

SIEMENS

SIMATIC NET

Industrial Remote Communication Remote Networks SCALANCE M-800

Getting Started

Preface

Connecting SCALANCE M-800 to WAN

1




SCALANCE M-800 as DHCP server

2

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

 DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.
 WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.
 CAUTION
indicates that minor personal injury can result if proper precautions are not taken.
NOTICE
indicates that property damage can result if proper precautions are not taken.


If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

 WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Preface

Purpose

The configuration of the SCALANCE M is shown based on examples.

IP settings for the examples

Note

The IP settings used in the examples were freely chosen.

In a real network, you would need to adapt these IP settings to avoid possible address conflicts.

General naming conventions

The designation . . .	stands for . . .
SCT	Security Configuration Tool
SINEC PNI	SINEC Primary Network Initialization
Device	M87x M81x M826 S615
M87x	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4
M81x	SCALANCE M812-1 SCALANCE M816-1
M826	SCALANCE M826-2
S615	SCALANCE S615
M-800	SCALANCE M874-2 SCALANCE M874-3 SCALANCE M876-3 SCALANCE M876-4 SCALANCE M812-1 SCALANCE M816-1 SCALANCE M826-2 SCALANCE M804PB

Further documentation

- Operating instructions

These documents contain information on installing and connecting the products and on approvals for the products. The configuration and the integration of the devices in a network are not described in these instructions.

- SCALANCE M874, M876

Entry ID: 74518712

<https://support.industry.siemens.com/cs/ww/de/view/109475909/en>

- SCALANCE M812, M816

Entry ID: 90316607

<https://support.industry.siemens.com/cs/ww/de/view/90316607/en>

- SCALANCE M804PB:

Entry ID: 109759601

<https://support.industry.siemens.com/cs/ww/en/view/109759601>

- SCALANCE M826:

Entry ID: 99450800

<https://support.industry.siemens.com/cs/ww/de/view/99450800/en>

- SCALANCE S615:

Entry ID: 109475909

<https://support.industry.siemens.com/cs/ww/de/view/109475909/en>

- "Web based Management" configuration manual

This document is intended to provide you with the information you require to commission and configure devices using the Web Based Management.

- SCALANCE M-800:

Entry ID: 109751635

<https://support.industry.siemens.com/cs/ww/de/view/109751635/en>

- SCALANCE S615:

Entry ID: 109751632

<https://support.industry.siemens.com/cs/ww/de/view/109751632/en>

- Configuration manual Command Line Interface

This document contains the CLI commands supported by the devices.

- SCALANCE M-800

Entry ID: 109751634

<https://support.industry.siemens.com/cs/ww/de/view/109751634/en>

- SCALANCE S615

Entry ID: 109751633

<https://support.industry.siemens.com/cs/ww/de/view/109751633/en>

- Industrial Ethernet Security – Basics and Application
This document contains information about working with the SCT (Security Configuration Tool).
Entry ID: 56577508 (<https://support.industry.siemens.com/cs/ww/de/view/56577508/en>)
- SIMATIC NET Industrial Ethernet Network manual
This document contains information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network.
Entry ID: 27069465 (<https://support.industry.siemens.com/cs/ww/de/view/27069465/en>)

SIMATIC NET manuals

You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:

- using the search function:
Link to Siemens Industry Online Support
(<https://support.industry.siemens.com/cs/ww/en/ps>)
Enter the entry ID of the relevant manual or the article number of the device as the search term.
- In the navigation panel on the left hand side in the area "Industrial Communication":
Link to the area "Industrial Communication"
(<https://support.industry.siemens.com/cs/ww/en/ps/15247/man>)
Go to the required product group and make the following settings:
"Entry list" tab, Entry type "manual"

Training, Service & Support

You will find information on Training, Service & Support in the multi-language document "DC_support_99.pdf" on the data medium supplied with the documentation.

SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary on the Internet at the following address:

50305045 (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/industrialsecurity>

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SCALANCE, SINEMA, CP 343-1, CP 443-1, CP 1628

Table of contents

	Preface	3
1	Connecting SCALANCE M-800 to WAN.....	9
1.1	Procedure in principle.....	9
1.2	Setting up the SCALANCE M-800 and the network.....	11
1.3	Connecting M826 to SHDSL.....	12
1.4	Adapting IP settings	17
1.4.1	Configuration with the Primary Network Initialization (SINEC PNI)	18
1.4.2	Configuration with DCP Discovery	19
1.5	Starting Web Based Management	21
1.6	Logging in to Web Based Management	24
1.7	Specifying device information	26
1.8	Setting the time	27
1.9	Additional configuration steps with the SCALANCE M87x and SCALANCE M81x.....	29
1.9.1	Configuring access parameters for the SCALANCE M87x	29
1.9.2	Configuring access parameters for the SCALANCE M81x	32
1.9.3	Setting up the DDNS hostname.....	35
1.10	Additional steps in configuration with the SCALANCE M826 in 4-wire operation.....	37
1.10.1	Configuring SHDSL	37
1.11	Additional steps in configuration with the SCALANCE M826 in routing mode	39
1.11.1	Creating IP subnet.....	39
1.11.2	Configuring routes	40
1.12	Allow access	42
2	SCALANCE M-800 as DHCP server.....	47
2.1	Configuring dynamic IP address assignment	49
2.2	Specifying DHCP options	51
2.3	Configuring static IP address assignment	53
	Index	55

Connecting SCALANCE M-800 to WAN

1.1 Procedure in principle

This section provides an overview of how a SCALANCE M-800 with the factory settings can be integrated in a network and configured. This can be a mobile wireless network (SCALANCE M87x) or a wired network (SCALANCE M812, SCALANCE M816 or SCALANCE M826). The device is assigned an IP address. Configuration is performed using the Web Based Management (WBM).

Structure for SCALANCE M874 and SCALANCE M81x

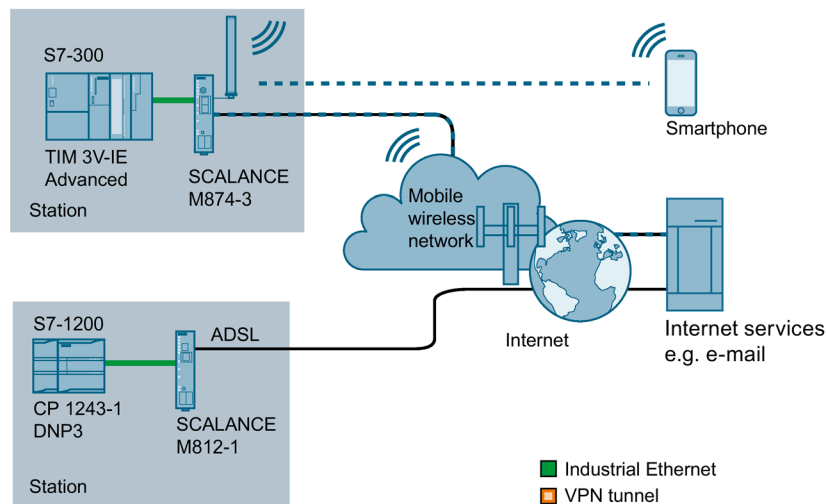


Figure 1-1 Internet access via a mobile wireless network with the SCALANCE M874-3 via ADSL with the SCALANCE M812-1

Required components

- SCALANCE M-800
- Optional if the device is not mounted directly. Standard rail with fittings
- A power supply 24 VDC or 12 VDC with cable connector and terminal block connector
- A network cable complying with the IE FC RJ-45 standard for Industrial Ethernet
- One PC for the configuration

1.1 Procedure in principle

Additionally with the SCALANCE M87x

- A suitable antenna
- A SIM card of your mobile wireless provider

The required services, for example the Internet, must be enabled.

Additionally with the SCALANCE M81x

- Activation for ADSL

Steps in configuration

The required steps in configuration depend in part on the device you are using. If the SCALANCE M826 is used in 2-wire operation, only the configuration step "Setting up SCALANCE M-800 and the network" is required. After this, the SCALANCE M826 is ready for operation immediately (out of the box).

1. Setting up SCALANCE M-800 and the network.
For the SCALANCE M826, note the additional information in the section "Connecting SCALANCE M826 with SHDSL"
2. If necessary, configure the device with Primary Network Initialization (SINEC PNI) or DCP Discovery.
3. If applicable, adapt the IP configuration of the PC.
4. Start Web Based Management.
5. Log in to Web Based Management.
6. Configure the SCALANCE M-800.
 - Specify device information
 - Set the time of day
 - Only with the devices SCALANCE M87x and SCALANCE M81x:
Configure access data
 - Only with the devices SCALANCE M87x and SCALANCE M81x:
Set up the host name
 - Only with the SCALANCE M826 in 4-wire operation:
Configure SHDSL
 - Allow access

1.2 Setting up the SCALANCE M-800 and the network

Note

Note the security instructions in the operating instructions before you commission the device.

Procedure

1. Unpack the SCALANCE M-800 and check the device for damage.
2. Only with with the SCALANCE M87x: Insert the SIM card.
3. Connect the power supply.

 WARNING
--

Use safety extra-low voltage only
--

The SCALANCE M874 is designed for operation with safety extra-low voltage. This means that only safety extra-low voltages (SELV) complying with IEC950/EN60950/VDE0805 can be connected to the power supply terminals.
--

The power supply unit for the SCALANCE M power supply must meet NEC Class 2, according to the National Electrical Code(r) (ANSI / NFPA 70).

