SIEMENS

SIMATIC NET

Industrial Wireless LAN
SCALANCE W-700

Configuration Manual

04/2013
C79000-G8976-C238-04

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.

Table of contents

Introduction

1

1.1 Information on the SCALANCE W-700 Configuration Manual

Validity of the configuration manual

This Configuration Manual covers the following products:

- SCALANCE W788-1PRO
- SCALANCE W788-2PRO
- SCALANCE W788-1RR
- SCALANCE W788-2RR
- SCALANCE W744-1PRO
- SCALANCE W746-1PRO
- SCALANCE W747-1RR

- SCALANCE W786-1PRO
- SCALANCE W786-2PRO
- SCALANCE W786-3PRO
- SCALANCE W786-2RR

- SCALANCE W784-1
- SCALANCE W784-1RR
- SCALANCE W744-1
- SCALANCE W746-1
- SCALANCE W747-1

The section "Configuration with the Command Line Interface" also applies to the following product:

- IWLAN/PB Link PN IO

This Configuration Manual applies to the following software version:

- SCALANCE W-700 firmware as of version 4.5.

Note

These Operating Instructions do not apply to the SCALANCE W786-2HPW.

Functions of the SCALANCE W-700

The following table shows the firmware version as of which the individual functions of the SCALANCE W-700 are available:

Firmware version	Function
V4.0	• PNIO functionality • Aeroscout
V4.1	• iHOP
V4.3	• iPCF-MC • Dual client • DHCP server on client

Note

Order no. 6GK57xx-xSx00-2Ax6

Devices with order no. 6GK57xx-xSx00-2Ax6 can only be updated to version V3.4.11.

Purpose of the Configuration Manual

This Configuration Manual is intended to provide you with the information you require to install, commission and operate IWLAN devices correctly. It explains how to configure IWLAN devices and how to integrate IWLAN devices in a WLAN network.

Orientation in the documentation

Apart from the Configuration Manual you are currently reading, the following documentation is also available from SIMATIC NET on the topic of Industrial Wireless LANs:

● Operating Instructions (compact) SCALANCE W788-xPRO/RR

This document ships in paper form with the device and is also available in digital form on the SCALANCE W-700-CD. It contains information on mounting, connecting up and approvals for the following products:

– SCALANCE W788-1PRO

– SCALANCE W788-2PRO

– SCALANCE W788-1RR

– SCALANCE W788-2RR

– SCALANCE W744-1PRO

– SCALANCE W746-1PRO

– SCALANCE W747-1RR

- Operating Instructions (compact) SCALANCE W786-xPRO/RR

  This document ships in paper form with the device and is also available in digital form on the SCALANCE W-700-CD. It contains information on mounting, connecting up and approvals for the following products:

  – SCALANCE W786-1PRO

  – SCALANCE W786-2PRO

  – SCALANCE W786-3PRO

  – SCALANCE W786-2RR

- Operating Instructions (compact) SCALANCE W784-xPRO/RR

  This document ships in paper form with the device and is also available in digital form on the SCALANCE W-700-CD. It contains information on mounting, connecting up and approvals for the following products:

  – SCALANCE W784-1

  – SCALANCE W784-1RR

  – SCALANCE W744-1

  – SCALANCE W746-1

  – SCALANCE W747-1

- System Manual Structure of an Industrial Wireless LAN

  Apart from the description of the physical basics and a presentation of the main IEEE standards, this also contains information on data security and a description of the industrial applications of wireless LAN.
  You should read this manual if you want to set up WLAN networks with a more complex structure (not simply a connection between two devices).

- System manual RCoax

  This system manual contains both an explanation of the technical basis of RCoax cables as well as a description of the SIMATIC NET RCoax components and their functionality. The installation / commissioning and connection of RCoax components is explained.

- Manual Gateway IWLAN/PB Link PNIO for Industrial Ethernet

  The user documentation for the IWLAN/PB Link PNIO. This device is a gateway between IWLAN and PROFIBUS.

1.2 Type designations

Abbreviations used

The information in the manuals for the SCALANCE W-700 product family often applies to more than one product variant. In such situations, the designations of the products are shortened to avoid having to list all the type designations. The following table shows how the abbreviations relate to the product variants.

Product group	The designation . . . stands for . . .	Product name
Ethernet client modules (IP30, cabinet installation)	W74x-1	W744-1 W746-1 W747-1
Ethernet client modules (IP65, installed outside a cabinet)	W74x-1PRO/RR	W744-1PRO W746-1PRO W747-1RR
All Ethernet client modules SCALANCE W	W74x	W744-1 W746-1 W747-1 W744-1PRO W746-1PRO W747-1RR
Access points (IP30, cabinet installation)	W784-1xx	W784-1 W784-1RR
Access points (IP65, installed outside a cabinet, extreme climatic requirements)	W786-xPRO/RR	W786-1PRO W786-2PRO W786-3PRO W786-2RR
Access points (IP65, installed outside a cabinet)	W788-xPRO/RR	W788-1PRO W788-2PRO W788-1RR W788-2RR
Access points with the "RR" range of functions	W78x-xRR	W784-1RR W786-2RR W788-1RR W788-2RR

Product group	The designation . . . stands for . . .	Product name
All SCALANCE W access points	W78x	W788-1PRO W788-2PRO W788-1RR W788-2RR W786-1PRO W786-2PRO W786-3PRO W786-2RR W784-1 W784-1RR
All SCALANCE W devices	W -700	W788-1PRO W788-2PRO W788-1RR W788-2RR W744-1PRO W746-1PRO W747-1RR W786-1PRO W786-2PRO W786-3PRO W786-2RR W784-1 W784-1RR W744-1 W746-1 W747-1

Description

2

2.1 Network structures

Standalone configuration with the SCALANCE W access point

This configuration does not require a server and the SCALANCE W access point does not have a connection to a wired Ethernet. Within its transmission range, the SCALANCE W78x forwards data from one WLAN node to another.

The wireless network has a unique name. All the devices exchanging data within this network must be configured with this name.
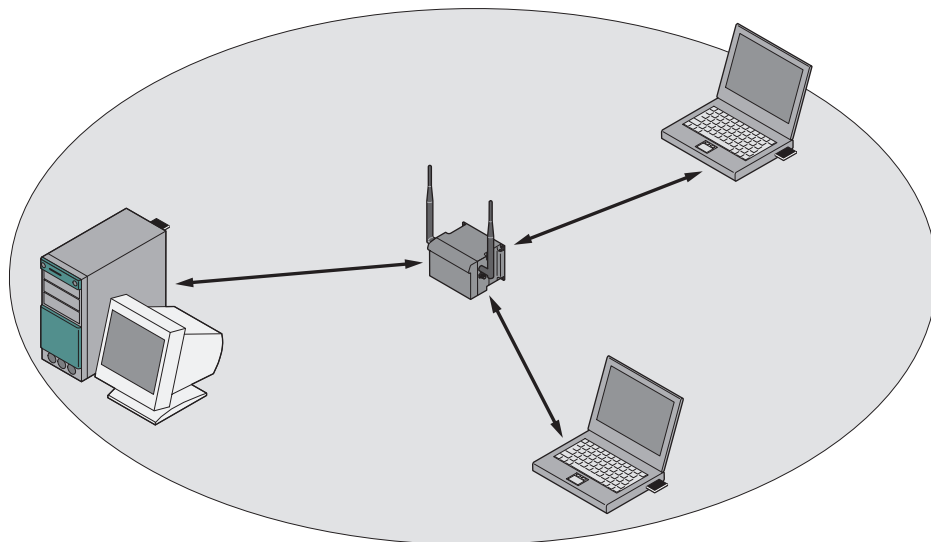
Figure 2-1   Standalone configuration of a SCALANCE W access point. The gray area symbolizes the wireless range of the SCALANCE W78x.

Ad hoc networks

In ad hoc mode, nodes communicate with each other directly (connection 4) without involving a SCALANCE W access point. The nodes access common resources (files or even devices, for example printers) of the server (connections 1 to 3 in the figure). This is, of course, only possible when the nodes are within the wireless range of the server or within each other's range.
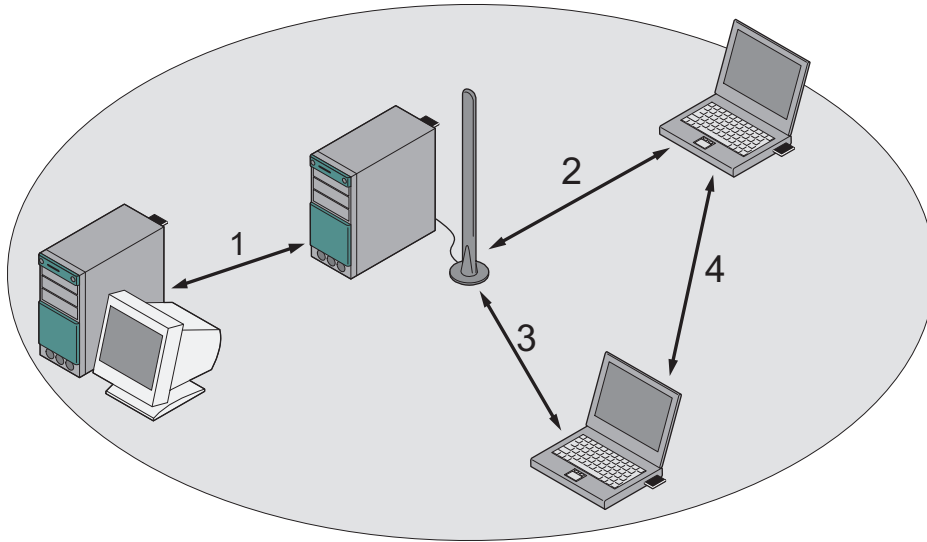
Figure 2-2   Ad hoc network without SCALANCE W access point

Wireless access to a wired Ethernet network

If one (or more) SCALANCE W access points have access to wired Ethernet, the following applications are possible:

● A single SCALANCE W as gateway:

A wireless network can be connected with a wired network over a SCALANCE W78x.

● Span of wireless coverage for the wireless network with several SCALANCE W78x access points:

The SCALANCE W78x access points are all configured with the same unique SSID (network name). All nodes that want to communicate over this network must also be configured with this SSID.

If a mobile station moves from the coverage range (cell) of one SCALANCE W78x to the coverage range (cell) of another SCALANCE W78x, the wireless connection is maintained (this is called roaming).
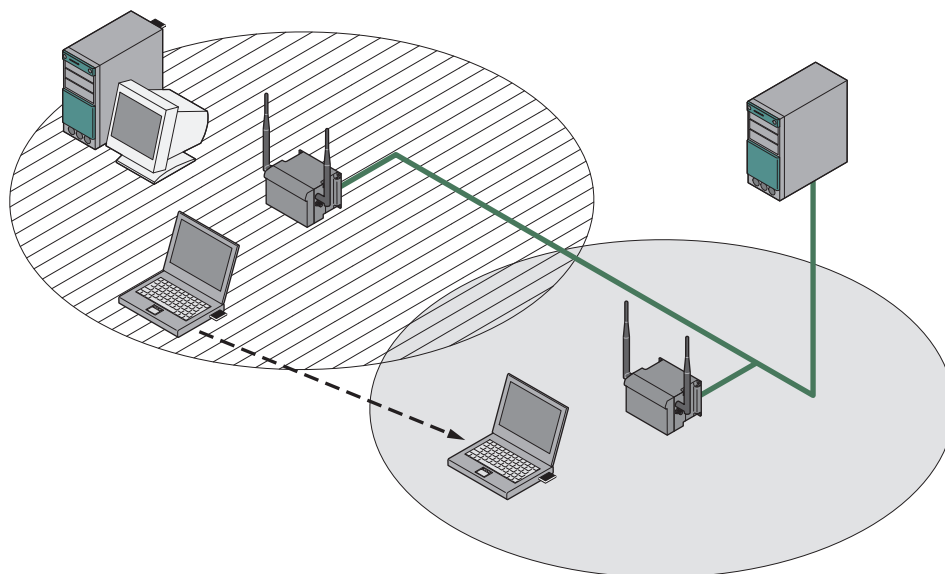
Figure 2-3   Wireless connection of a mobile station over two cells (roaming)

Multichannel configuration

If neighboring SCALANCE W access points use the same frequency channel, the response times are longer due to the collisions that occur. If the configuration shown in the figure is implemented as a single-channel system, computers A and B cannot communicate at the same time with the SCALANCE W access points in their cells.

If neighboring SCALANCE W access points are set up for different frequencies, this leads to a considerable improvement in performance. As a result, neighboring cells each have their own medium available and the delays resulting from time-offset transmission no longer occur.

Channel spacing should be as large as possible; a practical value would be 25 MHz (five channels). Even in a multichannel configuration, all SCALANCE W access points can be configured with the same network name.
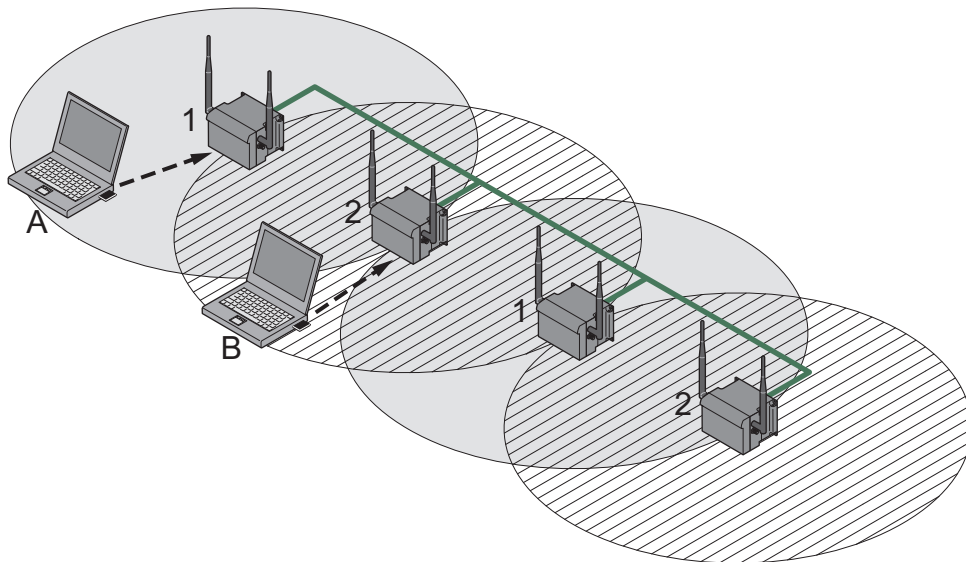
Figure 2-4   Multichannel configuration on channels 1 and 7 with four SCALANCE W access points

Wireless Distribution System (WDS)

WDS allows direct connections between SCALANCE W access points and or between SCALANCE W and other WDS-compliant devices. These are used to create a wireless backbone or to connect an individual SCALANCE W to a network that cannot be connected directly to the cable infrastructure due to its location.

Two alternative configurations are possible. The WDS partner can be configured both using its name and its MAC address.
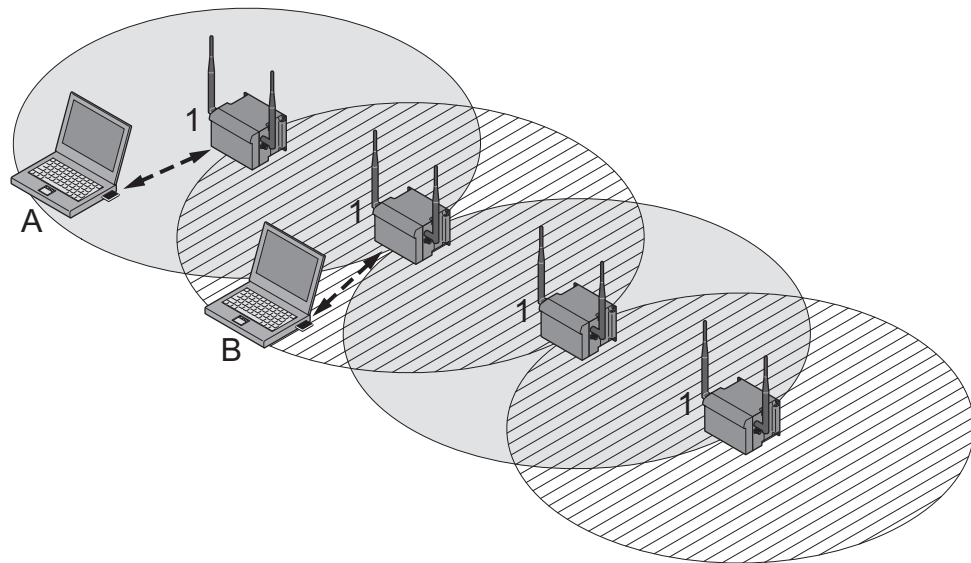
Figure 2-5   Implementation of WDS with four SCALANCE W access points

Redundant Wireless LAN (RWLAN)

RWLAN allows a redundant, wireless connection between two SCALANCE W access points with at least two WLAN interfaces. This is used to set up a redundant wireless backbone that cannot be implemented as a wired network due to its location but nevertheless has high demands in terms of availability.

Two alternative configurations are possible. The RWLAN partner can be configured both using its name and its MAC address.
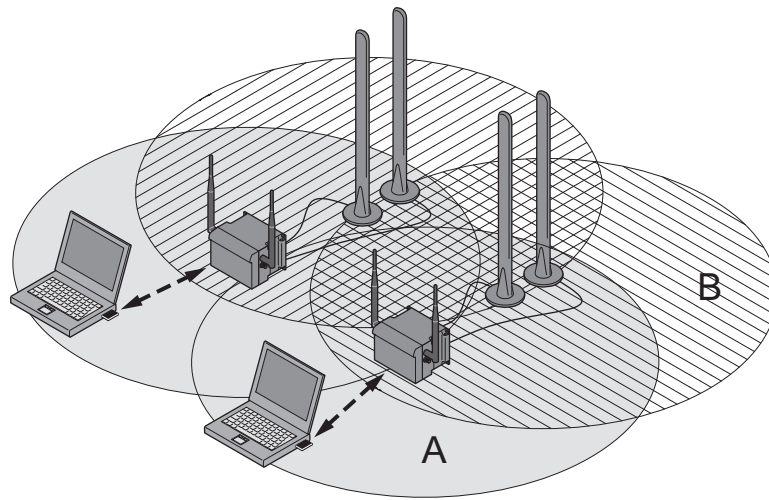
Figure 2-6   Implementing RWLAN with two SCALANCE W access points with at least two WLAN interfaces. As an alternative, data transfer is possible over one of the two wireless adapters.

Network access with a SCALANCE W74x or SCALANCE W78x in client mode

The device can be used to integrate wired Ethernet devices (for example SIMATIC S7 PLC) in a wireless network.
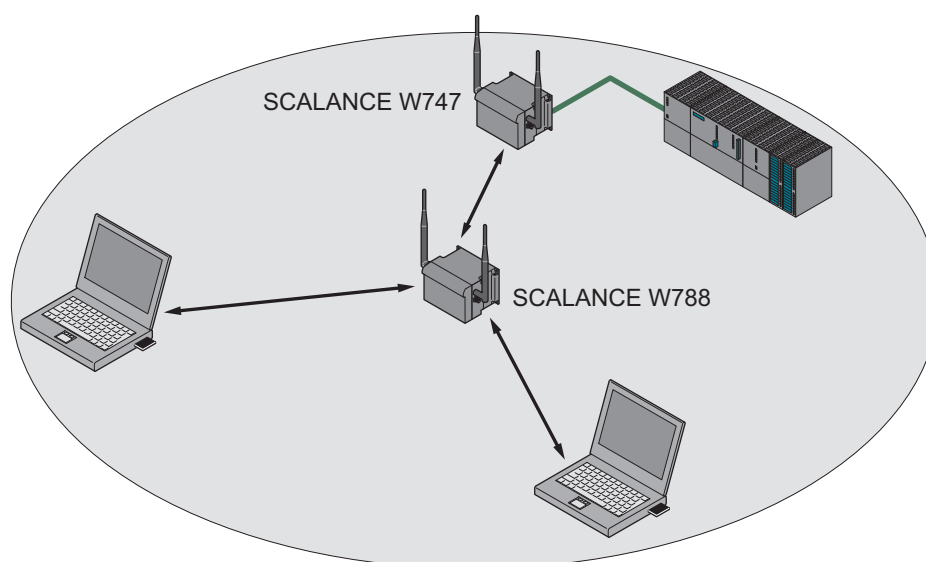
Figure 2-7   Connecting a SIMATIC S7 PLC to a wireless LAN using a SCALANCE W744.

Connecting a SIMATIC Mobile Panel 277F IWLAN or an ET200pro IWLAN

Using a SCALANCE W78x access point, mobile panels or ET200pro IWLAN devices can also be integrated in an existing IWLAN structure.
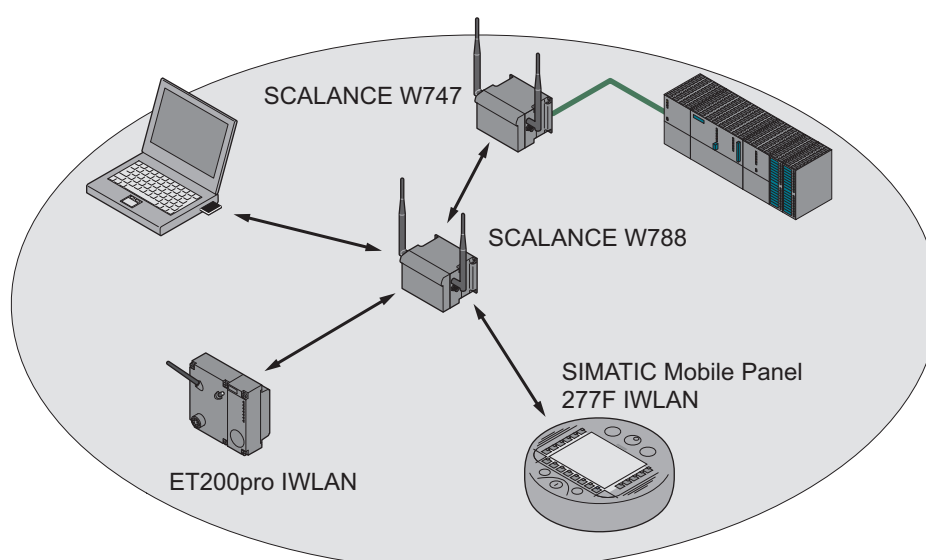
2.2 Possible applications of SCALANCE W-700 devices

Note

The SIMATIC NET WLAN products use OpenSSL.

This is open source code with license conditions (BSD).

Please refer to the current license conditions.

Since the driver includes encryption software, you should also adhere to the appropriate regulations for your specific country.

Possible applications of the SCALANCE W788-xPRO/RR
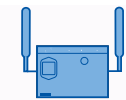
The SCALANCE W788-xPRO/RR is equipped with an Ethernet port and one or two wireless LAN ports. This makes the device suitable for the following applications:

- The SCALANCE W788-xPRO/RR forwards data within its transmission range from one node to another without a connection to wired Ethernet being necessary.

- The SCALANCE W788-xPRO/RR can be used as a gateway from a wired to a wireless network.

- The SCALANCE W788-xPRO/RR can be used as a wireless bridge between two networks.

- The SCALANCE W788-xPRO/RR can be used as a bridge between two different frequencies.

With a SCALANCE W788 with two WLAN ports, you can also implement a redundant wireless connection to a SCALANCE W78x with at least two WLAN ports.

Possible applications of the SCALANCE W744-1PRO
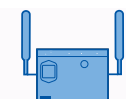
The SCALANCE W744-1PRO is equipped with an Ethernet port and a wireless LAN port. This makes the device suitable for the following applications:

- The SCALANCE W744-1PRO is used to connect a device with an Ethernet port (for example, a SIMATIC PLC with Industrial Ethernet communications processor) to a WLAN.

- The SCALANCE W744-1PRO can be used as a gateway from a wired to a wireless network. One node in the wired network is supported.

Possible applications of the SCALANCE W746-1PRO
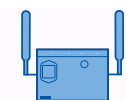
The SCALANCE W746-1PRO provides the same functionality as the SCALANCE W744-1PRO. The device can also connect up to 8 stations with IP communication on the Ethernet port to a wireless cell.

Possible applications of the SCALANCE W747-1RR

The SCALANCE W747-1RR provides the same functionality as the SCALANCE W746-1PRO. The device is also capable of optimized data transfer and handover times in iPCF mode.

Note

For PNIO communication, we always recommend that you enable the iPCF mode.

Possible applications of the SCALANCE W786
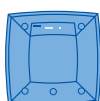
The SCALANCE W786 is equipped with an Ethernet port and up to three wireless LAN ports. This makes the device suitable for the following applications:

- Due to its extended temperature range, the SCALANCE W786 can be recommended in particular for outdoor applications.
- The SCALANCE W786 forwards data within its transmission range from one node to another without a connection to wired Ethernet being necessary.
- The SCALANCE W786 can be used as a gateway from a wired to a wireless network.
- The SCALANCE W786 can be used as a wireless bridge between two networks.
- The SCALANCE W786 can be used as a bridge between two cells operating at different frequencies.

With a SCALANCE W786 with more than one WLAN port, you can also implement a redundant wireless connection to a SCALANCE W78x with at least two WLAN ports.

Possible applications of the SCALANCE W784-1xx

The SCALANCE W784-1xx is equipped with an Ethernet port and a wireless LAN port. This makes the device suitable for the following applications:

- The SCALANCE W784-1xx forwards data within its transmission range from one node to another without a connection to wired Ethernet being necessary.
- The SCALANCE W784-1xx can be used as a gateway from a wired to a wireless network.
- The SCALANCE W784-1xx can be used as a wireless bridge between two networks.

Possible applications of the SCALANCE W744-1

The SCALANCE W744-1 is equipped with an Ethernet port and a wireless LAN port. This makes the device suitable for the following applications:

● The SCALANCE W744-1 is used to connect a device with an Ethernet port (for example, a SIMATIC PLC with Industrial Ethernet communications processor) to a WLAN.

● The SCALANCE W744-1 can be used as a gateway from a wired to a wireless network. One node in the wired network is supported.

Possible applications of the SCALANCE W746-1

The SCALANCE W746-1 has the functionality of the SCALANCE W744-1. The device can also connect up to 8 stations on the Ethernet interface to a wireless cell.

Possible applications of the SCALANCE W747-1

The SCALANCE W747-1 has the same functionality as the SCALANCE W746-1. The device also offers optimized data transfer and handover times in iPCF mode.

2.3 Product characteristics

Characteristics of SCALANCE W-700 devices

- The following applies to Korea:

  Note

  한국에서는 2.4GHz 대역의 802.11 b/g 모드만 지원됩니다.

- The Ethernet interface supports 10 Mbps and 100 Mbps, both in full and half duplex as well as autocrossing and autopolarity.

- Operating the wireless interface in the frequency bands 2.4 GHz and 5 GHz.

- The wireless interface is compatible with the standards IEEE 802.11a,

- IEEE 802.11b and IEEE 802.11g. In the 802.11a- and 802.11g mode, the gross transmission rate is up to 54 Mbps. In turbo mode, the transmission rate is up to 108 Mbps (not permitted in all countries and modes).

  Note

  If the SCALANCE W-700 is operated in turbo mode (A, G or H turbo), remember that the channels adjacent to the set transmission channel are also used for communication. Disturbances can therefore occur on these channels when there are neighboring wireless systems. The data throughput can also be reduced if there is competition for use of these channels.

- As an expansion of the 802.11a mode, it is also possible to operated according to the IEEE 802.11h standard. In 802.11h mode, the procedures "Transmit Power Control" (TPC) and "Dynamic Frequency Selection" (DFS) are used in the range 5.25 - 5.35 and 5.47 - 5.75 GHz. In some countries, this allows the frequency subband of 5.47 - 5.725 GHz to be used outdoors even with a higher transmit power.
  TPC is a technique of controlling the transmit power and can reduce it to the strength actually required. With dynamic frequency selection (DFS), the access point searches for primary users (for example radar) on a randomly selected channel before starting communication. If signals are found on the channel, this channel is disabled for 30 minutes and the availability check is repeated on another channel.
  The gross transmission rate is up to 54 Mbps in 802.11h mode.

- Support of the authentication standards WPA, WPA-PSK, WPA2, WPA2-PSK and IEEE 802.1x and the encryption methods WEP, AES and TKIP.

- Suitable for inclusion of a RADIUS server for authentication.

- Device-related and application-related monitoring of the wireless connection.

- The interoperability of the devices with Wi-Fi devices of other vendors was tested thoroughly.

- PNIO performance data
  Even in the planning phase of a plant, it is important to know the reaction time of IO communication and the delay time for data communication in a PROFIBUS, PROFINET IO or Industrial Ethernet network. To provide you with reliable information on typical plants with different topologies, various configurations have been set up and measured. Based on these measured values, you can do the following:

  – Design plants ideally in terms of their communication response and

  – Compare different plant configurations with each other

  You will find the measured values with the following link:
  http://support.automation.siemens.com/ww/view/en/25209605

- Before commissioning the SCALANCE W-700, check the wireless conditions on site. If you intend to use Industrial Wireless LAN systems and WirelessHART systems in the 2.4 GHz band, you will need to plan the use of the channels. At all costs, avoid parallel use of overlapping frequency ranges. The following overlaps exist with Industrial Wireless LAN and WirelessHART:

IWLAN channel IEEE 802.11b/g	WHART channel IEEE 802.15.4
1	11 - 16
6	15 - 20
7	16 - 21
11	20 - 25
13	21 - 25

Note

All SCALANCE W-700 access points can be reconfigured for client mode.

Note

For PNIO communication, we always recommend that you enable the iPCF mode.

Features of the SCALANCE W788 / W74x-1PRO/RR

Type	Number of WLAN ports	Number of supported IP nodes (3)	Number of supported MAC nodes (3)	iPCF mode (1)	Order no.
W788-1PRO	1	several	several	No	6GK5788-1AA60-2AA0
					6GK5788-1AA60-2AB0 (2)
W788-2PRO	2	several	several	No	6GK5788-2AA60-2AA0
					6GK5788-2AA60-2AB0 (2)
W788-1RR	1	several	several	Yes	6GK5788-1AA60-6AA0
					6GK5788-1AA60-6AB0 (2)
W788-2RR	2	several	several	Yes	6GK5788-2AA60-6AA0
					6GK5788-2AA60-6AB0 (2)
W744-1PRO	1	1	1	No	6GK5744-1AA60-2AA0
					6GK5744-1AA60-2AB0 (2)
W746-1PRO	1	several	several	No	6GK5746-1AA60-4AA0
					6GK5746-1AA60-4AB0 (2)
W747-1RR	1	several	several	Yes	6GK5747-1AA60-6AA0
					6GK5747-1AA60-6AB0 (2)

(1) The iPCF mode provides an optimized data throughput and minimum handover times.

(2) US variant

(3) In client mode.
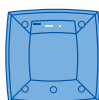
Features of the SCALANCE W786

Type	Number of WLAN ports	Number and type of Ethernet ports	Number of internal antennas	Number of R-SMA sockets for external antennas	Order no.
W786-1PRO	1	1 RJ-45	2 (diversity(2))	—	6GK5786-1BA60-2AA0
					6GK5786-1BA60-2AB0 (1)
W786-1PRO	1	1 RJ-45	—	2	6GK5786-1AA60-2AA0
					6GK5786-1AA60-2AB0 (1)
W786-1PRO	1	1 ST duplex multimode FO cable	2 (diversity(2))	—	6GK5786-1BB60-2AA0
					6GK5786-1BB60-2AB0 (1)

Type	Number of WLAN ports	Number and type of Ethernet ports	Number of internal antennas	Number of R-SMA sockets for external antennas	Order no.
W786-1PRO	1	1 ST duplex multimode FO cable	—	2	6GK5786-1AB60-2AA0
					6GK5786-1AB60-2AB0 [1]
W786-2PRO	2	1 RJ-45	4 (diversity[2])	—	6GK5786-2BA60-2AA0
					6GK5786-2BA60-2AB0 [1]
W786-2PRO	2	1 RJ-45	—	4	6GK5786-2AA60-2AA0
					6GK5786-2AA60-2AB0 [1]
W786-2PRO	2	1 ST duplex multimode FO cable	4 (diversity[2])	—	6GK5786-2BB60-2AA0
					6GK5786-2BB60-2AB0 [1]
W786-2PRO	2	1 ST duplex multimode FO cable	—	4	6GK5786-2AB60-2AA0
					6GK5786-2AB60-2AB0 [1]
W786-2RR	2	1 RJ-45	4 (diversity[2])	—	6GK5786-2BA60-6AA0
					6GK5786-2BA60-6AB0 [1]
W786-2RR	2	1 RJ-45	—	4	6GK5786-2AA60-6AA0
					6GK5786-2AA60-6AB0 [1]
W786-3PRO	3	1 RJ-45	—	6	6GK5786-3AA60-2AA0
					6GK5786-3AA60-2AB0 [1]
W786-3PRO	3	1 ST duplex multimode FO cable	—	6	6GK5786-3AB60-2AA0
					6GK5786-3AB60-2AB0 [1]

(1) US variant

(2) There are two internal antennas per WLAN port. The antenna used is always the one that provides the best possible data transmission (diversity).

Features of the SCALANCE W784-1xx / W74x-1

Type	Number of WLAN ports	Number of supported IP nodes	Number of supported MAC nodes	iPCF mode [1]	Order no.
W784-1	1	several	several	No	6GK5784-1AA30-2AA0
					6GK5784-1AA30-2AB0 [2]
W784-1RR	1	several	several	Yes	6GK5784-1AA30-6AA0
					6GK5784-1AA30-6AB0 [2]
W744-1	1	1	1	No	6GK5744-1AA30-2AA0
					6GK5744-1AA30-2AB0 [2]
W746-1	1	8	8	No	6GK5746-1AA30-4AA0
					6GK5746-1AA30-4AB0 [2]
W747-1	1	8	8	Yes	6GK5747-1AA30-6AA0
					6GK5747-1AA30-6AB0 [2]

(1) The iPCF mode provides an optimized data throughput and minimum handover times.

(2) US variant

2.4 Requirements for installation and operation of SCALANCE W-700 devices

Requirements for installation and operation of SCALANCE W-700 devices

A PG/PC with a network connection must be available in order to configure SCALANCE W-700 devices. If no DHCP server is available, a PC on which the Primary Setup Tool (PST) is installed is necessary for the initial assignment of an IP address to SCALANCE W-700 devices. For the other configuration settings, a computer with Telnet or an Internet browser is necessary.

2.5 C-PLUG

Configuration information on the C-PLUG

The C-PLUG is used to transfer the configuration of the old device to the new device when a device is replaced. When the new device starts up with the C-PLUG, it then continues automatically with exactly the same configuration as the old device. One exception to this can be the IP configuration if it is set over DHCP and the DHCP server has not been reconfigured accordingly.

Reconfiguration is necessary if you use WDS or redundancy with devices with more than one WLAN interface and use the MAC addresses and not the sysNames. These functions are then based on the MAC address that inevitably changes if a device is replaced.

Note

In terms of the C-PLUG, the SCALANCE W-700 devices work in two modes:

- **Without C-PLUG**
  The device stores the configuration in internal memory. This mode is active when no C-PLUG is inserted.

- **With C-PLUG**
  The configuration stored on the C-PLUG is displayed over the user interfaces. In this mode, the internal memory is neither read nor written. If changes are made to the configuration, the device stores the configuration directly on the C-PLUG. This mode is active when no C-PLUG is inserted. As soon as the device is started with a C-PLUG inserted, the SCALANCE W-700 starts up with the configuration data on the C-PLUG.

2.6 Biological compatibility

Electromagnetic fields and health

With regard to the question of whether electromagnetic fields (for example in association with industrial wireless LANs) can put human health at risk, we refer to a publication of BITKOM (German Association for information Technology, Telecommunication and New Media e. V.), dated December 2003:

"The same health guidelines apply to WLAN devices as to all other radio applications. These regulations are based on the protection concept of ICNIRP[1] or the corresponding recommendation of the European Council.

The independent German radiation protection commission (SSK) was commissioned by the federal German ministry of the environment to investigate the possible dangers - thermal and non-thermal - resulting from electromagnetic fields and came to the following conclusions[2]:

'The German Commission on Radiological Protection concludes that according to the latest scientific literature no new scientific research is available with respect to proven health hazards which would throw doubt upon the scientific evaluation which serves as the basis for the ICNIRP safety concepts and the recommendations of the EU commission.'

The SSK also concludes that below the current limit values, these is also no scientific suspicion of health risks.

This assessment agrees with those of other national and international scientific commissions and of the WHO (`www.who.int/emf`).

Accordingly and in view of the fact that WLAN devices are significantly below the scientifically established limit values, there are no health risks from the electromagnetic fields of WLAN products.

[1] International Council on Non-Ionizing Radiation Protection

[2] 'Limit Values and Precautionary Measures to Protect the General Public from Electromagnetic Fields' Recommendation of the Radiation Protection Commission (SSK) with scientific justification, Issue 29, 2001."

You will find further information on this topic under the following URL:

`www.bitkom.org`

2.7 Power over Ethernet (PoE)

General

"Power over Ethernet" (PoE) is a power supply strategy for network components according to 802.3af. The power is supplied over the Ethernet cables that connect the individual network components together. This makes an additional power cable unnecessary. PoE can be used with all PoE-compliant network components that require little power (max. 12.95 W).

Cable used for the power supply

- **Variant 1 (redundant wires)**
  In Fast Ethernet, the wire pairs 1, 2 and 3, 6 are used to transfer data. Pairs 4, 5 and 7, 8 are then used to supply power. If there are only four wires, the voltage is modulated onto wires 1, 2 and 3, 6 (see variant 2). This alternative is suitable for a data transmission rate of 10/100 Mbps. This type of power supply is not suitable for 1 Gbps because with gigabit Ethernet, all 8 wires are used for the data transmission.

- **Variant 2 (phantom power)**
  With phantom power, the power is supplied over the pairs that are used for data transfer, in other words, all eight (1 Gbps) or four (10/100 Mbps) wires are used both for the data transfer and the power supply.

A PoE-compliant end device must support both variant 1 and variant 2 over redundant wires. A PoE-compliant switch can supply the end device either using:

- Variant 1 or

- Variant 2 or

- Variant 1 and variant 2.

Endspan

With endspan, the power is supplied via a switch that can reach a device over an Ethernet cable. The switch must be PoE-compliant, for example a SCALANCE X108PoE.

Midspan

Midspan is used when the switch is not PoE-compliant. The power is supplied by an additional device between the switch and end device. In this case, only data rates of 10/100 Mbps can be achieved because the power is supplied on redundant wires.

A Siemens power insert can also be used as the interface for the power input. Since a power insert supports a power supply of 24 V DC, is it not 802.3af compliant. The following restrictions relating to the use of power inserts should be noted:

⚠ **WARNING**

Operate the power insert only when the following conditions apply:

- with extra low voltages SELV, PELV complying with IEC 60364-4-41
- in USA/CAN with power supplies complying with NEC class 2
- in USA/CAN, the cabling must meet the requirements of NEC/CEC
- Power load maximum 0.5 A.

Connectors / fitting connectors

Table 2- 1   Connectors

Device	Connectors	Cable
SCALANCE W788 SCALANCE W786 SCALANCE W784 SCALANCE S SCALANCE X	IE FC RJ-45 Plug or IE Hybrid RJ-45 Plug (only with SCALANCE W788) All cables listed comply with Cat5E	For 0-100 m: Industrial Ethernet FC TP standard cable or 0 - 90 m Industrial Ethernet FC TP standard cable + 10 m TP cord For 0-85 m: Industrial Ethernet FC TP marine/trailing or 0 - 75 m Industrial Ethernet FC TP marine/trailing cable + 10 m TP cord

Table 2- 2   Fitting connectors

PIN	Wire color	Use	
		Power over unused wires (10/100 Mbps only)	Phantom power
1	Yellow	Data	Data/power
2	Orange	Data	Data/power
3	White	Data	Data/power
6	Blue	Data	Data/power
4		Power	unused at 10/100 Mbps
5		Power	unused at 10/100 Mbps
7		Power	unused at 10/100 Mbps
8		Power	unused at 10/100 Mbps

LEDs for PoE on the SCALANCE W-700 device

The following table shows which LED lights up on the SCALANCE W-700 device when the device is supplied using PoE:

SCALANCE W-700 device	LED for PoE
SCALANCE W788-xx	green LED "L2"
SCALANCE W786-xx	green LED "PoE"
SCALANCE W784-xx	green LED "PoE"
SCALANCE X-108PoE	green LED "L1" or "L2"

Configuration / project engineering

3

3.1 Technical basics

3.1.1 Spanning Tree

Avoiding loops

The Spanning Tree algorithm detects redundant physical network structures and prevents the formation of loops by disabling redundant paths. It evaluates the distance and performance of a connection or bases the decisions on settings made by the user. Data is then exchanged only over the remaining connection paths.

If the preferred data path fails, the Spanning Tree algorithm then searches for the most efficient path possible with the remaining nodes.

Root bridge and bridge priority

The identification of the most efficient connection is always related to the root bridge, a network component that can be considered as a root element of a tree-like network structure. With the "Bridge Priority" parameter, you can influence the selection of the root bridge. The computer with the lowest value set for this parameter automatically becomes the root bridge. If two computers have the same priority value, the computer with the lower MAC address becomes the root bridge.

Response to changes in the network topology

If nodes are added to a network or drop out of the network, this may affect the optimum path selection for data packets. To be able to respond to such changes, the root bridge sends configuration messages at regular intervals. You can set the interval between two configuration messages with the "Hello Time" parameter.

Keeping configuration information up to date

With the "Max Age" parameter, you set the maximum age of configuration information. If a bridge has information that is older than the time set in Max Age, it discards the message and initiates recalculation of the paths.

New configuration data is not used immediately by a bridge but only after the period specified in the "Forward Delay" parameter. This ensures that operation is started with the new topology only after all the bridges have the required information.

3.1.2 iQoS

Client-specific bandwidth reservation

iQoS (Quality of Service) is technique with which clients are assigned a certain bandwidth. Due to this assignment, there is a high probability that data transmission to these clients will be within a defined period. This technique can be useful when response times must be guaranteed.

3.1.3 iPCF and iPCF-MC

Restrictions of the 802.11 standard

With wireless LAN complying with IEEE 802.11, the maximum data throughput cannot be achieved in a cell when there is a higher number of nodes due to the resulting collisions. A further restriction are the handover times that can be achieved with 802.11 standard mechanisms. With normal commercially available WLAN products, these are of the order of several hundred milliseconds.

New possibilities with iPCF

In an industrial environment, there are applications that require a deterministic response when there are large numbers of nodes and a high data throughput in a cell. A deterministic behavior is also required when changing cells with handover times of under 100 milliseconds.

To meet these requirements, the iPCF expansion (industrial Point Coordination Function) was developed. iPCF is available with the following products:

- SCALANCE W78x-xRR
- SCALANCE W747-1RR
- SCALANCE W747-1
- IWLAN/PB Link PN IO
- ET200pro IWLAN

iPCF ensures that the entire data traffic of a cell is ordered, controlled by the access point. By avoiding collisions, the throughput can be optimized even with large numbers of nodes. iPCF also allows fast cell changes.

How iPCF works

The basic principle of iPCF is that the access point scans all nodes in the cell cyclically. The same time, the scan includes the downlink traffic for this node. In the reply, the node sends the uplink data. The access point scans a new node at least every 5 ms.

The scan of a node can be seen by all other nodes in the cell. This allows a client to detect the quality of the link to the access point even when it is not communicating with the access point itself. If it does not receive a frame from the access point for a certain time, it starts to search for a new access point.

In iPCF mode, both the search for a new access point and the registration with this new access point have been optimized in terms of time. Handover times significantly below 50 ms are achieved.

Special features of iPCF-MC

iPCF-MC was developed to make the advantages of iPCF available to fully mobile nodes that communicate without being dependent on RCoax cable or directional antennas. With iPCF-MC, the client also searches for potentially suitable access points when it receives iPCF queries from the access point and the existing connection to an access point is working problem-free. This means that if a change to a different access point is necessary, this is achieved extremely quickly. In contrast to iPCF, the handover times for iPCF-MC are not dependent on the number of wireless channels being used.

3.1.4 Forced Roaming on IP Down

Functional description

"Forced Roaming on IP down" monitors the connection to a specific IP address cyclically. This is achieved using ICMP packets (Echo Request/Reply or Ping). If the IP connection aborts; in other words, there is no ping reply from the other end, a deauthentication frame is sent to all WLAN clients. The relevant WLAN interface is then disabled.

The IP connection continues to be monitored and the WLAN interface is enabled again as soon as the access point has received a ping reply from the pinged station.

The mechanism makes it possible, for example, to monitor a connection between wireless clients and a server. If the server can no longer be reached over the access point, the clients are deauthenticated and the WLAN interface of the access point is disabled. The clients roam and then connect to a different access point from which the server can be reached. As soon as the first access point can reach the server again, it re-enables its WLAN interfaces.

3.1.5 Link Check

Device-related connection monitoring

The Link Check function provides device-related connection monitoring for a maximum of ten wireless nodes logged on at the SCALANCE W78x. This service can be compared with the link on a wired connection. The function monitors whether the node is available over the wireless medium. If no packet is received from the node or sent successfully after half of the configured monitoring time, the SCALANCE W78x attempts to send a test packet to the node.

3.1.6 Redundancy

Redundant connection between two SCALANCE W78x devices

You can configure two SCALANCE W78x devices with two wireless interfaces so that there is a redundant wireless connection. The redundancy function causes an automatic failover to the second wireless interface if no data transfer is possible on the first wireless interface. The user is informed of the status of the redundant connection with the statuses "not connected", "connected", or "error" (communication error).

3.1.7 IP-Alive

Application-related connection monitoring

The IP-Alive function provides application-related connection monitoring of the wireless link.

It is useful to use IP-Alive on IP connections when it is known that they are used to send data cyclically. With IP-Alive, you specify a monitoring time for an IP address and a port. If you do not want to monitor a particular port but rather only the data traffic from a particular IP address, simply enter 0 in Port. This resets the monitoring with each frame from this IP address.

In contrast to the Link Check, the SCALANCE W78x does not start any checks until the monitoring time has elapsed. The SCALANCE W78x checks passively whether communication took place during the specified monitoring period. As with Link Check, you can also enter up to ten connections here.

3.1.8 MAC-based communication

Auto Find Adopt MAC / Adopt MAC manually

Frames in the direction from the client to the access point always have the MAC address of the WLAN interface as the source MAC address. As a result, the learning table at the access point end always has only the MAC address of the WLAN interface of the client. If the MAC address of a device connected to the client is adopted, both the MAC-based and the IP-based frames find their destination in precisely this device.

Other nodes located downstream from the client cannot be reached. The access point checks whether the destination MAC address matches the MAC addresses of the connected clients. Since a client can only adopt one MAC address, the access point does not find a match and discards the packets of several nodes.

Maximum possible number of MAC nodes downstream from the client: 1

Notes on the "Auto find 'Adopt MAC'" setting:

- As long as there is no link on the Ethernet interface, the device uses the MAC address of the Ethernet interface so that it can be reached in this status. In this status, the device can be found using the Primary Setup Tool.

- As soon as there is a link on the Ethernet interface, the device adopts the source MAC address of the first received frame.

Note

From the moment that the device adopts another MAC address (whether manually or automatically), the device no longer responds to queries of the Primary Setup Tool when the query is received over the WLAN interface. Queries of the PST over the Ethernet interface continue to be replied to.

Adopt Own MAC (only for W746-1 and W747-1 or W746-1PRO and W747-1RR and W78x in client mode)

If IP-based frames need to be sent to a device connected downstream from the client, the default setting Adopt Own Mac can be retained. The client registers with the MAC address of its Ethernet adapter. The IP packets are broken down according to an internal table and forwarded to the connected devices (IP mapping).

Communication at the MAC address level (ISO/OSI layer 2) is then only possible with a component downstream from the client if its MAC address was adopted by the client.

Maximum possible number of MAC nodes downstream from the client: 1

Layer 2 tunnel (only for W746-1 and W747-1 or W746-1PRO and W747-1RR and W78x in client mode)

With a "layer 2 tunnel", the client provides information about the devices downstream from it when it registers with an access point. This makes it possible to enter the MAC addresses of these devices in the learning table of the access point. The access point can forward MAC-based frames for the devices downstream from the client to the appropriate client.

In much the same way as with WDS, a separate port is created for the L2T client over which the Ethernet frames are sent without changing the destination MAC address.

Maximum possible number of MAC nodes downstream from the client: 8

3.1.9   IP-based communication

IP mapping (only for W746-1 and W747-1 or W746-1PRO and W747-1RR and W78x in client mode)

If there is more than one device connected downstream from the client and these should only be addressed with IP frames, you can implement WLAN access for several devices with one client. With IP mapping, the client maintains a table with the assignment of MAC address and IP address to forward incoming IP frames to the correct MAC address.

Maximum possible number of IP nodes downstream from the client: 8

3.1.10   AeroScout

Introduction

SCALANCE W-700 devices support tags of the AeroScout company. Tags are battery-operated sensor nodes that send out WLAN frames cyclically as multicast frames. There are numerous uses for these devices. In a WLAN installation with at least three access points, for example, the location of the tag can be detected. The tags can only be used in the 2.4 GHz band.

Hardware and function of an AeroScout tag

Among other things, AeroScout tags have the following features:

- **Ambient temperature sensor**
  If a tag is fitted to a device or material, it is possible to monitor whether a selected ambient temperature is being maintained.

- **Motion sensor**
  Here, a tag can also supply information indicating whether it is in motion or stationary. The areas of material flow and material handling engineering represent possible applications for this function.

- **Button**
  Regardless of the frames sent cyclically, a user can also send information by pressing a button.

- **LED**
  This provides information on the operating state of the tag.

Note

For more detailed information, please refer to the AeroScout documentation of (www.aeroscout.com).

Forwarding frames by the SCALANCE W-700

If the wireless interface of a SCALANCE W-700 receives an AeroScout frame, this is converted to a UDP packet and forwarded along with information on the signal strength (RSSI) via the backbone (either the Ethernet interface or a WDS connection). The SCALANCE W-700 does not process the data. This is done only by the target computer that receives and evaluates the UDP packet.

Note

It is **not** advisable to use PNIO communication and AeroScout together on one wireless interface.

Antenna configuration

To achieve optimum accuracy in the localization of AeroScout tags, we recommend the use of antennas with omindirectional characteristics.

3.1.11   iHOP

How iHOP works and the advantages of the iHOP function

The iHOP function is an adaptive frequency hopping technique in the frequency bands 2.4 and 5 GHz used in 802.11. At predefined intervals, the access point continuously changes it operating channel and informs the sequence of the next hops to the logged on clients. Along with precise time synchronization, this allows a simultaneous channel change by the access point and clients in a cell.

All configured channels are monitored permanently by the access point in terms of their quality (received signal strength, packet drop rates etc.) and evaluated relative to each other. The channels that are performing better are then the channels preferred by the access point. With this technique, it is possible to react dynamically to interference in certain frequency ranges.

3.1.12   Dual client

How dual client works

In the dual client technique, devices connect to a wireless network not through a WLAN client as normal but through two client devices. These two devices handle different functions. The active client handles the normal data traffic with the access point as would be the case without the second client connected.

Figure 3-1   Clients ① and ② are used in dual client mode. There is an active connection ⑥ between the client ② and the access point ④ via which data is exchanged. There is also a connection ⑥ between the client ① and the access point ③, however without data exchange (standby connection).

The second client known as the standby client scans the RF field permanently for alternative access points and always establishes a connection to the access point providing the best transmission quality. There is, however, no data transfer. The standby client also receives information on the quality of the connection between the active client and access point at regular intervals.

As soon as the connection quality of the standby client to the connected access point is better than the quality of the connection between the active client and access point, there is a switchover within a few milliseconds and the previous standby client takes over the data transfer. The previously active client now takes on the role of standby client and scans the RF field for access points.

3.2 Assignment of an IP address

3.2.1 Structure of an IP address

Address classes to RFC 1518 and RFC 1519

IP address range	Max. number of networks	Max. number of hosts/network	Class	CIDR
1.x.x.x through 126.x.x.x	126	16777214	A	/8
128.0.x.x through 191.255.x.x	16383	65534	B	/16
192.0.0.x through 223.255.255.x	2097151	254	C	/24
Multicast groups			D	
Reserved for experiments			E	

An IP address consists of 4 bytes. Each byte is represented in decimal, with a dot separating it from the previous one. This results in the following structure, where XXX stands for a number between 0 and 255:

XXX.XXX.XXX.XXX

The IP address is made up of two parts, the network ID and the host ID. This allows different subnets to be created. Depending on the bytes of the IP address used as the network ID and those used for the host ID, the IP address can be assigned to a specific address class.

