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

SINAUT ST7 Telecontrol– Configuration 8– Volume 2

Application Description • February 2011

Applikationen & Tools

Answers for industry.

SIEMENS

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These application examples do not relieve you of the 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

Preface

Objective of the application

It is the aim of this volume to introduce to you the internet /GPRS communication in the automation world.

For this purpose the Ethernet connection between the central station and the stations in Volume 1 is replaced with a secured internet /GPRS connection. A step-by-step configuration of the entire transmission path (EGPRS, DSL, Security) as well as the necessary changes to the SINAUT project Volume 1 are described using the example project.

Note This document is based on the example application of Volume 1 of the SINAUT Configuration 8. Volume 1 is available as an extra document on the HTML page.

Main contents of this application

This volume focuses on the following topics:

- the necessary basic terms on EGPRS/GPRS technology and security aspects
- in detail, all configuration steps necessary to initiate a VPN tunnel between the EGPRS Router MD741-1 and the security module SCALANCE S612.

Note Basic information and configuration with STEP 7, regarding the TIM 3V-IE, the TIM 4R-IE as well as the central station, with ST7cc WinCC is available in Volume 1.

Topics not covered by this application

The example project contains no technology-relevant program for control or coordinating the drives. It only serves for demonstrating the data exchange between station and central station. It is kept simple on purpose and programmed bit-by-bit, in order to illustrate the correlation between data in the CPUs and the central station.

Structure of this document

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

Components	Description
Application Description	This section provides a general overview of the contents. You will learn about the components used (standard hardware and software components and the specially created software).
Principles of Operation and Program structures	This part describes the detailed function processes of the involved hardware and software components, the solution structures and – where useful – the specific implementation of this application. You will need this section to get to know the interaction of the solution components, e.g. if you want to use them as basic elements for your own developments.
Setup, configuration and operation of the application	This part leads you step by step through the structure, important configuration steps, commissioning and operation of the application.

Components	Description
Appendix	This part of the documentation provides additional information such as z. B. Literaturangaben, Glossare etc..

Reference to the Automation and Drives Service & Support

This article is from the Internet application portal of the 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

Application Description

Content

Here you will be provided with a quick overview of the automation task as well as its solution. Furthermore, you will learn about the components used (standard hardware and software components).

1 Automation Task

1.1 Overview

Two waste water process stations can be controlled and monitored from the central station.

1.2 Requirements

In addition to the requirements in Volume 1 there are also the following requirements:

- the transmission of the process data occurs via a secured internet connection.
- It is not possible to have a landline/DSL connection at the stations.

2 Automation Solution

2.1 Overview of the overall solution

This solution uses the EGPRS router SINAUT MD741-1 as a main SIMATIC component in the stations and the security module SCALANCE S612 in the central station.

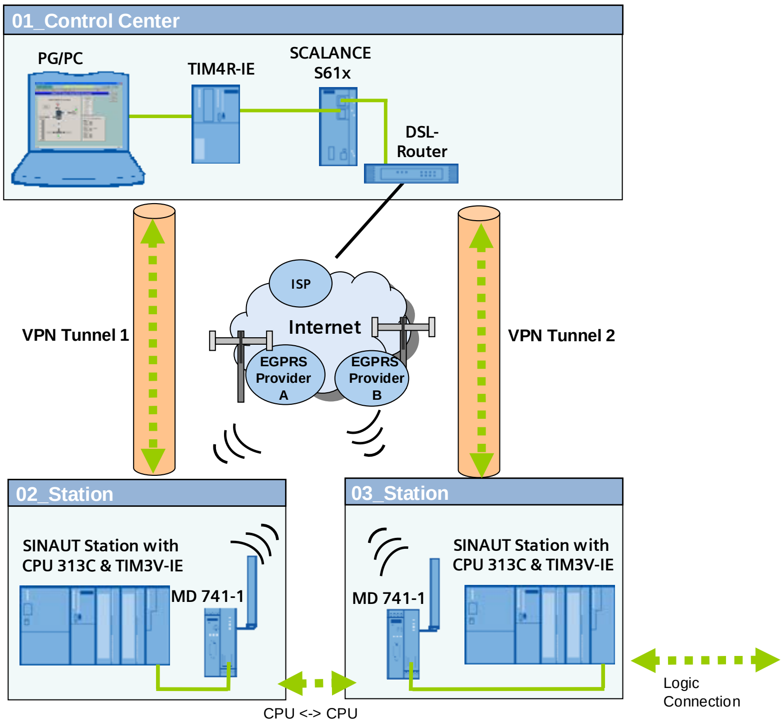
These two components establish IPSec-based tunnel connections (virtual private network, VPN) between

- the central station WinCC/ST7cc, which is connected to the internet via DSL
- several SINAUT stations which are connected to the internet via EGPRS or GPRS.
- This enables exchanging process data between a station and the control center or between the stations. (bi-directionality is possible)

Schematic layout

The following figure shows an overview of the realized solution of this configuration.

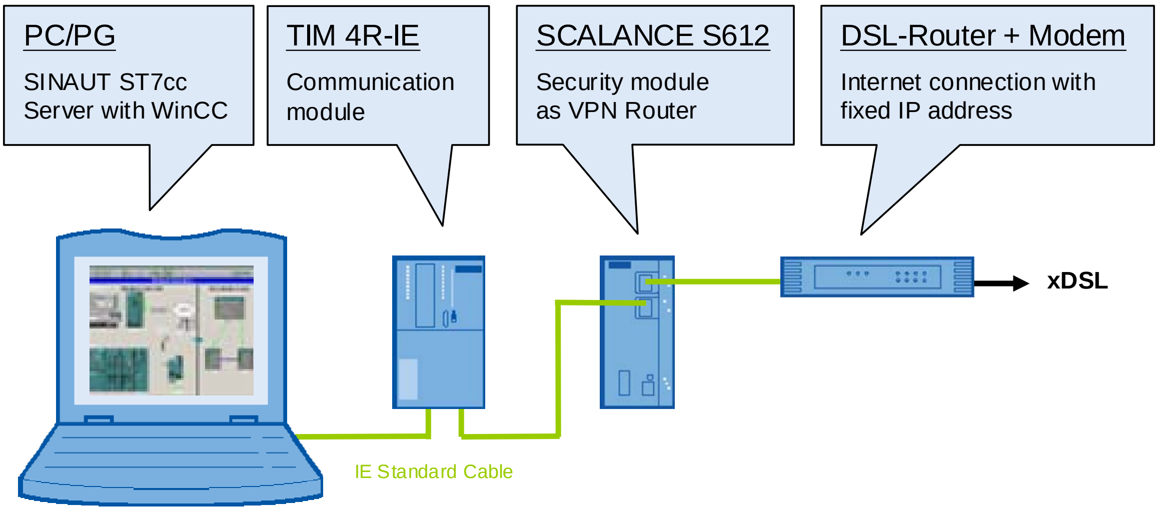
Figure 2-1



Configuration

Setup of the central station

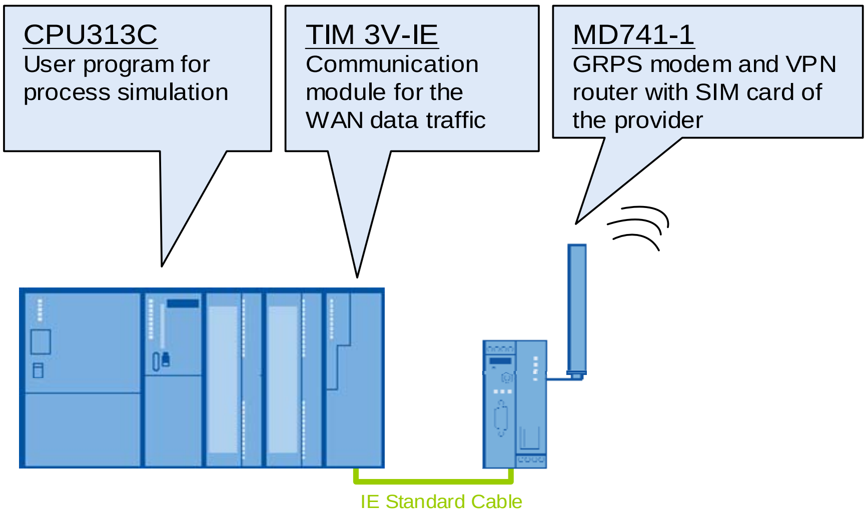
Figure 2-2


PC/PG
SINAUT ST7cc Server with WinCC
TIM 4R-IE
Communication module
SCALANCE S612
Security module as VPN Router
DSL-Router + Modem
Internet connection with fixed IP address
xDSL
IE Standard Cable

The central station consists of a standard Windows PC/PG. The PC is connected with a port of the TIM4R-IE via its integrated Ethernet interface. Via its second Ethernet port the TIM4R-IE is connected with the internal (secure) port of the SCALANCE S612. The DSL router is connected at the external (unsecured) port of the SCALANCE S612.

Setup of the SINAUT substations

Figure 2-3


CPU313C
User program for process simulation
TIM 3V-IE
Communication module for the WAN data traffic
MD741-1
GRPS modem and VPN router with SIM card of the provider
IE Standard Cable

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

2.2 Description of the core functionality

The MD741-1 router in the station establishes a VPN tunnel to the SCALANCE S612 security module in the central station via the internet. The station can communicate with the central station via this tunnel.

The communication between the stations (cross-communication) occurs via the TIM4R-IR in the central station.

Advantage of this solution

- SINAUT outstations are location independent and can be connected wireless almost anywhere (worldwide application)
- High availability of the communication through standardized mobile radio and internet technology.
- EGPRS and INTERNET secure short transfer times and are always online.
- Cost-effective data transmission due to payment based on data volumes
- VPN functionality enables a secure, protected and encoded data connection via the IPSec standard.
- High security by means of integrated firewall
- Simple and user-friendly configuration of the VPN tunnels using the Security Configuration Tool.
- Communication also between GPRS stations

Note This document only deals with the advantages of using an EGPRS router in connection with a SCALANCE S612.

2.3 Required hardware and software components

SINAUT ST7

Table 2-1

Component	Quantity	MLFB / order number	Note
TIM 4R-IE Firmware **V2.1.0**	1	6NH7800-4BA00	You can update the firmware of the TIM 4R-IE to Version 2.1.0. See \3\
TIM 3V-IE Firmware **V2.1.0**	2	6NH7800-3BA00	You can update the firmware of the TIM 3V-IE to Version 2.1.0. See \4\
SINAUT ST7 **V5.0 SP1**	1	6NH7997-0CA15-0AA0	You can update the SINAUT ST7 Tool V5.0 with SP1. See \5\
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 antennae Omnidirectional with 5m cable

Security

Table 2-2

Component	Quantity	MLFB / order number	Note
SCALANCE S612 **V2.3**	1	6GK5612-0BA00-2AA3	Optionally, you can update an existing SCALANCE S V2.1 to Version 2.3. See \6\.
Security Configuration Tool **V2.2.0.1**	1		SCT is delivered with SCALANCE S.

Note

You receive the update version V2.2.0.1 of the Security Configuration Tool V 2.1 via your local contact person.

The SCALANCE S V2.3 can be configured with the Security Configuration Tool V 2.2 or higher. The use of the Security Configuration Tool V2.2.0.1 is strongly recommended.

SIMATIC S7

Table 2-3

Component	Quantity	MLFB / order number	Note
PG	1	6ES7712-	Configurator
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	In „Service& Support news" (see \1\ in the appendix) you find information on the current enables.
Power supply PS307 5A	3	6ES7 307-1EA00-0AA0	
S7-CPU 313C	2	6ES7313-5BF03-0AB0	
Micro Memory Card	2	6ES7953-8LF11-0AA0	Mind. 64 kB
Front connector for signal modules	2	6ES7392-1BM01-0AA0	

LAN components

Table 2-4

Component	Quantity	MLFB / order number	Note
IE FC TP STANDARD CABLE	1	6XV1840-2AH10	Connecting line IE minimum ordering quantity 20m
IE TP XP CORD CABLE	1	6XV1870-3RH20	Crossed connecting line IE minimum ordering quantity 2m
RJ45 plug-in connector	10	6GK1901-1BB10-2AA0	Easy to assemble

Infrastructure

Table 2-5

Component	Quantity	MLFB / order number	Note
DSL Router + Modem with VPN pass through function (port forwarding)	1		Alternatively router with integrated modem or individually, e.g. Netgear RP614GR, Gigaset SE 515
Internet-Provider	1		
Fixed IP address	1		Contract with your Internet provider
SIM card	2		Station contract with a GSM network operator; released for EGPRS

Example files and projects

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

Table 2-6

Component	Note
23810112_SINAUT_INTERNET_DOKU_V20.pdf	This document
23810112_SINAUT_INTERNET_CODE_V20.zip	This ZIP file contains:
• STEP7_ INTERNET.zip	STEP 7& SINAUT ST7 project
• WinCC_ INTERNET.zip	WinCC & ST7cc project

Principles of Operation and Program Structures

Content

Here the background information on the topics GSM, GPRS. EGPRS and Security are discussed. Additionally, the settings are described which are performed in NETPRO so the project in Volume 1 can be used for (E)GPRS.

3 Functional Mechanisms

This chapter briefly discusses the underlying technologies and principles applied here.

3.1 Radio method

Part of the transmission path in this SINAUT example is the radio service GSM/GPRS

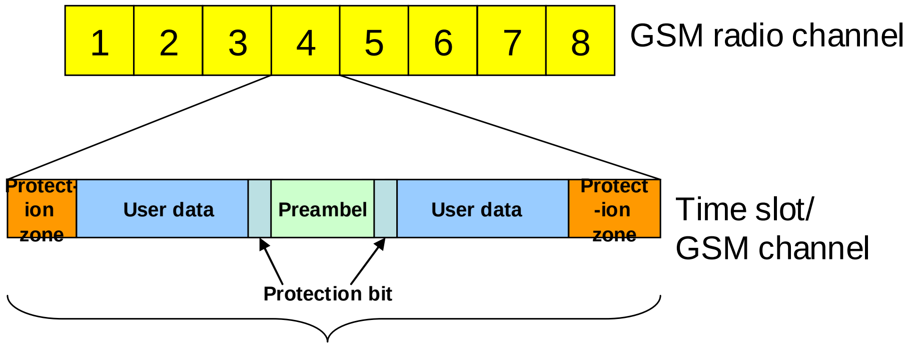
GSM

Global **S**ystem for **M**obile Communications (GSM) is a standardized fully digital mobile radio network. This network is used for mobile phones, transmitting circuit switched data (CSD) and short text messages (SMS).

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

Line transmission means, that for the entire connection time a GSM channel (time slot) is permanently assigned, and the data are always sent to the receiver through the same channel.

Figure 3-1



GSM permanently assigns a time slot accross the entire connection

For circuit switched data (CSD) the entire connection time is charged for by the network provider, irrespective of the transmitted data volumes.

Distribution

The following table lists the frequency bands as well as the national and international distribution.

Table 3-1

GSM standard	Send range	Distribution	Mobile phone providers 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 the uplink (mobile phone ➔ network) and Downlink (network ➔ mobile phone). This is explained using the example of GSM 900.

Table 3-2

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

GPRS

The **G**eneral **P**acket **R**adio **S**ervice (GPRS) is a method for packet-switched data transmission via the GSM networks. The data rate is higher here than those provided by the circuit switched GSM services.

Packet-switched means that no GSM channel is permanently reserved. At the sender, the message is divided into individual packages provided with additional information. This information informs the network of how the individual packages relate to each other and who receives the message. Using the GPRS system, the packages can be sent through different time slots of the network, which enables using free capacities. The receiver then compiles the packages in the correct order**.**

GPRS enables data traffic without establishing the connection and only charges for the transmitted data volume.

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

To obtain higher data rates during transmission several time slots can be combined with each other. Through the highest multislot class (class 12) a maximum of five time slots are bundled for one device. I.e. a maximum of five channels in total 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)

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

Table 3-3

Downlink	Uplink
1	4
2	3
3	2
4	1

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

This is on the one hand due to the fact, that the number of parallel usable GSM channels varies depending on network load and 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 MD741-1supports the highest multislot class (class 12). This results in a maximum practical data rate of **53.6 kbit/s** in uplink (4 GSM channels with CS2) or **53.6 kbit/s** in 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 Rates for **G**SM **E**volution) is an expansion of GPRS. EGPRS uses a different modulation method (8-PSK) than GPRS, which is more efficient. This enables achieving an up to four times faster data for EGPRS.