4. Connect the device to the network. This step depends on the device and the type of network:
 - **SCALANCE M87x** (mobile wireless network): Mount the antenna.
 - **SCALANCE M81x** (ADSL): Connect the device to the DSL socket on the splitter.
 - **SCALANCE M826** (SHDSL): Wire X1 with X2, for detailed information refer to the section "Connecting SCALANCE M826 to SHDSL".
5. Connect an Ethernet port (P1, P2, P3, P4) to the PC.
6. Turn the device on. After connecting up, the fault LED (F) is lit red
7. Now, turn on the PC.

1.3 Connecting M826 to SHDSL

The SCALANCE M826 can be operated in two ways:

- **2-wire operation**

When supplied, the two SHDSL interfaces are set so that two SCALANCE M826 can be connected via a point-to-point connection. Interface X1 is configured as CO (Central Office) and interface X2 a CPE (Customer Premises Equipment).

- **4-wire operation**

Both SHDSL interfaces are put together to form a single connection with a higher transmission rate. The two interfaces X1 and X2 of one device are configured as CO and the two interfaces X1 and X2 of the other device as CPE.

When supplied the SCALANCE M826 is configured so that there is no distinction between the internal and external network. The SCALANCE M826 is a transparent bridge and connects network nodes that are in the same IP subnet.

2-wire operation with factory settings (out of the box)

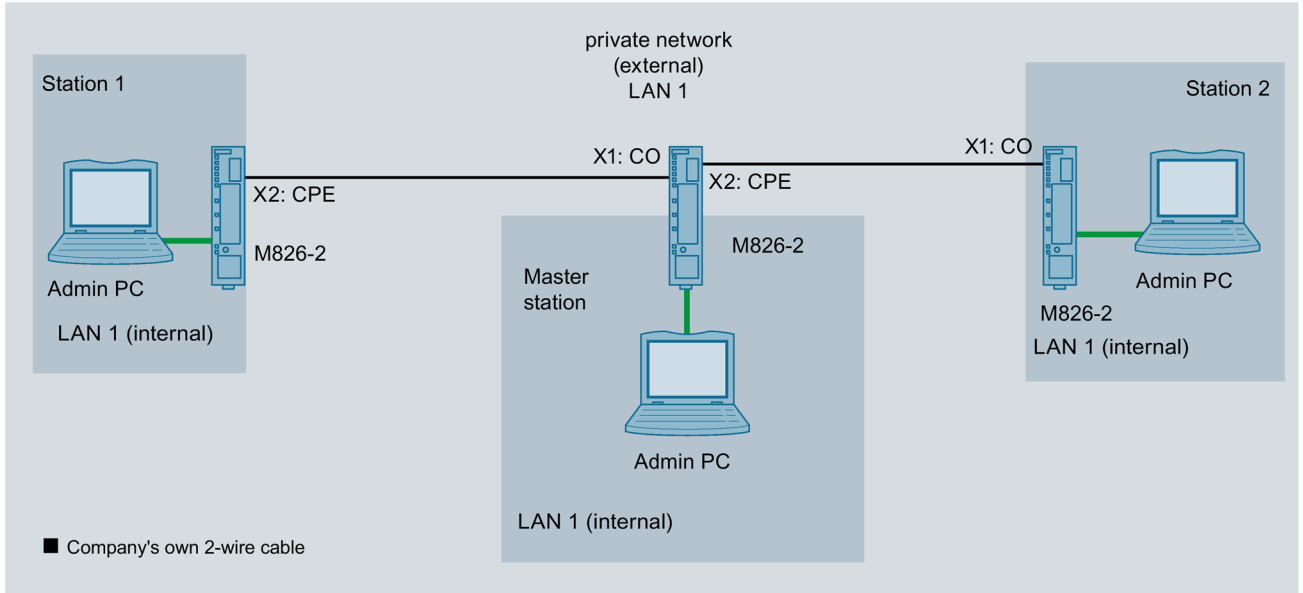


Figure 1-2 The admin PCs represent network nodes that are connected to an Ethernet interface of the relevant SCALANCE M826. The SCALANCE M826 are connected together via the company's own 2-wire cable.

Settings used

SHDSL Overview

Overview | Configuration | Connection Check

Enable PME Aggregation Function

Interface	Status	Role	Target SNR	Port Type
SHDSL 1	enabled	Central Office (CO)	Reliability (10 dB)	Switch-Port VLAN Hybrid
SHDSL 2	enabled	Customer Premises Equipment (CPE)	Reliability (10 dB)	Switch-Port VLAN Hybrid

Set Values Refresh

Figure 1-3 Factory settings for the devices of the configuration example

4-wire operation

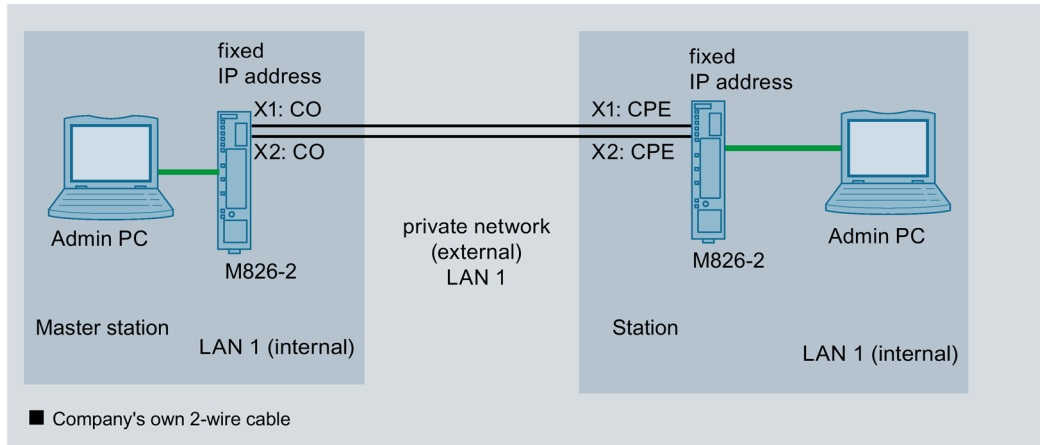


Figure 1-4 The admin PCs represent network nodes that are connected to an Ethernet interface of the relevant SCALANCE M826. The two SCALANCE M826 are connected together via two of the company's own 2-wire cables.

Settings used

		IP address
		Subnet mask
Master station	M826	192.168.100.1 255.255.255.0
	Admin PC	192.168.100.20 255.255.255.0
Station	M826	192.168.100.10 255.255.255.0
	Admin PC	192.168.100.40 255.255.255.0

In routing mode

In this example, three different IP subnets will be interconnected via the SCALANCE M826. For this connection, there must be a one SHDSL interface of a device in the role of CO and the other in the role of CPE. Since the SCALANCE M826 devices operate in routing mode, there is a division into external and internal networks. This means that the SHDSL interfaces and the Ethernet interfaces are located in different IP subnets. In this mode, the security functions (IPsec VPN, firewall, NAT/NAPT) are available.

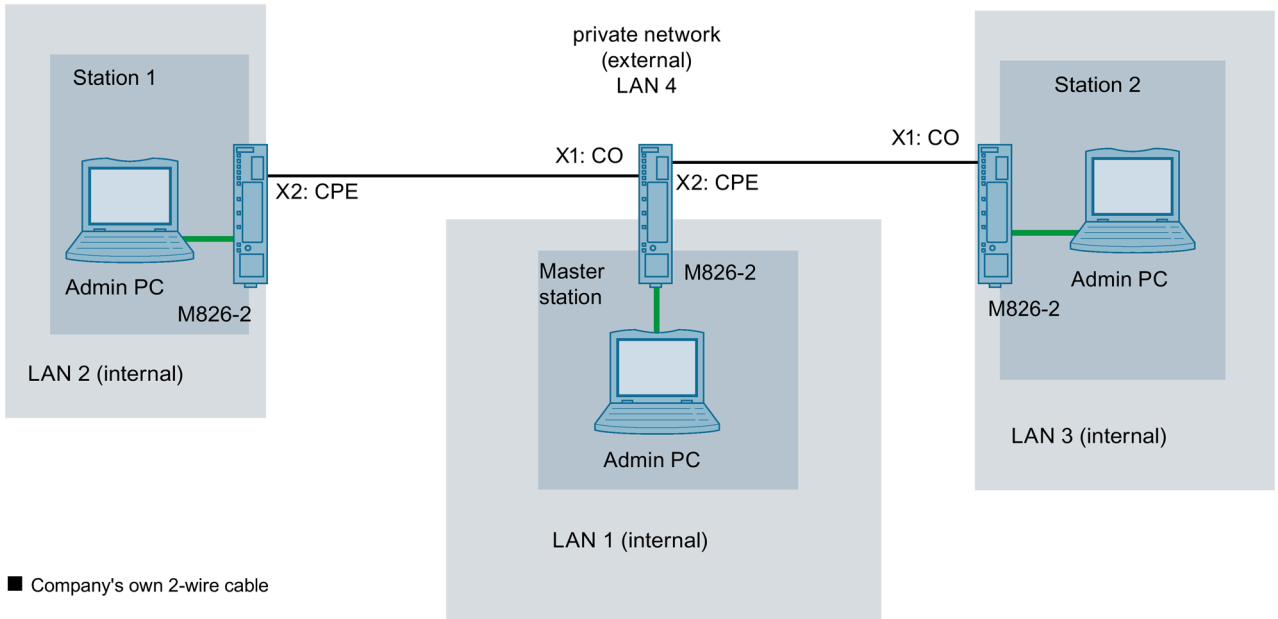


Figure 1-5 SCALANCE M826 in routing mode: The network nodes are in different IP subnets. The SHDSL interfaces are connected together via the company's own 2-wire cables.