Subnet mask

The bits of the host ID can be used to create subnets. The leading bits represent the address of the subnet and the remaining bits the address of the host in the subnet.

A subnet is defined by the subnet mask. The structure of the subnet mask corresponds to that of an IP address. If a "1" is used at a bit position in the subnet mask, the bit belongs to the corresponding position in the IP address of the subnet address, otherwise to the address of the computer.

Example of a class B network:

The standard subnet address for class B networks is 255.255.0.0; in other words, the last two bytes are available for defining a subnet. If 16 subnets must be defined, the 3rd byte of the subnet address must be set to 11110000 (binary notation). In this case, this results in the subnet mask 255.255.240.0.

To find out whether two IP addresses belong to the same subnet, the two IP addresses and the subnet mask are ANDed bit by bit. If both logic operations have the save result, both IP addresses belong to the same subnet, for example, 141.120.246.210 and 141.120.252.108.

Outside the local area network, the distinction between network ID and host ID is of no significance, in this case packets are delivered based on the entire IP address.

Note

In the bit representation of the subnet mask, the "ones" must be set left-justified (there must be no "zeros" between the "ones").

3.2.2 Initial assignment of an IP address

Configuration options

An initial IP address for a SCALANCE W-700 cannot be assigned using Web Based Management or the Command Line Interface over Telnet because these configuration tools require that an IP address already exists.

The following options are available to assign an IP address to an unconfigured device currently without an IP address:

- DHCP (default)
- STEP 7
- NCM PC
- Primary Setup Tool

Note

DHCP is enabled as default and following "Restore Factory Defaults and Restart". If a DHCP server is available in the local area network, and this responds to the DHCP request of a SCALANCE W-700, the IP address, subnet mask and gateway are assigned automatically when the device first starts up. "Reset to Memory Defaults" does not delete an IP address assigned either by DHCP or by the user.

3.2.3   Address assignment with DHCP

Properties of DHCP

DHCP (Dynamic Host Configuration Protocol) is a method for automatic assignment of IP addresses. It has the following characteristics:

- DHCP can be used both when a device starts up and during operation.

- The assigned IP address remains valid only for a particular time known as the lease time. Once this period has elapsed, the client must either request a new IP address or extend the lease time of the existing IP address.

- There is normally no fixed address assignment; in other words, when a client requests an IP address again, it normally receives a different address from the previous address. It is, however possible, to configure the DHCP server so that it assigns a fixed address.

Note

DHCP uses a mechanism with which the IP address is assigned for only a short time (lease time). If the device does not reach the DHCP server with a new request on expiry of the lease time, the assigned IP address, the subnet mask and the gateway are changed to static entries.

The device therefore remains accessible under the last assigned IP address even without a DHCP server. This is not the standard behavior of office devices but is necessary for problem-free operation of the plant.

Since the DHCP client also sends a RELEASE to the server, the server can assign this address to a further device so that inconsistencies can occur within the network.

Remedy:

After disabling DHCP, you should therefore

- change the IP address of the device to an address not assigned by DHCP

or

- remove the IP address assigned to the device from the address pool of the DHCP server.

Working with a mixture of dynamic address assignment and statically assigned addresses is not advisable.

3.2.4 Address assignment with the Primary Setup Tool

Introduction

The PST (Primary Setup Tool) is capable of assigning such an address to unconfigured devices without an IP address.

Prerequisite

This is only possible when the devices can be reached over Ethernet.

> **Note**
>
> For more detailed information, refer to the Primary Setup Tool configuration manual.
>
> You will find the PST at Siemens Industry Automation and Drives Service & Support on the Internet under entry ID 19440762 and with the following Link:
>
> Auto-Hotspot

3.3 The wizards of Web Based Management

3.3.1 Introduction

Principle of Web Based Management

The IWLAN device has an integrated HTTP server for Web Based Management. If an IWLAN device is addressed over an Internet browser, it returns HTML pages to the client computer depending on the user input.

The user enters the configuration data in the HTML pages sent by the IWLAN device. The IWLAN device evaluates this information and generates reply pages dynamically.

The great advantage of this method is that apart from a Web browser, no special software is required on the client.

Requirements for Web Based Management

Once you have assigned an IP address with the Primary Setup Tool, you can continue to configure the device with Web Based Management.

To use Web Based Management, you should ideally have a wired network connection between the IWLAN device and the client computer. In principle, it is possible to use Web Based Management over a wireless network, however the IWLAN device can be set so that access over a wireless network is disabled.

We recommend that you use the Microsoft Internet Explorer Version 5.5 or higher or Mozilla Firefox Version 1.5 or higher.

All the pages of Web Based Management require JavaScript. Make sure that your browser settings allow this.

Since Web Based Management is HTTP-based, you will have to allow access to Port 80 or Port 443 for HTTPS if you have a firewall installed.

Note

The screenshots in this section were created using the Microsoft Internet Explorer version 6.0. If you use a different browser (for example Mozilla), the appearance of the menus may differ.

The LED simulation of Web Based Management

The IWLAN device has one or more LEDs that provide information on the operating state of the device. Depending on its location, direct access to the IWLAN device may not always be possible. Web Based Management therefore displays simulated LEDs.

Activating the simulation

There is an HTML-based simulation of the LED status. Click on the green icon below the Console link to activate the simulation.
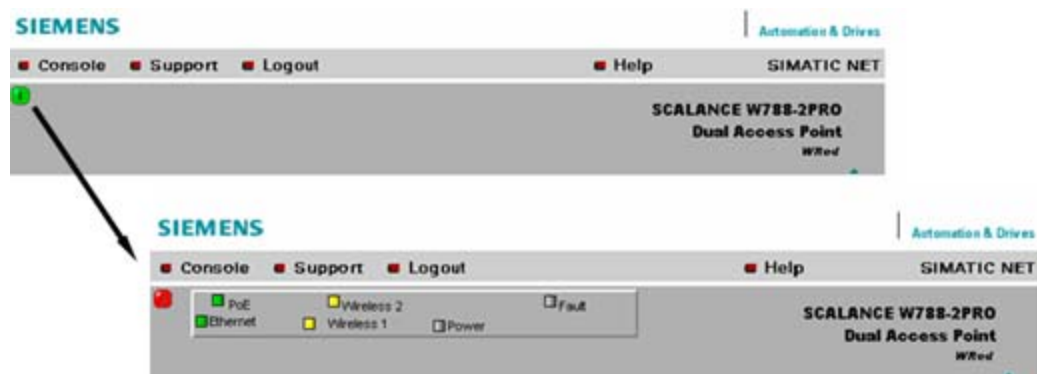
3.3.2 Starting Web Based Management and logging on

Procedure

Follow the steps below to establish a connection to a device using a Web browser:

1. In the address box of the Web browser, enter the IP address or the URL of the IWLAN device. If there is a problem-free connection to the IWLAN device, the Logon dialog of Web Based Management is displayed.
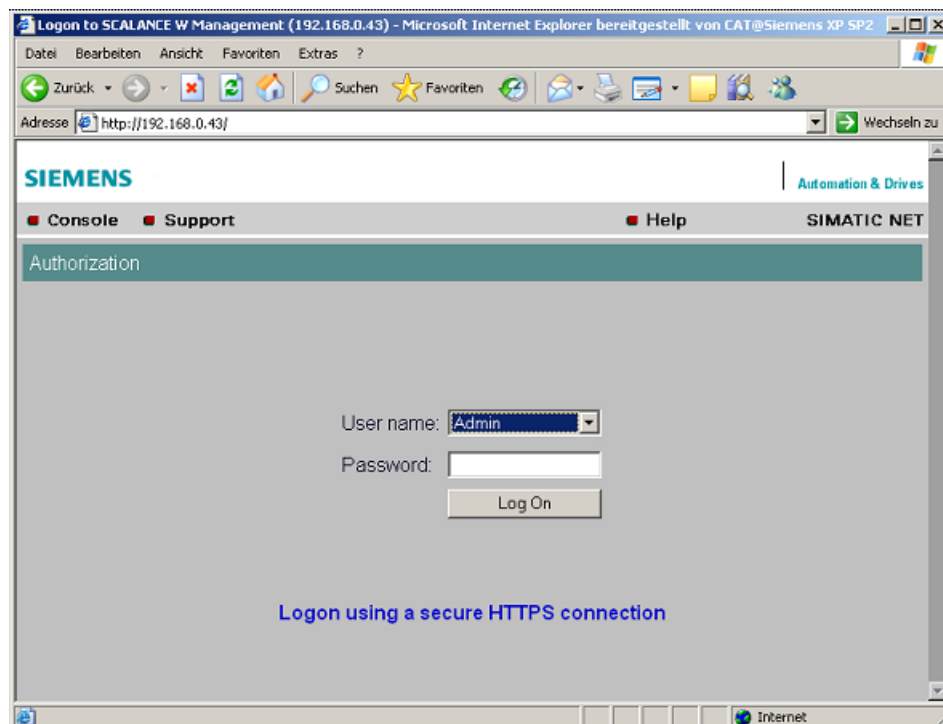
2. Open the "User name" drop-down list box and select the "Admin" entry if you want to change settings of the IWLAN device (read and write access). If you select the "User" entry, you only have read access to the configuration data of the IWLAN device.

3. Enter your password. If you have not yet set a password, the default passwords as shipped apply: Enter admin if you selected "Admin" as the user name or user if you selected "User".

4. Click the "Log On" button to start the logon.

Note

For the US variant of the IWLAN device, the password for the "admin" user has been changed; it can, however, be obtained from Siemens Support by specialists for professional WLAN installation.

Connection over HTTPS

Web Based Management also allows you to connect to the device over the secure connection of the HTTPS protocol.

Use the "Logon using a secure HTTPS connection" link in the logon screen (see figure above) or enter "https://" and the IP address of the IWLAN device in the address box of the Web browser and confirm with Enter. The "Security Alert" warning is displayed and asks you whether you want to continue the action. Confirm with "YES". The Login dialog of Web Based Management opens.

SSL certificate

You can load your p12 or pfx certificate with Web Based Management. This certificate is used by the HTTPS protocol to authenticate the device with the Web browser. You will find detailed information on the handling of certificates in section "Load & Save".

3.3.3 Selecting the wizards

Basic Wizard, Security Wizard and iPCF-Wizard

Web Based Management provides several wizards that allow straightforward commissioning without detailed knowledge of wireless technology. A wizard consists of a series of screens in which you enter the basic configuration data.

The following wizards are available:

- **Basic Wizard**
  For general settings to ensure the basic functionality of the device.

- **Security Wizard**
  The wizard for the security settings supports you when setting security-related parameters.

- **iPCF Wizard**
  This wizard is available for configuring iPCF (industrial Point Coordination Function).

Note

The iPCF Wizard is available only for the following device variants:
- SCALANCE W747-1
- SCALANCE W747-1RR
- SCALANCE W78x-xRR in client mode

Wizard status

After selecting the "Wizards" menu on the left-hand side of the dialog, the status of the wizards is displayed. When you have worked through a wizard completely, "Done" is displayed as the status. When you have worked through all the wizards, the "Wizards" entry also moves to the bottom end of the menu.
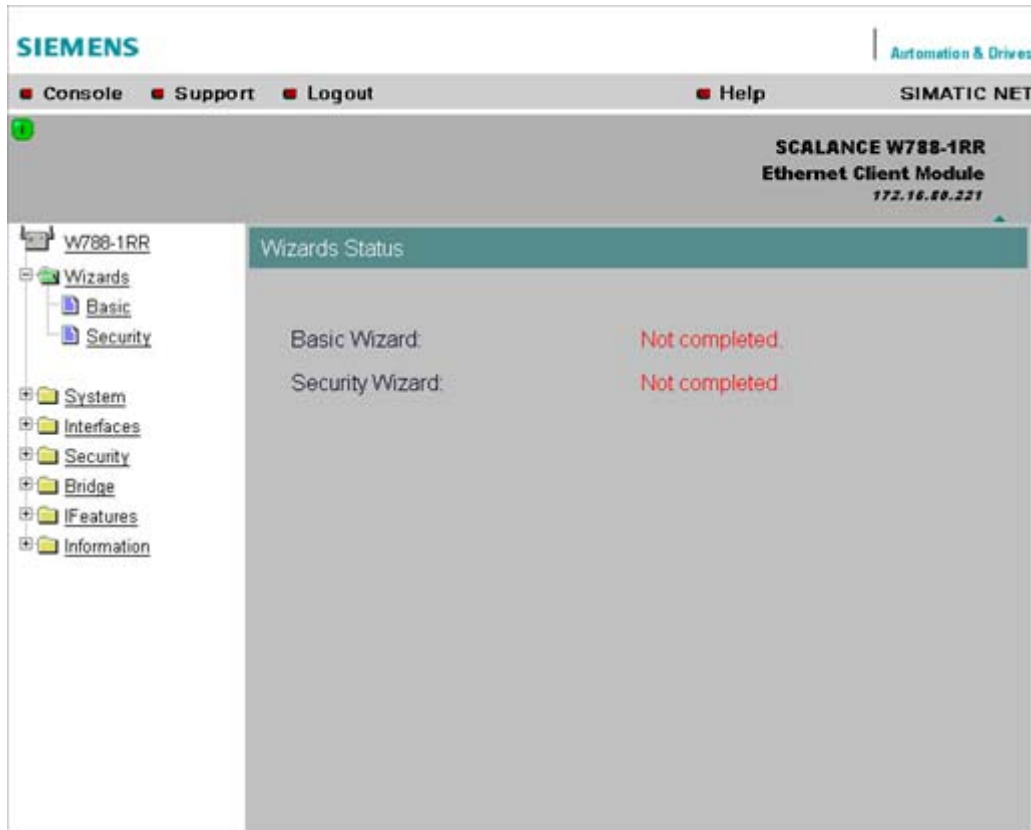
Note

Some pages of the wizards have a different content in access point mode and "Client" mode. In this case, there is a separate description for the alternatives.

You can specify the mode in the "System" menu.

3.4 Basic Wizard

3.4.1 IP settings

Description

One of the basic steps in configuration of an Ethernet device is setting the IP address. The IP address identifies a device in the network uniquely. On this page, you enter the information for the IP configuration of the IWLAN device.
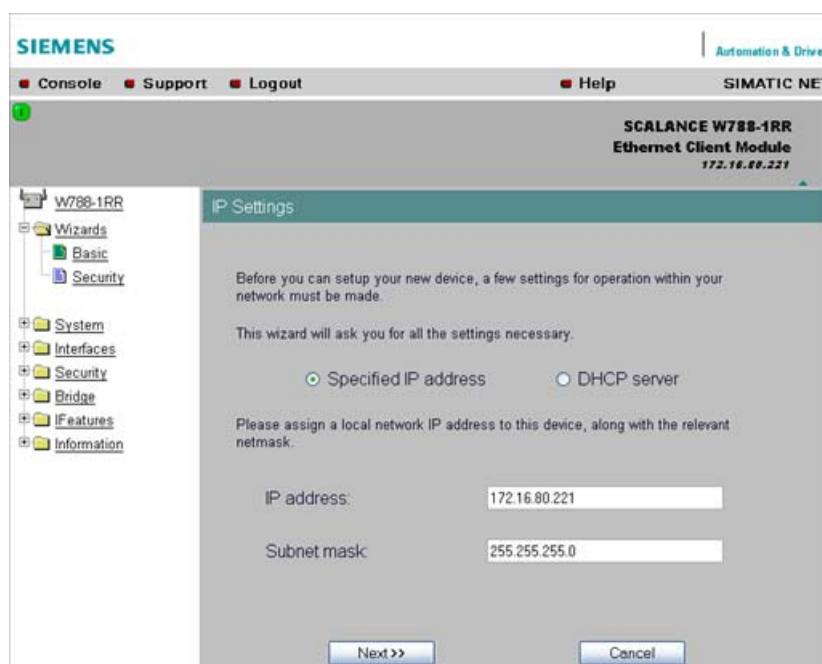
Specified IP address / DHCP server

There are two methods of assigning IP addresses to devices: The IP address can be set as a fixed permanent address or can be obtained dynamically from a DHCP server. Select "Specified IP Address" if you do not use a DHCP server.

IP address

The IP address of the IWLAN device. Here, you enter an address that is unique within the network.

Subnet mask

The subnet mask specifies the range of addresses within which communication can take place.

The four numbers of an IP address separated by periods are interpreted as a bit pattern. If a one is set at a bit position within the subnet mask, this means that only devices with an IP address that matches the IP address of the IWLAN device at this bit position can communicate with the IWLAN device management agent.

Example

Let us assume that the IP address of the IWLAN device is set to 192.168.147.189 and the subnet mask is set to 255.255.255.0. The bit pattern for 255 is 1111 1111. This means that the bit pattern of the first number of the IP address of a communication partner must match the bit pattern of the IWLAN device exactly at this point. The same applies to the second and third parts of the IP address. The IP address of a communication partner must therefore start with 192.168.147. The bit pattern of 0 is 0000 0000. This means that the bit pattern of the last part of the IP address of the partner device does not need to match the address of the IWLAN device at any point; in other words, it can be any number.

Note

Please note the following special feature if the IP address of a gateway was entered in the configuration of the SCALANCE W-700: If you assign an IP address to the SCALANCE W-700 that does not match the subnet mask, the IP address of the gateway will be reset to 0.0.0.0.

Example:
The subnet mask is 255.255.255.0 and you change the IP address of the SCALANCE W-700 from 192.168.147.189 to 192.168.148.189. This would reset the IP address of the gateway to 0.0.0.0.

3.4.2 System name

Description

The system name identifies a network node but means more to the user than the IP address.
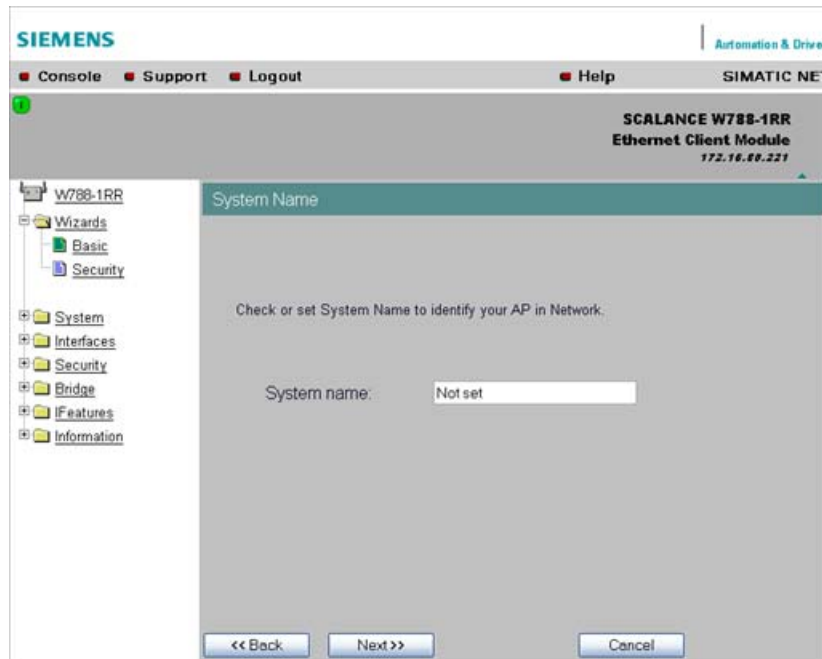
System name

In this box, you enter the system name for your IWLAN device. This parameter corresponds to the "sysName" SNMP parameter. The system name can be up to a maximum of 255 characters long. If you also want to use this parameter for WDS or redundancy, the maximum length is 30 characters.

3.4.3 Country code

___

Note

The correct country setting is mandatory for operation complying with the approvals. Selecting a country different from the country of use can lead to legal prosecution!
___

Description

Some countries have different frequency band divisions for WLAN communication. The regulations for maximum output power also differ from country to country. When you configure the IWLAN device, you must specify which local regulations are relevant for your location. You do this with the "Country Code" parameter.
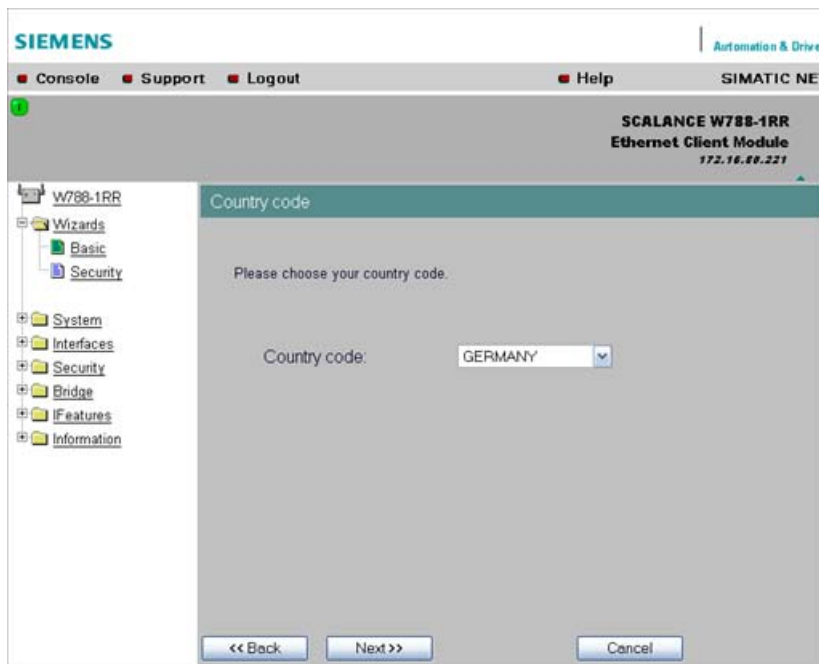
Country Code

In this list box, you select the country in which the IWLAN device will be operated. You do not need to know the data for the specific country, the channel division and output power are set by the IWLAN device according to the country you select.

3.4.4 Wireless settings

Description

On this page, you specify the configuration of the wireless network. This includes the network name and the transmission mode.
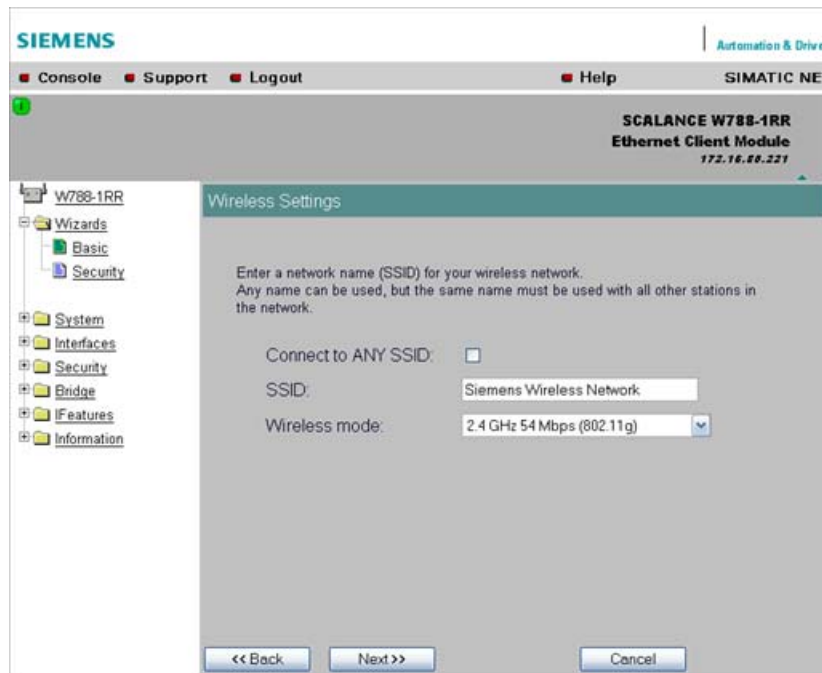
Note

The "Connect to ANY SSID" check box is available only for clients or access points operated in client mode.

Connect to ANY SSID

When this check box is selected, the client connects to the access point that allows the best possible data transfer and to which a connection is permitted based on the security settings.

SSID

Enter the name of your network in this box. The IWLAN device allows all characters except the percent character for the SSID. To ensure compatibility with partner devices, you should, however, not use any characters that are peculiar to a particular language (for example special German characters ä, ö etc.) or special characters in general. The string for SSID can be a maximum of 32 characters long.

Wireless Mode

Select a wireless mode that is supported by all partner devices.

With access points having more than one wireless interface, it is sometimes an advantage if you set a different transmission mode for each wireless interface. This provides ideal support for different clients. The effect of the *802.11.b + g* setting is that all the settings in the *Advanced G* menu are taken into account as far as possible but that compatibility with devices conforming to IEEE 802.11 b guaranteed.

3.4.5   Adopt MAC Address settings (only for clients or access points in client mode)

Assigning the MAC address

A MAC address must be specified for the device connected to the Ethernet port of the client or the access point in client mode before it can be reached. This MAC address is used by the client for wireless communication with the access point.

There are several ways in which this can be done:

* If there is precisely one MAC address to be served downstream from the client, there are two ways of doing this:

    – Automatically
      The client adopts the source MAC address of the first frame that it receives over the Ethernet interface.

    – Manual entry by the user.

* If there are up to eight MAC addresses to be served downstream from the client, "Layer 2 Tunnel" can be used:

This setting meets the requirements of industrial applications in which MAC address-based communication is required with several devices downstream from the client. Clients with this setting cannot connect to standard Wi-Fi devices and access points with firmware V3.0 or older.

Note

The "Layer 2 Tunnel" setting is only available for clients and for access points in client mode.

Note

IP mapping table

If "Layer 2 Tunnel" is configured for a client, the IP mapping table is not displayed.

The following devices can provide several Ethernet devices with access to a wireless network (IP mapping):

- SCALANCE W746-1PRO

- SCALANCE W746-1 and

- SCALANCE W747-1RR

- SCALANCE W747-1

- Access points operating in client mode

For an access point with MAC filtering, only one MAC address is visible to the client, there can be no filtering according to the MAC addresses of the Ethernet devices.

Note

Configuration limits

Several MAC nodes (for example PROFINET IO devices) are connected to the Ethernet interface of a client module and the "MAC mode" parameter is set to "Layer 2 Tunnel". The following configuration limits apply for reliable communication:

- No more than 8 nodes may be connected downstream from the L2T client.

- When transferring cyclic PROFINET IO data in iPCF mode, remember that the sum of the user data of all nodes connected to the client must not exceed a value of 2,300 bytes per cycle. This also includes the frame header. A SIMATIC user must therefore take into account not only the net data during configuration but also the headers.

MAC mode

Here, select how the client obtains a MAC address. The following are possible:

- **Auto find 'Adopt MAC'**
  The client automatically adopts the source MAC address of the first frame that it receives over the Ethernet interface.

- **Set 'Adopt MAC' manually**
  You enter the MAC address manually.

- **Adopt own MAC** (not supported by device variants SCALANCE W744-1PRO and W744-1)
  The client uses the MAC address of the Ethernet interface for the WLAN interface.

- **Layer 2 Tunnel** (not supported by device variants SCALANCE W744-1PRO and W744-1)
  The client uses the MAC address of the Ethernet interface for the WLAN interface. The network is also informed of the MAC addresses connected to the Ethernet interface of the client. Up to eight MAC addresses can be used.
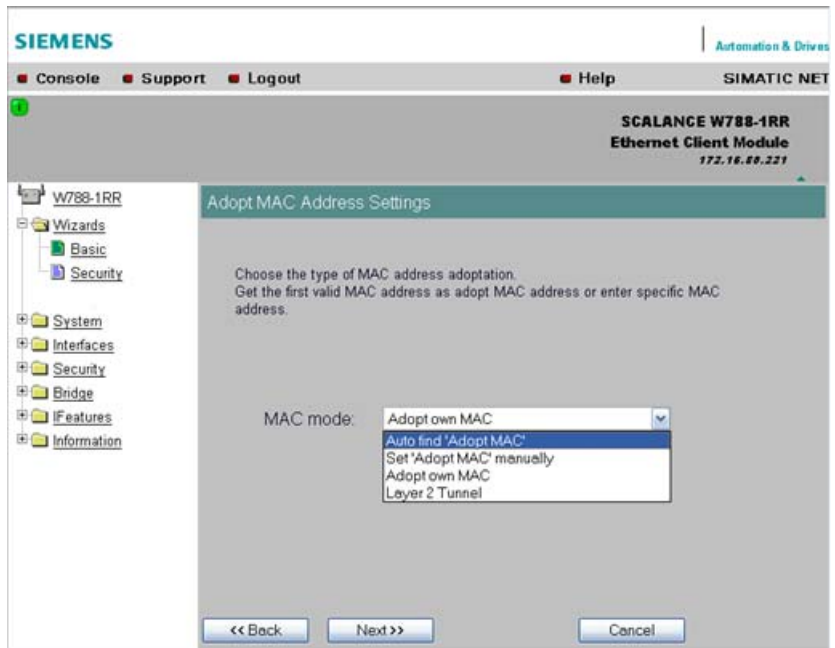
Adopt MAC

If you have selected the "Set 'Adopt MAC' manually" check box, here you will need to enter the MAC address of the device connected over Ethernet to the access point operating in client mode.

If you do not want layer 2 communication (layer 2 tunnel) to be handled over the access point operating in client mode, but only want higher-layer IP-based frames sent to one or more connected devices, you can also leave the default setting "Adopt Own Mac". In this mode, the client registers with the MAC address of its Ethernet adapter. The IP packets are broken down according to an internal table and forwarded to the connected devices.

The "Adopt MAC" box is hidden in the "Auto find 'Adopt MAC' " and "Layer 2 Tunnel" modes.

3.4.6 Channel settings

Description

An access point uses a specific channel within the frequency band for communication. You can either set this channel specifically or configure the access point so that the channel is selected automatically. A specific channel must be set, for example, in the following situations:

● Communication suffers from interference from another device (for example microwaves) or another wireless network.

● Use of the redundancy function. In this case, two well spaced channels or two different frequency bands must be selected (only in access point mode).

● Use of WDS. In this case, select a problem-free channel that is also used by the WDS partner (only in access point mode).

Outdoor AP/Client mode

Select this check box to enable the outdoor AP / client mode.

Auto Channel Select (in access point mode only)

Select this check box if you do not have any particular requirements regarding channel selection.

Radio Channel (in access point mode only)

Here, you select a channel suitable for your application. You can only select from this list if the "Auto Channel Select" check box is not selected. The entries in the list box depend on the previous selection made in the "Country code" box and on the mode (IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11h).

Antenna Type (only for devices with external antennas)

Select the type of external antenna connected to the device.

Antenna gain (in dBi) (only for devices with external antennas)

If you selected the "User defined" entry in the "Antenna Type" drop-down list box, you can enter the antenna gain manually in the unit "dBi".

Antenna cable length (in meters) (only for devices with external antennas)

Enter the cable length between the device and the external antenna in meters.

Note

When the devices are supplied, the WLAN interfaces are deactivated (exception IWLAN/PB Link PN IO). You can use these interfaces after you have worked through the Basic Wizard.

Note

If you use a second or third WLAN interface, make sure that you have adequate channel spacing.

3.4.7 Closing the Basic Wizard

Description

This page displays the parameters you have selected when you have completed all the entries for the basic configuration. "Adopt MAC Address" is displayed only for an access point in client mode.
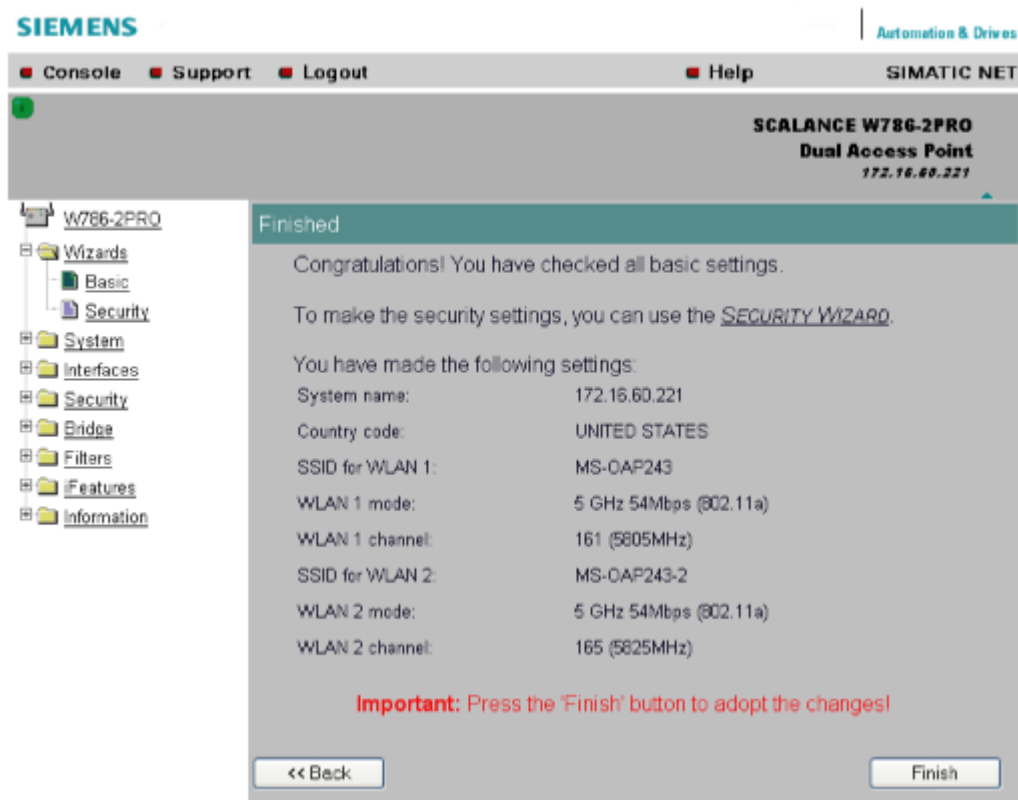
Finish

Click this button to close the Basic Wizard and to log on again with the modified IP address.

3.5 Security Wizard

3.5.1 Introduction

With the Security Wizard, you can specify security-related parameters without detailed knowledge of security technology in wireless networks.

Note

The IWLAN device can be operated even if you do not set the security parameters. Depending on the properties of your network, there is then, however, an increased risk of unauthorized access. You should therefore work through all the pages of the Security Wizard, so that you have at least basic security functions.

3.5.2 Security settings

Password

First, set a new admin password. Enter the string twice in the text boxes of this page. The password can be up to a maximum of 31 characters long.

Note

Permitted characters

When assigning the password, ASCII code 0x20 to 0x7e is used. The following characters are supported:

- The digits 0 to 9
- The letters abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ
- The special characters !$#%&'()*+,-./:;<=>?@[\]^_`{|}~ and the space

Until you set a password, the defaults set in the factory apply: The default password for the "admin" user is "admin". You can use the wizards only if you log on as administrator.

Note

For the US variant of the IWLAN device, the password for the "admin" user has been changed; it can, however, be obtained from Siemens Support by specialists for professional WLAN installation.
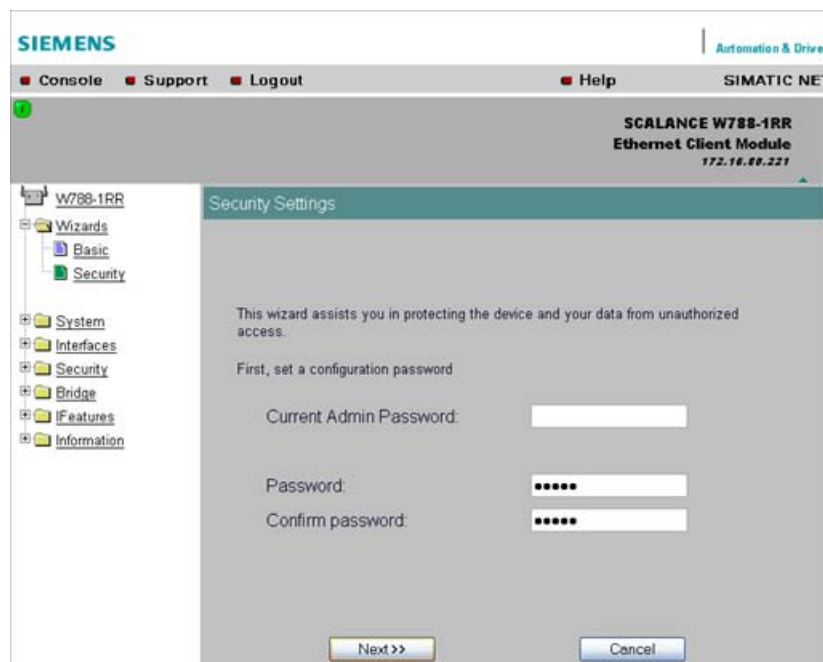
3.5.3 Security settings for the management interfaces

Protocols for configuration

In this page, you specify the protocols with which you can access the configuration of the IWLAN device. All protocols with a selected check box can be used for configuration. You should only select protocols that you actually use.

The protocol settings only take effect after exiting the Security Wizard and restarting. Even after selecting the "Web Based Management" entry, you still have the option of returning to earlier pages or exiting the wizard.

Specifying the network type for configuration

It is easier to restrict access to a wired network than to a wireless network. Web Based Management allows access to the IWLAN device for configuration to be restricted to computers linked to the IWLAN device by a cable. If you require this, check the box at the bottom of the page.
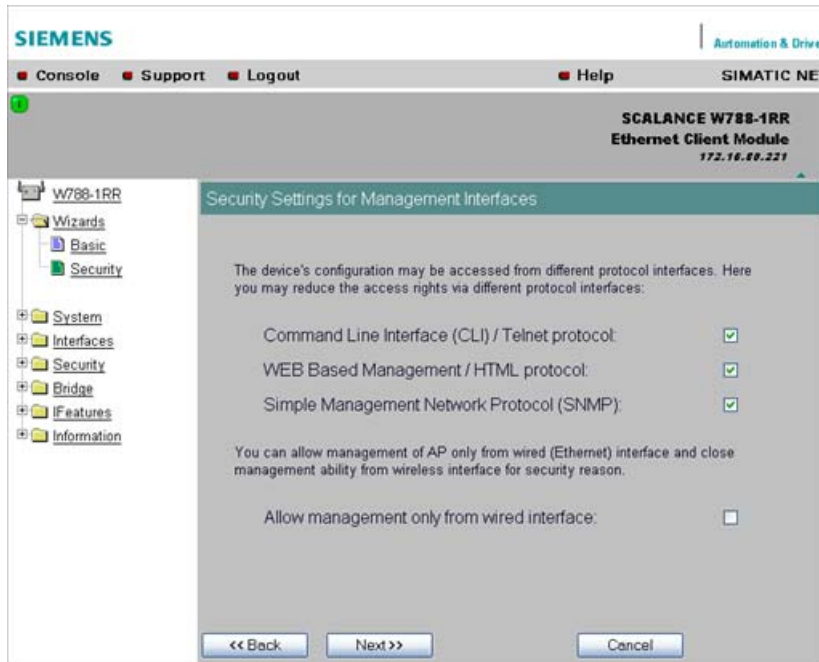
3.5.4   Security settings for the SNMP protocol

Access permissions when using the SNMP protocol

When using the SNMP protocol, you specify access permissions by means of the community string. A community string effectively combines the function of user name and password in one string; different community strings are defined for read and write permissions. More complex and more secure authentications are possible only in some SNMPv2 variants and in SNMPv3.

To preserve security, you should not use the default values "public" or "private".
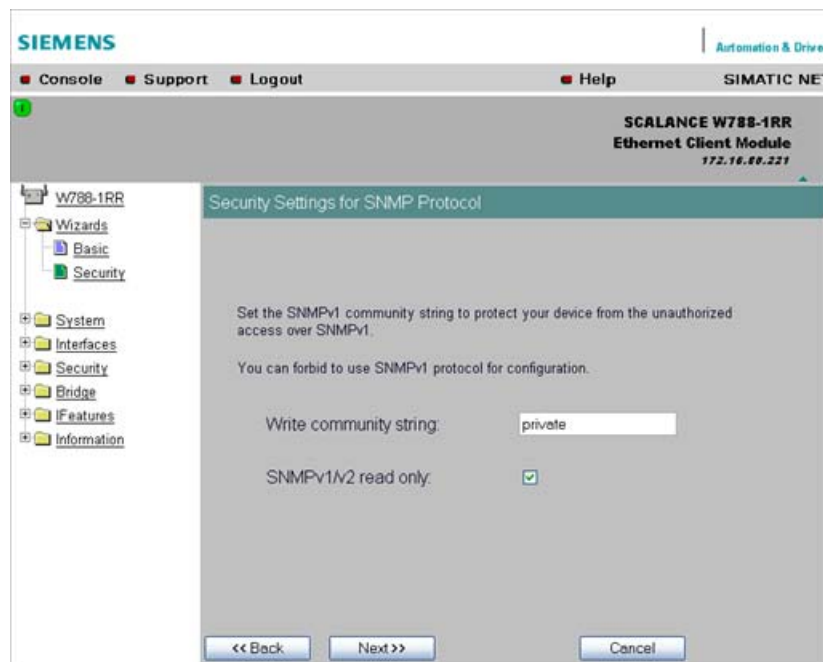
Write Community String

Here, you enter the write community string (maximum of 63 characters) for the SNMP protocol.

SNMPv1/v2 Read Only

If you select this check box, only read access is possible with the SNMP protocol V1 or V2.

3.5.5   Security settings for WLAN (page 1, only in access point mode)

Description

On this page, you make the security settings, including, for example, the authentication and encryption. If you configure a model with several wireless adapters, this page appears for each adapter. You can make different settings for each wireless adapter.

Network-specific security settings

On the first page of the security settings, you select settings that apply regardless of protocol-specific restrictions. The basic measures for securing a network against unauthorized access involve

● allowing only certain clients (those that have entered the network name (SSID) of the AP) to communicate with the access point.

● excluding clients that communicate over wireless connections from the wired part of the network.
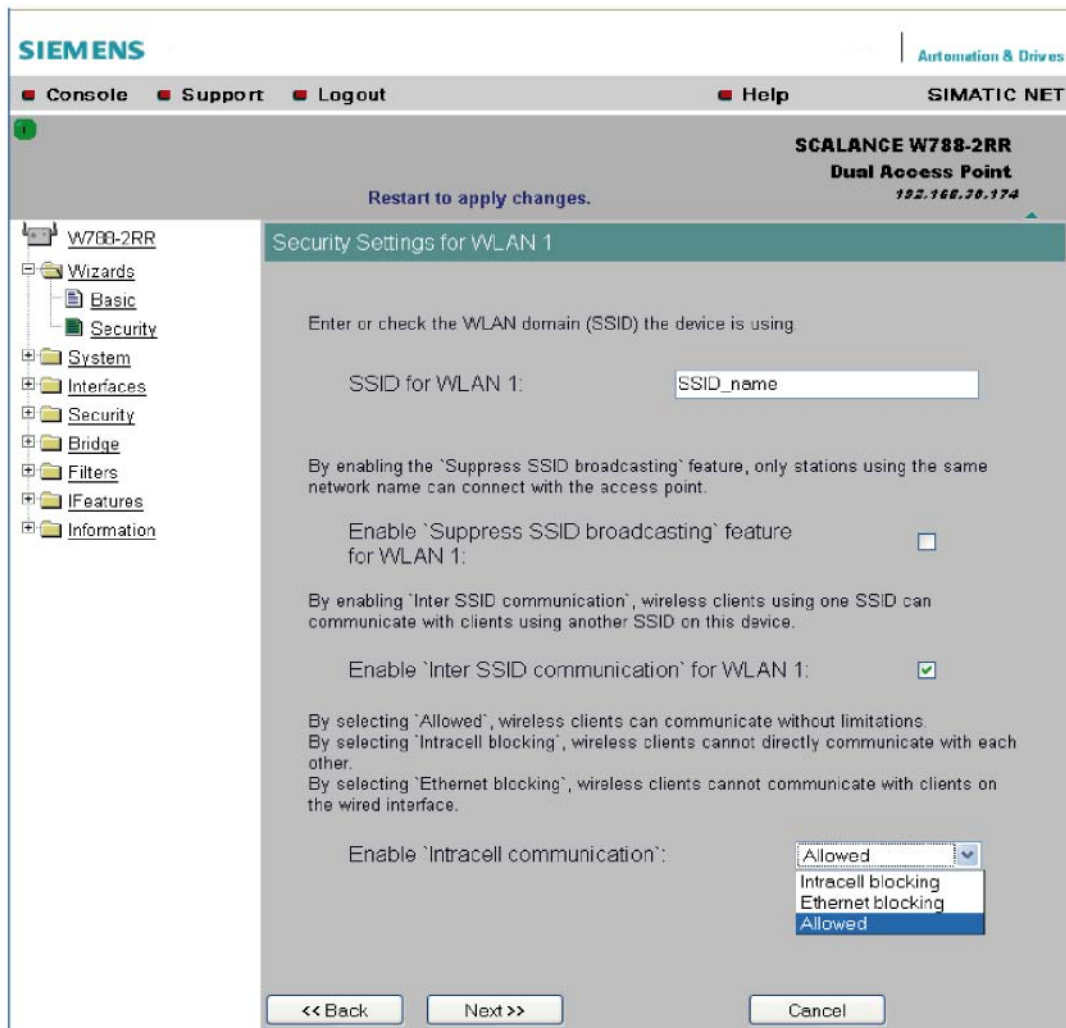
SSID for WLAN 1

Enter the name of your network in this box (maximum of 255 characters, 32 characters if you use the redundancy function). To avoid possible conflicts, this name should not include any umlauts (ä, ü, ö etc.).

Enable 'Suppress SSID broadcasting' feature for WLAN 1

Selecting this option means that the SSID is not visible for other devices. For this reason, the only stations that can connect to the access point are those that have the same name as was configured for the access point.

Note

Since no encryption is used for the SSID transfer, this function can only provide basic protection against unauthorized access. The use of an authentication method (for example WPA (RADIUS) or WPA-PSK if this is not possible) provides higher security. You must also expect that certain end devices may have problems with access to a hidden SSID.

Enable 'Inter SSID communication' for WLAN 1

Selecting this option allows communication between WLAN clients registered at different SSIDs of an access point.

Example 1	A SCALANCE W786-3PRO was defined with different SSIDs.
Example 2	A SCALANCE W788-1PRO is used with multiple SSIDs.

Note

On an access point, the Inter SSID communication function must be enabled on all WLAN interfaces or on all VAPs to allow communication between the clients with different SSIDs.

Note

If VLANs are configured for the SSIDs, this setting can prevent communication between the SSIDs according to the VLAN rules.

Enable 'Intracell communication'

With this drop-down list box, you can make the following settings:

- **Intracell blocking**
  This setting prevents WLAN client communication within an SSID.

- **Ethernet blocking**
  This setting prevents WLAN client communication over the Ethernet interface of the access point.

- **Allowed**
  This setting enables both WLAN client communication within an SSID as well as WLAN client communication over the Ethernet interface.

Overview of the communication options

To illustrate the situation, there is an overview of the effects of the "Inter SSID communication" and "Intracell communication" settings below.

Settings		Possible communication		
Inter SSID communication	Intracell communication	within an SSID	with another SSID	to the Ethernet network
Enabled	Allowed	x	X	X
Enabled	Intracell blocking		X	X
Enabled	Ethernet blocking	X	X	
Disabled	Allowed	X		X
Disabled	Intracell blocking			X
Disabled	Ethernet blocking	X		

3.5.6 Security settings for WLAN (page 2)

Predefined security levels

Authentication and encryption are tried and tested methods for increasing security in networks. Web Based Management provides four predefined security levels that specify suitable methods.
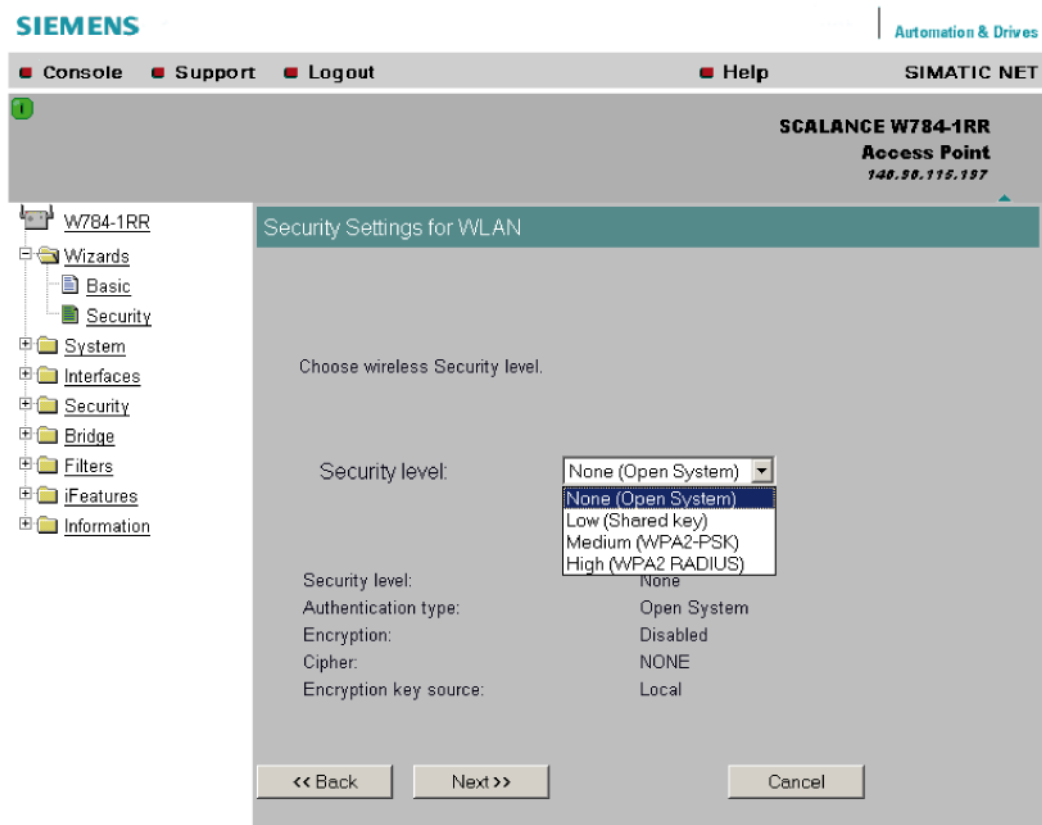
The following table indicates what the various security levels involve:

Visible in wizard	Security level	Authentication	Encryption	Type of encryption	Encryption key source
X	None	Open System	disabled	without	not applicable
	None	Open System	enabled as option	WEP	local
X	Low	Shared Key	enabled	WEP	local
X	Medium	WPA2-PSK (preshared Key)	enabled	TKIP / AES / AUTO	local
X	High	WPA2 (RADIUS)	enabled	TKIP / AES / AUTO	Server
	Medium	WPA-Auto-PSK (preshared Key)	enabled	TKIP / AES / AUTO	local
	High	WPA-Auto (RADIUS)	enabled	TKIP / AES / AUTO	Server

Authentication

Authentication basically means that some form of identification is required. Authentication therefore protects the network from unwanted access. In the "Security Level" box, you can choose between the following types of authentication:

- **None (Open System)**
  There is no authentication. Encryption with a fixed (unchanging) key can be selected as an option. To do this, define a key in the "Keys" menu. 5 or 13 ASCII or 10 or 26 hexadecimal characters specify a weaker key (40/104 bits). 16 ASCII or 32 hexadecimal characters, on the other hand, define a strong key (128 bits). Then select "Encryption" in the "Basic WLAN" menu.

- **Low (Shared Key)**
  In Shared Key authentication, a fixed key is stored on the client and access point. This is then used for authentication and encryption. In this case, you will have to store a WEP key after selecting "Low (Shared Key)".

- **Medium (WPA2-PSK)**
  WPA2-PSK is based on the WPA2 standard, WPA authentication, but operates without a RADIUS server. Instead of this, a key (pass phrase) is stored **on every** client and access point and this is used for authentication and further encryption. AES or TKIP is used as the encryption method, AES represents the standard method.

- **High (WPA2)**
  WPA2 (WI-File Protected Access 2) is a further development of WPA and implements the functions of the IEEE 802.11i security standard. WPA2 uses the additional encryption protocol CCMP with preauthentication that allows fast roaming in mobile ad hoc networks. A client can log on in advance at several access points so that the normal authentication can be omitted.
  A RADIUS server is used to authenticate the client with an access point. The client logs on at a RADIUS server based on a certificate (EAP-TLS) or a combination of user name and password (EAP-PEAP or EAP-TTLS / internal authentication method MSCHAPv2). As an option, the RADIUS server then identifies itself to the client using a certificate. Following successful authentication, the client and RADIUS server generate key material that is used for data encryption. AES or TKIP is used as the encryption method, AES represents the standard method.

- **Medium with WPA compatibility (WPA-Auto-PSK)**
  Select the "Medium" security level and check the "WPA compatibility"
  box so that an access point can process both "WPA-PSK" authentication as well as "WPA2-PSK". This is necessary when the access point communicates with different clients, some using "WPA-PSK" and others "WPA2-PSK". The same encryption method must be set on the clients.