Data rate for EGPRS

As for GPRS, in EGPRS up to five time slots can be combined with each other at the same time as well. The maximum data rate per time slot is 59.2 kbit/s. If four time slots are used for uplink or downlink, the maximum theoretical data rate is 236.8 kbit/s (4 x 59.2 kbit/s)

In practice, however, this theoretical value is very rarely reached. For EGPRS the modulation and coding scheme MCS8 is used by most of the providers. For scheme MCS8 the data rate per channel is fixed to 54.4kbits/s.

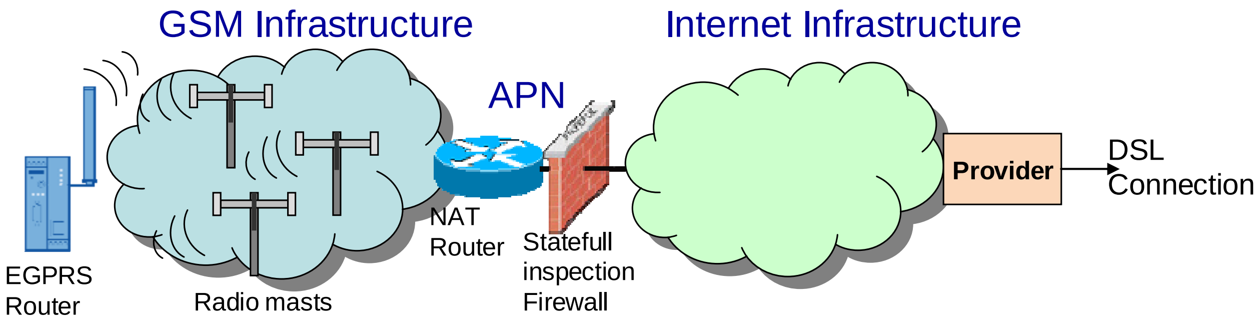
The data rate naturally also depends on the network load and the capability of the mobile device. The MD741-1 supports the highest multislot class (class 12) for which a maximum of four channels can be used for uplink or four for downlink. This results in a maximum practical data rate of **217.6 kbit/s** in 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 demonstrates the transmission path of the EGPRS chain.

Figure 3-2



The graphic shows all important components necessary for a GPRS connection via the internet.

Table 3-4

Component	Function	Note
EGPRS Router	EGPRS/GPRS client; can send data via the EGPRS/GPRS radio network;	Has an IP address assigned to it by the APN
APN	**A**ccess **P**oint **N**ame; 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: **web.vodafone.de** APN for D1: **internet.t-mobile** APN for E-Plus: **internet.eplus.de**
NAT Router	Mediates between internal, private networks and the public internet using NAT	**N**etwork **A**ddress **T**ranslation maps private IP addresses to public ones.
Statefull inspection Firewall	Protection wall; only allows answer packages to questions;	Packages from outside, which do not belong to a request triggered by the client, are rejected.
Provider	Local internet provider	

Transmission requirements

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

- Security: The transmission path must be save and protected from unauthorized access. In this example an IPSec tunnel (VPN) takes on that task.
- Stability: The transmission path must be stable. Regular monitoring by keep-alive protocols (NAT-T Keep Alive, Dead Peer Detection, Rx/Tx Delay Trigger, TCP-IP Keep Alive) is necessary.
- Bi-directionality: Data transmission must occur point-to-point in both directions.
- Accessibility: The DSL router in the control center must have a fixed public IP address.

Connection setup procedure

Due to the additional path via the internet service provider, the connection setup between MD741-1 and SCALANCE S goes through various stages which are explained below.

Table 3-5

Step	Description
1	The MD741-1 establishes an EGPRS data connection via the mobile radio network provider (APN) The mobile radio network provider forwards the GRPS data traffic to the internet.
2	The MD741-1 sends data packets with target address (IP address of the router) to the internet.
3	Provided, that the DSL connection of the control center with the internet has been established, the data packets are forwarded by the DSL router to the S612.
4	The VPN tunnel between MD741-1 and SCALANCE S is established.
5	The packet oriented data traffic can now take place.

3.3 EGPRS Router MD741-1

The MD741-1 Router establishes a secure IP data connection between remote station and service center via EGPRS or GPRS.

Basic requirements for operation

For operating the MD741-1 router a SIM card with EGPRS/GPRS service is required which is plugged into the router.

Note

The SIM cards which are enabled for GPRS, also support EGPRS. Whether the router logs into EGPRS or GPRS networks depends on the network coverage of the provider. Information on the network coverage of the provider is mainly available on the internet page of the provider.

The EGPRS router MD741-1 together with the quad band antennae ANT 794-4MR covers all four band widths of the GSM networks and can hence be employed almost worldwide.

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

Note

Please also note the country approvals for the MD741-1.

Link \2\

Properties of the MD741-1

For a secure radio data connection the router provides the following core functions:

- VPN Router: supports a safe data connection via an IPSec-secured VPN tunnel (Virtual Private Network)
- 3DES data encoding, AES encoding
- Firewall for protection from unauthorized access. The dynamic packet filter searches data packets using the source and target address (stateful packet inspection) and blocks the undesired data traffic (Anti-Spoofing)
- EGRPS Modem for a data communication in packages via GSM
- Bi-directional data connection
- Cyclic processing of protocol data for maintaining or monitoring the connection (NAT-T Keep Alive, Dead Peer Detection, Rx-Tx-Delay Trigger)

Configuration of the modem

The configuration of the router occurs via a standard browser via the web page integrated in the router via web-based management.

Explanation of important terms

In this section, the most important features of the MD741-1 are explained briefly.

Note Further information is available in the manual on MD741-1 (see /2/ in the appendix)

Table 3-6

Feature	Explanation
VPN (Virtual Private Network)	VPNs connect the computer or networks via the internet and provide for secured data transmission. The so-called tunnel is encoded. Using passwords, public keys or a digital certificate may guarantee the authentication of the VPN end products.
IPSec	IPsec is an expansion of the internet protocol (IP) and contains extensive security functions: • AH mechanism (Authentication Header) handles the authentication and identification of the source. • ESP (Encapsulation-Security-Payload) transmits the data encoded via UDP port 4500 • IKE (Internet Key Exchange) for exchanging the key via UDP Port 500
Anti-Spoofing	Anti-Spoofing prevents misuse of IP addresses and obscuring of the own identity
NAT-T Keep Alive	The MD741-1 sends UDP packets through the tunnel port 4500 in a fixed time frame (in this example, every 90 sec), to maintain the connection at the APN. The time after which a provider disconnects a connection without data transfer is not fixed and must be adjusted accordingly. For NAT-T Keep Alive no response is expected from the peer so the existence of the VPN tunnel cannot be proven this way.
Dead Peer Detection (DPD)	If no packets have been sent or received through the tunnel for and extended period of time (in this example after 150 seconds at the latest), the MD741-1 sends an UDP packet through port 4500. A response from the peer is expected and hence the status of the VPN tunnel is monitored. If a failure of the VPN tunnel is recognized, the MD741-1 tries 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 is used. DSL (Digital Subscriber Line) enables sending or receiving data with high transmission rate. Different transmission rates are available depending on DSL tariff and provider.

Technology for DSL via telephone

Data are mostly transmitted to the internet via the two-core copper cable connected to the telephone. It does not matter here whether it is an analog or an ISDN connection for the telephone. This method enables phoning and surfing at the same time, as the DSL data are transmitted in a different frequency range than the telephone data. The signals from the telephone socket are separated into language and data using a splitter. A modem is connected to the splitter which compiles the DSL conform data signals into computer data and vice versa. The PC can then be connected with the modem directly or via a router.

Requirements for the router

A secured EGPRS connection via the internet has the advantage, that the router has a **fixed IP address**. This refers to an IP address, which is permanently assigned to the router and so is permanently available under this address. This IP address is entered into the configuration of the MD 741-1 as a default value.

If the VPN tunnel is placed above a DSL router, it must master **Port Forwarding** and **IPSec pass through**. With Port Forwarding the router waits for data packets at a configured port and forwards them to a certain port in the internal network. For IPSec-based VPN tunnels, port 500 and 4500 must be forwarded to the VPN peer. Key exchange and authentication occur via port 500, the NAT-T Keep-Alive, Dead Peer Detection and the ESP packet packed in UDP packets via port 4500.

3.5 SCALANCE S

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

Properties of the SCALANCE S612/613 models

SCALANCE S61x modules have the following core properties:

- Supporting a secure data connection via a IPSec-secured VPN tunnel
- VPN-Server/ Client; supports up to 64 (S612) or 128 (S613) VPN tunnels simultaneously.
- Firewall for protection from unauthorized access. The firewall has the following functionalities:
  - Searching the data packets using the source and target address (stateful packet inspection)
  - Supporting Ethernet “Non-IP” messages
  - Band width limitation
- Router mode for operating SCALANCE S as NAT/NAPT router. Internal network may be an own subnet.
- Bridge mode to operate SCALANCE S in a flat network. Internal and external network are located in a subnet.

Configuration of the SCALANCE S module

The Security Configuration Tool (SCT) serves as a configuration tool for SCALANCE S modules and for generating configuration files for the MD741-1. All stations can be combined into a group here. This assignment defines 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 using the Security Configuration tool.
- Very simple configuration process

Note For further information see the SCALANCE S manual. See Appendix /3/

3.6 Security

Security requirements

- Data confidentiality: The user data must be encoded and protected from unauthorized access
- Station authentication: Only defined station must participate in the data communication. An authentication is required.
- Packet identification: It must be ensured, that data packets arrive at their target address unchanged.
- Secrecy: Networks behind the VPN Gateways should be hidden 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). Encoded data packages and authentication of the stations makes this possible. Authentication (proof of one’s own identity or checking the identity of the peer) occurs via a key (Pre-Shared Key) or certificates (X.509v3 certificates).

Pre Shared Key

Using a pre-shared key is a symmetrical crypto-system. Each station has only one secret key for coding and decoding of data packets. Authentication occurs via a joint password.

Certificates

Using certificates is an asymmetrical crypto-system, where each station has a set of keys. Each station has only one secret, private key and one public key of the peer. The private key enables decoding data, generating digital signatures and authentication. The public key enables encoding data packets for the peer.

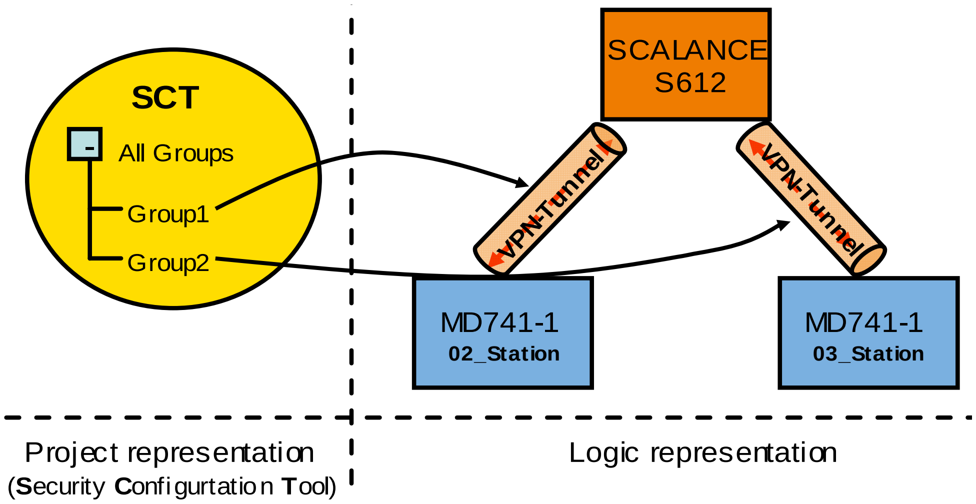
The authenticity of the public key of the peer (authentication) is checked via an additional certificate issued by a certification authority. For SCALANCE S the CA is the group from the configuration tool SCT, in which all nodes of a VPN tunnel are located. The group issues certificates to the group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

Note In this example the authentication occurs via certificates.

Logic representation of the VPN connection

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

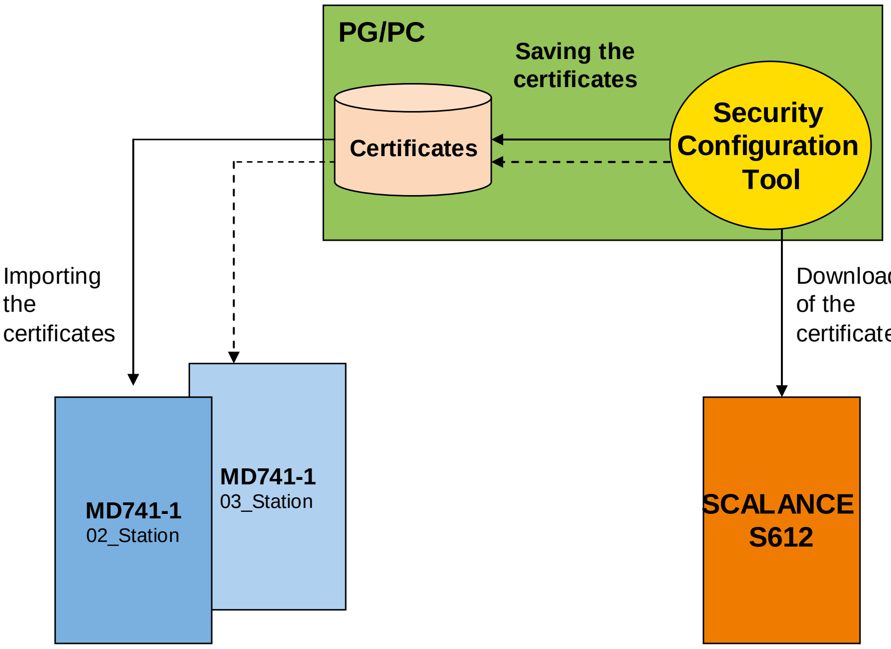
Figure 3-3



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

Distribution of certificates

Figure 3-4



Certificates = ***.p12 –File** (public & privat 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 transmission of data.

Targets

The aims of IPSec are:

- Authentication of stations
- Protection from unauthorized and unnoticed changes of the data packets (data integrity)
- Secrecy of the transmitted data packets.
- Protection against replay attacks; prevents repeated receiving of the same data package
- Key management

Protocols

IPSec is a standard which uses various protocols for security. The safety functions are achieved using the following mechanisms:

- The IP authentication header handles the authentication and identification of the source and provides data integrity.
- ESP (Encapsulation Security Payload) encodes the data and prevents unauthorized access.
- The Security Association (SA) is an agreement between the stations regarding the live of the key, the encoding algorithm, time for a new authentication etc.
- 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 stations.
  - In phase 1 a key is agreed, on how the public keys of the peer can be exchanged safely (ISAKMP-SA). Then the public keys are exchanged with each other (authentication). Using the CA certificate, the authenticity of the key is checked (authentication). If the life of the key has elapsed, a new key is generated for safe transmission of the public key.
  - Phase 2 is the encoded data transmission using the p12 certificate. If the life of the p12 certificate has elapsed, a new certificate is generated (IPSec-SA). Phase 1 starts again.

Operating modes

IPSec offers two operating modes. In these operating modes it is defined how the IP data packages must be expanded to the targets of IPSec are fulfilled.

- The **Transport mode** is used if the cryptographic endpoints are also communication send points (computer-computer connections)
- The **Tunnel mode** is selected if the cryptographic endpoints are only security gateways and remote subnetworks are coupled via an unsecured network.

IPSec data package

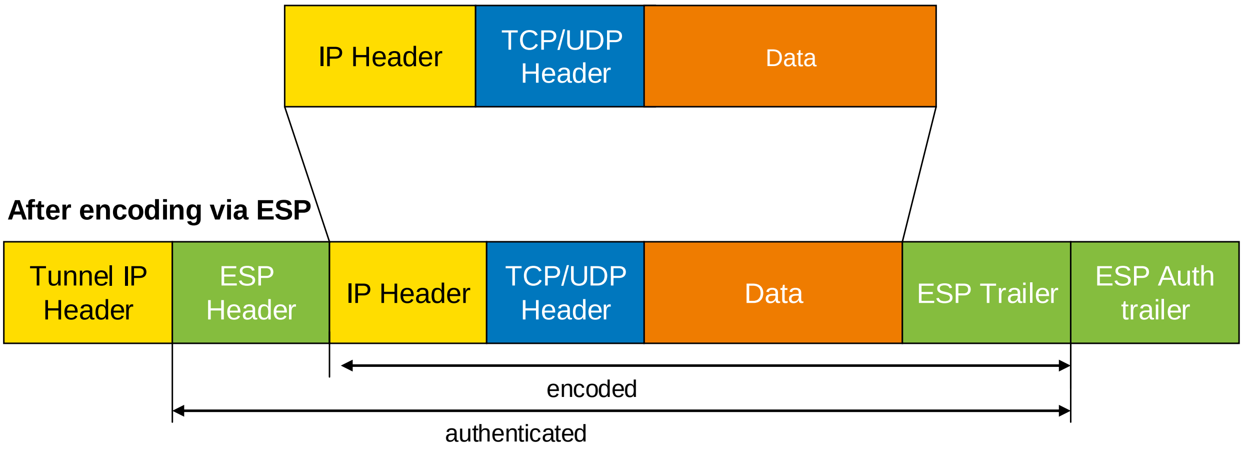
Between the VPN connection SCALANCE S612 and MD741-1 the data packages are transferred in tunnel mode. They are decoded by the VPN endpoints and forward the data packages to the actual address.

