

applications & TOOLS

**Redundancy and Access Control with
SCALANCE W**

SIEMENS

Configuration 12

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility of safely and professionally using, installing, operating and servicing equipment. In using these Application Examples, you recognize that Siemens cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice. If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications – e.g. catalogs – the contents of the other documents have priority.

Warranty, liability and support

We accept no liability for information contained in this document.

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

Copyright© 2008 Siemens I IA. Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of Siemens Automation & Drives.

For questions about this document, please use the following e-mail address:

online-support.automation@siemens.com

Preface

Objective of this application

This application shows the interaction of radio components and switches in a redundant network.

One focus is placed on the redundancy function and the access control of these components.

Main contents of this application

The following main points are discussed in this application:

- Integrating SCALANCE W and SCALANCE X into a network
- Configuring different functions of the SCALANCE modules:
 - Redundancy (**RSTP**)
 - Infrastructure (**WDS**)
 - Access control (**Access Control, RADIUS**)
 - Diagnostics (**Syslog, SNMP**)
- Creating network load by an FTP transfer
- Configuring the SNMP OPC server and changes of the device profiles
- Visualizing the network components using WinCC flexible via the **SIMATIC NET SNMP OPC server** by SIMATIC NET.

Note

This application mainly deals with the configuration of the SCALANCE W modules.

The [Integration of SCALANCE X into Office Networks](#) application (BID: 29217038) gives a detailed description of the office features and test scenarios for the SCALANCE X-300 and X-400 series.

Delimitation

This application does not include a description of

- the WinCC flexible visualization software
- Industrial Ethernet
- wireless LANs

Basic knowledge of these topics is required.

Structure of this document

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

Part	Description
Application Description	This section provides a general overview of the contents. You are informed on the components used (standard hardware and software components).
Principles of Operation and Program Structures	This part describes the detailed function processes of the hardware and software components involved, the solution structures and – where useful – the specific implementation of this application. It is only required to read this part if you want to familiarize yourself with the interaction of the solution components to use these components, e.g., as a basis for your own developments.
Setup, Configuration and Operation of the Application	This part leads you step by step through the structure, important configuration steps and the commissioning and operation of the application.
Appendix	In this chapter you will find further information on, e.g., literature, glossaries etc.

Reference to Automation and Drives Service & Support

This entry originates from the internet application portal of the A&D Service and Support. The following link will take you directly to the download page of this document.

<http://support.automation.siemens.com/WW/view/de/30805917>

Table of Contents

Table of Contents	5
Application Description	7
1 Automation task.....	7
2 Automation solution.....	9
2.1 Overview of the overall solution	9
2.2 Description of the main functionality	17
2.3 Visualization for the application	18
2.4 Required hardware and software components	23
2.5 Alternative solutions.....	26
2.5.1 Further office requirements.....	26
2.5.2 MAC-based access list	26
2.5.3 Professional network management	26
Principles of Operation	27
3 General principles of operation.....	27
3.1 SNMP OPC server.....	27
3.2 SNMP basics	28
3.3 WBM – Web-Based Management	32
3.4 File transfer using FTP	33
3.5 Redundancy method.....	36
3.6 WLAN infrastructure	45
3.7 Access control	47
3.7.1 Access IP list	47
3.7.2 IEEE 802.1X (RADIUS)	48
3.8 Diagnosis & network management	50
3.8.1 Syslog messages.....	50
3.8.2 The SNMP network management station	52
Setup, Configuration and Operation of the Application	57
4 Installation and commissioning	57
4.1 Installation of the hardware and software	57
4.2 Installation of the application software	61
4.2.1 Adjust the IP addresses.....	62
4.2.2 Configuration of the Station Configurator	72
4.2.3 Load STEP 7 project.....	75
4.2.4 Start WinCC flexible Runtime	75
5 Configuration	77
5.1 Configuration of the SNMP OPC server	77
5.1.1 Configuration of the SNMP OPC server	80

5.1.2	Changing the existing SCALANCE device profiles	84
5.2	Web-based management	86
5.3	Standard configuration of the SCALANCE W modules	88
5.3.1	Wizards of the SCALANCE W788-2	89
5.3.2	Wizards of both SCALANCE W788-1	96
5.3.3	Wizards of the SCALANCE W746-1	101
5.4	Configuration of the FTP server	107
5.5	Configuration of the redundancy method RSTP	110
5.6	Configuration of WDS	117
5.6.1	WDS in the SCALANCE W788-2	118
5.6.2	WDS in the first SCALANCE W788-1	119
5.6.3	WDS in the second SCALANCE W788-1	120
5.6.4	WDS link check	121
5.7	Configuration of the access control	122
5.7.1	Access rights for IP addresses	123
5.7.2	RADIUS server in Win2003 server	124
5.8	Syslog messages	162
6	Operating scenarios in the sample network	166
6.1	FTP scenario	167
6.2	Redundancy scenario	168
6.3	Access control scenario	171
6.4	Diagnosis scenario	174
	Appendix and Bibliography	179
7	Glossary	179
8	Bibliography	180
9	History	180

Application Description

1 Automation task

Introduction

Wireless networks are often used in office networks. The construction of industrial wireless local area networks (IWLAN) is gaining more and more importance compared to wired networks.

SIMATIC NET provides a series of high-performance and robust access points and clients that allow for the construction of reliable radio networks under industrial conditions. In addition, the radio components are equipped with a number of features which have so far been known only from office networks:

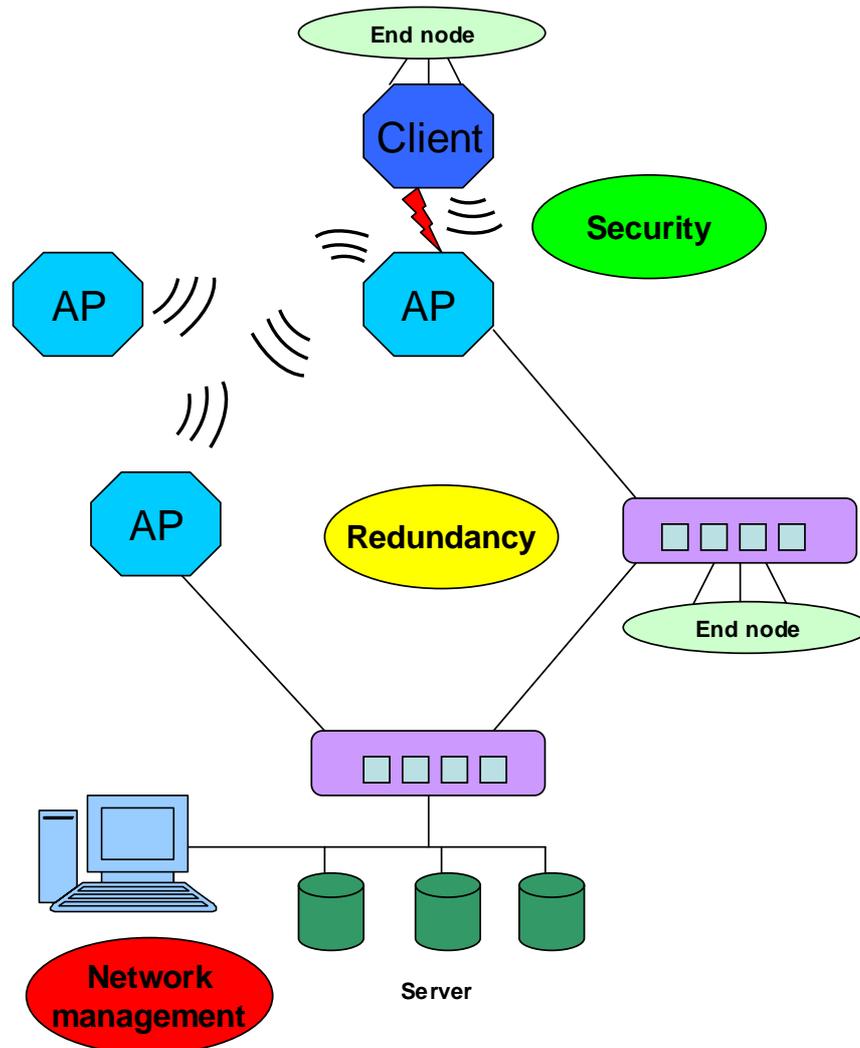
Among other things, wireless LANs provide the following advantages

- no danger of wire break,
- no additional wiring for additional nodes,
- no wiring faults,
- simple connection to moving or inaccessible nodes,
- high data throughput possible.

Overview of the automation task

The figure below provides an overview of the automation task.

Figure 1-1



Copyright © Siemens AG 2008 All rights reserved
30805917_SCALANCE_W_OFFICE_DOKU_v10_en.doc

Description of the automation task

The automation task is to integrate SCALANCE W and SCALANCE X switches into a common network. To ensure trouble-free operation, the following aspects must be considered:

- Office redundancy method
- Infrastructure
- Access control
- Diagnostic method

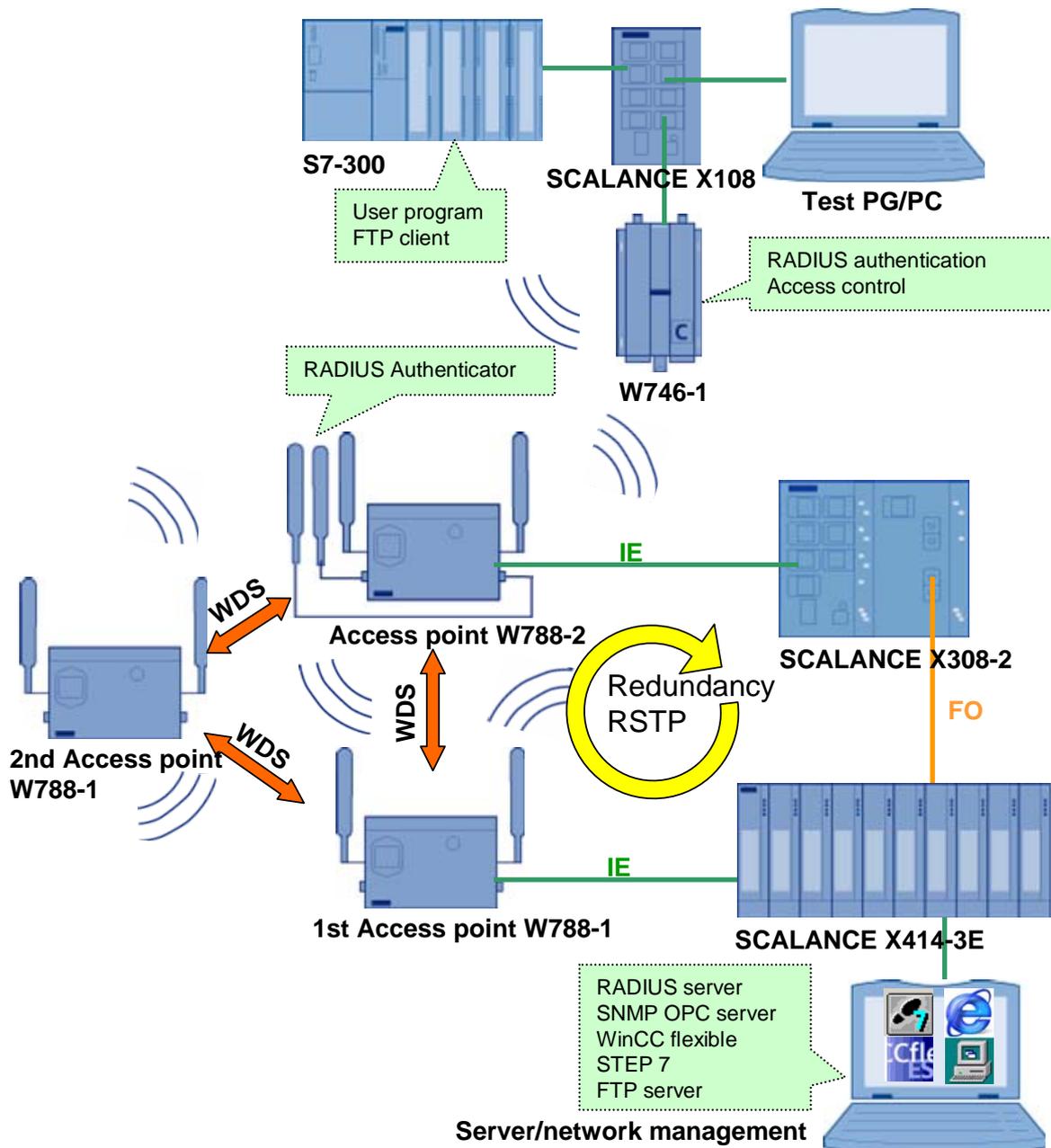
2 Automation solution

2.1 Overview of the overall solution

General overview

The following figure gives a schematic overview of the most important components of the solution:

Figure 2-1



Structure

The network shown has a redundant structure, i.e. if one of the paths fails, the second path is used for the data traffic after a short interruption.

Three SCALANCE W788-x access points and a W746-1 client are used as radio components in the data network shown. A SCALANCE X308-2 and a SCALANCE X414-3E are the wired nodes.

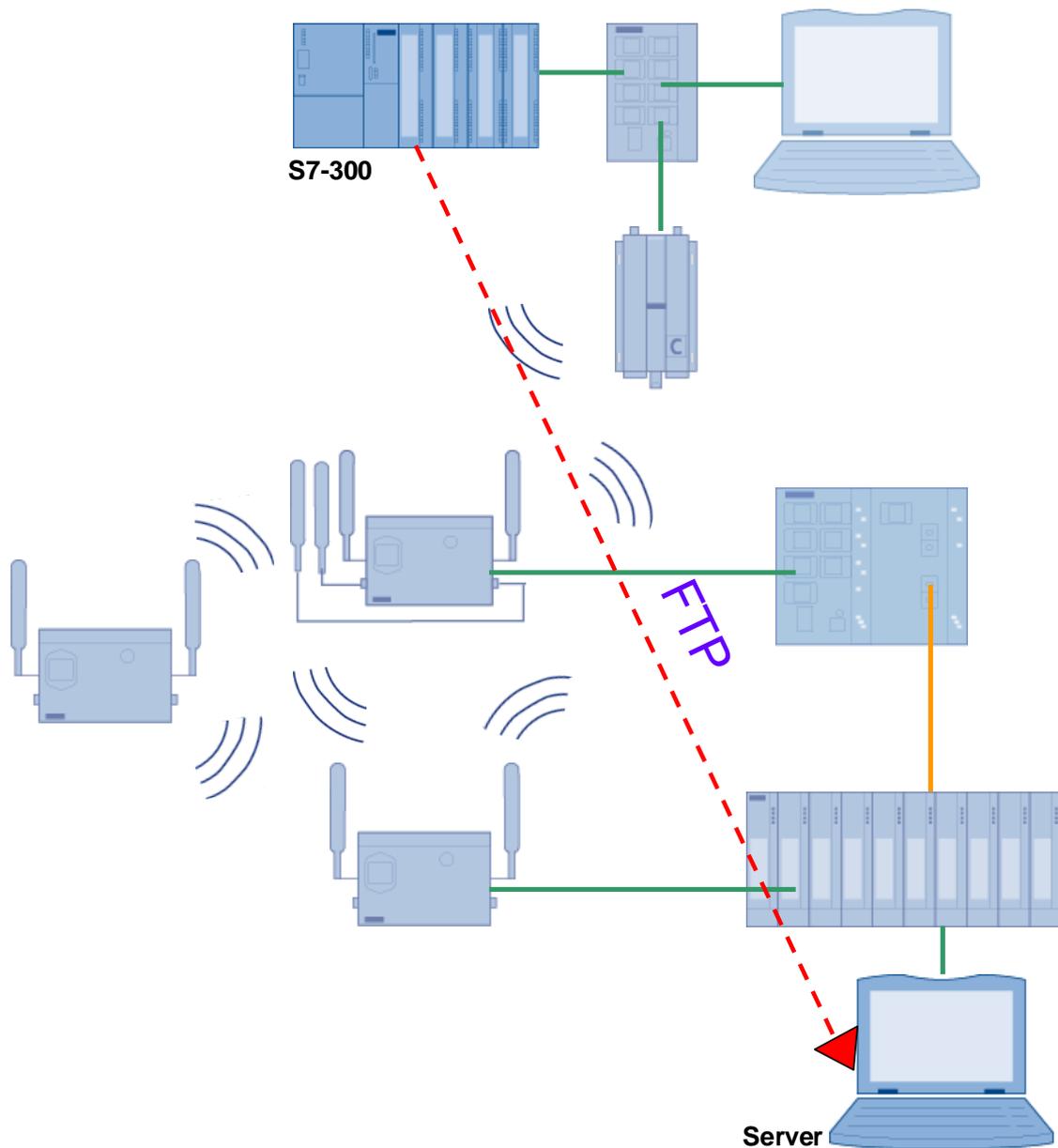
A SIMATIC S7-300 station is connected to the W746-1 client using a CP343-1 Advanced and a SCALANCE X108.