- **High with WPA compatibility (WPA-Auto)**
  Select the "High" security level and check the "WPA compatibility"
  box so that an access point can process both "WPA" authentication as well as "WPA2". This is necessary when the access point communicates with different clients, some using "WPA" and others "WPA2". The same encryption method must be set on the clients.

Encryption

Encryption protects the transferred data from eavesdropping and corruption. You can only disable encryption in the "Encryption" check box if you have selected "Open System" for authentication in the "Basic WLAN" menu. All other security methods include both authentication and encryption. Various schemes are used for encryption:

- **WEP** (**W**ired **E**quivalent **P**rivacy)
  A weak, symmetrical stream encryption method with only 40- or 104-bit long keys based on the RC4 algorithm (Ron's Code 4).

- **TAKING** (**T**emporal **K**ey **I**ntegrity **P**rotocol)
  A symmetrical stream encryption method with the RC4 algorithm (Ron's Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted packets.

- **EASY** (**A**dvanced **E**ncryption **S**tandard)
  Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TAKING.

- **AUTO**
  TAKING or EASY is used depending on the capability of the other station.

Encryption key source

The encryption key source indicates whether the key is configured locally and fixed (local) or whether it is negotiated by a higher protocol and an authentication server (server).

Security Level for WLAN

Select a security level that is supported by all clients. The content of the next page depends on the selected security level. If you select the security level "None", there is no following page since neither encryption nor authentication will be used.

3.5.7   Settings for the Low security level
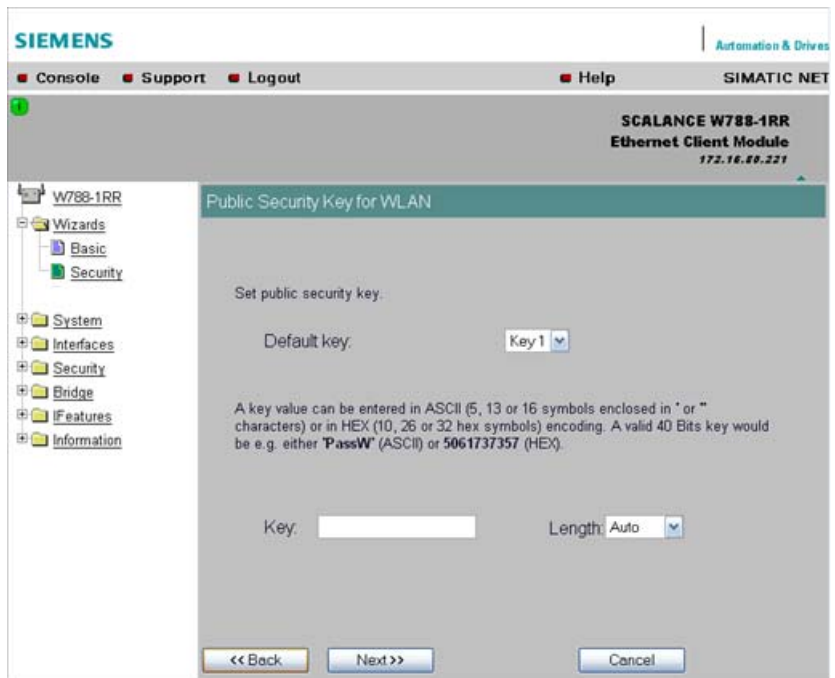
Default key

Select the key you want to specify.

Key

Enter the character string for the key here. The key can be entered as ASCII characters or alternatively as hexadecimal digits (0 – F). If the key was entered in ASCII format, this is later displayed in quotes.

Length

Select the key length you want to use here. If the length of the string in the Key input box is longer or shorter than the selected key length, an error message is displayed. The following key lengths are possible:

- 40 bits (5 ASCII characters or 10 hexadecimal numbers)

- 104 bits (13 ASCII characters or 26 hexadecimal numbers)

- 128 bits (16 ASCII characters or 32 hexadecimal numbers)

With the "AUTO" setting, the maximum key length is also 128 bits.

3.5.8 Settings for the Medium security level
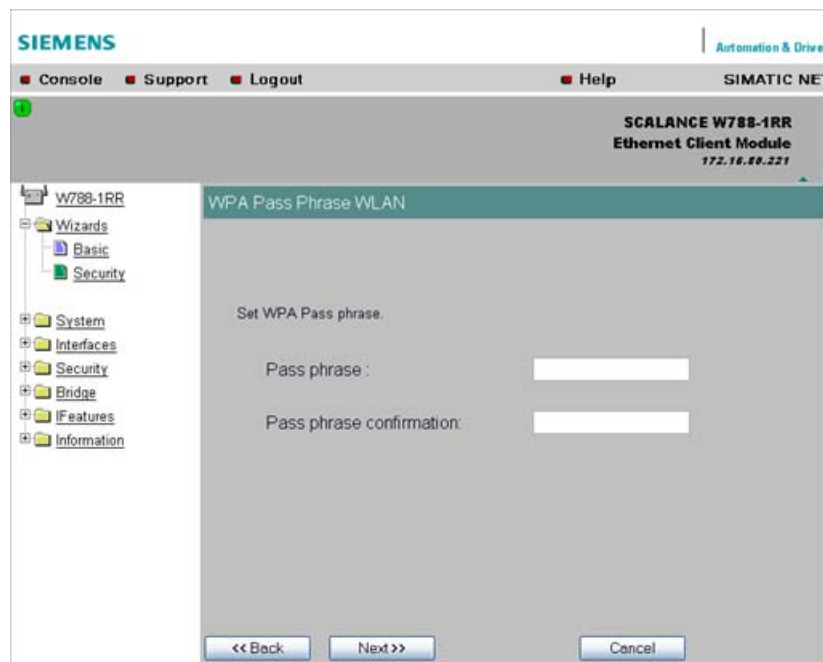
Pass phrase

Here, you enter a WPA(2) key. The key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. This initialization key must be known on both the client and the access point and is entered by the user at both ends.

Pass phrase confirmation

Here, you confirm the entered WPA(2) key.

Note

The key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. It should be selected so that is complex for example consisting of random numbers, letters (upper-/lowercase), have few repetitions and special characters. Do not use known names, words or terms that could be guessed. If a device is lost or if the key becomes known, the key should be changed on all devices to maintain security.

3.5.9 Settings for the High security level in access point mode
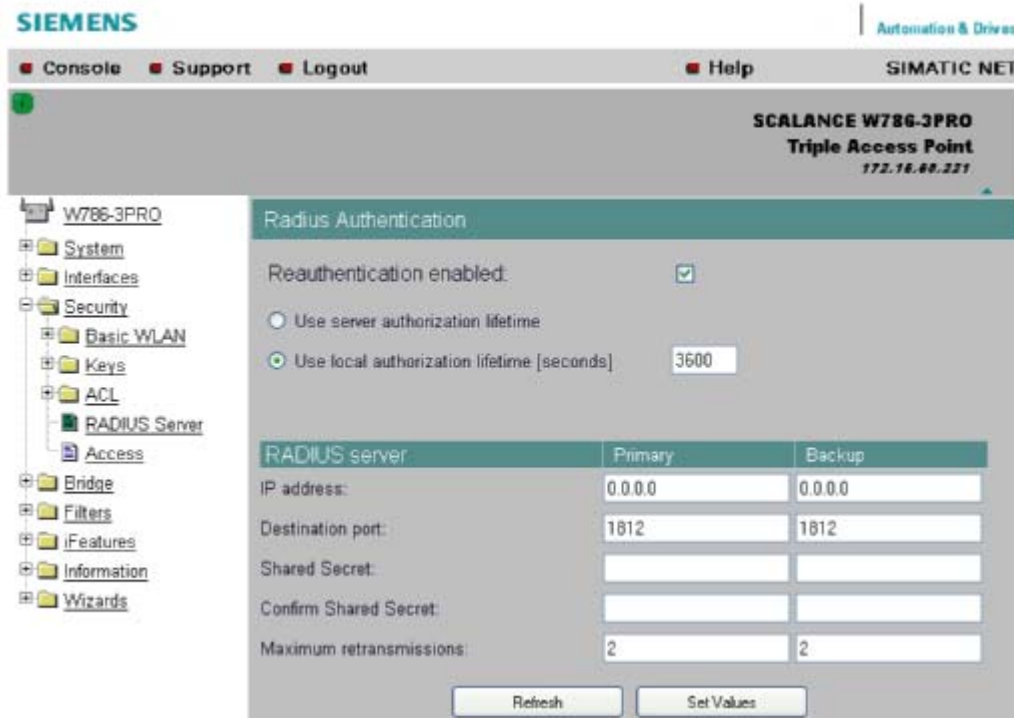
Reauthentication

Here, you decide whether the access point initiates a reauthentication for the clients. You can also select who sets the time after which the clients are forced to a reauthentication. If time management is local, enter the period of validity of the authentication in seconds. The minimum time is 1 minute (enter 60), the maximum time is 12 hours (enter 43200). The default is 1 hour (3,600 seconds).

RADIUS Server

You can enter the data for two RADIUS servers; the information in the "Backup" column is used if the server defined in the "Primary" column is not available. In this table, you can specify a password for the IP address and the destination port. The entry must be entered twice as confirmation. In the bottom input box, you enter the maximum number of attempted transfers.

3.5.10 Settings for the High security level in "Client" mode

Note

The following information applies only to clients or access points operating in client mode.
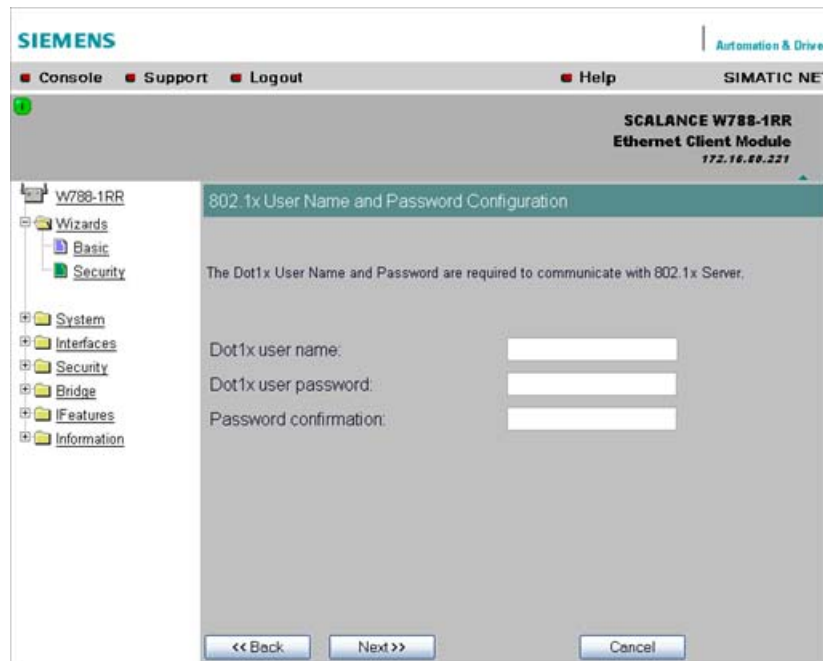
Dot1x user name

Here, enter the user name with which you want to register over the RADIUS server.

Dot1x user password

Here, enter the password for the above user name. The client logs on with the RADIUS server using this combination.

Password confirmation

Confirm the password here.

3.5.11 Overview of the selected settings

Settings after working through the Security Wizard

This page contains an overview of the selected security settings. If you want to change a setting, you can click the "Back" button to return to a previous page where you can enter a different value or make a different selection. The content of this page depends on whether the Wizard was used for an access point or a client or for an access point in client mode.

The security settings for a client or an access point in client mode do not display the following parameters:

- SSID for WLAN
- Suppress SSID broadcasting for WLAN
- Inter SSID communication for WLAN
- Intracell communication for WLAN
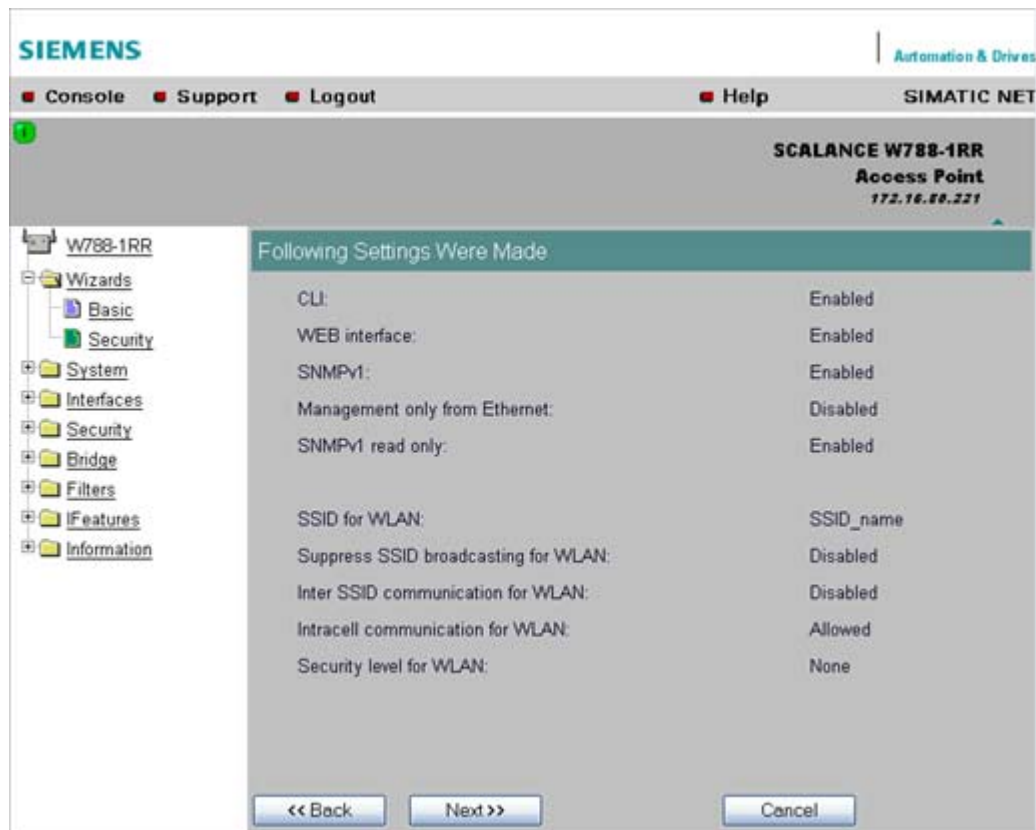
3.5.12 Exiting the Security Wizard

Further security settings

The last page of the wizard indicates other security measures that you can take. If you still want to make final modifications, you can open the relevant pages by clicking on the highlighted texts. The content of this page depends on whether the Wizard was used for an access point or a client or for an access point in client mode.

Finish

Click the "Finish" button to exit the Wizard. Your settings only take effect after you have restarted (*System > Restart* menu).
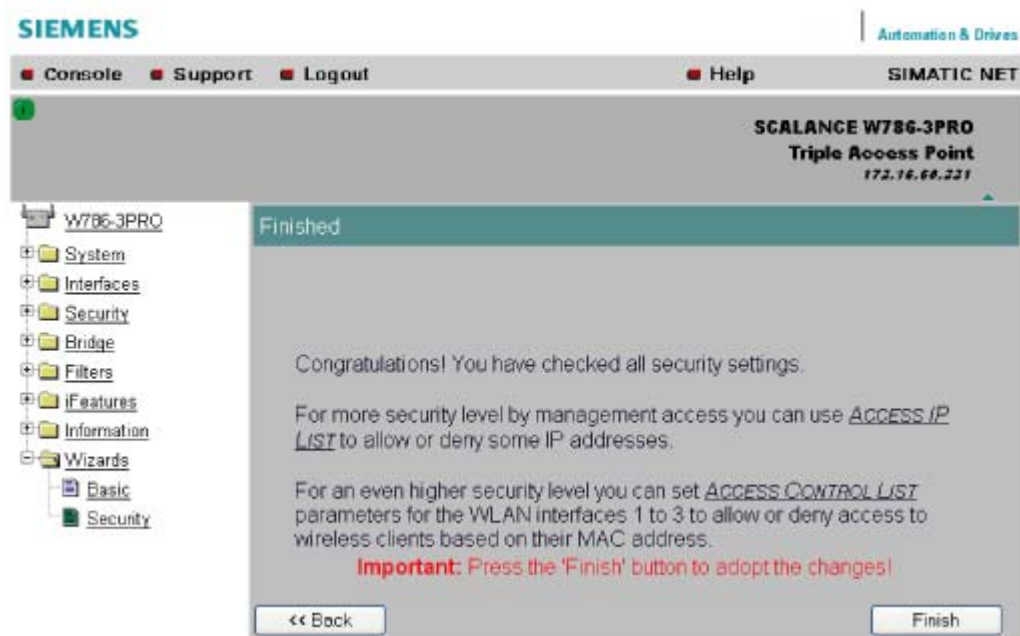
3.6 iPCF Wizard

3.6.1 Notes on the iPCF Wizard

Note

The iPCF Wizard is available only for the following device variants:

• SCALANCE W747-1
• SCALANCE W747-1RR
• SCALANCE W78x-xRR in client mode

Note

The iPCF Wizard also includes pages for specifying security settings. If you use iPCF, you do not therefore need to work through the Security Wizard.

3.6.2   industrial Point Coordination Function settings

Channel selection and transmit power

On this page, you make the setting is necessary for iPCF. The main advantage of suitable settings is that you can improve roaming times and reduce the interference affecting other systems or segments.

Note

When using iPCF, the following maximum data rates must be taken into account when setting the access point:

Wireless standard maximum data rate

IEEE 802.11a/h: 12 Mbps

IEEE 802.11b: 11 Mbps

IEEE 802.11g: 12 Mbps

Background scan ch. select

The *Background scan ch. select* restricts the number of channels on which the client scans for an access point. This reduces handover times and reduces the risk of real-time violation.

If you select the *Background scan ch. select* option, you also need to enter the channels on which access points in iPCF mode are within range in the next input box *Background scan channels*. If you do not define the channels, the node runs a time-intensive scan throughout the entire band.

Background scan channels

Here, enter the channels on which access points operating in iPCF mode can be reached by the client. If you enter more than one channel, each channel must be separated by a blank.

Transmit power

When using antennas, it may be necessary to reduce the transmit power to avoid exceeding the legal maximum transmit power or to restrict the visibility of the radio link. If necessary, select the required reduction in transmit power here.

A reduction of transmit power may also necessary to avoid interfering with other cells because a reduced transmit power means a reduction in the span of the cell.

Antenna Mode

This list box specifies the use of the antennas.
If "Diversity" is set, the access point uses only the antenna that allows the best possible data transmission. For each WLAN interface, both antennas must be connected. Both antennas should also be of the same type and they should also illuminate approximately the same space. If an access point is operated with the diversity setting and the two antennas span different cells, this can have negative effects.
Otherwise, you will need to select the connected antenna.

Note

If only one antenna is connected, the connected antenna must be set permanently. The second antenna socket must also have a 50 Ω terminator fitted.

3.6.3 Security settings for the WLAN

Security settings with iPCF

On this page, you specify the security level for the client. iPCF is a proprietary standard optimized for fast roaming and deterministic data transfer. With the current security mechanisms 802.1x and WPA, keys are negotiated using relatively time-consuming mechanisms, and they are therefore not available with iPCF.
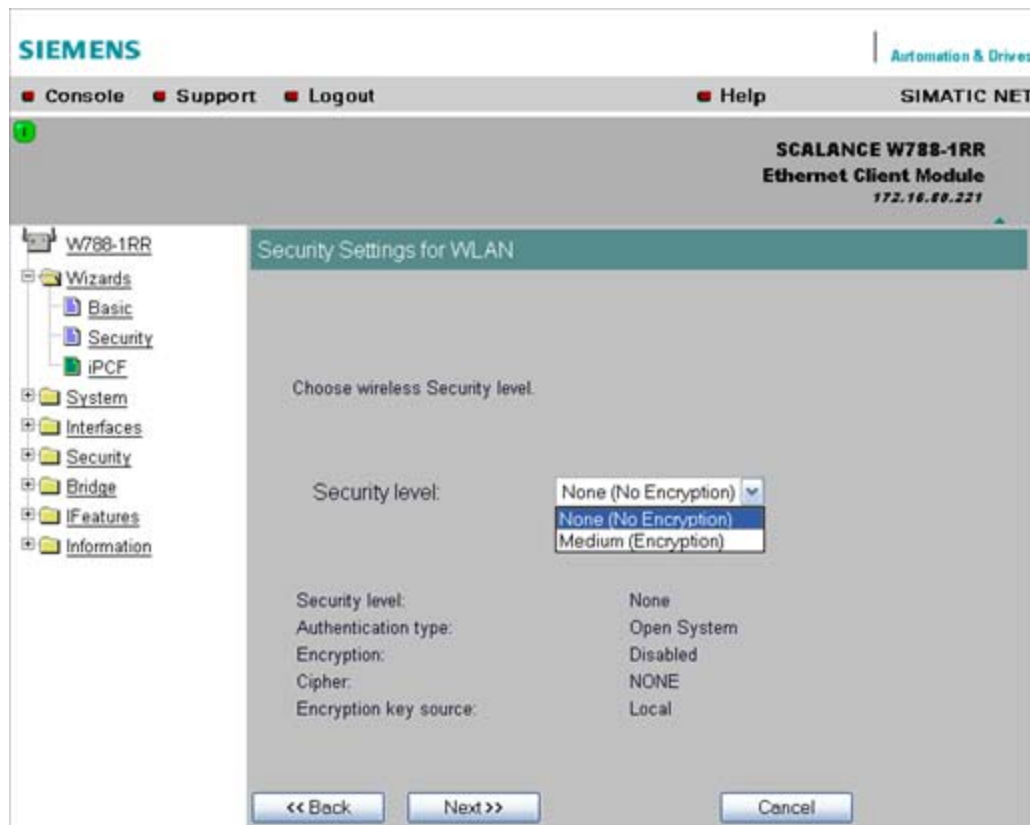
Security level

Select the security level you require for your wireless network in this box. The following are possible:

- **None (no encryption)**
  An open system without encryption.

- **Medium (Encryption)**
  Static keys are used. This is the recommended setting and you should use a 128-bit key.

3.6.4 Public Security Key for WLAN

Specifying the key

If you have selected the security level "Medium", you must specify the key on this page.
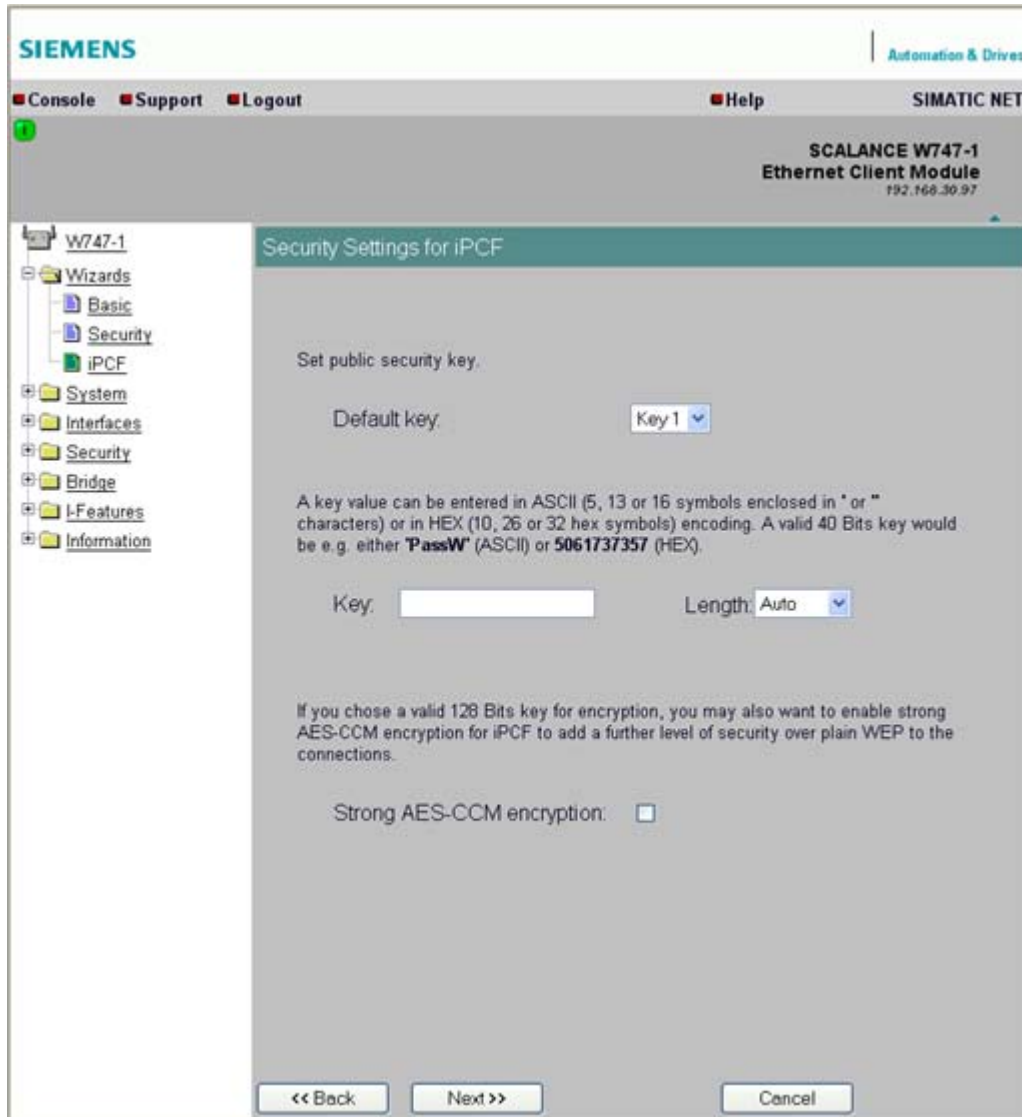
Default key

Select the WEP key you want to specify.

Key

Enter the character string for the key here. The key can be entered as ASCII characters or alternatively as hexadecimal digits (0 – F). If the key was entered in ASCII format, this is later displayed in quotes.

Note

Permitted characters

When assigning the password, ASCII code 0x20 to 0x7e is used. The following characters are supported:

- The digits 0 to 9
- The letters abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ
- The special characters !$#%&'()*+,-./:;<=>?@[\]^_`{|}~ and the space

---

Length

Select the key length you want to use here. If the length of the string in the "Key" input box is longer or shorter than the selected key length, an error message is displayed. The following key lengths are possible:

- 40 bits (5 ASCII characters or 10 hexadecimal numbers)
- 104 bits (13 ASCII characters or 26 hexadecimal numbers)
- 128 bits (16 ASCII characters or 32 hexadecimal numbers)

With the "Auto" setting, the maximum key length is also 128 bits.

Strong AES-CCM encryption

Select this check box if you want to use "Strong EASY-CCM" encryption.
You can only use the encryption method EASY-CCM in iPCF mode. Make sure that a 128-bit WEP key is defined in the "Security > Keys" menu. When you have selected the "Strong AES-CCM encryption" check box, the display in the "Security > Keys" menu changes to "128 bit AES" and the device uses AES-CCM.

3.6.5 Closing the iPCF Wizard

Closing the wizard

The last page of the iPCF Wizard shows you all the settings you have made so that you can make a final check.
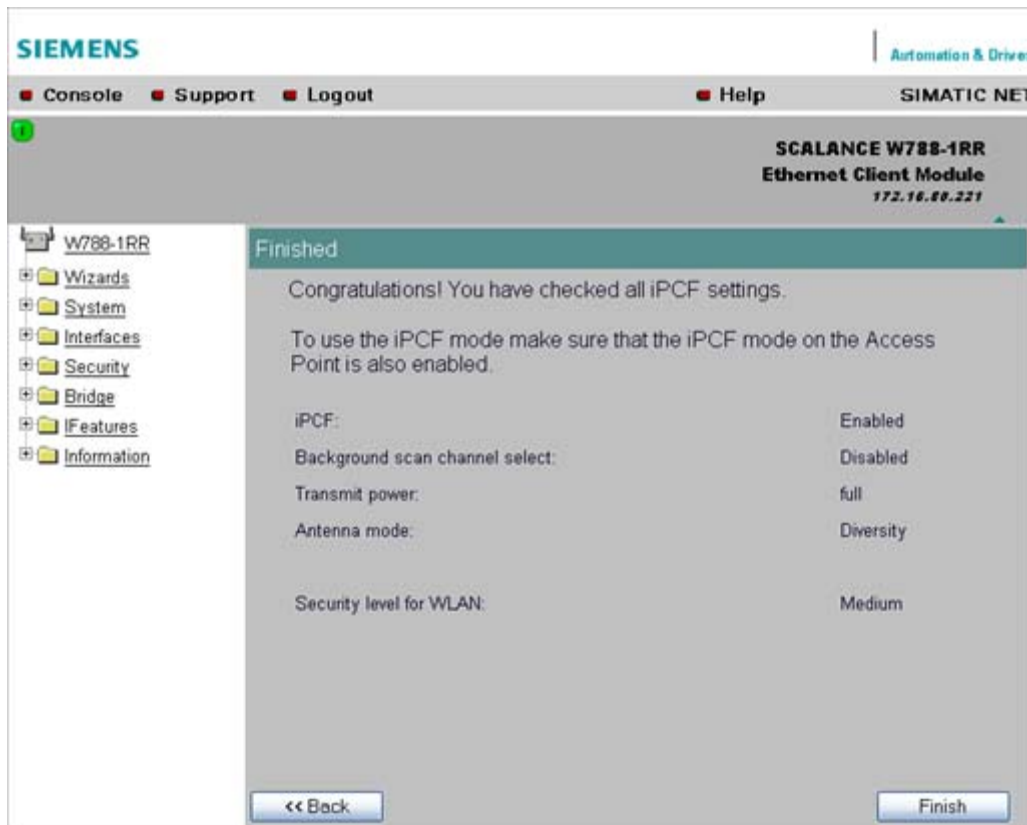
Finish

Click the Finish button to exit the iPCF Wizard. Your settings only take effect after you have restarted (**System > Restart** menu).

3.7 Configuration with Web Based Management

3.7.1 General information on Web Based Management

Navigation bar

You will find the following links in the upper menu bar of Web Based Management (WBM):

- **Console**
  This link opens a console window in which you can enter CLI commands.

- **Support**
  When you click this link, you open a SIEMENS AG support page in the Internet.

- **Logout**
  Close the current Web Based Management session by clicking on this link. The logon dialog is then displayed again.

- **Help**
  Clicking on this link opens the online help of Web Based Management in a separate browser window.

Updating the display with "Refresh"

Web Based Management pages that display current parameters have a "Refresh" button at the lower edge of the page. Click this button to request up-to-date information from the device for the current page.

Storing entries with "Set Values"

Pages in which you can make configuration settings have a "Set Value" button at the lower edge. Click this button to save the configuration data you have entered on the device.

Creating entries with "New"

Pages in which you can create lists have the "New" button at the lower edge. Click this button to create a new entry in the list.

Resetting a counter with "Reset Statistics"

With this button, you can reset the relevant counters.

Note on "User" login

> If you log on as "User", you will only have restricted use of WEB and Telnet. Since you only have read access, some commands do not exist in Telnet and some areas cannot be selected.

RRequired experience

> To be able to use the information in this chapter effectively, you should have a thorough knowledge of network technology and WLANs.

3.7.2   The System menu

3.7.2.1   System Information menu command

Mode and locale setting

> On this page, you make several basic settings for the IWLAN device, for example, the country and mode (access point or client).

Changing the mode of access points

> When the mode changes from access point mode to client mode and back, all the parameters are cleared except:

- IP address
- Subnet mask
- Gateway address
- SSID (only in access point mode)
- IP address of the default router
- DHCP flag
- System name
- System location
- System contact
- Device mode
- Country code
- User and Admin passwords

> The "Current system time" output box informs you about the system time. The "System up time" output box informs you about the time that has elapsed since the last restart.

Reading out the country list

In the address field of the Internet browser, enter
`https://<IP address of the IWLAN device>/countrylist.log`

and confirm with "Enter".

After logging in, you then obtain the country list with the following headers:

```
-----------------------------------------------------------------
COUNTRY   | MODE      | CH    | MHz     | PWR(EIRP)    | USAGE
-----------------------------------------------------------------
```

The table lists the permitted wireless modes and channels along with the corresponding channel frequencies for every possible country setting. The PWR(EIRP) rubric contains the permitted limit values for the transmit power, measured at the antenna. The limit values relate to the transmit power of the access point and the gain of the antenna being used.

Note

In the version for USA, you cannot select a country. The frequency bands for this country are already preset.

Country code

In this list box, you select the country in which the IWLAN device will be operated. You do not need to know the data for the specific country, the channel division and output power are set by the IWLAN device according to the country you select.

Device mode

You can specify whether or not the IWLAN device is used as access point or as client.

Current System time

This box contains information on the system time. The box is displayed only when an SNTP server was specified.

System up time

This box shows the time that has elapsed since the startup of the IWLAN device.

System name

In this box, you enter the system name for your IWLAN device. This parameter corresponds to the "sysName" SNMP parameter. The system name can be up to a maximum of 255 characters long. If you also want to use this parameter for WDS or redundancy, the maximum length is 30 characters.

System location

Enter the location of the IWLAN device, for example a room number.

System contact

Enter the name of a contact person responsible for managing the device in this box.

Description

Specifies the type of the SCALANCE W-700 device.

3.7.2.2 System Identification & Maintenance menu

Device information and device identification

The first part of this page shows information on the device, for example the order number and the firmware version. These text boxes cannot be edited. In the second part, you can enter your own identifiers for the device

Function Tag

Enter information relating to the function of the device here.

Location Tag

Here, you enter information on the location of the device.

3.7.2.3 IP Settings menu command

Configuration

Here, you decide whether you will use a DHCP server or whether you want to assign a fixed IP address to the IWLAN device. You can also set the IP address of a router and the default TTL.

Note

If you use a Radius server for authentication, this must the accessible over the management VLAN.

Specifying the IP address

IP address

Enter the IP address of the IWLAN device in this box.

Subnet mask

Enter the subnet mask for the specified IP address in this box.

Default router IP

Enter the IP address of the router or gateway in this box if you use one.

DHCP server

MAC address

The device identifies itself to the DHCP server based on the MAC address.

System address

The device identifies itself to the DHCP server based on the system name.

Client ID

The device identifies itself to the DHCP server based on the client ID.

Default TTL

The TTL (time to live) parameter specifies the maximum number of routers passed through by a data packet before it is discarded.

3.7.2.4　　Services menu command

Configuration

Here, you select the services with which access to the device will be possible. If, for example, the "SNMP Enabled" check box is not selected, neither write nor read access is possible using the SNMP protocol (v1,v2c,v3). If the SNMP protocol is not permitted, it is not possible to send SNMP traps.

To improve security, you should only enable the services that you actually use.

Note

Over SNMP, it is possible to disable all services and to allow read access only over SNMP. Following this, no further configuration of the device is possible.

If you only want to enable secure access over HTTPS when configuring the device, select the "HTTPS only" check box.
If you want to enable the response of the device to Ping signals, select the "Ping enabled" check box.

With the integrated SSH server, you have secure access to the CLI. In contrast to Telnet, the entire communication including user authentication is encrypted.

Notes on WEB Enabled in the Web Based Management

The "WEB Enabled" check box is selected and inactive because configuration with Web Based Management is no longer possible without the option of access with HTTP.

If you want to deactivate the option of configuration with Web Based Management, you can do this in the Security Wizard over Telnet and SNMP. Settings made using the Security Wizard only take effect after a restart on the device.

LLDP enabled

You can specify how the device handles LLDP data (Link Layer Discovery Protocol). You can make the following settings:

- **TX only**
  The device sends LLDP information.

- **RX only**
  The device receives LLDP information.

- **TX and RX**
  The device sends and receives LLDP information.

- **Disable**
  LLDP information is neither sent nor received. In this case, the device does not appear in the STEP 7 topology browser.

Primary Setup Unit (DCP)

Here, you decide whether or not the device can be accessed with DCP (Discovery and Configuration Protocol):

- **Enable**
  Device data can be both read and set with DCP.

- **Disable**
  Device data can be neither read nor set.

- **Read only**
  Device data can be read with DCP but cannot be modified.

Note

The "Disable" and "Read only" settings can cause disruption of PNIO activity. Select "Enable" if you want the device to handle PNIO communication.

3.7.2.5   Restart menu command

Restart

Click this button to restart the device. During a restart, the device is reinitialized, the internal firmware is reloaded, and the device runs a self-test. The learned entries in the address table are deleted. You can leave the browser window open while the device restarts.

Restore Memory Defaults

Click this button to reset the configuration. The following parameters (protected defaults) are not reset:

- IP address
- Subnet mask
- Gateway address
- SSID
- IP address of the default router
- DHCP flag
- System name
- System location
- System contact
- Device mode
- Country code

There is no automatic restart. This allows you to enter data using Web Based Management before the restart. The changes take effect only after a restart.

If you are logged on as user, the "Restore Memory Defaults" button is not visible.

Restore Factory Defaults and restart

Click on this button to restore the factory configuration settings. The protected defaults (see above) are also reset. The C-PLUG is reinitialized and formatted if it exists. An automatic restart is triggered.

Note

By resetting all the defaults, the IP address is also lost. The device can then only be accessed using the Primary Setup Tool unless the IP address is obtained over DHCP.

If you are logged on as user, the "Restore Factory Defaults" button is not visible.

3.7.2.6 Passwords menu command

Introduction

On this page, you can change current passwords for the IWLAN device. The default password for the "admin" user is "admin" (exception: the USA has a secret default password, that can be obtained by specialists for professional WLAN installations from Siemens support) and for the user, the password is "user". For security reasons, it is advisable to change the default passwords when the IWLAN device is commissioned. The new passwords can be a maximum of 31 characters long.

Note

Permitted characters

When assigning the password, ASCII code 0x20 to 0x7e is used. The following characters are supported:

- The digits 0 to 9
- The letters abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ
- The special characters !$#%&'()*+,-./:;<=>?@[\]^_`{|}~ and the space

---

Current admin password

Enter the current admin password in this input box.

User password

Enter the new password for the "user" in this input box.

User password confirmation

Enter the new password for the "user" again in this input box.

Admin password

Enter the new password for the "admin" user in this input box.

Admin password confirmation

Enter the new password for the "admin" user again in this input box.

Note

Web Based Management logs off after a certain time automatically if the user is inactive during this time.

3.7.2.7 Event Config menu command

System events of the device

On this page, you specify how the device reacts to system events. You can configure the reaction of the IWLAN device to the following events:

● Starting the device

● Change in the Ethernet status Link up / Link down

● Error when a user logs in

● Change in the power supply of the device (evaluating this event only makes sense when there is a redundant power supply).

● Change in the error status (error LED)

Note

System event when changing the redundant power supply

All SCALANCE W-700 devices provide the option of redundant power supply as well as the option of monitoring this redundancy. Depending on the device type there is a system event under the following conditions:

SCALANCE W784
System event when either the power at the four-pin connector (L1, L2) or Power over Ethernet fails. Redundancy at the four-pin connector (L1 and L2 connected) is not monitored.

SCALANCE W786
System event when either the power at the four-pin power input or Power over Ethernet fails. Redundancy at the power supply adapter 12 - 24 V DC (L1 and L2 are connected) is not monitored.

SCALANCE W788
System event when either the power at the hybrid connector or at the M12 connector fails. Redundancy at the hybrid connector (power contacts in the hybrid connector are connected as well as Power over Ethernet) is not monitored.

Additional system events for access points

If you use an IWLAN device in access point mode, you can configure additional system events:

● Events relating to the logging on and off of a client. If there are numerous logons and logoffs by WLAN clients, enabling this system event can impair the performance of this device, for example when controlling the device with Web Based Management.

● IP-Alive state change (application-specific connection monitoring)

● Link Check state change (device-specific connection monitoring)

● Events related to bandwidth reservation iQoS.

- Detection of access points on own or an overlapping wireless channel.
- Topology changes in Rapid Spanning Tree.
- Events related to iPCF with the device variants SCALANCE W78x-xRR.
- Events in conjunction with the Forced Roaming on IP down function .
- Change in the WDS connection status Link up / Link down.

With the device models that have more than one WLAN interface, the status of a redundant connection (redundant, not redundant, interrupted) is also a system event.

Reaction to system events

The following alternatives are available when the device reacts to a system event:

- The device sends an E-mail.
- The device sends an SNMP trap.
- The device sends a Syslog message.
- The device indicates an error (the error LED lights up).

By selecting the appropriate check boxes, you specify which events trigger which reactions on the device. With the check box in the "Functions enabled" row, you enable or disable the sending of E-mails or triggering of SNMP traps.

3.7.2.8 E-mail Config menu command

Sender and recipient of an E-mail

Here, you specify who the device sends an E-mail to as a reaction to configured events. You can also enter a sender. This allows you to recognize which device is involved and sent the E-mail. If you do not make an entry in the "From" box, the device uses the following sender: IWLANdevice@<IP address>

E-mail address

In this box, enter an E-mail address to which the IWLAN device sends an E-mail as soon as a situation occurs that was defined in the configuration.

SMTP server IP address

Enter an IP address of the mail server in this box.

SMTP server IP port

25 is entered in this box as the default value. You only need to change this value when the mail server is reached via a different port number.

"From" Field

In this box, enter the sender information that will appear in the E-mail sent by the IWLAN device. If you do not make an entry, the IWLAN device use the sender named above.

3.7.2.9 SNMP Config menu command

Configuration

Select the check boxes of the entries according to the SNMP functionality you want to use. SNMP version 3 allows permissions to be assigned and protocol level, authentication, and encryption. You specify groups and users in the Groups and Users submenus. You can also make entries there if the SNMPv3 enabled check box is not selected, however the entries are not applied.

SNMP enabled

Select this check box to enable communication between the IWLAN device and the SNMP protocol.

SNMPv1/v2c enabled

Select this check box if you want to use the SNMPv1/v2c range of functions.

SNMPv1/v2c read only

Select this check box if you only want to use read permissions with the the SNMP protocol.

SNMPv1 traps enabled

Select this check box if you want to send SNMPv1 traps.

Trap community string

In this box, you enter an authentication for the trap community.

Read community string

In this box, you enter an authentication for the read community (read permissions).

Write community string

In this box, you enter an authentication for the write community (write permissions).

SNMPv3 enabled

Select this check box if you want to use the SNMPv3 range of functions.

Note

When using SNMP version 3, you should disable SNMP V1 and V2c because the security settings of SNMP V3 can be bypassed by access over SNMP V1 or V2c.

Downloading the MIB of the SCALANCE W-700 using the Internet Explorer

Using the URL

`http://<IP_address>/snScalanceW.mib`

, you display the login window if you are not yet logged on. After you have logged on successfully, you can access the private MIB of the SCALANCE W-700. To save this on your PC, the source text view should be enabled. As of version V4.0, the MIB of the SCALANCE W-700 can be downloaded in the WBM in "System/Load&Save/HTTP" using the Private MIB file: "save" button.

3.7.2.10   SNMP Traps menu command

Traps

Here, you enter the IP addresses of up to 10 trap receivers. The device sends a trap to all the addresses you enter if their "Enable trap" check boxes are selected.

Note

During a warm or cold restart with a wireless connection (AP client, WDS, or WRED), there is no guarantee that the recipient can be reached at the time when the trap is sent. This leads to a loss of the message.

3.7.2.11   SNMP Groups menu command

Groups

This page displays the SNMPv3 groups. You can create a new group by clicking the "New" button and specifying the group name, the security level, and the write or read permissions. If you click on an entry in the "Group name" column, the "Edit SNMPv3" page opens.

Group name

Enter the name of the group in this box. The maximum number of characters is 31.

You can delete a group by selecting the check box in the "Del" column and clicking the "Set Values" button. If members are already entered in the group, you cannot delete the group nor is it possible to change the security level of the group.

There are three SNMPv3 security levels:

Security level	Special features	Comment
None	No authentication, no encryption.	
Auth/No Priv	Authentication with the MD5 or SHA algorithm, no encryption.	To display the members of the group, you must enter the authentication password (maximum of 63 characters).
Auth/Priv	Authentication with the MD5 or SHA algorithm, encryption with the DES3 algorithm.	To display the members of the group, you must enter the authentication password (maximum of 63 characters).

Read access

Select this check box if you only want to assign read permissions to a group. When you create a group, it should at least have read permissions. If you assign neither read nor write permissions to a group, the group exists but group members have no access.

Write access

Select this check box if you want to assign both read and write permissions to a group.

3.7.2.12   SNMP Users menu command

Users

This page displays the SNMPv3 users. You can create a new user by clicking the "New" button and specifying the user name and the group to which the user will belong. If necessary, you must also enter the passwords for the authentication and for the encryption.

You can delete a user by selecting the check box in the "Del" column and clicking the "Set Values" button. If you click on an entry in the "User name" column, the "Edit SNMPv3 User" page opens.

3.7.2.13   SSyslog menu command

Syslog according to RFC 3164 is used for transferring short, unencrypted text messages over UDP in the IP network. This requires a standard Syslog server.

Syslog configuration with the IWLAN device

The parameters used for the Syslog protocol are displayed and set in the **System -> Syslog** menu. The meaning of the parameters is as follows:

Syslog server

The server address decides the IP address to which the Syslog messages are sent. If no IP address is entered in this box, no Syslog messages are sent. If the Syslog server is not in the same network as the IWLAN device, an automatic attempt is made to establish a connection over the default gateway.

Enable log table

This check box decides whether all entries made in the log table are also sent as Syslog messages.

Enable auth log

This check box decides whether all entries made in the authentication log are also sent as Syslog messages.

3.7.2.14   SNTP Config menu command

Time-of-day synchronization in the network

SNTP is the acronym for Simple Network Time Protocol. A server uses this protocol to provide a uniform time throughout the entire network. Clients can synchronize themselves with this time.

SNTP server

If you enter the IP address of an SNTP server in the "SNTP server" text box and select the time zone of the IWLAN device in the "Time zone offset" list box, the IWLAN device uses the time information of this server. The IWLAN device adopts this time information without any further conversion relating to daylight-saving or standard time.

Update interval

In the "Update interval" text box, you enter the cycle time in seconds after which the IWLAN device calls up the time information from the SNTP server. With the "Refresh SNTP" button, you can synchronize with the SNTP server regardless of the selected update time.

Current system time

The "Current system time" box indicates the time and the date of the SNTP server if you have specified one.

3.7.2.15   Fault State menu command

Information on errors/faults

This page displays information on faults/errors that have occurred. You can delete this information if you click the "Remove Fault State" button.

If there are no more unanswered error/fault messages, the fault LED goes off.

Remove Fault State

When you click this button, you delete the information about the errors/faults that have occurred.

Link with some IP-Alive client(s) is/was down (Access Point)

This message appears when a client that is being monitored with IP-Alive can no longer be reached. Click on this message to display a full error list. You confirm an error message by clicking on it.

Link with some Link Check client(s) is/was down (Access Point)

This message appears when a client that is being monitored with Link Check can no longer be reached. Click on this message to display a full error list. You confirm an error message by clicking on it.

3.7.2.16   Load & Save menu command

Saving and loading device data

Clicking the Load & Save menu command first opens a page with the current firmware version. The "HTTP" and "TFTP" submenus allow you to save device data in external files or to transfer data from external files to the device. If the device is operated with a C-PLUG, the data from the loaded configuration file is stored on the C-PLUG. As long as the C-PLUG is inserted, the device works with the configuration on the C-PLUG.

You can save the following device data in external files:

- The configuration data of the device
- The private MIB file of the device (only via HTTP)
- the content of the log table
- The firmware of the device
- The client certificate (only for clients and access points in client mode)
- The server certificate (only for clients and access points in client mode)
- The SSL certificate

You can transfer the following data from external files to the device:

- The configuration data of the device
- The firmware of the device
- The client certificate (only for clients and access points in client mode)
- The server certificate (only for clients and access points in client mode)
- The SSL certificate

Note

When you download the configuration data to the device, it is restarted so that the new data is adopted correctly. The restart takes place automatically during the loading of HTTP and TFTP. The device can no longer be reached using the old IP address if the downloaded configuration data contains a new IP address.

Note

For SCALANCE W788-xPRO/RR and W74x-1PRO/RR only

As of firmware version V3.0, the file with the configuration data of the SCALANCE W-700 also includes the following information

- Version of the configuration file
- Firmware version with which this configuration file was created
- Order number (MLFB) of the device with which the configuration file was created

It is essential that the configuration on the C-PLUG was generated with a firmware version ≤ the firmware version on the destination device.

Example:

Configuration files created with a device with firmware V2.4 or older can be loaded without problems on devices with firmware version V3.0 (or V3.2 on the W786-xPRO and V3.3 on the W784-1xx/W74x-1). Configuration files generated with a device with firmware version V3.0 (or 3.2 or 3.3), cannot, however, be loaded on devices with firmware version V2.4 or older.

Reusing configuration data

Saving and reading in configuration data reduces the effort if several devices have the same configuration and when IP addresses are obtained over DHCP. Save the configuration data on a PC after you have configured an IWLAN device. Download this file to all other devices you want to configure. If necessary, you may need to assign an IP address to these devices first using the Primary Setup Tool.

How to load or save data over HTTPS

1. To load or save configuration data or the firmware, enter the name of the file from which the data will be taken and in which the data will be saved in the relevant input box.
   As an alternative, you can also use a file selection dialog that opens after you click the "Browse..." button.

2. Start the save function by clicking the Save button. Start the load from file function by clicking the "Load" button.

How to load or save data over TFTP

1. Enter the IP address of the TFTP server in the TFTP Server IP input box.

2. Enter the port of the TFTP server in the Port text box if the default value does not meet your requirements.

3. Click the Set Values button before you enter any further information for saving the data.

4. Specify the name of the file (maximum 32 characters) from which the data will be taken or where the data will be saved in the relevant input box for the configuration data or firmware.

5. Start the save function by clicking the Save button. Start the load from file function by clicking the Load button.

Configuration package

If security certificates for the client, server and/or SSL are installed on a client, when the configuration is saved, the client provides the option of saving the configuration file with the certificates as a configuration package. With the aid of the configuration package, clients can be replicated simply; in other words, identical settings and certificates are transferred to the clients in one step. Just as when you download the configuration file, this is followed by a restart. No special measures are necessary when downloading the configuration because the IWLAN device automatically recognizes the type of configuration file. An access point can also save the configuration along with the SSL certificate if such a certificate is already installed.

3.7.2.17 PNIO menu

Introduction

PROFINET IO, abbreviated to PNIO, allows communication with distributed IO devices on the basis of Ethernet. The main feature of PROFINET IO is the cyclic data traffic between IO controller and field device. WLAN devices can also handle PNIO communication via their Ethernet interface.

IWLAN devices and STEP 7

IWLAN devices are included in the hardware catalog of STEP 7 as of version V5.4.4. The Ethernet interface can be configured in STEP 7 where the diagnostics functions can also be used. The WLAN interface cannot be configured with STEP 7.

PNIO for client devices

If you want to use a client as a PNIO device, there are two ways of configuring the MAC-based communication:

- **Adopt Own MAC**
  In the network beyond the device, only IP communication and no PNIO is possible.

- **Layer 2 Tunnel**
  The WLAN client and the devices behind it can be used as PNIO devices.

Note

If "Auto find 'Adopt MAC'" or "Set 'Adopt MAC' manually" is set for a client, this device cannot be used as a PNIO device.

PNIO configuration

You have the following options available for the configuration:

- **PNIO AR Status**
  AR is the acronym for Application Relation. This identifies a PNIO connection to a controller. When data is being exchanged cyclically between an IWLAN device and a controller, "Online" is displayed here, otherwise "Offline".

- **PNIO Device Name**
  Enter the PNIO device name here.

- **Clear PNIO Fault State**
  Clears the PNIO fault state and sets the device to INC mode (in other words, PNIO mode is disabled).

3.7.2.18   C-PLUG menu command

Information on the content of the C-PLUG

This menu command provides you with detailed information on the C-PLUG. You can also format the C-PLUG or provide it with new content. As soon as the device is started with a C-PLUG inserted, the WLAN device starts up with the configuration data on the C-PLUG. Changes to parameters are stored on the C-PLUG and displayed over the Web and CLI.