Settings used

		Interface		IP address
Master station	M826	SHDSL (external)	Vlan 2	192.168.184.2 255.255.255.0
		Ethernet (internal)	Vlan 1	192.168.100.1 255.255.255.0
	Admin PC	Ethernet (internal)		192.168.100.20 255.255.255.0
Station 1	M826	SHDSL (external)	Vlan 2	192.168.184.22 255.255.255.0
		Ethernet (internal)	Vlan 1	192.168.11.2 255.255.255.0
	Admin PC	Ethernet (internal)		192.168.11.40 255.255.255.0

1.3 Connecting M826 to SHDSL

		Interface		IP address
Station 2	M826	SHDSL (external)	Vlan 2	192.168.184.42 255.255.255.0
		Ethernet (internal)	Vlan 1	192.168.50.2 255.255.255.0
	Admin PC	Ethernet (internal)		192.168.50.40 255.255.255.0

1.4 Adapting IP settings

Introduction

To be able to access a SCALANCE M-800 with the Web Based Management, the device must have an IP address.

You have the following options for assigning an IP address to devices with factory settings for the first time:

- Primary Network Initialization (SINEC PNI)
- DCP Discovery (as of firmware version V4.3)

Access via DCP is write-protected as soon as you enter the password of the factory-set user "admin". An IP address can be read, but can no longer be changed.

SCALANCE M826

The SCALANCE M826 is supplied without a preset IP address, because for this device there are applications that require no further configuration (out of the box). In these cases, no access to the Web Based Management is necessary and therefore no IP address either. The device will, however, attempt to obtain an IP address from a DHCP server if it is available in the network. In all other cases, the device must first be assigned an IP address.

SCALANCE M87x and SCALANCE M81x

The devices SCALANCE M87x and SCALANCE M81x are supplied with the following factory settings:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

If you enter the IP address "192.168.1.1" in the address box of a Web browser on a connected PC (in the examples called "admin PC"), you come directly to the WBM of the device. However, a change to the factory settings may be necessary due to address areas already configured in the existing network.

1.4.1 Configuration with the Primary Network Initialization (SINEC PNI)

Introduction

The following section describes the procedure for using the SINEC PNI.

Requirement

- Device with factory settings

Procedure

1. Start SINEC PNI.
If several network cards are installed in the PC, select the network adapter connected to SCALANCE M-800 in the "Settings" tab.
2. Click on the "Device List" tab in the navigation bar to switch to the "Device list" page.
3. Click the "Start network scan" button to scan the network for existing devices.
The scan settings configured on the "Settings" page are used. Adapt the settings according to your needs if necessary. After the scan, all devices that can be configured with the SINEC PNI are listed.
4. Select the checkbox in front of the device or multiple SCALANCE M-800 devices that you want to configure and click the "Configure device" button.
The "Device configuration" dialog window is displayed.
5. Enter the desired IP address and the subnet mask of the selected device in the "IP Configuration" tab. If you have selected multiple devices, in the "Start IP address" field enter the first IP address of an IP address range, which is assigned to the selected devices during loading.
Alternatively, you can select the DHCP option to have the IP address configuration of the device performed by a DHCP server.
6. Enter further desired parameters in the tabs "System", "PROFINET", "Device Credentials" and "PROFIBUS".
7. Click the "Load" button to transfer the configuration to the device.

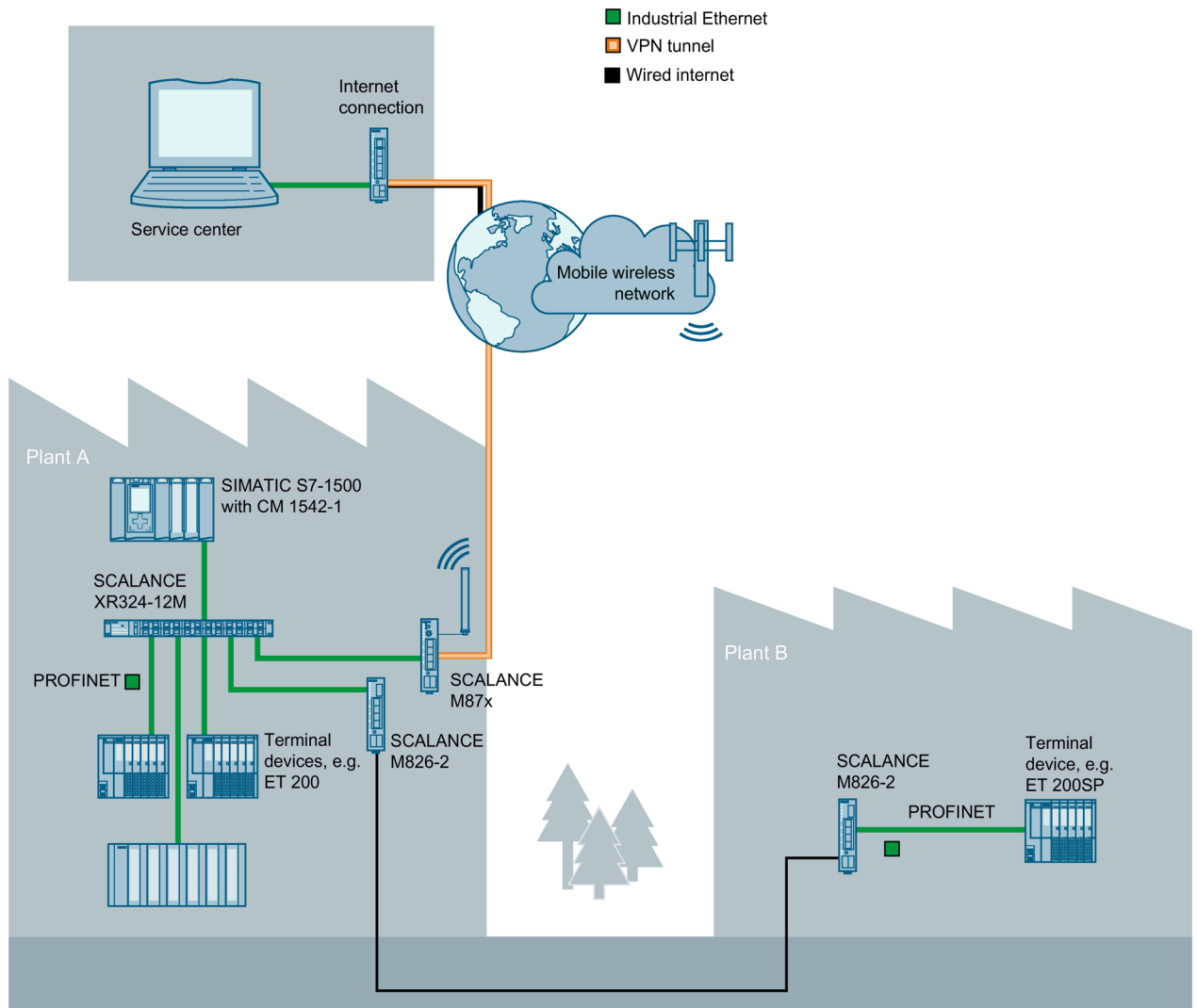
1.4.2 Configuration with DCP Discovery

Introduction

The network parameters of the SCALANCE M826-2 in the plant network are to be updated in this example configuration.

To do so, the PC in the service center establishes a WAN connection to a SCALANCE M87x, and the service technician accesses its WBM. On the WBM page "DCP Discovery and Set via DCP", the service technician can see all nodes that support the DCP protocol and can be accessed over the interface of the device, e.g. SCALANCE M826-2.

For the SCALANCE M826-2, the device name, the IP address, the subnet mask and the gateway address are updated. The devices can be identified on site by flashing of the respective device.



Requirement

- Firmware version V4.3 or later is installed on the devices.
- Device with factory settings

Procedure

1. Click "System > DCP Discovery" in the navigation area.
2. Click "Discover" button to start the search. After the search, all devices are listed that can be reached via the interface.

Discovery and Set via DCP

Interface:

Port	MAC Address	Device Type	Device Name	IP Address	Mask Address	Gateway Address	Name Status	IP Status	Timeout(s)	Blink
P1	00-1b-1b-03-b7-16	SCALANCE X-200	x-200	192.168.16.102	255.255.0.0	192.168.16.102	Discovered	Discovered/IP	5	<input type="button" value="Blink"/>
P1	00-1b-1b-38-5c-90	SCALANCE W-700	ap-w780	192.168.16.177	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	<input type="button" value="Blink"/>
P1	00-1b-1b-40-91-23	SCALANCE X-500	xr-500-1	192.168.16.150	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	<input type="button" value="Blink"/>
P1	00-1b-1b-9a-31-94	SCALANCE M-800		0.0.0.0	0.0.0.0	0.0.0.0	Discovered	Discovered/IP	5	<input type="button" value="Blink"/>
P1	00-1b-1b-a5-5d-98	SCALANCE W-700	cl-w770	192.168.16.107	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	<input type="button" value="Blink"/>
P1	00-1b-1b-b6-32-79	SCALANCE S-600	s615	192.168.16.42	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	<input type="button" value="Blink"/>
P1	00-1b-1b-c8-70-3a	SCALANCE X-300		192.168.16.33	255.255.255.0	192.168.16.33	Discovered	Discovered/IP	5	<input type="button" value="Blink"/>
P1	00-1b-1b-cd-3b-00	SCALANCE X-400		192.168.16.144	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	<input type="button" value="Blink"/>
P1	00-5e-1d-d2-76-00	SCALANCE X-500	xr-500-2	192.168.16.155	255.255.255.0	0.0.0.0	Discovered	Discovered/IP	5	<input type="button" value="Blink"/>
P1	08-00-06-70-29-d7	SCALANCE XB-200		192.168.16.200	255.255.255.0	192.168.16.200	Discovered	Discovered/IP	5	<input type="button" value="Blink"/>

1 - 10 of 14 entries [Show all](#) 1

With the aid of the table you can check the configuration of the devices. The SCALANCE M826 is supplied without a preset IP address, so it currently has the IP address 0.0.0.0.