Two additional PG/PCs are included. One PC/PG is used as a network diagnostic station, server and for engineering purposes. All server programs, as well as WinCC flexible and SNMP OPC server for network visualization are run on this PC. The other PC/PG is used as a test component for access control.

"FTP" overview

The following figure shows the components that are part of the "FTP" scenario:

Figure 2-2

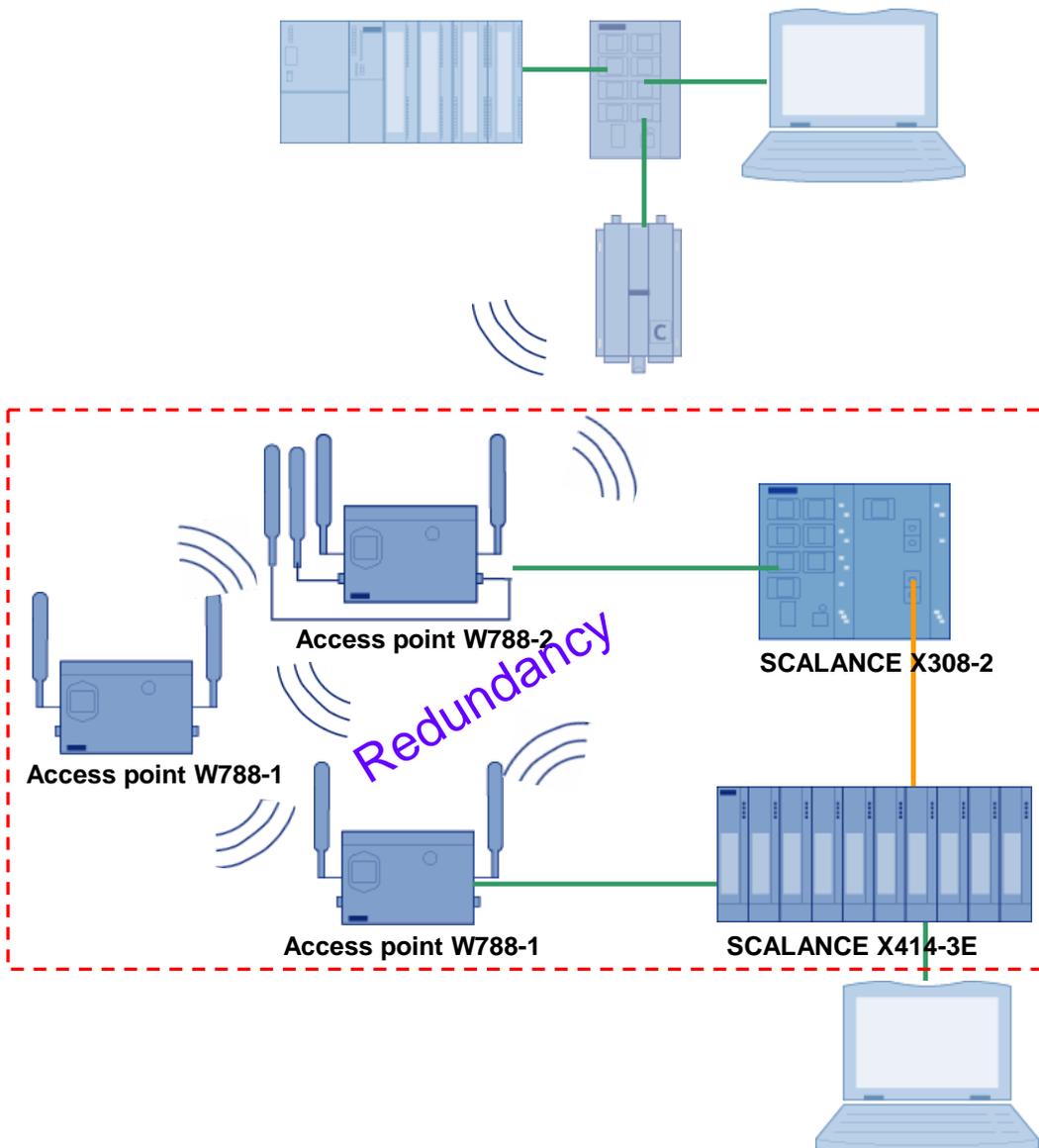


FTP data is exchanged between the S7-300 station and the server PC/PG. Once enabled, the FTP client in the CP343-1 Advanced sends a message to the FTP server every 20 seconds.

Overview of the "redundancy method"

The following figure shows the components that are part of the "redundancy method (RSTP)":

Figure 2-3

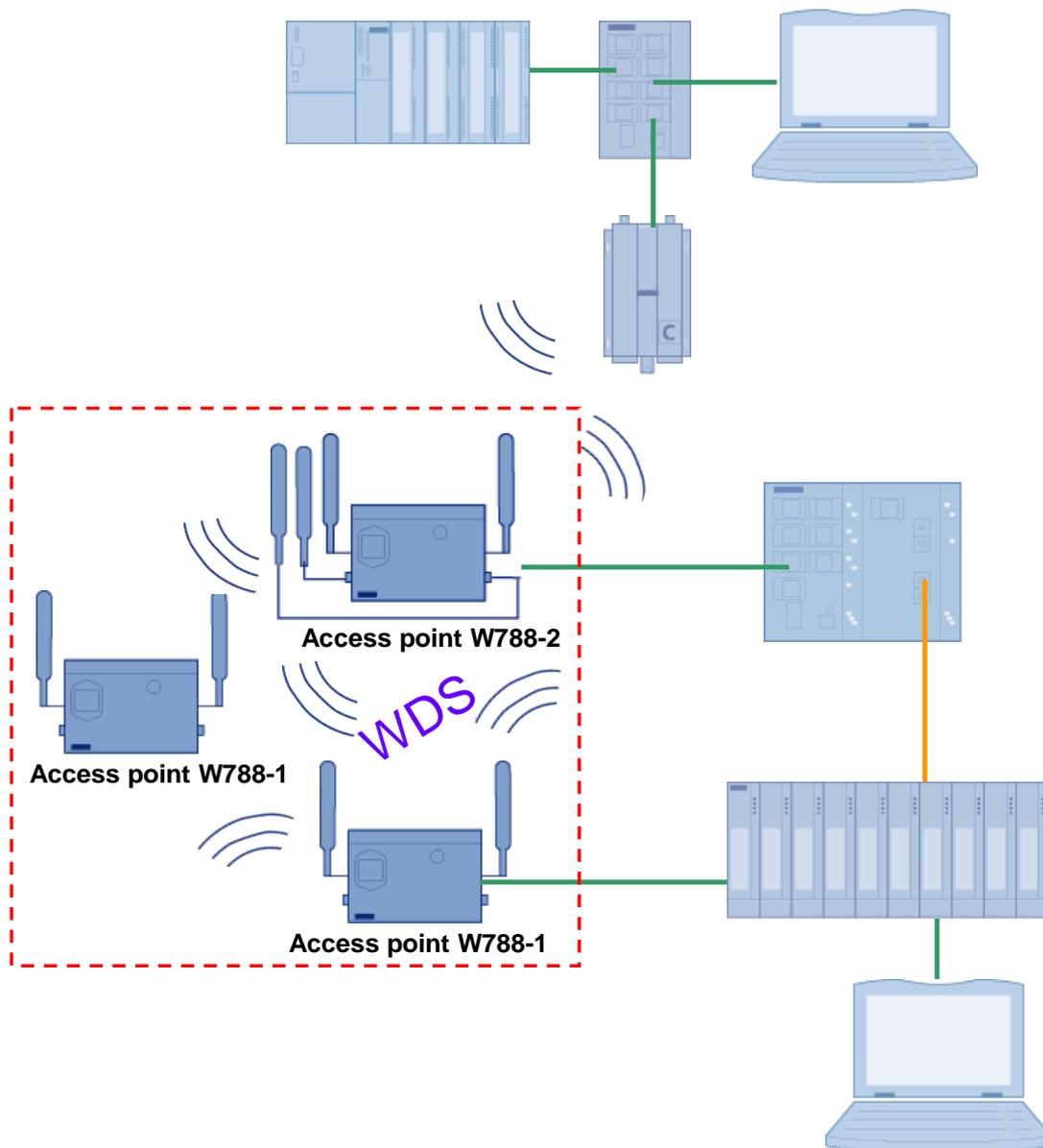


The redundancy method is configured in the two SCALANCE X modules and in the access points. The connection between the two SCALANCE X modules is configured in such a way that is used as the preferred connection.

Overview of the "Infrastructure in IWLAN"

The following figure shows the components that are part of the "Infrastructure in IWLAN (WDS)" scenario:

Figure 2-4

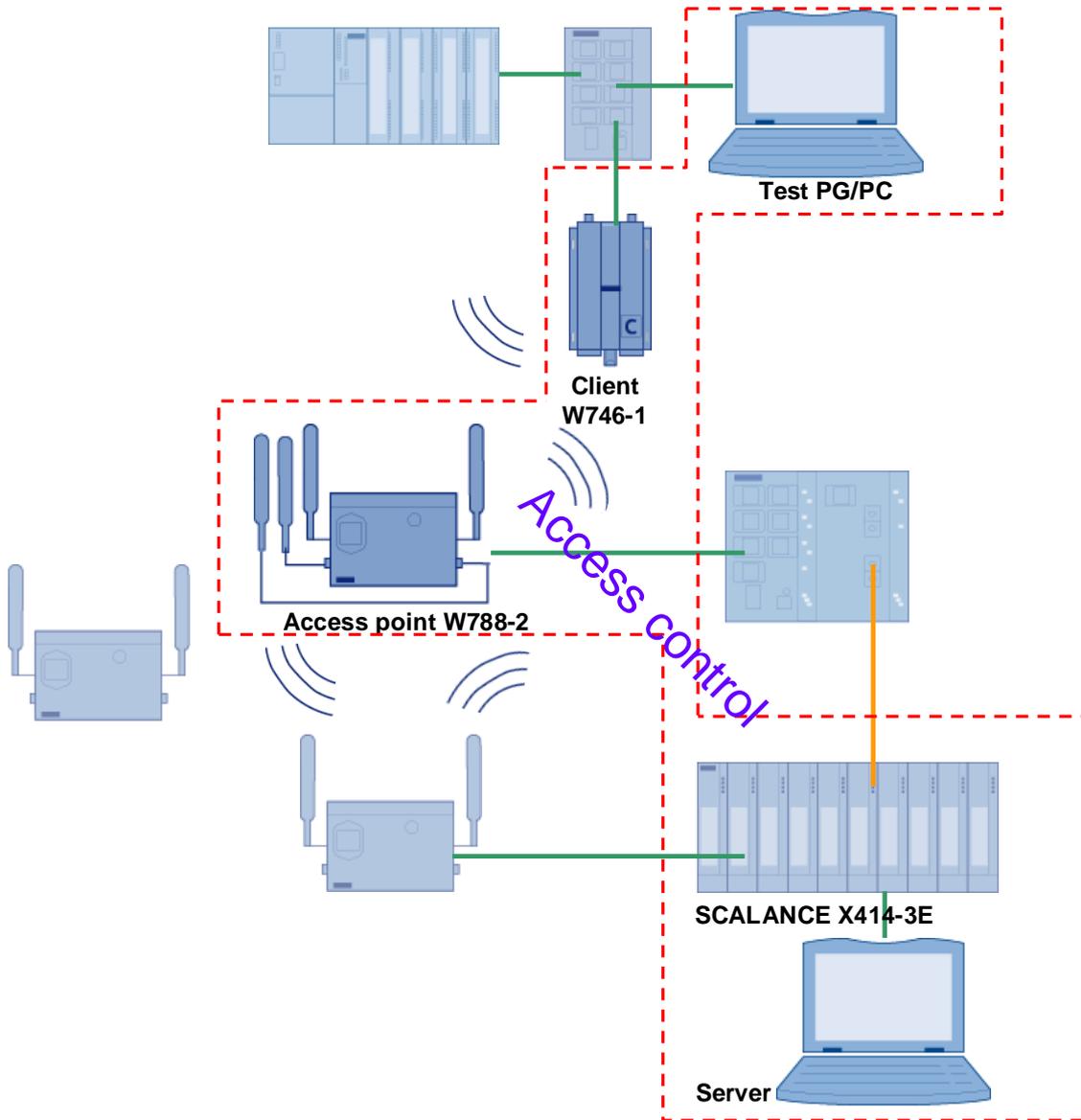


Large-area wireless networks require an appropriate infrastructure. The WDS introduced in this application is configured on all access points.