The data in the memory of the device only becomes accessible when the device restarts without a C-PLUG using the <Restart without C-PLUG> function.
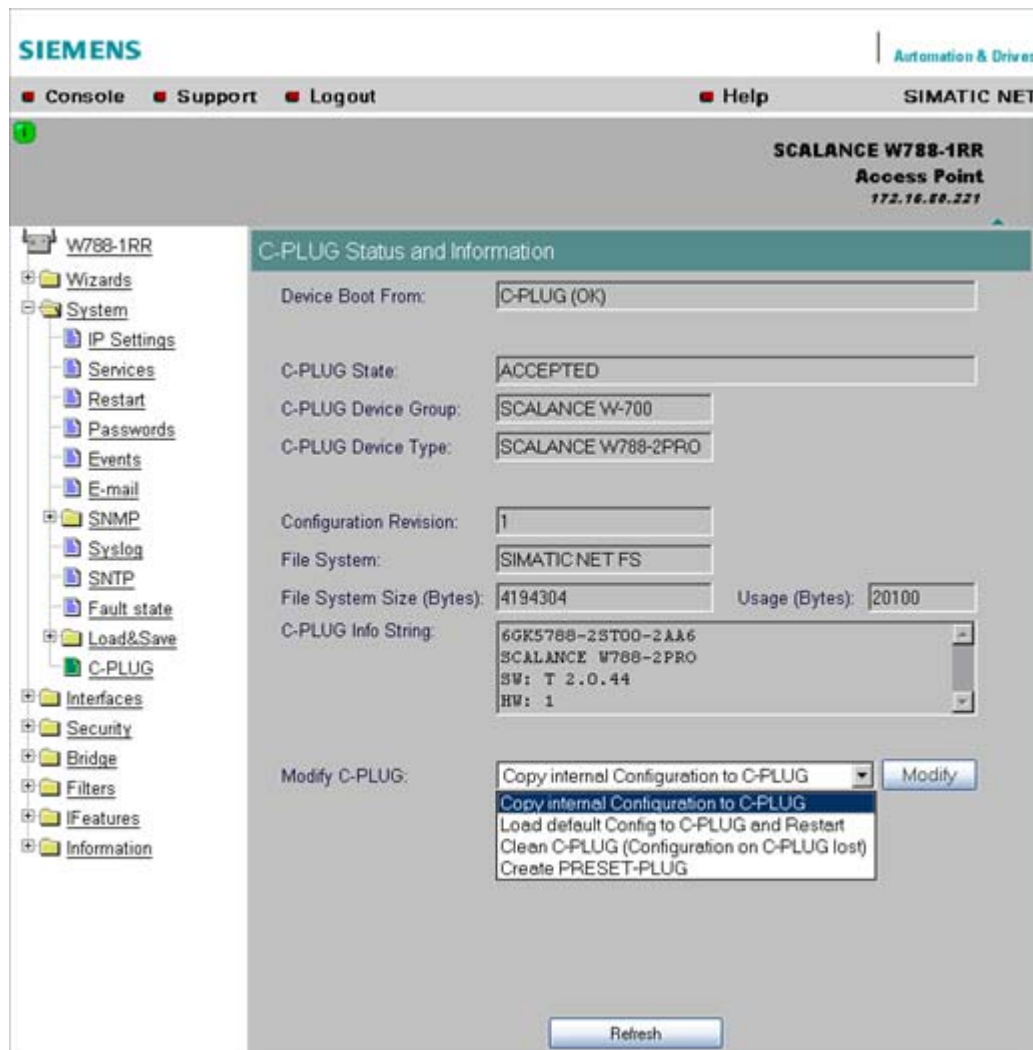
Note

In terms of the C-PLUG, the IWLAN devices work in two modes:

- **Without C-PLUG**
  The device stores the configuration in internal memory. This mode is active when no C-PLUG is inserted.
- **With C-PLUG**
  The configuration stored on the C-PLUG is displayed over the user interfaces. In this mode, the internal memory is neither read nor written. If changes are made to the configuration, the device stores the configuration directly on the C-PLUG. This mode is active when C-PLUG is inserted. As soon as the device is started with a C-PLUG inserted, the IWLAN device starts up with the configuration data on the C-PLUG.

C-PLUG State

This displays the status of the C-PLUG. The following are possible:

- **ACCEPTED**
  A C-PLUG with a valid and suitable content is inserted in the device.

- **NOT ACCEPTED**
  C-PLUG missing or invalid or incompatible content of an inserted C-PLUG. The status is also displayed when the C-PLUG was formatted during operation.

- **NOT ACCEPTED, HEADER CRC ERROR**
  A C-PLUG with a bad content is inserted.

- **NOT PRESENT**
  No C-PLUG is inserted in the device.

C-PLUG Device Group

Indicates the SIMATIC NET product line that used the C-PLUG previously.

C-PLUG Device Type

Indicates the device type within the product line that used the C-PLUG previously.

Configuration Revision

The version of the configuration structure. This information relates to the configuration options supported by the device and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove modules or extenders, it can, however, change if you update the firmware.

File System

Displays the type of file system on the C-PLUG.

File System Size

Displays the maximum storage capacity of the file system on the C-PLUG.

File System Usage

Displays the memory utilization of the file system of the C-PLUG.

C-PLUG Info String

Here, you will see all the additional information about the device that used the C-PLUG previously, for example, order number, type designation, and the versions of the hardware and software.

Modify C-PLUG

You can only make settings in this box if you are logged on as "Admin". Here, you decide how you want to change the content of the C-PLUG. The following alternatives are possible:

- **Copy internal Configuration to C-PLUG**
  The configuration in the internal flash memory of the IWLAN device is copied to the C-PLUG; this is followed by a restart.
  This function is required in the following important use case: The device has started up with a C-PLUG containing a bad configuration or a configuration different from the device. If you have not yet made any configuration changes after starting up the device, you can use this function to overwrite the content of the C-PLUG with the original device configuration from memory.

- **Load default Configuration to C-PLUG and Restart**
  A configuration with all the factory default values is stored on the C-PLUG. This is followed by a restart in which the device starts up with these default values.

- **Clean C-PLUG (Configuration on C-PLUG lost)**
  Deletes all data on the C-PLUG and starts a low-level formatting function. There is no automatic restart.

- **Create PRESET PLUG**
  Writes configuration data to a PRESET PLUG. For detailed information on this topic, refer to the section "Configuring with the PRESET-PLUG".

After making your selection, start the function by clicking the "Modify" button.

C-PLUG error message

If the device detects a C-PLUG error during startup, a message is displayed by Web Based Management. C-PLUG errors can have two causes:

- The C-PLUG contains bad data or data for a different device type.

- There is no C-PLUG in the device although a C-PLUG was present prior to the last shutdown of the device.

If there is a C-PLUG problem, the device starts up with a minimum configuration to allow the user to eliminate the problem.

Options

Here, select the further measures you want to take. The following alternatives are possible:

- **Restart without C-PLUG**
  Remove the C-PLUG from the device. After clicking the "Modify" button, the device starts with the internal configuration.

- **Format C-PLUG. Copy internal Configuration and Restart**
  The internal configuration of the device is copied to the C-PLUG and the device starts with this configuration.

- **Format C-PLUG. Set default Configuration and Restart**
  The factory defaults are stored on the C-PLUG and the device starts with this default configuration. The internal configuration of the device is not changed.

- **Reset to Factory Defaults**
  The factory defaults are stored on the C-PLUG and the device starts with this default configuration. The internal configuration of the device is also reset to the default values.

3.7.3 The Interfaces menu

3.7.3.1 Interfaces menu command

Introduction

The IWLAN device has one Ethernet interface and one or more WLAN interfaces that can be configured separately. In the pages of this menu, you can configure both the wired Ethernet interface and the IWLAN interface.

With the menu command Interfaces > WLAN1…3 > Virtual AP count in the Access Point mode, you can also configure up to eight virtual access points (VAP0 … VAP7) per wireless interface.

Note

VAPs are visible only after a virtual AP count > 0.

Ethernet MAC address

This box displays the MAC address of the IWLAN device.

Wireless 1 MAC address

This box displays the MAC address of the first wireless adapter.

Wireless 2 MAC address

This box displays the MAC address of the second wireless adapter.

Wireless 3 MAC address

This box displays the MAC address of the third wireless adapter.

3.7.3.2 Ethernet menu command

TTransmission speed and mode

For a wired Ethernet interface with an RJ-45 connector, you only specify the transmission speed / mode parameters and the crossing over of the Ethernet connection.

Note

If you specify the mode, you must make the same settings on the partner device.

For devices with an ST duplex multimode fiber-optic cable connector, there is no parameter assignment because only 100 Mbps full duplex is possible for this interface. The Ethernet MAC address and the current transmission speed/mode are displayed.

Note

If 10 Mbps is configured as the transmission speed or half duplex as the transmission mode, this can lead to restrictions in PNIO communication. Always select 100 Mbps and full duplex or "Auto" if you want the device to handle PNIO communication.

MAC address

This box displays the MAC address of the IWLAN device (wired connection).

Speed / mode

When you select the Auto entry in the "Speed / Mode" drop-down list box, the device sets a suitable speed and mode depending on the other network nodes and crosses over the Ethernet connection.

Current speed / mode

This box shows you the current transmission rate and the current mode being used on the IWLAN device.

Ethernet crossing

This box shows you the crossover status of Ethernet (MDI, MDIX). If you set "Auto" for "Speed/mode", "autocrossing" is enabled. Otherwise, you will need to set it manually.

3.7.3.3 WLAN menu command

Enable interface

Enable the interface by selecting "Enable Interface".

MAC address

This box displays the MAC address of the first or second wireless adapter of the IWLAN device.

Speed

This box shows the current transmission rate that has been achieved by the relevant wireless adapter.

Channel

This box shows the channel and frequency of the wireless interface.

SSID

This box shows the name of the wireless network to which the wireless adapter is assigned.

Network name (in access point mode only)

Enter the network name of the wireless network in the "SSID" input box. If you have used the Basic Wizard, a value is already entered here.

Infrastructure / Ad-Hoc (only for clients or access points in client mode)

Select Infrastructure to connect to an access point. "Ad hoc" is used to connect clients with each other without an access point. This is only possible when "Ad hoc" is set on all clients.

Wireless mode

Select the mode with which the selected wireless adapter will operate. The selected mode (default) must be supported by all partner devices.

Transmission mode

Specify the transmission mode in the "Wireless Mode" list box. If you have used the Basic Wizard, a value is already entered here.

Note

IEEE 802.11h transmission

It is not possible to select the 802.11h protocol in all country settings. It is specified by the configuration of "Country code" on the "System" page.

If the 802.11h protocol is selected, after applying the configuration with "Set Values", the comment (DFS is active for this country code) appears behind the "Enable Interface" check box.

With the automatically enabled Dynamic Frequency Selection function (DFS), prior to communication, the access point checks whether the configured or selected channel (see Auto Channel Select) is free of signals from a primary user (for example radar).

If signals of a primary user are found on the configured or selected channel, the access point follows the procedure outlined below:

- Auto channel select = enabled
  With automatic channel select, the access point changes to a different channel and repeats the availability check for this channel.
- "Auto channel select" = disabled
  If there is a fixed configured channel, the access point changes to the configured

alternative channel and repeats the availability check for this channel. If a primary user (for example radar) is discovered on the alternative channel, a further channel is selected at random.

Communication with clients is started only when no primary user has been discovered on the selected channel for one minute.

When operating PNIO systems with wireless standard 802.11h, make sure that no radar signals occur in the vicinity of the system. Due to the DFS strategy in 802.11h, there is a channel change if radar signals are detected.

Outdoor AP mode (only in access point mode) / Outdoor Client mode (only for clients or access point in client mode)

The device can be operated either in the indoor or outdoor mode. In indoor mode, all the country-dependent permitted channels and transmit power settings are available for operation in a building. In outdoor mode, the selection of country-dependent channels and the transmit power for operation are restricted for outdoor use. You enable this mode by selecting "Outdoor AP mode" or "Outdoor Client mode".

Channel Selection

On clients or access points in client mode, you can only set a channel in ad hod mode.

For access points, you have the following options: Select the "Auto Channel Select" check box if you want the access point to search for a free channel itself. If you want to specify a specific channel, make sure that "Auto Channel Select" is not selected. You can specify a suitable channel in the "Radio Channel" drop-down list box.

IEEE 802.11h transmission:

If you have selected the 802.11h protocol for transmission in access point mode and "Auto Channel Select" is not selected, the "Alt. radio channel" input box is displayed below "Radio channel". Here, you can select the alternative channel in case signals of a primary user are found on the main channel.

Make sure that the alternative channel is not being used by other access points.

In the IEEE 802.11h transmission mode, it is not practical to select the "WDS" mode. In WDS mode, all access points must use the same channel. If a signal from a primary user is detected by an access point, the channel is changed automatically and the existing connection is then terminated.

MAC address of the client (only for clients or access points in client mode)

A MAC address must be specified for the devices connected to the Ethernet port of the client before it can be reached. This MAC address is used by the client for wireless communication with the access point. This can be done automatically by the client adopting the MAC address of the first frame that it receives over the Ethernet interface. If this is required, "Auto find Adopt MAC" must be selected.

As long as the client is waiting for an Ethernet frame, it registers with the access point using its own MAC address. As soon as the first Ethernet frame is received, the client deregisters from the access point and immediately registers again with the MAC address from the Ethernet frame. If there is now a link-down on the Ethernet port, the client deregisters from the access point and registers again with its own MAC address.

If several devices are connected to the client, you should not select this setting.

You also have the option of specifying the MAC address of the connected device manually. To use this option, select "Set 'Adopt MAC' manually" and enter the MAC address of the device connected to the client in the "Adopt MAC" input box.

To be able to address an entire network of devices downstream from the client, "Adopt own MAC" must be selected. In this case, only layer 3 connections (TCP/IP) are possible. If up to eight MAC addresses need to be served downstream from the client, the "Layer 2 Tunnel" setting must be selected for the client. The settings "Adopt own MAC" and "Layer 2 Tunnel" are not available for the device variants SCALANCE W744-1 and SCALANCE W7441-PRO.

Note

The "Layer 2 Tunnel" functionality is supported by access points as of firmware version V3.1. This setting meets the requirements of industrial applications in which MAC address-based communication with several devices downstream from the client is required. Clients with this setting cannot connect to standard Wi-Fi devices and access points with firmware V3.0 or older.

Virtual AP count (only in access point mode)

If you want to configure virtual access points (VAPs) on this AP, set the number of virtual access points using the "Virtual AP count" drop-down list box. If "Virtual AP count = 0 and VLAN/Prio Tag" are disabled, no VAPs are created.

You can define up to a maximum of 8 VAPs. The settings of VAP0 are made directly in "Interfaces/WLAN", the settings for VAP1...7 can be found in the "Interfaces/WLAN/VAP1...7" submenus.

By using virtual access points, various SSIDs (maximum of 8 per WLAN interface) can be configured with different security settings. You can assign each virtual AP to a particular VLAN.

Connected to AP with MAC (client and access point in client mode)

This box shows the MAC address of the access point with which the client is connected.

Connected to AP with SSID (client and access point in client mode)

This box shows the SSID of the access point with which the client is connected.

Connected to AP with channel (client and access point in client mode)

This box shows the channel of the access point with which the client is connected.

Permitted Channels

This box displays the permitted channels.

Set Values

Apply the configuration by clicking "Set Values".

If you have configured virtual access points ("Virtual AP count > 0"), in "access point" mode, you will be requested to run a restart on the access point after clicking "Set Values".

3.7.3.4 Advanced menu command

Configuring transmission characteristics

On this page, you can specify details of the transmission characteristics. You only need to adapt the parameters on this page if the device cannot be used as it is intended with the default settings.

Transmit power

In the "Transmit Power" list box, you can specify the output power of the device. It may be necessary to reduce the transmit power when using antennas to avoid exceeding the maximum legal transmit power. Reducing the transmit power effectively reduces cell size.

Beacons

Beacons are packets that are sent cyclically by an access point to inform clients of its existence. In the "Beacon Interval" input box, you specify the interval (20 - 1000 ms) at which the device sends beacons.

In access point mode only
The "Data Beacon Rate DTIM" parameter (Delivery Traffic Indication Map) specifies how often the access point sends broadcast and multicast packets over the wireless interface. If you enter 1 in this box, the access point transmits broadcast and multicast packets directly after each beacon (recommended setting for normal network environments). The value 5 would mean that the access point collects the broadcast and multicast packets and sends them after every fifth beacon.

Increasing this value allows a longer sleep mode for the clients but means a greater delay for broadcast and multicast packets.

Note

The lowest basic rate in the INTERFACE\WLAN\DATARATES menu is used as the "Beacon Rate". The higher the data rate of the beacon, the shorter the range of the beacon.

RTS/CTS

RTS/CTS (Request To Send/Clear To Send) is a method for avoiding collisions based on the exchange of status information before sending the actual data (hidden node problem). To minimize network load resulting from the additional protocol exchange, this method is used only when a packet size that you select with the "RTS/CTS Threshold" is exceeded.

Fragmentation

The "Fragmentation Length Threshold" parameter specifies the maximum package size transferred on the wireless link. Large packets are divided up into small packets prior to transmission and then reassembled into the original size after they have been received. This can be beneficial if the transmission quality is poor because larger packets are more difficult to transmit. However fragmentation into smaller packets means a poorer throughput.

Repetitions

There are two situations in which packets are repeated. The hardware repetition is performed by the WLAN chip itself when it tries to repeat an unacknowledged packet immediately. The number of attempted repetitions is specified with the "Hardware Retry number" parameter.

If all hardware repetitions were unsuccessful, the packet is withdrawn and all other packets in the buffer are sent first. Following this, transmission of the packet is attempted again. The number of such repetitions is specified with the "Software Retry number" parameter.

The software repetition mechanism can be enabled or disabled with "Use Software Retry".

Shortened preamble with 802.11b

The 802.11b standard allows the use of shortened preambles in the wireless transmission of data packets. This increases the amount of user data. Older WLAN clients do not support this function. If you have problems with older WLAN clients, disable this function.

Antenna Gain

The "Antenna Gain" parameter describes the antenna gain in dBi of an antenna connected to a WLAN device.

You can set values for the following parameters:

- Antenna Type
- Antenna Gain
- Antenna cable length (in meters)

If "Antenna Type" is set to "User Defined", you can enter any value in the "Antenna Gain" box for the antenna gain. Otherwise, the preconfigured value of the selected "Antenna Type" is displayed. In the "Antenna cable length (in meters)" box, you enter the length of the connecting cable between the device and the antenna.

It is necessary to set a specific value to make sure that the regulations of the national authorities are adhered to. The national authorities, for example, specify all usable channels, the corresponding maximum transmit power and other conditions of use. You will find more detailed information on the regulations in your country using the countrylist.log.
Based on the settings for antenna gain and transmit power, the IWLAN device automatically selects the permitted channels. Under some circumstances, there may be fewer permitted channels available for antennas with a higher antenna gain than for antennas with a lower antenna gain.

Note

If you select "User defined", you have the option of entering dBi values as integers for the antenna gain in the range from 0 through 30 dBi. Please remember to take the losses of the antenna connecting cable into account.

> **Note**
>
> The correct antenna setting is mandatory for operation complying with the approvals. A false antenna gain entry can lead to legal proceedings!

Antennas

The "Antenna Mode" list box specifies the use of antennas.

- The Diversity setting takes the better of the two antennas for the data transmission. For each WLAN interface, both antennas must be connected. Both antennas should also be of the same type and they should also illuminate approximately the same space. If an access point is operated with the diversity setting and the two antennas span different cells, this can have negative effects.

- With the setting "Tx on A, Rx on B", antenna A is used to send and antenna B to receive.

- With the setting "Tx on B, Rx on A" antenna B is used to send and antenna A to receive.

With the settings "Diversity, Tx on A, Rx on B" and "Tx on B, Rx on A", both antennas must be connected on each WLAN interface. If only one antenna is connected, the connected antenna must be set permanently. The second antenna socket must also have a 50 Ω terminator fitted.

> **Note**
>
> For information on the location of the antenna sockets, refer to the section "Connectors for external antennas".

Scan for access points (only for clients and access points in client mode)

While the client is connected to an access point, it scans for other access points in the background with which it can connect when necessary. There are three modes for scanning access points that can be selected in the "Background scan mode" drop-down list:

- **Disabled**
  The client never scans for further access points as long as it is connected.

- **Scan if Idle**
  The client only scans for further access points when no data transfer has taken place for a certain time.

- **Scan Always**
  The client scans continuously for further access points. The "Background scan interval" parameter specifies the interval at which further access points are scanned.

To optimize the scanning for further access points when handing over or background scanning, you can specify channels for the client on which other access points can be found. To do this, select the "Background Scan Ch.Select" check box and enter the channels of the other access points in the "Background Scan Channels" input box. Separate the channel information with blanks.

Roaming threshold

If the client finds a better access point, it attempts to connect to it. Before it changes, the new access point must be better than the current access point by a certain value. The threshold at which the client changes to the new access point can be specified with the "Roaming threshold" parameter. The following settings are possible:

- **Low**
  Changes at a slightly higher field strength to the AP with the stronger signal.

- **Medium**
  Changes at a moderately higher field strength to the AP with the stronger signal.

- **High**
  Changes only at a significantly higher field strength to the AP with the stronger signal.

Restricted channels (in access point mode only)

The selection of channels used by an access point when establishing a wireless cell can be restricted. Such a restriction is advisable if you use "Auto channel select", the automatic channel change with IEEE 802.11h or iHOP. To do this, select the "Background Scan Ch.Select" check box and enter the channels of the other access points in the "Background Scan Channels" input box. Separate the channel information with blanks.

Roaming when there is no Ethernet interface (access point mode only)

If the wired Ethernet interface is no longer available (cable break, connector removed), a client connected over the wireless network is not aware of this. The access point can then force the logged-on IWLAN clients to roam by deactivating its WLAN interface. The client then attempts to log on at a different access point. You enable this feature by selecting the "Force roaming if link down on the Ethernet interface" check box.

Enable WMM

With wireless multimedia, multimedia frames are transferred according to the IEEE 802.11e standard with a higher priority.

Select the "Enable WMM" option if you want frames evaluated according to their priority and sent prioritized over the WLAN interface.

According to the Wi-Fi standard, prioritized frames are classified as follows:

Access category	Description	802.1d Tags
WMM voice priority	Highest priority Allows multiple simultaneous VoIP calls with a short wait time and good voice quality	7, 6
WMM Video priority	Prioritizes video data traffic compared with other data traffic An 802.11g or 802.11a channel can support 3-4 SDTV streams or 1 HDTV stream.	5, 4

Access category	Description	802.1d Tags
WMM best effort priority	Data traffic from older devices or from applications and devices that are not QoS-compliant. Data traffic that is less sensitive to delays, but is impaired by longer wait times, for example surfing the Web.	0, 3
WMM background priority	Data traffic with exacting requirements regarding wait times and data throughput.	2, 1

3.7.3.5   SSID List menu command

Note

The "SSID List" submenu is only available for clients and access points in client mode. You can specify the mode in the "System" menu.

How the client connects to the network

With this menu command, you can specify how the device connects to a network as client.

Connect to ANY SSID

- If the "Connect to ANY SSID" check box is selected, the device in client mode attempts to connect to the network with the best transmission quality and with suitable security settings. If the "Suppress SSID broadcasting" setting is made for an access point, the client cannot log on there with the ANY SSID.

- If this check box is not selected, the client attempts to connect to the network from the SSID list that has the best transmission quality.

An SSID is absolutely necessary in ad hoc networks and iPCF. The maximum number of SSIDs in the SSID list is restricted to 32.

Del

Select a check box in the "Del" column and click the "Set Values" button to delete an SSID entry.

Add new

Enter the character string for a new SSID in the "Add New" box and click the "Set Values" button if you want to define a new SSID.

3.7.3.6 Advanced G menu command

Properties of the 802.11g standard

The IEEE 802.11g is upwards compatible with IEEE 802.11b, both use the 2.4 GHz band. In contrast to 802.11b that specifies data rates up to 11 Mbps, 802.11g provides for data rates up to 54 Mbps. The 802.11g standard also uses the OFDM modulation scheme. This technology divides a data packet into several smaller packets that are transmitted at the same time at different frequencies.

Special options for 802.11g settings

The options you can set in the Advanced G submenu relate to the way in which management and control data (RTS/CTS frames, beacons) are sent in the 802.11g mode. You can also specify that the WLAN device only supports 802.11g-compatible devices.

Handling 802.11b clients

The access point automatically detects whether 802.11b clients exist in the area. To avoid 802.11g packets colliding with 802.11b packets, the access point can use the RTS/CTS method.

Using RTS/CTS

You can configure RTS/CTS as follows:

- With the "802.11g CTS mode" drop-down list box, you specify the use of RTS/CTS:

None	Do not use RTS/CTS.
Always	Always use RTS/CTS with 802.11g packets.
Auto	Only use RTS/CTS when there are 802.11b clients in area.

- You can set the data rate for RTS/CTS frames in the "802.11g CTS Rate" drop-down list box.

- With the "802.11g CTS Type" drop-down list box, you specify whether only a CTS or RTS/CTS is sent.

802.11g enhancements

With the "802.11g Short Slot Time" parameter, you specify whether or not the short slot time is used. This short slot time should be supported by all newer clients.

With the "802.11g Only Mode" parameter, you can specify that only 802.11g clients can log on at the access point and also that only 802.11g rates are permitted (in access point mode only). In this mode, only the OFDM modulation method is used. This prevents 802.11b devices from registering. If 802.11g Only mode is disabled, both 802.11b devices and 802.11.g devices can register with the access point.

Set to Default

Click this button to reset the settings for "Advanced G" to the factory default settings.

3.7.3.7 Data Rates menu command

Note

The "Data Rates" submenu is available only in access point mode.

Variable setting of the transmission rates

From the table showing all available data rates for the current WLAN mode (802.11b, g, a etc.), you can select any combination of these data rates. The access point will then use only the selected transmission rates for communication with the clients.

Data Rate

This column contains the nominal data speeds in Mbps.

Enabled

Select a check box to assign a data transmission rate to the current WLAN mode.

Basic Rate

Select a check box to declare a data transmission rate as the "basic rate". The "Basic Rate" parameter specifies that a client must be capable of this data rate to be able to connect to the access point.

Note

The "Default Values" button sets the selection of values to conform with the standard.

3.7.3.8 VAP menu command

Note

The "VAP" submenu is available only in access point mode.

Description

You can only complete the pages of the virtual access points VAP1...VAP7 if you have configured virtual access points ("Virtual AP count > 0") at the higher level "Interfaces > WLAN".

On this page, you can assign a separate SSID to the virtual access points; in other words, the access point operates in multiple SSID mode.

SSID

Enter the SSID of the VLAN here.

Make sure that you also store the SSID of this VLAN in the configuration of the client that you assign to this VLAN.

Note

You can configure separate security settings for each virtual access point (see section "Basic Wireless menu command")

The security settings of the VAPs must meet those of the relevant VLANs.

3.7.4 The Security menu

3.7.4.1 Security menu command

Introduction

In this menu, you configure the security settings with which you want to operate your device. Apart from selecting the authentication and encryption scheme, this also includes the decision as to whether or not an external Radius server is used and whether access is restricted based on MAC addresses (ACL).

3.7.4.2 Basic Wireless menu command

Authentication

Authentication basically means that some form of identification is required. Authentication therefore protects the network from unwanted access. In the "Security Level" box, you can choose between the following types of authentication:

- **Open System**
  There is no authentication. Encryption with a fixed (unchanging) key can be selected as an option. To do this, define a key in the "Keys" menu. 5 or 13 ASCII or 10 or 26 hexadecimal characters specify a weaker key (40/104 bits). 16 ASCII or 32 hexadecimal characters, on the other hand, define a strong key (128 bits). Then select "Encryption" in the "Basic WLAN" menu.

  Note

  With the following devices in iPCF mode, only the "Open System" setting is possible:
  - SCALANCE W78x-xRR
  - SCALANCE W747-1RR
  - SCALANCE W747-1
  - IWLAN/PB Link PN IO

- **Shared Key**
  In Shared Key authentication, a fixed key is stored on the client and access point. This is then used for authentication and encryption. In this case, you will have to store a WEP key after selecting "Low (Shared Key)".

  Note

  Only in access point mode:

  When using "Open System" with "Encryption" or "Shared Key" in conjunction with ACL lists, note the information in the Section "ACL menu command".

- **WPA2-PSK**
  WPA2-PSK is based on the WPA2 standard, WPA authentication, however, operates without a RADIUS server. Instead of this, a key (pass phrase) is stored **on every** client and access point and this is used for authentication and further encryption. AES or TKIP is used as the encryption method, AES represents the standard method.

  Note

  The key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. It should be selected so that is complex, (for example consisting of random numbers, letters (upper-/lowercase), have few repetitions and special characters). Do not use known names, words and terms that could be guessed. If a device is lost or if the key becomes known, the key should be changed on all devices to maintain security.

- **WPA2**
  WPA2 (Wi-Fi Protected Access 2) is a further development of WPA and implements the functions of the IEEE 802.11i security standard. WPA2 uses the additional encryption protocol CCMP with preauthentication that allows fast roaming in mobile ad hoc networks. A client can log on in advance at several access points so that the normal authentication can be omitted.
  A RADIUS server is used to authenticate the client with an access point. The client logs on at a RADIUS server based on a certificate (EAP-TLS) or a combination of user name and password (EAP-PEAP or EAP-TTLS / internal authentication method MSCHAPv2). As an option, the RADIUS server then identifies itself to the client using a certificate. Following successful authentication, the client and RADIUS server generate key material that is used for data encryption. AES or TKIP is used as the encryption method, AES represents the standard method.

- **WPA-Auto-PSK**
  Setting with which an access point can process both the "WPA-PSK" as well as the "WPA2-PSK" type of authentication. This is necessary when the access point communicates with different clients, some using "WPA-PSK" and others "WPA2-PSK". The same encryption method must be set on the clients.

- **WPA-Auto**
  Setting with which an access point can process both the "WPA" as well as the "WPA2" type of authentication. This is necessary when the access point communicates with different clients, some using "WPA" and others "WPA2". The same encryption method must be set on the clients.

Encryption

Encryption protects the transferred data from eavesdropping and corruption. You can only disable encryption if you have selected "Open System" for authentication. All other security methods include both authentication and encryption.

Encryption methods

If you have selected "Open System" including "Encryption" or "Shared Key" for authentication, you will need to define a key in the "Keys" menu (see section "Keys menu command").

- **WEP (Wired Equivalent Privacy)**
  A weak, symmetrical stream encryption method with only 40- or 104-bit long keys based on the RC4 algorithm (Ron's Code 4).

  If you have selected WPA-PSK or WPA (RADIUS) as the authentication, the following alternatives are available in the "Cipher" box:

- **TKIP (Temporal Key Integrity Protocol)**
  A symmetrical stream encryption method with the RC4 algorithm (Ron's Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted packets.

- **AES (Advanced Encryption Standard)**
  Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.

- **AUTO**
  AES or TKIP is used depending on the capability of the other station.

RADIUS authentication method (only for clients and access points in client mode)

If a client is authenticated over an external RADIUS server, you can use the "RADIUS authentication type" selection list to specify a method for external authentication. As default, the "Auto" value is selected so that the client provides a RADIUS server with all supported methods. Any other selection restricts the support by the client to this one method. This step may be necessary because some RADIUS servers do not evaluate the response of the client completely or correctly.

The following options are available:

- **EAP TLS (Extensible Authentication Protocol - Transport Layer Security)**
  Uses certificates for authentication

- **EAP TTLS (Extensible Authentication Protocol - Tunnel Transport Layer Security)**
  After the TLS tunnel is established, MS-CHAPv2 is used for internal authentication.

- **PEAP (Protected Extensible Authentication Protocol)**
  Protocol proposal as an alternative to EAP-TTLS from the IETF.

Additional Entries for WPA-PSK and WPA2-PSK

To use the WPA-PSK scheme, you must enter a string in the Pass Phrase box that is used by the client to initialize dynamic key generation.

Suppress SSID broadcasting (only in access point mode)

With the Suppress SSID broadcasting setting, the access point is only ever accessible to clients that know its SSID. This method can be used to protect the access point from unauthorized access.

Note

Since no encryption is used for the SSID transfer, this function can only provide basic protection against unauthorized access. The use of an authentication method (for example WPA (RADIUS) or WPA-PSK if this is not possible) provides higher security.

You must also expect that certain end devices may have problems with access to a hidden SSID.

Inter SSID communication (only in access point mode)

Selecting this check box allows communication between WLAN clients registered at different SSIDs of an access point.

Example 1:	A SCALANCE W78x-2xx or W786-3PRO was defined with different SSIDs.
Example 2:	A SCALANCE W78x-1xx is used with multiple SSIDs.

Note

On an access point, the Inter SSID communication function must be enabled on all WLAN interfaces or on all VAPs to allow communication between the clients with different SSIDs.

Note

If VLANs are configured for the SSIDs, this setting can prevent communication between the SSIDs according to the VLAN rules.

Intracell communication (only in access point mode)

You can select from the following settings:

- **Intracell blocking**
  This setting prevents WLAN client communication within an SSID.

- **Ethernet blocking**
  This setting prevents WLAN client communication over the Ethernet interface of the access point.

- **Allowed**
  This setting enables both WLAN client communication within an SSID as well as WLAN client communication over the Ethernet interface.

Overview of the communication options (in access point mode only)

To illustrate the situation, there is an overview of the effects of the "Inter SSID communication" and "Intracell communication" settings below.

Settings		Possible communication		
Inter SSID communication	Intracell communication	within an SSID	with another SSID	to the Ethernet network
Enabled	Allowed	X	X	X
Enabled	Intracell blocking		X	X
Enabled	Ethernet blocking	X	X	
Disabled	Allowed	X		X
Disabled	Intracell blocking			X
Disabled	Ethernet blocking	X		

VAP (in access point mode only)

For each virtual access point VAP1 to VAP7, you configure the following security settings described earlier:

- Authentication

- Enable encryption

- Encryption method

- Select the default WEP key

- Enter the WPA-PSK password

- Specifies the "Group Key Update Intervals" in WPA-PSK

- Enable "Suppress SSID broadcasting"

Where they apply, all other security parameters are adopted from the **Security > Basic > WLAN1** or **WLAN2** or **WLAN3** page.

3.7.4.3 Keys menu command

Specifying the WEP key

To allow you to enable the encryption for the Open System and Shared Key authentication methods, you must first enter at least one key in the key table. You can choose between several key lengths. 5 or 13 ASCII or 10 or 26 hexadecimal characters specify a weaker key (40/104 bits). 16 ASCII or 32 hexadecimal characters, on the other hand, define a strong key (128 bits).

You can also create keys for WDS Redundancy and ACL Private (these are not supported by all clients for ACL).

Note
Permitted characters

When assigning the password, ASCII code 0x20 to 0x7e is used. The following characters are supported:

*   The digits 0 to 9
*   The letters abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ
*   The special characters !$#%&'()*+,-./:;<=>?@[\]^_`{|}~ and the space

---

Del

Select the check box in the "Del" column and then click the "Set Values" button to delete a key.

Add New

Enter the character string for a new key in the "Add New" box and then click the "Set Values" button to specify a new key.

3.7.4.4 ACL menu command

Note

The "ACL" menu is available only in access point mode.

Access rights for individual clients

The access control list (ACL) is and assignment of MAC addresses and access rights.

If ACL is enabled, prior to data transfer, the access point checks whether the necessary permissions for the communication partner (identified by the MAC address) are entered in the ACL table.

Note

Since no encryption is used for MAC address transfer, this function can only provide basic protection against unauthorized access. The use of an authentication method (for example WPA (RADIUS) or WPA-PSK if this is not possible) provides higher security.

Enabling the ACL

In Web Based Management, there is a drop-down list box for the use of ACL.

To enable ACL, set the global share to either "Enabled" or "Strict":

- **Enabled**
  All clients entered in the ACL are handled according to the ACL entry. Clients not entered in the ACL have access to the access point. This setting can be used to deny access by certain clients.

- **Strict**
  All clients entered in the ACL are handled according to the ACL entry. Clients not entered in the ACL have no access to the access point. This setting can be used to allow access by certain clients.

- **Disabled**
  The access control list is not used.

Changing an entry in the ACL

Click the relevant MAC address to change the entry in the ACL. With the "Sel" check box, you decide whether or not an ACL entry is used. The "Del" check box is used to delete an entry from the ACL.

New entry in the ACL

Click the "New" button to create a new entry in the ACL. A page appears on which you can make the necessary settings. Enter the "MAC address" of the client in the "MAC Address" text box. You specify the access permissions of the client in the "Permission" drop-down list box:

- **Allow**
  The client has access to the access point.

- **Deny**
  The client does not have access to the access point.

- **Default Key**
  The client only has access to the access point when it uses the default key for encryption of the data. To allow this, you must specify a valid default key for the SCALANCE W78x (for example in the WBM "Security" menu) that is also used by the client.

- **Private Key**
  With this setting, you can use different keys for different clients. You first create the private keys with the "Keys" menu command. You can select one of these keys in the "Key number" drop-down list box. The client only has access to the access point when it uses this private key. For this function, the client must support private keys.

Note

The private key set in the ACL must also be available in the key list on the client. The client must also use this private key for communication in Security->Basic->WLAN (the key must be set),if "Open System" with "Encryption" or "Shared Key" is used.

The private key is used on this connection for the transferred unicast packets intended for the wireless client.

All multicast and broadcast packets are transferred with the public key set on the access point. The wireless client entered in the ACL list must therefore also enter this public key at the same location in its key list as the access point.

Example

In its cell, an access point uses the shared key setting with a 128-bit public key (default key 1) for encryption of the data traffic.

All wireless clients that register at this access point, require this public key at position 1 in their key list for communication.

If access for certain wireless clients is now restricted by the ACL list of the access point on the basis of a private key, the private key must first be stored in the key list of the access point and the appropriate wireless clients.

The next step is to enter the MAC addresses of these wireless clients in the ACL list of the access point and to assign the private key. If it is intended that these wireless clients should continue communication, the private key must be set on the wireless client directly under **Security->Basic->WLAN** and used for the encryption. Otherwise the clients could receive broadband or multicast packets, but no longer be addressed directly with unicast packets.

3.7.4.5 RADIUS Server menu command

Note

The "RADIUS" menu command is available only in access point mode.

Authentication over an external server

The concept of RADIUS is based on an external authentication server. A client can only access the network after the access point has verified the logon data of the client with the authentication server. Both the client and the authentication server must support the EAP protocol (Extensive Authentication Protocol). The IWLAN device supports the external authentication mechanisms EAP-TLS, EAP-TTLS and PEAP.

Reauthentication enabled

With this check box, you can decide whether or not the access point triggers a reauthentication. You can also select who sets the time after which the client is forced to a reauthentication. If time management is local, enter the lifetime of the authentication (in seconds).

Authorization lifetime

In this box, you enter the lifetime of the authentication (in seconds). The minimum time is 60 seconds, the maximum time is 12 hours (43200 seconds). The default is 1 hour (3600 seconds).

RADIUS server

You can enter the data for two RADIUS servers; the information in the "Backup" column is used when the server in the "Primary" column was defined as "not available".
In addition to the IP address and the port, you must also select and confirm a password to be used as a "shared secret".
Enter the maximum number of transmission attempts in the "Maximum retransmissions" box.

3.7.4.6   Access menu command

Access permissions for IP addresses

In this menu, you specify the access permissions for IP addresses. You can specify whether management access (SNMP, Telnet, WBM) is possible with the defined addresses:

● Management access is possible only with the defined addresses.

Or:

● Management access is possible with all IP addresses not included in the list.

Note

The defined access rights also apply to the PC used for configuration. If you have not entered the local IP address and have set the ACL mode to "Accessed", no further access to the IWLAN device is possible.

You should also note that the IP address of the client can change if you use DHCP without reservation.

Del

Select the check box in the "Del" column and then click the "Set Values" button to delete a list entry.

New

Click the "New" button to create a new entry. The "Edit Access IP List" page is displayed. Enter the IP address and then click the "OK" button to add the entry to the list.

Sel

Use the check box in the "Sel" column and select the IP address to which you want to assign access rights. At the top right of the list, you can select whether or not all selected IP addresses are assigned rights.

3.7.5 The Bridge menu

3.7.5.1 Bridge menu command

Introduction

A bridge is a network component that connects two networks. A bridge is not dependent on the protocol; management of the data packages is based on the physical address of the network nodes (MAC address).

The IWLAN device provides bridge functionality because it handles data exchange between wired and wireless Ethernet. The following sections describe the functions that are available and how you configure and use them.

Deleting aged bridge information

The IWLAN device saves the information about which MAC address can be reached over which port in a learning table. Entries in this list are deleted automatically when there is no further data transfer for the corresponding MAC addresses by selecting the check box "Aging enabled". You can decide the length of time after which addresses are deleted if no data is sent using the "Aging Time" parameter on the start page of the "Bridge" menu.

3.7.5.2 WDS menu command

Note

The WDS menu command is available only in access point mode and when iPCF is not enabled.

Communication between access points

In normal operation, the access point is used as an interface to a network and communicates with clients. There are, however, situations in which several access points need to communicate with each other, for example to extend wireless coverage or to set up a wireless backbone. This mode is possible with WDS (Wireless Distributed System).

Note
Only for SCALANCE W788-xPRO/RR

With the firmware update to ≥ V3.0, the SCALANCE W788-xRR devices need to be reconfigured if you use WDS or redundancy and use the MAC address and not the sysName.

These functions are then based on the MAC address that changed with the introduction of VAPs with V3.0.

Configuration

In the "MAC / sysName" column, enter the MAC address or the system name of the access point with which you want to communicate. If you select the "Enc" check box, encryption is used.

Note

Correct security settings for WDS mode

In WDS mode, make sure that the security settings are correct for all devices involved. If settings are incorrect or not compatible on the individual devices, no data exchange is possible due to incorrect authentication. Note that the "Link" box in WBM shows only the connection and not the authentication.

Note

In WDS mode, the following restrictions apply:

- All access points that will communicate with each other must use the same channel.
- You can select either WEP or WPA(2)_PSK as the encryption method.
  If you want to use WPA_PSK or WPA2_PSK as the encryption method, you will need to set the WPA_PSK, WPA2_PSK or WPA/WPA2-AUTOPSK mode in the security settings and the WPA pass phrase on the relevant interface (VAP0). If a different security level is selected, you cannot use WPA(2)-PSK with WDS.
  To activate WPA(2)-PSK, select the "WPA_PSK" entry instead of a key.
  Once you have selected WPA-PSK or WPA2-PSK for a connection, all WDS connections must be protected by at least a WEP key.
- If you want to attach a different access point from the SCALANCE W78x over WDS, you must configure the MAC address. Detection using the "sysName" parameter does not work in this situation.
- In the IEEE 802.11h transmission mode, it is not practical to select the WDS mode. In WDS mode, all access points must use the same channel. If a signal from a primary user is detected by an access point, the channel is changed automatically and the existing connection is then terminated.
- As soon as you use the same channel for more than one WLAN interface, you will have to set WDS addressing using MAC addresses. Configuration with "sysName" can lead to registering with the wrong interface and probable impairment of communication.

Del

Select the check box in the "Del" column and then click the "Set Values" button to delete an entry from the list.

Sel

Select the check box in the "Sel" column and then click the "Set Values" button to assign a WDS function to an entry.

Link

> This column displays a green LED symbol for each active WDS connection. If there is no connection, a red LED symbol is displayed.

Enc

> Select this check box to be able to enable encryption in the "Key" column.

Key

> Select the key you want to use for encryption from the drop-down list box.

New Key

> If necessary, you can enter a new key for communication with the IWLAN device.

Edit Keys

> Clicking this button opens the "Security > Keys menu"

3.7.5.3 VLAN menu command

Note

The "VLAN" menu command is available only in access point mode.

Assignment and management of the VLAN IDs

> The "Current VLAN Configuration" page displays a table with an overview of the configured VLAN IDs (VID). The assignment of the configured ports of the access point is also displayed as a member of these VLANs.

> The "Name" is used to identify an entry within the current table. "Member List" displays 'U' for untagged member of a VLANs or '–' if a port is not member of a VLAN. The sequence is sorted from left to right in ascending order; in other words, according to the ID of the interface (WLAN 1, WLAN 1 VAP 1, WLAN 2 VAP 2… or WLAN 1 WDS 1, WLAN 1 WDS 2...).

> Entries in red, indicate members in the table, entries in black indicate the configured port VLAN IDs.

If an interface is member of a VLAN ID, that is not the same as the port VID, frames arriving from Ethernet with this VLAN ID are accepted. Outgoing frames, however, always have the port VLAN ID.

Click on "VID" or "Name" to open the configuration page for VLAN IDs. With "New", you create a new VLAN ID, with "Refresh", you can update the table.

Note

The Ethernet interface does not remove VLAN tags from outgoing frames.

If the VLAN is active, the WLAN interfaces always remove all VLAN tags from the outgoing frames.

The WLAN interfaces do not, however, remove any VLAN tags if no VLAN configuration is enabled.

Member List	Description
U	If VID equals port VID; in other words untagged frames from WLAN are given this VID.
U	If the port is a member of the VID; in other words, tagged frames from Ethernet are forwarded on this port.
—	If the port is not a member of the VID; in other words, all the frames coming from Ethernet are blocked / discarded with the corresponding VLAN ID. Frames containing unconfigured VIDs and untagged frames are always blocked if the VLAN is active.

VLAN ID settings

The VLAN ID box allows you to enter a new VID as long as no port is assigned explicitly as "Member". Otherwise, the VID can no longer be modified.

Representation	Settings	Description
1	**-**	Field can be edited. If all editable boxes are displayed in this way and if the VID is not configured as port VID, the VID is deleted when you exit this page. Clicking on the field changes to depiction 2.
2	**U**	Field can be edited. Clicking on the box changes to depiction 1.
3	**–**	Field cannot be edited. AI entries for VLAN membership are being used.
4	**U**	Field cannot be edited. VID corresponds to the port VID

Representation	Settings	Description
5	**U**	Field cannot be edited. Corresponding port is set to "all VIDs",
6	**X**	Field cannot be edited. Corresponding port is not configured so no VID can be assigned.

Ports

This page shows you an overview of the ports in the form of a table.

- **SSID**
  SSID for WLAN interface, no entry for WDS or management and redundancy.

- **Priority**
  Configured priority of the port.

- **Port VID**
  VLAN ID directly assigned to the port.

- **Member**
  The VLAN membership assigned to the port.

- **Enabled**
  VLAN support can then be enabled / disabled directly.

Note

If you use a Radius server for authentication, this must be accessible over the management VLAN. Among other things, the management port also handles the functions: HTTP, HTTPS, WBM, Telnet, SSH, Ping, DHCP, TFTP, SNMP, SNTP and Syslog.

Note

The IP and MAC-based nodes downstream from a client with enabled layer 2 tunnel function (L2T client) adopt the same VLAN properties as the client.

Example: An L2T client is connected to the access point over the WLAN1 VAP3 interface. WLAN1 VAP3 is a member of the VLAN ID 33 that is assigned priority 6. For the L2T port, this means that the devices connected downstream from the L2T client and the client itself are also members VLAN ID 33 with priority 6.

Specifying VLAN settings

Click on an entry in the "Port" column to open the dialog box. You can select from the following settings:

Enable VLAN

Select the "Enable VLAN" check box if you want to enable the VLAN function. If "Enable VLAN" is selected, all frames of this VAP are given a VLAN tag.

User priority

Specify the priority of the frames of this VAP with the "User priority" drop-down list box. The priority is evaluated by the connected VLAN-compliant switches (for example, SCALANCE X-400) of the network. The priority rises with the ascending numbers:

Note

The priority generally increases with the ascending numbers. The exception is priority 0, that has a higher priority than priority classes 1 and 2 and has the same priority as class 3.

- **0 - Best Effort (BE)**
  Normal data traffic

- **1 - Background (BK)**
  Non time-critical data traffic

- **2 - Spare (--)**
  This priority is reserved.

- **3 - Excellent Effort (EE)**
  Data traffic with highest priority

- **4 - Controlled Load (CL)**

- **5 - Video (VI), < 100 ms latency and jitter**
  Video/multimedia

- **6 - Voice (VO), < 10 ms latency and jitter**
  Voice over IP
  PNIO

- **7 - Network Control (NC)**
  Internal network control frames

Default setting is "0 - Best Effort (BE)".

Note

Both voice over IP and PNIO have priority 6.

Port VLAN ID

Here, you enter the VLAN ID (VID) of the VLAN on which the virtual access point will communicate.

The individual VLANs are configured in the VLAN-compliant Industrial Ethernet switches (for example SCALANCE X-400). The VID of a VLAN is in the range from 1 to 4094.

VLAN membership

Here, you specify the VLANs for which the virtual access point will be a member or which other VLANs the port VLAN ID (VID) entered above will be assigned to.

The following assignments are possible:

● **all configured VIDs**
  The VAP is a member of all VLANs.

● **specific VID sonly**
  The VAP is member only of the VLANs entered below.

Here, enter the VLAN ID (VID) of up to 8 VLANs in which the VAP will be a member.

3.7.5.4   Learning Table menu command

Assignment of MAC address and port

The learning table contains the information about whether a MAC address can be reached over the wired Ethernet interface or over the wireless interfaces. The IWLAN device obtains this information from the active data exchange. The learning table also contains information on clients and on up to eight devices connected downstream from it operating in the "Layer 2 Tunnel" mode.

3.7.5.5   ARP Table menu command

Assignment of MAC address and IP address

The ARP protocol (Address Resolution Protocol) obtains the corresponding MAC address of a known IP address. The page of this menu command also indicates the interface over which an address can be reached. The last column indicates how the information was obtained.

3.7.5.6   Spanning Tree menu command

> **Note**
>
> The "Spanning tree" menu command is available only when you use the access point mode.

Avoiding loops on redundant connections

The spanning tree algorithm allows network structures to be created in which there are several connections between two stations. Spanning tree prevents loops being formed in the network by allowing only one path and deactivating the other (redundant) ports for data traffic. If there is an interruption, the data can be sent over an alternative path. The functionality of the spanning tree algorithm is based on the exchange of configuration and topology change frames.

Definition of the network topology using the configuration frames

Network components exchange configuration frames known as BPDUs (Bridge Protocol Data Unit) with each other to calculate the topology. The root bridge is selected and the network topology created using these frames. The root bridge is the bridge that controls the spanning tree algorithm for all involved components. BPDUs also bring about the status change of the bridge ports.

Rapid Spanning Tree

The rapid spanning tree algorithm is based on the spanning tree algorithm. This was optimized in terms of the reconfiguration time. Typical reconfiguration times for Spanning Tree are between 20 and 30 seconds. With rapid spanning tree, the reconfiguration times are around 1 second. This was achieved by the following measures:

- **Edge Ports**
  A port defined as an edge port is activated after the hello time (the time between two configuration frames). When the hello time has elapsed, the station can be certain that no further configuration frame will arrive and that this port is an edge port. If the user wants to avoid the hello time, spanning tree can be disabled at this port.

- **Point to Point (direct communication between two neighboring stations)**
  By directly linking network components, a status change (reconfiguration of the ports) can be made without any delays. A point-to-point connection can, for example, be a WDS connection between two access points.

- **Alternate Port (substitute for the root port)**
  A substitute for the root port is configured. If the connection to the root bridge is lost, the station can establish a connection over the alternate port without any delay by reconfiguring.

- **Filter table**
  In rapid spanning tree, ports affected by a reconfiguration are immediately deleted from the filter table. With spanning tree, on the other hand, the point at which a port is deleted is decided by the time when the port was entered in the filter table.

- **Reaction to events**
  Rapid spanning tree reacts to events, for example an aborted connection, without delay. There is no waiting for timers as in spanning tree.

In principle, therefore with rapid spanning tree, alternatives for many parameters are preconfigured and certain properties of the network structure taken into account to reduce the reconfiguration time.

Note

Rapid Spanning Tree with redundant wireless traffic

Note the following special feature when using Rapid Spanning Tree with automatic path costs calculation (path costs = 0) with a redundant wireless connection:

The basis of the automatic calculation is always the maximum data rate of the first wireless interface, even it the data traffic is being handled over the redundant connection of the second wireless interface.

(Rapid) Spanning Tree configuration

The parameters used for the (Rapid) Spanning Tree protocol are displayed in the "(Rapid) Spanning Tree Properties" menu. If necessary, modify the following parameters to specify how the (rapid) spanning tree algorithm operates:

Enable (R)STP

Select the "Enable (R)STP" check box if you want to use the (rapid) spanning tree algorithm. If the check mark is not set, all ports are automatically in the 'Forwarding' status.

Version

The version decides whether the Rapid Spanning Tree protocol (RSTP) is used or whether the device is operated in compatibility mode of the Spanning Tree protocol (STP).

Bridge priority

The identification of the most efficient connection is always related to the root bridge, a network component that can be considered as a root element of a tree-like network structure. With the "Bridge Priority" parameter you can influence the selection of the root bridge.

The bridge with the highest priority (in other words, with the lowest value for this parameter) becomes the root bridge. If several network components in a network have the same priority, the station whose MAC address has the lowest numeric value will become the root bridge. Both parameters, bridge priority and MAC address together form the Bridge Identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the propagation time of the frames. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 through 61440.

