALANCE S. Select the SCALANCE S module line in the right window and click the <b>Transfer</b> icon.	
22.	In the next dialog, click the <b>Start</b> button to initiate transmission.	
23.	Create another directory named <b>MD741_Remote1</b> under <b>D:\SINAUT_Configuration8</b> . Save the configuration for the MD741-1 of <b>Remote Station1</b> in this directory. Select the modem module line 2 and click the <b>Transfer</b> icon. Define the previously created directory as target directory for the configuration files and certificates. Acknowledge the next dialog with <b>Yes</b> for a new certificate password or with <b>No</b> to use a default password.	 <p>The .p12 certificate is password protected. You can either use the project name of the SCT as password or define a new one.</p> <p><b>Note:</b> We recommend to define a new password.</p>

## 5 Installation and Commissioning

### 5.3 Commissioning the example project

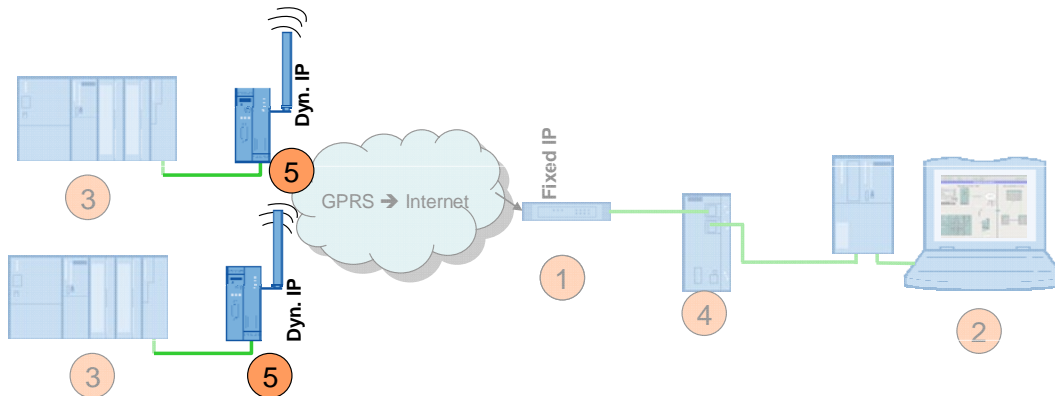
No-	Action	Remarks / Notes
24.	<p>Create another directory named <b>MD741_Remote2</b> under <b>D:\SINAUT_Configuration8</b>. Save the configuration for the MD741-1 of <b>Remote Station2</b> in this directory</p> <p>Continue in the same way as for the other MD741-1 of Remote Station1.</p>	 <p><b>Note:</b> Please save the certificates for the second station in a new directory, as recommended. Otherwise, any peer certificates with the same name will be saved to the same directory and overwritten.</p>
25.	<p>The target directory includes a text file for configuration of the MD741-1, the CA certificate and the p12 certificate.</p>	 <p>Configuration1.MFBA3@ Configuration1.Remot... Configuration1.S612.cer G9A54.Group1.p12</p>

**Note** If you use the MD740-1 router (instead of MD741-1), configure both remote stations in one VPN group by moving the two MD740-1 units into one group by drag&drop.

**Note** The MD740-1 routers should always be included in one VPN-group.

### 5.3.5 Configuring MD741-1

Figure 5-6



Commissioning of the MD741-1 router is performed in three steps:

- configure the PIN settings
- insert the SIM card into the device
- further configuration settings

#### Required PC/PG IP address

Table 5-8

Action	Settings
When configuring the MD741-1 router, assign an IP address to your PG/PC which is located in the same network as your MD741-1.	After delivery or after reset to factory settings, the address of the MD741-1 is set to 192.168.1.1.

### 5.3.6 MD741-1 of 02\_Station

#### Step 1: PIN configuration

To enable communication of the MD741-1 router via the GPRS network, the device must know the PIN of the SIM card.


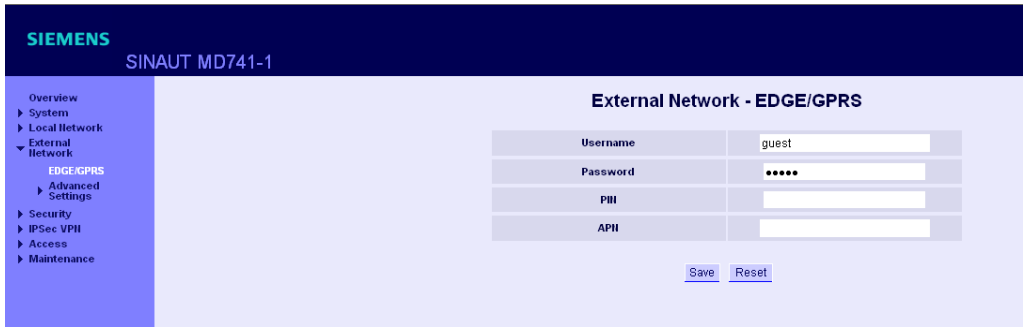
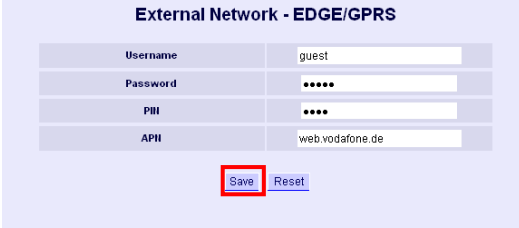
**ATTENTION** Enter the PIN for the MD741-1 router before you insert the SIM card.