Overview of the "Access control"

The following figure shows the components that are part of the "Access control" scenario:

Figure 2-5

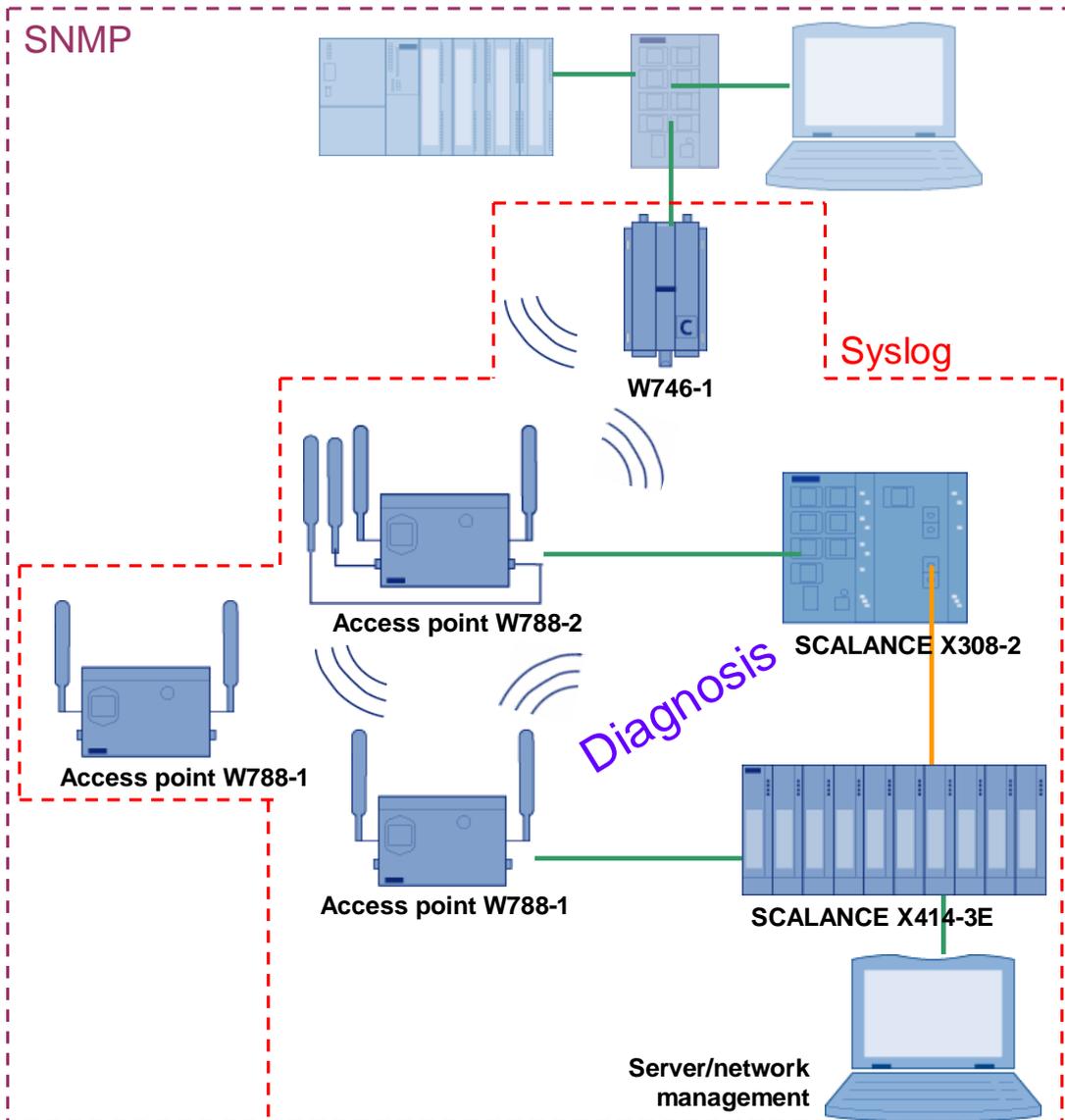


Safety aspects are very important in the use of radio technology. This is why the access control between an access point and a client/test PC/PG is demonstrated.

Overview of "diagnostic method"

The following figure shows the components that are part of the "Syslog and SNMP" scenario:

Figure 2-6



Copyright © Siemens AG 2008 All rights reserved
30805917_SCALANCE_W_OFFICE_DOKU_v10_en.doc

The diagnostic method acts across the entire network, all components are included.

A network diagnostic station visualizes the components using SNMP variables.

Overview of the methods

The following table lists the various methods with their respective standard functions:

Table 2-1

Method	Function
FTP	In the FTP data transfer, process data is sent using the FTP protocol . (RFC 959)
Redundancy method	In the redundancy method, the RSTP (Rapid Spanning Tree Protocol) is employed. (IEEE Standard 802.1w)
Infrastructure in IWLAN	The Wireless Distribution System (WDS) is used for constructing an infrastructure.
Access control	The following functions are configured as access control against unauthorized nodes: <ul style="list-style-type: none">• Access rights for IP addresses• RADIUS (IEEE Standard 802.1X)
Diagnostic method	The following methods are applied for the diagnosis of the network: <ul style="list-style-type: none">• SNMP (RFC 1157)• Syslog (RFC 3164/ RFC 3195)

2.2 Description of the main functionality

Apart from data communication, the Industrial Wireless LAN by SIMATIC NET offers a number of features that are partly known from office networks.

- Redundancy
- Infrastructure
- Access control
- Diagnostics

IT functionality

- The **redundancy method** is used for protecting the communication in a network. The network redundancy provides alternative paths which are used during the failure of a communication connection. Multi-paths are deactivated via the RSTP in order to avoid forbidden loops and double or overtaking messages. The alternative paths are only activated if a connection has failed.
- The **infrastructure in IWLAN** enables the network and its ranges to be extended without additional wiring.
- The **access control** is used to refuse unauthorized access to the network. This is done by establishing permitted IP addresses or a certain login method.
- If an event occurs within the network, the SCALANCE W is able to respond to this event using several standardized **diagnostic methods**. For example, Syslog and SNMP are employed in this application.

The following table shows how the IT functionality is assigned to the SCALANCE modules for this application:

Table 2-2

No.	Main function	Description
1.	Redundancy method (RSTP) (IEEE Standard 802.1w)	<ul style="list-style-type: none"> • All SCALANCE W • All SCALANCE X
2.	Infrastructure in IWLAN	<ul style="list-style-type: none"> • All W788-x access points
3.	Access control (Access Control, RADIUS) (IEEE Standard 802.1X)	<ul style="list-style-type: none"> • W746-1 client • W788-2 access point
4.	Diagnostic method (SNMP/Syslog) (RFC 3164/ 2821)	<ul style="list-style-type: none"> • All SCALANCE W • All SCALANCE X

2.3 Visualization for the application

General overview of WinCC flexible

The figure below shows the general overview of the network:

Figure 2-7

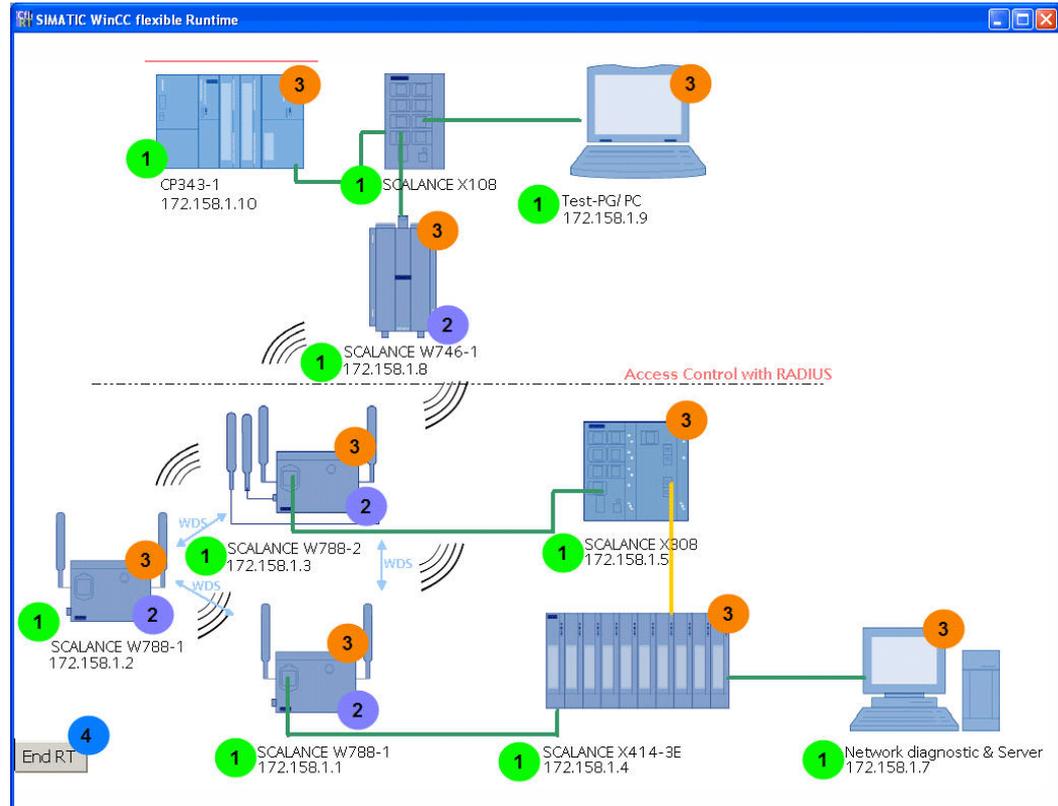


Table 2-3

No.	Item	Description
1.	Name and IP address of the network node	The IP address is determined from the SNMP information.
2.	SCALANCE W modules	A mouse-click opens a new window.
3.	Network nodes	The display is controlled by SNMP information; in case of an error or communication failure, the node is displayed red.
4.	"End RT" button	The runtime is ended.

SCALANCE W788-1 overview

A mouse-click on the first SCALANCE W788-1 opens the following window:

Figure 2-8

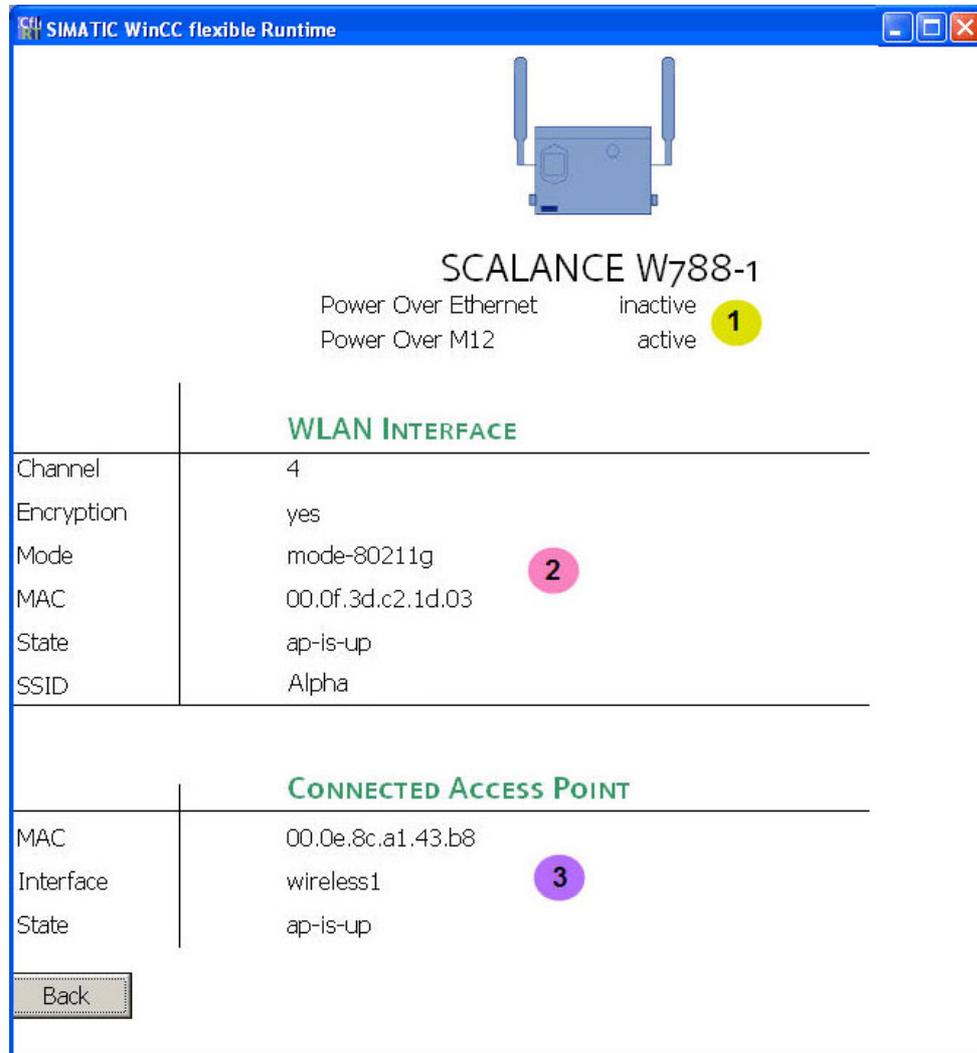


Table 2-4

No.	Item	Description
1.	Power supply status	The information is gathered from SNMP variables.
2.	Status of and information on the wireless interface of the SCALANCE W	The information and the status are read from SNMP variables and displayed.
3.	Status of and information on the connected access point	The information and the status are read from SNMP variables and displayed.

SCALANCE W788-1 overview

A mouse-click on the second SCALANCE W788-1 opens the following window:

Figure 2-9

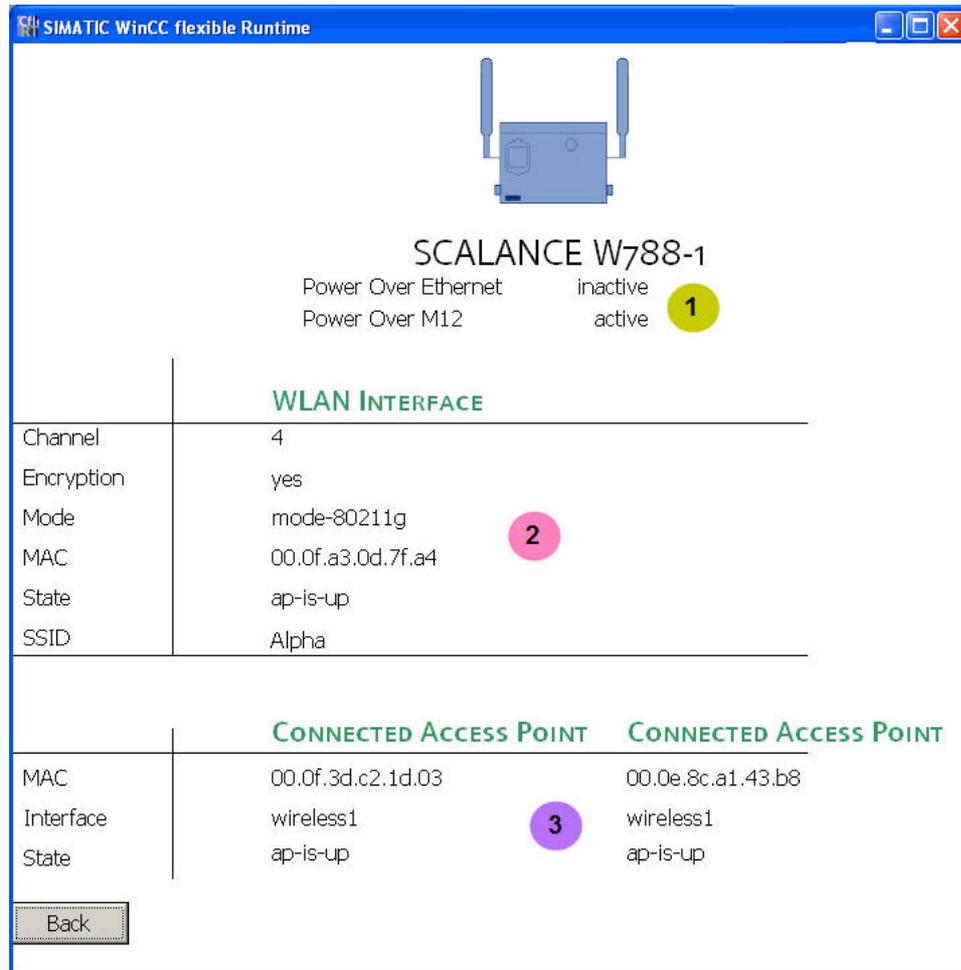


Table 2-5

No.	Item	Description
1.	Power supply status	The information is gathered from SNMP variables.
2.	Status of and information on the wireless interface of the SCALANCE W	The information and the status are read from SNMP variables and displayed.
3.	Status of and information on the connected access points	The information and the status are read from SNMP variables and displayed.

SCALANCE W788-2 overview

A mouse-click on the SCALANCE W788-2 opens the following window:

Figure 2-10

SCALANCE W788-2
Power Over Ethernet inactive **1**
Power Over M12 active

	WLAN INTERFACE 1	WLAN INTERFACE 2
Channel	4	1
Encryption	yes	yes
Mode	mode-80211g 2	mode-80211b 2
MAC	00.0e.8c.a1.43.b8	00.0e.8c.a1.43.c0
State	ap-is-up	ap-is-up
SSID	Alpha	Beta

	CLIENT/AP 1	CLIENT/AP 2
MAC	00.0f.3d.c2.1d.03	00.0e.8c.98.c1.f1
Interface	wireless1 3	wireless2 3
State	ap-is-up	associated

Back

Table 2-6

No.	Item	Description
1.	Power supply status	The information is gathered from SNMP variables.
2.	Status of and information on the wireless interface of the SCALANCE W	The information and the status are read from SNMP variables and displayed.
3.	Status of and information on the connected access point and client	The information and the status are read from SNMP variables and displayed.