Max Age

Max Age is the time (between 6 and 40 seconds) that a bridge waits for a configuration frame (BPDU). When this time has elapsed, the bridge attempts to reconfigure the network. The default setting for this parameter is 20 seconds.

Hello time

Each bridge regularly sends configuration frames (BPDUs). The interval (1 to 10 seconds) between two such frames is the "Hello time". The default for this parameter is 2 seconds.

Forward Delay

New configuration data is not used immediately by a bridge but only after the period (between 4 and 30 seconds) specified in the "Forward Delay" parameter. This ensures that operation is started with the new topology only after all the bridges have the required information. The default for this parameter is 15 seconds.

L2T Edge Port

Select this check box if there can be an end device on a layer 2 tunnel port. Otherwise a reconfiguration of the network will be triggered whenever a link to this port is modified.

L2T Auto Edge Port

Select this check box if you want to detect automatically at all layer 2 tunnel ports whether or not an end device is connected.

Spanning Tree Port settings

Port-specific parameters

This page displays the current port parameters. The settings are made either using the automatic function of the IWLAN device or by the user.

The columns of the port table show the following information:

- **Port**
  Specifies the ports to which the information relates. WLAN1 VAP2, for example, relates to the virtual access point VAP2 on the first WLAN interface.

- **Priority**
  You set the priority of the ports of a bridge with this parameter.
  If the path calculated by spanning tree is possible over several ports of a switch, the port with the highest priority (in other words the lowest value for this parameter) is selected. A value from 0 through 240 can be specified for the priority; the default is 128.

- **STP Cost & RSTP**
  These parameters are used to calculate the path that will be selected. The lower the value, the greater the probability that the corresponding path will be used. If several ports of a bridge have the same value, the port with the lowest port number will be selected. Depending on whether STP or RSTP was selected as the version, the value of STP Cost or RSTP Cost will be used.
  The calculation of the path costs is based mainly on the transmission speed. The higher the achievable transmission speed, the lower the value for Path Cost should be.
  Typical values for spanning tree and rapid spanning tree are as follows:
  (The values can, however, also be set individually.)

Data rate	Path costs STP	Path costs RSTP
100 Mbps	19	200,000
54 Mbps	33	370,370
48 Mbps	36	416,666
36 Mbps	43	555,555
24 Mbps	53	833,333
18 Mbps	58	1.111.111
12 Mbps	83	1,666,666
11 Mbps	90	1,818,181
10 Mbps	100	2,000,000
9 Mbps	111	2,222,222
6 Mbps	166	3,333,333
5.5 Mbps	181	3,636,363
2 Mbps	500	10,000,000
1 Mbps	1000	20,000,000

- **Edge**
  The following entries are possible in the this column.
  yes There is an end device on this port.
  no There is a spanning tree or rapid spanning tree device on this port.
  If an end device is connected, an IWLAN device can switch over the port more quickly without taking into account spanning tree frames. If a spanning tree frame is received despite this setting, the port automatically changes to the no setting for further stations.

  Note

  If clients with the layer 2 tunnel function enabled connect to the access point, a separate port is opened for each of these clients. These ports cannot, however, be configured for Rapid Spanning Tree. The settings (for example, priority and path costs etc.) of the cell over which the client is connected to the access point are adopted.

- **Point-to-Point (P.t.P.)**
  There is a point-to-point link when two RSTP-compliant network components are connected together over this port. There are three possible statuses :

  - **ForceTrue**
    Even with half duplex, a direct link is assumed.

  - **ForceFalse**
    Despite a full duplex connection, a point-to-point link is not assumed.

  - **Auto**
    Point-to-point is detected automatically. If the port is set to half duplex (shared media connection), a direct link is not assumed.

  - Example: A WDS connection between access points is always a half duplex connection. With the setting ForceTrue, a direct connection is assumed. With Auto, a direct connection is not assumed.

- **Enabled**
  Shows whether spanning tree is enabled or disabled for the port.

Configuration of a port for (Rapid) Spanning Tree

If you click on a port name in the first column, you open the "(Rapid) Spanning Tree Port Properties" page where you can make the following settings:

Enable (R)STP

Select this check box if you want the port to use the (rapid) spanning tree protocol.

Priority

Here, enter a value between 0 and 240 for the port priority. The lower the value, the higher the priority of the port.

Admin Path Cost

Here, you can enter a value for the parameter "STP" (between 1 and 65535) or "RSTP Path Cost" (between 0 and 200000000). The relevant value is then used depending on the selected version.
If you enter a zero for the "RSTP" value, the value for the path costs is calculated automatically.

Admin Edge Port

Select this check box if an end device is connected to this port, otherwise a reconfiguration of the network will be triggered by every link change.

Auto Edge Port

Enable this option if you want a connected end device to be detected automatically on this port.

Admin Point to Point Status

Here, there are three possible settings:

- **Shared media Connection** is selected:
  This corresponds to "ForceFalse" in the port table.

- **Point to Point Connection** is selected:
  This corresponds to "ForceTrue" in the port table.

- **Point to Point Connection** and **Shared Media Connection** are selected:
  This corresponds to "Auto" in the port table.

Note

Point-to-point means a direct connection between two stations. A shared media connection would, for example, be a connection from the Ethernet port to a hub or a WDS connection between two access points.

3.7.5.7   Storm Threshold menu command

Note

The "Storm Threshold" menu command is available in access point and in client mode. The function can only be used in client mode if NAT is disabled.

Limitation of broadcast and multicast frames

Storm Threshold is the maximum number of broadcast or multicast frames per second forwarded by the IWLAN device. If this limit is exceeded, the IWLAN device stops processing such frames for 30 seconds.

Enable Storm Thresholds

Select this check box to enable the "Storm Threshold" function.

Address Threshold

In this box, you enter the maximum number of broadcast or multicast frames with the same source MAC address that are forwarded per second.

Interface Threshold

In this box, enter the maximum number of broadcast or multicast frames that can be received and forwarded by a specific interface.

3.7.5.8   NAT menu command

Note

This menu item is available only with the following device variants:
- SCALANCE W746-1PRO
- SCALANCE W746-1
- SCALANCE W747-1RR
- SCALANCE W747-1
- SCALANCE W78x in client mode only

What is NAT?

With Network Address Translation (NAT), the IP address in a data packet is replaced by another. NAT is normally used on a gateway between a private LAN and an external network with globally valid IP addresses. A local IP address of the internal LAN is changed to an external global IP address by a NAT device at the gateway.

To translate the internal into the global IP address, the NAT device maintains a translation list.

What is NAPT?

In "Network Address Port Translation" (NAPT) or "Port Address Translation" (PAT), several internal source IP addresses are translated into the same external source IP address. To identify the individual source nodes, the port of the source device is also stored in the translation list of the NAT gateway and translated for the external address.

If several local clients send a query to the same external destination IP address over the NAT gateway, the gateway enters its own external source IP address in the header of these forwarded frames. Since the forwarded frames have the same global source IP address, the NAT gateway assigns the frames to the clients using different port number.

Note

NAT/NAPT is possible only on layer 3 of the ISO/OSI reference model. To use the NAT function, the networks must use the IP protocol.

When using the ISO protocol that operates at layer 2, it is not possible to use NAT.

NAT properties of the SCALANCE devices

When using the following WLAN clients as a NAT gateway, the WLAN clients must be connected with the local Ethernet devices over the Ethernet port:

- SCALANCE W746-1PRO
- SCALANCE W746-1
- SCALANCE W747-1RR
- SCALANCE W747-1
- W78x in client mode

The local IP address of the WLAN client on the Ethernet devices must be entered as the gateway address.

The address assignment differs depending on the communication direction:

- **From the Ethernet device to the NAT gateway**: "Dynamic" address assignment (NAT)
  The continuous address assignment is made automatically.

- **From the NAT gateway to the Ethernet device**: "Static" address assignment (NAPT)
  The address assignment is fixed and must be set as a parameter.

32 entries can be set as NAT gateways per WLAN client.

Configuration

Set the configuration on the "IP Network Address Translation" page with the following settings:

Enabled / Disabled

Select "Enabled" or "Disabled" from the drop-down list box at the top right if you want to enable or disable NAT.
A restart is necessary before the change takes effect.

Local IP address for Ethernet

Here, you enter the local IP address for the Ethernet port of the WLAN client.

Local subnet mask for Ethernet

Enter a subnet mask for the local Ethernet network here, if applicable.

Del

Select the "Del" check box if you want to delete the previous entries on this page.

Sel

Select the "Sel" check box if you want to enable the current entries.

Type

Here, you select the assignment TCP or UDP for the following global port. Parameters for TCP and UDP frames are set separately.

Global Port

Enter the number of the global port (for TCP or UDP).

Note

If the port is already occupied by a local service (for example Telnet), a warning is displayed. In this case, avoid using port 23 (Telnet), port 22 (SSH) and ports 80/443 (http/https: availability of the client with the WBM) as global port.

Local Address

Enter the local IP address of the Ethernet device here.

Local Port

Enter the number of the local port of the Ethernet device here.

Note

The following instructions apply only to the IP parameter assignment using the PST tool.

When the module is accessed with PST by a configuration computer, the address assignment differs depending on the interface:

- **PST over the wireless interface:**
  The "global" address is changed.
- **PST over the Ethernet interface:**
  The "local" address is changed.

Function of the DHCP server

Clients of the SCALANCE W-700 series or access points operating in client mode have a DHCP server. This server handles the address assignment for devices downstream of a client operating as a NAT gateway.

Note

The SCALANCE W744-1PRO and W744-1 devices cannot be used as DHCP servers.

Requirements

The following requirements must be met before you can use DHCP server of the SCALANCE W-700:

- NAT must be enabled for the client

- The devices in the local area network downstream from the client must be configured so that they request an IP address from a DHCP server.

Properties of the DHCP server

Note the following points if you use the DHCP server of the SCALANCE W-700:

- The DHCP server issues IP addresses only to devices connected to the Ethernet interface of the SCALANCE W-700.

- The DHCP server adopts the settings for the gateway and subnet mask from the configuration for NAT.

- The lease time for assigned IP addresses is fixed at 3600 seconds.

- The address assignment is not retained in the power supply of the client is interrupted or when the device is restarted. When power returns, you should therefore make sure that the nodes in the local area network request an IP address again. You should therefore only use dynamic address assignment for the following nodes:

  – Nodes that are used temporarily in the subnet such as service devices.

  – Nodes that have been assigned an IP address and send this as the "preferred address" the next time they request an address from the DHCP server (for example PC stations).

Service Location Protocol (SLP)

The Service Location Protocol is used to locate network services. In conjunction with devices of the type SCALANCE W786-2HPW, it is used in preference to other protocols to allow a HiPath access point to find a HiPath wireless controller on the WLAN side of a NAT gateway. For more detailed information on this topic, refer to the HiPath documentation. You can configure the SLP Directory Agent parameter for the DHCP server of a SCALANCE W-700.

Configuration

To configure the DHCP server on the "NAT" side, make the following settings:

DHCP Server enabled

Select this check box if you want to use the DHCP server of the SCALANCE W-700. This is only possible if you enabled NAT ("Enabled" selected in the drop-down list in the "IP Network Address Translation" row).

IP Pool start address

The start address of the range used for dynamic address assignment. The entire range for the dynamic address assignment must be located completely in the range specified by the subnet mask of the NAT configuration.

IP Pool end address

The end address of the range used for dynamic address assignment. The value in this box must be higher than the value in the "IP Pool start address" box.

SLP Directory Agent

A network node functioning as a directory agent stores information on the services available in the network. You can enter a maximum of 12 IP addresses of directory agents in this text box separated by commas.

New

Click this button to open a dialog box for the static assignment of addresses and ports for NAPT (Network Address Port Translation). To allow access from within a WAN to individual devices downstream from a client, different IP addresses are signed in the local area network and a single IP address with different port information in the WAN. You can make the following settings:

Type
The following alternatives are possible:

- TCP

- UDP

Global Port
Here, you enter a unique port for each node that will be used in the WAN.

Local Address
The IP address of the node in the local area network.

Local Port

The port in the local network via which a node communicates. You can enter the same port in the local area network for more than one node.

Note

If the DHCP server is enabled in conjunction with NAT, the WBM "Information" menu contains the menu item "NAT DHCP Server" with the IPNAT DHCP server lease table. This table contains the following information:

- MAC address
- IP address
- Type (dynamic or static, currently only dynamic)
- Remaining lease time of the IP address ("Rem. Time" column)
- Client ID

3.7.5.9   IP Mapping Table menu command

Note

This menu item is available only with the following device variants:

- SCALANCE W746-1PRO
- SCALANCE W746-1
- SCALANCE W747-1RR
- SCALANCE W747-1
- SCALANCE W78x in client mode

Note

IP mapping table

If "Layer 2 Tunnel" is configured for a client, the IP mapping table is not displayed.

WLAN access by several devices over a client

With the devices listed in the first paragraph, you can provide access to the WLAN for several devices with one client. This means that you do not need to equip every device with its own wireless client.

This so-called IP mapping is possible only if the connected devices are addressed only by IP frames. Communication at MAC address level (ISO/OSI layer 2) can

- be established with one component whose MAC address is configured on the client,
- be established with a maximum of eight components if the "Layer 2 Tunnel" function is selected.

The "Layer 2 Tunnel" setting meets the requirements of industrial applications in which MAC address-based communication takes place with several devices downstream from the client. Clients with this setting cannot connect to standard Wi-Fi devices and access points with firmware V3.0 or older.

MAC Mode

IP frames in the direction from the client to the access point always have the MAC address of the WLAN interface as the source MAC address. As a result, the ARP tables at the access point end always contain only the MAC address of the WLAN interface of the clients.

If there are further devices downstream from the client, the "Auto find 'Adopt MAC'" option should not be enabled. In this case, the MAC address would be assigned indiscriminately to the first device that signals over Ethernet.

If there is only IP communication between the access point and the client, the default setting "Adopt own MAC" can be retained. If you also want MAC address-based frames to be sent by devices behind the client, select the settings "Adopt MAC manually", "Auto find 'Adopt MAC'" or "Layer 2 Tunnel".

MAC address/IP address assignment

The client maintains a table with the assignment of MAC address and IP address to be able to send incoming IP frames to the correct MAC address. The "IP Mapping Table" menu command displays this table. In principle, any number of device is can be reached downstream from a client using IP. The client can manage up to eight devices.

Since the data throughput of a wireless connection cannot be increased indefinitely, a maximum of the devices should be managed by one client.

3.7.6 The Filters menu

3.7.6.1 Filters menu command

Note

The "Filters" menu command is available only in access point mode.

Below, you will find an explanation of the menu commands with which you can configure various filters and their parameters. This involves the following three filters:

- MAC Filter
- MAC Dir Filter
- Protocol filter

3.7.6.2 MAC Filters menu command

MAC filter

If the MAC filter is activated, communication with clients on the Ethernet side is possible only when their source MAC addresses are entered in the table. As an alternative, there is a possible setting with which access is denied for all specified MAC addresses. You can enter a maximum of 50 MAC addresses in the table.

With IP mapping of a access point in client mode, only the MAC address assigned to this device is relevant, the MAC addresses of the devices downstream from it on the Ethernet side are irrelevant for filtering.

Non-directional MAC Address Filter

On this page, you decide whether or not addresses will be filtered by the MAC filter. You can select from the following options:

WDS

If the "WDS" check box is selected, there is also filtering over the WDS ports.

Del

Select the check box for an entry you want to delete and then click the "Set Values" button to delete a list entry.

Sel

In this column, select the check boxes of all the list entries you want to include in the filtering in the account.

Selected MACs

With this check box, you can decide how the MAC addresses in the "Selected" column are handled during filtering. If you select "Blocked", the IWLAN device does **not** send the selected MAC addresses.

3.7.6.3   MAC Dir Filter menu command

Restriction of the data traffic between MAC addresses

It is possible to filter the data traffic intended for wireless clients linked to the access point. This filter is used to permit a specified MAC address access only to other specified MAC addresses. You can specify several source addresses or entries for one destination address. The communication of the destination address is then restricted to these entries. If a destination address is not entered in the filter, it is not subjected to any restrictions. On this page, you can select from the following settings:

Directional MAC Address Filter

With this check box, you can decide whether or not addresses are filtered.

Del

Select the check boxes for an entry you want to delete and then click the "Set Values" button to delete a list entry.

Sel

In this column, select the check boxes of all the list entries you want to include in the filtering in the account. The IWLAN device does not send any data packets between the devices of a selected entry.

New

After clicking this button, an input dialog for new entries opens. Enter the MAC address of the two devices for which you want to use the MAC Dir filter.

3.7.6.4 Protocol Filter menu command

Protocol selection

Without protocol filtering, the access point processes all data packets regardless of the protocol being used. To increase data security and to reduce load, it can nevertheless be useful to prevent communication using certain protocols.

Here, you are not restricted to the protocols included in the list in this menu. If necessary, you can add your own entries to this list. You can specify a maximum of 50 Ethernet II protocols for which filtering is required.

Protocol filter

On this page, you can decide whether or not protocols are filtered. If you select "Disabled", the IWLAN device executes all protocols. If you select "Enabled", the device filters according to the entries on this page. You can select from the following options:

Del

There is only a check box in this column for self-defined entries. In this case, you can delete a list entry by selecting the check box and then clicking the "Set Value" button.

Sel

The filter applies to all protocols for which the check box is selected in the "Select" column.

New

As default, this list contains a selection of the most common protocols. If you want to define a filter for protocols that are not listed here, you can add your own entries by clicking on the "New" button; the "Insert Ethernet Protocol" dialog opens with two input boxes. Enter the ID for the protocol in hexadecimal format in the "Index" box. The permitted values are 0x0001 and 0xFFFF. It is not necessary to enter the 0x ID for hexadecimal numbers.
Enter the protocol name in the "Name" box and confirm with "OK".

Selected protocols

With this check box, you can decide how the protocols in the "Selected" column are handled during filtering. If you select "Blocked", the IWLAN device does not send the selected protocols. If you select "Forwarded", the IWLAN device only allows communication with the specified protocols.

3.7.7 The I-Features menu

3.7.7.1 iQoS menu command (in access point mode only)

Note

This function is not available in iPCF mode.

Client-specific bandwidth reservation

iQoS (Quality of Service) is technique with which clients are assigned a certain bandwidth. Due to this assignment, there is a high probability that data transmission to these clients will be within a defined period. This technique can be useful when response times must be guaranteed. If non-iQoS-clients put too much load on the network, they can be logged off from the AP to guarantee data traffic for iQoS clients.

Note

To ensure problem-free functioning of the iQoS mode, the number of clients with bandwidth reservation is restricted to four.

Note

If the user reserves data for critical clients, this data rate also includes the frame header (in other words, 802.11, MAC, IP, TCP, and S7 header). A SIMATIC user must therefore take into account not only the net data during configuration but also the headers.

---

iQuality of Service

On this page, you can decide whether or not the IWLAN device reserves bandwidth. If you select "Disabled", bandwidth reservation is disabled. If you select "Enabled", the IWLAN device reserves bandwidth according to the entries on this page. If you select "Enable (Static)", bandwidth reservation is based only on the minimum data transmission rate. You can select from the following options:

Del

Select the check box for an entry you want to delete and then click the "Set Values" button to delete a list entry.

Sel

The bandwidth reservation applies to all devices for which the check box is selected in the "Select" column.

New

> After clicking this button, an input dialog for new entries opens. Enter the MAC address of the device and the bandwidth reserved for this device.

Response Time

> In the "Response Time" input box, you enter the required response time of the access point over the wireless interface. Remember that this value represents the transmission time for the data from the access point to the client. The data transmission rate for nodes not included in the list is reduced according the value specified.

3.7.7.2   iPCF menu command

Note

The iPCF menu command is available only for the following device variants:

- SCALANCE W78x-xRR
- SCALANCE W747-1RR
- SCALANCE W747-1
- IWLAN/PB Link PN IO

Note

With SCALANCE W78x-xRR devices, iPCF may only be enabled for one WLAN interface.

When should iPCF be used?

> iPCF can be recommended, in particular, when a high data throughput is required despite a large number of nodes or when extremely short handover times are required.
>
> With PNIO data traffic (**P**rofi**N**ET **IO**), the iPCF mechanism was further optimized by handling PNIO traffic with high priority.

Note

For PNIO communication, we always recommend that you enable the iPCF or iPCF-MC mode.

Stable PNIO communication is only possible when it is guaranteed that a WLAN client is in a cell with more than 60% (-65 dBm) signal strength at all times. This can be checked by activating and deactivating the various segments.

This does not mean that the client needs to change when there is a signal strength less than 60% (-65 dBm). It is only necessary to make sure that a segment with adequate signal strength would be available.

What restrictions result from using iPCF?

The iPCF mechanism is a development of Siemens AG and functions only with nodes on which iPCF is implemented. With an access point with two WLAN interfaces, it is, however, possible to set both iPCF and standard WLAN at the same time. iPCF was optimized for the use of RCoax cable at the access point and achieves optimum performance only with this configuration.

Configuration

Select the "iPCF Enabled" check box to enable the iPCF mode.

With the SCALANCE W78x-xRR models, you can also set optimized support of PNIO if you select the "PNIO support enabled" check box. In this case, you must also set the "PNIO update time". The PNIO update time must match the configured PNIO update time.

AES-CCM encryption

You can only use the AES-CCM encryption method in iPCF mode. Make sure that a 128-bit WEP key is defined in the "Security > Keys" menu. When you have selected the "Strong AES-CCM encryption" check box, the display in the "Security > Keys" menu changes to "128 bit AES" and the device uses AES-CCM.

Optimization for omnidirectional antennas in conjunction with iPCF

Up to the SCALANCE W-700 firmware version V3.0, the use of the iPCF function is optimized for applications in which the RCoax cable is used as the antenna or directional antennas are used. In such applications, the client can always establish an optimum wireless connection to an access point.

As of firmware V3.1, the "Antenna Pattern" function was introduced that optimizes its use for cells with omnidirectional antennas. Due to the grater mobility of the clients in the illuminated space and the greater overlapping of cells, large fluctuations is signal strength are possible in this application. This makes it very difficult for the client to find an time to roam and to connect to the "correct" access point. On the one hand, the need to change must be detected as early as possible, while on the other, stable communication should not be delayed by roaming to often. This situation is now alleviated by an additional setting for omnidirectional antennas.

You should, however, bear in mind that the illumination of the RF field by RCoax or directional antennas is always more stable than by omnidirectional antennas. With "free space" wireless applications, the PROFINET IO cycle times must be adapted to the generally poorer wireless conditions.

Antenna Pattern

With the "Antenna Pattern" function, you can select one of the settings "Leaky/Directional Antenna" and "Omni-Antenna". The function is activated over the Web interface of the access point and affects the scan behavior of the logged-on clients. When the function is enabled, the data rates provided by the access point are also adapted to the application. We strongly recommend that you retain this default setting for the data rates.

PNIO update times

When setting the update time, make sure that you note the following situations otherwise there is a risk that you will not be able to establish stable communication:

Case a: Your system operates in a single cell; in other words the clients do not need to support roaming to another cell.

In this case, update times >= 8 ms are supported.

Case b: Your system operates with two cells on two different channels.

In this case, update times >= 16 ms are supported.

Case c: Your system operates with several cells and with more than 2 channels and the clients roam between cells.

In this case, the PNIO update time should be set higher than 16 ms.

Note

Roaming time for "free space" applications with omnidirectional antennas

Adapting the scan behavior to free space conditions, significantly increases the time required for roaming and has a detrimental effect on the PROFINET IO cycle time. The increase in roaming time is proportional to the number of channels to be scanned.

If you are using two cells that are operated with the Omni "Antenna-Pattern" setting, and when all clients have entered these two channels as "bkchannel", PNIO update times of 64 ms can be achieved.

Note

We strongly advise that you check the local wireless characteristics prior to commissioning. You will find detailed information on the topic of "Wireless LAN in a PROFINET IO Environment" on the Internet under the following entry ID: http://support.automation.siemens.com/WW/view/en/31938420

3.7.7.3   iPCF-MC menu command

Note

The iPCF-MC menu command is available only for the following device variants:

- SCALANCE W78x-2RR
- SCALANCE W747-1RR
- SCALANCE W747-1

When should iPCF-MC be used?

iPCF was developed to achieve short handover times when roaming between cells. However, iPCF achieves optimum performance only with RCoax cables. The iPCF-MC technique allows short handover times even for freely mobile clients and when a lot of cells are involved or a large number of channels is being used.

Note

For PNIO communication, we always recommend that you enable the iPCF or iPCF-MC mode.

Stable PNIO communication is only possible when it is guaranteed that a WLAN client is in a cell with more than 60% (-65 dBm) signal strength at all times. This can be checked by activating and deactivating the various segments.

This does not mean that the client needs to change when there is a signal strength less than 60% (-65 dBm). It is only necessary to make sure that a segment with adequate signal strength would be available.

What restrictions result from using iPCF-MC?

The iPCF-MC mechanism is a development of Siemens AG and functions only with nodes on which iPCF-MC is implemented.

How iPCF-MC works

iPCF-MC uses the two wireless interface of the access point in different ways: One interface works as the management interface and sends a beacon every five milliseconds. The other interface transfers the useful data.

The following requirements must be met before you can use iPCF-MC:

● All "RR" variants of SCALANCE W-700 access points with at least two interfaces can be used as the access points. All SCALANCE W-700 "RR" variants are suitable as clients.

● The management interface and data interface must be operated in the same frequency band and must match in terms of their wireless coverage. iPCF-MC will not work if both wireless interfaces are equipped with directional antennas that cover different areas.

● The management interfaces of all access points to which a client can change must use the same channel. A client scans only this one channel to find accessible access points.

● Transmission based on IEEE 802.11h cannot be used for the management interface. 802.11h is possible for the data interface.

Configuration

The SSID and the security settings only need to be configured for the data interface; they then apply automatically to the management interface.

Settings for access points

The following settings can be made:

● **iPCF-MC enabled**
if the check box is selected, iPCF-MC mode is enabled.

● **Strong AES-CCM encryption**
If this check box is selected, AES-CCM encryption is used. This is possible only if a 128-bit WEP key is defined in the "Security > Keys" menu.

● **PNIO update time**
Here, enter the PNIO update time configured for the network to which the access point is connected. The lowest value for the update time is 32 ms.

● **Interfaces**
Here, you specify which WLAN interface transfers the useful data ("data interface") and which interface sends the beacons ("management interface").

● **Channels**
This displays the channel and the frequency for the selected WLAN interfaces.

Note

Channel for the management interface

The management interfaces of all access points to which a client can change must use the same channel.

You can set the channel in the "Interfaces" menu of the WBM or in the branch "CLI\Interfaces\WLAN1" (or WLAN2) in the CLI.

Settings for clients

The following settings can be made:

- **iPCF-MC enabled**
  if the check box is selected, iPCF-MC mode is enabled.

- **Strong AES-CCM encryption**
  If this check box is selected, AES-CCM encryption is used. This is possible only if a 128-bit WEP key is defined in the "Security > Keys" menu.

- **Background scan interval**
  This parameter specifies the time between two client background scans (specified in iPCF cycles). If, for example, you select two, the client runs a background scan only in every second iPCF cycle.
  A lower value for the background scan interval provides the basis for fast roaming, however this means that no high data throughput can be achieved. A higher value should be selected for a high data throughput.

Note

iPCF and iPCF-MC are not compatible with each other and cannot be used at the same time on a device.

3.7.7.4 Forced Roaming on IP Down menu command (in access point mode only)

Note

Forced roaming on IP Down cannot be used in conjunction with iPCF or WDS on the same WLAN interface.

Configuration

After selecting the "Forced Roaming on IP Down" check box, you can configure the following parameters:

Forced Roaming on IP down

This function checks the IP connection to the specified host periodically. The WLAN interface is enabled or disabled depending on the current IP connection.

Destination IP address

The IP address of the device for which a connection will be monitored.

Interval (100 - 5000 ms)

Cycle time in milliseconds after which the IP connection will be checked.

Maximum lost packets (1 - 5)

Maximum number of consecutive lost packets after which the WLAN interface is deactivated.

WLAN interface state

Current status of the WLAN interface

3.7.7.5 Link Check menu command (in access point mode only)

Note

This function is not available in iPCF mode.

Note

With the Link Check function, you can only monitor connections to WLAN clients; use along with redundancy or WDS is not possible.

Table of monitored devices

In this table, you can see the following setting options available:

Link Check

In this drop-down list box, you specify whether the connection monitoring is:

● Enabled or

● Disabled

 Sel

Only connections to devices for which the check box in the "Sel" column is selected will be monitored.

Del

You can delete entries in the table by selecting the relevant check box in the "Del" column and clicking the "Set Values" button.

System event for connection abort

You can specify how the access point reacts to a connection abort (or to the reestablishment of a connection) in the **System > Events** menu.

3.7.7.6 Redundancy menu command (in access point mode only)

> **Note**
>
> The redundancy function described here is available only for access points that have more than one wireless adapter and that are not operated in iPCF mode.
>
> You can use the **WEP** encryption method.

Configuration with sysName

Instead of the MAC addresses, you can also configure the redundant partners with the "sysName" parameter. Beacons contain this parameter which is why the redundant device is detected using beacons.

> **Note**
>
> With the firmware update to to V3.0, the SCALANCE W78x-xRR devices need to be reconfigured if you use WDS or redundancy and use the MAC address and not the sysName.
> These functions are then based on the MAC address that changes with the introduction of VAPs with V3.0.

> **Note**
>
> If IEEE 802.1x or WPA is used, a "private key" must be selected for the redundant connection.

Redundancy enabled

Select this check box to enable the redundancy function.

Encryption enabled

Select this check box to enable the encryption of the data traffic.

Use system name / Use MAC addresses

The access point with which you want a redundant connection can be defined by:

- Use of the MAC address of its two interfaces or
- Use of the "System Name" parameter.

MAC address / System name

The input option for the relevant data appears depending on whether you select "Use system name" or "MAC addresses".

Encryption Key

Select the key you want to use for communication.

Link status

A connected link is indicated by a green LED symbol, a disconnected link by a red LED symbol.

3.7.7.7   IP Alive menu command (in access point mode only)

Table of monitored devices

In this table, you can see the following setting options available:

IP Alive

In the "IP Alive" drop-down list box, you specify whether the connection monitoring is:

- Enabled or
- Disabled

Sel

Only connections to IP addresses for which the check box in the "Sel" column is selected will be monitored.

Del

You can delete entries in the table by selecting the relevant check box in the "Del" column and clicking the "Set Values" button.

Monitoring independent of the port

With IP-Alive, you specify a monitoring time for an IP address and a port. If you do not want to monitor a particular port but rather only the data traffic from a particular IP address, simply enter 0 in Port. This resets the monitoring with each frame from this IP address.

System event for connection abort

You can specify how the access point reacts to change in the IP-Alive status in the **System > Events** menu.

Note

The IP-Alive function is not available in iPCF mode.

Note

If the IP Alive function does not detect any data traffic for the specified time, the status of the IP address is set to "Offline" and the error status activated. The error status must be confirmed before the IP Alive function sets the status for active data traffic back to "Online".

3.7.7.8　AeroScout menu

Information on AeroScout

This page shows a table with information on forwarding AeroScout frames:

- **Tag Information forwarding**
  In the management program that evaluates the AeroScout frames, you can specify whether or not an IWLAN device will forward frames. Here, you can see which setting was made in the management program.

- **AeroScout module**
  For each WLAN interface of the IWLAN device, you can specify how the AeroScout frames are handled. If you have enabled forwarding, "Enabled" is displayed here, otherwise "Disabled".

- **Engine port**
  The IWLAN device expects UDP packets from the management program at port 1144.

- **Response port**
  The IWLAN device forwards received AeroScout frames to the port specified here.

- **Response IP**
  The IP address of the computer on which the management program for evaluation of the AeroScout frames is running.

- **Multicast address**
  The tag sends frames as multicast. This multicast address is configured in the management program and displayed here.

- **Acknowledgements sent**
  The number of acknowledgments sent by the IWLAN device reflects the number of received UDP frames.

- **Messages dropped**
  The number of frames not forwarded. If, for example, an AeroScout tag is configured so that it sends on channel 1, the IWLAN device does not forward a frame received on channel 6.

- Whether or not the IWLAN device forwards AeroScout frames can be set separately for each WLAN interface.

- **AeroScout tags enabled**
  The IWLAN device forwards AeroScout frames when the check box is selected.

Note

The AeroScout function is not available in iPCF mode. Aeroscout can also not be used in the 5 GHz band or in "Turbo" mode.

3.7.7.9 iHOP menu command

Note

The iHOP menu command is available only for the following device variants:

*   SCALANCE W78x-2RR
*   SCALANCE W747-1RR
*   SCALANCE W747-1

Which settings influence iHOP?

The channels used by the iHOP function are specified with the following two parameters:

*   "Restricted channels" in the *Interfaces > WLANx >Advanced* menu (access point mode)

*   "Background scan channels" in the *Interfaces > WLANx > Advanced* menu (client mode)

When specifying the channels used, make sure that at least the same or more channels are defined on a client.

Example:
Access point A uses channels 1 and 6, access point B channels 11 and 13. The two access points are located in adjacent and partially overlapping cells. Within the area covered by both access points, there is a client whose "Background scan channels" include channels 1, 6, 11 and 13. The client can therefore communicate with both access points.

In the *Interfaces > WLANx* menu, you can select an additional mode [Mixed 5 GHz/2.4 GHz 54 Mbps (802.11 a + g)] in the "Wireless mode" drop-down list box after enabling the iHop function. If this mode is selected, it is possible to use the channels of both frequency ranges.

Note

If you select the mode "Mixed 5 GHz/2,4 GHz 54 Mbps (802.11 a + g)", you must not use antennas that are approved only for one frequency range. The use of RCoax is also not possible in this case.

Note

To achieve handover times in the range of a few hundred milliseconds, it is advisable to use no more that six channels in the iHOP system.

What restrictions result from using iHOP?

The iHOP function cannot be used at the same time as the PROFINET IO or PROFIsafe function.

Configuration

1. Select the "Enable" check box to enable the iHOP mode.

2. Select the wireless mode in the *Interfaces > WLANx* menu.

3. Select the *Interfaces > WLANx >Advanced* menu command and specify the channels in "Background scan channels" / "Restricted channels". The channels entered in "Restricted channels" must be a subset of the channels entered in "Background scan channels".

4. Enable "Background / Restricted channel select"

Note

If you operate a system with the iHOP function, you cannot use channels that are being used by existing PNIO systems with iPCF.

3.7.7.10   Dual client menu command

Note

The Dual Client menu command is available only for the following device variants:

- SCALANCE W78x-xRR
- SCALANCE W747-1RR
- SCALANCE W747-1

When should Dual Client be used?

The use of the dual client mechanism is particularly advisable when a high data throughput as well as very short handover times are required and security mechanisms according to IEEE 802.11i are being used.

Requirements for dual client

For each dual client connection, there must be two client devices connected over Ethernet. The two clients do not need to be of the same type.

The dual client mechanism is a development of Siemens AG. This means that both the clients and the access points involved must support this mechanism.

What restrictions result from using dual client?

Dual client cannot be used at the same time as other I features (iQoS, iPCF, iPCF-MC, iHOP). Standard WLAN clients can, however, establish a connection to an access point with which devices have already logged on in dual client mode.

Conditions for the use of RSTP

In conjunction with the Rapid Spanning Tree Protocol (RSTP), remember the following points:

● In the subnet in which clients in dual client mode are located there must be no network components with (R)STP functionality activated.

● All bridge ports of a SCALANCE W-700 access point that represent a station in dual client mode are automatically defined as edge ports when (R)STP is used. The creation of redundant network paths is prevented by the internal functionality of the dual client mechanism.

Dual Client enabled

Select this check box to enable dual client mode.

Mode

Here, you can see the interface over which the dual client mechanism will be handled.

Note

Roaming threshold

On the clients operating in dual client mode, the "Roaming threshold" parameter must have the same value. You will find the configuration option for this parameter in Web Based Management in the Interfaces > WLAN1 > Advanced menu.

3.7.8   The Information menu

3.7.8.1   Information menu command

System events and information on the protocols

The pages of this menu display tables contain information on system events and on the behavior of the following protocols:

● IP

● TCP

● UDP

● ICMP

● SNMP

3.7.8.2 Log Table menu command

Logging system events

This page lists system events and the time at which they occurred. You can specify which events are included here in the **System > Events** menu.

If you position the mouse pointer over a time value, the system time and date are displayed.

Clear

Click this button to delete the content of the table.

3.7.8.3 Auth Log menu command

Logging authentication

The pages of this menu contain a table with information on successful or failed authentication attempts.

Filter

With this check box, you select the authentication methods entered in this list.

Add

You can include the MAC address of a registered node directly in the "Access Control" list by selecting the check box beside the MAC address you want to include.

Rem

Select the check boxes for an entry you want to delete and then click the "Set Values" button to delete an entry from the list.

MAC address

The MAC address is displayed in this box.

Time

This box displays the date and time of the SNTP server if you have specified an SNTP server.

Event

This box displays the authentication statuses.

3.7.8.4 Versions menu command

Current versions and order numbers

This page displays information on the device:

- Hardware version
- Order number (MLFB)
- Boot software version
- Firmware version
- Ethernet MAC address
- Engineering mode
- Type of network attachment (RJ-45 electric/ST optical)
- Antenna mounting (internal/external)

3.7.8.5 Client List menu command

Note

This menu command is available only in access point mode.

You can select from the following settings:

Update

By selecting the "Update" check box, the list is updated automatically every 3 seconds. If you click on the MAC address of a client, you will receive additional information on this client.

Unit

With this check box, you can change the unit (dBm and %) for the measured values.

Logged-on clients

The table shows all the clients logged on at the access point along with certain additional information (wireless channel, status etc.).

- **MAC address**
  The MAC address of the client.

- **If#**
  This specifies the wireless interface over which the client is connected.

- **Signal**
  The signal strength of the client. The user can choose between percentage and dBm.

- **Age**
  Displays the time that has elapsed since the last client activity was detected.

- **Sec**
  This indicates whether encryption is enabled.

- **Channel**
  The current channel over which the client communicates with the access point.

- **State**
  The current state of the clients. The available options are as follows:

  – **Associated**
    The client is logged on.

  – **Active**
    This device is the active part of a dual client.

  – **Standby**
    This device is the part of a dual client that scans for access points.

3.7.8.6   Available WLAN menu command

Note

The "Available WLAN" menu command is only available for clients and access points in client mode.

You can make the following settings on this page:

Update

By selecting the "Update" check box, the list is updated automatically every 3 seconds. If you click on the MAC address of a client, you will receive additional information on this client.

Unit

With this check box, you can change the unit (dBm and %) for the measured values.

Available access points

This displays all access points to which the device can establish a wireless connection.

Note

If the iPCF mode is enabled on a SCALANCE W747-1RR or the IWLAN/PB Link PN IO, the display is different. Since the client does not run a background scan in this case, the only access points displayed are those to which the client had already established a connection.

If iPCF mode is disabled, the access points with which the client could connect are displayed after a successful background scan. If, for example, the security settings of the client do not match those of an access point, this access point would not appear in the list.

- **MAC Address**
  The MAC address of the access point.

- **Signal**
  The signal strength of the access point. The user can choose between percentage and dBm.

- **Sec**
  This indicates whether encryption is enabled.

- **Channel**
  The current channel over which the access point communicates with the device.

- **State**
  The current state of the access point. The available options are as follows:

  - **AP connected**
    A connection exists to this access point.

  - **AP conn. Actv**
    This connection exists between the access point and the active part of a dual client.

  - **AP conn. Stby**
    A standby connection exists between the access point and the part of a dual client that runs background scans.

- **SSID**
  Shows the SSID of the client.

3.7.8.7 Ethernet menu command

Information on the Ethernet interfaces

This menu command provides information on the current settings of the Ethernet interface. The current operating data is also displayed here.

Type

Contains information on the type of interface.

Description

Contains information on the interface.

MAC address

Displays the MAC address of the interface.

Last change

Indicates the time at which the interface last changed to the operational status "up".

Operational status

Displays the current operational status.

Admin status

Shows the readiness for operation of the interface.

Speed

Displays the bandwidth speed in Mbps.

Duplexity

Shows the mode "Full duplex" or "Half duplex".

Maximum packet size

Shows the maximum packet size that can be sent and received on the interface.

Unknown protocols

Displays the number of unknown protocols.

Output queue length

Displays the number of packets in the send buffer.

Total bytes

Displays the number of sent and received bytes.

Unicast packets

Displays the number of sent and received unicast packets.

Non-unicast packets

Displays the number of sent and received broadcast and multicast packets.

Discards

Displays the number of sent and received discard packets. Packets that are not recognized are discarded.

Errors

Displays the number errors in sent and received packets.

Note

There are no CLI commands for this menu command.

3.7.8.8   WLAN menu command

Information on the WLAN interface

This menu command provides information on the current settings of the WLAN interface. The current operating data is also displayed here. There is a separate menu for each wireless interface when the model has more than one wireless interface.

Traffic statistics on Wireless Interface

Statistics of the data to be transmitted are displayed here. The following values are displayed:

● **Association / Authentication Frames**
The frames relevant for registration are counted. A distinction is made between the registration frames Association and Authentication and the deregistration frames Disassociation and Deauthentication.

● **Signal strength**
The signal strength is displayed as an average of the last received frames or at the sending end of the last received Acknowledge frames.

● **Frame count**
Counter for all successfully received or sent frames.

● **Management frames**
Counts all received or sent management frames.

● **RTS frames**
Is incremented when a CTS frame is received in response to an RTS frame.

● **Avg. Rate**
Displays an average data rate of the most recently received or sent data frames.

● **Data frame count**
Counts all received or sent data packets.

● **Data bytes count**
Displays the sum of all received or sent bytes in a data frame.

● **Unicast**
Shows the sum of all received or sent unicast data.

● **Multicast**
Shows the sum of all received or sent multicast data.

● **Broadcast**
Shows the sum of all received or sent broadcast data.

Errors

This page displays statistics of the transmission errors that have occurred. If an increased number of errors (percentage) occurs, you should check the settings for the WLAN interface(s), the setup of the devices and the connection quality. The following values are shown in the table:

Receive Errors

- **ACL discarded frames**
  Number of client registration attempts that were blocked by the Access Control List. The percentage after the number of errors relates to the total number of received frames; this value is only calculated in the device is operating in access point mode.

- **Fragmentation errors**
  Number of failed fragmentations; in other words, at least one fragment of a frame was not received or received too late. The percentage shown following the number of errors relates to the total number of received data frames.

- **Encryption errors**
  Is incremented if a frame is received in which the WEP bit is set and the device operates without encryption, or the reverse situation when a frame is received without a set WEP bit and encryption is enabled. The percentage shown following the number of errors relates to the total number of received data frames.

- **Duplicate frames**
  Number of duplicated frames received. The percentage shown following the number of errors relates to the total number of received frames.

- **FCS errors**
  Number of frames in which the checksum was incorrect. The percentage shown following the number of errors relates to the total number of received frames including FCS errors.

- **Decrypt CRC error**
  Number of frames in which the checksum for the encrypted data buffer was incorrect. The percentage shown following the number of errors relates to the total number of received data frames.

Transmit Errors

- **Transmission errors**
  Is incremented when a frame could not be sent successfully despite hardware retries. The percentage shown following the number of errors relates to the total number of sent frames including failed send attempts.

- **Dropped frames**
  Number of frames that were discarded. Either the frame could not be sent successfully despite all the retries or the frame has not yet been sent and the recipient has logged off in the meantime. The percentage shown following the number of errors relates to the total number of sent frames.

- **Acknowledged errors**
  Number of frames that were not confirmed by an acknowledge. The percentage shown following the number of errors relates to the total number of sent unicast frames (both those sent without errors and those sent with errors).

- **RTS errors**
  Number of sent RTS frames that were not acknowledged by a CTS. The percentage shown following the number of RTS errors relates to the total number of sent RTS frames (both those sent without errors and those sent with errors). This value is relevant only for frames that exceed the value of the RTS/CTS parameter.

- **Retry count**
  Number of frames sent successfully that required one or more retries. The percentage shown following the number of errors relates to the total number of sent unicast frames.

- **One retry count**
  Number of frames sent successfully that required exactly one retry. The percentage shown following the number of errors relates to the total number of sent unicast frames.

- **Multiple retry count**
  Number of frames sent successfully that required more than one retry. The percentage shown following the number of errors relates to the total number of sent unicast frames.

Overlap AP

Note

This menu command is available only in access point mode.

For optimum data throughput, it is important that the set wireless channel is not used by other access points. In the 2.4 GHz band (802.11b or 802.11g), there is overlapping of the wireless channels so that an access point occupies not only the set channel but also the two or three adjacent channels. You should therefore make sure that there is adequate channel spacing to neighboring access points.

The "Overlap AP" page shows all access points that are visible on the set or adjacent channels (at 2.4 GHz). If entries exist here, the maximum data throughput of the access point will be restricted.

- **Type**
  Shows the type of connection. The types AP (infrastructure mode) and AdHoc exist.

- **MAC address**
  The MAC address of the wireless devices.

- **Channel**
  The channel on which the found wireless device transmits.

- **Signal**
  Shows the signal strength with which the other wireless devices are received at the AP. The stronger the signal, the greater the probability that they interfere with each other. There is also the possibility that they interfere with each other even at low signal strengths.

- **Age**
  Shows when the last activity was detected by the wireless device.

- **SSID**
  Shows the SSID of the other wireless device.

3.7.8.9 iQoS menu command

Information on bandwidth reservation

The pages of this menu provide information on iQoS. The clients are grouped as follows:

Traffic Statistics

- **Critical Compliant (CC)**
  This involves clients that were defined as critical and that are currently meeting the requirements you set for the bandwidth and response time.

- **Critical Non-Compliant (CNC)**
  The CNC clients are also clients with strict requirements regarding the response time and bandwidth. In contrast to the CC clients, however, these clients are not currently meeting these requirements.

- **Non-Critical Satisfied (NCS)**
  These clients do not have fixed requirements regarding the response time and minimum bandwidth. Their communication is currently restricted by iQoS.

- **Non-Critical Regulated (NCR)**
  These clients are also non-critical clients whose communication is, however, currently being restricted by iQoS in favor of critical clients.

- **Non-Critical Non-Responsive (NCNR)**
  Some clients that require no acknowledgment whatsoever for their communication (for example UDP traffic) cannot be regulated by iQoS. These are classified as NCNR.

- **Number of Clients**
  Shows the number of clients.

- **Framerate**
  Shows the number of frames per second.

Associated Clients Statistics

- **AID**
  Shows the 802.11 association ID.

- **SI**
  Shows the time period in which the client has a frame sent to it (in ms).

- **TX Bytes**
  Transferred bytes of the client being used.

- **TX Bytes**
  Received bytes of the client being used.

3.7.8.10   Spanning Tree menu command

Status of the Spanning Tree protocol

The upper part of the page shows the "RootID" and the "BridgeID". Both IDs are made up of their priority and their MAC address. Together, this results in the 16 character long ID. The RootID is the ID of the bridge that is currently the root bridge. The BridgeID shows the ID of the local device.

Below this, you can see values for the Topology Change event. The first value is a counter indicating how often the tree structure has changed since restarting. The value beside this, shows the time since the last switchover event.

You will also find the following values in the table:

- **Port Name**
  Plain language name of the port, for example Ethernet or WLAN1 WDS1.

- **Enabled**
  Indicates whether the (R)STP is enabled for this port. If the port is not enabled, no further frames are forwarded over this port.

- **Cost**
  Indicates the path costs for the port.

- **Priority**
  Indicates the current priority of the port.

- **Edge**
  Shows whether or not the port is an edge port.

- **P.t.P.**
  Shows whether or not the AP is connected directly to another (R)STP device

- **Port State**
  With STP, a port can adopt three states:

  - Discarding
    No frames are forwarded from or to this port. The port has been disable by the user or the protocol (for example, when a redundant path has been detected).

  - Learning
    The port receives packets in the same way as in listening mode, but does not forward them. The MAC addresses are also entered in the "Learning Bridge".

  - Forwarding
    The port is fully enabled. Frames can be received and sent.

  - Disabled
    The port is not currently in use.

- **State**
  Here, the state of the port in relation to the root bridge is displayed. The "ROOT" state means that the port is connected directly with the root bridge. "DESIGNATED" identifies all ports that are not directly at the root but that are enabled. Ports that are blocked are in the "BLOCKED" state.

3.7.8.11 IP menu command

Information on the IP protocol

The pages of this menu contain a table with information on the IP protocol. For more detailed information on the individual values in the table, refer to:

ftp://ftp.rfc-editor.org/in-notes/rfc1213.txt

Note

There are no CLI commands for this menu command.

3.7.8.12 TCP/UDP menu command

Information on the TCP/UDP protocol

The pages of this menu contain a table with information on the TCP/UDP protocol. For more detailed information on the individual values in the table, refer to:

ftp://ftp.rfc-editor.org/in-notes/rfc1213.txt

Note

There are no CLI commands for this menu command.

3.7.8.13 ICMP menu command

Information on the ICMP protocol

The pages of this menu contain a table with information on the ICMP protocol. For more detailed information on the individual values in the table, refer to:

ftp://ftp.rfc-editor.org/in-notes/rfc1213.txt

Note

There are no CLI commands for this menu command.

3.7.8.14   SNMP menu command

Information on the SNMP protocol

The pages of this menu contain a table with information on the SNMP protocol. For more detailed information on the individual values in the table, refer to:

ftp://ftp.rfc-editor.org/in-notes/rfc1213.txt

Note

There are no CLI commands for this menu command.

3.7.8.15   Signal Recorder menu command

Note

The signal recorder is available only for clients and access points in client mode and the IWLAN/PB Link PN IO.

Signal strength indicators

The Signal Recorder can record or display the signal strength of the connected access point. Using this data, you can locate areas with an inadequate signal strength. The Signal Recorder can be particularly advantageous when the client moves along a fixed path (for example suspension track).

- Procedure for WLAN clients:
  Using the URL
  http://<IP address>/Signal.txt
  or the URL
  http://<IP address>/Signal.log
  you can download the generated signal file. If you are not yet logged in, this opens the login window in which you must log in.

- Procedure for IWLAN/PB LINK PN IO:
  1. Enable the FTP server
  2. Enter `ftp <ip address>` in a DOS box.
  3. Log in as admin (default password admin)
  4. Enter the command get signal.txt.
  The signal.txt file is then stored in the directory from which the ftp command (point 2) originated.

Displaying the instantaneous value

The upper half of the window contains an instrument for displaying the graphic representation of the currently calculated dBm value in real time. Depending on your browser and the network load, the display is updated approximately every 500 ms. Apart from the graphic display, the current dBm value is also displayed in plain language. The MAC address of the access point with which the client is currently connected along with the frequency, channel and average transmission rate are also displayed and updated.

You can start and stop the graphic display with the buttons:

- **Start display** and
- **Stop display**

Note

Working with the graphic display can cause a not insignificant network load that can disturb time- and throughput-critical processes (PNIO).

Recording a series of measurements

The lower half of the window includes not only the operator controls for graphic display of the instantaneous value but also the controls for the actual signal recorder. You can set the interval between the acquisition of two measuring points as well as the total number of measuring points. Follow the steps outlined below:

Start recording / Stop recording

The recorder is controlled with the buttons:

- **Start recording** and
- **Stop recording**

Save recorder file / Display recorder graph

As soon as measuring points have been recorded and the recorder has been stopped, the following buttons are available:

- **Save recorder file**
  the measured values can be loaded directly from the client as a file in CSV format and imported into a suitable evaluation program.
  The CSV file contains the MAC address of the access point for every measuring point, the current number of the measurement, the raw value of the RSSI, the dBm value and its corresponding percentage value, a roaming indicator, the channel and the transmission rate.

- **Display recorder graph**
  The dBm values over time are displayed. If the client roams during the measurement, blue bars indicate the event. If you move the mouse pointer over such a bar or over the flag at the top of the bar, a tooltip with the MAC addresses of the two access points appears.

Print graph

With the "Print graph" button, it is easy to print the table. You will, however, need to make certain settings in the browser:

- Mozilla Firefox 1.5:
  In the "File" => "Page setup..." dialog, make sure that the "Print Background (colors & images) check box is enabled in the "Options" group box.

- Microsoft Internet Explorer 6.0:
  In "Tools" => "Internet Options" => "Advanced", the "Print background colors and images" check box must be enabled under "Printing".

The signal recorder itself does not cause any significant load in the network that could affect other processes.

Both parts of the signal recorder can be operated independently.

Below, you will find a few tips that will help you to obtain useful measurements with the signal recorder:

- Use a fixed data rate in the configuration.

- Where possible, the iPCF mode with as low an update time as possible should be set for the measurements.