Table 5-9

No.	Action	Remarks/Notes
1.	Connect the PC with the Ethernet connector of the MD741-1.	After delivery or return to factory settings, the address of the MD741-1 is set to 192.168.1.1.
2.	Start a browser and enter the address <b>https://[ip-adresse MD741-1]</b> .	Acknowledge the safety prompt that appears after successful connection setup with <b>Yes</b> .
3.	Enter the user name and password.	The default settings are: <b>User name: admin</b> <b>Password: sinaut</b>


## 5 Installation and Commissioning

### 5.3 Commissioning the example project

No.	Action	Remarks/Notes
4.	The administrator website opens. The default language is German. In the drop-down menu in the top right corner you can change the language. Click <b>Go</b> to accept this language setting for the MD741-1.	
		
5.	Select "External Network > EDGE/GPRS".	
		
6.	<p>Enter the access data for your APN in the <b>Username</b> and <b>Password</b> fields (identical in both lines). The default setting in these two fields is <b>guest</b>.</p> <p>For Vodafone: <b>Username: guest</b> <b>Password: guest</b></p> <p>Enter the address of your access point name in the <b>APN</b> field.</p> <p>For Vodafone: <b>web.vodafone.de</b></p> <p>For T-Mobile: <b>internet.t-mobile</b></p> <p>Enter the PIN of your SIM card in the <b>PIN</b> field. Click the <b>Save</b> button to save your settings.</p>	

## Step 2: Inserting the SIM card

Table 5-10


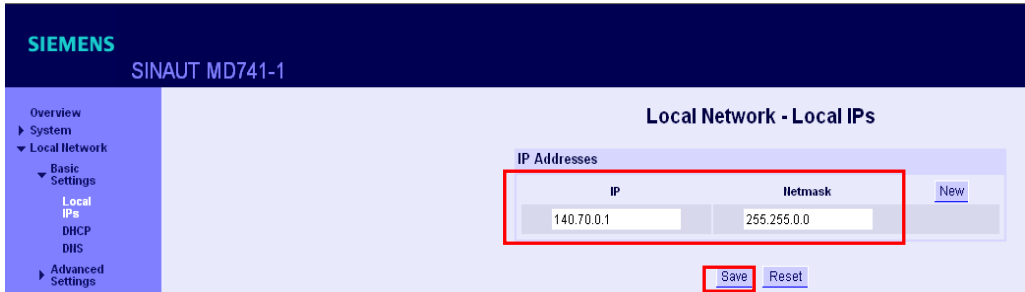
No.	Action	Remarks/Notes
1.	Disconnect the MD741-1 router from power.	
2.	Insert the SIM card as shown in the picture and connect the router to power again.	

### Note

The MD741-1 router will now attempt to establish a connection to the EGPRS/GPRS network. After successful connection setup, LED S (Status) lights up statically. LED C (connect) is ON with short interruptions, if the MD741-1 is logged in at GPRS, and it lights up statically, if the MD741-1 is logged in at EGPRS. LED Q (quality) indicates the field intensity.

**Step 3: Further configuration settings****IP address**

Table 5-11

Nr	Action	Remarks/Notes
1.	Open the administrator website for the MD741-1 again. Select the <b>Overview</b> screen for information about the connection in the EDGE or GPRS network, the signal strength and the IP address assigned by the provider.	
		
2.	<p>Select "Local Network &gt; Basic Settings &gt; Local IPs". Change the internal IP address of the MD741-1 according to Table 5-1.</p> <p>Click <b>Save</b> to accept your settings.</p> <p><b>Note:</b> After this step, you have to adjust the IP address of your PC/PG accordingly (e.g. 140.70.0.20) before you open the website of the MD741-1 again.</p>	
		



## Configuring the VPN connection

**Note** For further configuration settings, please read the text file generated by the Security Configuration Tool.

Figure 5-7

**MD741-1**

{  
Configuration of MD741-1: Remote1

**1** IPsec VPN > Certificates > Upload \*.p12-file  
Configuration1.MFBA3@G9A54.Group1.p12

IPsec VPN > Certificates > Upload remote certificate  
X.509 Zertifikat Configuration1.S612.cer

**2** IPsec VPN > Conections - Edit Settings  
Remote1 in connection with S612  
Authentication method: X.509 Zertifikat Configuration1.S612.cer  
Remote ID: MC268@G9A54  
Local net address: 140.70.0.0  
Local subnet mask: 255.255.0.0  
Remote net address: 192.168.3.0  
Remote subnet mask: 255.255.255.0  
Address of the remote site's VPN gateway: 217.175.91.54

**3** IPsec VPN > Conections - Edit IKE  
**Settings Phase 1 - ISAKMP SA**  
ISAKMP-SA encryption: 3DES-168  
ISAKMP-SA hash: SHA1  
ISAKMP-SA mode: Main Mode  
ISAKMP-SA lifetime: 86400  
  
**Settings Phase 2 - IPsec SA**  
IPsec-SA encryption: 3DES-168  
IPsec-SA hash: SHA1  
IPsec-SA lifetime: 86400  
  
DH/PFS-group: DH-2 1024  
NAT-T: AN  
DPD-delay: 150 seconds  
DPD-timeout: 60 seconds  
DPD-maximum failures: 5  
}