There is the possibility to secure the data package using ESP and/ or Authentification Header (AH). The MD741-1 uses only the encoding via ESP.

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

Figure 3-5

Data package prior to encoding



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

Table 3-7

Header	Function
Tunnel IP Header	This IP header contains the address of the cryptographic endpoint (VPN gateway).
ESP Header	Through ESP the original IP data package and the ESP trailer are encoded. The ESP header provides protection from 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 number and stores the number of inserted bits.
ESP Authentication Trailer	Contains the integrity test value for authentication and integrity of the message

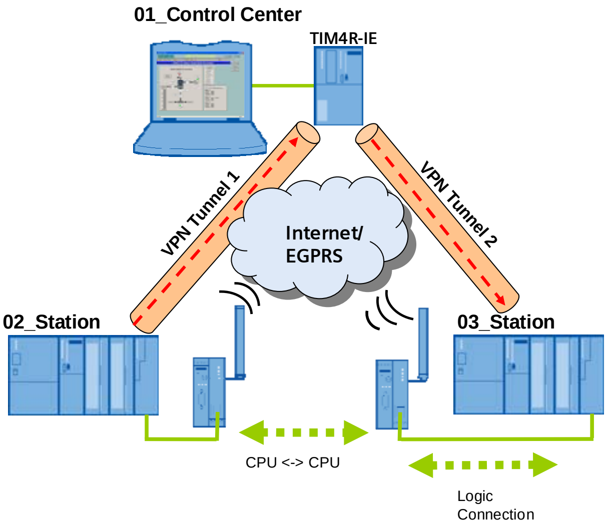
3.7 Cross-communication via EGPRS

Through the application of the TIM4R-IE in the central station the communication between the outstations (GPRS stations) is possible.

The GPRS stations, 02_Station and 03_Station can send and receive data between each other in the central station via the TIM4R-IE. The TIM4R-IE has been configured as GPRS central station for this purpose.

This works as follows. For example, station 2 sends data to station 3. The telegrams are forwarded to the central TIM through the VPN tunnel 1. The TIM forwards the telegrams to station 3 through the VPN tunnel 2.

Figure 3-6



4 Explanations for the Example Program

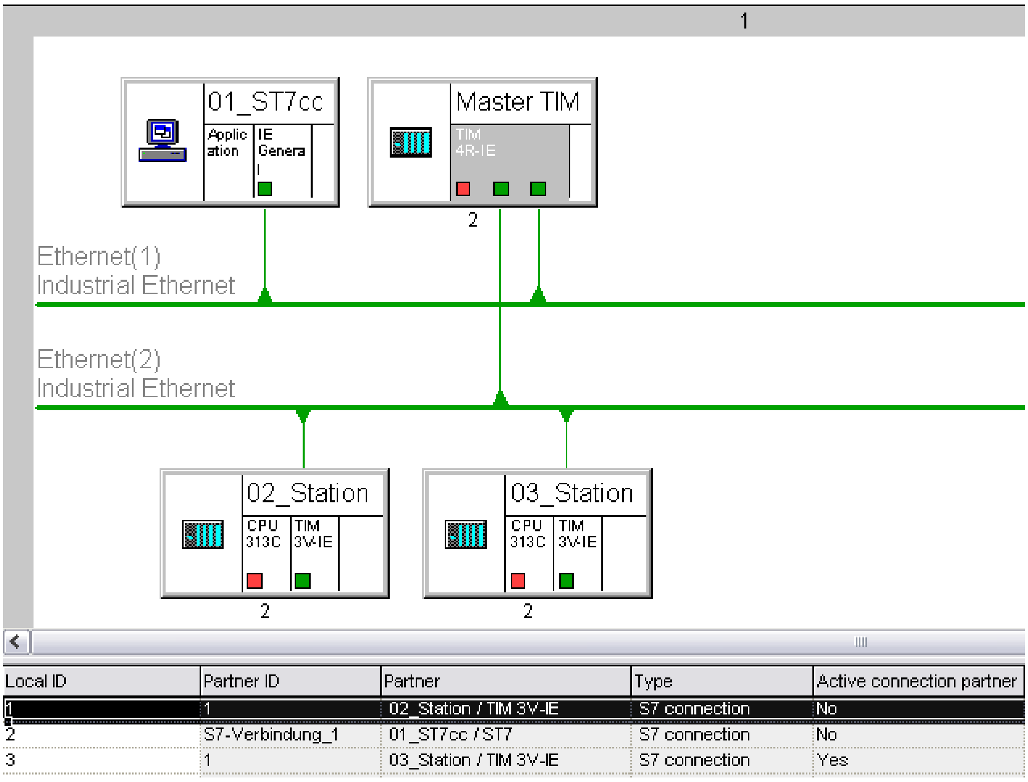
In this chapter, the settings are described which are performed in NETPRO so the project in Volume 1 can be used for EGPRS. These settings have already been integrated in the STEP7 project for Volume 2 and need not be made by the user for the example project.

4.1 Set IP Addresses for the ST7cc computer and the TIMs

NetPro

The connection between the S7 station and the TIM central station through the VPN tunnel is a mere point to point Ethernet connection. The following figure displays an extract from NetPro:

Figure 4-1



Local ID	Partner ID	Partner	Type	Active connection partner
1	1	02_Station / TIM 3V-IE	S7 connection	No
2	S7-Verbindung_1	01_ST7cc / ST7	S7 connection	No
3	1	03_Station / TIM 3V-IE	S7 connection	Yes

Default Router

In reality, the connection via EGRPS and internet runs via several subnets. The SIMATIC station, the central station TIM and the ST7cc control center must therefore be informed of 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 central station uses the SCALANCES as router. For this reason the Ethernet port of the TIM which is connected to the SCALANCE S is configured as follows:

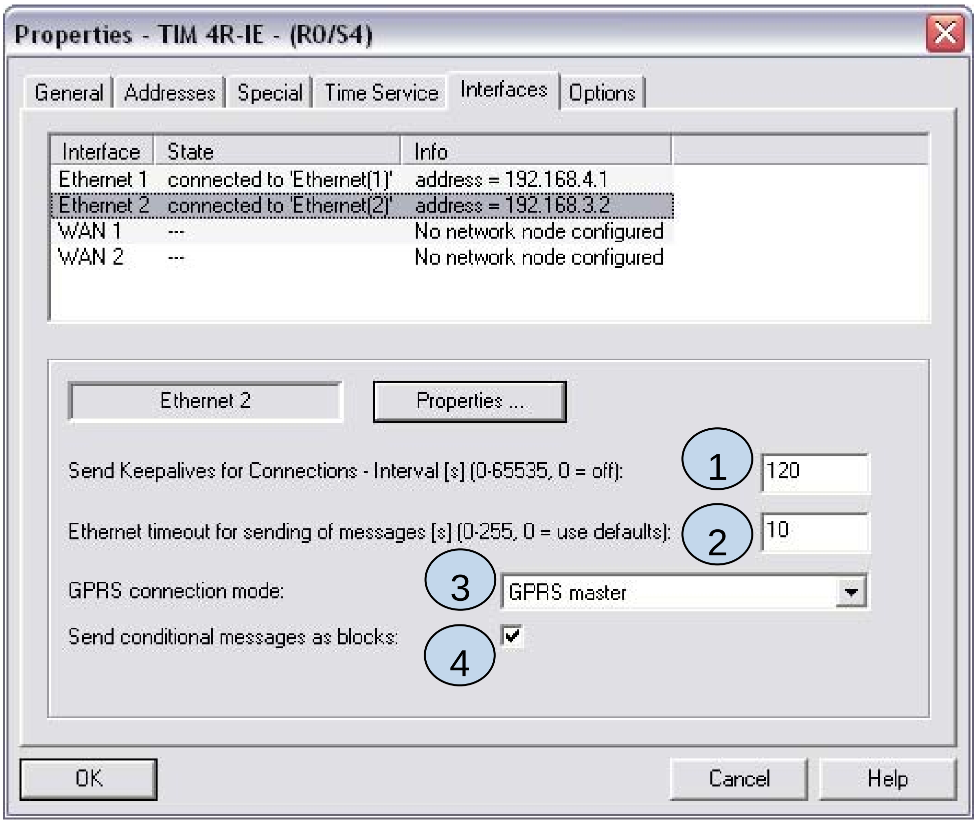
IP address: **192.168.3.2**

Subnet mask **255.255.255.0**

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

The following figure shows the additional settings for the central station TIM so the TIM is used as GPRS central station.

Figure 4-2



Properties - TIM 4R-IE - (R0/S4)

Interface	State	Info
Ethernet 1	connected to 'Ethernet(1)'	address = 192.168.4.1
Ethernet 2	connected to 'Ethernet(2)'	address = 192.168.3.2
WAN 1	---	No network node configured
WAN 2	---	No network node configured

Ethernet 2 Properties ...

Send Keepalives for Connections - Interval [s] (0-65535, 0 = off): 120

Ethernet timeout for sending of messages [s] (0-255, 0 = use defaults): 10

GPRS connection mode: GPRS master

Send conditional messages as blocks: ☑

4.1 Set IP Addresses for the ST7cc computer and the TIMs

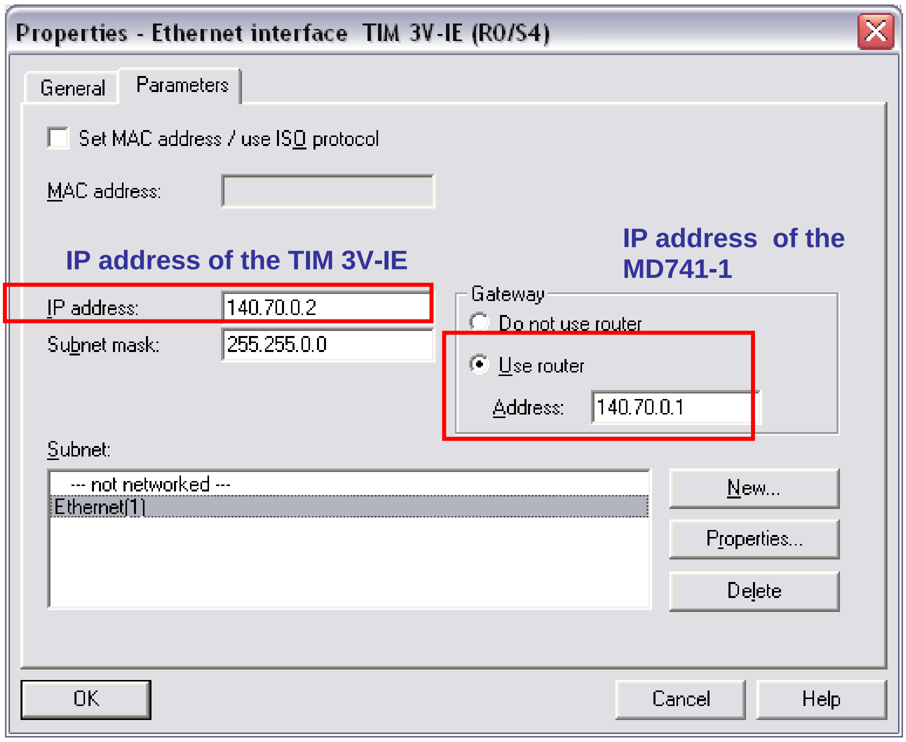
Table 4-1

No	Property	Description
1	Send Keepalives for Connections- Interval [s]	With this parameter, the **TCP/ IP Keep Alive Interval** of the TIM is set. The given time should be shorter than the **Dead Peer Detection** of the MD741-1 (150 sec). Recommended are 120 sec.
2	Ethernet timeout for sending of messages [s]	Normally, the acknowledgement of a send message in the EGPRS/GPRS network occurs within 1-2 sec. For high network load this may take longer. In practice, a value of 10 seconds has been proven.
3	GPRS connection mode	EGPRS/GPRS is a point-to-point connection between station and central station. Cross-connections from station to station are only possible via an additional TIM 4V-IE in the central station which takes on the routing of data messages. Each TIM in the SINAUT project must give its connection node at the GPRS network: **“GPRS station”** (for all TIMs in the stations) **“GPRS control center”** (for the TIM in the central station)
4	Send conditional messages as blocks	Activating the conditional message enables collecting smaller data packets in the intermediate memory of the TIM and to transmit them in larger blocks. TIM transmits the collected data: • after a scope of 202 bytes has been reached. • if an important message must be transmitted immediately, all messages in the intermediate memory are transmitted as well • if the TCP/IP Keep Alive interval runs out, the saved messages are transmitted instead of the Keep Alive.

4.1.3 Station 2 and 3

Stations 2 and 3 use your MD741-1 Router as a gateway. The TIM in station 2 is configured as in the following figure:

Figure 4-3



Properties - Ethernet interface TIM 3V-IE (R0/S4)

☐ Set MAC address / use ISO protocol

MAC address:

IP address of the TIM 3V-IE

IP address: 140.70.0.2

Subnet mask: 255.255.0.0

IP address of the MD741-1

Gateway

○ Do not use router

● Use router

Address: 140.70.0.1

Subnet:

--- not networked ---

Ethernet(1)

Additionally the TIM3V-IE 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 startup we offer you a finished STEP 7 / SINAUT example project as a download. This software example supports you in the first steps and tests with this configuration. It enables a quick function test of hardware and software interfaces between the here described products.

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

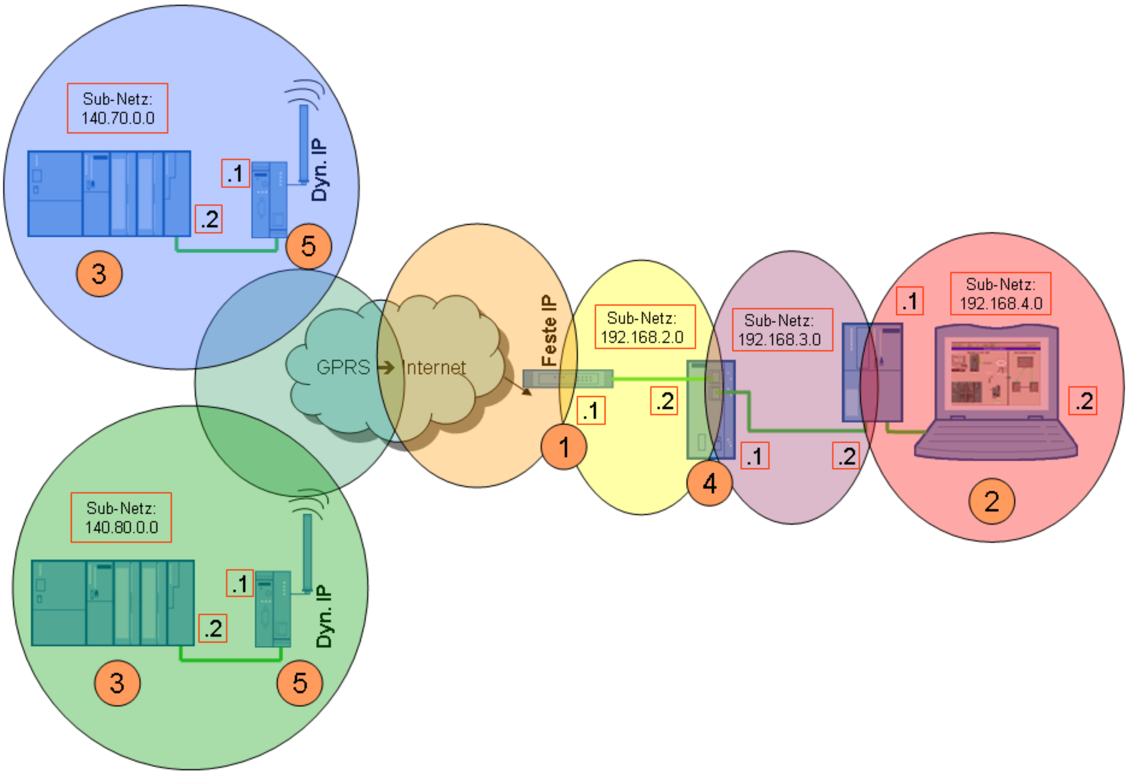
The following chapters take you step by step through the necessary configuration.