3. Enter the required values in the "IP Address" and "Subnet Mask" boxes. The assigned IP address must match your network and should be unique within the network.
4. Click on "Set Values". The status of the IP address changes from "Discovered" to "Configured".

1.5 Starting Web Based Management

Depending on the device and the example shown, the admin PC is assigned the following IP address:

- **SCALANCE M87x and SCALANCE M81x**

	IP address Subnet mask
Admin PC	192.168.1.20 255.255.255.0

- **SCALANCE M826**

	IP address Subnet mask
Admin PC 1	192.168.1.20 255.255.255.0
Admin PC 2	192.168.1.40 255.255.255.0

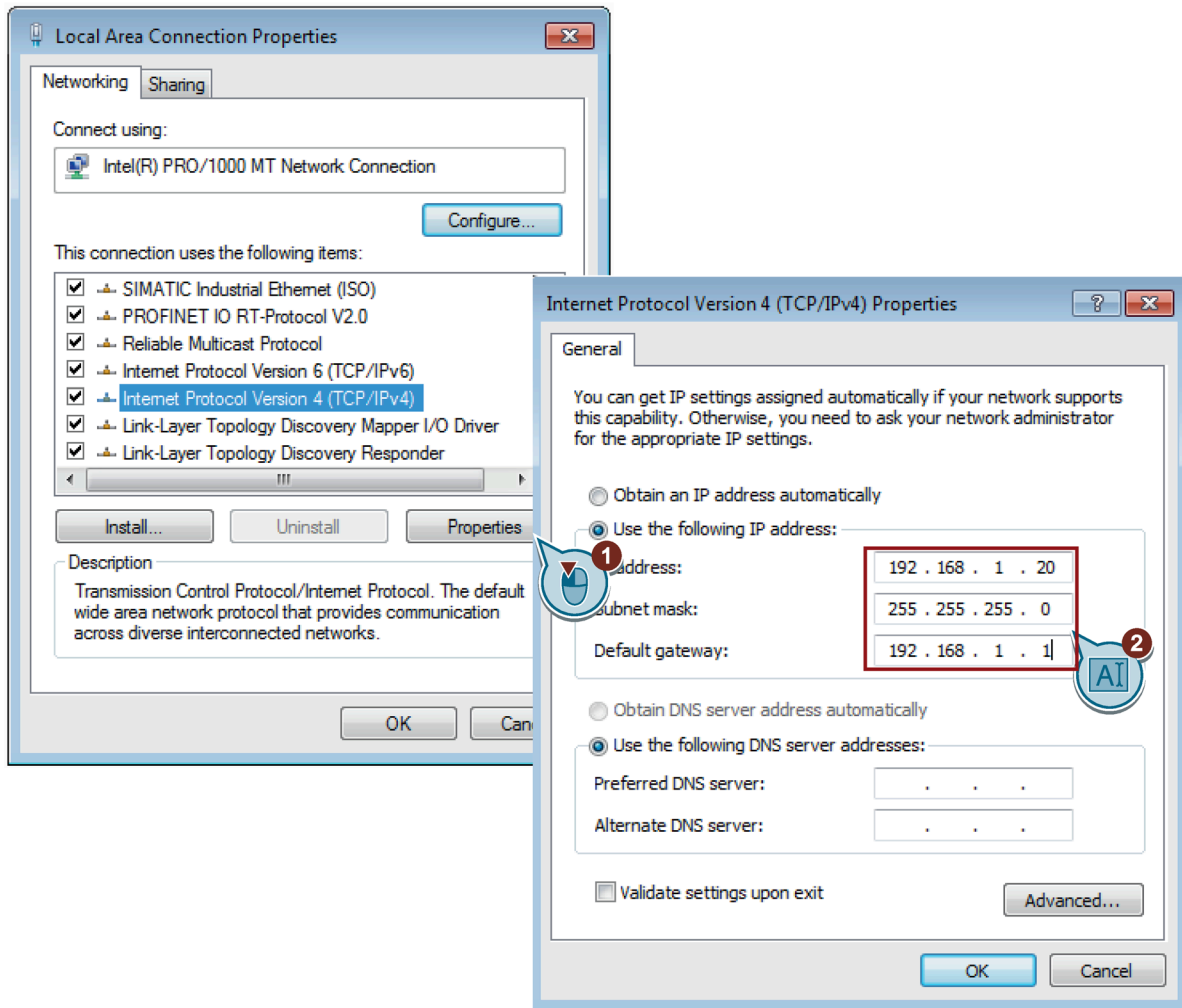
Procedure

1. On the Admin PC, open the Control Panel with the menu command "Start" > "Control Panel".
2. Click "Network and Sharing Center" and select the "Change adapter settings" option in the navigation menu on the left.
3. Right-click on the "LAN Connection" symbol and select the "Properties" menu command.
4. In the "Local Area Connection Properties" dialog, enable the "Internet Protocol Version 4 (TCP/IPv4)" check box.

- 5. Enter the values assigned to the admin PC from the table in the relevant boxes.

Note

The IP address used in the following figure for the standard gateway 192.168.1.1 must be adapted if the factory setting is not used for the IP address of the SCALANCE M-800.



- 6. Confirm the dialogs with "OK" and close the Control Panel.

7. Enter the IP address "192.168.1.1" in the address box of the Internet browser.

Access via HTTPS is enabled as default. If you access the device via HTTP, the address is automatically redirected to HTTPS.

A message relating to the security certificate appears. Acknowledge this message and continue loading the page.

Note**Information on the security certificate**

Because the device can only be administered using encrypted access, it is delivered with a self-signed certificate. If certificates with signatures that the operating system does not know are used, a security message is displayed. You can display the certificate.

8. If there is a problem-free connection to the device, the logon page of Web Based Management (WBM) is displayed.

English ▾ Go

SIEMENS

Name

Password

[Login](#)

LOGIN

Name:

Password:

[Login](#)

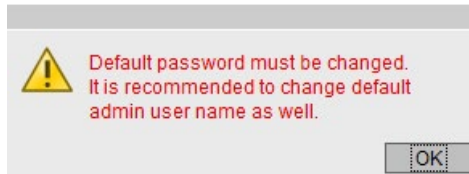
[Switch to insecure HTTP](#)

For information about browser compatibility please refer to the manual

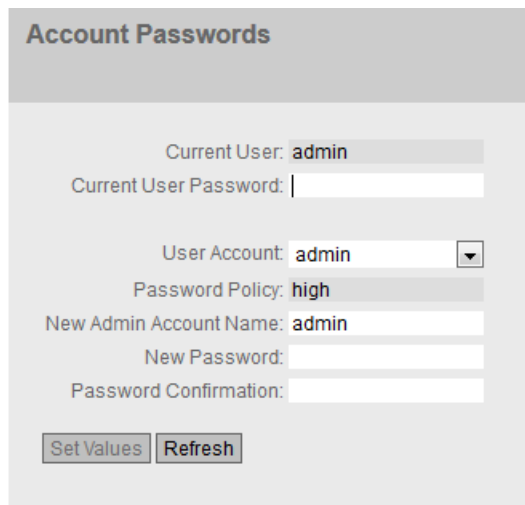
1.6 Logging in to Web Based Management

Procedure

1. Log in with the user name "admin" and the password "admin". You will be prompted to change the password. You can also rename the user preset in the factory "admin" once. Afterwards, renaming "admin" is no longer possible.

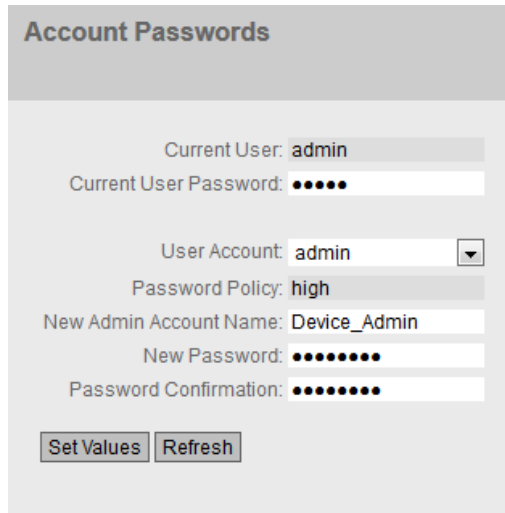


2. Confirm the dialog. The "Account Passwords" WBM page is opened automatically.

The "Account Passwords" configuration page. It has a title bar "Account Passwords". Below it, there are several fields: "Current User:" with the value "admin" in a dropdown; "Current User Password:" with an empty text input; "User Account:" with a dropdown menu showing "admin"; "Password Policy:" with the value "high" in a dropdown; "New Admin Account Name:" with the value "admin" in a text input; "New Password:" with an empty text input; and "Password Confirmation:" with an empty text input. At the bottom, there are two buttons: "Set Values" and "Refresh".

3. Enter the default password "admin" in "Current User Password".
4. Change the user name for "New Admin Account Name".
5. For "New Password", enter the new password. The new password must be at least 8 characters long and contain upper case letters, lower case letters, numbers and special characters.

- Repeat the new password in "Password Confirmation" as confirmation. The entries must match.