## 1

## Upload certificates

Figure 5-8

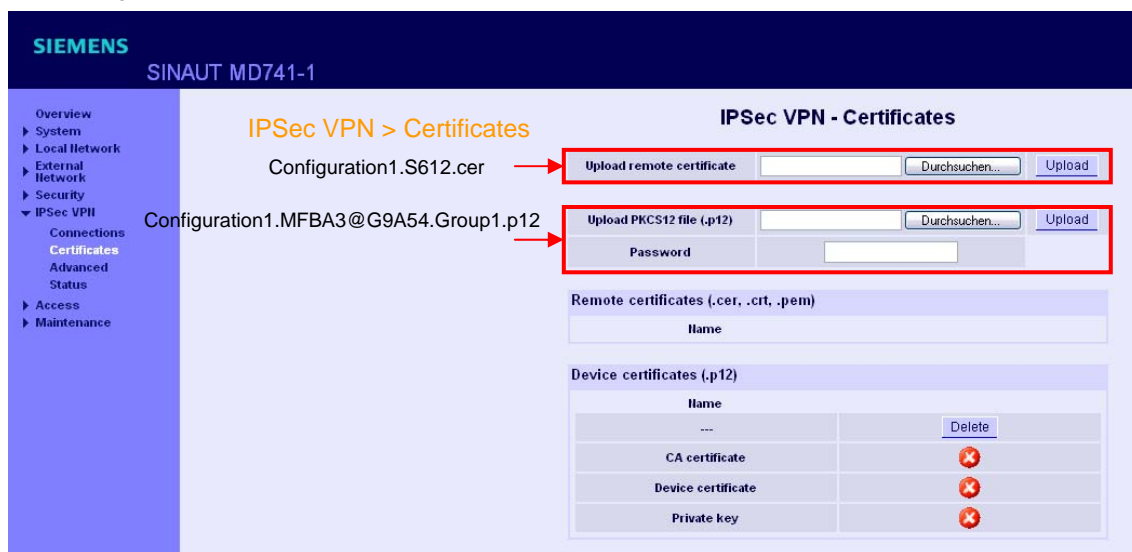


Table 5-12

No.	Action	Remarks/Notes
1.	Change over to "IPSec VPN > Certificates". Click the <b>Browse</b> button to find the directory where the configuration data and certificates for the MD741-1 are stored.	D:\SINAUT_Configuration8MD741_Remote 1
2.	Open the remote certificate (.cer) stated in your text file.	Here: Configuration1.S612.cer
3.	Click the <b>Upload</b> button to import the certificate. In the <b>Remote Certificates</b> field you can see that the certificate has been imported.	
4.	Import your own certificate (p.12) by clicking the <b>Browse</b> button to find the directory where the configuration data and certificates for the MD741-1 are stored.	
5.	Open your own certificate (.p12) stated in your text file.	Here: Configuration1.MFBA3@G9A54.Group1.p12
6.	Enter the password you have specified for the certificate in the Security Configuration Tool.	Use either the SCT project name or a new password.

No.	Action	Remarks/Notes
7.	Click <b>Upload</b> to import the certificate. In the <b>Device Certificates</b> field you can see that the certificate has been imported.	<div><div>IPSec VPN - Certificates</div><div><div>Upload remote certificate</div><div><div></div></div><div>Durchsuchen...</div><div>Upload</div></div><div><div>Remote certificates (.cer, .crt, .pem)</div><div><div>Name</div><div>Configuration1.S612.cer</div><div>Delete</div></div></div><div><div>Device certificates (.p12)</div><div><div>Name</div><div>Configuration1.MFBA3@G9A54.Group1.p12</div><div>Delete</div></div><div><div>CA certificate</div><div></div><div>✓</div></div><div><div>Device certificate</div><div></div><div>✓</div></div><div><div>Private key</div><div></div><div>✓</div></div></div></div>

## 2 Create and edit a connection

Table 5-13


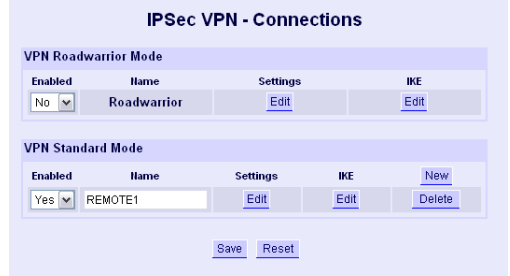
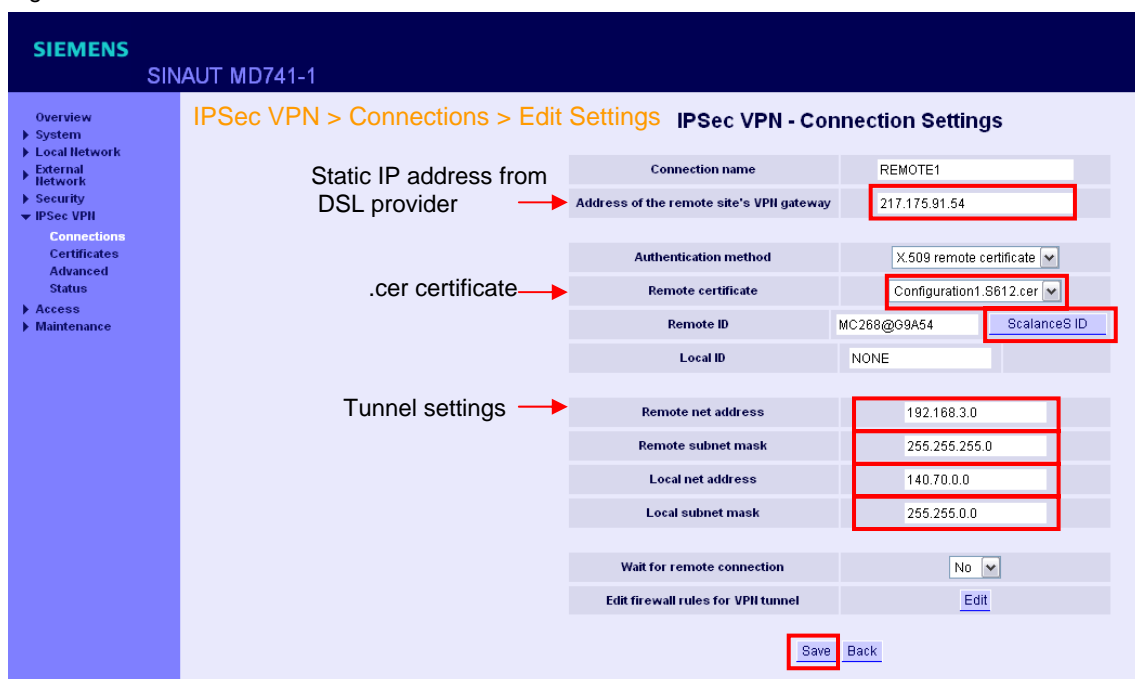
No.	Action	Remarks/Notes
1.	Select "IPSec VPN > Connections".	
2.	Click <b>New</b> to create a new connection and define a new name. In this example the connection name <b>REMOTE1</b> has been chosen.  Click <b>Save</b> to confirm your settings.	