5 Installation and Commissioning

5.1 Hardware / structural setup and installation of the software

The following figure shows the various subnets and configuration points which are relevant here.

Figure 5-1



The following table gives you an overview of the IP addresses used. Cells with the same color belong to one subnet respectively. Modules with two addresses (internal/external) work 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
Central Station	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

For this configuration the following software packages are required:

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

Note

The order of software installation is available in Volume 1.

In addition to Volume 1 the Security Configuration Tool is installed. Follow the instructions of the installation program.

5.2 Installation of the example project

Table 5-2

No	Action	Remark/Figure
1.	Unzip the file 23810112_SINAUT_INTERNET_Code_V20.zip	The directory ***D:\SINAUT_Configuration8*** is used below as project directory.
2.	Unzip the file WinCC_INTERNET.zip	The WinCC project is now filed at ***D:\SINAUT_Configuration8\WinCC_Internet\ DemoTIM3V-IE\ DemoTIM3V-IE.MCP***
3.	Start STEP 7 and retrieve STEP 7_INTERNET.zip to **D:\SINAUT_Configuration8**	The STEP 7 project is now filed at ***D:\SINAUT_Configuration8\ Demo_INTERNET***

5.3 Commission the example project

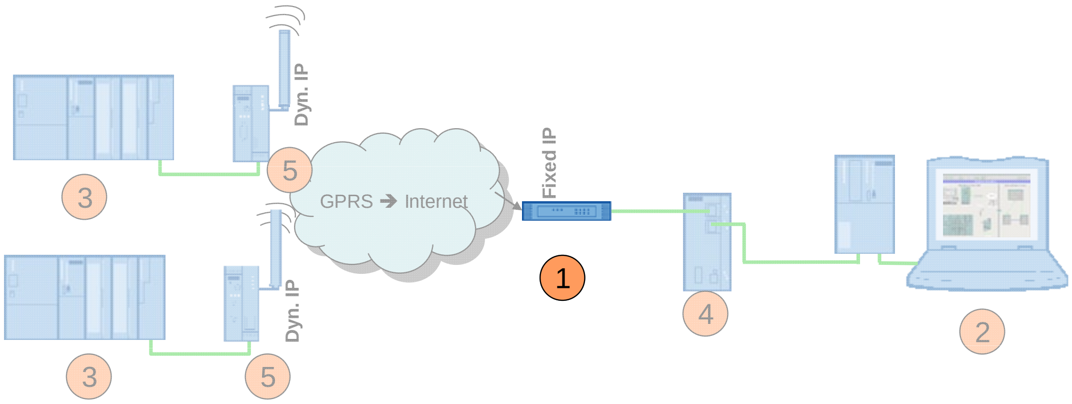
In the following chapters the required configuration steps of the individual components are explained.

Table 5-3

Number	Configuration step	Chapter
1	Configuring the DSL Router	5.3.1
2	Configuring the central station	5.3.2
3	Downloading the central TIM of station 2 and 3	5.3.3
4	Configuring SCALANCE S and the VPN tunnel	5.3.4
5	Configuration the MD741-1	5.3.5

5.3.1 Configuring the DSL Router

Figure 5-2



No specific router is discussed for the configuration as the operating screens differ from router to router.

Most routers have a web page for the configuration.

Required PC/PG IP address

For the configuration of the router you must assign an IP address to your PG/PC which is located in the same network than your router.

Configuration

Table 5-4

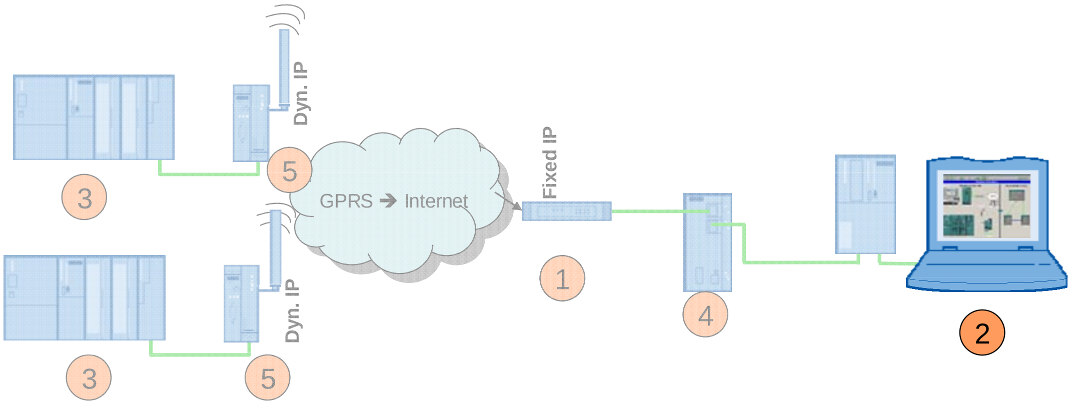
No	Action	Remark / note
1.	Open the configuration user interface of the router	This may be an additional software, “Telnet” or a web page.
2.	Enter the connection data for your internet connection.	Login, password etc, which you received from your provider.

No	Action	Remark / note
3.	Switch off the DynDNS server.	Your internet access has a fixed IP address.
4.	Enter your DNS server.	The address is available together with the access data.
5.	Specify a LAN IP address for the router	192.168.2.1
6.	Switch off the DHCP server.	The SCALANCE S and the PC receive a fixed address.
7.	Forward **UDP-Port 500** and to the same ports of the **4500** 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 In some routers there is the "**IPSec Pass through**" function. Activate this function (if it explicitly exists in your router) in order to support IPSec.

5.3.2 Configuring the central station

Figure 5-3



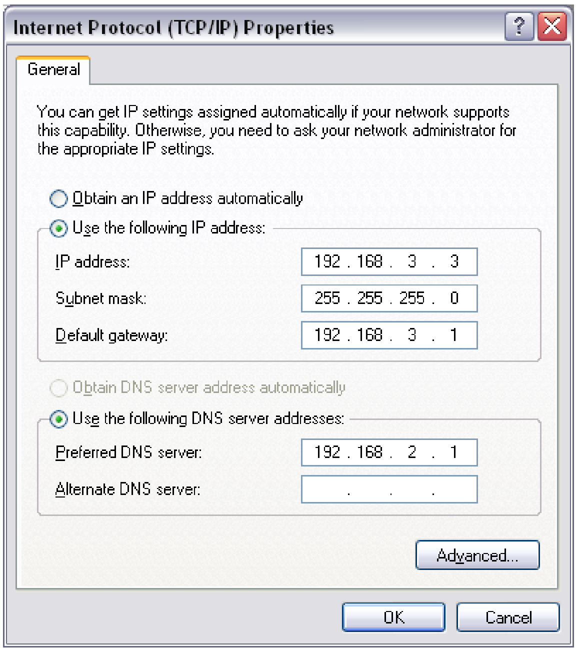
The following settings must be made:

- Assign IP address
- Change computer name to CONTROLROOM
- PC station initial startup:
  - setting the component configurator
  - setting the access point

Change IP address

Loading the various modules (SCALANCE S, MD741-1, TIM) requires changing the IP address of the PCs/PGs frequently. This section shows the steps required for this. The figure shows the network settings to which you must change the PG/PC at the end of the configuration (after chapter 5.3.7)!

Table 5-5

No.	Action	Remark / note
1.	Open the **Internet Protocol (TCP/IP) Properties** by selecting **`Start -> Settings -> Network Connection ->Local Connections`** Select the options field **Use following IP-address** and fill in the field according to the screenshot on the right. Select the option field **Use following DNS Server** and enter the DNS server according to the screenshot. Close the dialog boxes with "OK".	 Internet Protocol (TCP/IP) Properties General You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. ○ Obtain an IP address automatically ● Use the following IP address: IP address: 192 . 168 . 3 . 3 Subnet mask: 255 . 255 . 255 . 0 Default gateway: 192 . 168 . 3 . 1 ○ Obtain DNS server address automatically ● Use the following DNS server addresses: Preferred DNS server: 192 . 168 . 2 . 1 Alternate DNS server: . . .
2.	If you PG has an IWLAN interface, switch this off.	

Computer name and PC station

How the computer name is changed, and how the PC station is configured for initial operation, has already been explained sufficiently step-by-step in Volume 1. Please take the information on the procedure from this volume. (See chapter 6.3.1 and 6.3.4 in Volume 1)

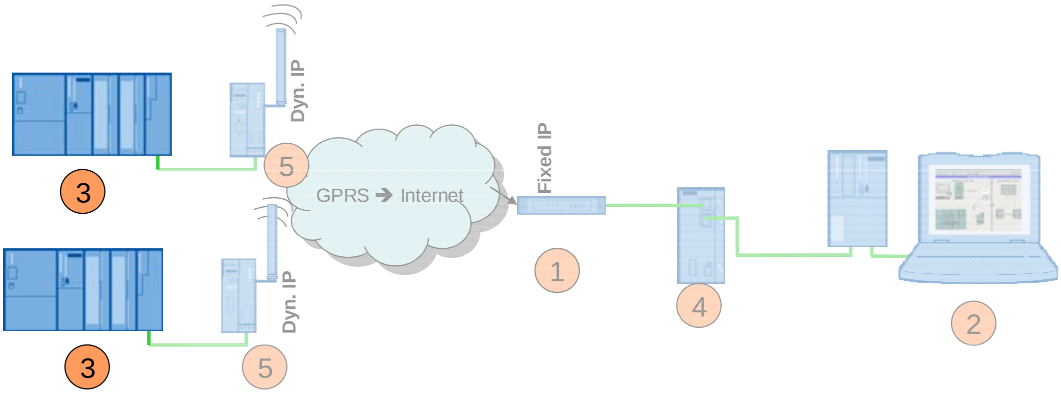
Note

The included STEP 7 project for this Volume 2 serves a basis for the configuration of the PC station.

Please make sure you are using the IP address and xdb-file defined for Volume 2. (see table 5-1)

5.3.3 Downloading the central TIM of station 2 and 3

Figure 5-4



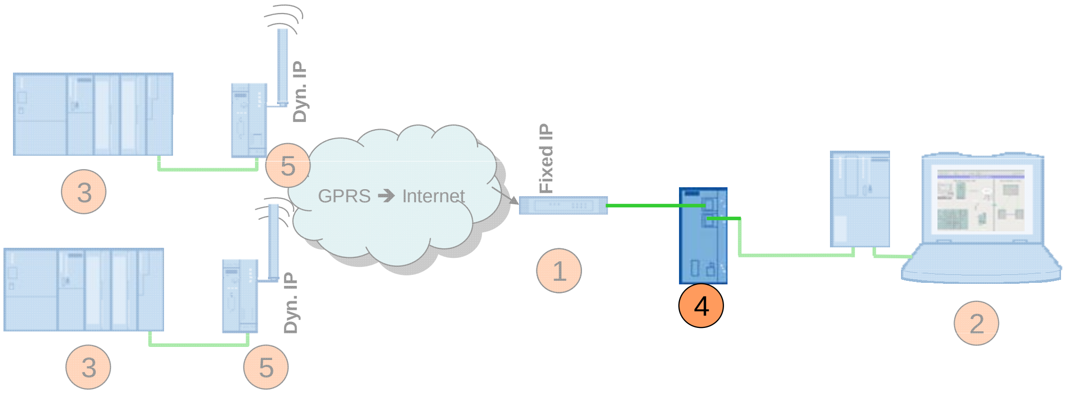
The provided STEP 7 project, which has already been configured with the correct IP addresses for the second volume, serves as a basis for configuring the stations and the central TIM.

Table 5-6

No	Action	Remark/Figure
3.	For loading the SINAUT **02_Station** please change the IP address of your PC/PG to IP address: **140.70.0.20** Subnet Mask: **255.255.0.0**	
4.	Prior to loading the STEP 7 project into the CPU, the IP address of the TIM module must be changed according to Table 5-1.	The configuration of the IP address in the TIM is explained in Volume 1 chapter 6.3.2.
5.	For loading the SIMATIC station, please connect the PC/PG with the TIM via the crossed connection cable.	Ensure that the TIM 3V-IE has been assigned the IP address **140.70.0.2** /subnet mask 255.255.0.0.
6.	Repeat this process for station 3 and the central TIM.	Use an uncrossed patch cable for the central TIM.
7.	Subsequently you set the IP address of the PC according to table 5-1.	

5.3.4 Configuring SCALANCE S and the VPN tunnel

Figure 5-5



This section shows the necessary steps in the Security Configuration Tool, to generate two VPN tunnels to the MD741-1 in the stations.

Note

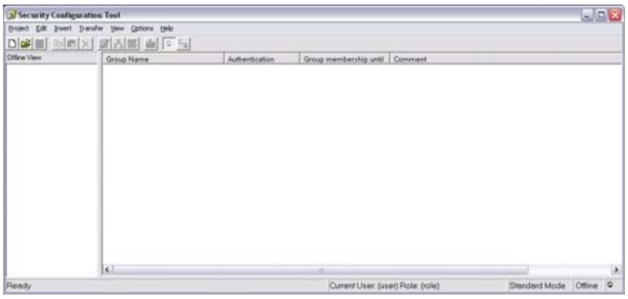
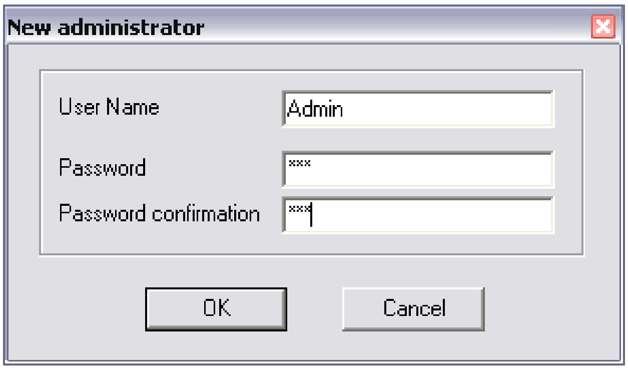
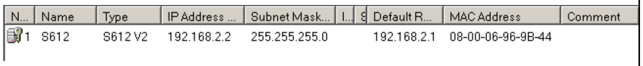
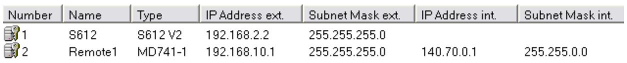
Reset the SCALANCE S612 to factory settings prior to configuration. This ensures, that no other certificates / VPN connections are saved in the SCALANCE S and the IP address of SCALANCE S is set to 0.0.0.0.