SCALANCE W746-1 overview

A mouse-click on the SCALANCE W746-1 opens the following window:

Figure 2-11

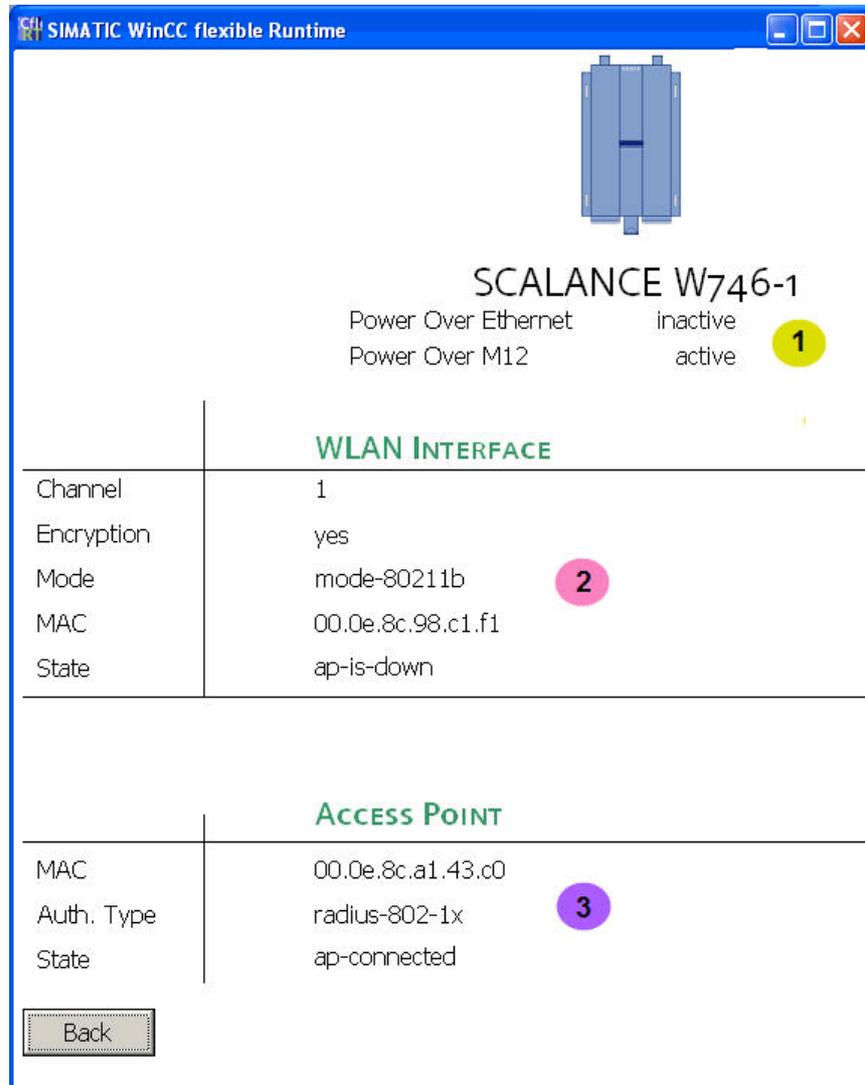


Table 2-7

No.	Item	Description
1.	Power supply status	The information is gathered from SNMP variables.
2.	Status of and information on the wireless interface of the SCALANCE W	The information and the status are read from SNMP variables and displayed.
3.	Status of and information on the connected access point	The information and the status are read from SNMP variables and displayed.

2.4 Required hardware and software components

Hardware components

Table 2-8

Component	No.	MLFB/order number	Note
SCALANCE X308-2	1	6GK5308-2FL00-2AA3	As of V2.2
SCALANCE X414-3E	1	6GK5414-3FC00-2AA2	As of V2.2; the SCALANCE X414-3E has a modular structure.
MM492-2 media module	1	6GK5492-2AL00-8AA2	2 X 1GBIT/S MULTIMODE SC additional module for the SCALANCE A414-3E
SCALANCE W788-2	1	6GK5788-2AA60-2AA0	As of FW V3.4.4
SCALANCE W788-1	2	6GK5788-1ST00-2AA6	As of FW V3.4.4
SCALANCE W746-1	1	6GK5746-1AA30-4AA0	As of V3.3.15
SCALANCE X108	1	6GK5108-0BA00-2AA3	Another switch can also be used.
CPU 313C	1	6ES7313-5BF03-0AB0	
CP343-1 Advanced	1	6GK7343-1GX21-0XE0	
Power Supply PS 307 5A	3	6ES7 307-1EA00-0AA0	Power supply unit with 24V output voltage
PC/PG	1		With Microsoft Windows XP Professional SP2
Server	1	Standard industrial PC	With Microsoft Windows Server 2003 Standard Edition Service Pack 2

Accessories

Table 2-9

Component	No.	MLFB/order number	Note
IE FC standard cable GP 2x2	1	6XV1 840-2AH10	Minimum order quantity 20m
IE FC RJ45 plug 180	10	6GK1 901-1BB10-2AA0	
IE stripping tool		6GK1 901-1GA00	Stripping tool for Ethernet cables
SIMATIC NET FO STANDARD CABLE 50/125	1	6XV1873-6AH20	Prepared with 2X2 SC plugs, length: 2m
MPI cable	1	6ES7901-0BF00-0AA0	For connecting SIMATIC S7 and PG, length: 5m

Component	No.	MLFB/order number	Note
Antenna for second interface of SCALANCE W788-2	1	6GK5795-6MR00-0AA6	Another antenna can also be used. Make sure that the clearance between the antennas of both interfaces is at least 50cm.
Power M12 cable connector	1	6GK1907-0DC10-6AA3	Content: 3 pieces

SIMATIC software components

Table 2-10

Component	No.	MLFB/order number	Note
SIMATIC STEP 7 V5.4 SP 3	1	6ES7810-5CC10-0YC5	Or higher
SIMATIC NET SOFTNET S7 LEAN 2006	1	6GK1704-1LW64-3AA0	Maximum 8 connections The SIMATIC NET software CD is included with the license.
SIMATIC NET IE SNMP OPC-SERVER BASIC/2006	1	6GK1706-1NW64-3AA0	
SIMATIC WinCC flexible 2007 Advanced	1	6AV6613-0AA01-1CA5	V1.2

Additional software

The following software components are freeware and available free of charge via the internet:

Table 2-11

Component	No.	Note
FTP server software	1	For FTP reception; e.g., Jana Server
Syslog server software	1	For receiving the Syslog messages; e.g., Kiwi Syslog Daemon by Kiwi Enterprises
Network sniffer	1	For monitoring the data traffic; e.g., Wireshark

Sample files and projects

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

Table 2-12

Component	Note
30805917_SCALANCE_W_OFFICE_CODE_v10.zip	This zip file contains the STEP 7 project, the WinCC flexible project, device profiles and standard MIBs
30805917_SCALANCE_W_OFFICE_DOKU_v10_d.pdf	This document.

2.5 Alternative solutions

2.5.1 Further office requirements

Apart from the IT functionalities already mentioned, the SCALANCE X-300, X-400 and W families also support further features used in the office environment:

Note

The [Integration of SCALANCE X into Office Networks](#) application (BID: 29217038) gives a detailed description of further office features and test scenarios for the SCALANCE X-300 and X-400 series.

2.5.2 MAC-based access list

Alternatively to the RADIUS server authentication, SCALANCE W access points support the access control list. The concept of an ACL is based on the assignment of MAC addresses and access rights. The following access rights are available:

- **Allow:** The client with the configured MAC address is allowed to access the access point.
- **Deny:** The client with the configured MAC address is denied the access to the access point.
- **Default Key:** The client with the configured MAC address is only allowed to access the access point if the default key is used for encoding.
- **Private Key:** The client with the configured MAC address is only allowed to access the access point if the private key is used for encoding. Different keys can be created for the individual clients.

2.5.3 Professional network management

Network monitoring using SNMP variables and WinCC flexible is a simple and cost-efficient way of monitoring and diagnosing the network.

An alternative are professional network management systems, which can take on many tasks at once. These include, for example:

- documentation, network analysis,
- diagnostics, recording and
- generating statistics of errors and message types.

Extensive statistics, recordings and information enable errors to be quickly localized and pinpointed.

Principles of Operation

Content

This part describes the detailed function processes of the hardware and software components involved, the solution structures and – where useful – the specific implementation of this application.

It is only required to read this part if you want to know how the individual solution components interact.

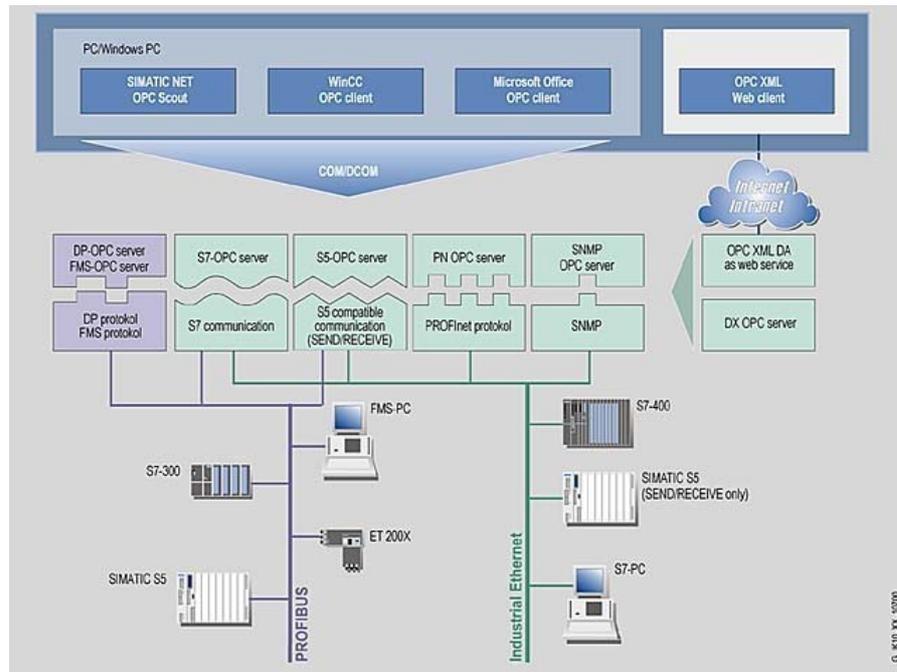
3 General principles of operation

3.1 SNMP OPC server

What is OPC?

OPC is a manufacturer-independent software interface that enables data to be exchanged between hardware and software. The OPC interface is part of the software that runs on a PC as a platform for operator control and monitoring systems or other applications.

Figure 3-1



OPC server

Manufacturers of modules supplying process data (communications systems, measuring instruments, etc.) provide their module with an OPC server that interfaces to the respective data source. Aside from these services, the OPC server provides information from any data source to the OPC client; these sources can be hardware-driven data sources or

software components. Each OPC server has a unique name for identification.

SNMP OPC server

The SNMP OPC server enables the user to monitor SNMP-capable network components and IP devices such as the SCALANCE X308-2 and SCALANCE W switch also in plants. The SNMP OPC server is used as a compiler from SNMP to the OPC interface of the HMI system. Read and write access to the respective device information is possible. This enables the diagnosis of individual devices up to a complete network infrastructure and a control (only possible during write access) of device properties, e.g., activating and deactivating individual ports.

3.2 SNMP basics

What is SNMP?

SNMP – **S**imple **N**etwork **M**anagement **P**rotocol – is a UDP-based protocol that has been designed especially for the administration of data networks and has meanwhile established as a de-facto standard in TCP/IP devices. The individual nodes in the network – network components or terminals – feature a so-called SNMP agent that provides information in a structured form. This structure is referred to as MIB (**M**anagement **I**nformation **B**ase). In the network node, the agent is usually implemented as a firmware functionality.

Management Information Base – MIB

A MIB (Management Information Base) is a standardized data structure consisting of different SNMP variables, which are described by a language independent of the target system.

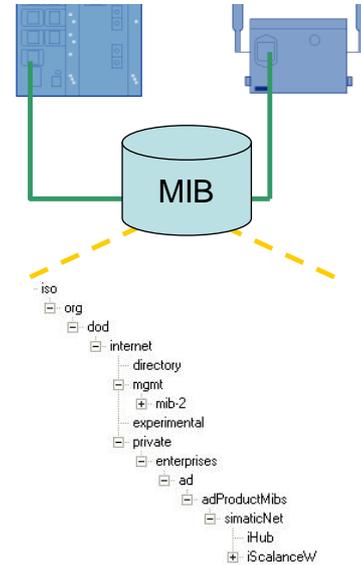
The cross-vendor standardization of the MIBs and the access mechanisms also enable to monitor and control a heterogeneous network with components made by different manufacturers.

If component-specific, non-standardized data is required for network monitoring, this data can be described by the manufacturers in so-called "private MIBs".

The figure below shows the different possible variables from the MIB.

Figure 3-2

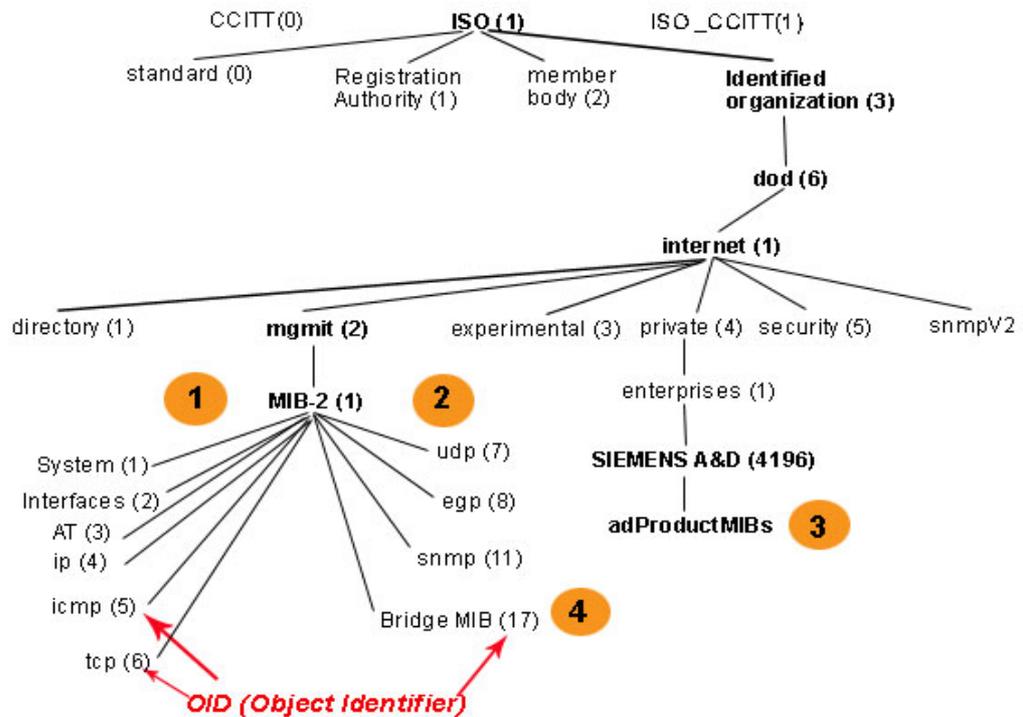
- 1 **Standardized data**
 - System information such as network statistics, counters, tables
- 2 **Extended standardized data**
 - e.g., data on network load (TMON) for switches
- 3 **Device-specific data**
 - e.g., status of the redundant power supply
- 4 **Bridge MIB**
 - e.g., topological view using an "Office tool"



The MIB information has a hierarchical structure.