- Make sure that there is enough data communication during the measurement because the statistics functions evaluate incoming frames.

- The measurement setup should be run through 2-3 times with the same parameters to find out whether losses of signal strength always occur at the same position.

- Selective measurements at a fixed position should be made over a certain time.
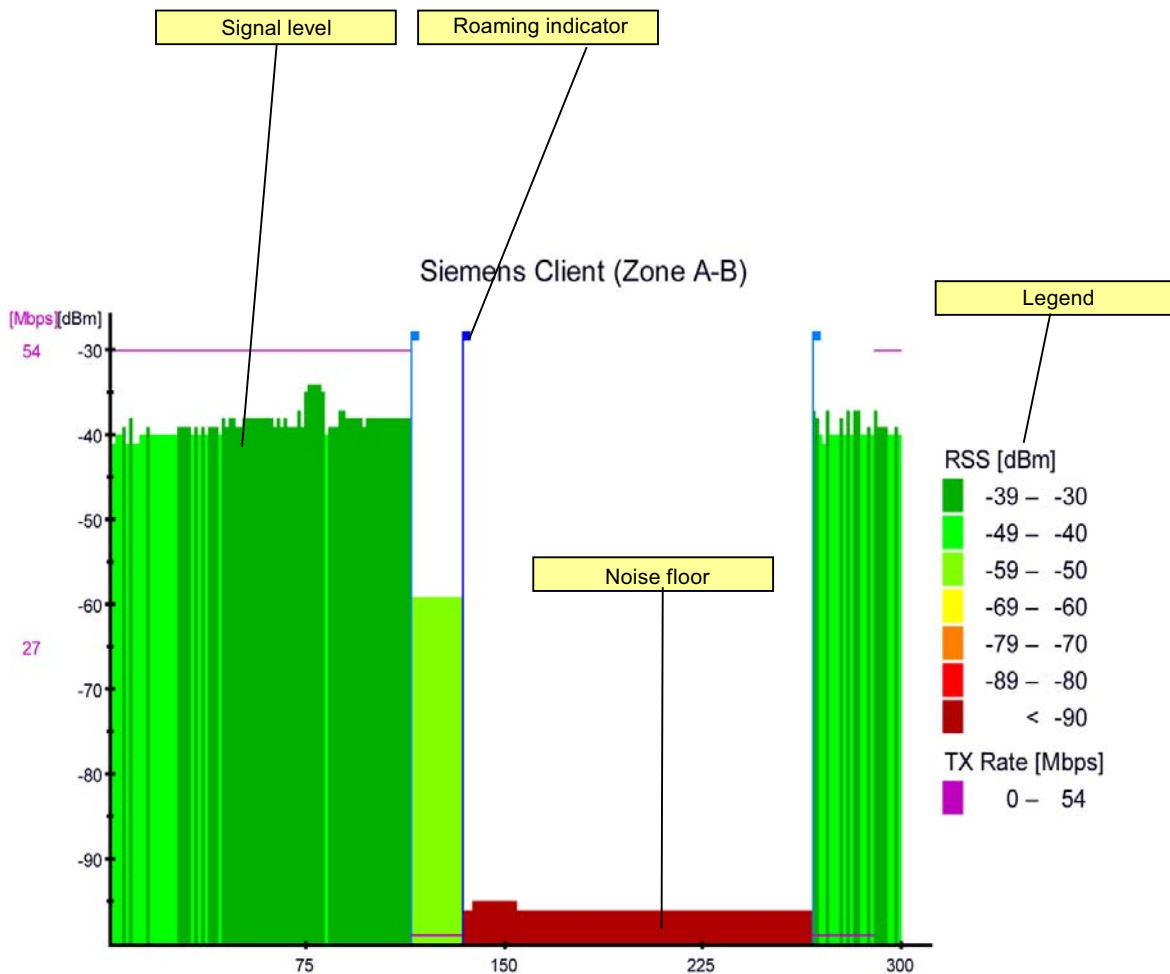
Recorded 300 samples, interval time 150 ms, min. -96 dBm, max. -34 dBm.

The following values are shown in the recording:

- **Roaming indicator**
  This value appears when the client connects to another or to no access point and the MAC address of the access point changes as a result.

- **Average data rate (Tx rate)**
  The average data rate is not displayed over the entire screen since it could overlap the signal level.

- **Noise floor**
  The noise floor represents the lower end of the technically possible transmission of the device. This means that when the noise floor is exceeded (the useful signal is louder than the noise floor), this is where the system dynamics begins. For this reason, this level is visible only when the client has no connection to an AP (indicated in the figure above by the MAC address 00-00-00-00-00-00).

- **Legend**
  Data rate (Tx rate) in Mbps
  RSS Received Signal Strength in dBm
  System name of the client (above the graphic)

3.8 Configuration with the Command Line Interface

3.8.1 General information on the Command Line Interface

Introduction

With the Command Line Interface (CLI), you can configure all the settings of a SCALANCE W-700 and an IWLAN/PB Link PN IO. The CLI therefore provides the same options as Web Based Management. You should read the detailed explanations of the parameters in the section "Configuration with Web Based Management".

The CLI also allows remote configuration over Telnet.

Note

You should only use the command line interface if you are an experienced user. Even commands that bring about fundamental changes to the configuration are normally executed without a prompt for confirmation.

Configuring an IWLAN/PB Link PN IO with the CLI

The IWLAN/PB Link PN IO only uses configuration over CLI. The "Comment" column in the following table shows which command is available for which device.

Starting the CLI in a Windows console

Follow the steps outlined below to start the Command Line Interface in a Windows console:

1. Open a Windows console and type in the command "telnet" followed by the IP address of the SCALANCE W-700:

   ```
   C:\>telnet <IP address>
   ```

2. Enter your login and password.

   As an alternative, you can also enter the command "telnet" followed by the IP address of the SCALANCE W-700 in the **Start > Run** menu.

Starting the CLI in Web Based Management

You can also call the CLI from Web Based Management. Click on the Console entry in the upper menu bar of Web Based Management. A console opens in which you can log on with your login and password. The IP address is adopted by Web Based Management.

Note

This function is not available in the Internet Explorer as of version 7.

Shortcuts for commands

As an alternative, instead of entering full CLI commands, you can simply enter the first letter or the first few letters of the command and then press the Tab key. The Command Line Interface then displays a command starting with the letter or letters you typed in. If the command displayed is not the command you require, press the Tab key again to display the next command.

Directory structure

Before you can enter a command in the Command Line Interface, you must first open the required menu or submenu. The following tables contain the commands of a menu and a description of them. The menu containing the commands is shown before the table. The table lists only the commands themselves.

Symbols for representing CLI commands

CLI commands generally have one or more parameters that are represented in the syntax description as follows:

- Mandatory parameters are shown in pointed brackets.
  Example: `<IP address>`

- Optional parameters are shown in square brackets.
  Example: `[E|D]`
  If you omit an optional parameter, the commands output the currently set value.

- Alternative input values are separated by the pipe character. In this case, you specify **one** of the listed values as the parameter.
  Example: `[E|D]`
  you enter either "E" or "D".

- If a numeric value is required as a mandatory parameter, you can also specify a range of values:
  Example: `<0 ... 255>`
  You enter a value between 0 and 255.

Cross-menu commands

You can use the commands in the following table in any menu.

CLI\ ... >

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
/	Moves you up to the highest menu level.	✓	✓	✓	✓	✓	✓
..	Moves you one menu level down.	✓	✓	✓	✓	✓	✓
?	Displays the commands and submenus available in the menu.	✓	✓	✓	✓	✓	✓
exit	Closes the CLI/Telnet session.	Cannot be called using the command shortcuts.					
		✓	✓	✓	✓	✓	✓
restart	Restart of the SCALANCE W-700 or IWLAN/PB Link PN IO	Cannot be called using the command shortcuts.					
		✓	✓	✓	✓	✓	✓
info	Displays information on the current menu item. Is not available in all menus.	✓	✓	✓	✓	✓	✓

3.8.2 The CLI\SYSTEM menu

3.8.2.1 CLI\SYSTEM menu command

Mode and locale setting

With the commands in this menu, you set the locale and mode (access point or client).

CLI\SYSTEM>

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`password [admin│user] [password]`	Specifies a password for access to the device.		Maximum of 31 characters.					
			✔	✔	✔	✔	✔	✔
`apmode [E│D│H]`	E	Access Point	—	—	—	—	✔	✔
	D	Client						
	H	HiPath Access Point (only available for SCALANCE W788-2RR prior to hardware redesign)						
`country [xx│?]`	Specifies properties for specific countries. The country codes ("xx") correspond to ISO 3166. You can see which countries you can set after entering the "country ?" command. A list of countries appears with the corresponding 2-digit code.		This command is not available in the version for USA.					
			✔	✔	✔	✔	✔	✔
`contact [name]`	Assigns a value to the *sysContact* MIB variable.		Maximum of 255 characters.					
			✔	✔	✔	✔	✔	✔
`name [system name]`	Assigns a value to the *sysName* MIB variable.		Maximum of 255 characters. If you want to use the name in WDS or redundancy, the maximum length is 32 characters.					
			✔	✔	✔	✔	✔	✔
`location [location]`	Assigns a value to the *sysLocation* MIB variable.		Maximum of 255 characters.					
			✔	✔	✔	✔	✔	✔
`ping [-c n │ -s] <IP│Name>`	For connection test to partner.		Telnet only					
	-c (counter) for the number n of ICMPs		✔	✔	✔	✔	✔	✔
	-s stops the connection test for all devices							

3.8.2.2 CLI\SYSTEM\IM menu command

Information on the device

> With the commands in this menu, you can specify information on the function and the location of the device.
>
> **CLI\SYSTEM\IM>**

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`functag [function information]`	Sets the information on the function of the device	—	✓	✓	✓	✓	✓
`loctag [location information]`	Sets the information on the location of the device	—	✓	✓	✓	✓	✓

3.8.2.3 CLI\SYSTEM\IP menu command

IP address assignment

> With the commands in this menu, you specify how the device obtains its IP address.
>
> **CLI\SYSTEM\IP>**

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`ip [IP address]`	Specifies the IP address for the SCALANCE W-700.	When you enter a valid IP address, enabled DHCP is automatically disabled.					
		—	✓	✓	✓	✓	✓
`subnet [subnet mask]`	Specifies the subnet mask.	—	✓	✓	✓	✓	✓
`gateway [IP address]`	Specifies the IP address of the router.	—	✓	✓	✓	✓	✓
`dhcp [E|D]`	Enable / disable DHCP server.	—	✓	✓	✓	✓	✓
`ttl [TTL value]`	Sets the TTL (Time To Live) parameter.	Default value: 64					
		—	✓	✓	✓	✓	✓
`dhcptype [M|N|C]`	Specifies how a device will be identified:	—	✓	✓	✓	✓	✓
	M — MAC address						
	N — Device name						
	C — Client ID						

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`clientid`	Specifies a client-ID for the device.	—	✓	✓	✓	✓	✓

3.8.2.4 CLI\SYSTEM\SERVICES menu command

Configuration options

With the commands in this menu, you select the services (SNMP, Web Based Management etc.) with which access to the device will be possible.

CLI\SYSTEM\SERVICES>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`telnet [E|D]`	Enable / disable configuration of the device over Telnet.	Only WEB and SNMP					
		✓	✓	✓	✓	✓	✓
`ttimeout [E|D|timeout in s]`	Enables / disables the time restriction for a Telnet session or sets the time.	✓	✓	✓	✓	✓	✓
`ssh [E|D]`	Enables / disables configuration of the device over secure Telnet.	✓	✓	✓	✓	✓	✓
`snmp [E|D]`	Enable / disable SNMP.	—	✓	✓	✓	✓	✓
`mail [E|D]`	Enable / disable E-mail.	—	✓	✓	✓	✓	✓
`web [E|D]`	Enable / disable configuration of the device over Web Based Management.	—	✓	✓	✓	✓	✓
`httpsonly [E|D]`	Enable / disable access for configuring only over HTTPS.	—	✓	✓	✓	✓	✓
`psu [E|D|RO]`	Enable / disable access to the device with the Primary Setup Tool or allow read only access.	—	✓	✓	✓	✓	✓
`ping [E|D]`	Enable / disable response of the device to Ping.	—	✓	✓	✓	✓	✓

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`lldp [T|R|E|D]`	Configuration of the Link Layer Discovery Protocol:		—	—	✔	✔	✔	✔
	T	The device sends LLDP information.						
	R	The device receives LLDP information.						
	E	The device sends and receives LLDP information.						
	D	LLDP information is neither sent nor received.						
`ftpserv [E|D]`	Enable / disable the FTP server on the device. Required for downloading the Signal.TXT file generated by the Signal Recorder.		✔	—	—	—	—	—

3.8.2.5 CLI\SYSTEM\RESTARTS menu command

Default settings and restart

With the commands in this menu, you can restore the factory settings of the device and restart the device.

CLI\SYSTEM\RESTARTS>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`restart`	Restart the device.	This command can be called from all menus, however not using the shortcut commands.					
		✔	✔	✔	✔	✔	✔
`memreset`	Resets the factory settings and triggers a restart (the protected settings are not deleted).	After restoring the factory settings, restart manually.					
		✔	✔	✔	✔	✔	✔
`defaults`	Resets to the factory settings (the protected settings are also deleted).	✔	✔	✔	✔	✔	✔

3.8.2.6 CLI\SYSTEM\EVENT menu command

Syntax of the Command Line Interface

For each of the four possible reactions E-mail, trap, log and fault, either "E" (Enabled = setting is enabled) or "D" (Disabled = setting is disabled) must be entered as the parameter. If, for example, an E-mail is sent when the device restarts (first parameter "CW") and an entry is made in the log table but neither a trap nor an error is generated, the following command must be entered:

`setec CW E D E D` (for SCALANCE W-700)

`setec CW D E D` (for IWLAN/PB Link PN IO)

Note

The IWLAN/PB LINK PN IO does not support E-mail. As a result, the second parameter for enabling/disabling the E-mail option is omitted.

CLI\SYSTEM\EVENT>

Commands available only for access points and client modules (not for IWLAN/PB Link PN IO):

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`setec CW <E|D> <E|D> <E|D> <E|D>`	Reactions when the SCALANCE W-700 restarts.	—	✓	✓	✓	✓	✓
`setec LU <E|D> <E|D> <E|D>`	Reaction to the "Link Up" event on the Ethernet interface.	If the error status was triggered only due to a link down event, the error states is cleared and the error LED goes off.					
		—	✓	✓	✓	✓	✓
`setec LD <E|D> <E|D> <E|D>`	Reaction to the "Link Down" event on the Ethernet interface.	—	✓	✓	✓	✓	✓
`setec AF <E|D> <E|D> <E|D>`	Reaction to a bad authentication over Web Based Management, CLI, or SNMP.	The SNMP trap "AuthFault" is sent only if there is a bad SNMP authentication.					
		—	✓	✓	✓	✓	✓
`setec PM <E|D> <E|D> <E|D> <E|D>`	Reaction to a change of power supply over the M12 power connection.	—	✓	✓	✓	✓	✓
`setec PE <E|D> <E|D> <E|D> <E|D>`	Reaction to a change of power supply over Ethernet.	—	✓	✓	✓	✓	✓

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`setec FC <E|D> <E|D> <E|D>`	Reaction to a change in the error status.	—	✓	✓	✓	✓	✓
`setec CP <E|D> <E|D> <E|D>`	Reaction when the cycle time in iPCF mode with PNIO support could not be kept to.	—	—	—	✓	—	✓

Commands available only for access points (not for access points in client mode, clients, IWLAN/PB Link PN IO):

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`setec AP <E|D> <E|D> <E|D> <E|D>`	Reaction to detection of an access point on own or an overlapping wireless channel.	—	—	—	—	✓	✓
`setec MS <E|D> <E|D> <E|D> <E|D>`	Reaction when the update time in iPCF mode with PNIO support cannot be kept to due to an additional client.	This command is available only with the following device variants: • SCALANCE W788-1RR • SCALANCE W788-2RR • SCALANCE W786-2RR • SCALANCE W784-1RR					
		—	—	—	—	—	✓
`setec CT <E|D> <E|D> <E|D> <E|D>`	Reaction when the specified update time in iPCF mode with PNIO support cannot be kept to.	This command is available only with the following device variants: • SCALANCE W788-1RR • SCALANCE W788-2RR • SCALANCE W786-2RR • SCALANCE W784-1RR					
		—	—	—	—	—	✓
`setec IS <E|D> <E|D> <E|D> <E|D>`	Reaction to a change in the connection status on a client for which the IP-alive monitoring is activated.	If the connection status changes, an event is triggered. If the connection no longer exists, the error state is triggered and the error LED is lit.					
		—	—	—	—	✓	✓
`setec LI <E|D> <E|D> <E|D> <E|D>`	Reaction when establishing a connection monitored with the *Link Check* function.	—	—	—	—	✓	✓
`setec IQ <E|D> <E|D> <E|D> <E|D>`	Reaction to a change in the iQoS status.	—	—	—	—	✓	✓
`setec RD <E|D> <E|D> <E|D> <E|D>`	Reaction to a change in the	—	—	—	—	✓	✓

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`<E|D>`	redundancy event status.	This command is available only with devices that have at least two interfaces.					
`setec CA <E|D> <E|D> <E|D>`	Reaction when a client logs on.	—	—	—	—	✔	✔
`setec CD <E|D> <E|D> <E|D>`	Reaction when a client logs off.	—	—	—	—	✔	✔
`setec FR <E|D> <E|D> <E|D>`	Reaction to the forced roaming on IP down function.	—	—	—	—	✔	✔
`setec ST <E|D> <E|D> <E|D>`	Reaction to a topology change by (rapid) spanning tree.	—	—	—	—	✔	✔
`setec WD <E|D> <E|D> <E|D>`	Reaction to the connection status of WDS.	—	—	—	—	✔	✔

Commands available only for the IWLAN/PB Link PN IO (not for access points and clients):

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`setec CW <E|D> <E|D> <E|D>`	Reactions to an IWLAN/PB Link PN IO restart.	✔	—	—	—	—	—
`setec P1 <E|D> <E|D> <E|D>`	Reaction to a change of power supply over power connection 1.	✔	—	—	—	—	—
`setec P2 <E|D> <E|D> <E|D>`	Reaction to a change of power supply over power connection 2.	✔	—	—	—	—	—
`setec FC <E|D> <E|D>`	Reaction to a change in the error status.	✔	—	—	—	—	—
`setec CP <E|D> <E|D>`	Reaction when the cycle time in iPCF mode with PNIO support could not be kept to.	✔	—	—	—	—	—

3.8.2.7 CLI\SYSTEM\EMAIL menu command

Sender and recipient of an E-mail

With the commands in this menu, you specify that the device sends an E-mail when certain events occur. You can also set a sender address.

CLI\SYSTEM\EMAIL

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`mail [E|D]`	Enable / disable the E-mail service.	—	✓	✓	✓	✓	✓
`smtp <IP address> [:port number]`	Specifies the IP address and the port number of the SMTP server.	—	✓	✓	✓	✓	✓
`from [text for sender field]`	Specifies the sender of E-mails from SCALANCE W-700.	—	✓	✓	✓	✓	✓
`email [E-mail address]`	Specifies the address(es) to which the SCALANCE W-700 sends E-mails.	Several E-mail addresses can be entered separated by semicolons.					
		—	✓	✓	✓	✓	✓

3.8.2.8 CLI\SYSTEM\SYSLOG menu command

Time-of-day synchronization in the network

CLI\SYSTEM\SYSLOG>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`server    [IP address]`	Specifies the IP address of the Syslog server.	Can only be changed with Admin rights.					
		✓	✓	✓	✓	✓	✓
`logs     [ D │ E ]`	Specifies whether the log entries are also sent to the Syslog server.	Can only be changed with Admin rights.					
		✓	✓	✓	✓	✓	✓
`auths    [ D │ E ]`	Specifies whether the authentication log entries are also sent to the Syslog server.	Can only be changed with Admin rights.					
		✓	✓	✓	✓	✓	✓

3.8.2.9   CLI\SYSTEM\SNMP menu command

Enabling SNMP

With the commands in this menu, you configure general SNMP parameters (enabling SNMP, traps and community strings)

CLI\SYSTEM\SNMP>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`snmp [E│D]`	Enables / disables SNMP.	Enables / disables SNMPv1, v2c, v3 and traps.					
		—	✔	✔	✔	✔	✔
`snmpv1 [E│D]`	Enables / disables SNMPv1/v2c.	Enables / disables SNMPv1, v2c and traps.					
		—	✔	✔	✔	✔	✔
`snmpv3 [E│D]`	Enables / disables SNMPv3.	The special features of SNMPv3 undertake effect after you disable SNMPv1. Enabling SNMPv3 does not automatically disable SNMPv1.					
		—	✔	✔	✔	✔	✔
`snmpro [E│D]`	Enables / disables SNMPv1/v2c read only.	—	✔	✔	✔	✔	✔
`getcomm [read community string]`	Specifies the read community string, maximum length 63 characters	The default is "public".					
		—	✔	✔	✔	✔	✔
`setcomm [write community string]`	Specifies the write community string, maximum length 63 characters.	The default is "private".					
		—	✔	✔	✔	✔	✔
`trapcomm [trap community string]`	Specifies the trap community string, maximum length 63 characters.	The default is "public".					
		—	✔	✔	✔	—	—
`traps [E│D]`	Enables / disables SNMPv1 traps	Traps are then enabled, if SNMP v1, v2c is also enabled.					
		—	✔	✔	✔	✔	✔

3.8.2.10 CLI\SYSTEM\SNMP\GROUP menu command

Managing SNMP groups

With the commands in this menu, you manage SNMP groups (creating, deleting etc.).

CLI\SYSTEM\SNMP\GROUP>

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`add <Name>` `[NOAUTH|AUTH|PRIV]` `[R|W]`	Adds an SNMPv3 group with the following security settings		Write access without read access is not possible.					
			—	✓	✓	✓	✓	✓
	NOAUTH	No authentication, no encryption						
	AUTH	Authentication with MD5 or SHA algorithm, no encryption						
	PRIV	Authentication with MD5 or SHA algorithm and encryption with the DES3 algorithm						
	Write and read access can also be set for the group:							
	R	Read access						
	W	Write access						
`edit <Index>` `[NOAUTH|AUTH|PRIV]` `[RE|RD|WE|WD]`	Changes the security level of the group and sets the access rights. You can display the index of the group with the "info" command.		You cannot edit the authentication and encryption settings unless the group is empty. Preventing read access also prevents write access. Permitting write access also permits read access.					
			—	✓	✓	✓	✓	✓
	RE	Enables read access						
	RD	Disables read access						
	WE	Enables write access						
	WD	Disables write access						
`delete <Index>`	Deletes the SNMPv3 group from the group list at the index position.		Is only possible to delete a group if it is empty.					
			—	✓	✓	✓	✓	✓
`clearall`	Clears all SNMP groups that are empty.		—	✓	✓	✓	✓	✓

3.8.2.11   CLI\SYSTEM\SNMP\USER menu command

Managing SNMP users

With the commands in this menu, you manage SNMP users (creating, deleting etc.).

CLI\SYSTEM\SNMP\USER>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`add <user name> <group name>` `[NONE|MD5|SHA]` `[authentication pw]` `[encryption pw]`	Assigns an SNMPv3 user to a group.	The authentication password and the encryption password can be a maximum of 63 characters long.					
	If authentication is necessary for the group, the algorithm must be specified as a parameter (MD5 or SHA). If encryption is necessary for the group, the encryption password must be specified as a parameter.	—	✓	✓	✓	✓	✓
`edit <index> <group name>` `[NONE|MD5|SHA]` `[authentication pw]` `[encryption pw]`	Changes the group assignment, the authentication algorithm, and the encryption password of the SNMPv3 user.	—	✓	✓	✓	✓	✓
`delete <Index>`	Deletes an SNMPv3 user from the list at the point identified by the index.	—	✓	✓	✓	✓	✓
`clearall`	Deletes all SNMPv3 users.	—	✓	✓	✓	✓	✓

3.8.2.12 CLI\SYSTEM\SNMP\TRAP menu command

Enabling SNMP traps, specifying trap recipients

With the commands of this menu, you configure SNMP traps.

CLI\SYSTEM\SNMP\TRAP>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`traps [E|D]`	Enables / disables SNMP traps.	Traps are then enabled, if SNMP v1, v2c is also enabled.					
		✓	✓	✓	✓	✓	✓
`settrap <entry> <IP address> <E|D>`	Specifies the IP address of the trap recipient "entry" ("entry" between 1 and 10) and enables / disables the sending of traps to this recipient.	✓	✓	✓	✓	✓	✓
`clearall`	Deletes all entries from the trap configuration table.	✓	✓	✓	✓	—	—

3.8.2.13 CLI\SYSTEM\SNTP menu command

Time-of-day synchronization in the network

With the commands in this menu, you specify the SNTP server and the time zone.

CLI\SYSTEM\SNTP>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`server [IP address]`	Specifies the IP address of the SNTP server.	—	✓	✓	✓	✓	✓
`tzone [hours]`	Specifies the deviation of the time zone of the SCALANCE W-700 according to UTC (Universal Time Conversion) in hours.	—	✓	✓	✓	✓	✓
`tzonemin [0|15|30|45]`	Minutes specified for the time zone.	—	✓	✓	✓	✓	✓
`interval [60...86400]`	Time of the SNTP update interval in seconds.	—	✓	✓	✓	✓	✓
`refresh`	Update of the SNTP time.	—	✓	✓	✓	✓	✓

3.8.2.14   CLI\SYSTEM\PNIO menu command

PNIO functionality for SCALANCE W-700 devices

With the commands of this menu, you configure the PNIO functionality.

CLI\SYSTEM\PNIO>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`devname <device name>`	Specifies the PNIO device name.	—	—	✓	✓	✓	✓
`allowdex [Y|N]`	Specified whether or not PNIO communication can take place.	—	—	✓	✓	✓	✓
`clear`	Clears the PNIO fault state and sets the device to the INC mode.	—	—	✓	✓	✓	✓

3.8.2.15   CLI\SYSTEM\FAULT menu command

Information on errors/faults

With the command in this menu, you display information on errors/faults that have occurred.

CLI\SYSTEM\FAULT>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`fault [OFF]`	Display the fault status and cause of the fault. The "OFF" parameter resets the fault LED and the fault status. Ideally, however, the cause of the problem should be eliminated.	You can reset the LED and the fault status with the command: "fault OFF". Ideally, however, the cause of the problem should be eliminated.					
		✓	✓	✓	✓	✓	✓
`ipacknow [Index|All]`	Displays or acknowledges (clears) the IP Alive messages requiring acknowledgment.	The fault state remains active until all the fault messages have been acknowledged. The fault state and the Fault LED are cleared if the only reason was an IP Alive error message. The command cannot be executed in client mode.					
		—	—	—	—	✓	✓

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`linkack [Index|All]`	Displays or acknowledges (clears) the Link Check messages requiring acknowledgment.	The fault state remains active until all the fault messages have been acknowledged. The fault state and the Fault LED are cleared if the only reason was a Link Check error message. The command cannot be executed in client mode.					
		—	—	—	—	✓	✓

3.8.2.16   CLI\SYSTEM\LOADSAVE menu command

Saving and loading device data

With the commands in this menu, you can save data from the device or load data to the device (configuration data, firmware, authentication data etc.).

CLI\SYSTEM\LOADSAVE>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`server [IP address] :[port number]`	Specifies the IP address and the port of the TFTP server.	✓	✓	✓	✓	✓	✓
`fwname [file name]`	Specifies the name of a file from which the firmware will be loaded or in which the firmware will be saved. This name can be a maximum of 32 characters long.	✓	✓	✓	✓	✓	✓
`fwload`	Loads the firmware from a file.	✓	✓	✓	✓	✓	✓
`fwsave`	Saves the firmware in a file.	✓	✓	✓	✓	✓	✓
`cfgname [file name]`	Specifies the name of a file from which the configuration data will be loaded or in which the configuration data will be saved.	✓	✓	✓	✓	✓	✓
`cfgload`	Loads the configuration data from a file	✓	✓	✓	✓	✓	✓
`cfgsave`	Saves the configuration data in a file.	✓	✓	✓	✓	✓	✓
`logname [file name]`	Specifies the name of a file in which the log table will be saved.	✓	✓	✓	✓	✓	✓
`logsave`	Saves the log table in a file.	✓	✓	✓	✓	✓	✓

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`cltcert <certificate>`	Specifies the name of the certificate for the client.	Available only for clients or access points in client mode.					
		✓	✓	✓	✓	✓	✓
`srvcert <certificate>`	Specifies the name of the certificate for the server.	Available only for clients or access points in client mode.					
		✓	✓	✓	✓	✓	✓
`cltpass <password>`	Authorizes use of the certificate.	Available only for clients or access points in client mode.					
		✓	✓	✓	✓	✓	✓
`cltsave`	Saves the client certificate in a file.	Available only for clients or access points in client mode.					
		✓	✓	✓	✓	✓	✓
`cltload`	Downloads the client certificate from a file.	Available only for clients or access points in client mode.					
		✓	✓	✓	✓	✓	✓
`cltdel`	Deletes the client certificate.	Available only for clients or access points in client mode.					
		✓	✓	✓	✓	✓	✓
`srvsave`	Saves the server certificate in a file.	Available only for clients or access points in client mode.					
		✓	✓	✓	✓	✓	✓
`srvload`	Downloads a server certificate from a file.	Available only for clients or access points in client mode.					
		✓	✓	✓	✓	✓	✓
`srvdel`	Deletes the server certificate.	Available only for clients or access points in client mode.					
		✓	✓	✓	✓	✓	✓
`pkgsave`	Saves the Configuration Package in a file over a TFTP server.	✓	✓	✓	✓	✓	✓
`sslcert`	Specifies the name of SSL certificate.		✓	✓	✓	✓	✓
`sslpass`	Specifies the password for SSL certificate.		✓	✓	✓	✓	✓
`sslsave`	Saves the SSL certificate in a file via TFTP.		✓	✓	✓	✓	✓
`sslload`	Loads the SSL certificate from a file using TFTP.		✓	✓	✓	✓	✓
`ssldel`	Deletes the SSL certificate.		✓	✓	✓	✓	✓

Note

The functionality can be controlled over SNMP with the OID 1.3.6.1.4.1.4196.1.1.4.100.1.5.1.19 (snDownloadEcmCfgPackageControl) and is also available for access points. Working with this function is analogous to working with the other OIDs in this group.

3.8.2.17 CLI\SYSTEM\C-PLUG menu command

Changing the data on a C-PLUG

With the commands in this menu, you write configuration data to a C-PLUG.

CLI\SYSTEM\C-PLUG>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`initdef`	Reinitializes the C-PLUG and copies the default configuration to the C-PLUG.	All information is deleted.					
		✓	✓	✓	✓	✓	✓
`initmem`	Reinitializes the C-PLUG and copies the configuration currently stored on the device to the C-PLUG.	All information is deleted.					
		✓	✓	✓	✓	✓	✓
`bootfrom [MEMORY]`	Displays the source medium from which the configuration is currently being read: C-PLUG or MEMORY. The changes only take effect after the next restart!	If the C-PLUG was removed, you specify that the configuration should be read from internal memory. If a C-PLUG is inserted, the device always attempts to read the configuration from the C-PLUG. The "bootfrom [MEMORY]" command then has no effect.					
		✓	✓	✓	✓	✓	✓
`cleanplug`	Erases the C-PLUG.	✓	✓	✓	✓	✓	✓
`preplug <dev>`	Writes the configuration data to a PRESET PLUG. The "dev" parameter specifies the device for which the PRESET PLUG will be suitable:	—	✓	✓	✓	✓	✓
	1	SCALANCE W788-1PRO					
	2	SCALANCE W788-2PRO					
	3	SCALANCE W788-1RR					
	4	SCALANCE W788-2RR					
	5	SCALANCE W744-1PRO					
	6	SCALANCE W746-1PRO					
	7	SCALANCE W747-1RR					
	8	IWLAN/PB Link					

3.8.3 The CLI\INTERFACES menu

3.8.3.1 CLI\INTERFACES\ETHERNET menu command

Settings for WLAN and Ethernet

With the commands of this menu, you configure the Ethernet interface.

CLI\INTERFACES\ETHERNET>

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`ethspeed` `[A｜100F｜100H｜10F｜10H]`	Specifies the transmission speed and mode of the Ethernet interface:		—	✔	✔	✔	✔	✔
			This command is available only on devices with an RJ-45 connector.					
	O	Automatic selection by the device						
	100F	100 Mbps full duplex						
	100H	100 Mbps half duplex						
	10F	10 Mbps full duplex						
	10H	10 Mbps half duplex						
`ethcross [E｜D]`	Specifies whether or not a crossover cable is used on the Ethernet interface:		—	✔	✔	✔	✔	✔
			This command is possible only when the transmission speed is not set automatically by the device ("etherspeed" command with parameter "A").					
	D	Standard cable not crossover	This command is available only on devices with an RJ-45 connector.					
	E	Crossover cable						

3.8.3.2 CLI\INTERFACES\WLAN1 (or \WLAN2 or \WLAN3) menu command

Network name, transmission mode and channel selection

With the commands in this menu, you set the network to which the device belongs and select the channels.

CLI\INTERFACES\WLAN1> (or \WLAN2 or \WLAN3)

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`port [E|D]`	Enable / disable wireless port.		—	✓	✓	✓	✓	✓
`adhoc [E|D]`	Select ad hoc or infrastructure mode.		Available only in the client mode. Not with iPCF.					
			—	✓	✓	✓	✓	✓
`vapno [0 ... 7]`	Specifies the number of virtual access points.		—	—	—	—	✓	✓
`adopt [MAC address]`	MAC address of the device connected to the client over Ethernet.		Available only in the client mode.					
			—	✓	✓	✓	✓	✓
`ssid [network name]`	Assigns a network name (SSID).		Only available in access point mode.					
			✓	✓	✓	✓	✓	✓
`mode [A|B|G|H|T|U|X]`	Selects the transmission standard:		✓	✓	✓	✓	✓	✓
	O	802.11a	Depending on the locale setting, some settings may not be possible and will then be rejected. 802.11a/g/h Turbo cannot be set in all countries.					
	B	802.11b						
	G	802.11g						
	H	802.11h						
	T	802.11a Turbo						
	U	802.11h Turbo						
	X	802.11g Turbo						
`autoadopt [E|D|OWN|L2T]`	Automatic adoption of the MAC address of the device connected to the client over Ethernet. The OWN parameter means that the client registers with the access point with its own Ethernet MAC address. With this setting, however, only IP data traffic is possible. The L2T parameter activates layer 2 tunneling. The client uses the MAC address of the Ethernet interface for the WLAN interface. The network is also informed of the MAC addresses connected to the Ethernet interface of the client.		Available only in the client mode. The OWN and L2T parameters are not supported by the device variants SCALANCE W744-1 and SCALANCE W744-1PRO.					
			—	✓	✓	✓	✓	✓
`autoch [E|D]`	Enable / disable the channel selection by the SCALANCE W78x.		Only available in access point mode.					
			—	—	—	—	✓	✓
`channel [1 ... 167]`	Specifies the wireless channel.		—	—	—	—	✓	✓
`outdoor [E|D]`	Enable / disable outdoor AP mode.		✓	✓	✓	✓	✓	✓

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`altchan [channel]`	Enters the channel number of the alternative DFS channel.	Possible only in 802.11h transmission.					
		—	—	—	—	✔	✔
`anyssid [E|D]`	With ANY SSID, the client connects to the best access point in the environment in which it is permitted to connect.	Available only in the client mode. Not with iPCF.					
		✔	✔	✔	✔	✔	✔
`802.11G`	Opens the "ADVANCED G" menu (802.11g).	✔	✔	✔	✔	✔	✔
`ADVANCED`	Opens the "ADVANCED" menu.	✔	✔	✔	✔	✔	✔
`DATARATES`	Opens the "DATARATES" menu.	—	—	—	—	✔	✔
`VAP1`	Opens the "VAP1" menu	Displayed only when vapno > 0.					
		—	—	—	—	✔	✔
`VAP2`	Opens the "VAP2" menu	Displayed only when vapno > 1.					
		—	—	—	—	✔	✔
`VAP3`	Opens the "VAP3" menu	Displayed only when vapno > 2.					
		—	—	—	—	✔	✔
`VAP4`	Opens the "VAP4" menu	Displayed only when vapno > 3.					
		—	—	—	—	✔	✔
`VAP5`	Opens the "VAP5" menu	Displayed only when vapno > 4.					
		—	—	—	—	✔	✔
`VAP6`	Opens the "VAP6" menu	Displayed only when vapno > 5.					
		—	—	—	—	✔	✔
`VAP7`	Opens the "VAP7" menu	Displayed only when vapno > 6.					
		—	—	—	—	✔	✔

3.8.3.3 CLI\INTERFACES\WLAN1\ADVANCED (or \WLAN2\ADVANCED or \WLAN3\ADVANCED) menu command

Configuring transmission characteristics

With the commands in this menu, you specify the parameters for the transmission characteristics such as the size at which a packet is fragmented or the antenna(s) to be used.

CLI\INTERFACES\WLAN1\ADVANCED> (or \WLAN2\ADVANCED or \WLAN3\ADVANCED) menu command

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`power [0...4]`	Specifies by how many dB the transmit power will be reduced compared with full power:	✔	✔	✔	✔	✔	✔
	0 Full power						
	1 -3 dB, half						
	2 -6 dB, quarter						
	3 -9 dB, eighth						
	4 Minimum power, -12 dB						
`beacon [20 ... 1000]`	Sets the beacon interval in milliseconds.	—	✔	✔	✔	✔	✔
`dtim [1 ... 255`	Sets the data beacon rate.	Only available in access point mode.					
		—	—	—	—	✔	✔
`rtsthr [1 ... 2346]`	Specifies the packet size as of which RTS/CTS is used.	—	✔	✔	✔	✔	✔
`fragthr [256 ... 2346]`	Specifies the size as of which packets are fragmented.	Not with iPCF					
		—	✔	✔	✔	✔	✔
`rchannel [channels]`	Selection of certain channels on which the access point can set up a cell. Enter the channels separated by blanks.	Only available in access point mode.					
		—	—	—	—	✔	✔
`rchsel [E│D]`	Enables/disables the "rchannel" function.	Only available in access point mode.					
		—	—	—	—	✔	✔
`bkscan [D│I│A]`	Specifies the mode in which the client scans for further access points.	—	✔	✔	✔	✔	✔
	D Disabled	Available only in the client mode.					
	I Scan if idle	Not with iPCF					
	O Scan always						
`bkscanint [200 ... 60000]`	Interval at which the client scans for further access points.	Available only in the client mode.					
		Not with iPCF					
		—	✔	✔	✔	✔	✔
`bkchannel [channels]`	Selects certain channels on which the client searches for further access points. The channels are entered separated by spaces.	Available only in the client mode.					
		✔	✔	✔	✔	✔	✔
`bkchsel [E│D]`	Enables / disables scanning for further access points on specific channels.	Available only in the client mode.					
		✔	✔	✔	✔	✔	✔
`force [E│D]`	Enables / disables roaming if the connection is lost on Ethernet interface.	Only available in access point mode.					
		—	—	—	—	✔	✔

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`roamthr`	Decides the threshold at which the client changes to another AP.		✔	✔	✔	✔	✔	✔
	low	Changes at a slightly higher field strength to the AP with the stronger signal.						
	medium	Changes at a moderately higher field strength to the AP with the stronger signal.						
	high	Changes only at a significantly higher field strength to the AP with the stronger signal.						
`swretry [E|D]`	Enables / disables the software retry functionality.		Not with iPCF					
			—	✔	✔	✔	✔	✔
`swretno [0 ... 15]`	Specifies the number of software retries.		✔	✔	✔	✔	✔	✔
`hwretno [0 ... 15]`	Specifies the number of hardware retries.		Not with iPCF					
			—	✔	✔	✔	✔	✔
`preamb [E|D]`	Enables / disables the short preamble.		When this function is enabled, higher data rates according to IEEE 802.11b are supported (higher performance).					
			✔	✔	✔	✔	✔	✔
`antenna [A|B|SA|SB|D]`	Specifies which antennas are used:		✔	✔	✔	✔	✔	✔
	O	Only antenna A	With the IWLAN/PB Link PN IO with one antenna socket, the default (Antenna A) must not be changed.					
	B	Only antenna B						
	SA	Antenna A sending, antenna B receiving.						
	SB	Antenna B sending, antenna A receiving.						
	D	Use the better of the two antennas (antenna diversity).						
`noise [A|L|M|H]11`	Set the noise filter.		✔	✔	✔	✔	✔	✔
	O	Automatic	A strong noise filter allows a more stable connection but also a shorter transmission range.					
	L	Low						
	M	Medium						
	H	High						

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`wmm [E│D]`	Enables / disables frame transmission taking into account priority.		Not with iPCF					
			✔	✔	✔	✔	✔	✔
`antgain [0...30]`	Entry of the antenna gain in dBi.		✔	✔	✔	✔	✔	✔
`anttype [0...n]`	Entry of the antenna type:		✔	✔	✔	✔	✔	✔
	0	User defined	To display the list, enter "anttype ?".					
	1	ANT792-6MN - gain: 6 dBi (2.4 GHz)						
	2	ANT793-6MN - gain: 6 dBi (5 GHz)						
	3	ANT795-6MN - gain: 6 dBi (2.4 GHz) 8 dBi (5 GHz)						
	4	ANT795-6DN - gain: 9 dBi (2.4 GHz) 9 dBi (5 GHz)						
	5	ANT792-8DN - gain: 14 dBi (2.4 GHz)						
	6	ANT793-8DN - gain: 18 dBi (5 GHz)						
	7	ANT792-4DN (RCoax Antenna) - gain: 4 dBi (2.4 GHz)						
	8	ANT793-4MN (RCoax Antenna) - gain: 6 dBi (5 GHz)						
	9	RCoax leaky wave cable - gain: 0 dBi (2.4 GHz) 0 dBi (5 GHz)						
	10	ANT795-4MR - gain: 3 dBi (2.4 GHz) 5 dBi (5 GHz)						
	11	ANT795-4MS - gain: 4 dBi (2.4 GHz) 5 dBi (5 GHz)						
`antcable [0 ... 30]`	Entry of the length of the antenna cable in meters.		✔	✔	✔	✔	✔	✔

3.8.3.4 CLI\INTERFACES\WLAN1\SSID (or \WLAN2\SSID or \WLAN3\SSID) menu command

Connection to a network

With the command in this menu, you configure the way in which a client connects to a network.

> **Note**
>
> The SSID List submenu is only available for clients and access points in client mode.

CLI\INTERFACES\WLAN1\SSID> (or \WLAN2\SSID or \WLAN3\SSID)

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`add <network name>`	Adds a network name (SSID) to the SSID list.	Available only in the client mode.					
		✔	✔	✔	✔	✔	✔
`edit <index> <network name>`	Changes the network name (SSID) at the <index> location in the SSID list.	Available only in the client mode.					
		✔	✔	✔	✔	✔	✔
`delete <index>`	Deletes the network name (SSID) from the SSID list at the <index> location.	Available only in the client mode.					
		✔	✔	✔	✔	✔	✔
`clearall`	Clears all network names (SSID) from the SSID list.	✔	✔	✔	✔	—	—

3.8.3.5 CLI\INTERFACES\WLAN1\802.11G (or \WLAN2\802.11G or \WLAN3\802.11G) menu command

Special options of the 802.11g standard

With the commands in this menu, you can configure specific properties of the 802.11g standard. You can, for example, specify how management and control data is sent in 802.11g mode.

CLI\INTERFACES\WLAN1\802.11G (or \WLAN2\802.11G or \WLAN3\802.11G)

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`ctsmode [0│1│2]`	Specifies whether the RTS/CTS method is used for 802.11g packets:		✔	✔	✔	✔	✔	✔
	0	Do not use CTS.	Not with iPCF.					
	1	Always use CTS.						
	2	CTS depending on whether 802.11b clients exist.						
`ctsrate [0│1│2│3]`	Specifies the data rate for 802.11g CTS frames:		✔	✔	✔	✔	✔	✔
			Not with iPCF					
	0	1 Mbps						
	1	2 Mbps						
	2	5.5 Mbps						
	3	11 Mbps						
`ctstype [0│1]`	Specifies the method for avoiding 802.11g packet collisions:		✔	✔	✔	✔	✔	✔
			Not with iPCF					
	0	CTS only						
	1	RTS/CTS						
`sslot [E│D]`	Enables / disables short slot times between data packets.		✔	✔	✔	✔	✔	✔
`only11g [E│D]`	When this is enabled, only the OFDM modulation technique is supported.		✔	✔	✔	✔	✔	✔
			Not with iPCF					

3.8.3.6 CLI\INTERFACES\WLAN1\DATARATES (or \WLAN2\DATARATES or \WLAN3\DATARATES) menu command

Variable setting of the transmission rates

With the commands of this menu, you can configure the transmission rate.

CLI\INTERFACES\WLAN1\DATARATES (or \WLAN2\DATARATES or \WLAN3\DATARATES)

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`info`	The following overview shows you the available transmission rates and their current configuration.	—	—	—	—	✔	✔
`default`	Enables the default setting for the current WLAN mode	—	—	—	—	✔	✔
`edit` `<rate> <E | D> <E | D>`	Changes the settings for the specified data rate (in Mbps). The two parameters indicate whether the rate should be used or is defined as "Basic Rate". Overview:	—	—	—	—	✔	✔

Rate	Enabled	Basic Rate	Example: The command "edit 5.5 d d" disables the data rate 5.5 Mbps. The overview shows the default setting for the 802.11g mode.
1	X	X	
2	X	X	
5.5	X	X	
6	X		
9	X		
11	X	X	
12	X		
18	X		
24	X		
36	X		
48	X		
54	X		

3.8.3.7 CLI\INTERFACES\WLAN1\VAP1..7 (or \WLAN2\VAP1..7 or \WLAN3\VAP1..7) menu command

Virtual access points

Note

Before you can configure this submenu command, you will need to enter the number of virtual access points using the "vapno" command in the "CLI\INTERFACES\WLAN1" menu.

With the commands in this menu, you make settings for virtual access points.

CLI\INTERFACES\WLAN1\VAP1..7> (or \WLAN2\VAP1..7 or \WLAN3\VAP1..7)

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`vap [E│D]`	Enable / disable virtual access point.	Only available in access point mode.					
		—	—	—	—	✓	✓
`ssid [network name]`	Assigns a network name (SSID).	Only available in access point mode.					
		—	—	—	—	✓	✓

3.8.4 The CLI\SECURITY menu

3.8.4.1 CLI\SECURITY menu command

Configuration of the SCALANCE W-700

With the command in this menu, you specify how the SCALANCE W-700 is configured.

CLI\SECURITY>

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`mgmteth [E│D]`	Configuration of the SCALANCE W-700 is:		—	✓	✓	✓	✓	✓
	E	Possible only over the wired Ethernet port.						
	D	Possible over all interfaces						

3.8.4.2 CLI\SECURITY\BASIC\WLAN1 (or \WLAN2 or \WLAN3) menu command

Security settings of the SCALANCE W-700

With the commands in this menu, you specify the security settings of the SCALANCE W-700.

CLI\SECURITY\BASIC\WLAN1> (or \WLAN2 or \WLAN3)

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`defkey [1|2|3|4]`	Selects the default WEP key.		✔	✔	✔	✔	✔	✔
`wpaphrase [WPA password]`	Enter the WPA-PSK password.		The password can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long.					
			✔	✔	✔	✔	✔	✔
`authent [0|1|2|3|4|5|6|7|8]`	Specifies the authentication type. For the parameter n, enter a number between 0 and 4 for the authentication type:		✔	✔	✔	✔	✔	✔
	0	Open System						
	1	Shared Key						
	2	WPA (RADIUS)						
	3	WPA-PSK						
	4	802.1x (RADIUS)	With the authentication types 7 (WPA-Auto) and 8 (WPA-Auto-PSK), the encryption method of WPA and WPA2 or of WPA-PSK & WPA2-PSK must be the same. Not with iPCF					
	5	WPA2						
	6	WPA2-PSK						
	7	WPA-Auto						
	8	WPA-Auto-PSK						
`encrypt [E|D]`	Encryption enabled / disabled.		✔	✔	✔	✔	✔	✔
`cipher [OFF|AUTO|WEP|AES|TKIP]`	Specifies the encryption scheme.		✔	✔	✔	✔	✔	✔
`grkint [interval]`	Specifies the "Group Key Update Intervals" in WPA-PSK.		Interval in seconds, (0; 36…36000), 0 = OFF					
			—	—	—	—	✔	✔
`supssid [E|D]`	Enable / disable Close Wireless System functionality.		—	—	—	—	✔	✔
`intracom [A|I|E]`	Allowed / Intracell or Ethernet blocking)		—	—	—	—	✔	✔
	Allowed	no restriction of data traffic						
	Intracell	blocking of data traffic between the clients in the cell						
	Ethernet	blocking of data traffic to Ethernet						

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`ssidcom [E|D]`	(Enable / Disable communication to other SSIDs)		—	—	—	—	✓	✓
	Enable	data traffic with other SSIDs permitted						
	Disable	data traffic with other SSIDs blocked						
`username [name]`	Specifies the user name for the RADIUS server.		✓	✓	✓	✓	✓	✓
	In client mode only.							
`password [password]`	Specifies the password for the RADIUS server.		✓	✓	✓	✓	✓	✓
	In client mode only.							
radauth	Sets the RADIUS authentication type to AUTO EAP_TLS EAP_TTLS PEAP		✓	✓	✓	✓	✓	✓
	In client mode only.							
`chkserver [E|D]`	Enables / disables authentication of the server.		✓	✓	✓	✓	✓	✓
	In client mode only.							
`preauth`	Enables preauthentication for WPA2		✓	✓	✓	✓	✓	✓
	In client mode only.							
`aging`	With WPA2, sets the renewal interval for the PMK in minutes		✓	✓	✓	✓	✓	✓
	In client mode only.							

3.8.4.3 CLI\SECURITY\BASIC\WLAN1\VAP1..7 (or \WLAN2\VAP1..7 or \WLAN3\VAP1..7) menu command

Security settings of the virtual access point

> **Note**
>
> Before you can configure this submenu command, you will need to enter the number of virtual access points using the "vapno" command in the "CLI\INTERFACES\WLAN1" menu.

With the commands in this menu, you specify the security settings of the virtual access point.

CLI\SECURITY\BASIC\WLAN1\VAP1> (or \WLAN2\VAP1 or \WLAN3\VAP1)

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78 x	W78x RR
`defkey [1|2|3|4]`	Select the default WEP key.		—	—	—	—	✓	✓
`wpaphrase [WPA password]`	Enter the WPA-PSK password.		The password can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long.					
			—	—	—	—	✓	✓
`authent [0|1|2|3|4|5|6|7|8]`	Specifies the authentication type. For the parameter n, enter a number between 0 and 4 for the authentication type:		—	—	—	—	✓	✓
	0	Open System						
	1	Shared Key						
	2	WPA (RADIUS)						
	3	WPA-PSK						
	4	802.1x (RADIUS)	With the authentication types 7 (WPA-Auto) and 8 (WPA-Auto-PSK), the encryption method of WPA and WPA2 or of WPA-PSK & WPA2-PSK must be the same.					
	5	WPA2						
	6	WPA2-PSK						
	7	WPA-Auto						
	8	WPA-Auto-PSK						
`encrypt [E|D]`	Encryption enabled / disabled.		—	—	—	—	✓	✓
`cipher [OFF|AUTO|WEP|AES|TKIP]`	Specifies the encryption scheme.		—	—	—	—	✓	✓
`grkint [interval]`	Specifies the "Group Key Update Intervals" in WPA-PSK.		Interval in seconds, (0; 36…36000), 0 = OFF					
			—	—	—	—	✓	✓
`supssid [E|D]`	Enable / disable Close Wireless System functionality.		—	—	—	—	✓	✓
`intracom [A|I|E]`	Allowed / Intracell or Ethernet blocking)		—	—	—	—	✓	✓
	Allowed	no restriction of data traffic						
	Intracell	blocking of data traffic between the clients in the cell						
	Ethernet	blocking of data traffic to Ethernet						
`ssidcom [E|D]`	(Enable / Disable communication to other SSIDs)		—	—	—	—	✓	✓
	Enable	data traffic with other SSIDs permitted						
	Disable	data traffic with other SSIDs blocked						

3.8.4.4 CLI\SECURITY\KEYS\WLAN1 (or \WLAN2 or \WLAN3) menu command

Specifying the WEP key

With the commands in this menu, you enter a key in the key table and edit it.