An instruction for resetting the configuration to factory settings is available in the SCALANCE S manual chapter 2.1.7 /3/

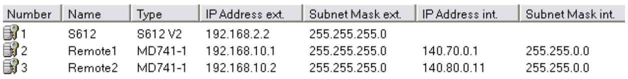
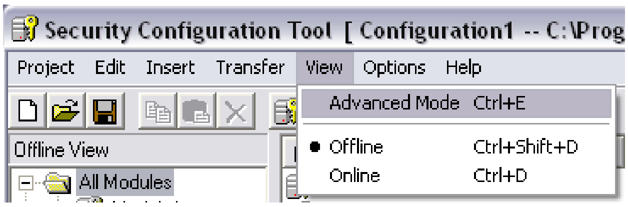
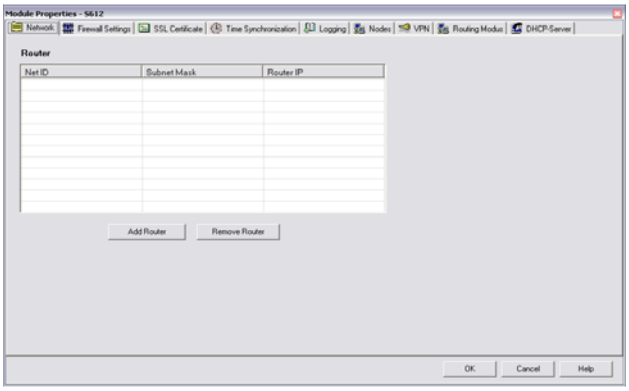
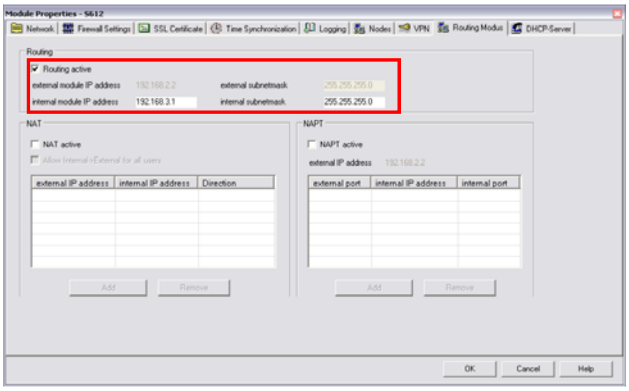
For configuring the SCALANCE S please enter the IP address **192.168.2.3** for your PC/PG. (subnet mask 255.255.255.0)

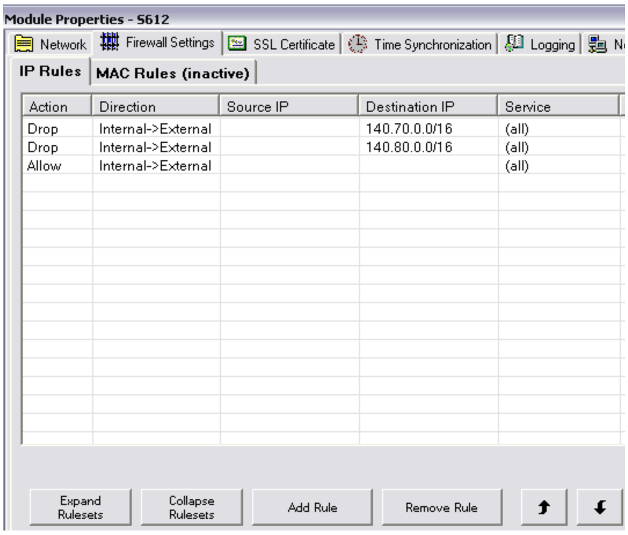
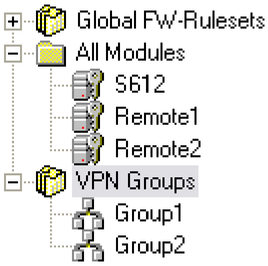
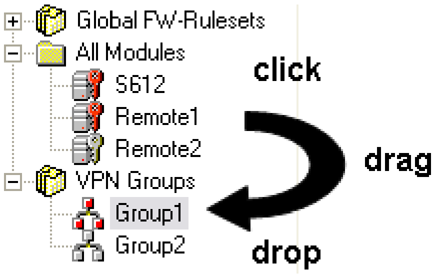
VPN tunnel configuration station 2/3 – SCALANCE S in the control center

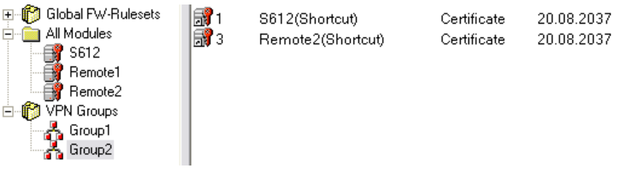
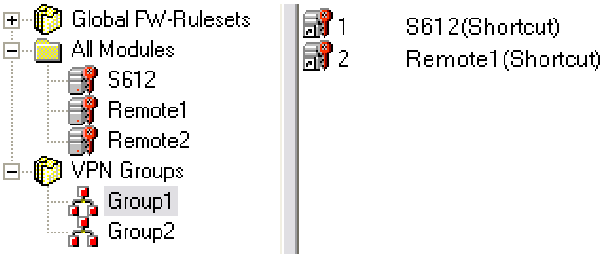
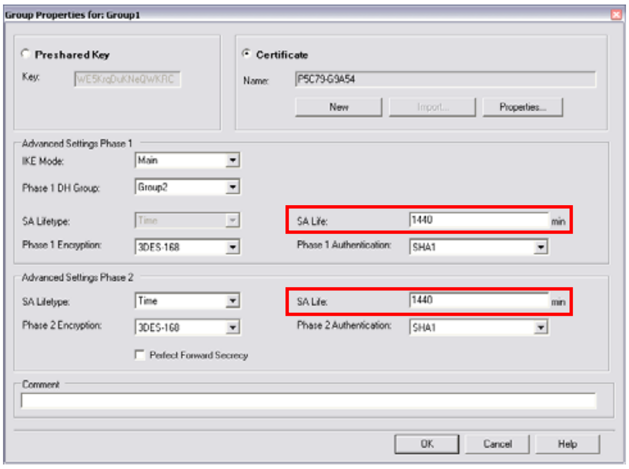
Table 5-7

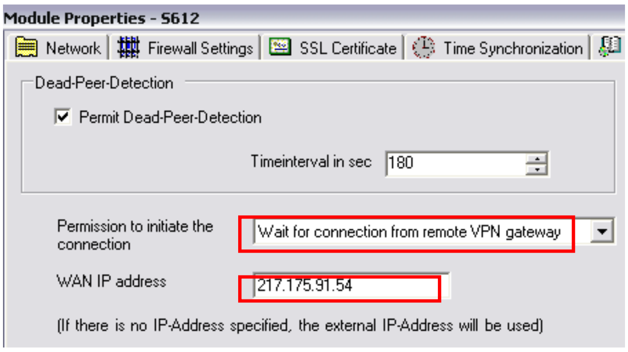
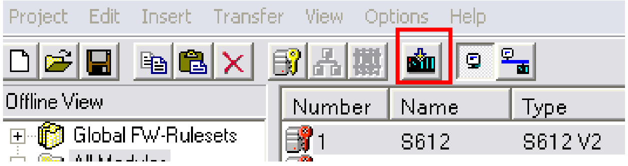
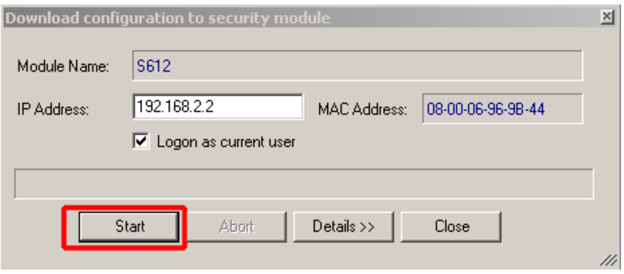
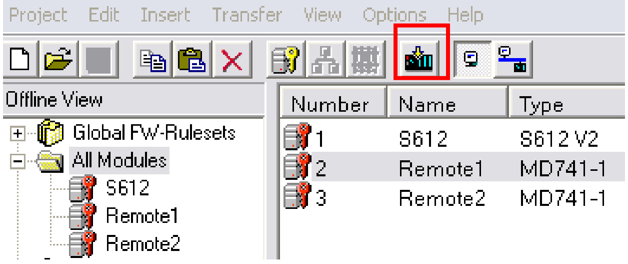
No.	Action	Remark / note
1.	Open the Security Configuration Tool (SCT). **`Start -> SIMATIC -> SCALANCE -> Security -> Security Configuration Tool`**	 Security Configuration Tool Project Edit Insert Transfer View Options Help Offline View Group Name Authentication Group membership until Comment Ready Current User: (user) Role: (role) Standard Mode Offline
2.	Create a new project with **`Project -> New`**. You will be prompted for User Name and Password. Complete this dialog. Admin; Password: VPN) and close it with **OK**.	New administrator User Name: Admin Password: *** Password confirmation: ***
3.	The first module is automatically added. Change the module line as follows: **Name:** S612 **Type:** S612 V2 **IP Address ext.**: 192.168.2.2 **Subnet Mask ext:** 255.255.255.0. **Default Router:** 192.168.2.1 The **MAC address** is available at your SCALANCE S. It is printed on the front casing.	N... Name Type IP Address ... Subnet Mask... I... S Default R... MAC Address Comment 1 S612 S612 V2 192.168.2.2 255.255.255.0 192.168.2.1 08-00-06-96-9B-44
4.	Insert a new module with **`Insert -> Module`**.	
5.	Change the second module line as follows. **Name**: Remote1 **Type:** MD741-1 **IP Address ext.:** keep default settings **Subnet Mask ext**: keep default settings **IP Address int:** 140.70.0.1 **Subnet Mask int**: 255.255.0.0	Number Name Type IP Address ext. Subnet Mask ext. IP Address int. Subnet Mask int. 1 S612 S612 V2 192.168.2.2 255.255.255.0 2 Remote1 MD741-1 192.168.10.1 255.255.255.0 140.70.0.1 255.255.0.0 **Note:** The SCT requires an external IP address for the MD741-1. However, it is specified dynamically by the mobile radio network provider and cannot be entered here. Keep the default IP address of the SCT (here: 192.168.10.1).
6.	Insert a new module with **`Insert -> Module`**.	

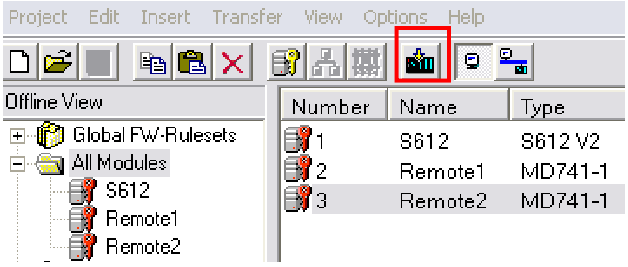
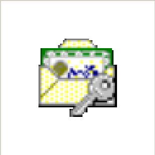
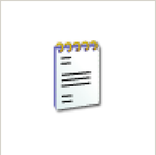
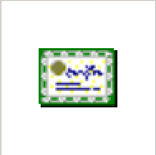
<table>
<tr><th>No.</th><th>Action</th><th>Remark / note</th></tr>
<tr><td>7.</td><td>Change the third module line as follows.
<b>Name</b>: Remote2
<b>Type:</b> MD741-1
<b>IP Address ext.:</b> keep default settings
<b>Subnet Mask ext</b>: keep default settings
<b>IP Address int:</b> 140.80.0.11
<b>Subnet Mask int</b>: 255.255.0.0

Save your project.</td><td>
<table>
<tr><th>Number</th><th>Name</th><th>Type</th><th>IP Address ext.</th><th>Subnet Mask ext.</th><th>IP Address int.</th><th>Subnet Mask int.</th></tr>
<tr><td>1</td><td>S612</td><td>S612 V2</td><td>192.168.2.2</td><td>255.255.255.0</td><td></td><td></td></tr>
<tr><td>2</td><td>Remote1</td><td>MD741-1</td><td>192.168.10.1</td><td>255.255.255.0</td><td>140.70.0.1</td><td>255.255.0.0</td></tr>
<tr><td>3</td><td>Remote2</td><td>MD741-1</td><td>192.168.10.2</td><td>255.255.255.0</td><td>140.80.0.11</td><td>255.255.0.0</td></tr>
</table></td></tr>
<tr><td>8.</td><td>Select <b><code>View -> Advanced Mode</code></b> to go to the advanced mode of the SCT. Confirm the following dialog box with <b>Yes</b>. In the advanced mode there are further settings options.</td><td>
</td></tr>
<tr><td>9.</td><td>Select the first module line (SCALANCE S module). Double-click to open the Properties dialog.</td><td>
</td></tr>
<tr><td>10.</td><td>Switch to the <b>Routing Mode</b> tab. Activate the <b>Routing active</b> mode and enter <b>internal IP address</b> (192.168.3.1) and <b>subnet mask</b> (255.255.255.0).
Close Module Properties dialog with OK.</td><td>
Module Properties - S612
Routing
☑ Routing active
external module IP address 192.168.2.2 external subnetmask 255.255.255.0
internal module IP address 192.168.3.1 internal subnetmask 255.255.255.0
NAT
☐ NAT active
☐ Allow Internal->External for all users
NAPT
☐ NAPT active
external IP address 192.168.2.2
</td></tr>
</table>

No.	Action	Remark / note
11.	If you have used the function **NAT active** in step 10 make the following settings: Go to the **Firewall Settings** (**Firewall**) tab. Use the **Add Rule** button to enter a new drop rule. As **Destination IP** you enter the IP address of the remote subnet. Remote1: 140.70.0.0/16 (MD741-1 in Station_02) Repeat the same procedure for the second router! Remote2: 140.80.0.0/16 (MD741-1 in Station_03) At last enter an Allow rule for access from your local network (SCALANCE local network) via the SCALANCE and DSL router to the internet. Click **OK** to apply the settings.	Module Properties - S612 Network · Firewall Settings · SSL Certificate · Time Synchronization · Logging · N IP Rules · MAC Rules (inactive) Action · Direction · Source IP · Destination IP · Service Drop · Internal->External · · 140.70.0.0/16 · (all) Drop · Internal->External · · 140.80.0.0/16 · (all) Allow · Internal->External · · · (all) Expand Rulesets · Collapse Rulesets · Add Rule · Remove Rule A drop rule should be inserted for every destination subnet. If no VPN tunnel has been set up yet, all packages addressed to the MD741-1 are rejected. The last firewall rule allows all remaining packages to other stations. With this rule the firewall from internal to external will be open, for all packages which have not been rejected.
12.	Select the **VPN Groups** in **Offline View** and click the right mouse-button. Now create a new group via **`Insert Group`**. Repeat this process a second time.	Global FW-Rulesets All Modules S612 Remote1 Remote2 VPN Groups Group1 Group2 **Note:** Alternatively you can configure all modules in the same group. This makes the VPN properties and the certificates for all MD741-1 identical.
13.	The **S612** and the MD741-1 **Remote1** are placed in **Group1**. Select the modules **S612** and **Remote1** individually in the same column and draw them into **Gruppe1** via drag&drop.	Global FW-Rulesets All Modules S612 Remote1 Remote2 VPN Groups Group1 Group2 click drag drop

No.	Action	Remark / note
14.	The **S612** and the MD741-1 **Remote2** are placed in **Group2**. Select the modules **S612** and **Remote2** individually in the same column and draw them into **Gruppe2** via drag&drop.	 Global FW-Rulesets All Modules S612 Remote1 Remote2 VPN Groups Group1 Group2 1 S612(Shortcut) Certificate 20.08.2037 3 Remote2(Shortcut) Certificate 20.08.2037 **Note:** A group represents a VPN connection. Only nodes which are part of this group can participate in the VNP tunnel communication.
15.	Select e.g. **Group1** in the column. All stations of the group hence a VPN connection are listed.	 Global FW-Rulesets All Modules S612 Remote1 Remote2 VPN Groups Group1 Group2 1 S612(Shortcut) 2 Remote1(Shortcut)
16.	For each group the group properties must still be adjusted: A double-click on the group makes the window with the Properties appear.	
17.	Change the SA Lifetimes to 1440 minutes. Click OK to close the dialog box. Repeat the same procedure for the other group!	 Group Properties for: Group1 ○ Preshared Key Key: WE5KrqDuKNeQWKRC ● Certificate Name: P5C79-G9A54 Advanced Settings Phase 1 IKE Mode: Main Phase 1 DH Group: Group2 SA Lifetype: Time SA Life: 1440 min Phase 1 Encryption: 3DES-168 Phase 1 Authentication: SHA1 Advanced Settings Phase 2 SA Lifetype: Time SA Life: 1440 min Phase 2 Encryption: 3DES-168 Phase 2 Authentication: SHA1 □ Perfect Forward Secrecy Comment New Import... Properties... OK Cancel Help
18.	Change back to the module lines and select the first module line (SCALANCE S).	