Figure 5-9



SIEMENS SINAUT MD741-1

IPSec VPN > Connections > Edit Settings IPSec VPN - Connection Settings

Static IP address from DSL provider → Address of the remote site's VPN gateway: 217.175.91.54

.cer certificate → Remote certificate: Configuration1.S612.cer


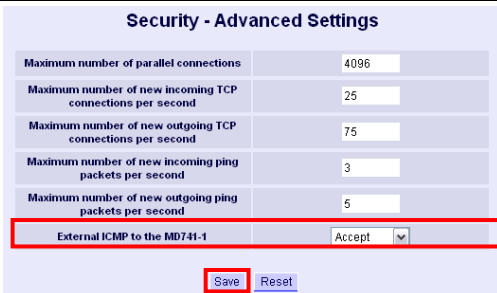
Tunnel settings → Remote net address: 192.168.3.0  
Remote subnet mask: 255.255.255.0  
Local net address: 140.70.0.0  
Local subnet mask: 255.255.0.0

Wait for remote connection: No

Edit firewall rules for VPN tunnel: Edit

Save Back

Table 5-14

No.	Action	Remarks/Notes
1.	Click the <b>Edit</b> button under <b>Settings</b> to open the connection properties dialog.	
2.	Enter the fixed IP address of your DSL connection as <b>Remote Gateway Address</b> .	Here: 217.175.91.54
3.	Select your .cer certificate under <b>Remote Certificate</b> .	
4.	Click the <b>ScalanceS ID</b> button to confirm your <b>Remote ID</b> settings.	
5.	Enter the address settings for the local and remote network as stated in your text file. Click <b>Save</b> to confirm your settings.	
6.	Select "Security > Advanced Settings". Set the parameter <b>External ICMP to the MD741-1</b> to <b>Accept</b> . Then click <b>Save</b> to confirm your settings.	

### Testing the VPN connection

After all settings have been transferred to the MD741-1, the EGPRS router will automatically establish a VPN tunnel to the SCALANCE S612 unit. This can be monitored

- at the green VPN LED on the MD741-1 and
- on the router website under "IPSec VPN -> Status"

Figure 5-10



### Note

If you have specified other IKE or NAT-T settings in your SCT project than used in this example, please follow the instructions under points 3 and 4.

## 3

## IKE settings

Table 5-15


No.	Action	Remarks/Notes
1.	The button <b>IKE Edit</b> takes you to the dialog for additional IKE settings.	
2.	Enter the settings according to your text file and confirm your settings with <b>Save</b> .	

Figure 5-11

**IPSec VPN - IKE Settings**

**Phase 1 - ISAKMP SA**

ISAKMP-SA encryption	3DES-168
ISAKMP-SA hash	MD5 or SHA-1
ISAKMP-SA mode	Main mode
ISAKMP-SA lifetime (seconds)	86400

**Phase 2 - IPsec SA**

IPsec-SA encryption	3DES-168
IPsec-SA hash	MD5 or SHA-1
IPsec-SA lifetime (seconds)	86400

DH/PFS group	DH-2 1024
IAT-T	On
Enable dead peer detection	Yes
<b>DPD - delay (seconds)</b>	<b>150</b>
DPD - timeout (seconds)	60
DPD - maximum failures	5

In this field, the cyclic time interval for **Dead Peer Detection** can be changed. The default setting is 150 seconds.

**Note**

We recommend to use the default DPD parameter settings for the DM741-1 in most applications. With this value it takes up to approx. 8 to 9 minutes until disconnection of the tunnel will be noticed. You may set the DPD to a lower value, so that disconnection of the tunnel will be identified earlier. A reduction of the DPD value, however, increases the data volume.

## Advanced Settings for NAT-T Keep Alive

4

To keep the NAT gateway at the APN alive, an NAT-T Keep Alive will be sent after a certain period. The default setting is 60 seconds. On the MD741-1 website under "IPSec VPN > Advanced" you can change this period.

Figure 5-12

The screenshot shows the SIEMENS SINAUT MD741-1 web interface. On the left is a navigation menu with options: Overview, System, Local Network, External Network, Security, IPSec VPN (selected), Connections, Certificates, Advanced (highlighted), Status, Access, and Maintenance. The main content area is titled 'IPSec VPN - Advanced Settings'. It contains a table of settings:

NAT-T keepalive interval (seconds)	60
Phase 1 timeout (seconds)	15
Phase 2 timeout (seconds)	10
DynDNS tracking	Nein

At the bottom right of the settings table are 'Save' and 'Reset' buttons.

### 5.3.7 Additional settings recommended for the MD741-1

In addition to the settings described in chapter 5.3.6, we recommend the following:

- change the password
- setting the system time
- activate HTTPS remote access

#### Changing the password

Change the password of the MD741-1 as follows:

Table 5-16

Nr	Action	Remarks/Notes
1.	Select "Access > Password".	
2.	Enter the desired password and repeat it once again for confirmation. Click <b>Save</b> to confirm your settings.	
3.	The prompt <b>Password changed</b> appears. Enter the password again to log in to the MD741-1 website.	