The following figure shows the structure of the standard MIB (MIB-2) and the occurrence of the possible variable types mentioned above:

Figure 3-3

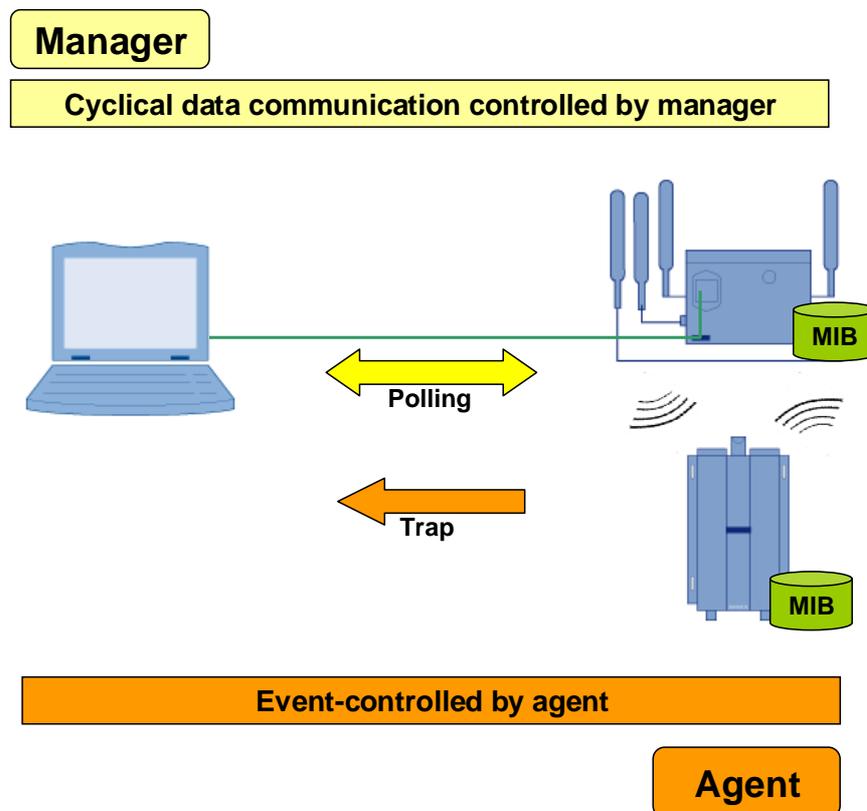


The OID (Object Identifier) describes the address of the MIB object. The address of standardized MIB objects is set by default. Private MIB objects are always stored in the "Enterprise" directory. The manufacturer is responsible for the addresses in this structure. The only requirement is to register the manufacturer number.

Data flow for SNMP

The figure below shows the data flow for SNMP:

Figure 3-4



A network management solution based on SNMP works according to the client-server model. The management station (SNMP client) can poll information from the agents to be checked, which act as servers.

The MIB information is cyclically called from the management station and visualized if required. In addition, the nodes are also capable of reporting specific statuses to the network management station via traps without explicit requests. With SNMP, not only monitoring the nodes but also instructions for controlling the devices are possible. These instructions include activating or deactivating a port on a network component.

Communication between agent and network management station is performed in the background and causes only an insignificant network load.

Device profiles

A device profile describes the scope of the variables of a device such as the SCALANCE X310 that are mapped to the OPC server. Only variables included in the device profile can be integrated into an application.

The SNMP OPC server also includes a so-called MIB compiler, which is used to adapt existing profiles or create new profiles. This is done by entering the required SNMP variables from the public and, if required, private MIBs into the profile.

SIMATIC devices featuring special SNMP agents, e.g., switches (SCALANCE X), the CP1616, CP443-1 Industrial Ethernet communications processors etc., are already included in the STEP 7 directory with their device profiles. For IP-capable devices without individual SNMP agent, the SNMP manager can at least determine the IP address and the status of the connection to this network node using the common TCP/IP "ping" status check and provide this information to the SNMP OPC server.

Note

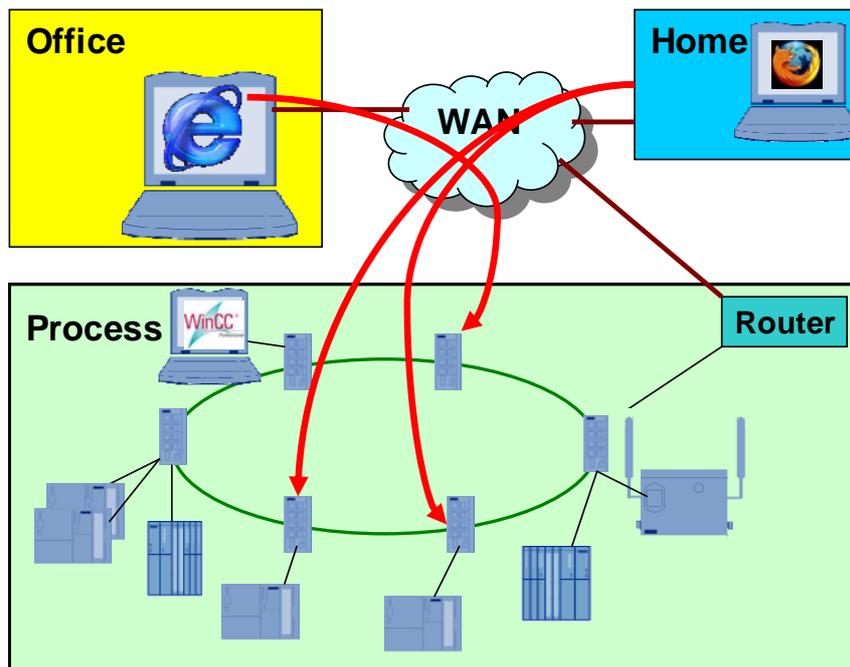
The prepared device profiles are located in the following directory:

<STEP 7InstallationDirectory>/S7DATA/snmp/profile

3.3 WBM – Web-Based Management

Web-based management enables the parameterization and monitoring of network nodes and network components such as the SCALANCE modules or terminals via standard internet browsers such as Internet Explorer or Firefox.

Figure 3-5



A browser is used to call HTML pages containing the desired information in the modules. The corresponding module dynamically supplies these HTML pages with information.

This requires only the IP address of the SCALANCE module and a password to be able to perform a read and/or write access to the information as a user or administrator.

Note

When using the web-based management, no proxy sever must be set in the connection properties of the internet browser.

3.4 File transfer using FTP

Description

The File Transfer Protocol (FTP) is a method of transferring data reliably via TCP/IP using commands. FTP is **client-server** oriented and available to almost any platform. Two separate channels are used for the FTP data connection:

- Port 21 for authentication and command transfer
- Port 20 for the data transfer

FTP types

There are two options for transferring data between server and client:

- **Private FTP:** Data transfer is only permitted for registered users who must log on to the FTP server with their user ID and password.
- **Public FTP:** Data exchange is possible to everybody logging on as **Anonymous**.

Process sequence

The File Transfer Protocol enables data transfer via TCP/IP networks. For this purpose, the client establishes a data connection to one of the servers, transfers data or requests special data and disconnects. This application simulates a production plant in the SIMATIC S7-300 and selected data is sent cyclically to the server using special FTP blocks.

The file transfer is done using a private FTP, i.e. the CP343-1 IT must log on to the FTP server with its user name and password. The login data, the password and the IP address of the FTP server are stored in the DB10.

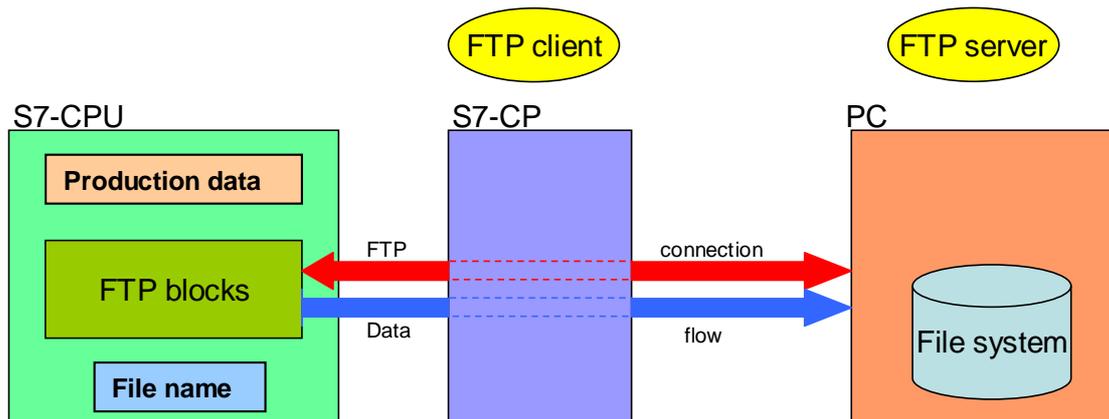
Figure 3-6

Address	Name	Type	Initial value
0.0		STRUCT	
+0.0	IP_ADR	STRING[100]	'172.158.1.7'
+102.0	user	STRING[32]	'CP341'
+136.0	password	STRING[32]	'admin'
+170.0	filename	STRING[220]	'DB100_.txt'
+392.0	CP_ADR	WORD	W#16#110
+394.0	GAB_FILLER	INT	0
+396.0	FILETYPE	STRING[4]	'.txt'

Note If you change the login data in the DB10, the changes must also be made in the FTP server.

Schematic representation

Figure 3-7



The FTP blocks

Special blocks for the FTP data transfer are provided in the SIMATIC library. The following table gives you an overview of the available blocks.

Table 3-1

Block	Function
FTP_CONNECT	Establish connection to the FTP server
FTP_STORE	Save data to FTP server
FTP_RETRIEVE	Retrieve data from the FTP server
FTP_DELETE	Delete data on the FTP server
FTP_QUIT	Disconnect from the FTP server

For FTP commands, it is absolutely necessary to observe the order of the commands.

- FTP_STORE, FTP_RETRIEVE and FTP_DELETE can only be called up after a successful FTP_CONNECT.
- FTP_CONNECT cancels with an error if a connection already exists.
- FTP_QUIT cancels with an error if there is no connection.

The STEP 7 program

Figure 3-8

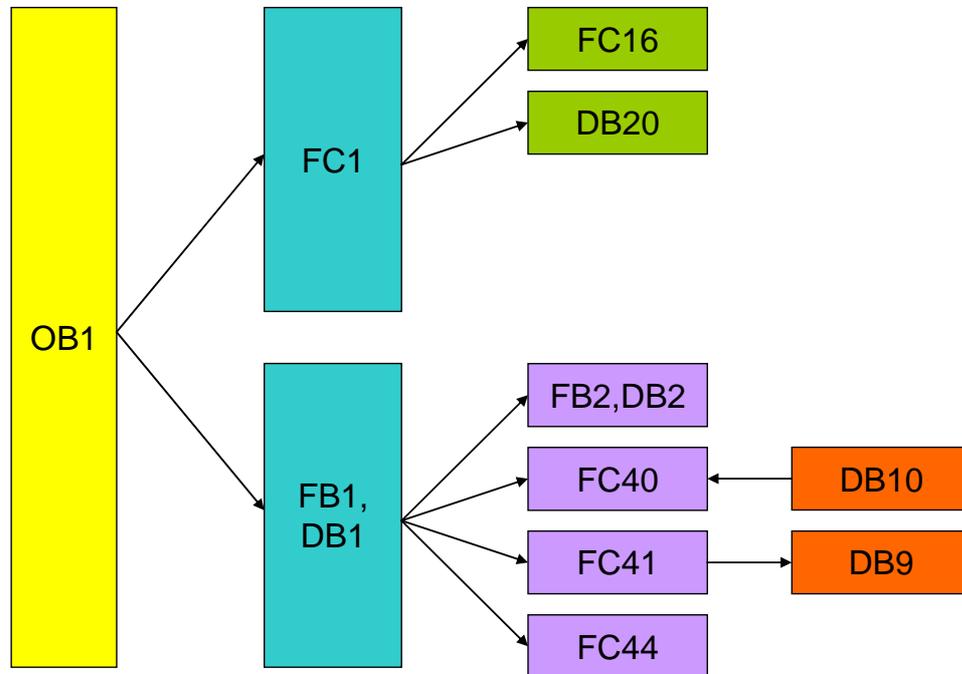


Table 3-2

Number	Name	Function
OB1		Organization block; is called once per cycle.
FC1	FILL_DB	Simulates data and writes it to the DB20.
FB1, DB1	SEND_FILE	Controls the FTP transfer using the FTP blocks via a step sequence.
FC16	I_STRNG	Library block; converts an INTEGER into a STRING.
DB20	DATA	Simulation data
FB2, DB2	FILE_NAME	Generates the file name comprising body+date+extension.
FC40	FTP_CONNECT	FTP function block; establishes the connection to the FTP server.
FC41	FTP_STORE	FTP function block; saves data as a file on the FTP server.
FC44	FTP_QUIT	FTP function block; disconnects from the FTP server.
DB10	FTP_DATA	Contains login data for the FTP server.
DB9	FTP_BUFFER	Buffer for the FC41

3.5 Redundancy method

Redundancy is a method for increasing the reliability of a network or a system. A meshed network, as used in this application, is an example of redundant networks. The nodes are connected to each other by several paths. If one component fails, or a connection is blocked, the network communication is still guaranteed and the downtimes are reduced.

Otherwise, through the redundant connections, message packages are also transmitted twice, which leads to errors and increased network load.

To prevent this loop formation, the SCALANCE modules of SIMATIC NET support the spanning tree method STP/RSTP.

The spanning tree method

The **spanning tree method** has been specified for the MAC layer. It prevents the occurrence of double data packages in a switched Ethernet network. The switches use a defined method to find the optimal path to the other nodes and deactivate double connections.

The switches continuously exchange configuration messages, so-called BPDUs (Bridge Protocol Data Unit). By means of the MAC addresses of the packages passing through, the switches independently learn the topology of the network. The network is considered as a tree.

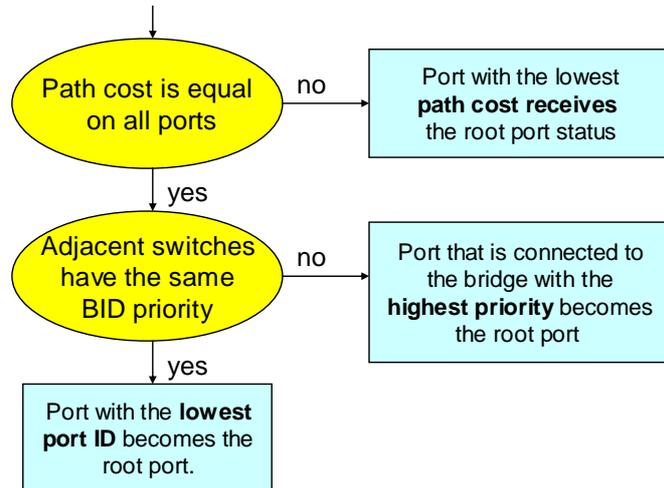
Process sequence

The suitable path through the network is selected as follows:

After initializing the switches, a **root bridge** is first of all determined. Every switch has an ID of which it informs the group. The bridge ID is 8 bytes long (2 bytes bridge priority and 6 bytes MAC address). The switch with the lowest bridge ID (i.e. highest priority) becomes the **root bridge**. All other paths are determined from this root bridge. Apart from the bridge ID, the switch also has a port ID (1 byte port priority and port number).