No.	Action	Remark / note
19.	Open the Properties of the SCALANCE S modules via double-click. Now go to the **VPN** tab. Set the **Dead Peer Detection** of the S612 to 180 seconds. This function prevents that old, not valid VPN tunnels will be shown in the online view. The SCALANCE S **waits for the connection** of the MD741-1. Change the permission to initiate the connection accordingly. As the **WAN-IP Address** you specify the **fixed IP-Address** of your DSL router. Click OK to close the dialog box.	 Module Properties - S612 Network Firewall Settings SSL Certificate Time Synchronization Dead-Peer-Detection ☑ Permit Dead-Peer-Detection Timeinterval in sec: 180 Permission to initiate the connection: Wait for connection from remote VPN gateway WAN IP address: 217.175.91.54 (If there is no IP-Address specified, the external IP-Address will be used) Note: • The Dead-Peer-Detection für SCALANCE S must be set to a higher value than in the MD741-1. (Default setting for the MD741-1 is 150 seconds) • DynDNS is not supported by SCALANCE S.
20.	Connect your PC/PG with the external port of the SCALANCE S.	The SCALANCE S has no default IP Address. Download occurs via the given MAC address
21.	Load the configuration into the SCALANCE S. Select the SCALANCE S module line in the right window and click **Transfer**.	 Project Edit Insert Transfer View Options Help Offline View Global FW-Rulesets Number / Name / Type 1 / S612 / S612 V2
22.	In the following dialog you start the transmission to SCALANCE S by pressing **Start**	 Download configuration to security module Start Abort Details >> Close Module Name: S612 IP Address: 192.168.2.2 MAC Address: 08-00-06-96-9B-44 ☑ Logon as current user
23.	Create another directory **MD741_Remote2** in **D:\ SINAUT _Configuration9**. There you save the configuration for the MD741-1 of **Remote Station1**. Select the modem module line 2 and click **Transfer**. As a target directory you specify the just generated directory for the configuration files and certificates. Acknowledge the following dialog with **Yes** for a new certificate password or with **No** for a default password.	 Project Edit Insert Transfer View Options Help Offline View Global FW-Rulesets All Modules S612 Remote1 Remote2 Number / Name / Type 1 / S612 / S612 V2 2 / Remote1 / MD741-1 3 / Remote2 / MD741-1 The .p12 certificate is password protected. You have the option of using the project name of the SCT as a password or to assign a different one. **Note:** It is recommended to assign a new password.

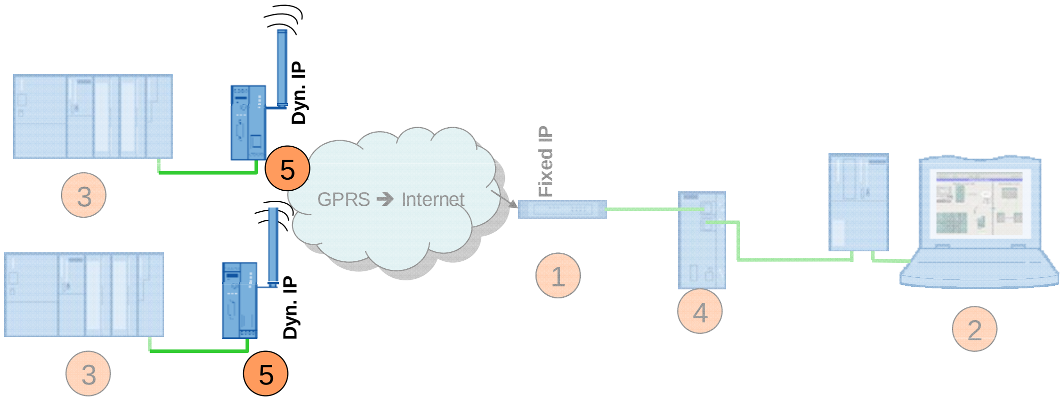
No.	Action	Remark / note
24.	Create another directory **MD741_Remote2** in **D:\ SINAUT _Configuration8**. There you save the configuration for the MD741-1 of **Remote Station2**. Continue as for the other MD741-1 of Remote Station1.	 Project Edit Insert Transfer View Options Help Offline View Global FW-Rulesets All Modules S612 Remote1 Remote2 Number / Name / Type 1 / S612 / S612 V2 2 / Remote1 / MD741-1 3 / Remote2 / MD741-1 **Note:** Please save the certificates for the second station into a new directory as recommended. Otherwise the peers certificates with the same name are saved to the same directory and will be overwritten there.
25.	In the target directory, a text file is saved for configuring the MD741-1, the CA certificate and the p12 certificate.	 Configuration1.MFBA3@ G9A54.Group1.p12  Configuration1.Remot...  Configuration1.S612.cer

Note If you use the MD740-1 Router (instead of MD741-1) configure both remote stations in one VPN –group by inserting both MD740-1 in one group per Drag&Drop.

Note The MD740-1 Router should always be inserted in one VPN-group.

5.3.5 Configuration the MD741-1

Figure 5-6



Commissioning the MD741-1 occurs in three steps:

- execute PIN configuration
- insert SIM card into the device

- further configurations

Required PC/PG IP address

Table 5-8

Action	Setting
For the configuration of the MD741-1 you assign an IP address to your PG/PC which is located in the same network as your MD741-1.	According to the factory settings the MD741-1 has the address 192.168.1.1.

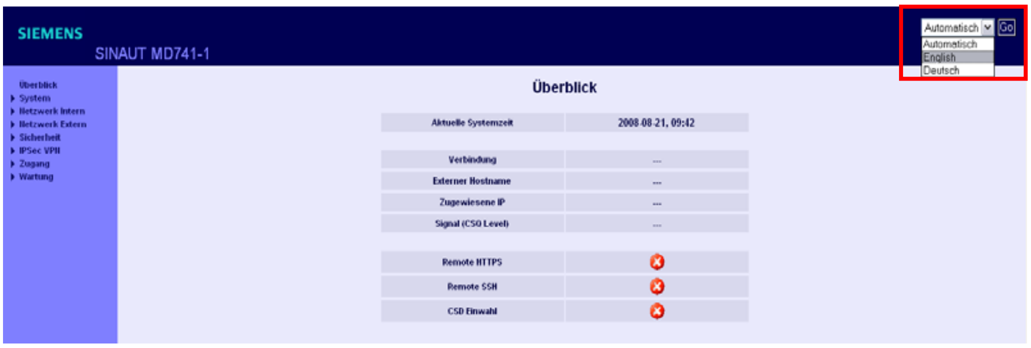
5.3.6 MD741-1 of 02_Station

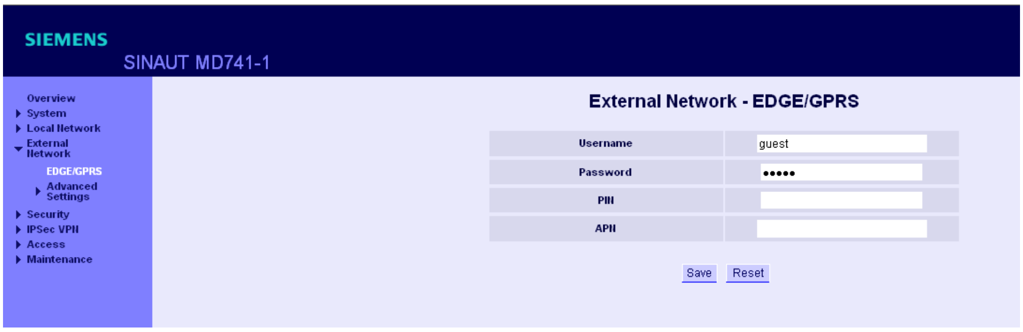
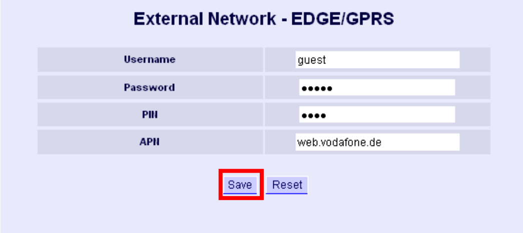
Step 1: PIN configuration

For the MD741-1 to be able to communicate via the GPRS network, the PIN of the SIM card must be announced to the device.

ATTENTION **First announce the PIN to the MD741-1 and then insert the SIM card.**

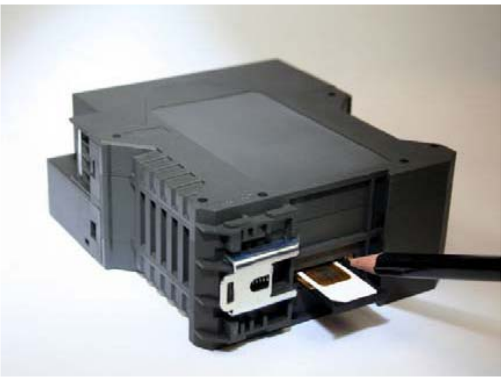
Table 5-9

No	Action	Remark / note
1.	Connect the PC with the Ethernet connector of the MD741-1.	According to the factory settings the MD741-1 has the address 192.168.1.1.
2.	Start a browser and enter the address **https://[ip-adresse MD741-1]**.	After successful connection, a security dialog appears which you acknowledge with **Yes**.
3.	Enter user name and password.	The default settings are: **User name: admin** **Password: sinaut**
4.	The administrator website opens The default language is German. You can set the language in the top right field and accept the settings to the MD741-1 with **go**.	
	 SIEMENS SINAUT MD741-1 Automatisch Go Automatisch English Deutsch Überblick System Netzwerk Intern Netzwerk Extern Sicherheit IPSec VPN Zugang Wartung Überblick Aktuelle Systemzeit 2008-08-21, 09:42 Verbindung --- Externer Hostname --- Zugewiesene IP --- Signal (CSQ Level) --- Remote HTTPS ☒ Remote SSH ☒ CSD Einwahl ☒	
5.	Go to **`External Network -> EDGE/GPRS`**	

No	Action	Remark / note
	 SIEMENS SINAUT MD741-1 Overview System Local Network External Network EDGE/GPRS Advanced Settings Security IPSec VPN Access Maintenance External Network - EDGE/GPRS Username: guest Password: ••••• PIN: APN: Save Reset	
6.	In **Username** and **Password** (identical in both lines) you enter the access data for your APN. The default setting for both fields is **guest**. For Vodafone: **Username: guest** **Password: guest** In **APN** you enter the address of your Access Point name. For Vodafone: **web.vodafone.de** For T mobile: **internet.t-mobile** Under **PIN** you enter the PIN of your SIM card. Save the settings by selecting **Save**.	 External Network - EDGE/GPRS Username: guest Password: ••••• PIN: •••• APN: web.vodafone.de Save Reset

Step 2: Insert SIM card

Table 5-10

No.	Action	Remark / note
1.	Separate the MD741-1 from the power supply	
2.	Insert the SIM card as in the picture and connect the router to the power supply.	

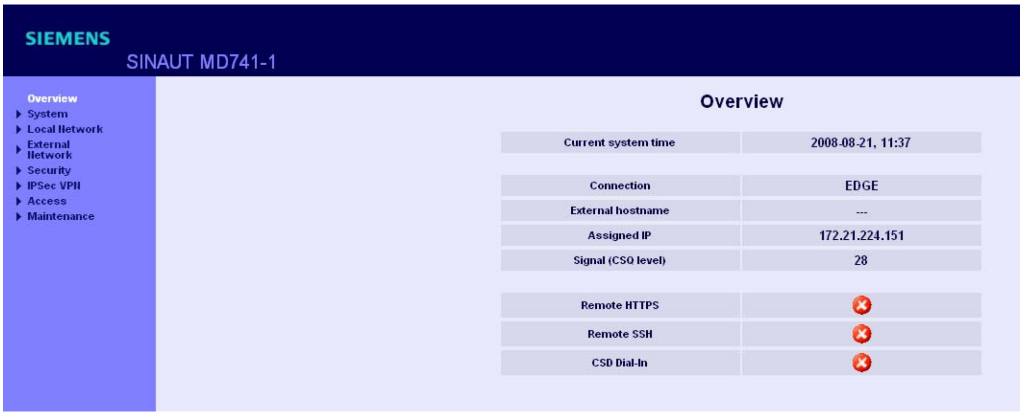
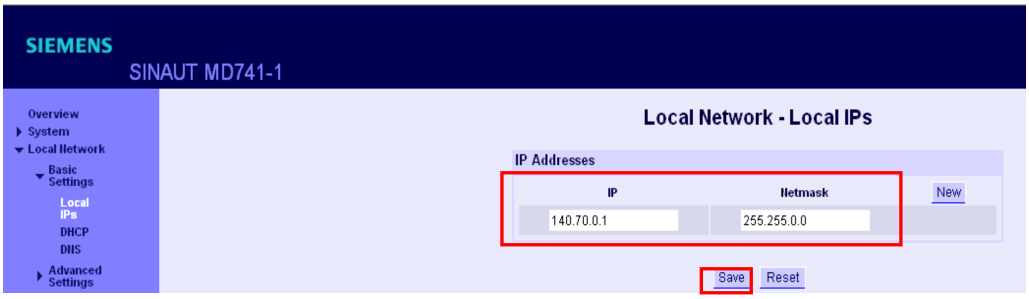
Note

The MD741-1 will now attempt to initiate a connection with the EGPRS/GPRS network. When the connection has been established, the LED S (status) lights up statically. The LED C (Connect) is ON with short interruptions if MD74-1 is logged in at GPRS and lights statically if MD741-1 is logged in at EGPRS. LED Q (quality) indicates the field intensity.

Step 3: Further configurations

IP Address

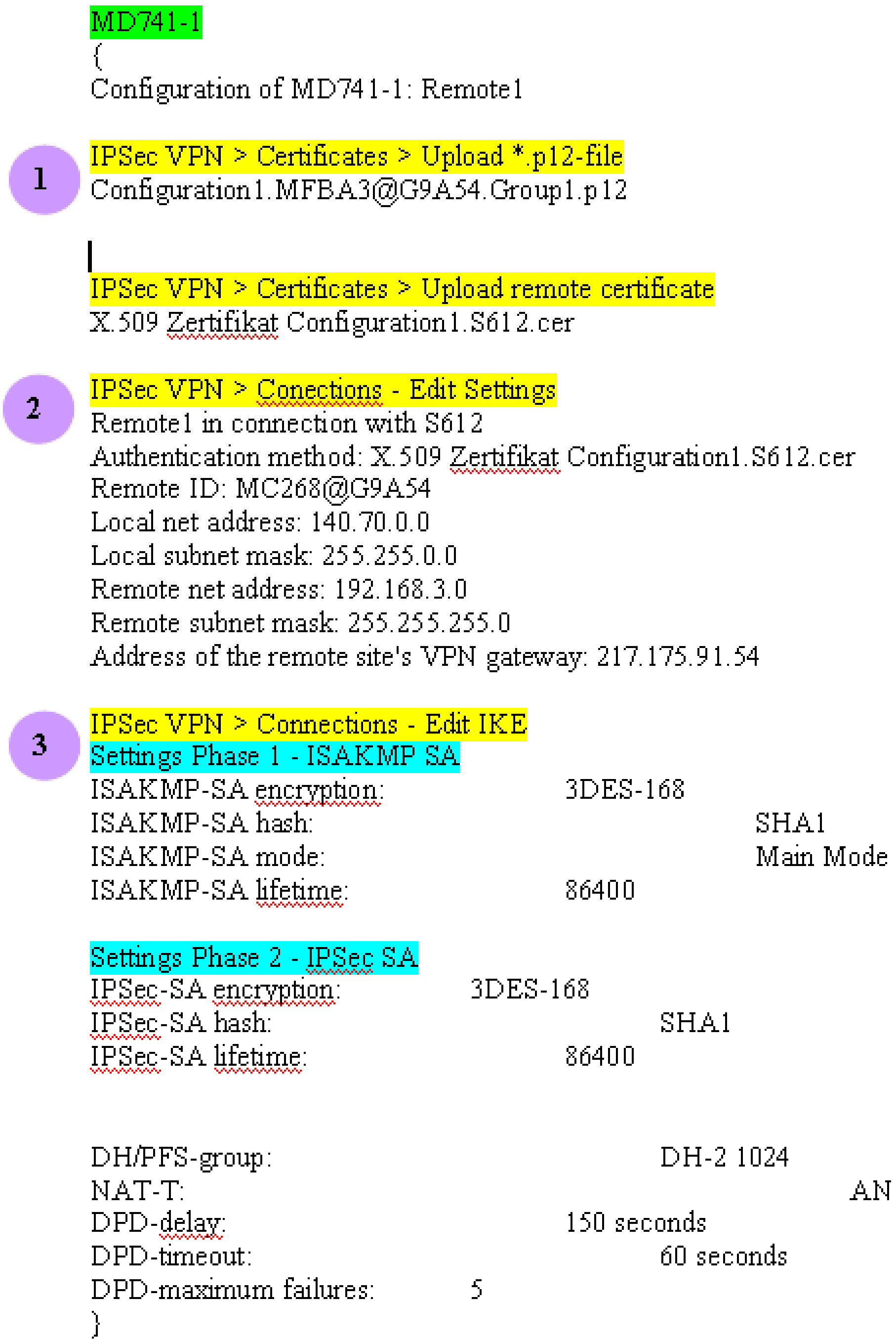
Table 5-11

No.	Action	Remark / note
1.	Open the administrator website of the MD741-1 again. The **`Overview`** mask shows you information on the connection in EDGE or GPRS network, the signal strength and the IP address assigned by the provider	
	 SIEMENS SINAUT MD741-1 Overview System Local Network External Network Security IPSec VPN Access Maintenance Overview Current system time: 2008-08-21, 11:37 Connection: EDGE External hostname: --- Assigned IP: 172.21.224.151 Signal (CSQ level): 28 Remote HTTPS: ✗ Remote SSH: ✗ CSD Dial-In: ✗	
2.	Go to **`Local Network -> Basic Settings -> Local IPs.`** Change the internal IP address of the MD741-1 according to ##. Accept the settings with **Save**. **Note:** You have to adjust the IP address of your PCs/PGs accordingly (e.g. 140.70.0.20) and then open the website of the MD741-1 again.	
	 SIEMENS SINAUT MD741-1 Overview System Local Network Basic Settings Local IPs DHCP DNS Advanced Settings New Save Reset Local Network - Local IPs IP Addresses IP: 140.70.0.1 Netmask: 255.255.0.0	

Configuring the VPN connection

Note For further configurations, the text file helps which was generated with the Security Configuration tool.