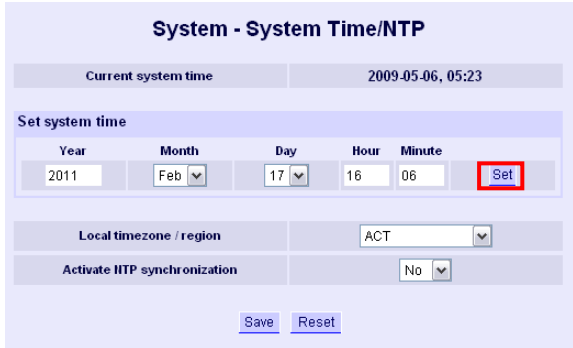
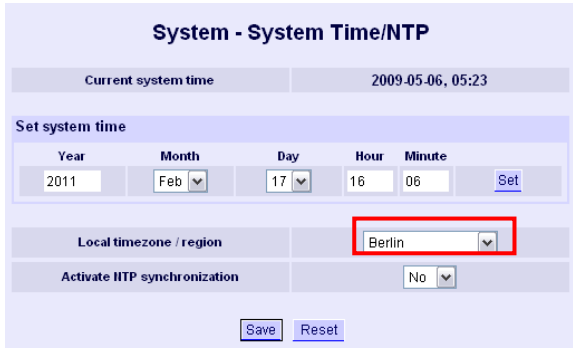
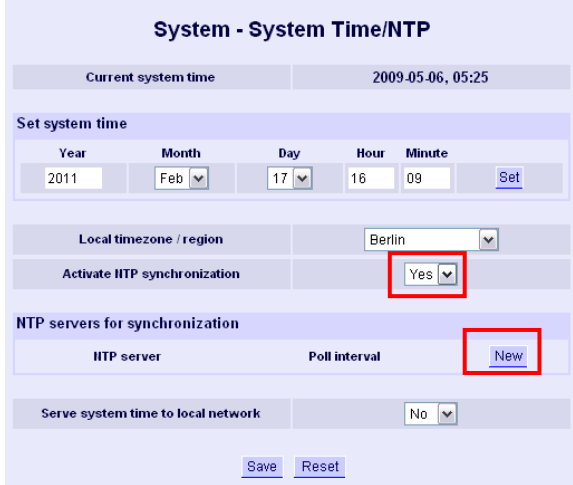
## 5 Installation and Commissioning

### 5.3 Commissioning the example project

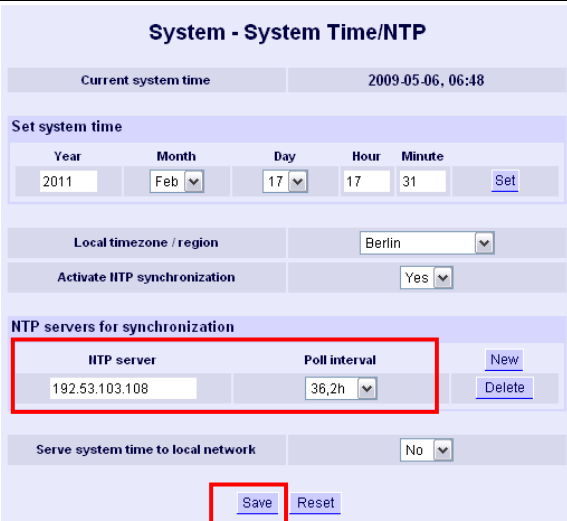
#### Setting the system time

To enable the proper analysis of log files, the system time in the MD741-1 must be set correctly. You may either choose the variant of transmitting the system time of the PC to the MD741-1 or you may set the parameters for synchronization via an NTP server.

Table 5-17

No.	Action	Remarks/Notes
1.	Select "System > System Time".	
2.	The <b>Set system time</b> field shows the computer clock time. Use this time information or define another one by hand. Then click the <b>Set</b> button.	
3.	As an alternative, you may just select a specific region (a city within your time zone).	
4.	Click <b>Yes</b> to activate NTP synchronization.  Then click <b>New</b> to add a new NTP server.	



No.	Action	Remarks/Notes
5.	<p>Use the field <b>Polling Interval</b> to define the poll interval for the MD741-1 system time.</p> <p>Click <b>Save</b> to confirm your settings.</p>	

### HTTPS remote access

This function enables access to the MD741-1 unit from a control center or from a computer connected to the secure internal port of SCALANCE S via a secured VPN tunnel.

The following functions can be performed easily from the control center:

- configure the MD 741-1
- retrieve log files
- perform firmware updates

#### Note

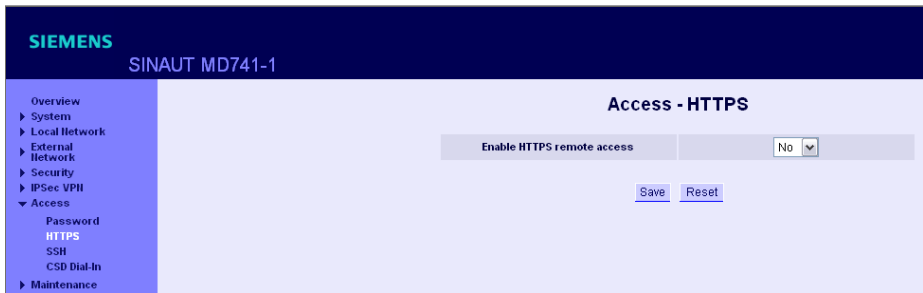
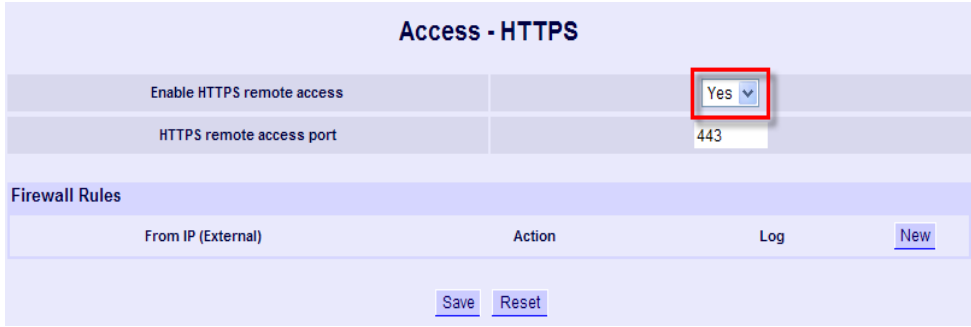
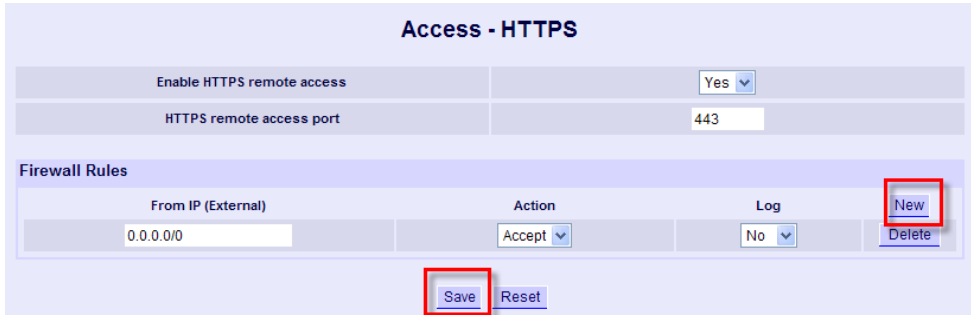
Please do not modify the **IPSec VPN** via HTTPS remote access in order to avoid an interruption of the VPN tunnel so that the MD741-1 will not be accessible any more.

## 5 Installation and Commissioning

### 5.3 Commissioning the example project

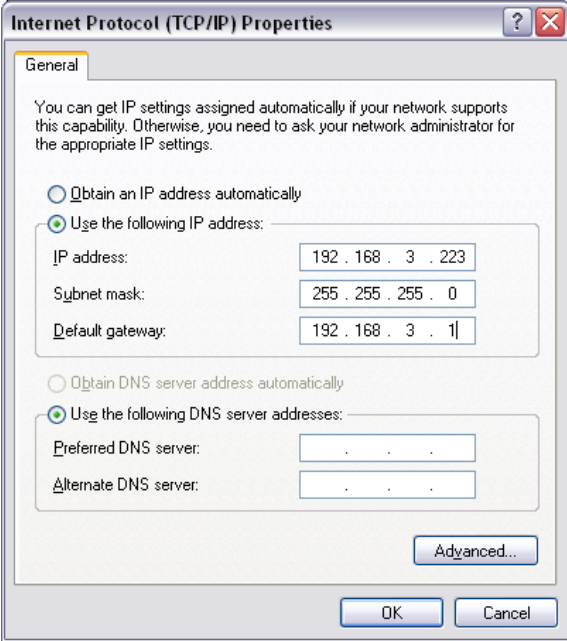
Proceed as follows to activate the function for HTTPS remote access:

Table 5-18

No.	Action
1.	<p>Select "Access &gt; HTTPS".</p> 
2.	<p>Click <b>Yes</b> to activate the function <b>HTTPS remote access</b>.</p> <p>Here you can select another port.</p> 
3.	<p>At the end you must define a firewall rule for HTTPS access by clicking the button "New" in the <b>Firewall Rules</b> field.</p> <p>Access via HTTPS will function only after a new firewall rule has been specified.</p> 
4.	Click <b>Save</b> to confirm your settings.

To enable access to the MD741-1 from your remote computer, the following settings are to be made on the computer.

Table 5-19


No.	Action	Remarks/Notes
1.	Connect your computer to the internal port of SCALANCE S.	
2.	Open the TCP/IP Properties dialog of your computer and use the internal IP address of SCALANCE as default gateway.	
3.	Start a browser and enter the address <b>https://[ip-adresse MD741-1]</b> .	If you have defined another port for HTTPS remote access, e.g. the port 442, then use the address <b>https://[ip-adresse MD741-1:Port Number]</b> , e.g. https://140.70.0.1:442 .

### 5.3.8 New features available for MD741-1 V 1.0.38 or higher

#### VPN monitoring

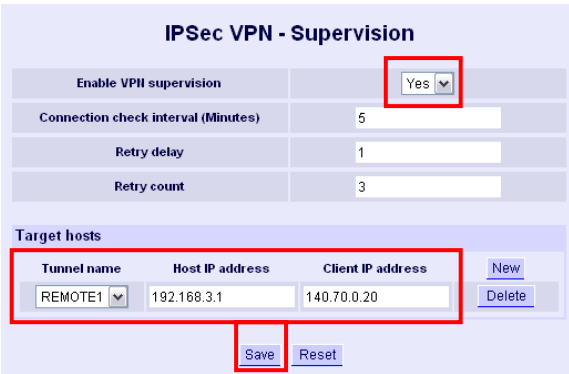
In order to identify disconnection of the tunnel more quickly, you can activate an IPSec VPN supervision function as follows:

Table 5-20

No.	Action	Remarks/Notes
1.	Select "IPSec VPN > Supervision".	