CLI\SECURITY\KEYS\WLAN1>
(or \WLAN2 or \WLAN3)

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`add <Len> <Key> [index]`	Adds at a key at the end or at the specified index in the table.	Indexes from 5 onwards are private keys					
		—	—	—	—	✓	✓
`edit <Index> <Len> <Key>`	Changes the key at the index location.	✓	✓	✓	✓	✓	✓
`delete <Index>`	Deletes the key at the index location.	✓	✓	✓	✓	✓	✓
`clearall`	Deletes all keys.	✓	✓	✓	✓	✓	✓

3.8.4.5 CLI\SECURITY\ACL\WLAN1 (or \WLAN2 or \WLAN3) menu command

Editing the access control list (ACL)

With the commands in this menu, you edit the entries in the access control list.

CLI\SECURITY\ACL\WLAN1>
(or \WLAN2 or \WLAN3)

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`aclmode [E|D|S]`	Global release of ACL:		—	—	—	—	✓	✓
	E	Enable	Only in access point mode					
	D	Disable						
	S	Strict						
`add <MAC> [A|Y|K|P][key]`	Create a new entry in the ACL:		—	—	—	—	✓	✓
	MAC	MAC address of the client	Only in access point mode					
	O	Allow						
	Y	Deny						
	K	Default key						
	P	Private key						
	Key	Key index for private key						

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`edit <index> [E│D] [A│Y│K│P] [key]`	Change an existing ACL entry:		—	—	—	—	✓	✓
	index	Number of the ACL entry	Only in access point mode					
	E	Enable						
	D	Disable						
	O	Allow						
	Y	Deny						
	K	Default key						
	P	Private key						
	Key	Key index for private key						
`delete <index>`	Delete an existing ACL entry: index number of the ACL entry		Only in access point mode					
			—	—	—	—	✓	✓
`clearall`	Deletes all ACL entries.		Only in access point mode					
			—	—	—	—	✓	✓

3.8.4.6 CLI\SECURITY\RADIUS menu command

Authentication over an external server

With the commands in this menu, you set, for example IP addresses, ports and password.

CLI\SECURITY\RADIUS>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`server [IP address]`	Specifies the IP address of the primary RADIUS server.	—	—	—	—	✓	✓
`server B [IP address]`	Specifies the IP address of the backup RADIUS server.	—	—	—	—	✓	✓
`port [port]`	Specifies the port of the primary RADIUS server.	—	—	—	—	✓	✓
`port B [port]`	Specifies the port of the backup RADIUS server.	—	—	—	—	✓	✓
`secret [password]`	Specifies the password for the primary RADIUS server.	—	—	—	—	✓	✓
`secret B [password]`	Specifies the password for the backup RADIUS server.	—	—	—	—	✓	✓
`maxreq [max. number]`	Maximum number of requests to the RADIUS server.	—	—	—	—	✓	✓

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`maxreq B [max. number]`	Maximum number of requests to the RADIUS server (backup server).		—	—	—	—	✓	✓
`reauth [E|D]`	Enables / disables reauthentication.		—	—	—	—	✓	✓
`Time_scr [S|L]`	Sets the time for reauthorization.		—	—	—	—	✓	✓
	S	Server						
	L	Local						
`authprd [time in s]`	Period for repeating authentication.		The default is 3600 s.					
			—	—	—	—	✓	✓

3.8.4.7   CLI\SECURITY\ACCESS menu command

Access permissions for IP addresses

With the commands in this menu, you specify the access permissions for IP addresses.

CLI\SECURITY\ACCESS>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`access [E|D]`	Enable / disable access control list.	—	✓	✓	✓	✓	✓
`statmgmt [A|D]`	It is possible to access or not possible to access the IP addresses of the access control list (Accessed / Denied).	—	✓	✓	✓	✓	✓
`add <IP>`	Adds a new IP address.	—	✓	✓	✓	✓	✓
`edit <Index|IP> [E|D]`	Enables / disables the entry in the table specified by the index or IP address.	—	✓	✓	✓	✓	✓
`delete <index|IP>`	Deletes the entry.	—	✓	✓	✓	✓	✓
`clearall`	Clears the access control list.	—	✓	✓	✓	✓	✓
`edit_r [E|D] [IP_1 IP_2]`	Adds a new IP range or edits the IP range.	—	✓	✓	✓	✓	✓
`delete_r`	Deletes an IP range.	—	✓	✓	✓	✓	✓
`clear_r`	Clears all IP ranges.	—	✓	✓	✓	✓	✓

3.8.5 The CLI\BRIDGE menu

3.8.5.1 CLI\BRIDGE menu command

Deleting aged bridge information

With the command in this menu, you specify the time after which old bridge information in the learning table is deleted.

CLI\BRIDGE>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`aging [E│D│aging time]`	Enables / disables automatic deletion of information on the assignment of MAC addresses and ports. With the Aging time parameter, you can change the time.	Values between 10 s and 1,000,000 s can be set for the aging time. The default value is 300 s (5 min).					
		—	✓	✓	✓	✓	✓
`learn`	Displays the learning table.	—	✓	✓	✓	✓	✓
`arp`	Displays the ARP table.	—	✓	✓	✓	✓	✓
`ipmap`	Displays the IP mapping table	—	✓	✓	✓	✓	✓
`STORMTHR`	Opens the storm threshold menu	—	✓	✓	✓	✓	✓
`NAT`	Opens the NAT menu	—	✓	✓	✓	✓	✓

3.8.5.2   CLI\BRIDGE\WDS\WLAN1 (or \WLAN2 or \WLAN3) menu command

Increasing network span with WDS

With the commands in this menu, you set the WDS mode (Wireless Distributed System) to increase the network span or to set up a wireless backbone.

CLI\BRIDGE\WDS\WLAN1>-(or \WLAN2 or \WLAN3)

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`edit <Index> [E|D] [SE|SD] [key]`	Changes the WDS connection specified by Index. With [E|D], you enable / disable the connection. With [SE|SD], you enable / disable the encryption. With [Key], you enter the key.	—	—	—	—	✔	✔
`delete <Index>`	Deletes the connection with the specified index.	—	—	—	—	✔	✔
`clearall`	Deletes all WDS connections.	—	—	—	—	✔	✔

3.8.5.3 CLI\BRIDGE\VLAN\VLAN_ID menu command

VLAN

With the commands in this menu, you specify the VLAN-ID.

CLI\BRIDGE\VLAN\VLAN_ID>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`info`	Shows the currently configured VLANs and their relationship to the ports.	—	—	—	—	✔	✔
`add <VLAN-ID> [u [ports]]`	Inserts a new VLAN. Ports: Specifies the port that will be configured for the VLAN. u: The port is a member of the VLAN, frames are sent without a VLAN tag. Examples: add 100 u 2 4 Creates an entry with the VLAN-ID 100. Ports 2 and 4 are members of this VLAN.	—	—	—	—	✔	✔
`edit <VLAN-ID> [- [ports],] [u [ports],]`	Changes the membership of ports in a VLAN. The parameters correspond to those of the add command. Examples: edit 100 - 2 Port 2 no longer belongs to the VLAN with ID 100.	—	—	—	—	✔	✔
`delete <VLAN-ID>`	Deletes the VLAN with the specified VLAN ID from the configuration of the SCALANCE W78x.	—	—	—	—	✔	✔

3.8.5.4 CLI\BRIDGE\VLAN\PORTS menu command

VLAN ports

With the commands in this menu, you set the properties of the VLAN port.

CLI\BRIDGE\VLAN\PORTS>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`info`	Displays an overview of the ports and corresponding VLAN settings.	—	—	—	—	✓	✓
`vlan <Port> <E|D>`	Enables / disables VLAN for the specified port.	—	—	—	—	✓	✓
`portvid <Port> <VLAN-ID>`	Frames received at the specified port without a VLAN tag are given a VLAN tag with the <VLAN-ID>.	—	—	—	—	✓	✓
`portprio <Port> <Priority>`	The priority assigned to untagged frames according to 802.1d.	—	—	—	—	✓	✓
`member <Port> <all|specific>`	The specified port is a member of all VLANs or only the VLAN configured in VLAN ID (specific, see above).	—	—	—	—	✓	✓

3.8.5.5 CLI\BRIDGE\SPANNING menu command

Spanning Tree properties

With the commands in this menu, you set the Spanning Tree properties.

CLI\BRIDGE\SPANNING>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78 x	W78x RR
`info`	Shows the current spanning tree configuration.	—	—	—	—	✓	✓
`spanning [E|D]`	Enables (E) or disables (D) the (R)STP algorithm.	—	—	—	—	✓	✓
`version [R	S]`	Specifies whether the Rapid Spanning Tree (R) or Spanning Tree (S) mode is used.	—	—	—	—	✓	✓
`bridge [0 ... 61440]`	This specifies the bridge priority for the SCALANCE W-700.	Default value: 32768					
		—	—	—	—	✓	✓
`maxage [6....40]`	Maximum age for configuration information. (specified in seconds).	Default value: 20 s					
		—	—	—	—	✓	✓
`hellotm [1...10]`	Specifies the interval between two BPDUs in seconds.	Default value: 2 s					
		—	—	—	—	✓	✓
`fwd_delay [4...30]`	Specifies the delay time for the effectiveness of configuration information (specified in seconds).	Default value: 15 s					
		—	—	—	—	✓	✓
`l2tadedge [T|F]`	Enable this option (parameter "T") if there can be an end device on a layer 2 tunnel port. Otherwise a reconfiguration of the network will be triggered whenever a link to this port is modified.	—	—	—	—	✓	✓
`l2tauedge [T|F]`	Enable this option (parameter "T") if you want to detect automatically at all layer 2 tunnel ports whether or not an end device is connected.	—	—	—	—	✓	✓

3.8.5.6 CLI\BRIDGE\SPANNING\PORTS menu command

Spanning tree port

With the commands in this menu, you set the Spanning Tree port properties.

CLI\BRIDGE\SPANNING\PORTS>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`info`	Displays the current spanning tree configuration.	—	—	—	—	✔	✔
`portstp <E│D> [ports]`	Enables / disables the spanning tree algorithm for the specified ports.	—	—	—	—	✔	✔
`portprio <Port> [0 ... 240]`	Specifies the priority of the port.	—	—	—	—	✔	✔
`stp_cost <Port> [1 ... 65535]`	Specifies the path costs for the port if Version is set to STP.	—	—	—	—	✔	✔
`rstp_cost <Port> [0 ... 200000000]`	Specifies the path costs for the port if Version is set to RSTP. If the value is 0, the value is calculated.	—	—	—	—	✔	✔
`edgeport <Port> [T│F]`	Specifies whether or not an edge port (T) or a station (F) that supports spanning tree or rapid spanning tree is attached to this port. If a (rapid) spanning tree protocol is received, the value F is displayed automatically.	—	—	—	—	✔	✔
`autoedge <Port> [T│F]`	Enable this option (parameter "T") if you want a connected end device to be detected automatically on this port.	—	—	—	—	✔	✔
`ptpport <port> <A│T│F>`	The point-to-point link establishes a direct link between two stations. In this case, you have the following options:	—	—	—	—	✔	✔
	O The port recognizes a PtP port based on the duplexity. If the connection is full duplex, it is assumed to be PtP, if it is half duplex, no PtP connection is assumed (shared medium).						
	T Specifies a PtP link, even though half duplex is being used.						
	F Specifies that there is no PtP link over the relevant port even with full duplex.						

3.8.5.7 CLI\BRIDGE\STORMTHR menu command

Storm threshold

With the commands in this menu, you set the storm threshold properties.

CLI\BRIDGE\STORMTHR>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`stormthr <E|D>`	Enables / disables the storm threshold function.	✓	✓	✓	✓	✓	✓
`broadcast <limit value>`	Specifies the maximum number of broadcast packets per second from the same source MAC address.	✓	✓	✓	✓	✓	✓
`multicast <limit value>`	Specifies the maximum number of multicast packets per second from the same source MAC address.	✓	✓	✓	✓	✓	✓
`broad_eth <limit value>`	Specifies the maximum number of incoming broadcast packets per second for the Ethernet interface.	✓	✓	✓	✓	✓	✓
`multi_eth <limit value>`	Specifies the maximum number of incoming multicast packets per second for the Ethernet interface.	✓	✓	✓	✓	✓	✓
`broad_1 <limit value>` `broad_2 <limit value>`	Specifies the maximum number of incoming broadcast packets per second for the first or second wireless interface.	✓	✓	✓	✓	✓	✓
`multi_1 <limit value>` `multi_2 <limit value>`	Specifies the maximum number of incoming multicast packets per second for the first or second wireless interface.	✓	✓	✓	✓	✓	✓

3.8.5.8 CLI\BRIDGE\NAT menu command

NAT (Network Address Translation)

With the commands in this menu, you set the NAT properties.

CLI\BRIDGE>nat

Note

This menu command is only available for clients and access points in client mode.

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`nat [E|D]`	Enables/disables NAT	—	—	✓	✓	✓	✓
`ip [IP address]`	Sets the local IP address for the Ethernet port	—	—	✓	✓	✓	✓
`subnet [Subnet mask]`	Sets the subnet mask for the Ethernet port	—	—	✓	✓	✓	✓
`dhcps [E|D]`	Enables / disables the DHCP server. The DHCP server can only be enabled if NAT is also enabled.	—	—	✓	✓	✓	✓
`startip [IP address]`	First address of the range from which addresses for the local area network are assigned.	—	—	✓	✓	✓	✓
`endip [IP address]`	Last address of the range from which addresses for the local area network are assigned.	—	—	✓	✓	✓	✓
`slpda [IP address list]`	IP addresses of directory agents. You can enter a maximum of 12 IP addresses separated by commas.	—	—	✓	✓	✓	✓
`STATIC`	Opens the "STATIC" menu	—	—	✓	✓	✓	✓
`info`	Shows all static NAT entries.	—	—	✓	✓	✓	✓
`add <TCP|UDP> <G port> <L IP> <L port>`	Creates a new static NAT entry. <G port> names the global port. The <L IP> parameter is the IP address in the local area network , <L port> is the local port.	—	—	✓	✓	✓	✓
`edit <Index> <E|D> [TCP|UDP] [G port] [L IP] [L port]`	Changes a static NAT entry with the specified <Index>. <G port> names the global port. The <L IP> parameter is the IP address in the local area network , <L port> is the local port.	—	—	✓	✓	✓	✓

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`delete <Index>`	Deletes the static NAT entry with the specified <Index>.	—	—	✓	✓	✓	✓
`clearall`	Deletes all static NAT entries.	—	—	✓	✓	✓	✓

3.8.5.9　CLI\BRIDGE\NAT\STATIC menu command

NAT STATIC

With the commands in this menu, you set the NAT STATIC properties.

CLI\BRIDGE\NAT>STATIC

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`add <Type> <G-Port> <L-IP> <L-Port>`	Add a static NAT entry:		—	—	✓	✓	✓	✓
	Type	TCP or UDP						
	G-Port	Global Port						
	L-IP	Local IP						
	L-Port	Local Port						
			In client mode only					
`edit <Index> <E|D> [type] [G-Port] [L-IP] [L-Port]`	Edit a static NAT entry:		—	—	✓	✓	✓	✓
	Index	Index in table						
	Type	TCP or UDP						
	G-Port	Global Port						
	L-IP	Local IP						
	L-Port	Local Port						
			In client mode only					
`delete <Index>`	Deletes a static NAT entry		—	—	✓	✓	✓	✓
			In client mode only					
`clearall`	Deletes all static NAT entries		—	—	✓	✓	✓	✓
			In client mode only					

CLI\BRIDGE\NAT\STATIC>info

Index	Enabled	Type	Global Port	Local IP	Local Port
1	X	TCP	21	172.27.138.2	1026

Example of static information

3.8.6 The CLI\FILTERS menu

3.8.6.1 CLI\FILTERS\MAC1FLT menu command

MAC Filter

With the commands in this menu, you set the MAC filter properties.

CLI\FILTERS

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`protshow`	Shows an overview of the editable protocol filters.	—	—	—	—	✔	✔
`mac1show`	Shows an overview of the editable MAC1 filters.	—	—	—	—	✔	✔
`mac2show`	Shows an overview of the editable MAC2 filters.	—	—	—	—	✔	✔

CLI\FILTERS\MAC1FLT>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`fltmac1 <E|D>`	Enables / disables the filter.	—	—	—	—	✔	✔
`statmac1 [F|B]`	If the value is set to F (forwarding), only packets with a source address contained in the table are forwarded. In mode B (blocking), these packets are blocked and all others are forwarded.	—	—	—	—	✔	✔

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`add <MAC addr.>` `[description]`	Adds a new address to the filter list. The optional description has no influence on the list and simply serves as information for the user.	—	—	—	—	✔	✔
`edit <Number│MAC> [E│D]` `[description]`	Changes the specified value.	—	—	—	—	✔	✔
`check_wds <E│D>`	Enables / disables checking including the WDS ports. With the E setting, the WDS ports are also monitored.	—	—	—	—	✔	✔
`delete <Number│MAC>`	Deletes the entry from the list.	—	—	—	—	✔	✔
`clearall`	Deletes all entries from the list.	—	—	—	—	✔	✔

3.8.6.2 CLI\FILTERS\MAC2FLT menu command

MAC-dependent communication paths

With the commands in this menu, you specify which device (MAC address) can communication with which devices (MAC address).

CLI\FILTERS\MAC2FLT>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`fltmac2 <E│D>`	Enables / disables the MAC filter.	—	—	—	—	✔	✔
`add <SourceMAC>` `<DestMAC>`	Adds a new entry with source and destination address to the filter.	—	—	—	—	✔	✔
`edit <Index> [E│D]` `[SourceMAC]` `[DestMAC]`	Changes the entry specified by Index. With [E│D], you can enable / disable the entry.	—	—	—	—	✔	✔
`delete <Index>`	Deletes the entry at the specified index position.	—	—	—	—	✔	✔
`clearall`	Deletes all entries for the MAC filter.	—	—	—	—	✔	✔

3.8.6.3 CLI\FILTERS\PROTO menu command

Protocol filters

With the commands in this menu, you set the protocol filter properties.

CLI\FILTERS\PROTO>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`fltprot <E|D>`	Enables / disables the protocol filter.	—	—	—	—	✔	✔
`statprot <F|B>`	The selected protocols are forwarded / not forwarded.	—	—	—	—	✔	✔
`add <Pattern> [description]`	Adds a new entry. A hexadecimal value is expected for the "Pattern" value. The user can enter a short note for this protocol as the description.	—	—	—	—	✔	✔
`edit <Index> [E|D] [Pattern] [description]`	Changes of enables / disables the filter entry.	—	—	—	—	✔	✔
`delete <Index>`	Deletes the filter entry.	—	—	—	—	✔	✔
`clearall`	Deletes all entries from the table.	—	—	—	—	✔	✔

3.8.7 The CLI\IFEATURES menu

3.8.7.1 CLI\IFEATURES\IQOS\WLAN1 (or \WLAN2 or \WLAN3) menu command

---

Note

This function is not available in firmware version 3.2.

Client-specific bandwidth reservation - Quality of Service (iQoS)

With the commands in this menu, you set the properties of the iQOS mode or obtain information on iQoS.

CLI\IFEATURE\IQOS\WLAN1> (or \WLAN2 or \WLAN3)

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`iqos [E|D]`	Enables / disables iQOS functionality.	—	—	—	—	✔	✔
`static [E|D]`	Enables / disables the calculation of the minimum transmission rate.	—	—	—	—	✔	✔
`response [response time]`	Specifies the response time for a client with bandwidth reservation.	15 – 1000 ms, default 50 ms					
		—	—	—	—	✔	✔
`add <MAC> <Max_BW> [E|D]`	Creating a critical client.	—	—	—	—	✔	✔
`edit <Index> <Max_BW> <E|D>`	Changes the setting of a client	—	—	—	—	✔	✔
`delete <Index>`	Deletes a critical client	—	—	—	—	✔	✔
`clearall`	Deletes all critical clients	—	—	—	—	✔	✔

The CLI also supplies detailed information on iQoS. In this view, the first part displays the current configuration, in other words whether iQoS is enabled, , whether the calculations and reservations are based on the static "worst-case" assumptions (static = enabled) or the current situation (static = disabled). The number of configured critical clients is also displayed.

```
Telnet 192.168.1.9                                                    _|□|×|
CLI\IFEATURES\IQOS\WLAN1>info

iQoS                         : enabled
static                       : disabled
Guarantie Time               : 50 ns
Critical Clients             : 1
Index !    MAC Address       ! Bandwidth (kbit/s) ! Enabled ! Accepted
-----------------------------+--------------------+---------+---------
    1 ! 08-00-06-2A-BB-06 !                 200 !    X    !    X

Traffic statistics (Timestamp: 100016 ms):

                        ! CC       ! CNC     ! NCS      ! NCR     ! NCNR
------------------------+----------+---------+----------+---------+--------
 Number of clients      ! 1        ! 0       ! 3        ! 0       ! 0
 Framerate              ! 193      ! 0       ! 470      ! 0       ! 0

Associated Clients:

 AID !    MAC Address       !  SI (ms) ! Status ! TX bytes    ! RX bytes
-----+------------------+----------+--------+-------------+-----------
    4 ! 00-0D-88-65-13-B1 !     1.62 ! NCS    ! 241711      ! 43041
    3 ! 00-05-5D-9A-13-FF !     1.62 ! NCS    ! 10049620    ! 10063453
    2 ! 08-00-06-2A-BB-06 !     0.0  ! CC     ! 509256      ! 512666
    1 ! 00-50-8B-5E-0B-DB !     1.62 ! NCS    ! 557405      ! 566839

SI   = shaper interval
CC   = critical compliant
CNC  = critical non-compliant
NCS  = non-critical satisfied
NCR  = non-critical regulatedNCR
NCNR = non-critical non-responsive

CLI\IFEATURES\IQOS\WLAN1>
```

The "Traffic statistics" table shows how many clients are currently in each status and how many packets of a particular class were sent for each of these classes.

The "Associated Clients" table provides an overview of all clients, their current classification, and the volume of sent and received data. The shaper interval (SI) is also is displayed for each client. The shaper interval is the minimum spacing between two packets of a client set by iQoS. For NCS clients, the SI is selected so that their bandwidth is twice the size of the current bandwidth.

3.8.7.2 CLI\IFEATURES\IPCF\WLAN1 (or \WLAN2 or \WLAN3) menu command

industrial Point Coordination Function (iPCF)

With the commands in this menu, you set the properties of iPCF.

CLI\IFEATURES\IPCF\WLAN1> (or \WLAN2 or \WLAN3)

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`ipcf [E|D]`	Enables or disables iPCF mode.	✓	—	—	✓	—	✓
`encrp [E|D]`	Enables / disables AES-CCM encryption	✓	—	—	✓	—	✓
`pnio [E|D]`	Enables or disables optimized PNIO support.	Only on SCALANCE W78x-xRR models (access point).					
		—	—	—	—	—	✓
`update [time]`	Specifies the PNIO update time for cyclic PNIO data exchange (in milliseconds). This value must match the configured PNIO cycle time. Valid values: 4, 8, 16, 32, 64, 128, 256, 512.	Only on SCALANCE W78x-xRR models (access point).					
		—	—	—	—	—	✓
`antpatt [0|1]`	Matches scanning to directional/RCoax antennas or omnidirectional antennas.						
	0 — Directional/RCoax antenna	—	—	—	—	—	✓
	1 — Omnidirectional antennas						

3.8.7.3 CLI\IFEATURES\IPCF-MC menu command

Rapid roaming for freely mobile clients

With the commands of this menu, you configure the iPCF-MC mode.

CLI\IFEATURES\ iPCF-MC>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`ipcf_mc [E|D]`	Enables / disables the iPCF-MC mode.	—	—	—	✓	—	Only 2RR
`data_int [1|2]`	Specifies the data interface.	—	—	—	—	—	Only 2RR
`mgt_int [1|2]`	Specifies the management interface.	—	—	—	—	—	Only 2RR

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`update [time]`	Specifies the PNIO update time for cyclic PNIO data exchange (in milliseconds). This value must match the configured PNIO cycle time. Valid values: 32, 64, 128, 256, 512.	—	—	—	—	—	Only 2RR
`encrp [E|D]`	Enables / disables strong AES-CCM encryption.	—	—	—	✔	—	Only 2RR
`bkscanint [1 ... 10]`	Sets the time for the background scan interval as a multiple of the PNIO update time.	—	—	—	✔	—	—

3.8.7.4 CLI\IFEATURES\FORCED_ROAM\WLAN1 (or \WLAN2 or \WLAN3) menu command

Cyclic connection monitoring of an IP address

With the commands in this menu, you set the properties of the forced roaming mode.

CLI\IFEATURES\FORCED_ROAM\WLAN1> (or \WLAN2 or \WLAN3)

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`froam [E|D]`	Enables of disables forced roaming on IP down.	—	—	—	—	✔	✔
`ip [IP address]`	Monitors the connection to this IP partner.	—	—	—	—	✔	✔
`interval [100 – 5000]`	Specifies the monitoring cycles to the IP partner in milliseconds.	—	—	—	—	✔	✔
`lostpkts [1 – 5]`	Specifies the maximum number of unanswered pings before the WLAN interface is disabled.	—	—	—	—	✔	✔
`vap [1 – 7]`	Before you can configure this submenu command, you will need to enter the number of virtual access points using the "vapno" command in the "CLI\INTERFACES\WLAN1" menu.	—	—	—	—	✔	✔

3.8.7.5 CLI\IFEATURES\LINKCHECK menu command

Device-related connection monitoring

With the commands in this menu, you set the properties of device-related connection monitoring.

CLI\IFEATURES\LINKCHECK>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`linkchk [E|D]`	Enable / disable device-related connection monitoring.	—	—	—	—	✔	✔
`add <MAC> [timeout]`	Adds a new MAC address for connection monitoring and specifies the monitoring time. No time is specified, the default is 500 ms.	—	—	—	—	✔	✔
`edit <Index|MAC> [E|D] [timeout]`	Modifies, enables, or disables an entry.	—	—	—	—	✔	✔
`delete <index|MAC>`	Deletes the specified entry from the list.	—	—	—	—	✔	✔
`clearall`	Deletes all entries for connection monitoring.	—	—	—	—	✔	✔
`acknow [Index|All]`	Displays or acknowledges (clears) the Link Check messages requiring acknowledgment.	The fault state remains active until all the fault messages have been acknowledged. The fault status and the LED are cleared if the reason for the fault status was only a link check error message.					
		—	—	—	—	✔	✔

3.8.7.6 CLI\IFEATURES\REDUNDANCY menu command

Redundant connection

With the commands in this menu, you set the properties of the redundant connection between two devices.

CLI\IFEATURES\REDUNDANCY>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`mac1 <MAC address>`	Specifies the device that will be operated redundantly along with the first wireless adapter.	—	—	—	—	✔	✔
`mac2 <MAC address>`	Specifies the device that will be operated redundantly along with the second wireless adapter.	—	—	—	—	✔	✔
`name [system name]`	Instead of the MAC addresses, you can also specify the sysName of the device.	—	—	—	—	✔	✔
`wepkey1 [key index]`	Specifies the WEP key of the device that will be operated redundantly along with the first wireless adapter.	—	—	—	—	✔	✔
`wepkey2 [key index]`	Specifies the WEP key of the device that will be operated redundantly along with the second wireless adapter.	—	—	—	—	✔	✔
`wep [E|D]`	Enables / disables encryption.	—	—	—	—	✔	✔
`redun [E|D]`	Enables / disables the redundancy function	—	—	—	—	✔	✔

3.8.7.7 CLI\IFEATURES\IP_ALIVE menu command

Application-related connection monitoring

With the commands in this menu, you set the properties of application-related connection monitoring.

CLI\IFEATURES\IP_ALIVE>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`ipalive <E|D>`	Enables / disables application-related connection monitoring.	—	—	—	—	✓	✓
`add <E|D> <IP address> <:Port> <Timeout>`	Adds a new IP address to the connection monitoring and enables / disables monitoring for this IP address.	—	—	—	—	✓	✓
`edit <Index|IP addr.> [:port] [E|D] [timeout]`	Modifies, enables, or disables the entry specified by the index or IP address.	—	—	—	—	✓	✓
`delete <Index|IP addr.`	Deletes the node to be monitored.	—	—	—	—	✓	✓
`clearall`	Deletes all entries for connection monitoring.	—	—	—	—	✓	✓
`acknow [Index|All]`	Displays or acknowledges (clears) the IP Alive messages requiring acknowledgment.	The fault state remains active until all the fault messages have been acknowledged. The fault state and the Fault LED are cleared if the only reason was an IP Alive error message. The command is not visible in the client mode.					
		—	—	—	—	✓	✓

3.8.7.8 CLI\IFEATURES\AEROSCOUT\WLAN1 (or WLAN2 or WLAN3) menu command

Forwarding of AeroScout frames

With the command in this menu, you enable the forwarding of AeroScout frames

CLI\IFEATURES\AEROSCOUT\WLAN1> (or WLAN2 or WLAN3)>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`aero [E|D]`	Enable / disable forwarding of AeroScout frames.	—	—	—	—	✓	✓

3.8.7.9 CLI\IFEATURES\IHOP menu command

Industrial Hop (iHop)

With the commands in this menu, you set the properties of the iHop procedure.

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`ihop [E | D]`	Enables/disables the iHop function	—	—	—	✓	—	✓

3.8.7.10 CLI\IFEATURES\DUAL_CLIENT menu command

Wireless network connection via two client devices

With the commands of this menu, you configure the dual client mode.

CLI\IFEATURES\DUAL_CLIENT>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`dc [E|D]`	Enables / disables the dual client mode.	—	—	—	✓	—	✓

3.8.8 The CLI\INFORM menu

3.8.8.1 CLI\INFORM menu command

System events and information on the protocols

The pages of this menu provide information on system events and protocols.

CLI\INFORM>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78 x	W78x RR
`spanning`	Displays information on spanning tree.	—	—	—	—	✓	✓
`WLAN1`	Opens the WLAN1 menu	✓	✓	✓	✓	✓	✓
`WLAN2`	Opens the WLAN2 menu	—	—	—	—	✓	✓
`ETHERNET`	Opens the ETHERNET menu	—	✓	✓	✓	✓	✓
`LOG`	Opens the LOG menu	✓	✓	✓	✓	✓	✓
`AUTHLOG`	Opens the AUTHLOG menu	✓	✓	✓	✓	✓	✓
`SIGNAL`	Open the signal recorder menu	✓	✓	✓	✓	✓	✓
						In client mode only	

3.8.8.2 CLI\INFORM\LOG menu command

System events and information on the protocols

The pages of this menu display tables contain information on system events and on the behavior of the protocols (IP, TCP, UDP, and ICMP, SNMP).

CLI\INFORM\LOG>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`events <show │ clear>`	Displays or deletes the log table.	✓	✓	✓	✓	✓	✓
`addevent <Text>`	Adds an event to the log table.	✓	✓	✓	✓	✓	✓
`eventmax [Max count]`	Sets the maximum number of log entries.	The default is 400.					
		✓	✓	✓	✓	✓	✓

3.8.8.3 CLI\INFORM\AUTHLOG menu command

Logging authentication

The pages of this menu contain a table with information on successful or failed authentication attempts.

CLI\INFORM\AUTHLOG>

Command	Description		Comment					
			IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`show [0...8]`	Displays the authentication entries. By specifying a parameter, the display can be limited to specific information:		✓	✓	✓	✓	✓	✓
	0	All						
	1	Good						
	2	All Errors						
	3	802.11 Errors						
	4	ACL Errors						
	5	RADIUS Errors (request denied, password rejected etc.)						
	6	802.1x Errors (timeout, no response from RADIUS or WPA server)						
	7	Deauthenticated Errors						
	8	Deassociated errors						
`clear`	Deletes all entries.		✓	✓	✓	✓	✓	✓

3.8.8.4 CLI\INFORM\WLAN1 (or \WLAN2 or \WLAN3) menu command

Logged-on clients

All the logged-on clients along with certain additional information (wireless channel, status etc.) are displayed here.

CLI\INFORM\WLANx>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`station [MAC]`	Displays information on the connected stations. Enter the MAC address after the "Station" command.	✓	✓	✓	✓	✓	✓
`stasort [mac|sig]`	Displays information on the connected stations. This can be sorted according to ;AC addresses or signal strength. Enter either "mac" or "sig" after the "Stasort" command to display the information sorted.	✓	✓	✓	✓	✓	✓
`apinfo`	Displays information on the access point.	—	—	—	—	✓	✓
`scan`	Displays all the access points in the area. Possible only if iPCF is disabled.	✓	✓	✓	✓	✓	✓
`scanww`	Displays all access points regardless of the country code.	—	✓	✓	✓	✓	✓
`noise`	Shows disturbances on the individual channels.	✓	✓	✓	✓	✓	✓
`overlap`	Shows the access points on the set or adjacent channels.	—	—	—	—	✓	✓
`over_age [1 ... 7200]`	Changes the aging interval (in minutes) for the list of neighboring access points. If an AP is inactive for longer than the time set here, it is removed from the list. Enter a number of minutes after the "over age" command.	—	—	—	—	✓	✓
`vap`	Displays all configured SSIDs (VAPs).	—	—	—	—	✓	✓
`resetStats`	Resets the statistics that are displayed with the Station command.	✓	✓	✓	✓	✓	✓

3.8.8.5 CLI\INFORM\ETHERNET menu command

Information on the Ethernet interface

This menu command provides information on the current settings of the Ethernet interface. The current operating data is also displayed here.

CLI\INFORM\ETHERNET>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`stats`	Shows the statistics of the Ethernet interface.	—	✓	✓	✓	✓	✓
`resetStats`	Resets the statistics to zero.	—	✓	✓	✓	✓	✓

3.8.8.6 CLI\INFORM\IQOS\WLAN1 (or \WLAN2 or \WLAN3) menu command

Information on bandwidth reservation

The pages of this menu provide information on iQoS.

CLI\INFORM\IQOS\WLAN1> (or \WLAN2 or \WLAN3)

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`info`	Displays information on iQos.	—	—	—	—	✓	✓

The CLI also supplies detailed information on iQoS. In this view, the first part displays the current configuration, in other words whether iQoS is enabled, , whether the calculations and reservations are based on the static "worst-case" assumptions (static = enabled) or the current situation (static = disabled). The number of configured critical clients is also displayed.

```
Telnet 192.168.1.9                                                    _ □ ×

CLI\IFEATURES\IQOS\WLAN1>info

iQoS                          : enabled
static                        : disabled
Guarantie Time                : 50 ms
Critical Clients              : 1
Index !    MAC Address        ! Bandwidth (kbit/s) ! Enabled ! Accepted
--------+-------------------+-------------------+---------+----------
    1 ! 08-00-06-2A-BB-06 !                  200 !    X    !    X

Traffic statistics (Timestamp: 100016 ms):

                     ! CC       ! CNC      ! NCS      ! NCR      ! NCNR
---------------------+----------+----------+----------+----------+--------
 Number of clients   ! 1        ! 0        ! 3        ! 0        ! 0
 Framerate           ! 193      ! 0        ! 470      ! 0        ! 0

Associated Clients:

 AID !    MAC Address      ! SI (ms) ! Status ! TX bytes    ! RX bytes
-----+-------------------+---------+--------+-------------+------------
    4 ! 00-0D-88-65-13-B1 !    1.62 ! NCS    ! 241711      ! 43041
    3 ! 00-05-5D-9A-13-FF !    1.62 ! NCS    ! 10049620    ! 10063453
    2 ! 08-00-06-2A-BB-06 !    0.0  ! CC     ! 509256      ! 512666
    1 ! 00-50-8B-5E-0B-DB !    1.62 ! NCS    ! 557405      ! 566839

SI   = shaper interval
CC   = critical compliant
CNC  = critical non-compliant
NCS  = non-critical satisfied
NCR  = non-critical regulatedNCR
NCNR = non-critical non-responsive

CLI\IFEATURES\IQOS\WLAN1>
```

The "Traffic statistics" table shows how many clients are currently in each status and how many packets of a particular class were sent for each of these classes.

The "Associated Clients" table provides an overview of all clients, their current classification, and the volume of sent and received data. The shaper interval (SI) is also is displayed for each client. The shaper interval is the minimum spacing between two packets of a client set by iQoS. For NCS clients, the SI is selected so that their bandwidth is twice the size of the current bandwidth.

3.8.8.7 CLI\INFORM\SIGNAL menu command

Display of the current signal strength and recording of a series of measurements

With the commands in this menu, you set the properties of the signal recorder.

CLI\INFORM\SIGNAL>

Command	Description	Comment					
		IWLAN/ PB Link PN IO	W744	W746	W747	W78x	W78x RR
`recstart <interval> [number of recording points]`	Starts signal recording.	This command is only available in the client mode.					
	The interval at which the current signal is recorded can be between 1 and 1000 milliseconds.	✔	✔	✔	✔	✔	✔
	A value between 1 and 20000 is possible for the number of recording points.						
`recstop`	Stops signal recording prematurely.	This command is only available in the client mode.					
		✔	✔	✔	✔	✔	✔
`dispstart [interval]`	Displays the current signal strength cyclically on the CLI.	This command is only available in the client mode.					
	The interval can be between 100 and 10000 milliseconds	✔	✔	✔	✔	✔	✔
`dispstop`	Stars cyclic output of the signal strength.	This command is only available in the client mode.					
		✔	✔	✔	✔	✔	✔
`signame [filename]`	Entry of a file name for the signal recording.	This command is only available in the client mode.					
		✔	✔	✔	✔	✔	✔
`save`	Saves the signal recording via TFTP.	This command is only available in the client mode.					
		✔	✔	✔	✔	✔	✔

3.9 Configuring with the PRESET plug

3.9.1 How the PRESET-PLUG works

Multiple use of configuration data

With the PRESET PLUG, it is simple to assign a configuration to SCALANCE W-700 devices and the IWLAN/PB Link PN IO. You transfer an existing configuration to any number of other devices using the PRESET PLUG. This procedure is particularly useful when commissioning a lot of IWLAN clients with the same parameter settings because you do not need to set parameters for each client manually.

Note

To avoid duplicating IP addresses, the IP parameters are not changed but are retained when you use the PRESET PLUG.

If the PRESET PLUG is inserted, the WLAN interface of the device is deactivated. WLAN operation with a PRESET PLUG insert it is not possible.

Note
Only for SCALANCE W788-xPRO/RR

With a SCALANCE W788 access point version V3.0, it is not possible to create a PRESET-PLUG for the IWLAN/PB Link PN IO version V1.1. Please use a version V2.4 SCALANCE W788 or older. If you update the IWLAN/PB Link PN IO to firmware V1.2, the configuration is available again on a PRESET PLUG (created with V3.1).

3.9.2 Creating a Configuration with a new PRESET PLUG

Procedure

Follow the steps below to save a configuration on a PRESET PLUG:

1. Insert the PRESET PLUG in the C-PLUG slot of a powered-down device with the required configuration and then turn on the device.

2. Start Web Based Management and select the **System > C-PLUG** menu.

3. In the "Modify C-PLUG" drop-down list box, select the "Create PRESET-PLUG" entry.

4. In the "PRESET PLUG for" box, specify the device for which you want to create the PRESET PLUG. The PRESET-PLUG created in this way functions only with the device type you selected. The figure above shows an example of the possible selections for a SCALANCE W747-1RR.

Note

If you want to create a PRESET-PLUG with a device that has greater functionality than the destination device to be configured, remember the following:

If you create a PRESET-PLUG with a SCALANCE W78x-xPRO/RR or a W746-1xx or W747-1xx for the SCALANCE W744-1xx as destination device, you can, for example, set parameter values for iPCF or "Layer 2 Tunnel". These values are, however, ignored by the destination device because these functions are not supported by a SCALANCE W744-1xx.

To avoid duplicating MAC addresses, the "Adopt MAC" parameter is not set to "Adopt MAC manually" when using the PRESET-PLUG.

---

5. Click on the "Modify" button to transfer the configuration of the device to the PRESET PLUG.

6. Turn the device off and remove the PRESET PLUG.

3.9.3 Changing a PRESET PLUG that already contains configuration data

Procedure

Follow the steps below to change the configuration data on a PRESET PLUG:

1. Insert the PRESET PLUG in the C-PLUG slot of a powered-down SCALANCE W-700 and then turn on the device. The P1 and R1 LEDs flash yellow to signal that the PRESET PLUG was detected.

2. Start Web Based Management; there you will see the current settings of the PRESET PLUG.

3. Make the required changes to the configuration.

4. In the "Modify C-PLUG" drop-down list box, select the "Create PRESET-PLUG" entry.

5. In the "PRESET PLUG for" box, specify the device for which you want to create the PRESET PLUG.

6. Click the "Modify" button to transfer the configuration of the device to the PRESET PLUG.

7. Turn the device off and remove the PRESET PLUG.

3.9.4 Putting a device into operation with a PRESET PLUG

Procedure

Note

To work correctly, the PRESET PLUG must have a content that matches the target device.

Follow the steps below to put a device into operation with the configuration data on a PRESET PLUG.

1. Insert the PRESET PLUG in the C-PLUG slot of the device to which you want to assign a configuration.

2. Turn on the power to the device. The LEDs "P1" and "R1" (and "Rx" on a SCALANCE W-700 with more than one wireless interface) flash yellow to signal that the PRESET PLUG was detected.

3. Press the reset button beside the C-PLUG briefly to save the settings of the PRESET PLUG on the device.

4. When all the data has been transferred from the PRESET PLUG to the device, the LEDs stop flashing and are permanently lit.

5. Turn the device off and remove the PRESET PLUG.

Note

The next time the device starts up, it uses the settings from the PRESET PLUG and the previous IP configuration.

3.10 PROFINET IO functionality

3.10.1 Configuring with PROFINET IO

Using PROFINET IO

One option for diagnostics, parameter assignment, and generation of alarm messages of the connected SCALANCE W-700 devices is to use PROFINET IO. Here, you can see how you can use the options of PROFINET IO for a connected SCALANCE W-700.

Note

The SCALANCE W744-1PRO and W744-1 devices cannot be used as PNIO devices.

In the example, it is assumed that a PNIO-Controller V2 is already configured with a PROFINET IO chain (see also PROFINET IO System Manual).

Note

STEP 7 V5.4 SP4 is required.

Based on the example of a SCALANCE W-700, the following section shows a hardware configuration with a PROFINET IO line.
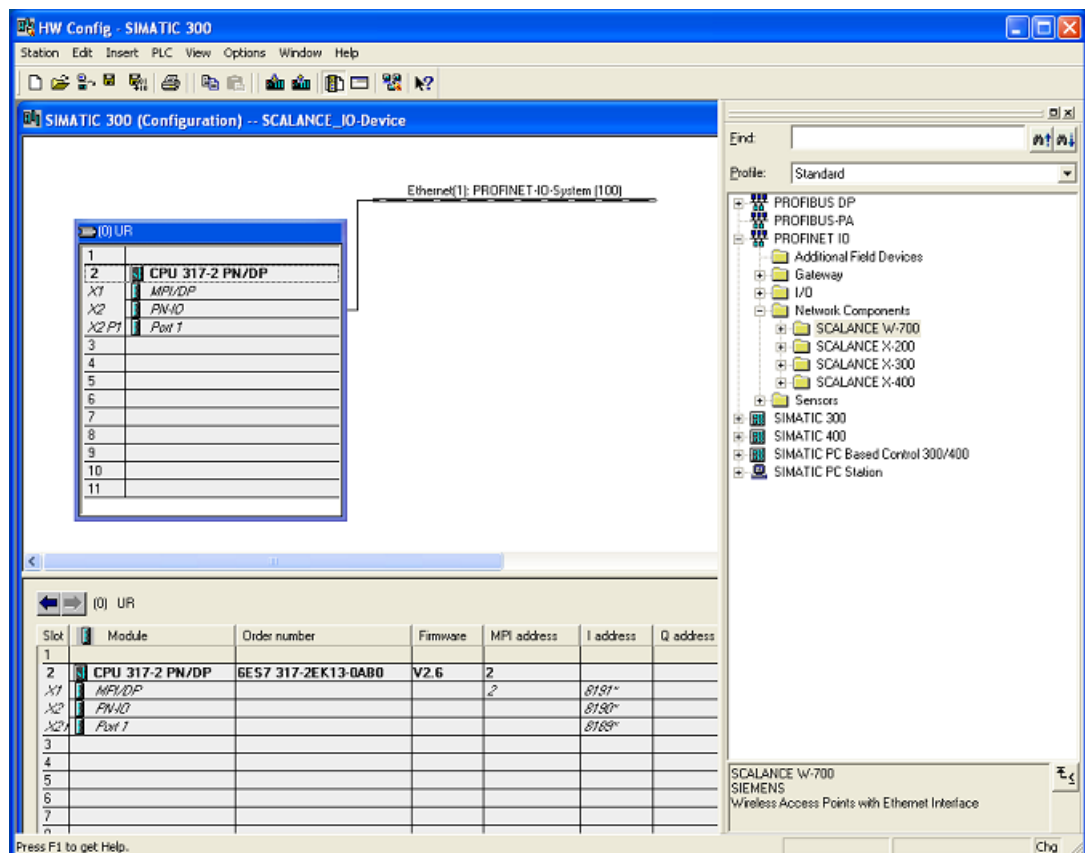
Figure 3-2   Setup of the station in HW Config

Including a SCALANCE W-700

To include a SCALANCE W-700 as a PN IO device, this must exist in the module catalog under PROFINET IO.

Procedure

If the devices are not yet included in STEP 7, follow the steps below:

1. In the dialog, select HW Config -> Options "Install GSD files".
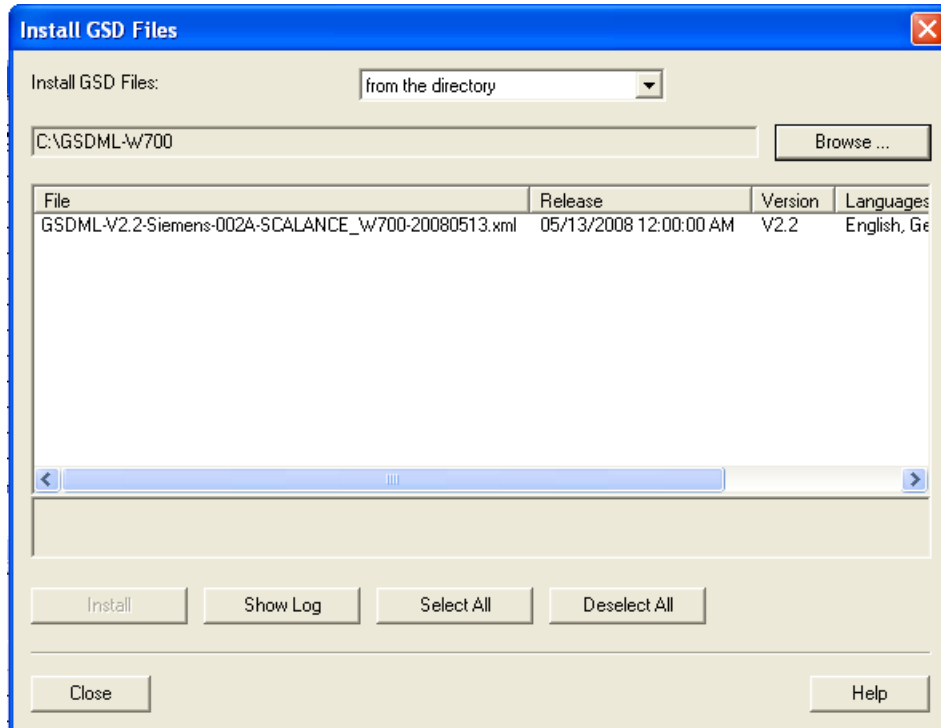   The following screen appears:

Figure 3-3   Installing GSD files

2. Using the "Browse" function go to the supplied xml file (for example GSDML-V2.2-Siemens-002A-SCALANCE_W700-YYYYMMDD.xml - Y, M and D stand for the issue date of the file).