The other switches become **designated bridges** and select a **root port** from their ports in the direction of the root bridge. This selection is also performed by means of BPDUs that the root bridge sends to the switches.

Figure 3-9



Note

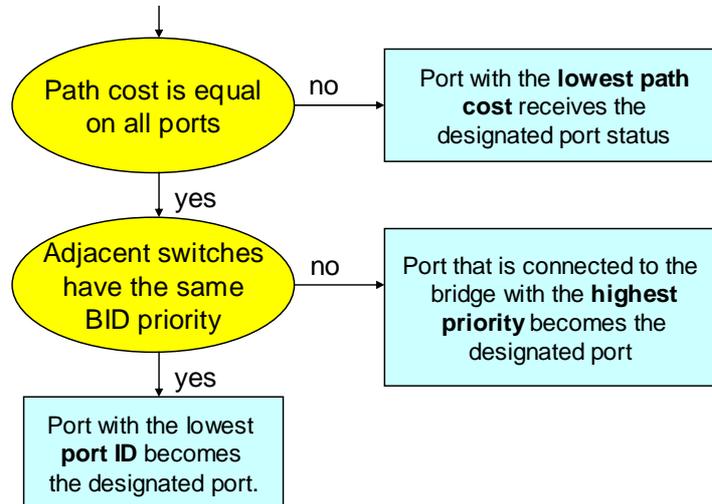
The path cost is the reciprocal value of the bandwidth of a switch port: 1000/line capacitance in Mbps.

The status of individual ports and information on the path cost can be monitored in the web-based management.

With SCALANCE X under **Switch -> Spanning tree -> Ports**
With SCALANCE W under **Information -> Spanning tree.**

The **designated ports** are determined from the other ports which are connected by a different switch. This is also done by sending BPDUs. This time the switches send messages to the connected partners.

Figure 3-10



If something has changed in the network topology, or if a switch is no longer reached, the network must be reorganized. This recalculation of the tree takes up to 30 seconds at the worst. During this time, the spanning-tree-capable switches must not forward any packages in the network except for spanning tree information.

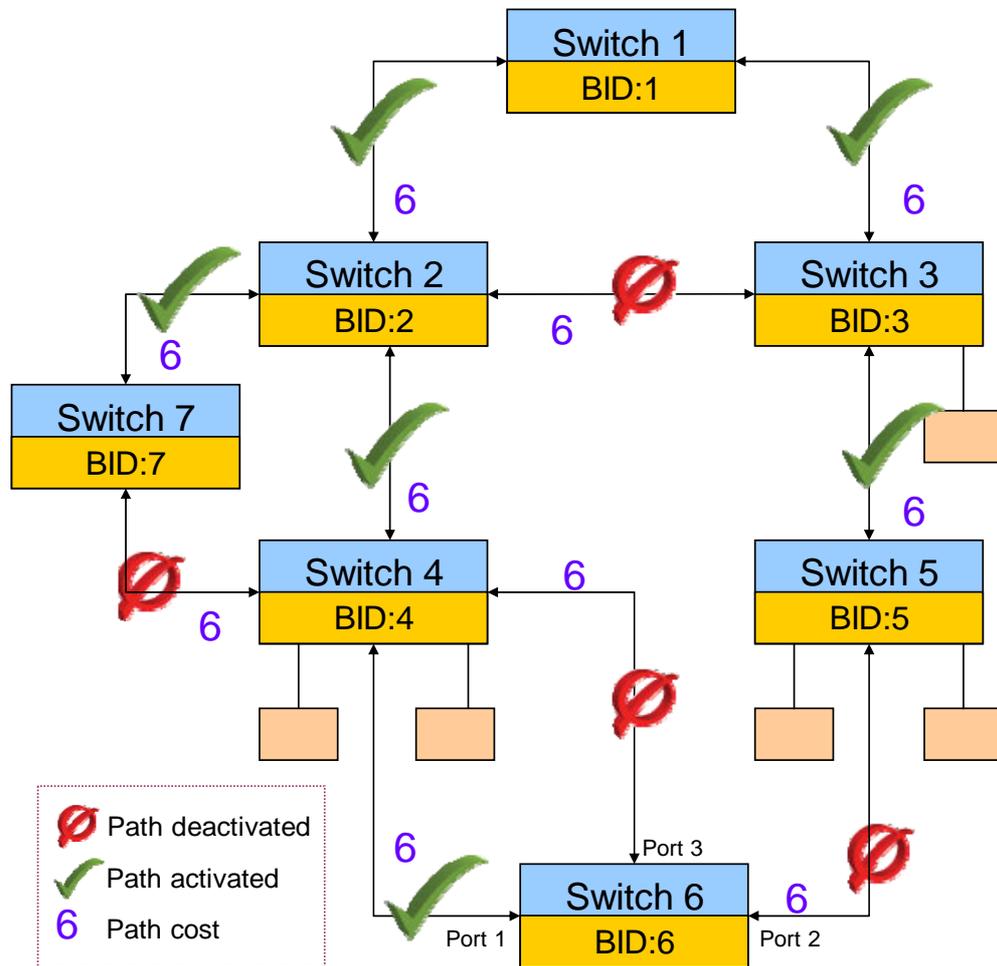
Rapid spanning tree

The rapid spanning tree method is based on the spanning tree method. It was optimized with regard to the reconfiguration time which lies in the seconds range for the rapid spanning tree method.

Example of a network configuration according to RSTP

The figure below shows a meshed network. RSTP is used to find the optimal path to all nodes and deactivate redundant connections.

Figure 3-11



Copyright © Siemens AG 2008 All rights reserved
30805917_SCALANCE_W_OFFICE_DOKU_v10_en.doc

The following table explains the principle of operation of this spanning tree example:

Table 3-3

Step	Action	Note
1.	Switch 1 is declared the root bridge.	Switch 1 has the lowest bridge ID.
2.	The path between switch 2 and switch 3 is deactivated.	The path cost between switch 2 (or 3) and switch 1 using this path is higher. The path cost between switch 2 (or 3) and switch 1 is 6. The path cost between switch 2 (or 3) and switch 1 leading via switch 3 (or 2) is 12.
3.	The path between switch 4 and switch 7 is deactivated.	The path cost between switch 4 and switch 1 using this path is higher. The path cost between switch 4 and switch 1 leading via switch 2 is only

Step	Action	Note
		12. The path cost between switch 4 and switch 1 leading via switches 7 and 2 is 18.
4.	The path between switch 6 and switch 5 is deactivated.	The path cost between switch 6 and switch 2 is the same in both directions (i.e. either via switch 4 or via switch 5). As switch 4 has the lower ID (higher priority), the port and thus the path to switch 5 is deactivated.
5.	The path between switch 6 and switch 4 is deactivated.	The level of port priority decides on the deactivation.

Bridge parameters with (R)STP

This screenshot shows the configuration window of the SCALANCE X for setting the STP parameters of the switch.

Figure 3-12

The screenshot shows the 'Spanning Tree Configuration' window with the following parameters:

Parameter	Value
Bridge Priority	32768
Root Priority	32768
Bridge Address	00-0E-8C-9A-D8-25
Root Address	00-0E-8C-9A-D8-24
Root Port	-
Root Cost	0
Topology Changes	3
Last Topology Change	44m
Bridge Hello Time [s]	2
Root Hello Time [s]	2
Bridge Forward Delay [s]	15
Root Forward Delay [s]	15
Bridge Max Age [s]	20
Root Max Age [s]	20

The parameters have the following meaning:

Table 3-4

STP parameter	Description
Bridge Priority	2-byte and unique identification of the switch; part of the bridge ID. The higher the priority, the lower the bridge ID. The value set here must be divisible by 4096.
Bridge Hello Time	Interval between sending the configuration messages (BPDUs) in seconds. The shorter this interval, the faster the switchover of a redundant connection. Recommended range: 1-10s

STP parameter	Description
Bridge Forward Delay	Delay time when using new configuration messages in seconds; new BPDUs are not used until the forward delay time has elapsed. This ensures that the new topology is only started after all modules are provided with the necessary information. If the value is too low, not all nodes use the new configuration information yet, which causes a recalculation to be started. Recommended value: 4-30s
Bridge Max Age	Indicates the maximum waiting time for a message in seconds. Once this time has elapsed without the receipt of a configuration message, the switch attempts to reconfigure the network. The lower the value, the higher the risk of unnecessary recalculation processes of new paths in the event of connection interruptions. Recommended range: 6-40s

Note The lower the number in the "Bridge Priority" field, the higher the priority and the lower the bridge ID.

Port parameters with (R)STP

This screenshot shows the configuration window of the SCALANCE X for setting the port parameters of the switch.

Figure 3-13

(Rapid) Spanning Tree Port Configuration

Port:

(R)STP enabled Admin Edge Port

Priority: Admin Point to Point Status:

Admin Path Cost: Point to Point Connection

Path Cost: Shared Media Connection

Table 3-5

STP parameter	Description
Port Priority	1-byte and unique identification of the switch; part of the port ID. The higher the priority, the lower the port ID.
Admin Path Cost	Freely selectable path cost specification; if the value is 0, the path cost is calculated using the line capacitance.
Path Cost	Calculated value for the path cost (if Admin Path Cost has value 0) or Admin Path Cost value.
Admin Edge Port	Must be activated if an end node is connected to this port.

(R)STP status overview

The following section shows the **RSTP status overview** of the SCALANCE W788-1. The upper part displays information on the current ID, MAC address and priority of both the root bridge and the switch itself. Port-related information is shown below.

Figure 3-14

(Rapid) Spanning Tree Protocol Status							
Spanning Tree:	enabled	Version:	RSTP				
RootID:	8000000e8c9ad824	BridgeID:	800008000693d3d8				
Root priority:	32768 (0x8000)	Bridge priority:	32768 (0x8000)				
Root MAC:	00-0E-8C-9A-D8-24	Bridge MAC:	08-00-06-93-D3-D8				
Topology changes:	4	Time since topology change:	0 days, 0:47:32				
Port Name	En	Cost	Priority	Edge	P.t.P.	Port State	Role
Ethernet	-	100	128	X	-	DISCARDING	DISABLED
WLAN 1	X	33	128	X	-	FORWARDING	DESIGNATED
WLAN 1 VAP 1	-	100	128	X	-	DISCARDING	DISABLED
WLAN 1 VAP 2	-	100	128	X	-	DISCARDING	DISABLED
WLAN 1 VAP 3	-	100	128	X	-	DISCARDING	DISABLED
WLAN 1 VAP 4	-	100	128	X	-	DISCARDING	DISABLED
WLAN 1 VAP 5	-	100	128	X	-	DISCARDING	DISABLED
WLAN 1 VAP 6	-	100	128	X	-	DISCARDING	DISABLED
WLAN 1 VAP 7	-	100	128	X	-	DISCARDING	DISABLED
WLAN 1 WDS 1	X	33	128	-	-	FORWARDING	ROOT
WLAN 1 WDS 2	X	33	128	-	-	DISCARDING	ALTERNATE
WLAN 1 WDS 3	-	100	128	-	-	DISCARDING	DISABLED
WLAN 1 WDS 4	-	100	128	-	-	DISCARDING	DISABLED
WLAN 1 WDS 5	-	100	128	-	-	DISCARDING	DISABLED
WLAN 1 WDS 6	-	100	128	-	-	DISCARDING	DISABLED
WLAN 1 WDS 7	-	100	128	-	-	DISCARDING	DISABLED
WLAN 1 WDS 8	-	100	128	-	-	DISCARDING	DISABLED

The columns have the following meaning:

Table 3-6

information	Function
Port Name	Plain text name of the port
Enabled	Indicates whether RSTP has been activated for this port.
Cost	Path cost for this port
Priority	Current priority of the port
Edge	Indicates whether the port is connected to an end node.
P.t.P	Indicates whether the AP is directly connected to another RSTP device.
Port State	Status of the port: <ul style="list-style-type: none"> • DISCARDING: no messages are sent from or to this port. The port is deactivated. • LEARNING: The port receives packages, however, does not forward them. Furthermore, the MAC addresses are entered in the "learning bridge". • FORWARDING: The port is enabled.
Role	Status of the port with regard to the root bridge: <ul style="list-style-type: none"> • ROOT: The port is the root port and directly connected to the root bridge. • DESIGNATED: Port that is not directly connected to the root bridge but enabled. • EDGE: No further switches are connected to this port. • ALTERNATE: Alternative path to the ROOT when the topology has been changed. Is not included in the current topology. • BLOCKED: Blocked port • DISABLED: The port is currently not in use.

3.6 WLAN infrastructure

For implementing a complex radio LAN network, planning with regard to the application environment and the expected data load is indispensable. Aspects such as ground plan, building material, environment and range must be considered critically in order to achieve an optimal radio connection.

During normal operation, several clients communicating with each other are logged on to one access point. There are also applications with several access points communicating with each other, e.g., to cover a larger radio area or build up wireless backbones (large networks which are connected to each other).

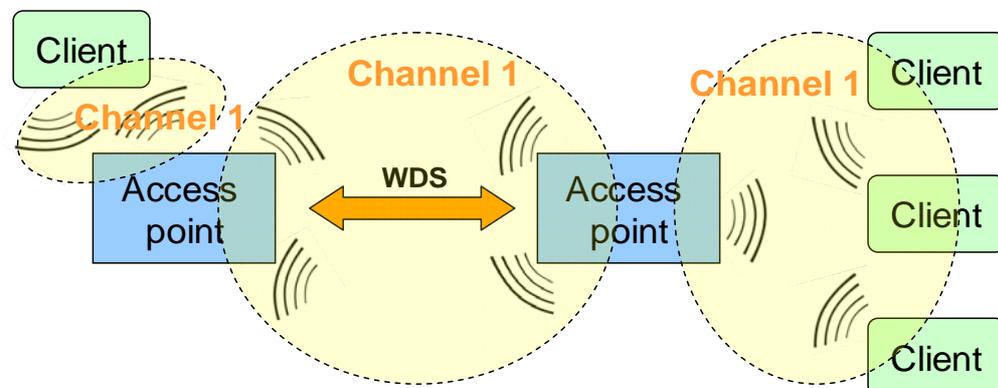
Wireless Distribution System (WDS)

The wireless distribution system is a distribution system where several base stations (access points) are connected to each other, in order to cover a larger area. The access points do not have to be wired but transfer data by radio. The access point partner can be configured both using its name or its MAC address.

Schematic representation

The following figure illustrates this scenario:

Figure 3-15

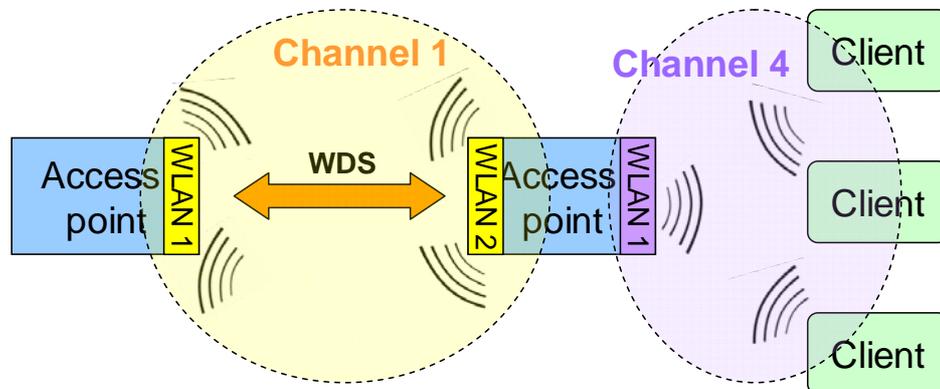


Restrictions

The following general requirements/restrictions must be observed when using WDS:

- All access points that are connected by the wireless distribution system must use the same radio channel.
- If WDS has been configured on one access point and clients are also logged on, the usable bandwidth of the access point is halved because every data package must be transferred twice. This can be corrected using a SCALANCE W with two WLAN interfaces that can be operated in parallel on different radio channels.