## 5 Installation and Commissioning

### 5.3 Commissioning the example project

No.	Action	Remarks/Notes
2.	<p>Click <b>Yes</b> to activate the VPN supervision function.</p> <p>In the <b>Target hosts</b> area, select the tunnel to be supervised.</p> <p>Enter the internal IP address of SCALANCE S as <b>Host IP address</b>.</p> <p>Use a free IP address from the internal network of the MD741-1 as client IP address.</p> <p>Click <b>Save</b> to confirm your settings.</p>	

#### 5.3.9 MD741-1 of 03\_Station

Configuration of this MD741-1 EGPRS router is performed in the same way as the MD741-1 of the 02\_Station and will not be described in detail here.

Perform the following steps using the text file which was generated for this modem.

- perform PIN configuration
- insert the SIM card in the device
- Further settings for tunnel configuration

Use **03\_Station** as name for this connection.

The text file and the certificates are available under

**D:\SINAUT\_Configuration8\ MD741\_03\_Station.**

#### Note

Use a standard Ethernet cable to connect the PC/PG with the MD741-1 in Station 3 for configuration. The MD741-1 supports the “autocrossing” function and enables a point-to-point connection with an uncrossed Ethernet cable.

## 6 Operation of the Application

### 6.1 Final configuration

After all modules have been loaded, change the IP address of the PCs/PGs as described in Table 5-5.

Connect all stations as shown in Figure 5-1.

### 6.2 Commissioning of the ST7cc control center and function test

#### Note

Commissioning of the ST7cc control center is only briefly discussed in this chapter. For a detailed step-by-step instruction, please refer to Volume 1.

#### Commissioning

For the commissioning of the ST7cc control center, proceed as follows:

- Start WinCC and open the project  
***D:\SINAUT\_Configuration8\WinCC\_INTERNET\DemoTIM3V-IE\DemoTIM3V-IE.MCP.***
- Start ST7cc config (under “START > SIMATIC > ST7cc > ST7cc config”) and open the project ***D:\SINAUT\_Configuration8\..DemoTIM3V-IE\ST7cc\ST7\_Project.XML.***
- Open ST7cc Config to activate the project for Runtime and to download the server settings to the system.
- Start ST7cc Runtime (“START > SIMATIC > ST7cc > ST7cc Runtime”).
- Wait until the ST7cc Server running.
- Start WinCC Runtime.

#### Operating scenarios

In WinCC Runtime you can see whether a connection with the stations has been established. The image typical for the stations are displayed in green.

The operating scenarios are identical to those described in Volume 1 and are available in chapter 7 of the Volume 1 documentation.

## 7 Diagnostics

### 7.1 Diagnostic options

In this section we show you some options of how the transmission chain can be diagnosed.

#### MD741-1

The system log file contains further information about the VPN and system events. Select "System > Log" and click the **Download** button.

Figure 7-1

```
25.8.2008 10:06,3173XX,{null},{null},{null},SERVICE_MASK=0,4,UH,41,CURRENT SYSTEM VERSION,1.028
25.8.2008 10:06,3173XX,{null},{null},{null},SERVICE_MASK=899,4,APL,51,HARDWARE ID,SINAUT MD741 1
25.8.2008 10:06,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=899,4,APL,52,SOFTWARE ID,SINAUT MD741 1
25.8.2008 10:06,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=899,4,GSML,53,GSM STARTING,
25.8.2008 10:06,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=495591,4,APL,0,SYSTEM STARTING,Success
25.8.2008 10:06,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=495591,4,GSML,54,MOBILE MODULE CONNECT,
25.8.2008 10:07,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=495591,4,GSML,55,MOBILE POWER ON,
25.8.2008 10:07,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=495591,4,GSML,56,RIN REQUESTING,
25.8.2008 10:07,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=495591,4,GSML,58,PIN REQUIRED,
25.8.2008 10:07,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=495591,4,GSML,57,PIN READY,Success
25.8.2008 10:07,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=495591,4,GSML,60,GSM ATTACH,Connecting...
25.8.2008 10:07,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=495591,4,GSML,60,GSM ATTACH,Success
25.8.2008 10:07,3173XX,CSQ=---,STAT=---,COPS=---,SERVICE_MASK=495591,4,GSML,61,GPRS CONNECTION,Connecting...
25.8.2008 10:07,3173XX,CSQ=31,STAT=1,COPS=26201,SERVICE_MASK=495591,4,GSML,61,GPRS CONNECTION,Connect
25.8.2008 10:07,3173XX,CSQ=31,STAT=1,COPS=26201,SERVICE_MASK=495591,4,APL,3,GPRS CONNECTION ESTABLISHED,GPRS connect
25.8.2008 10:07,3173XX,CSQ=31,STAT=1,COPS=26201,SERVICE_MASK=495615,4,APL,8,IP ASSIGNED,172.21.227.178
25.8.2008 10:07,3173XX,CSQ=31,STAT=1,COPS=26201,SERVICE_MASK=495615,4,VPN,47,VPN_CONNECTED,
```

#### Note

For more information about diagnostic options, please refer to the MD741-1 manual (see [/2/](#) in the appendix).

The Security Configuration Tool provides various online functions for diagnosis.

- The communication status shows the availability and type of VPN connections to the individual stations.

Figure 7-2

[illegible]

### Note

Diagnosis of the S612 is also possible via the internal interface.

The diagnosis can be viewed, even if the PC/PC is currently used as an ST7cc control center.

- The Status tab provides an overview of the module, the current module configuration settings and the utilization of the internal memory.