Account Passwords

Current User: admin

Current User Password: ●●●●

User Account: admin

Password Policy: high

New Admin Account Name: Device_Admin

New Password: ●●●●●●

Password Confirmation: ●●●●●●

Set Values Refresh

- Click the "Set Values" button.

Result

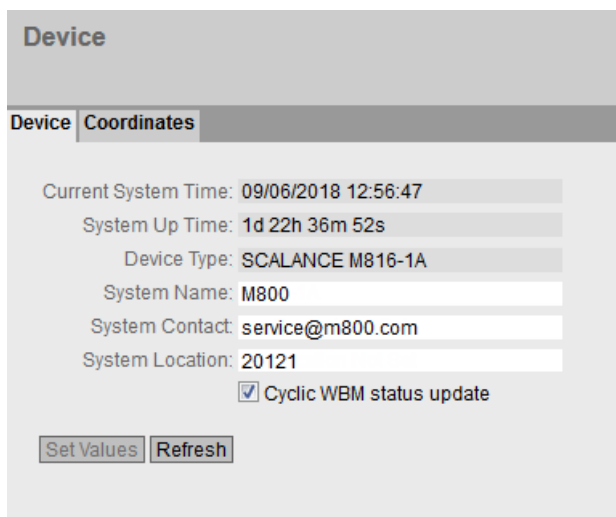
The changes take immediate effect and access via DCP is write-protected.
The Basic Wizard starts to support you when configuring the device parameters.

1.7 Specifying device information

To allow better identification of the SCALANCE M-800, specify general device information.

Procedure

1. In the navigation area click on "System > General" and in the content area on the "Device" tab.
2. In "System Name", enter a name for the device.
3. Enter the contact person responsible for the device in "System Contact".
4. Enter the identifier for the location at which the device is installed in "System Location", for example the room number.



The screenshot shows a configuration page titled "Device" with two tabs: "Device" and "Coordinates". The "Device" tab is active. The page displays the following information:

- Current System Time: 09/06/2018 12:56:47
- System Up Time: 1d 22h 36m 52s
- Device Type: SCALANCE M816-1A
- System Name: M800
- System Contact: service@m800.com
- System Location: 20121
- Cyclic WBM status update

At the bottom of the form, there are two buttons: "Set Values" and "Refresh".

5. Click the "Set Values" button.

Result

The general device information for the SCALANCE M-800 has been specified.

1.8 Setting the time

The date and time are kept on the SCALANCE M-800 to check the validity (time) of certificates and for the time stamps of log entries. You can set the system time yourself manually or have it synchronized automatically with a time server. There are a number of time servers on the Internet that can be used to obtain the current time precisely. For this example, the time server is configured using NTP.

Note

Manual time setting - reaction after interrupting the power supply

Note that the time is reset to the factory setting if the power supply is interrupted. On return of the power, you need to set the system time again. As result, certificates can lose their validity.

Synchronization using a time server

Synchronization of the system time using a public time server creates additional data traffic on the connection. This may result in additional costs, depending on your subscriber contract.

Requirement

- The NTP server is reachable.
- The IP address of the NTP server is known.
For this example, a time server (e.g. 192.53.103.108) of the Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig is used (Federal Institute of Physical and Technical Affairs - metrology institute). As an alternative the Fully Qualified Domain Name (FQDN) can be specified, for example "pool.ntp.org".

1.8 Setting the time

Procedure

1. In the navigation area click on "System > System Time" and in the content area on the "NTP Client" tab.

Network Time Protocol (NTP) Client

Manual Setting | **Sntp Client** | NTP Client | SIMATIC Time Client | NTP Server

NTP Client
 Secure NTP Client only

Current System Time: 02/23/2017 09:21:57
 Last Synchronization Time: 02/23/2017 08:06:57
 Last Synchronization Mechanism: Manual
 Time Zone: +00:00

NTP Server Index: 1

Select	NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval	Key ID	Hash Algorithm	Key
<input type="checkbox"/>	1	0.0.0.0	123	64	1	DES	

1 entry.

Create Delete Set Values Refresh

2. In "Time zone", enter the local time difference to world time (UTC). For Central European Summer time (CEST) +02:00.
3. Click "Create". A new entry is created in the table.
4. In "NTP Server Address", enter the IP address 192.53.103.108.
5. If necessary, change the port in "NTP Server Port". As default, 123 is set.
6. In "Poll Interval", enter the interval for synchronization. As default, 64 is set.
7. Enable "NTP Client".
8. Click on "Set Values".

Result

System time using NTP is set. Click "Refresh" to refresh the WBM page.

Network Time Protocol (NTP) Client

Manual Setting | **Sntp Client** | NTP Client | SIMATIC Time Client | NTP Server

NTP Client
 Secure NTP Client only

Current System Time: 02/23/2017 09:12:24
 Last Synchronization Time: 02/23/2017 08:06:57
 Last Synchronization Mechanism: Manual
 Time Zone: +00:00

NTP Server Index: 1

Select	NTP Server Index	NTP Server Address	NTP Server Port	Poll Interval	Key ID	Hash Algorithm	Key
<input type="checkbox"/>	1	192.53.103.108	123	64	1	DES	

1 entry.

Create Delete Set Values Refresh

1.9 Additional configuration steps with the SCALANCE M87x and SCALANCE M81x

1.9.1 Configuring access parameters for the SCALANCE M87x

Requirement

- The services are enabled, e.g. Internet.
- The following data is available:
 - PIN number
 - APN
 - User name and password for the APN

Enter the PIN number

1. Click on "Interfaces > Mobile" in the navigation area and on the "SIM" tab in the content area.
2. In "PIN", enter the PIN number.
3. Enable the mobile wireless interface.
4. Click on "Set Values".

Configure APN

1. Click on the "Operator" tab in the content area.
 2. Specify the access data for the APN.
 - If your mobile wireless provider is included in the table, no further configuration is necessary.
- or
- In "Country List", select the country in which the device will be used.
 - In "Provider List", select the appropriate mobile wireless provider. If a mobile wireless provider is listed more than once for a country, select the entry with the PLMNID that matches the SIM.
- or
- If your mobile wireless provider is not included in the table and not in the list of providers, enable the entry "Manual". When the "Manual" entry is enabled, all other entries are automatically ignored.
 - Complete the boxes PLMNID, Operator Name, APN, User Name (optional), Password (optional) and Password Confirmation (optional).
 - To adopt the entry click on "Create" and "Set Values".

Operator

SIM |
 Operator |
 Connection Check

Country List: - ▼

Provider List: - ▼

PLMNID:

Operator Name:

APN:

User Name:

Password:

Password Confirmation:

Select	PLMNID▼	Operator Name	APN	User Name	Password	Password Confirmation	Enabled
<input type="checkbox"/>	Manual						<input type="checkbox"/>
<input type="checkbox"/>	26207	O2	internet	guest	●●●●●●	●●●●●●	<input checked="" type="checkbox"/>
<input type="checkbox"/>	26203	Eplus	internet.eplus.de	guest	●●●●●●	●●●●●●	<input checked="" type="checkbox"/>
<input type="checkbox"/>	26202	Vodafone	web.vodafone.de	guest	●●●●●●	●●●●●●	<input checked="" type="checkbox"/>
<input type="checkbox"/>	26201	T-Mobile	internet.t-mobile	guest	●●●●●●	●●●●●●	<input checked="" type="checkbox"/>

5 entries.

Create |
 Delete |
 Set Values |
 Refresh

Result

The PIN number and the APN are configured. The M87x4 connects to the mobile wireless network after approximately 30 seconds. You can check whether or not the connection is established in "Information > Mobile > Overview".

There the name of your mobile wireless provider should appear in "Provider". For a functioning connection, the signal strength should be higher than 104 dBm.

Note

This page provides the option of automatic updating. Click on the symbol with the two arrows in the upper display area to enable this function.

The screenshot shows the 'Mobile Overview' page with the 'Signal Recorder' tab selected. The page displays various mobile network parameters. A 'Refresh' button is located at the bottom left of the data area.

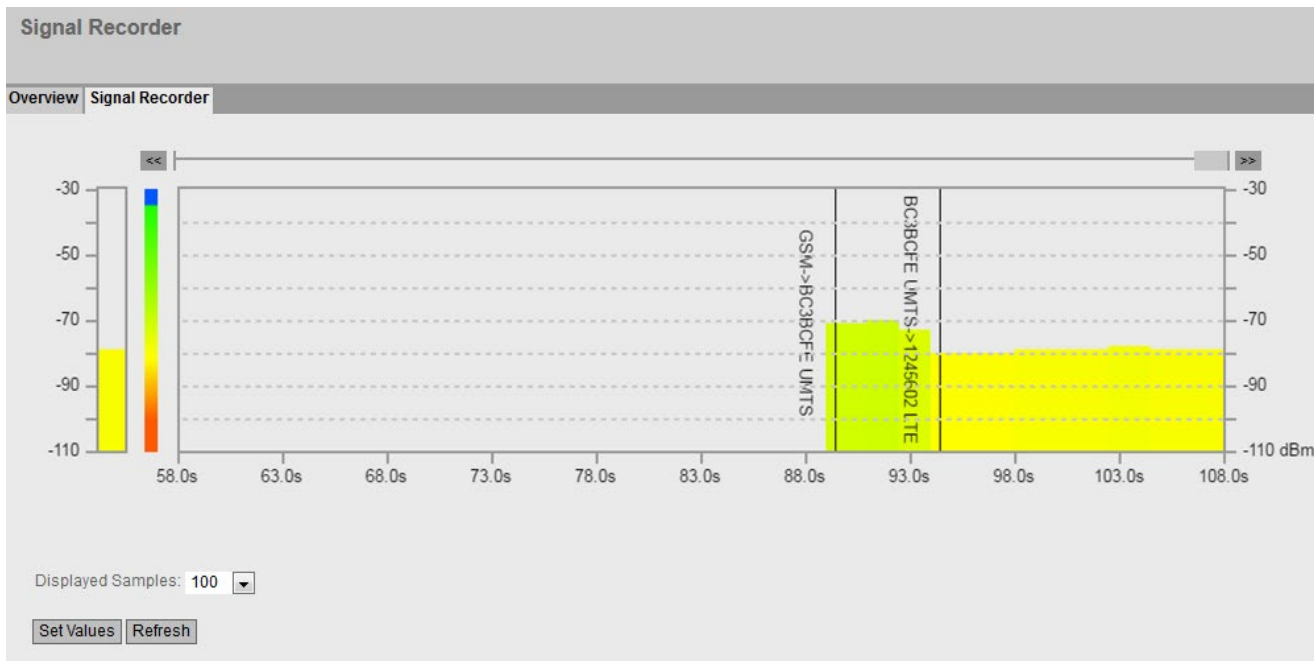
Overview	Signal Recorder
IMEI:	
SIM Status:	present
PIN Status:	PIN valid
IMSI:	
Phone Number:	
Connection Status:	connection-established
Packet Switch Status:	GPRS/EGPRS not available in currently used cell
Cell ID:	
LAC:	
Signal Strength:	-102 dBm, 5 CSQ
Mobile Chip Temperature:	41°C
Provider:	
APN:	
External IP Address:	
DNS Server(s):	192.168.1000.20