Figure 3-16



- WDS cannot be operated using the iPCF function. iPCF (industrial Point Coordination Function) is a proprietary method for controlling the data traffic within a radio cell that has been adapted especially to industrial requirements.
- The use of IEEE 802.11h (range adjustment, indoor and outdoor channels) is not permissible for WDS paths.

3.7 Access control

The access control is used to refuse unauthorized access to the network. In this application two methods are used.

- Access IP list
- IEEE 802.1X (RADIUS)

3.7.1 Access IP list

Description

The access IP list assigns certain access rights to IP addresses. This allows for a restriction of the web-based management access to defined addresses for the SCALANCE W modules.

Figure 3-17

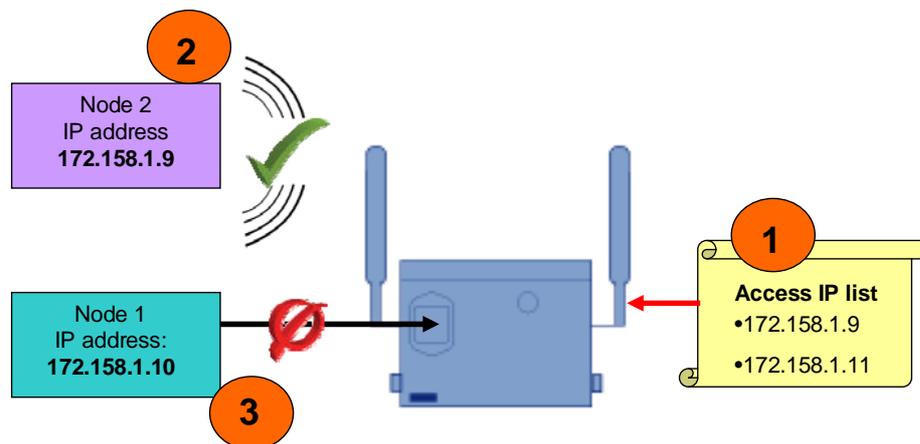


Table 3-7

No.	Action
1.	An access IP list was created in the SCALANCE W and IP addresses enabled for management access.
2.	Node 1 is allowed to access the SCALANCE W management because its IP address has been configured in the list.
3.	Node 2 is denied the access to the SCALANCE W management because its IP address is not included in the access IP list.

3.7.2 IEEE 802.1X (RADIUS)

Description

RADIUS stands for **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice and is a client-server protocol for

- authentication
- authorization and for
- accounting

of nodes in the network. This access control is based on an external authentication server.

If the RADIUS function has been activated on one access port, the node that wants to connect to the network via this access point must first authenticate itself before being granted access to the network.

Process sequence

The SCALANCE switch (authenticator) requests the authentication information from the node (supplicant) and forwards it to the RADIUS server (authentication server). The authentication server checks the access authorization of the supplicant and informs the authenticator whether the supplicant will be granted access to the network. Depending on the response of the authentication server, the authenticator enables the port or disables it.

This network record shows the negotiation process between the SCALANCE switch and the RADIUS server:

Figure 3-18

```
172.158.1.3      172.158.1.7      RADIUS  Access-Request(1) (id=10, l=228)
172.158.1.7      172.158.1.3      RADIUS  Access-challenge(11) (id=10, l=109)
172.158.1.3      172.158.1.7      RADIUS  Access-Request(1) (id=11, l=237)
172.158.1.7      172.158.1.3      RADIUS  Access-Accept(2) (id=11, l=265)
```

The RADIUS protocols have the following meaning:

Table 3-8

Protocol	Description
Access Challenge	Is sent by a RADIUS server as a response to an access request message. This message is a query to the supplicant because the RADIUS server needs more information for authentication.
Access Request	Is sent from an authenticator in order to request the authentication and authorization for a connection attempt.
Access Accept	Is sent by a RADIUS server as a response to an access request message. This message informs the authenticator that the connection attempt is authenticated and authorized.

Authentication type

The authentication type describes the mode of authentication the access client uses for authentication. A distinction is made between

- CHAP (Challenge Handshake Authentication Protocol)
- EAP (Extensive Authentication Protocol)
- PEAP (Protected Extensive Authentication Protocol)
- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)
- MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol)

Note

The SCALANCE W746-1 supports the PEAP and MS-CHAP v2 authentication types.

Schematic representation

Figure 3-19

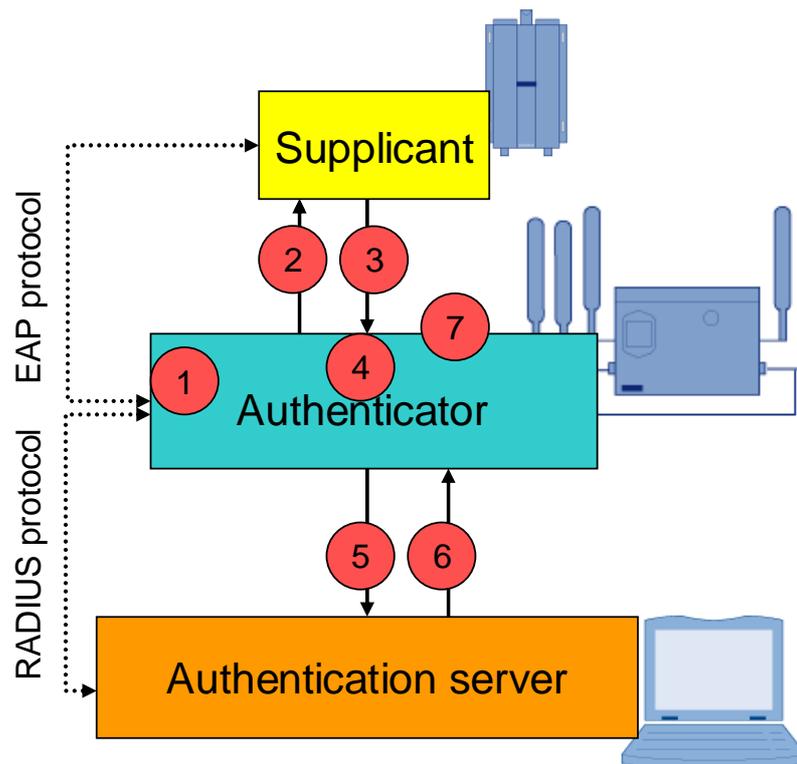


Table 3-9

No.	Description
1.	The RADIUS function was activated in the access point the node (supplicant) wants to connect to.
2.	The SCALANCE W (authenticator) sends an EAP request identity to the supplicant.
3.	The supplicant responds with its identity response.
4.	The authenticator converts the EAP protocol into a RADIUS protocol.
5.	The authenticator sends the message to the RADIUS server (authentication server).
6.	The authentication server checks the authorization of the supplicant and sends the result to the authenticator.
7.	If the supplicant was accepted, the authenticator enables the WLAN. Otherwise, the WLAN remains disabled.

3.8 Diagnosis & network management

Diagnostic methods are a must for every network. These methods can help to recognize and eliminate errors or failures in a network quickly.

3.8.1 Syslog messages

Description

Syslog is an application that transfers simple plain text messages in the network using UDP.

The components of a Syslog message are:

- The error message in plain text.
- Priority of the message. The following stages are differentiated here:
 - Emerg: very severe error, failure
 - Alert: severe error
 - Crit: error, critical state
 - Warning: warnings
 - Notice: normal messages
 - Info: information
 - Debug: mostly insignificant information
- Generator of the Syslog message (facility).
- Header with time stamp and IP address of the sender.

Process sequence

If a configured event occurs, the SCALANCE components automatically generate a Syslog message and send it to the Syslog server.

Events to be reported

The following events are reported via a Syslog message:

- Cold and warm start
- Link change (link up/link down)
- Failed authentication
- Error status change
- Change in the RSTP topology

Figure 3-20

Date	Time	Priority	Hostname	Message
07-31-2008	02:31:46	Local0.Debug	172.158.1.3	[LOGTABLE] Restart 45: 00:03:11: Overlap-AP found: AP 'Funkloch' [00:0F:3D:C2:1D:03] found on channel 4 (signal: 12 %)
07-31-2008	02:30:48	Local0.Debug	172.158.1.3	[LOGTABLE] Restart 45: 00:02:12: Overlap-AP found: AP 'BMS-FEU2-54-TEL-09122-99210' [00:02:6F:36:4F:86] found on channel 4 (signal: 10 %)
07-31-2008	02:29:56	Local0.Debug	172.158.1.3	[LOGTABLE] Restart 45: 00:01:20: Overlap-AP found: AP 'Funkloch' [00:0E:8C:A1:43:B8] found on channel 4 (signal: 47 %)
07-31-2008	02:29:52	Local0.Debug	172.158.1.3	[LOGTABLE] Restart 45: 00:01:16: Overlap-AP found: AP 'BlackHole' [00:0E:8C:A1:43:C0] found on channel 1 (signal: 61 %)
07-31-2008	02:29:02	Local0.Debug	172.158.1.8	[LOGTABLE] Restart 46: 00:00:05: Power Ethernet is off
07-31-2008	02:29:01	Local0.Debug	172.158.1.8	[LOGTABLE] Restart 45: 00:00:00: Cold start performed
07-31-2008	02:29:01	Local0.Debug	172.158.1.8	[AUTHLOG] 00:00:04 device 00-0E-8C-A1-43-C0 with event 'client associated'
07-31-2008	02:29:01	Local0.Debug	172.158.1.8	[AUTHLOG] 00:00:04 device 00-0E-8C-A1-43-C0 with event 'client authenticated'
07-31-2008	02:29:00	Local0.Debug	172.158.1.3	[AUTHLOG] 00:00:18 device 00-0E-8C-98-C1-F1 with event 'client pass RADIUS successful'
07-31-2008	02:28:59	Local0.Debug	172.158.1.3	[LOGTABLE] Restart 45: 00:00:17: (R)STP: topology change detected.
07-31-2008	02:28:59	Local0.Debug	172.158.1.3	[AUTHLOG] 00:00:15 device 00-0E-8C-98-C1-F1 with event 'client associated'
07-31-2008	02:28:59	Local0.Debug	172.158.1.3	[AUTHLOG] 00:00:15 device 00-0E-8C-98-C1-F1 with event 'client authenticated'
07-31-2008	02:28:59	Local0.Debug	172.158.1.3	[LOGTABLE] Restart 45: 00:00:15: (R)STP: topology change detected.
07-31-2008	02:28:59	Local0.Debug	172.158.1.3	[LOGTABLE] Restart 45: 00:00:14: Power Ethernet is off
07-31-2008	02:28:59	Local0.Debug	172.158.1.3	[LOGTABLE] Restart 45: 00:00:14: WLAN 1 WDS 1 is on

Prerequisites

The following prerequisites are required for the Syslog function in SCALANCE:

- The Syslog function must be activated in the switch.
- The Syslog function must be active for the respective event.
- There must be a Syslog server in the network.
- The IP address of the Syslog server must be made known to the switch.

The events and the required address can be configured using the web-based management.

3.8.2 The SNMP network management station

A network management station manages the complete network and the nodes.

Description

The visualization for the network management station of this application was generated in WinCC flexible. Apart from a general overview of the network, it also displays individual information on the SCALANCE W modules.

All the data and information is polled from the components via SNMP.

Process sequence

The configuration of the SNMP OPC server includes the definition of the complete SNMP data from the MIBs of the SNMP-capable devices that is to be mapped to OPC variables. This information is automatically polled by the SNMP OPC server from the SNMP agents of the accessible devices at regular intervals.

By means of the OPC variables, the SNMP OPC server provides the data received in this way to the OPC client – in this case the HMI system (WinCC flexible RT).

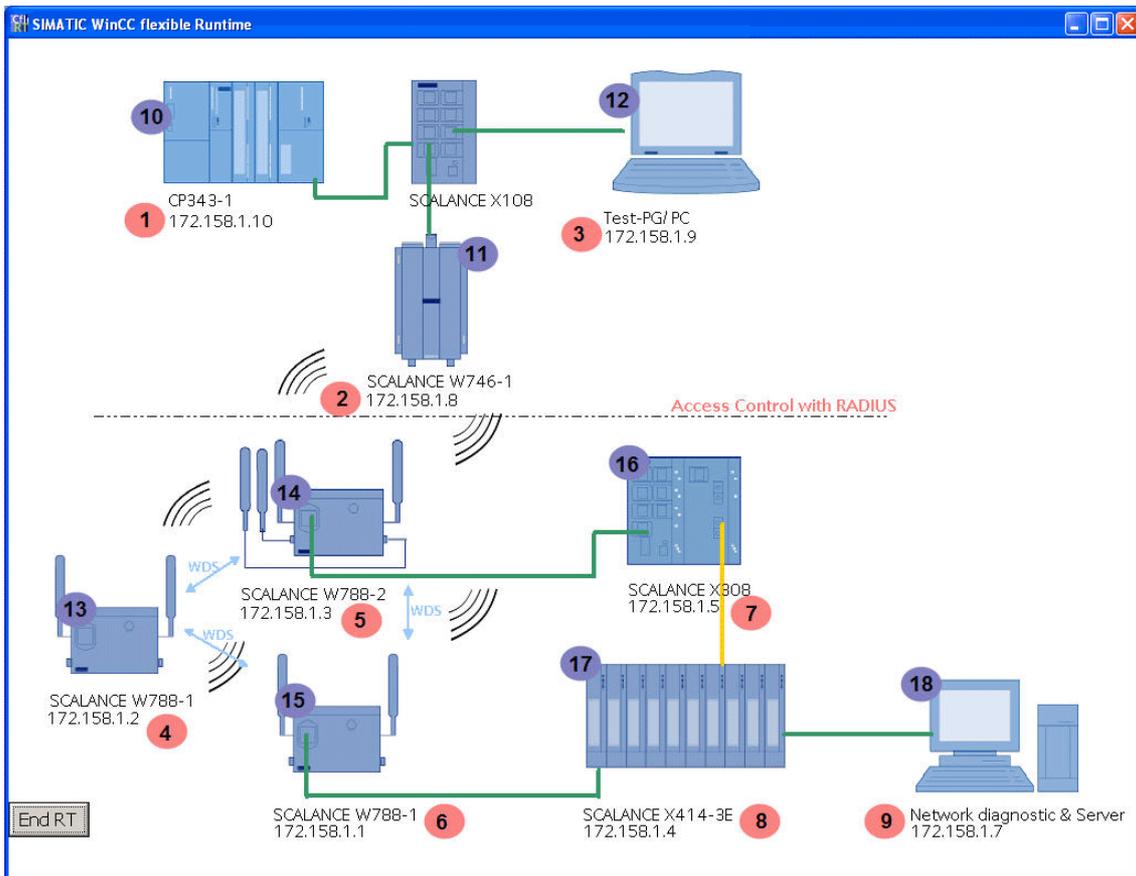
OPC variable

If the connection to one or several devices is interrupted, e.g., by link down of the HMI port on the SCALANCE X414-3E switch, the OPC variables that are now no longer supplied are marked as invalid. However, the OPC server permanently provides variables on the status of the connection.