3. Then adopt the file with "Install". The SCALANCE W-700 is now included in the module catalog

4. Take the SCALANCE W-700 you require from the HW catalog - here, for example, SCALANCE W786-1PRO (PROFINET IO **>** Network Components **>** SCALANCE W-700 **>** SCALANCE W786-1PRO). Drag the selected SCALANCE to the PROFINET IO system.
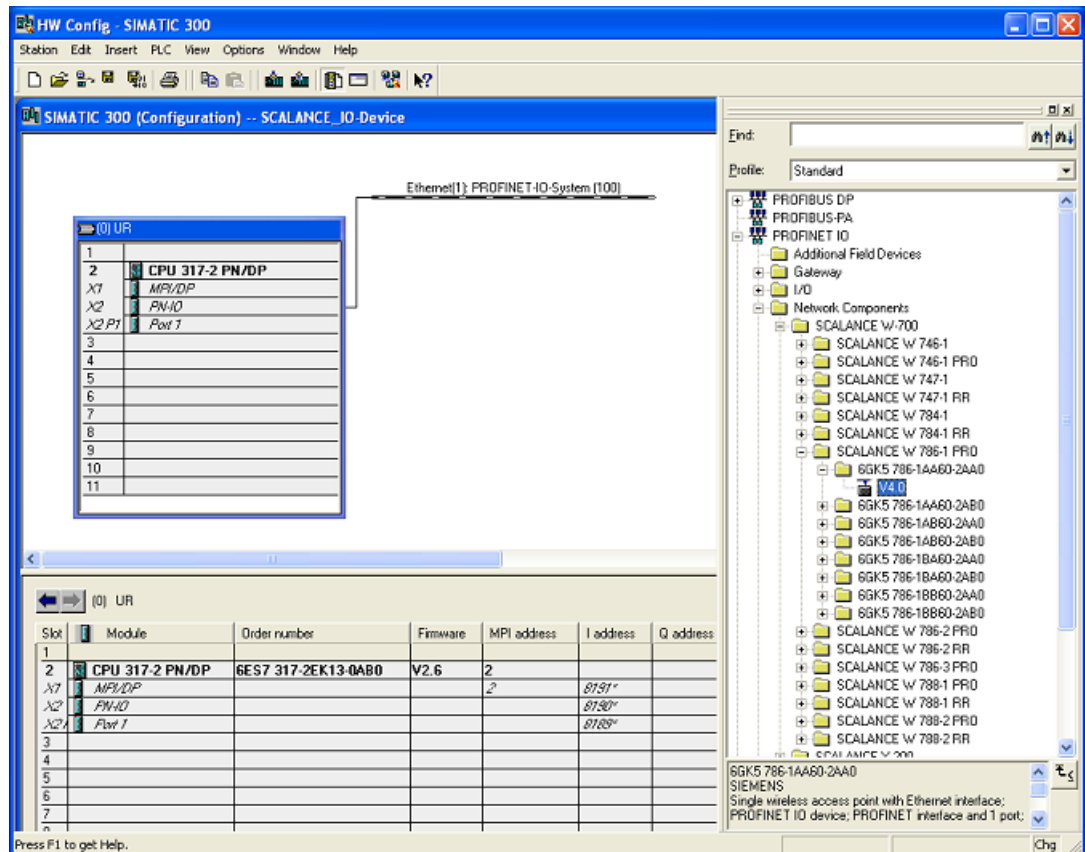
Figure 3-4   Inserting a SCALANCE W-700

5. Click on the "(1)SCALANCE" icon so that the slots of the SCALANCE W786 are displayed in the lower part of the screen. By double-clicking on slot=0, you can set the global parameters of the device (substitute module) as shown in the figure below.
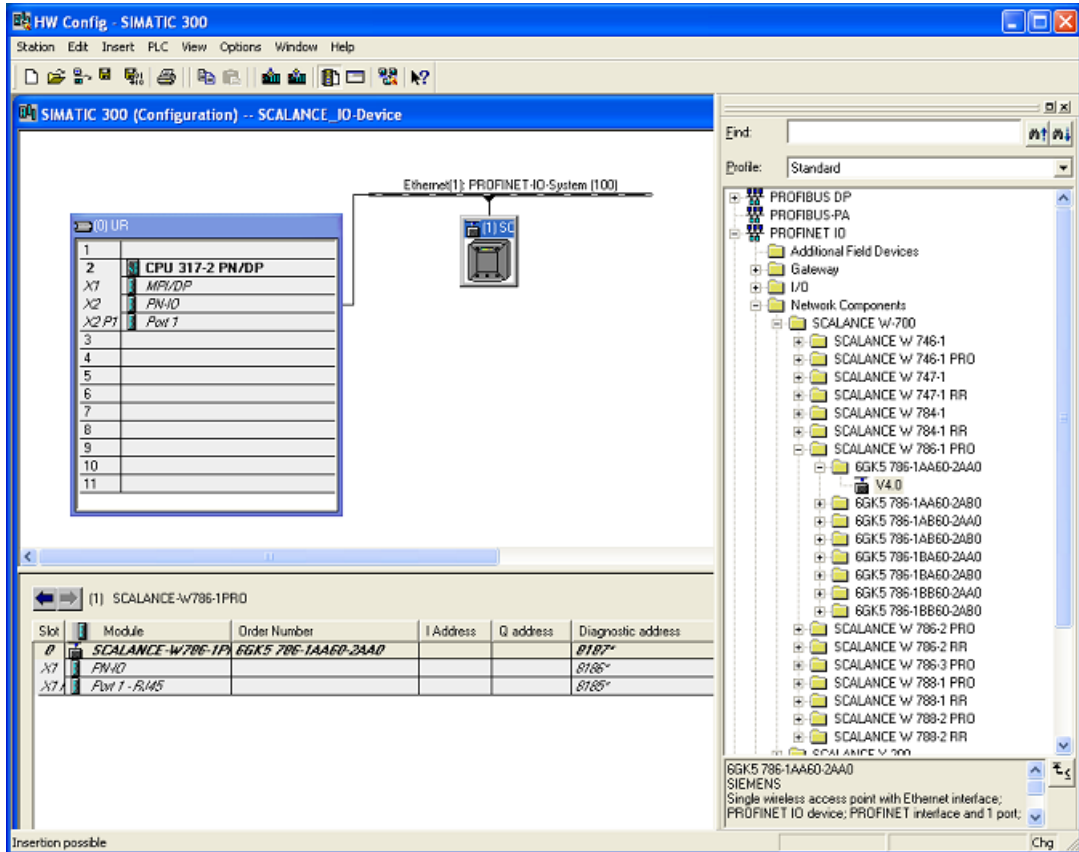
Figure 3-5   HW Config: Setting the global parameters

6. You can set the parameters assigned to the relevant module on slot 0.

7. Click on the slots of the ports to set the port-specific parameters.

8. Open the "Object Properties dialog in HW Config (right-click on the Icon -> Object Properties) and enter the name of the PROFINET IO device. Click OK to exit the dialog.
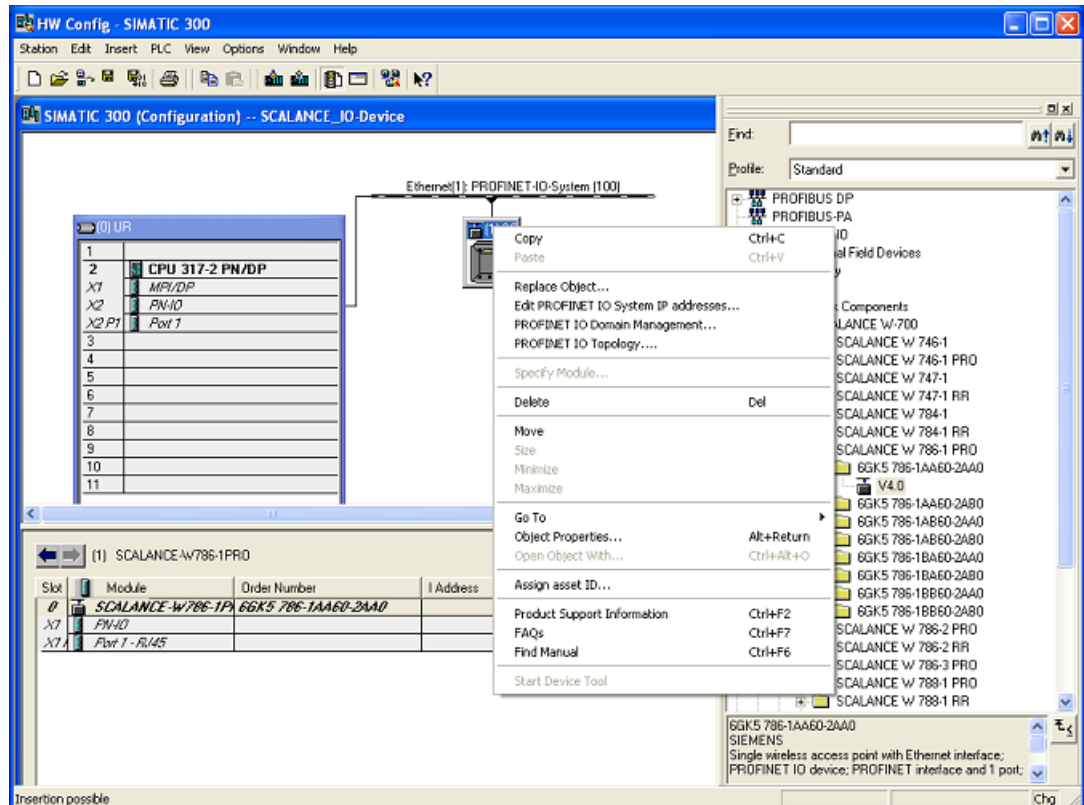
Figure 3-6   HW Config: Context menu of the device

9. Select the Station > Save and Compile menu command.

10. Interconnect the devices over the network and turn on the power supplies of the networked devices.

11. To transfer the name to the SCALANCE W786-1PRO, you require an online connection from the PG to the PROFINET IO device. Select "PLC > Ethernet > Assign device name" to open the relevant dialog.
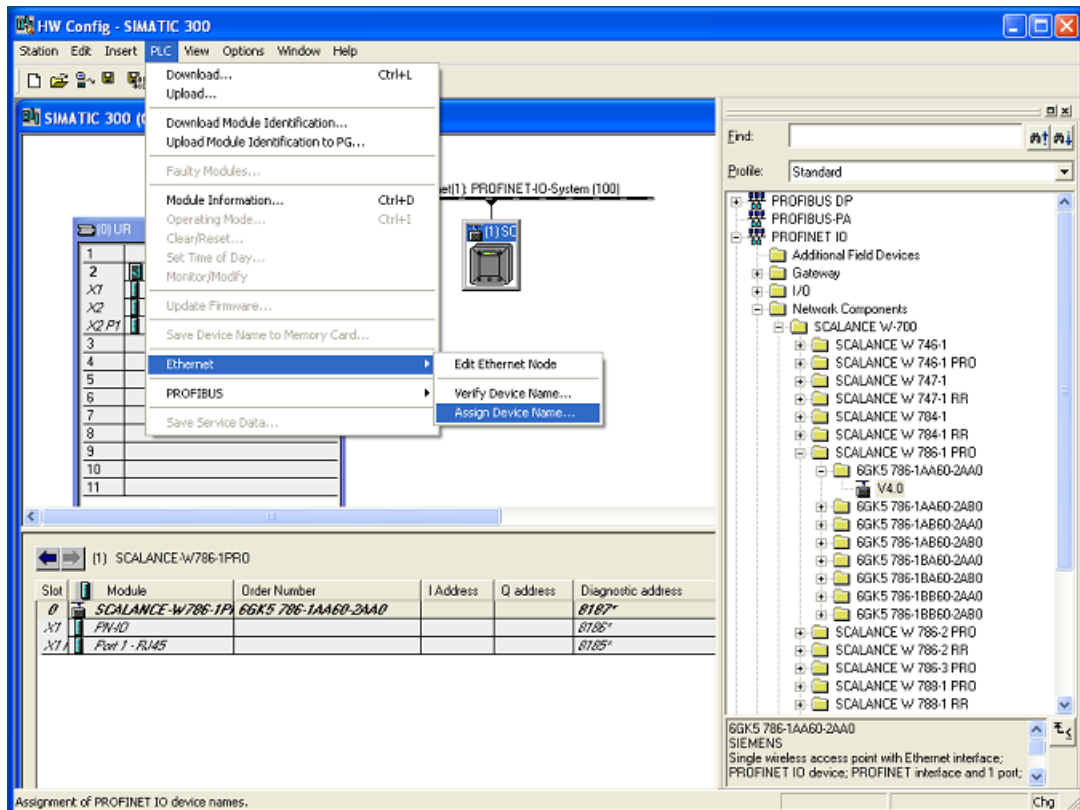
Figure 3-7   Assigning a device name in HW Config

12. If you are using multiple PROFINET IO devices, multiple PROFINET IO devices are also indicated in the "Assign device name" dialog. In this case, you should compare the MAC address of the device with the indicated MAC address and select the correct IO device. With the "Flashing On / Off" button, you can check the device assignment visually (the LED of the Ethernet port flashes on the selected SCALANCE W786), Click the "Assign name" button in the "Assign device name" dialog. The device name is stored permanently on the SCALANCE W786. After assigning the name, the device name you assigned appears in the dialog box.

13. Download the hardware configuration to the controller (in this example, the CPU317-2PN/DP). Select PLC > Download to Module

---

Note

With general errors in PROFINET IO mode, such as the failure of communication between PROFINET IO controller and device, the error LED ("F") is lit on the device and the following entries are made in the log table:

- Fault state changed to: Failure (PROFINET IO alarm! Use STEP 7 for diagnostics)

The diagnostic buffers of the configured module provide detailed information on the error status and are accessible using STEP 7.

3.10.2   Settings in HW Config

Power supply monitoring and C-PLUG monitoring on the SCALANCE W-700

Here, you decide how the SCALANCE W-700 reacts to a problem in the power supply or to a C-PLUG fault.

Redundant power supply

- Not monitored
  The failure of one of the two power supplies does not cause an alarm.

- Monitored
  The failure of one of the two power supplies causes an alarm.

C-PLUG monitoring

- Not monitored
  The C-PLUG is not monitored.

- Monitored
  A C-PLUG fault causes an alarm.
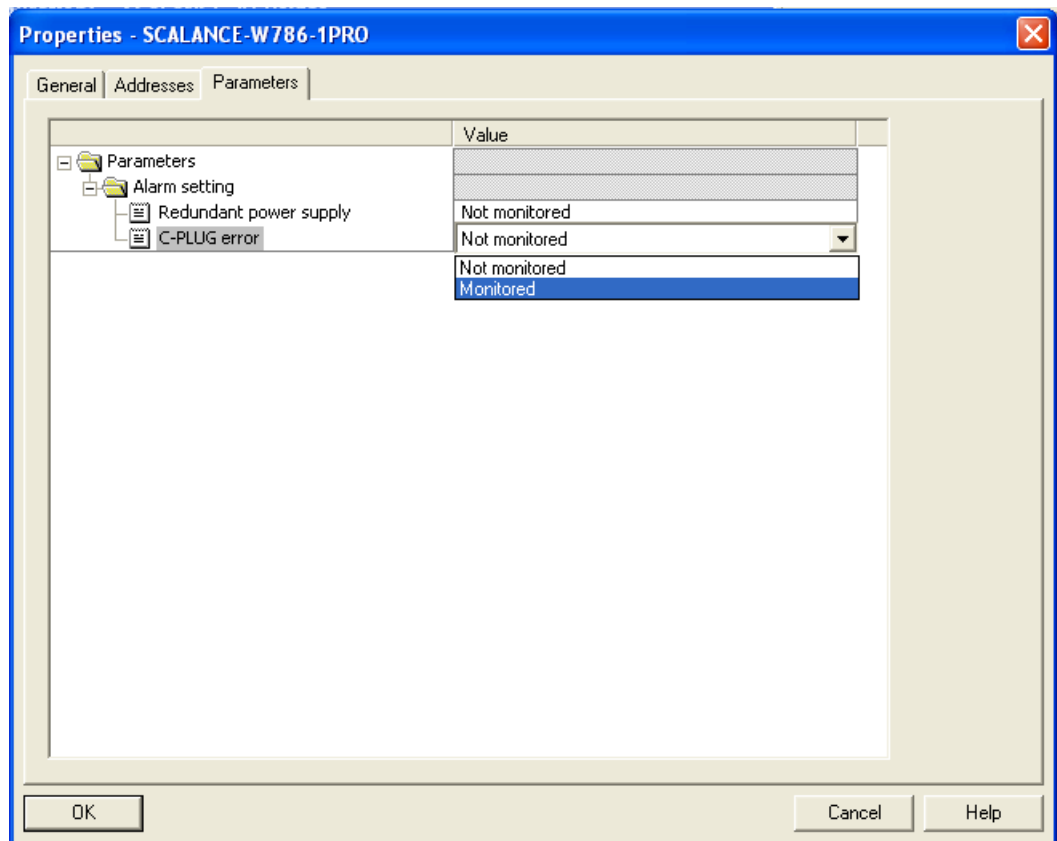
Figure 3-8   Settings for monitoring the power supply and the C-PLUG in the "Properties" dialog

Port-specific settings

Here, you make the settings for the Ethernet port of the SCALANCE W-700. In the dialog below, this is done based on the example of a SCALANCE W786-1PRO.
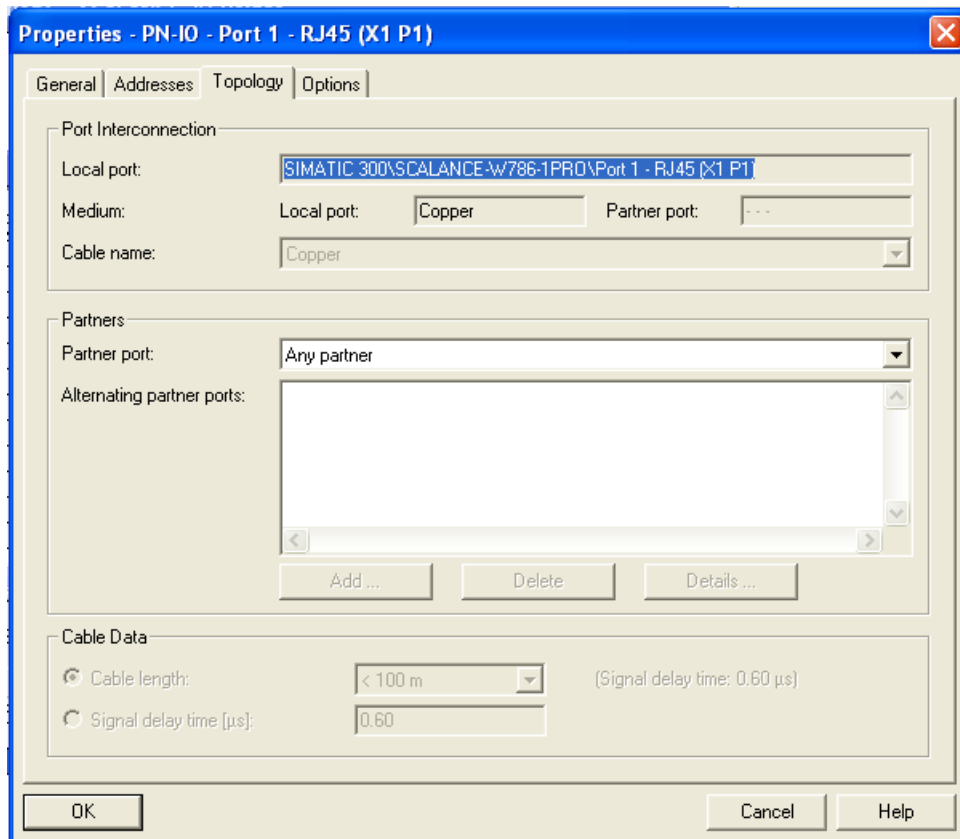

Figure 3-9   Settings for the Ethernet interface

Transmission mode

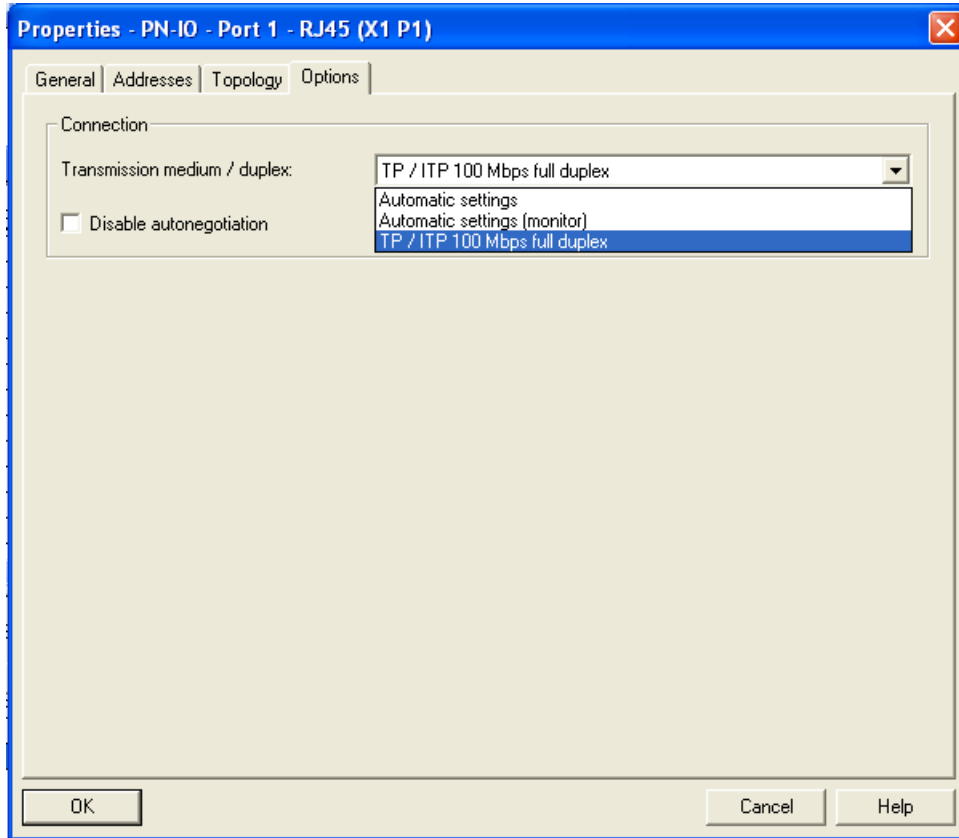In the "Options" section, you can make settings for the transmission mode.

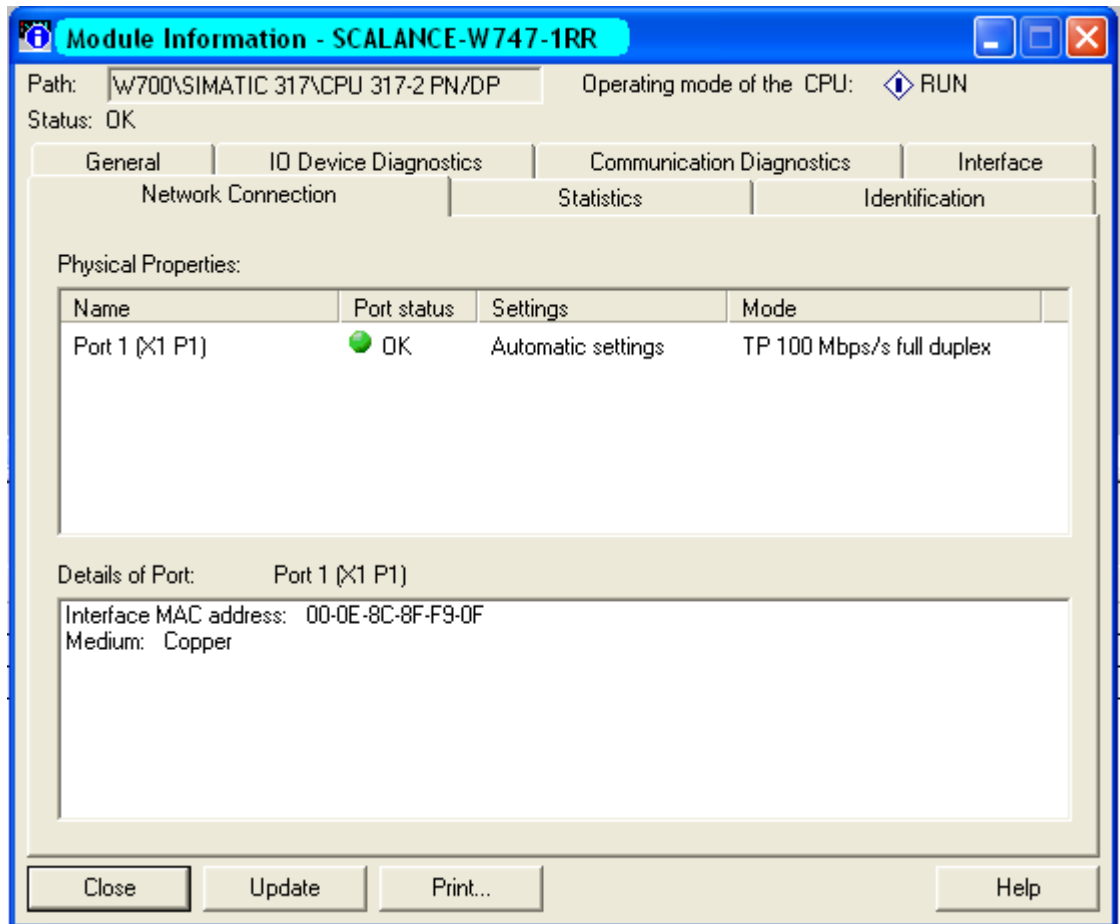Figure 3-10   Options relating to the transmission mode in the "Properties" dialog

Figure 3-11   "Network attachment" property of a SCALANCE W-700

3.10.3 Access options over PROFINET IO

Slot Functions

SCALANCE W-700s have a subslot per port in slot 0. Functions that cannot be assigned uniquely to one port are assigned to the device access point (slot 0).

Slot 0	Subslot 1	• Alarms • Data records (4.5)	Device Access Point (DAP) • Interface connection • C-PLUG • Redundant power supply
	Subslot 8001	• Alarms (IEC) • Data records (IEC)	Ethernet port 1 • Alarm response • Port state

Generating alarms

The user configures exactly the assignment and required properties of the ports. This makes it necessary to match the configuration and installation. If the setting in STEP 7 requires that port 1 is not linked, this must be taken into account during installation. The power fault mask set by STEP 7 is stored retentively and the port fault mask is reset. If you exit DataEX, the settings in the fault mask made by STEP 7 are retained and continue to apply without PROFINET operation.

● Effect of other signaling mechanisms during DataEX
The fault mask is displayed as set by STEP 7 both in the Web interface and in CLI. Changes are not possible.

Data record 4:

Access: Read-write,

Structure:

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh:

Byte BlockVersionLow:

DWord Alarm_enable; };

BlockType:

1: Constant

BlockLength:

6: Constant in device data, designates the length without Type+ Length

BlockVersionHigh:

1: Constant in device data, designates the major version

BlockVersionLow:

1: Constant in device data, designates the minor version

Enable_alarms:

This bit list specifies what is to be monitored. If a bit is set, this alarm source is enabled.

Reserved Bit 2 - 31	C-PLUG Bit 1	Red_power Bit 0
0	0: No C-PLUG monitoring	0: No monitoring of the redundant power supply
	1: Missing or incorrect C-PLUG generates alarm	1: Monitoring of the redundant power supply

Data record 5:

Supplies the current alarm setting for this port

Access: Read-only

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh;

Byte BlockVersionLow;

DWord status; };

BlockType:

1: Constant

BlockLength:

6: Constant in device data, designates the length without Type+ Length

BlockVersionHigh:

1: Constant in device data, designates the major version

BlockVersionLow:

1: Constant in device data, designates the minor version

Status:

Reserved Bits 8-31	C-PLUG_status Bits 4-7	Reserved Bits 2-3	Fault_line_status Bit 1	Power line redundancy Bit 0
0	Information regarding the configuration plug of the network component 0: C-PLUG inserted and ok 1:C-PLUG not inserted 2: C-PLUG inserted but not ok (incorrect type) 3: C-PLUG inserted but not ok (checksum error)		Information regarding the current state of the signaling contact 0: Fault line passive 1: Fault line active	This bit provides information about the redundant power supply 0: not redundant 1: redundant

Note
C-PLUG

For detailed information on the topic of C-PLUGs, refer to the sections "Description" and "Configuration with Web Based Management".

In the following situations, PNIO does not start up:

*   A C-PLUG for the wrong type is inserted
*   When a CRC error occurs
*   The configuration of the device requires a C-PLUG, but this is not inserted.

Upkeep and maintenance

4

4.1 Loading new firmware over FTP

Procedure

You can load new firmware on a SCALANCE W-700 over FTP even if the device is not reachable over WEB Based Management or the CLI. This may be the situation if there was a power down during a firmware update. Follow the steps below to load new firmware using FTP:

1. Turn off the power to the device.

2. Now press the Reset button and reconnect the power to the device while holding down the button.

3. Hold down the button until the red fault LED (F) starts to flash after approximately 2 seconds.

4. Now release the button. The bootloader waits in this state for a new firmware file that you can download by FTP.

5. Connect a PC to the SCALANCE W-700 over the Ethernet interface.

6. Assign an IP address to the SCALANCE W-700 with the Primary Setup Tool.

7. Open a DOS box and change to the directory where the file with the new firmware is located and then execute the command "ftp <ip address>".
   As an alternative, you can use a different FTP client.

8. Enter "siemens" as both the login and password.

9. Load the new firmware with the command "put <firmware>".

10.Once the firmware has been transferred completely to the device, the device is restarted automatically.

4.2 Restoring the default parameter settings

Procedure

Follow the steps below to reset the device parameters to the factory settings:

Note

When you reset the device parameters, all previously changed settings are lost!

---

1. Turn off the power to the device.

2. Now press the Reset button and reconnect the power to the device while holding down the button.

3. Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit.

4. Now release the button and wait until the fault LED (F) goes off again.

5. The device then starts automatically with the default parameters.

Troubleshooting/FAQ

<div align="right">

5

</div>

5.1   Disrupted data transmission due to the received power being too high

Causes and effects of excessive received power

If the received power at the input of a WLAN is too high, this overdrives the amplifier circuit. Overdrive can occur on clients and access points. If the received power on the IWLAN device is higher than -40 dBm, this can lead to disruptions in communication. The current received power [in dBm] is displayed in WBM in the Information > Available WLAN (on clients) or Information > Clients List (on access points) menu. The power of the input signal on the IWLAN device is influenced by the following factors:

● Distance between the WLAN partners

● Reflections of the electromagnetic waves by parts of the building

● "Transmit power" setting in Web Based Management of the access point or client.

Remedy

If communication is disrupted by an excessive received power (greater than -40 dBm), you can eliminate the problem in the following ways:

● Increase the distance between the transmitter and receiver.

● Reduce the transmit power of the IWLAN partner with suitable settings in Web Based Management or in the Command Line Interface.

5.2 Changing from MLFB 6GK57xx-xSx00-2Ax6 to MLFB 6GK57xx-xAA60-xAx0

New hardware

The hardware redesign of the Scalance W components with MLFB 6GK57xx-xSx00-2Ax6 with the introduction of new MLFBs was necessary to equip the devices with a power supply conforming with Power over Ethernet (PoE) to IEEE 802.3af. Following the redesign, the devices also have a new IWLAN wireless module.

The following table shows the order numbers of the devices before and after the hardware redesign:

Previous MLFB …	… is replaced by MLFB (redesigned hardware)
6GK5744-1ST00-2AA6	6GK5744-1AA60-2AA0
6GK5744-1ST00-2AB6	6GK5744-1AA60-2AB0
6GK5746-1ST00-2AA6	6GK5746-1AA60-4AA0
6GK5746-1ST00-2AB6	6GK5746-1AA60-4AB0
6GK5746-1ST00-2BA6	6GK5746-1AA60-4BA0
6GK5747-1SR00-2AA6	6GK5747-1AA60-6AA0
6GK5747-1SR00-2AB6	6GK5747-1AA60-6AB0
6GK5788-1ST00-2AA6	6GK5788-1AA60-2AA0
6GK5788-1ST00-2AB6	6GK5788-1AA60-2AB0
6GK5788-1SR00-2AA6	6GK5788-1AA60-6AA0
6GK5788-1SR00-2AB6	6GK5788-1AA60-6AB0
6GK5788-2ST00-2AA6	6GK5788-2AA60-2AA0
6GK5788-2ST00-2AB6	6GK5788-2AA60-2AB0
6GK5788-2SR00-2AA6	6GK5788-2AA60-6AA0
6GK5788-2SR00-2AB6	6GK5788-2AA60-6AB0

Continued use of existing configuration

When changing from products (access points and Ethernet clients) from device before the hardware redesign (MLFB 6GK5788-xSx00-2xx6 or MLFB 6GK574x-1Sx00-2xx6) to device with the new hardware (MLFB 6GK5788-xAA60-xAx0 or MLFB 6GK574x-1AA60-xAx0), the old configurations on C-PLUG, Preset Plug and in the config.cfg configuration file can, in principle, continue to be used. However, note the points listed below.

● The devices use IWLAN cards with different wireless properties. When adopting a configuration created a device before the hardware redesign (MLFB 6GK5788-xSx00-2xx6 or MLFB 6GK574x-1Sx00-2xx6), the displayed parameter for the transmit power is adapted without resulting in changes in the transmit power.
For example, a device with MLFB 6GK5746-1AA60-4AA0 (new hardware) has a maximum transmit power of 17 dBm at the setting "Half, 1/2 (-3dBm)" when using antennas from the available range. A device with MLFB 6GK5746-1ST00-2AA6 (before the hardware redesign) with the "Transmit Power" parameter set to "Full (-0 dB)" also has a maximum transmit power of 17 dBm. The parameters for other transmit power settings are also adapted analogously.

● "Antennas" selection menu in the Web interface:
If a configuration that was created with a device before the hardware redesign (MLFB 6GK5788-xSx00-2xx6 or MLFB 6GK574x-1Sx00-2xx6) is adopted, the antenna type is automatically adapted to the value "User Defined". The value set previously for the antenna gain parameter is adopted.
For example, the value "ANT795-6MR, 5m cable" is automatically converted to "User defined" with the appropriate antenna gain. This conversion is handled by the new device automatically when it is restarted after adopting the old configuration.

Wherever possible, the parameters are adapted/transferred automatically. There are, however, some configurations that can cause problems and cannot be be handled automatically by the firmware:

● Selecting channels in frequency bands with different limit values for transmit power:
If a configuration that was created with a device before the hardware redesign (MLFB 6GK5788-xSx00-2xx6 or MLFB 6GK574x-1Sx00-2xx6) is adopted, it is possible that the list of selectable channels is restricted due to the different wireless properties.
This may mean that devices can no longer be reached via the wireless interface! When replacing devices having MLFB 6GK57xx-xSx00-2Ax6 with MLFB 6GK57xx-xAA60-xAx0, we therefore strongly recommend that these are checked in a test environment to make sure that they adopt the channel selection unchanged. The channel selection is, for example dependent on the set transmit power and can be influenced by modifications to the relevant parameters.
Once a device with new hardware (MLFB 6GK57xx-xAA60-xAx0) has been assigned parameters with a configuration file from a device before the redesigned hardware (MLFB 6GK5788-xSx00-2xx6 or MLFB 6GK574x-1Sx00-2xx6), all the parameters relating to national approvals are checked (as usual). You will find information on the transmit power of the devices in the supplied documentation.

Miscellaneous

- During a transitional period, it is possible that some national approvals are not yet available for the devices with new hardware (MLFB 6GK57xx-xAA60-xAx0). This is because the certification process can take longer in some countries. You should therefore make sure that the devices are approved for your application by checking the following Internet page: http://www.siemens.com/simatic-net/ik-info

- Operation of the devices with new hardware (MLFB 6GK5788-2AA60-6Ax0) as thin access points with HiPath WLAN controller (as familiar with 6GK5788-2SR00-2Ax6, W788-2RR) is still being clarified and is not currently supported. For this application with a HiPath Wireless Controller, users could try out the devices of the type SCALANCE W786-2HPW.

Admin password for the USA variant

The default password of the devices before the hardware redesign is "admin" for the USA variant if you have selected "admin" as the user name.

Note

The following points relate only to device before the redesigned hardware.

Power over Ethernet

The power supply of the device before the redesigned hardware (MLFB 6GK5788-xSx00-2xx6 or MLFB 6GK574x-1Sx00-2xx6) is not electrically isolated from the housing.

Hybrid connector

When replacing a device before the redesigned hardware (MLFB 6GK5788-xSx00-2xx6 or MLFB 6GK574x-1Sx00-2xx6) with a device the new hardware (MLFB 6GK5788-xAA60-xAx0 or MLFB 6GK574x-1AA60-xAx0), a previously used hybrid connector can continue to be used unchanged.

Assignment of the power wires with a hybrid cable 2 x 2 + 4 x 0.34

Wire color code (standard)	Brown	Brown	Black	Black
Function	24 V	24 V	Ground	Ground
Power supply module	1	2	3	4

Assignment of the power wires with an IE FC TP standard cable 4 x 2 GP

Wire color code (standard)	White / blue (1)	Blue	White / brown (1)	Brown
Function	24 V	24 V	Ground	Ground
Power supply module	1	2	3	4

(1) White wire of the pair

Grounding

⚠ CAUTION
Damage to the device due to potential differences
There must be no potential difference between the following parts otherwise there is a risk that the device will be destroyed: • Ground potential of the power supply and ground potential of the antenna ground. • Ground potential of the power supply and a grounded housing. • Ground potential of the power supply and the ground potential of the device connected to Industrial Ethernet (for example PC, AS-300, AS-400 etc.). Connect both grounds to the same foundation earth or use an equipotential bonding cable.

5.3 Notes on secure network design

Keynote

Note the following information about protecting your network from attacks:

- **Use a secure connection with HTTPS**

  In contrast to HTTP, HTTPS allows you secure access for configuring the WLAN clients and the access points using Web Based Management. For more detailed information, refer to the section "Web Based Management".

- **Use WPA2/ WPA2-PSK with AES**

  Use only WPA2/AES to prevent password misuse. WPA2/ WPA2-PSK with AES provides the highest security.

- **Protect your network from man-in-the-middle attacks**

  To protect your network from man-in-the-middle attacks, a network topology is recommended, that makes it more difficult for an attacker to tap into the communications path between two end devices.

  – You can, for example, protect WLAN devices by arranging so that the agent IP is accessible only via a separate management VLAN.

  – A further option is to install a separate HTTPS certificate on the WLAN client / access point. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange. You can install the HTTPS certificate via HTTP.

- SNMPv3 provides you with highest possible security when accessing the WLAN devices via SNMP. For more detailed information, refer to the section "System > SNMP".

Appendix A

<div style="text-align: right; font-size: 2em;">A</div>

A.1 Private MIB variables of the SCALANCE W-700

Downloading the MIB of the SCALANCE W-700 using the Internet Explorer

Using the URL

`http://<IP_address>/snScalanceW.mib`

, you display the login window if you are not yet logged on. After you have logged on successfully, you can access the private MIB of the SCALANCE W-700. To save this on your PC, the source text view should be enabled. As of version V4.0, the MIB of the SCALANCE W-700 can be downloaded in the WBM in "System/Load&Save/HTTP" using the Private MIB file: "save" button.

OID

The private MIB variables of the SCALANCE W78x have the following object identifiers:

```
iso(1).org(3).dod(6).internet(1).private(4).
  enterprises(1).ad(4196).adProductMibs(1).simaticNet(1).
  iScalanceW(4)
```

Variables for access points and clients

The following table shows the private MIB variables available for access points and clients:

Name	OID	Description	Number of objects
snDownload	1.3.6.1.4.1.4196.1.1.4.100.1.5	Download information and control variables for image, configuration file, events table.	17
snNvLog	1.3.6.1.4.1.4196.1.1.4.100.1.6	Log for events.	8
snTrapInfo	1.3.6.1.4.1.4196.1.1.4.100.1.7	Information on traps.	6
snGen	1.3.6.1.4.1.4196.1.1.4.100.1.8	General information, not conforming with MIB-2.	23
snTcpip	1.3.6.1.4.1.4196.1.1.4.100.1.10	IP address, Subnet Mask, Default Gateway, DHCP Status…	5
snScalanceWCommon	1.3.6.1.4.1.4196.1.1.4.100.2.1	SCALANCE W-700 - specific settings.	24
snScalanceWFilter	1.3.6.1.4.1.4196.1.1.4.100.2.4	Protocol filters and storm threshold settings	18
snScalanceWStats	1.3.6.1.4.1.4196.1.1.4.100.2.5	Information on WLAN 1 and WLAN 2 interfaces.	62
snScalanceWDevices	1.3.6.1.4.1.4196.1.1.4.100.2.6	AP mode: List and information on all clients currently "associated" or connected. Client mode: List of devices with which the client is currently connected.	49

Name	OID	Description	Number of objects
snScalanceWScan	1.3.6.1.4.1.4196.1.1.4.100.2.7	Client mode: List of reachable WLANs and information whether the clients can connect to them.	11
snScalanceWAccess	1.3.6.1.4.1.4196.1.1.4.100.2.9	List of IP addresses that can access the management interface.	5

Variables available only for access points

Name	OID	Description	Number of objects
snScalanceWAcl	1.3.6.1.4.1.4196.1.1.4.100.2.8	Information and settings for the Access Control Lists.	9
snScalanceWVirtualAp	1.3.6.1.4.1.4196.1.1.4.100.2.10	Information on the currently configured virtual APs.	17

Traps for access points and clients

Name	Specific index	Variables	Description
snScalanceWPowerLineDown	32	snScalanceWChangedPowerLine - The power line where the last power down occurred. 1-M12, 2-Ethernet Power	This is generated if there is a power down on M12 or the Ethernet power connector.
snScalanceWPowerLineUp	32	snScalanceWChangedPowerLine - The power line where the last power up occurred. 1-M12, 2-Ethernet Power	This is generated if there is a power up on M12 or the Ethernet power connector.
snScalanceWFault	41	snScalanceWFaultValue - Fault value: 0 = no fault, bit 0 = power M12 is off, bit 1 = link down, bit 2 = internal error, bit 23 = Link Check error, bit 24 = IP Alive broken, bit 25 = power ethernet is off, bit 26 = Cold/warm start, bit 27 = C-PLUG error, bit 28 = iQoS error, bit 29 = Redundancy error, bit 30 = PNIO error	This is generated if the snScalanceWFaultValue variable is changed. The bit is set to "1" according to the event that has occurred.
snScalanceWIQOS	51	snScalanceWIQOSValue - Description of the last snScalanceWIQOS trap	

Name	Specific index	Variables	Description
snScalanceWLinkCheckOff	81	snScalanceWLinkCheckValue - Description of the last snScalanceWLinkCheckOff Trap	This is generated if a timeout occurs with a client monitored with Link Check.
snScalanceWLinkIntegrityOn	82	snScalanceWLinkCheckValue - Description of the last snScalanceWLinkCheckOn trap	This is generated if a client monitored with Link Check logs on again at the AP following a timeout.
snScalanceWClientAuthenticated	85	SnScalanceWClientsIndex - An index of the client in the snScalanceWClients table	This is generated when a client logs on at the AP.
snScalanceWClientDeAuthenticated	86	SnScalanceWClientsIndex - An index of the client in the snScalanceWClients table	This is generated when a client logs off from the AP.
snScalanceWRedundancy	53	SnScalanceWRedundancyValue- Description of the last redundancy trap. SnScalanceWRedundancyState- Status of redundancy connection	This is generated if the status of the redundant connection changes, for example when the connection of wireless interface A aborts.

Traps available only for access points

Name	Specific index	Variables	Description
snScalanceWOverlapAP	101	snScalanceWOverlapAPValue - Description of the last OverlapAP trap.	Is generated when an access point is detected on the device's own or an overlapping wireless channel.
snScalanceWiPCFPNIOmaxSTAs	111	snScalanceWPNIOValue - Description of the last snScalanceWiPCFPNIOmaxSTAs or snScalanceWiPCFPNIOCycleTime trap	Is generated when there are too many clients registered for the specified update time in iPCF mode with PNIO support.
snScalanceWiPCFPNIOCycleTime	112	snScalanceWPNIOValue - Description of the last snScalanceWiPCFPNIOmaxSTAs or snScalanceWiPCFPNIOCycleTime trap	Is generated when the specified update time in iPCF mode with PNIO support cannot be kept to.
snScalanceWForcedRoamingVapStateChanged	121	snScalanceWVirtualApIndex - Index of the VAP snScalanceWVirtualApState - Current State of the VAP unknown (0) authenticated (1) associated (2) powersafe (3) adhoc (4) joined (5) vap-is-up (6) vap-starting (7) vap-is-down (8) locked (9) vap-connected (10)	Generated when the status of the VAP changes.

Appendix B

B

B.1 MIB files supported by SCALANCE W-700

MIB files available for the SCALANCE W-700

The following table shows the MIB files available for a SCALANCE W-700:

MIB	Root OID	Reference
AUTOMATION-SYSTEM-MIB (Siemens)	1.3.6.1.4.1.4329.6.3.2	Vendor specific
BRIDGE MIB	1.3.6.1.2.1.17	RFC1493
IANA-ADDRESS-FAMILY-NUMBERS-MIB	1.3.6.1.2.1.72	RFC2233
IANAifType-MIB	1.3.6.1.2.1.30	RFC2233
IEEE8021-PAE-MIB	1.0.8802.1.1.1	IEEE 802.1X
IEEE802dot11-MIB	1.2.840.10036	IEEE 802.11
IF-MIB	1.3.6.1.2.1.31	RFC2233
LLDP-EXT-DOT3-MIB	1.0.8802.1.1.2.1.5.4623	
LLDP-EXT-PNO-MIB	1.0.8802.1.1.2.1.5.3791	
LLDP-MIB	1.0.8802.1.1.2	IEEE 802.1AB
NatMib (WindRiver)	1.3.6.1.4.1.731.100	Vendor specific
RFC1155-SMI		
RFC1212		
RFC1213-MIB	1.3.6.1.2.1	
RFC1215		
RSTP-MIB	1.3.6.1.2.1.17.11	RFC4318
SNMP-FRAMEWORK-MIB	1.3.6.1.6.3.10	RFC2571
SNMP-MPD-MIB	1.3.6.1.6.3.11	RFC2572
SNMP NOTIFICATION MIB	1.3.6.1.6.3.13	RFC2573
SNMP-TARGET-MIB	1.3.6.1.6.3.12	RFC2573
SNMP USER-BASED SM MIB	1.3.6.1.6.3.10.1.1.1	RFC2574
SNMPv2-CONF		RFC1904
SNMPv2-MIB	1.3.6.1.2.1.1	RFC1907
SNMPv2-SMI		RFC1902
SNMPv2-TC		RFC1903
SNMP-TM	1.3.6.1.6.1.1	RFC1906
SNMP VIEW-BASED ACM MIB	1.3.6.1.6.3.16	RFC2575
SN-SCALANCE-PRIV-MIB (Siemens)	1.3.6.1.4.1.4196	Vendor specific
WRS-MASTER-MIB (WindRiver)	1.3.6.1.4.1.731	Vendor specific

Appendix C

<div style="text-align: right; font-size: 3em;">C</div>

C.1 Underlying standards

Standards met by SCALANCE W-700 devices completely or partly

The following table lists some of the standards for SCALANCE W-700 devices.

Name of the standard	Topic
IEEE 802.1AB	Link Layer Discovery Protocol (LLDP)
IEEE 802.1D-1998	Media Access Control (MAC), bridges
IEEE 802.1Q	Virtual Bridged LANs (VLAN Tagging, Port Based VLANs)
IEEE 802.1W-2004	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1X	Port Based Network Access Control
IEEE 802.3-2002	Ethernet
IEEE 802.3af	Power over Ethernet (PoE)
IEEE 802.11	Wireless Local Area Network
IEEE 802.11a	Wireless standard for use of the 5 GHz frequency band
IEEE 802.11b/g	Wireless standard for use of the 2.4 GHz frequency band
IEEE 802.11e	Quality of Service
IEEE 802.h	Spectrum and transmit power management extension in the 5 GHz band in Europe

Glossary

Access Point

A (Wireless) Access Point (WAP) is an electronic device that functions as the interface between a mobile wireless network and a wired computer network. End devices (clients) establish a wireless connection to the wireless access point over a wireless adapter. The access point is connected to a permanently installed communication network over a cable.

ACL

Access Control List. List with MAC addresses with the right to access the mobile wireless network.

Ad hoc network

Mobile wireless network between individual devices (point-to-point).

AeroScout

AeroScout tags are battery-operated sensor nodes that send out WLAN frames cyclically as multicast frames. Among other things, they also have an ambient temperature sensor and a motion sensor.

AES

Advanced Encryption Standard, Encryption according to the Rijndael algorithm.

ARP

Address Resolution Protocol

The ARP protocol is used for address resolution. Its task is to find the corresponding network hardware address (MAC address) for a given protocol address.

An ARP protocol implementation is often found on hosts on which the Internet protocol family is used. IP forms a virtual network on the basis of IP addresses. These must be mapped to the given hardware addresses when the data is transported. To achieve this mapping, the ARP protocol is often used.

Bandwidth

Maximum throughput of a connecting cable (normally specified in bps).

Broadcast

A broadcast is like "calling all all stations": Broadcast packets are received by all nodes configured to receive broadcasts.

Broadcast address

A broadcast in a computer network is a message with which data packets are sent by one node to all other nodes of a network. If a message is intended for all nodes in a network, a broadcast address is used as the destination address.

DFS

Dynamic Frequency Selection. With the Dynamic Frequency Selection function, that is also part of the 802.11h expansion, an automatic channel change is possible if another user or technical device is discovered on a channel during operation. This includes, for example, radar systems that also transfer data in the 5 GHz frequency band. Before a channel is used, it is checked to make sure that no other system is already using the channel or frequency range. If another user is discovered, data transmission on the channel is stopped and the device changes to a free channel.

This is intended to avoid influence by WLAN systems operating according to 802.11a in the 5 GHz band.

DHCP

Dynamic Host Configuration Protocol

ESS

Extended Service Set. ESS is a link between two or more cells of a WLAN (BSS - Basic Service Set) and a larger mobile wireless network.

Firewall

One or more devices that allow or prevent data access to interconnected networks according to given security restrictions.

Handover

A handover is the procedure in a mobile wireless network (for example a mobile wireless network complying with IEEE 802.11) during which the mobile client changes from one cell to another or from one channel to another while a data connection exists.

HTTPS

HyperText Transfer Protocol Secure

Protocol for the encryption and authentication of communication between Web server and Web browser in the World Wide Web.

HTTPS is an expansion of HTTP for secure transmission of confidential data with the aid of SSL.

IEEE

Institute of Electrical and Electronics Engineers

IEEE 802.11

Standard for mobile wireless networks in the 2.4 GHz range with transmission rates of up to 2 Mbps.

IEEE 802.11a

Standard for mobile wireless networks in the 5 GHz range with transmission rates of up to 54 Mbps.

IEEE 802.11b

Standard for mobile wireless networks in the 2.4 GHz range with transmission rates of up to 11 Mbps.

IEEE 802.11e

Enhancement of the wireless LAN standard to support Quality of Service (QoS).

IEEE 802.11g

Standard for mobile wireless networks in the 2.4 GHz range with transmission rates of up to 54 Mbps.

IEEE 802.11h

The IEEE 802.11a standard expanded by TPC and DFS.

IEEE 802.11i

Among other things, the standard describes the WPA2 method, the TKIP procedure and the AES encryption algorithm. IEEE 802.11i removes a series of weak points in the WEP security mechanism.

IEEE 802.1x

The heart of the standard is the use of a Radius server as the authentication server. In addition to this, in IEEE 802.1x, the entire communication is encrypted.

Industrial Ethernet

A bus system complying with IEEE 802.3 (ISO 8802-2)

IP address

The IP address consists of 4 bytes. Each byte is represented in decimal, with a dot separating it from the previous one. This results in the following structure, where XXX represents a number between 0 and 255 (dotted decimal notation): `xxx.xxx.xxx.xxx`

The IP address is made up of two parts, the network ID and the host ID. This allows different subnets to be created. Depending on the bytes of the IP address used as the network ID and those used for the host ID, the IP address can be assigned to a specific address class:

Address Class	Address class identifier	Network address and node address
O	Byte 1 (possible value 1 - 126) (Byte 1 is the byte furthest left.)	Byte 2 to byte 4 Possible value in each case 0 - 255. 0.0.0 must not be assigned, 255.255.255 is the broadcast address.
B	Byte 1 (possible value 128 - 191) Byte 2 (possible value 0 - 255)	Byte 3 and byte 4 Possible value in each case 0 - 255. 0.0 must not be assigned, 255,255 is the broadcast address.
C	Byte 1 (possible value 192 - 223) Bytes 2 and 3 (possible value in each case 0 - 255)	Byte 4 Possible value 1 - 254. 0 must not be assigned, 255 is the broadcast address.
D	Byte 1 (possible value 224 - 239) multicast addresses	Byte 2 to byte 4 Possible value in each case 0 - 255 0.0.0 must not be assigned. There are several multicast addresses with a special meaning, for example 224.0.0.1 All systems of the subnet 224.0.0.2 All routers of the subnet

iPCF

The industrial Point Coordination Function is a communications protocol with which data traffic between the access point and connected stations is controlled to avoid collisions. Using iPCF, the data throughput can be optimized even with a high number of nodes. iPCF also allows fast cell changes.

PROFINET IO

PROFINET IO, abbreviated to PNIO, allows communication with distributed IO devices on the basis of Ethernet. The main feature of PROFINET IO is the cyclic data traffic between IO controller and field device.

PST

Primary Setup Tool

QoS

Quality of Service (QoS) is a general term that indicates the correct functionality of all interactive components of a telecommunications network. Depending on the communications standard (for example IP), error parameters are detected and recorded with which the operation of the technology is continuously monitored and that form the basis for any necessary maintenance. In a general sense, QoS means the quality characteristics of a network as a whole from the perspective of the user of a particular service.

RADIUS

Remote Authentification Dial In User Service. A method in which the authentication is handled on a separate server.

Roaming

Free movement of wireless LAN nodes even beyond the boundaries of an access point's cell. The nodes and can move from one cell to the next without any noticeable interruption.

Server

A server is a device or generally an object that can provide certain services at the request of a client.

Services

Services provided by a communication protocol.

SINEMA E

The planning, simulation and configuration software SINEMA E is used to plan and configure IWLAN applications. It can be used to visualize IWLAN networks, for example according to coverage, data transfer rate, signal/noise ratio and overlapping taking into account environmental and device characteristics.

SNMP

Simple Network Management Protocol. Standardized protocol for exchange of network management information.

SSID

The **S**ervice **S**et **Id**entifier (SSID) is used to identify a mobile wireless network based on IEEE 802.11.

Subnet mask

The subnet mask specifies which parts of an IP address are assigned to the network number. The bits in the IP address whose corresponding bits in the subnet mask have the value 1 are assigned to the network number.

System

All the electrical equipment within a system. A system includes, among other things: Programmable logic controllers, devices for operator control and monitoring, bus systems, field devices, drives, power supply cabling.

TCP/IP

TCP = Transport Connection Protocol; IP = Internet Protocol

TKIP

Temporal **K**ey Integrity **P**rotocol. Scheme for cyclic changing of keys in WLANs.

TPC

The Transmit-Power Control function (TPC) introduced as a supplementary function by the 802.11h enhancement for 5 GHz components allows an automatic adaptation of the transmit power. Information on the attenuation values and the expected budget reserves in received power are taken into account. TPC is also intended to make sure that the maximum permitted transmit power of a channel specified by the relevant regulatory bodies is not exceeded by the component. TPC attempts to operate with the minimum transmit power between the communicating stations or between access point and station.

WBM

Web **B**ased **M**anagement. HTTP-based configuration method in which an HTTP server is used in the relevant device.

WDS

Wireless **D**istribution **S**ystem. Radio links for connecting the access points for an extended service set (ESS).

WEP

Wired Eqivalence Privacy is an optional part of the IEEE 802.11 standard. WEP specifies methods of authentication and encryption working with fixed keys stored on the device. All devices that want to access a network in which WEP is used must first be supplied with the same keys. The keys can also only be renewed manually.

Wi-Fi

Wireless Fidelity. Specification for wireless networks.

The Wi-Fi Alliance is a group of WLAN manufacturers that tests and certifies the interoperability of WLAN products. Wi-Fi is a certification of WLANs according to 802.11b and is performed by WECA, the WiFi parent organization. This certification confirms the interoperability of WLAN products operating in compliance to the 802.11b standard.

The Wi-Fi Alliance also develops standards. The WiFi Alliance has developed its own architectures for security procedures that have not yet been standardized such as the WiFi Protected Architecture (WPA) to be able to test the compatibility of the various manufacturers' products.

For real-time transmission, the Wi-Fi Alliance has specified Wi-Fi Multimedia (WMM) for transmissions with guaranteed quality of service (QoS).

WPA

Wi-Fi Protected Access is a method specified by the die Wi-Fi alliance to close the security gaps in WEP. Authentication using a server is stipulated (802.1x). The dynamic exchange of keys at each frame introduces further security. Users can choose between TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard).
Although WPA was never officially part of the IEEE 802.11 standards family, it has become very widespread in a very short time. This, however, applies only to the WPA procedure described above using TKIP. The optional possible implementation of WPA on the basis of AES, on the other hand, did not become established and is therefore irrelevant in everyday practice. AES only took on practical value only with the development of the later WPA2 standard.

WPA-PSK

WPA-PSK is a weakened form of WPA. In this method, authentication is not established by a server but is based on a password. This password must be configured manually on the client and server. Wherever possible, you should change to the WPA method to achieve greater security.

Index