Refresh

The "Signal Recorder" page shows the signal strength for the cell into which the device is currently booked. Using the graphical display, you can check the orientation of the mobile radio antenna and correct it, if necessary.

1.9 Additional configuration steps with the SCALANCE M87x and SCALANCE M81x

When there is a change in the cell, this is displayed by a vertical black line. The cell IDs (old > new) are displayed in the line. When the mobile network changes as well, this is also indicated. The display is updated automatically in a 500 ms cycle.



1.9.2 Configuring access parameters for the SCALANCE M81x

Requirement

- The services are enabled, e.g. Internet.
- The following access data is known from your DSL provider:
 - User name and password for ADSL access
 - DSL parameter

Configuring ADSL

1. Click "Interfaces" > "DSL" in the navigation area

The screenshot shows the "DSL Configuration" web interface. It features a header with the title "DSL Configuration". Below the header, there are several configuration options and input fields:

- Enable DSL Interface
- Enable PPPoE Passthrough
- Account: [text input field]
- Password: [text input field]
- VCI: 32 [text input field]
- VPI: 1 [text input field]
- Encapsulation: ilc [dropdown menu]
- Protocol: PPPoE [dropdown menu]
- Noise Margin Delta DS: +0.0 [text input field]
- Enable Vlan ID
- Vlan ID: 0 [text input field]
- Forced Disconnect
- Time for Forced Disconnect: 04:00 [text input field]

At the bottom of the form, there are two buttons: "Set Values" and "Refresh".

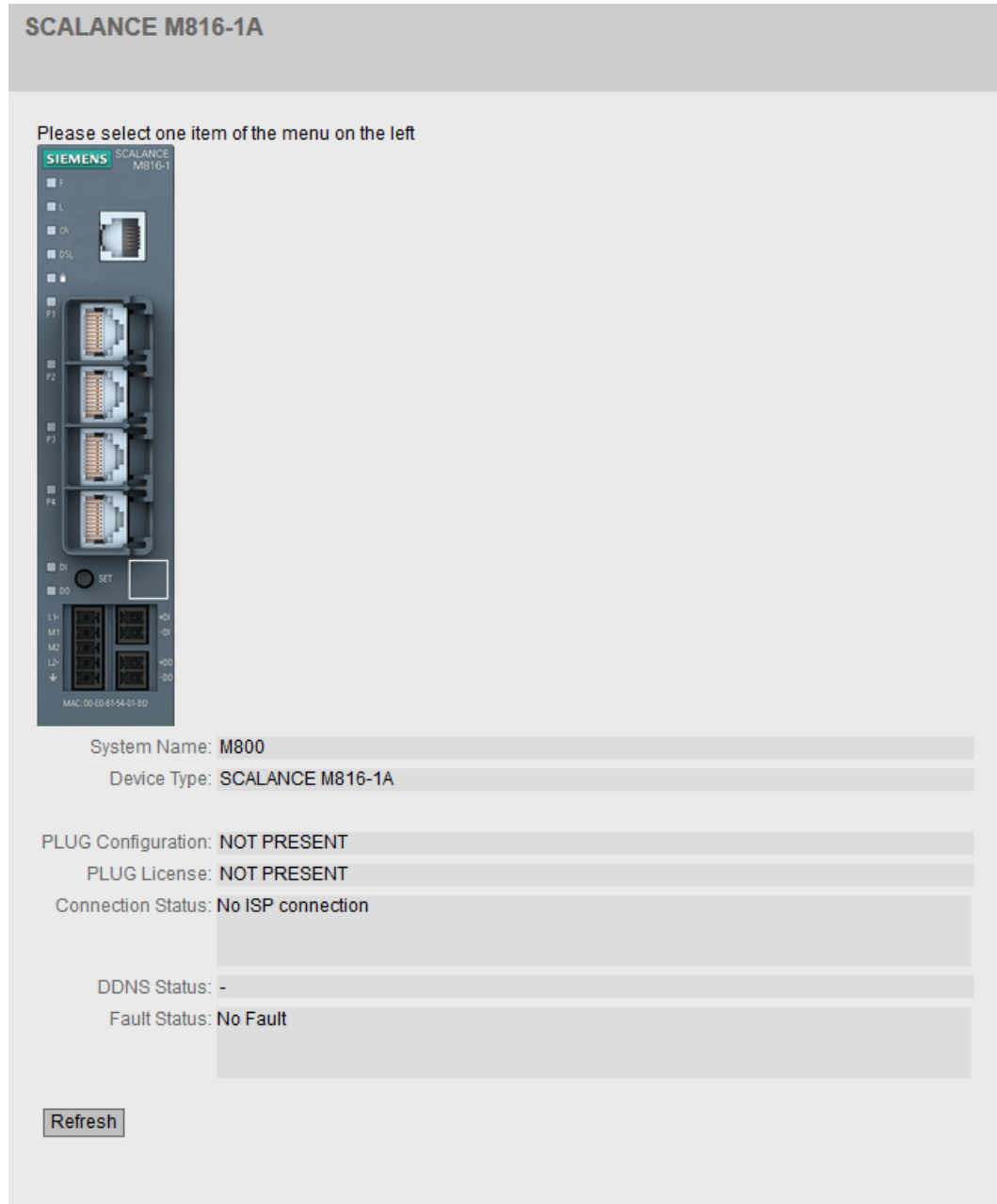
2. Enable the DSL interface.
3. Disable PPPoE passthrough to set up the access data for the SCALANCE M81x. The connected devices can use this DSL connection.

If "Enable PPPoE Passthrough" is selected, the access data cannot be configured. In this case the SCALANCE M81x is used as a modem. Each individual connected device sends its access data to the SCALANCE M81x and establishes its own Internet connection.

4. Enter the user name and the password for the ADSL access.
5. Enter the settings for VCI / VPI. You will receive the settings from your DSL provider.
6. In "Encapsulation" select the required protocol.
7. Click on "Set Values".

Result

The DSL connection is set up. The device connects to the Internet after approximately 30 seconds. You can check whether the connection is established in "Information > Start Page".



You will find more detailed information on the connection in "Information > DSL".

DSL Overview

DSL Overview | DSL Data Rate | DSL Streams

Modem Status: showtime-sync
 Latency Type: unknown
 External IP Address: 192.168.50.1
 DNS Server(s): 192.168.100.20

Refresh

1.9.3 Setting up the DDNS hostname

DDNS stands for "dynamic domain name system". If you log the SCALANCE M-800 on to a DDNS service, the device can be reached from the external network under a hostname, e.g. "example.no-ip.com".

The DNS server of the DDNS service manages the assignment of IP address to hostname. The client informs the DNS server of its currently assigned IP address. The DNS name server registers the current hostname - IP address assignment and passes this on to other domain name servers in the Internet. This means that the SCALANCE M-800 can always be reached using its hostname.

Requirement

- User name and password that give you the right to use the DDNS service
- Registered hostname, e.g. example.no-ip.com

Procedure

1. Click on "System > DNS" in the navigation area and on the "DDNS Client" tab in the content area.
2. In "Host", enter the hostname that you have agreed with your DDNS provider for the device, e.g. example.no-ip.com.
3. For "User name", enter the user data and for "Password / Password Confirmation" the password that allows you to use the DDNS service. Your DDNS provider will give you this information.

4. Select the appropriate check box in the "enabled" column for one of the two services "No-IP" or "DynDNS".

DDNS Client

DNS Client | DNS Proxy | **DDNS Client**

Service	Enabled	Host	User name	Password	Password confirmation
No-IP	<input type="checkbox"/>	example.no-ip.com	username	*****	*****
DynDNS	<input type="checkbox"/>				

5. Click on "Set Values".

Result

The DDNS client is activated. The DDNS client on the SCALANCE M-800 synchronizes the assigned IP address with the hostname registered in the DDNS service.

1.10 Additional steps in configuration with the SCALANCE M826 in 4-wire operation

1.10.1 Configuring SHDSL

Procedure

1. In the navigation area, click on "Interfaces > SHDSL > Configuration".
2. For "Port-Type" leave "Switch-Port VLAN Hybrid" enabled.
3. Specify the role of the interfaces. The two interfaces need to have the same role on both devices.