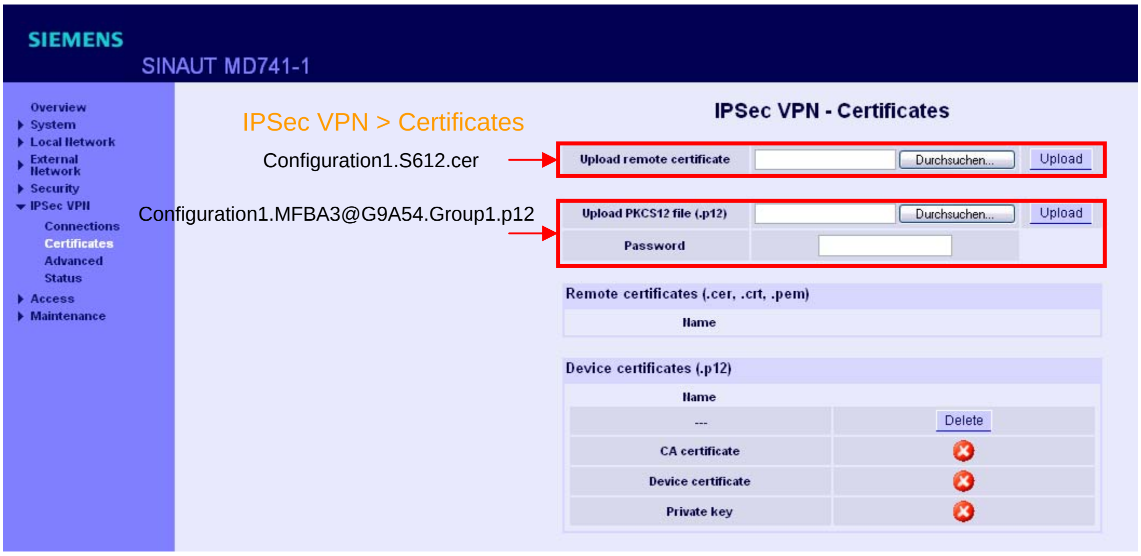
Figure 5-7



```
MD741-1
{
Configuration of MD741-1: Remote1

IPSec VPN > Certificates > Upload *.p12-file
Configuration1.MFBA3@G9A54.Group1.p12

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

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

IPSec VPN > Connections - 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 Create certificates

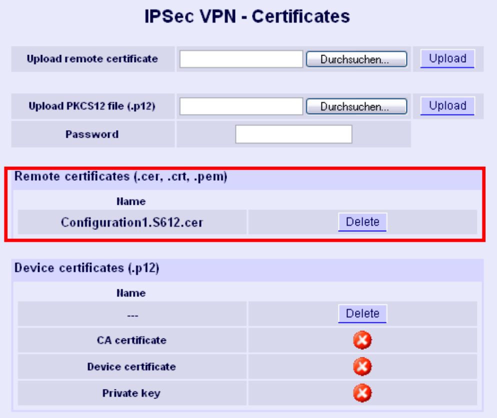
Figure 5-8

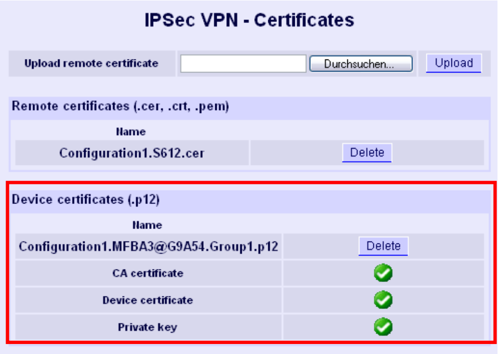


Configuration1.S612.cer

Configuration1.MFBA3@G9A54.Group1.p12

Table 5-12

No	Action	Remark / note
1.	Go to **`IPSec VPN -> Certificates.`** Use the **Browse…** button to go to the directory in which you have saved the configuration data and certificates for the MD741-1.	**D:\SINAUT_Configuration8\MD741_Remote 1**
2.	Open the remote certificate (.cer), which is given in your text file.	Here: Configuration1.S612.cer
3.	Import the certificate with **Upload.** In **Remote Certificates** it is indicated that the certificate has been imported.	 IPSec VPN - Certificates Upload remote certificate – Durchsuchen... – Upload Upload PKCS12 file (.p12) – Durchsuchen... – Upload Password Remote certificates (.cer, .crt, .pem) Name Configuration1.S612.cer – Delete Device certificates (.p12) Name --- – Delete CA certificate Device certificate Private key
4.	To import your own certificate (.p12) you use the **Browse…** button to go to the directory in which you have saved the configuration data and certificates for the MD741-1.	
5.	Open your own certificate (.p12), which is given 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.	Either the SCT project name or a new password.

No	Action	Remark / note
7.	Import the certificate with **Upload.** In **Device Certificates** it is indicated that the certificate has been imported.	 IPSec VPN - Certificates Upload remote certificate [ ] Durchsuchen... Upload Remote certificates (.cer, .crt, .pem) Name: Configuration1.S612.cer – Delete Device certificates (.p12) Name: Configuration1.MFBA3@G9A54.Group1.p12 – Delete CA certificate ✓ Device certificate ✓ Private key ✓

2 Create and process connection

Table 5-13

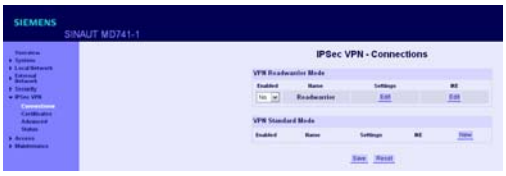
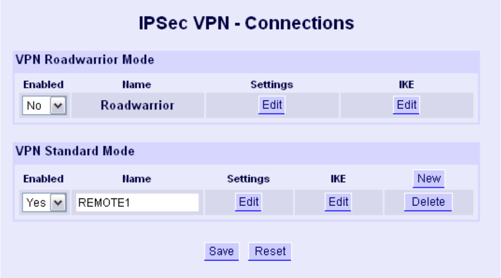
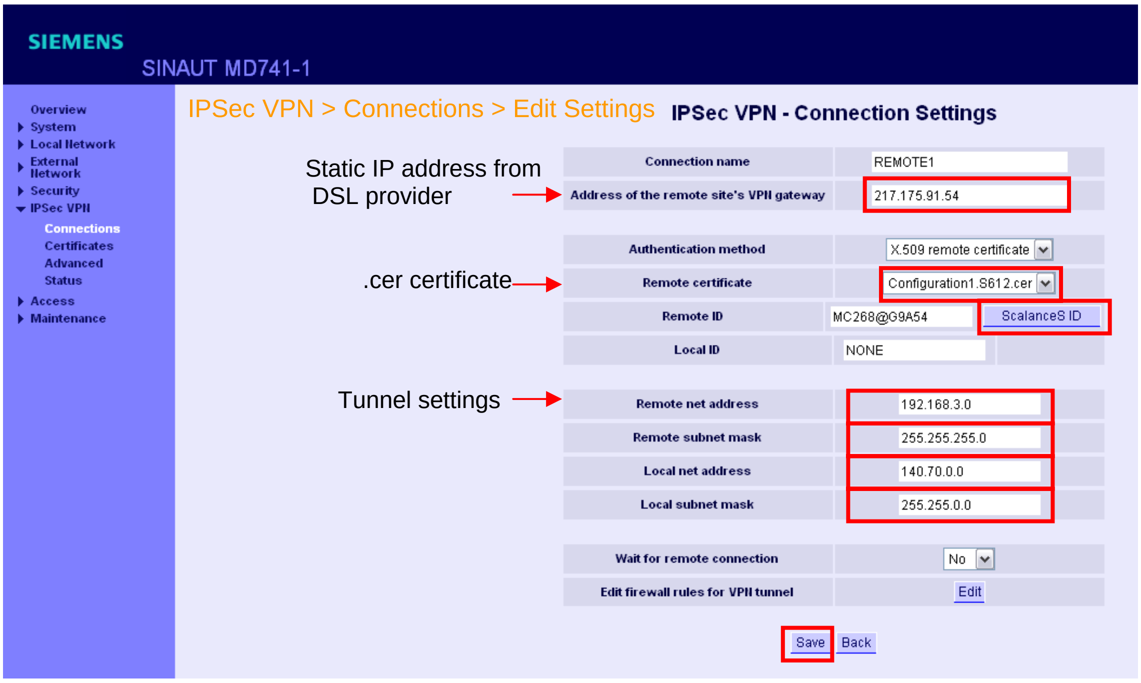
No.	Action	Remark / note
1.	Go to **`IPSec VPN -> Connections.`**	 SIEMENS SINAUT MD741-1 Overview System Local Network External Network Security IPSec VPN Connections Certificates Advanced Status Access Maintenance IPSec VPN - Connections VPN Roadwarrior Mode Enabled Name Settings IKE No Roadwarrior Edit Edit VPN Standard Mode Enabled Name Settings IKE New Save Reset
2.	Generate a new connection with **New**. In this example **REMOTE1** was used for the connection name. Accept the settings with **Save**.	 IPSec VPN - Connections VPN Roadwarrior Mode Enabled: No – Name: Roadwarrior – Settings: Edit – IKE: Edit VPN Standard Mode Enabled: Yes – Name: REMOTE1 – Settings: Edit – IKE: Edit – New / Delete Save Reset

Figure 5-9



IPSec VPN - Connection Settings

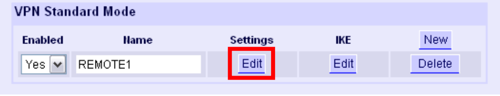
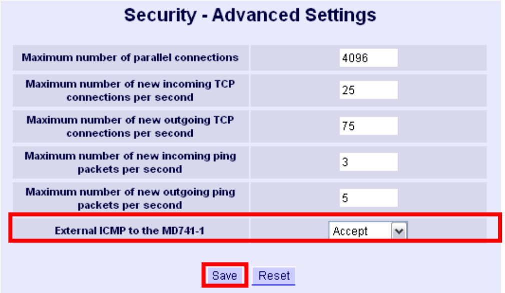
Static IP address from DSL provider

.cer certificate

Tunnel settings

Connection name	REMOTE1
Address of the remote site's VPN gateway	217.175.91.54
Authentication method	X.509 remote certificate
Remote certificate	Configuration1.S612.cer
Remote ID	MC268@G9A54
Local ID	NONE
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

Table 5-14

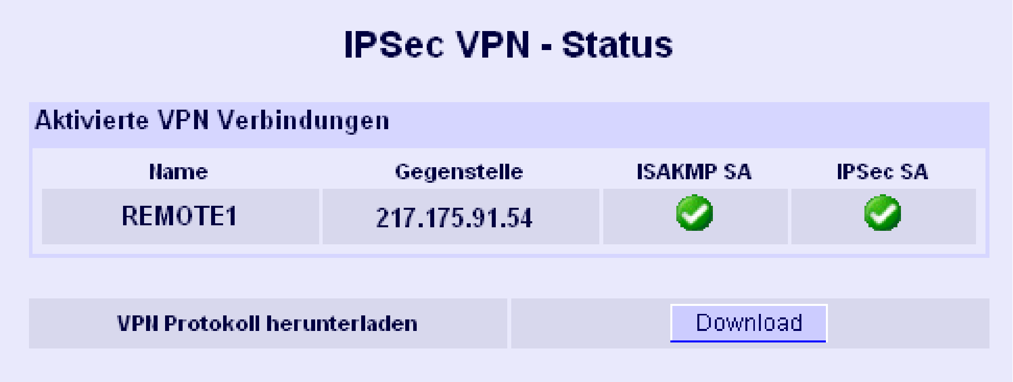
No.	Action	Remark / note
1.	Use the **Settings Edit** button to switch to the connection properties.	 VPN Standard Mode Enabled: Yes Name: REMOTE1 Settings: Edit IKE: Edit New Delete
2.	As **remote Gateway Address** you enter the **fixed IP Address** of your DSL connection	Here: 217.175.91.54
3.	In **Remote Certificate** you select your .cer certificate.	
4.	Click on the **ScalanceS ID** button in order to accept the **Remote ID**.	
5.	Enter the settings for the addresses of the local and the opposite network according to your text file. Accept the settings with **Save**.	
6.	Go to **`Security -> Advanced Settings`** Set the parameter **External ICMP to the MD741-1** to **Accept.** Accept the settings with **Save**.	 Security - Advanced Settings Maximum number of parallel connections: 4096 Maximum number of new incoming TCP connections per second: 25 Maximum number of new outgoing TCP connections per second: 75 Maximum number of new incoming ping packets per second: 3 Maximum number of new outgoing ping packets per second: 5 External ICMP to the MD741-1: Accept Save Reset

VPN connection test

As soon as all settings have been transferred to the MD741-1, the EGPRS router automatically initiates a VPN tunnel to SCALANCE S612. This can be viewed

- at the green LED VPN at the MD741-1 and
- on the website of the router at **`IPSec VPN -> Status`**

Figure 5-10



IPSec VPN - Status

Aktivierte VPN Verbindungen

Name	Gegenstelle	ISAKMP SA	IPSec SA
REMOTE1	217.175.91.54	✓	✓

VPN Protokoll herunterladen: Download

If you have made IKE or NAT-T settings in your SCT project that are different than in this example, please follow points 3 and 4.

3

IKE settings

Table 5-15

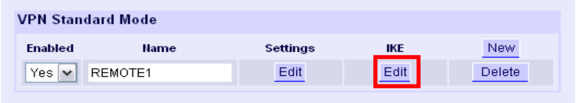
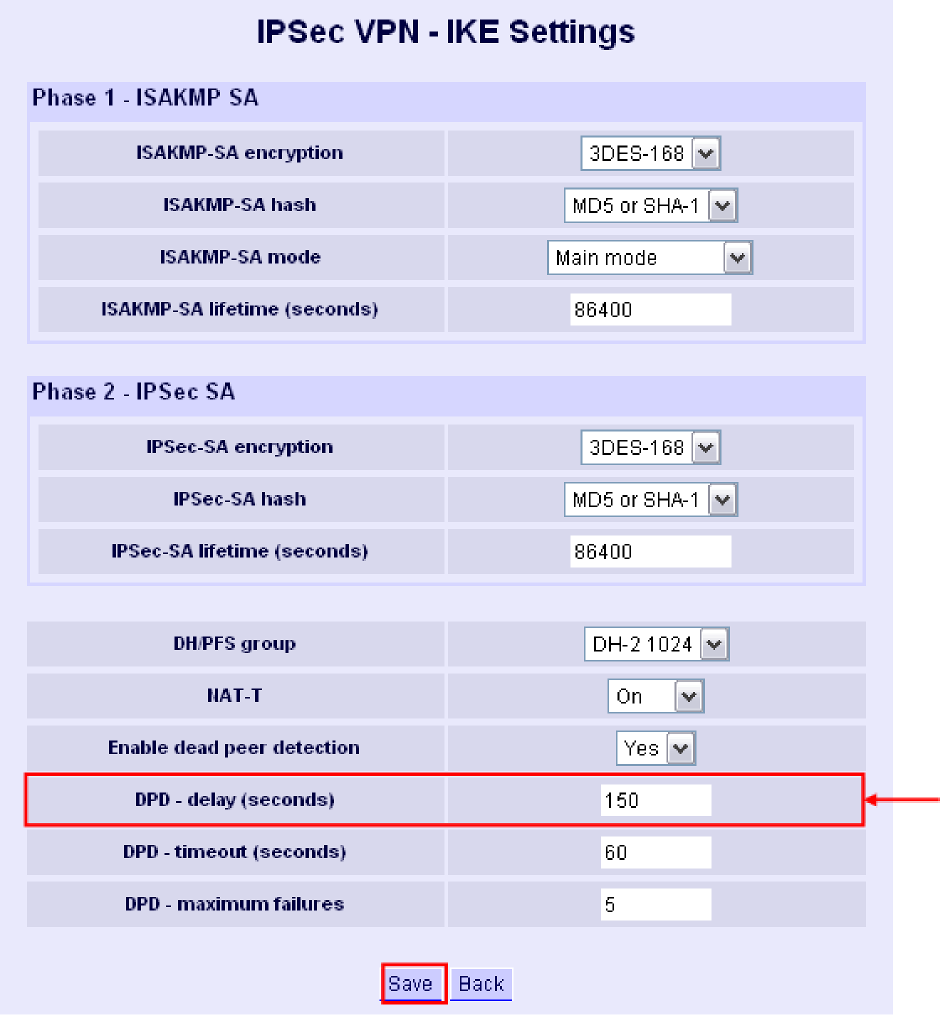
No.	Action	Remark / note
1.	The **IKE Edit** button takes you to the additional IKE settings.	 VPN Standard Mode Enabled: Yes · Name: REMOTE1 · Settings: Edit · IKE: Edit · New / Delete
2.	Enter the settings according to your text file and accept the settings with **Save**.	

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
NAT-T	On
Enable dead peer detection	Yes
DPD - delay (seconds)	150
DPD - timeout (seconds)	60
DPD - maximum failures	5

Here the cyclic time window **Dead Peer Detection** can be changed. Default setting is 150 seconds.

Hinweis

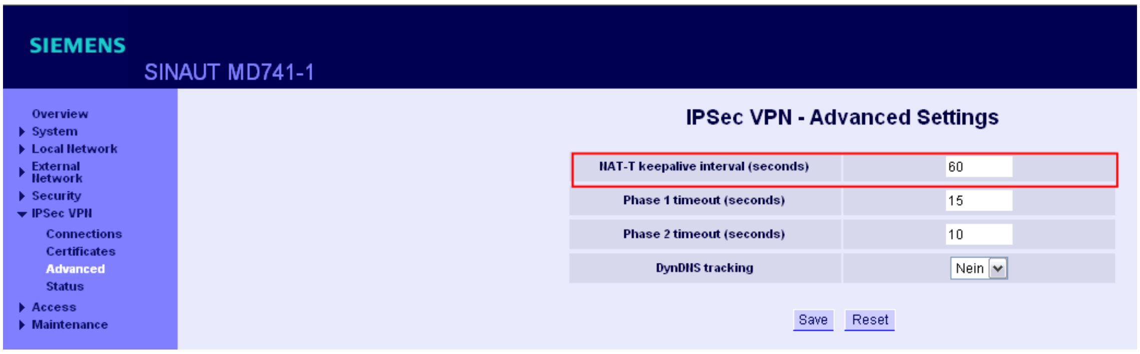
The default setting for the DPD- parameter of the DM741-1 is recommended for most applications. With this value it can take up to roughly 8 to 9 minutes to be noticed that the tunnel is aborted. You can set this value lower so that an abortion of the tunnel will be identified quicker. Is the DPD value reduced then a higher data volume will be produced.

4

Advanced Settings NAT-T Keep Alive