Figure 7-3

**S612 [Online View]**

Tabs: Status | Date and Time | System Log | Audit Log | Packet Filter Log | Communication Status | Internal Nodes

**Overview**

Hardwaretype:	Scalance S612_V2	Mode:	routing
IP Address extern:	192.168.2.2	MAC Address extern:	08-00-06-96-9B-44
IP Address intern:	192.168.3.1	MAC Address intern:	08-00-06-96-9B-44
Serial ID:	VPT5050638	HW Release:	1
MLFB:	6GK56120BA002AA3	CPlug:	No
Firmware Version:	V02.01.00.00 _10.00.00.01 14.12.2006		

**Local Time**

Current Time:	05.02.2007 14:27:23	Clock Source:	local
Operating time:	06:34:23		

**Configuration**

Created:	31.01.2007 08:24:56	Loaded:	31.01.2007 09:05:19
Name:	Configuration1	Storage Source:	
Author:	Team4		

**File system**

In use / total	RAM: 120320 / 3982848	Bytes:	Usage in %:	3,02
	Flash: 48128 / 5787648	Bytes:	Usage in %:	0,83

## Sniffer

A network sniffer, e.g. Wireshark (previously Etherreal), is used to record the data traffic between the stations. At the end of a record, the data is shown in the form of packages which can be easily analyzed.

## SINAUT ST7 diagnosis and service

The SINAUT ST7 diagnostics and service tool offers various functions for the inspection of connections, interfaces and communication. It also provides information on the firmware and software components of the network stations.

### Note

For further information on SINAUT ST7 diagnostics, please refer to the SINAUT ST7 system manual, Volume 2 – Software (see [1/](#) in the appendix)



## 7.2 What can I do, if

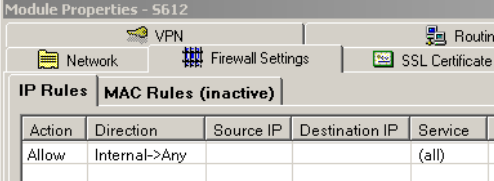
### ... no GPRS connection can be established?

Table 7-1

No.	Action	Remarks/Notes
1.	Do you have a valid SIM card?	
2.	Check the APN and SIM card details you have entered on the MD741-1 website. Have these settings been correctly transferred to the device?	Are the APN address and the associated ID actually the correct codes of your provider? Have you entered the PIN correctly in both lines?
3.	Is the SIM card properly inserted?	

### ... the VPN tunnel cannot be set up?

Table 7-2

No.	Action	Remarks/Notes
1.	Check all settings at the modem and SCALANCE S.	Have the IP addresses been assigned correctly? Do the MD741-1 settings comply with the text file?
2.	Have port 500 and port 4500 been forwarded to SCALANCE S in the DSL router?	If the DSL router offers an IPSec function, deactivate this function in the router!
3.	Connect a second PC with Ethereal between DSL router and SCALANCE S. Check whether there is any data traffic between these modules. Sniff the data packets as well. If no data traffic takes place, the DSL router probably blocks communication with SCALANCE S. Check the router settings.	ISAKMP packets (Port 500) and ESP packets (Port 4500) must appear in the data packages.
4.	Check the router functionality of SCALANCE S by calling an internet page with the PC/PG.	This is affected by enabling a connection in the direction <b>Internal -&gt; Any</b> in the firewall of the SCALANCE S (in SCT by selecting the SCALANCE S612 Properties -> <b>Firewall Settings</b> ). Then download SCALANCE anew. 

## Appendix – Links & Literature

### 8 Literature

#### 8.1 Literature

This list is by no means complete and only reflects a selection of suitable information.

Table 8-1

	Topic	Title
/1/	SINAUT ST7 Software	SINAUT ST7 System Manual Volume 2: Software <a href="http://support.automation.siemens.com/WW/view/en/24619519">http://support.automation.siemens.com/WW/view/en/24619519</a>
/2/	MD741-1	EGPRS Router SINAUT MD741-1 System Manual <a href="http://support.automation.siemens.com/WW/view/en/31385703">http://support.automation.siemens.com/WW/view/en/31385703</a>
/3/	SCALANCE S	SCALANCE S Manual <a href="http://support.automation.siemens.com/WW/view/en/21718449">http://support.automation.siemens.com/WW/view/en/21718449</a>

#### 8.2 Internet links

This list is by no means complete and only reflects a selection of suitable information.

Table 8-2

	Topic	Title
\1\	Siemens I IA/DT Customer Support	<a href="http://support.automation.siemens.com">http://support.automation.siemens.com</a>
\2\	Country approval for MD741-1	<a href="http://support.automation.siemens.com/WW/view/en/24795895">http://support.automation.siemens.com/WW/view/en/24795895</a>
\3\	Download of Firmware V2.1.0 for the SINAUT communication module TIM4R-IE	<a href="http://support.automation.siemens.com/WW/view/en/42782142">http://support.automation.siemens.com/WW/view/en/42782142</a>
\4\	Download of Firmware V2.1.0 for the SINAUT- communication modules TIM 3V-IE / TIM 3V-IE Advanced	<a href="http://support.automation.siemens.com/WW/view/en/42781378">http://support.automation.siemens.com/WW/view/en/42781378</a>
\5\	Download of SP1 (Service Pack 1) for SINAUT ST7 Engineering 9/2009 (V5.0)	<a href="http://support.automation.siemens.com/WW/view/en/42781067">http://support.automation.siemens.com/WW/view/en/42781067</a>
\6\	Download of Firmware V2.3 for Scalene S	<a href="http://support.automation.siemens.com/WW/view/en/37352999">http://support.automation.siemens.com/WW/view/en/37352999</a>

## 9 History

Table 9-1 History

Version	Date	Revisions
V2.3	31.08.2011	SCT V2.3 integrated. Volume 2: Supplementation in chapter 5.3.7 (Table 5-18, Point 3) and corrections have been made.
V2.2	22.02.2011	HTTPS, VPN supervision and other MD741-1 features added
V2.1	14.02.2011	Notes and corrections added.
V2.0	18.05.2009	Update of the application for MD 741-1. Cross communication between two stations added.
V1.0	20.03.2007	First issue