M826 in the master station	X1	Central Office (CO)
	X2	Central Office (CO)
M826 in the station	X1	Customer Premises Equipment (CPE)
	X2	Customer Premises Equipment (CPE)

4. For "Predefined Profile", select "Reliability". The following parameters are set automatically.
5. Click on "Set Values".

SHDSL Configuration

Overview
Configuration
Connection Check

Interface: SHDSL 2

Status: enabled

Port Type: Switch-Port VLAN Hybrid

Role: Central Office (CO)

Predefined Profile: -

Extended Mode: Disabled

PAM: PAM-16 + PAM-32

Lineprobing: Enabled

SNR Model: Worst Case

Target SNR: Reliability (10 dB)

Min. Link Data Rate [kbps]: 192

Max. Link Data Rate [kbps]: 5696

Power Regulation: Normal

PBO Value: 0

1.10 Additional steps in configuration with the SCALANCE M826 in 4-wire operation

- 6. In the navigation area click "Interfaces" > "SHDSL" > "Overview".
- 7. Enable the PME aggregation function.

When enabled, the SHDSL interfaces or the 2-wire cables are put together to form a single connection with a higher transmission rate.

- 8. Click on "Set Values".

SHDSL Overview

Overview | Configuration | Connection Check

Enable PME Aggregation Function

Interface	Status	Role	Target SNR	Port Type
SHDSL 1	enabled	Central Office (CO)	Reliability (10 dB)	Switch-Port VLAN Hybrid
SHDSL 2	enabled	Central Office (CO)	Reliability (10 dB)	Switch-Port VLAN Hybrid

Set Values Refresh

Result

The SHDSL connection is set up. The devices negotiate the connection parameters. This means that the devices use the transmission rate at which the data can be sent and received reliably.

1.11 Additional steps in configuration with the SCALANCE M826 in routing mode

1.11.1 Creating IP subnet

In routing mode, the interfaces are handled differently.

- Ethernet interface: Connection of the internal IP subnet (vlan 1)
- SHDSL interface: Connection of the external IP subnet (vlan 2)

The Ethernet interface or the internal IP subnet has already been configured with the SINEC PNI. For this configuration example, only the IP subnet for the SHDSL interface or for the external IP subnet needs to be configured. The same steps need to be taken on all devices.

Procedure

1. Click on "Layer 3 > Subnets" in the navigation area and in the "Configuration" tab in the content area.
2. For "Interface (Name)" select the entry "vlan2".
3. For "Interface Name" you can enter a name.
4. Enter the value assigned to the M826 from the "Settings used (Page 12)" table.
5. Click on "Set Values".

Connected Subnets Configuration

Overview | Configuration

Interface (Name): vlan2 (external) ▼

Interface Name: external

MAC Address: 00-1b-1b-9a-32-2e

DHCP

IP Address: 192.168.184.42

Subnet Mask: 255.255.255.0

Broadcast IP Address: 192.168.184.255

Address Type: Primary

TIA Interface

Set Values Refresh

Result

The IP subnets have been created. The IP subnets are displayed in the "Overview" tab.

Connected Subnets Overview

Overview | Configuration

Interface: VLAN1

Select	Interface	TIA Interface	Interface Name	MAC Address	IP Address	Subnet Mask	Address Type	IP Assgn. Method	Address Collision Detection Status
<input checked="" type="checkbox"/>	vlan1	yes	INT	00-1b-1b-9a-32-2e	192.168.1.48	255.255.255.0	Primary	Static	Not supported
<input type="checkbox"/>	vlan2	-	external	00-1b-1b-9a-32-2e	192.168.184.42	255.255.255.0	Primary	Static	Not supported

2 entries.

Create Delete Refresh

1.11.2 Configuring routes

The master station and the stations are in different IP subnets. To allow the master station to communicate with the stations, the appropriate routes need to be created on the M826.

M826 in the master station: Configuring routes

- Click "Layer 3 > Static Routes" in the navigation area.
- Configure the routes with the following settings:
 - Route to station 1

Destination Network	192.168.11.0
Subnet Mask	255.255.255.0
Gateway	192.168.184.22 external IP address of the M826 in station 1
Administrative Distance	-1

- Route to station 2

Destination Network	192.168.50.0
Subnet Mask	255.255.255.0
Gateway	192.168.184.42 external IP address of the M826 in station 2
Administrative Distance	-1

1.11 Additional steps in configuration with the SCALANCE M826 in routing mode

3. When you have entered the values, click "Create".
4. To update the display, click "Refresh".

Static Routes

Destination Network:

Subnet Mask:

Gateway:

Interface:

Administrative Distance:

Select	Destination Network	Subnet Mask	Gateway	Interface	Administrative Distance	Status
<input type="checkbox"/>	192.168.11.0	255.255.255.0	192.168.184.22	vlan2	not used	inactive
<input type="checkbox"/>	192.168.50.0	255.255.255.0	192.168.184.42	vlan2	not used	inactive

2 entries.

M826 in the stations: Configuring routes

1. Click "Layer 3 > Static Routes" in the navigation area.
2. Configure the route to the master station with the following settings:

Destination Network	192.168.100.0
Subnet Mask	255.255.255.0
Gateway	192.168.184.2 external IP address of the M826 in the master station
Administrative Distance	-1

3. When you have entered the values, click "Create".
4. To update the display, click "Refresh".

Result

The routes have been created. The SCALANCE M826 in the master station can communicate with the stations.

Using the ping function, the communications connection can be tested. For example, can the Admin PC in station 1 be reached by the Admin PC in the master station?

1.12 Allow access

The firewall is enabled as default. The following access is not allowed:

- Access from internal to external.
- Access from external to internal.
- Data exchange between different internal VLANs.
- Data exchange with the device from different zones.

You have the following options for allowing access:

- Allow globally

The predefined firewall rules specify which of the zones (VLAN1, VLAN2, ... or PPP) may access which services of the SCALANCE M-800. With predefined rules it is possible to permit data exchange between the zones (internal VLAN1 to external PPP0). The firewall rule for the opposite direction is permitted by stateful packet inspection.

- Allow certain services

Here, you define firewall rules that allow individual services for a single node or all services for the node for access to the station or network.

In this example, configure the firewall rules that only allow the device with IP address 192.168.100.10 access to the entire Internet. For the access, the services HTTP (TCP port 80) and DNS (UDP port 53) are required.

Predefined rules

1. Click on "Security > Firewall" in the navigation area and on the "Predefined IPv4 rules" tab in the content area.
2. Click on "Set Values".

Predefined IPv4

General | **Predefined IPv4** | IP Services | ICMP Services | IP Protocols | IP Rules

Allow device services:

Interface	All	HTTP	HTTPS	DNS	SNMP	Telnet	IPsec VPN	SSH	DHCP	Ping	System Time	Cloud Connector
vlan1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Allow Internet access for a certain device and a certain service (HTTP)

Create HTTP and DNS services

1. Click on "Security > Firewall" in the navigation area and on the "IP Services" tab in the content area.
2. Under "Service Name", enter e.g. "HTTP" and click "Create". A new entry is created in the table.
3. Configure HTTP with the following settings:

Transport	TCP
Destination Port (Range)	80 (standard port)

4. Click on "Set Values".
5. A new entry is created in the table.
6. Under "Service Name", enter e.g. "DNS" and click "Create". A new entry is created in the table.
7. Configure DNS with the following settings:

Transport	UDP
Destination Port (Range)	53 (standard port)

8. Click on "Set Values".

Internet Protocol (IP) Services

General | Predefined IPv4 | IP Services | ICMP Services | IP Protocols | IP Rules

Service Name:

Select	Service Name	Transport	Source Port (Range)	Destination Port (Range)
<input type="checkbox"/>	DNS	UDP	* <input type="text"/>	53
<input type="checkbox"/>	HTTP	TCP	* <input type="text"/>	80

2 entries.

Create Delete Set Values Refresh

1.12 Allow access

Only allow the IP service for a specific device

1. Click on "Security > Firewall" in the navigation area and on the "IP Rules" tab in the content area.
2. Click "Create". A new entry is created in the table.
3. Configure the firewall rule for HTTP with the following settings:

Action	Accept
From	vlan1 (INT)
To	ppp0 or usb0
Source (Range)	192.168.100.10 (the required device)
Destination (Range)	0.0.0.0/0 (all addresses)
Service	HTTP

4. Click on "Set Values".
5. Click "Create". A new entry is created in the table.
6. Configure the firewall rule for DNS with the following settings:

Action	Accept
From	vlan1 (INT)
To	ppp0 or usb0
Source (Range)	192.168.100.10 (the required device)
Destination (Range)	0.0.0.0/0 (all addresses)
Service	DNS

7. Click on "Set Values".

Internet Protocol (IP) Rules

General | Predefined IPv4 | User Specific | IP Services | ICMP Services | IP Protocols | IP Rules

IP Version: IPv4

Rule Set: -

show all

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service	Log	Precedence	Assign to	Assigned	Label
<input type="checkbox"/>	IPv4	Accept	vlan1 (INT)	ppp0	0.0.0.0/0	192.168.100.0/24	all	none	0	<input type="checkbox"/>	-	NETMAP
<input type="checkbox"/>	IPv4	Accept	ppp0	vlan1 (INT)	192.168.20.0/24	0.0.0.0/0	all	none	1	<input type="checkbox"/>	-	NETMAP
<input type="checkbox"/>	IPv4	Accept	IPsec M876_to	vlan1 (INT)	192.168.10.0/24	0.0.0.0/0	all	none	2	<input type="checkbox"/>	-	NETMAP
<input type="checkbox"/>	IPv4	Accept	vlan1 (INT)	IPsec M876_to	0.0.0.0/0	192.168.100.0/24	all	none	3	<input type="checkbox"/>	-	NETMAP