To maintain the NAT Gateway at the APN the NAT-T Keep Alive is sent after a certain time. Default setting is 60 seconds. You can change this time on the web page of the MD741-1 at **`IPSec VPN -> Advanced`**.

Figure 5-12



IPSec VPN - Advanced Settings

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

5.3.7 MD741-1 of 03_Station

This EGPRS Router MD741-1 is configured analog to the MD741-1 of 02_Station and is not described in detail here.

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

- execute PIN configuration
- insert SIM card into the device
- Further configurations

Use **03_Station** as connection name.

The text file and the certificates are available at

D\SINAUT_Configuration8\ MD741_03_Station.

Note

For the configuration you connect the PC/ PG with the MD741-1 in Station3 via a standard Ethernet cable. The MD741-1 supports the “autocrossing” function, which 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, you change the IP address of the PCs/PGs according to table 5-5.

Connect all stations according to figure 5-1.

6.2 Commissioning the ST7cc control center and radio test

Note Commissioning the ST7cc control center is briefly discussed in this chapter. A precise step-by-step instruction is available in Volume 1.

Startup

Commissioning the ST7cc control center requires the following steps:

- Start WinCC and open project ***D:\SINAUT_Configuration8\WinCC_INTERNET\ DemoTIM3V-IE\ DemoTIM3V-IE.MCP***.
- Start ST7cc config (at START -> SIMATIC -> ST7cc -> ST7cc config) and open the project ***D:\SINAUT_Configuration8\... DemoTIM3V-IE\ST7cc\ST7_Project.XML***.
- Activate the project for runtime in ST7cc config and load the server settings into the system.
- Start ST7cc Runtime (START -> SIMATIC -> ST7cc -> ST7cc Runtime).
- Wait until the ST7cc server is running.
- Start WinCC runtime.

Operating scenarios

Whether a connection with the stations has been established can be recognized in the WinCC Runtime. The picture typicals for the stations are indicated as green.

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

7 Diagnostics

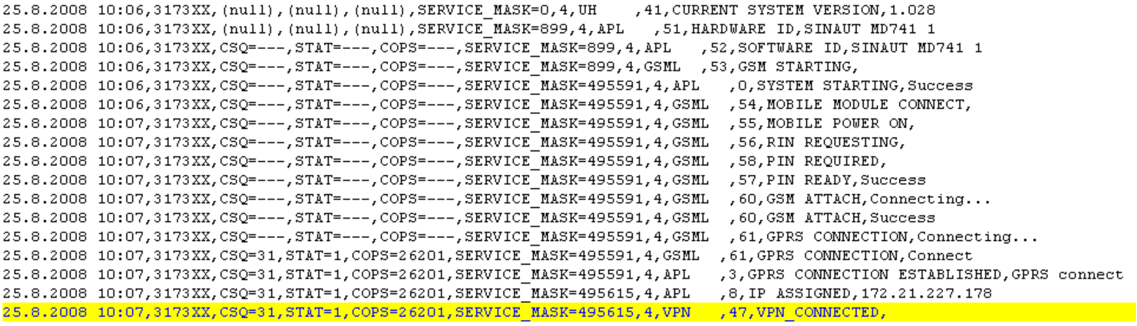
7.1 Diagnostic capabilities

Here we show you the options of how to diagnose the transmission chain.

MD741-1

You can obtain more on the VPN and system events in the system log file. Go to **`System -> Log`** and click on **Download**.

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

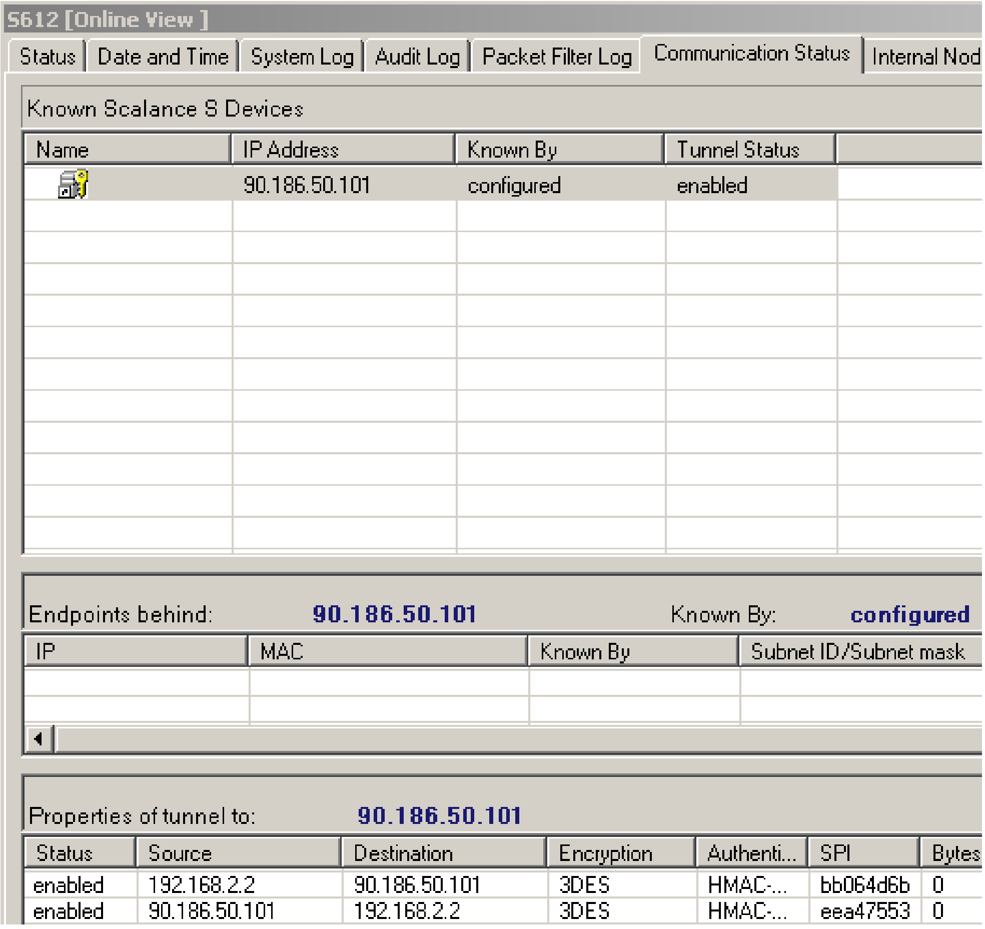
More information on further diagnostic capabilities is available in the manual on MD741-1 (see /2/ in the appendix)

Security Configuration Tool

The Security Configuration Tool has various online functions which enable a diagnosis.

- The communication status indicates whether and which VPN connections exist with which station.

Figure 7-2



Known Scalance S Devices

Name	IP Address	Known By	Tunnel Status
	90.186.50.101	configured	enabled

Endpoints behind: **90.186.50.101** Known By: **configured**

IP	MAC	Known By	Subnet ID/Subnet mask

Properties of tunnel to: **90.186.50.101**

Status	Source	Destination	Encryption	Authenti...	SPI	Bytes
enabled	192.168.2.2	90.186.50.101	3DES	HMAC-...	bb064d6b	0
enabled	90.186.50.101	192.168.2.2	3DES	HMAC-...	eea47553	0

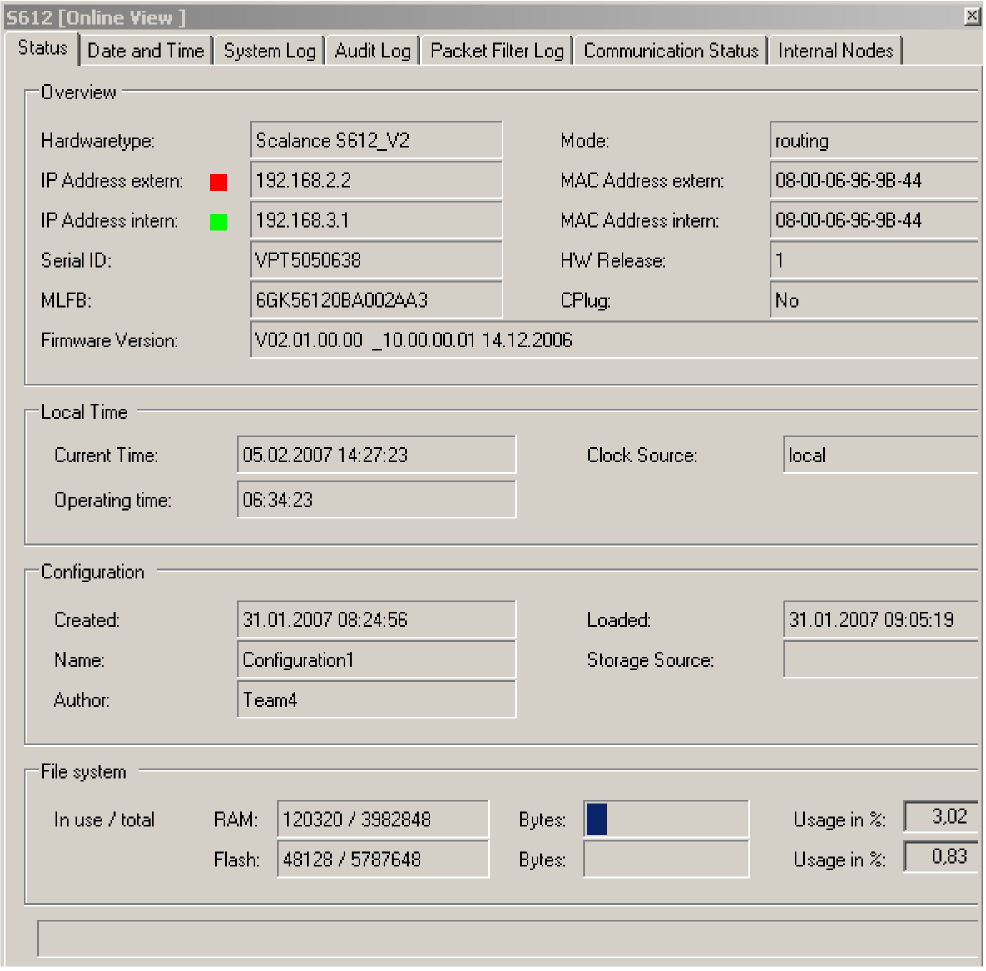
Note

Diagnostics of S612 is also available via the internal interface.

You can look at the diagnosis even if the PG/PC has just been used as ST7cc control center.

- The status gives an overview of the module, the current configuration in the module, as well as the load of the internal memory.

Figure 7-3



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 (former Ethereal), records the data traffic between stations. At the end of the recording, the data are depicted in form of packets and can be easily analyzed.

SINAUT ST7 Diagnostics and Service

The SINAUT ST7 Diagnostics and Service Tool provides functions for checking the connections, interfaces and communication. The firmware and software components of the network nodes can be read off.

Note Further information on the SINAUT ST7 diagnostics are available in the SINAUT ST7 system manual, Volume 2 Software (see /1/ in the appendix)

7.2 What to do if

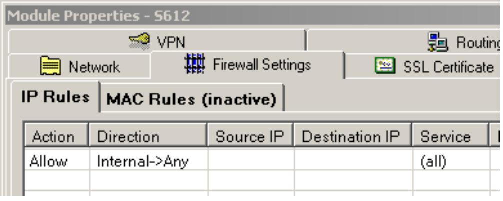
… no GPRS connection established?

Table 7-1

No.	Action	Remark / note
1.	Is the SIM card still valid?	
2.	Check the details on your APN and SIM card which you have entered on the website of the MD741-1. Were the settings transferred afterwards into the device?	Is the APN Address and the respective access code that of your provider? Have you entered the PIN correctly in both lines?
3.	Was the SIM card inserted correctly?	

… the VPN tunnel is not initiated?

Table 7-2

No.	Action	Remark / note
1.	Check all settings at modem and SCALANCE S.	Have the IP addresses been assigned correctly? Do the settings in the MD741-1 correspond with those of the text file ?
2.	Were Port 500 and Port 4500 forwarded to the SCALANCE S in the DSL router?	If the DSL router itself has IPSec functionality, switch it off in the router!
3.	Connect a second PC with Etherreal between DSL router and SCALANCE S. Check whether a data traffic occurs between these modules. Sniff the data packets as well. If no data traffic takes place, the DSL router is probably blocking the 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 the SCALANCE S, by calling an internet page with the PC/PG.	To do this you have to enable a connection towards **Internal -> Any** in the firewall of the SCALANCE S (in SCT in Properties of SCALANCE S612 -> **Firewall Settings**). Then load the SCALANCE again.  Module Properties - S612 VPN Routing Network Firewall Settings SSL Certificate IP Rules MAC Rules (inactive) Action Direction Source IP Destination IP Service Allow Internal->Any (all)

Appendix and List of Further Literature

8 Bibliography

8.1 Bibliographic References

This list is by no means complete and only provides a selection of appropriate sources.

Table 8-1

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

8.2 Internet Links

This list is not complete and only represents a selection of relevant literature.

Table 8-2

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

9 History

Table 9-1 History

Version	Datum	Modification
V1.0	20.03.2007	First issue
V2.0	18.05.2009	Application updated for MD 741-1 Expansion for cross communication between two stations
V2.1	14.02.2011	Notes and corrections have been inserted.