4 entries.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Allow an internal node access to the Internet

1. Click on "Security > Firewall" in the navigation area and on the "IP Rules" tab in the content area.
2. Click "Create". A new entry is created in the table.
3. Configure the firewall rule for HTTP with the following settings:

Action	Accept
From	vlan1 (INT)
To	ppp0 or usb0 (depending on the device)
Source (Range)	0.0.0.0/0 (all addresses)
Destination (Range)	0.0.0.0/0 (all addresses)
Service	all

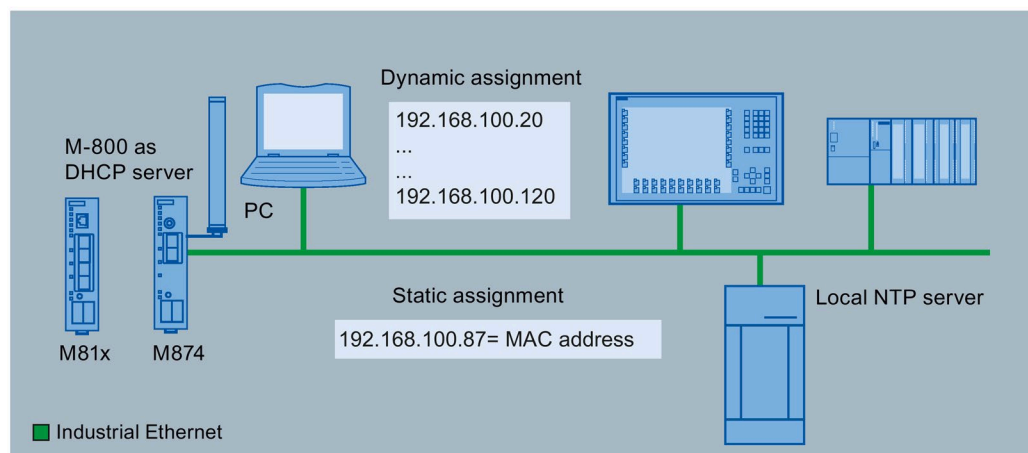
4. Click on "Set Values".

SCALANCE M-800 as DHCP server

If you want to use the device to manage the network configuration, you can use the device as a DHCP server. This allows IP addresses to be assigned automatically to the devices connected to the internal network.

In this example, both static and dynamic IP address assignments are configured.

SCALANCE M-800 as DHCP server



Required devices/components

- SCALANCE M-800 as DHCP server
1 x M874, 1 x M812 or M816 (optionally also: a suitably installed standard rail with fittings)
- 1 x 24 V power supply with cable connector and terminal block plug
- 1 x PC with which the SCALANCE M-800 is connected.
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet

Setting used

In the configuration example, the SCALANCE M-800 has the following IP address setting:

- IP address 192.168.100.1
- Subnet mask: 255.255.255.0

Requirement

- The SCALANCE M-800 can be reached via the admin PC and you are logged in to the WBM as "admin".

Steps in configuration

1. Configuring dynamic IP address assignment (Page 49)
2. Specifying DHCP options (Page 51)
3. Configuring static IP address assignment (Page 53)

2.1 Configuring dynamic IP address assignment

The devices whose MAC address or whose client ID was not specified specifically, are assigned a random IP address from a specified address range.

Procedure

1. Click on "System > DHCP" in the navigation area and on the "DHCP server" tab in the content area.

2. Click "Create". A new row with a unique number (pool ID) is created in the table.
3. Enter the network address range in "Subnet". Since the device being used is operating both as a gateway and a DNS relay, the IP address 192.168.100.1 must be in the network address range. In this example the network address: 192.168.100.0/24 (= 192.168.100.0 / 255.255.255.0) is used.
4. In "Lower IP Address", enter the IP address 192.168.100.20 that specifies the start of the dynamic address band and that is located within the network address range.
5. In "Upper IP Address", enter the IP address 192.168.100.120 that specifies the end of the dynamic address band and that is located within the network address range.
6. Click on "Set Values".
7. To activate the DHCP server, select "DHCP Server".
8. Enable "Probe address with ICMP echo before offer" to enable the ping function. With this ping, the DHCP server checks whether or not the IP address has already been assigned.

2.1 Configuring dynamic IP address assignment

- 9. To enable the configured DHCP pool, select the check box in the "Enable" column.
- 10. Click on "Set Values".

Dynamic Host Configuration Protocol (DHCP) Server

DHCP Client | DHCP Server | DHCP Options | Static Leases

DHCP Server
 Probe address with ICMP Echo before offer

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
<input type="checkbox"/>	1	vlan1	<input checked="" type="checkbox"/>	192.168.100.0/24	192.168.100.20	192.168.100.120	3600

1 entry.

Create Delete Set Values Refresh

Result

The DHCP server can assign up to 100 IP addresses from a set address band. This is only possible if the connected devices are configured so that they obtain the IP address from a DHCP server.

2.2 Specifying DHCP options

Further information can be transferred to the DHCP client using DHCP options. The various DHCP options are defined in RFC 2132.

The DHCP options 1, 3, 6, 66 and 67 are created automatically when the IPv4 address band is created. With the exception of option 1, the options can be deleted.

In this example, the following DHCP options are created.

DHCP option		Information contained
1	Netmask	The subnet mask to match the IP address For this example the subnet mask is: 255.255.255.0
3	Default gateway	IP address of the default gateway Without this information, the DHCP client is only assigned an IP address by the DHCP server and it can only communicate with the nodes in the internal network.
6	DNS server	IP address of the DNS server Without this information, the DHCP client is not automatically assigned a DNS server. To allow name resolution, a DNS server must be known to the DHCP client. This can also be configured manually.
66	TFTP server	TFTP Server Address This informs the DHCP client of the TFTP server to which it will connect.
67	Bootfile Name	The DHCP client uses this file when it boots.

Procedure

1. Click on "System" > "DHCP" in the navigation area and on the "DHCP Options" tab in the content area.

Dynamic Host Configuration Protocol (DHCP) Options

DHCP Server | DHCP Options | Static Leases

Pool ID: 1

Option Code:

Select	Pool ID	Option Code	Use Interface IP	Value
<input type="checkbox"/>	1	1	<input type="checkbox"/>	255.255.255.0
<input type="checkbox"/>	1	3	<input checked="" type="checkbox"/>	0.0.0.0
<input type="checkbox"/>	1	6	<input checked="" type="checkbox"/>	0.0.0.0
<input type="checkbox"/>	1	66	<input type="checkbox"/>	
<input type="checkbox"/>	1	67	<input type="checkbox"/>	Bootfile name not set

5 entries.

2. Enable "Use Interface IP" for the DHCP options 3 and 6. Click on "Set Values". The IP address of the device is entered automatically as the value.

3. Enter "42" in "Option Code".
4. Click "Create". A new row is created in the table.
5. In "Value", enter the IP address of the NTP server.
6. Click on "Set Values".

Result

Dynamic Host Configuration Protocol (DHCP) Options

DHCP Server | DHCP Options | Static Leases

Pool ID: 1

Option Code:

Select	Pool ID	Option Code	Use Interface IP	Value
<input type="checkbox"/>	1	1		255.255.255.0
<input type="checkbox"/>	1	3	<input checked="" type="checkbox"/>	192.168.100.1
<input type="checkbox"/>	1	6	<input checked="" type="checkbox"/>	192.168.100.1
<input type="checkbox"/>	1	42		192.168.100.87
<input type="checkbox"/>	1	66		
<input type="checkbox"/>	1	67		Bootfile name not set

6 entries.

The DHCP options are configured. If a DHCP client requests an IP address, in addition to the host IP address, it also receives the information entered in the DHCP options.

See also

Configuring static IP address assignment (Page 53)

2.3 Configuring static IP address assignment

For nodes in permanent operation, static IP address assignment should be preferred, for example for a local NTP server. The IP address of the NTP server is used in the DHCP option.

As long as the NTP server can be reached at the same IP address, the DHCP option will work correctly. If the IP address changes, the DHCP option contains incorrect information.

For the example, the IP address is assigned to the MAC address of the NTP server. This means that the NTP server always has the same IP address.

In this configuration example, the NTP server can be reached with the following IP address setting:

IP address	Subnet mask
192.168.100.87	255.255.255.0

Requirement

- The NTP server obtains the IP address from a DHCP server and identification is based on the MAC address.

Procedure

1. Click on "System" > "DHCP" in the navigation area and on the "Static Leases" tab in the content area.

Static Leases

DHCP Server | DHCP Options | Static Leases

Pool ID: 1

Client Identification Method: Ethernet MAC

Value:

Select	Pool ID	Identification Method	Value	IP Address
<input type="checkbox"/>	1	MAC	00-1b-1b-cd-f2-18	192.168.100.87

1 entry.

Create Delete Set Values Refresh

2. For "Pool ID", select "1".
3. For "Identification Method", select the entry "Ethernet MAC".
4. In "Value", enter the MAC address of the NTP server.
5. Click "Create". A new row is created in the table.

2.3 Configuring static IP address assignment

6. In "IP Address", enter the IP address of the NTP server.
7. Click on "Set Values".

Result

The NTP server always has the IP address 192.168.100.87.

Index

G

Glossary, 5

S

Service & Support, 5
SIMATIC NET glossary, 5

T

Training, 5