SNMP variables for the general overview

The following figure shows the variables used for the general overview of the visualization:

Figure 3-21



Copyright © Siemens AG 2008 All rights reserved
30805917_SCALANCE_W_OFFICE_DOKU_v10_en.doc

These variables are used for the display of the IP addresses:

Table 3-10

No.	Name	Data type	OPC item ID
1.	CP343_IP	String	SNMP:[CP343-1]&ipaddress()
2.	W746_IP	String	SNMP:[W746-1]&ipaddress()
3.	Test_PC_IP	String	SNMP:[Test_PC]&ipaddress()
4.	W788-1_2_IP	String	SNMP:[W788-1_2]&ipaddress()
5.	W788-2_IP	String	SNMP:[W788-2]&ipaddress()
6.	W788-1_1_IP	String	SNMP:[W788-1_1]&ipaddress()
7.	SCALANCE X300_IP	String	SNMP:[SCALANCE X308]&ipaddress()
8.	SCALANCE X400_IP	String	SNMP:[SCALANCE X414]&ipaddress()
9.	Server_IP	String	SNMP:[Server]&ipaddress()

These SNMP variables provide the status of the node:

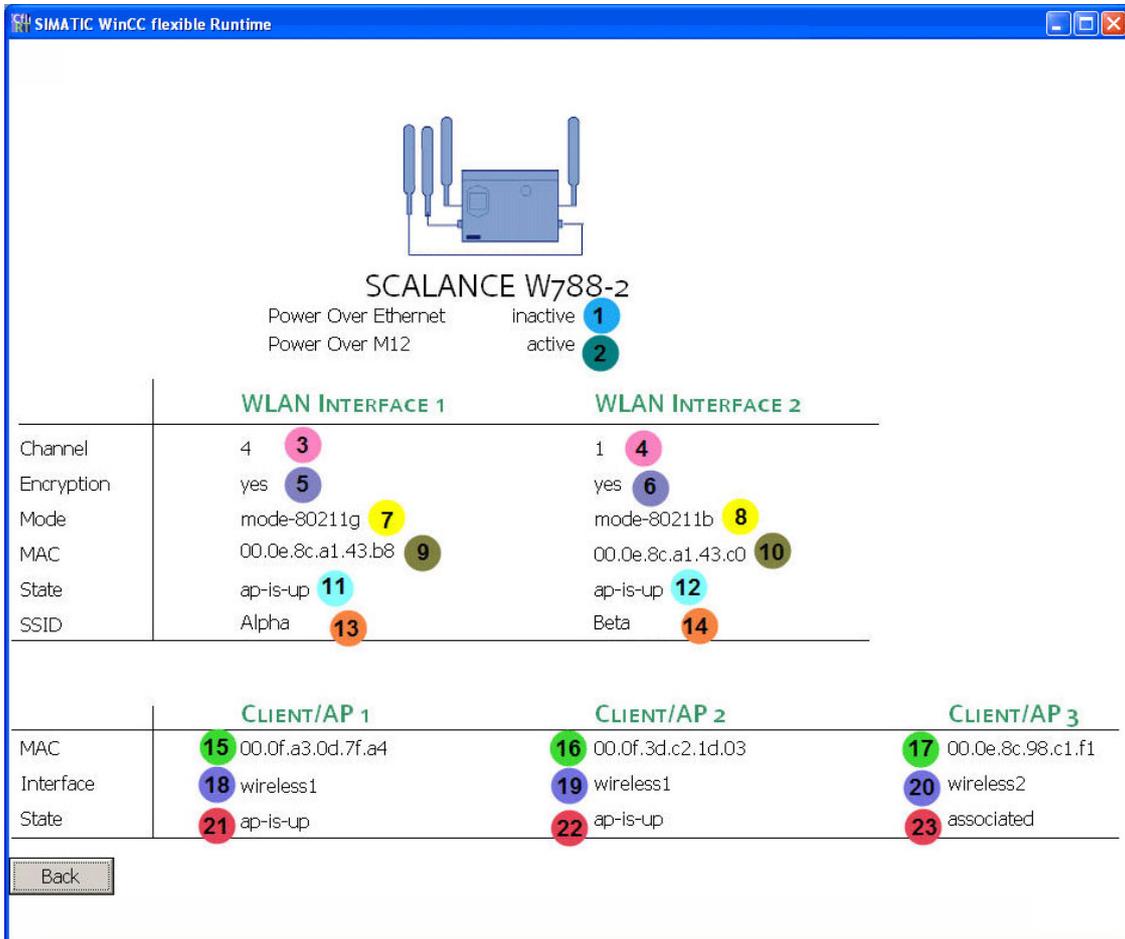
Table 3-11

No.	Name	Data type	OPC item ID
10.	CP343_State	Byte	SNMP:[CP343-1]&statepathval()
11.	W746_State	Byte	SNMP:[W746-1]&statepathval()
12.	Test_PC_State	Byte	SNMP:[Test_PC]&statepathval()
13.	W788-1_2_State	Byte	SNMP:[W788-1_2]&statepathval()
14.	W788-2_State	Byte	SNMP:[W788-2]&statepathval()
15.	W788-1_1_State	Byte	SNMP:[W788-1_1]&statepathval()
16.	SCALANCE X300_State	Byte	SNMP:[SCALANCE X308]&statepathval()
17.	SCALANCE X400_State	Byte	SNMP:[SCALANCE X414]&statepathval()
18.	Server_State	Byte	SNMP:[W788-2]&statepathval()

SCALANCE W information

The SNMP variables for displaying information are identical for all SCALANCE W modules. This is why not all four SCALANCE W WinCC flexible figures are explained here but the occurrence of the SNMP variables is illustrated using one figure instead.

Figure 3-22



Copyright © Siemens AG 2008 All rights reserved
30805917_SCALANCE_W_OFFICE_DOKU_v10_en.doc

These variables are used for the SCALANCE W information:

Table 3-12

No.	Name	Data type	OPC item ID
1.	PowerOverEthernet	Long	SNMP:[W788-2]snScalanceWPowerSupplyEthernetState
2.	PowerOverM12	Long	SNMP:[W788-2]snScalanceWPowerSupplyM12State
3.	Channel_WLAN1	Long	SNMP:[W788-2]snScalanceWStatsChannel.1
4.	Channel_WLAN2	Long	SNMP:[W788-2]snScalanceWStatsChannel.2
5.	Encrypt_WLAN1	Long	SNMP:[W788-2]snScalanceWStatsEncryption.1
6.	Encrypt_WLAN2	Long	SNMP:[W788-2]snScalanceWStatsEncryption.2
7.	Mode_WLAN1	Long	SNMP:[W788-2]snScalanceWStatsWlanMode.1
8.	Mode_WLAN2	Long	SNMP:[W788-2]snScalanceWStatsWlanMode.2
9.	MAC_WLAN1	String	SNMP:[W788-2]snScalanceWStatsMAC.1
10.	MAC_WLAN2	String	SNMP:[W788-2]snScalanceWStatsMAC.2

No.	Name	Data type	OPC item ID
11.	StateonWLAN1	Long	SNMP:[W788-2]snScalanceWStatsState.1
12.	StateonWLAN2	Long	SNMP:[W788-2]snScalanceWStatsState.2
13.	SSID_WLAN1	String	SNMP:[W788-2]snScalanceWStatsSSID.1
14.	SSID_WLAN2	String	SNMP:[W788-2]snScalanceWStatsSSID.2

The following variables are polled for the display of the status of the connected client/access point:

Table 3-13

No.	Name	Data type	OPC item ID
15.	MAC_Client1	String	SNMP:[W788-2]snScalanceWDevicesMAC.1
16.	MAC_Client2	String	SNMP:[W788-2]snScalanceWDevicesMAC.2
17.	MAC_Client3	String	SNMP:[W788-2]snScalanceWDevicesMAC.3
18.	Client1onInterface	Long	SNMP:[W788-2]snScalanceWDevicesInterface.1
19.	Client2onInterface	Long	SNMP:[W788-2]snScalanceWDevicesInterface.2
20.	Client3onInterface	Long	SNMP:[W788-2]snScalanceWDevicesInterface.3
21.	State_Client1	Long	SNMP:[W788-2]snScalanceWDevicesState.1
22.	State_Client2	Long	SNMP:[W788-2]snScalanceWDevicesState.2
23.	State_Client3	Long	SNMP:[W788-2]snScalanceWDevicesState.4

Setup, Configuration and Operation of the Application

4 Installation and commissioning

4.1 Installation of the hardware and software

This chapter describes which hardware and software components have to be installed. The descriptions and manuals as well as delivery information included in the delivery of the respective products should be observed in any case.

For the hardware components, please refer to chapter 2.4. Please follow the instructions listed in the table below to install the hardware components:

CAUTION Do not switch on the power supply until the last step has been completed!

Prepare the required connection cables.

Table 4-1

No.	Action	Comment
1.	Prepare five Ethernet cables from the specified accessories for the Ethernet connection cables.	Alternatively, you can also use pre-assembled Ethernet cables.

Installation of PC

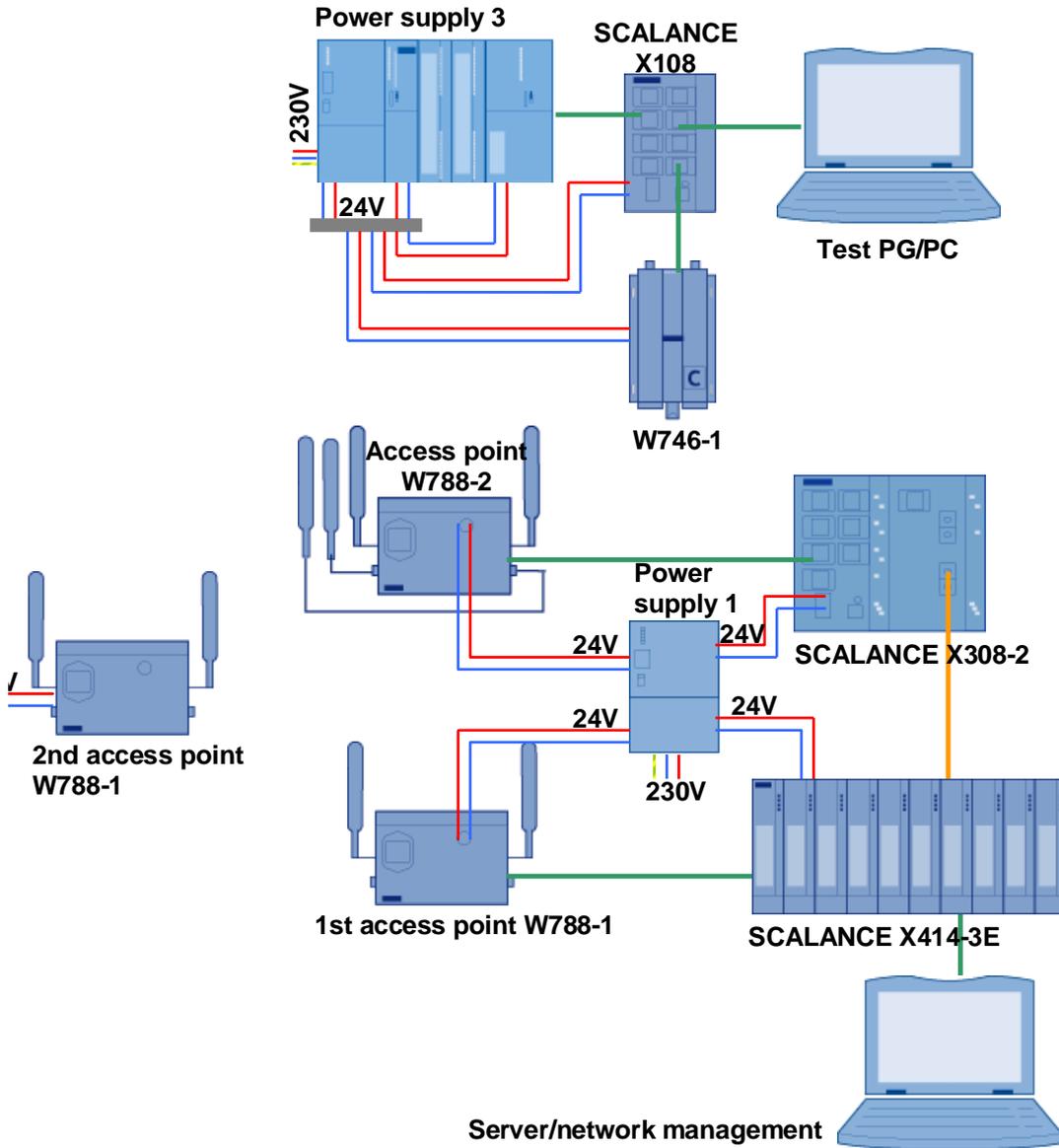
Table 4-2

No.	Action	Comment
1.	Install one Ethernet card respectively into the two PC/PGs.	When you are using a field PG, this card already exists.

Overview

The figure below shows the setup of the application:

Figure 4-1



Installation of the network

Table 4-3

No.	Action	Comment
1.	Connect the SCALANCE X308-2 and X414-3E, as well as the access points W788-2 and W788-1 to power supply 1.	
2.	Connect the second W788-1 to power supply 2.	
3.	Connect the S7-CPU to the CP343-1 Advanced via the backplane bus.	
4.	Connect the CPU, the CP, the SCALANCE X108 and the W746-1 WLAN client to power supply 3.	
5.	Supply a voltage of 230VAC for all power supplies.	
6.	Plug the MM492-2 media module into slot 5 of the SCALANCE X414-3E.	Slot 5 has a Gigabit port.
7.	Connect the server PC and the first access point W788-1 to the SCALANCE X414-3E using Ethernet cables.	Port 9.3: → server PC Port 9.4: → W788-1
8.	Connect the W788-2 to the SCALANCE X308-2 using an Ethernet cable.	W788-2 to port 6 of the SCALANCE X308-2
9.	Connect the SCALANCE X308-2 to the SCALANCE X414-3E using fiber-optic cable.	Port 10 of the X308-2 to port 5.1 on the X414-3E
10.	Connect the CP343-1 IT, one PC and the W746-1 to the SCALANCE X108 using Ethernet cables.	
11.	Connect an antenna to the second WLAN interface of the W788-2.	

Note The installation guidelines for all components must always be observed.

Installation of the standard software

Note The server PC is used for network management, engineering and as a server.

Install the following software on the server PC.

Table 4-4

No.	Action	Comment
1.	Install STEP 7 V5.4 SP3.	Follow the instructions of the installation program.
2.	Install SIMATIC NET Edition 2006.	Follow the instructions of the installation program.
3.	Install WinCC flexible 2007	Follow the instructions of the installation program.
4.	Transfer all required licenses.	

Installation of the freeware software

Install the following software packages on the server.

Table 4-5

No.	Action	Comment
1.	Install an FTP server software.	e.g., Jana Server
2.	Install a Syslog server software.	e.g., Kiwi Syslog Daemon by Kiwi Enterprises
3.	Install a network sniffer.	e.g., Wireshark

4.2 Installation of the application software

General preparations

Unzip the file **30805917_SCALANCE_W_OFFICE_v10.zip**.

This folder contains

- the archived STEP 7 project IWLAN.zip,
- the device profiles for the SCALANCE modules and
- a zip-file with standard MIBs.

Retrieve the STEP 7 project

Table 4-6

No.	Action	Comment
1.	Open the SIMATIC MANAGER and retrieve the STEP 7 project iwlan.zip .	Under File -> Retrieve

Reset the SCALANCE modules to the factory settings prior to configuration. This ensures that no other connections or settings are saved and the IP address of the SCALANCE modules is set to 0.0.0.0.

For instructions on resetting to the default values, please refer to the [SCALANCE X Manual](#) (BID: 19625108) or to the [SCALANCE W 78x Manual](#) (BID: 28529396).

4.2.1 Adjust the IP addresses

Overview of the IP addresses used

The following table gives you an overview of the components and the IP addresses to be assigned.

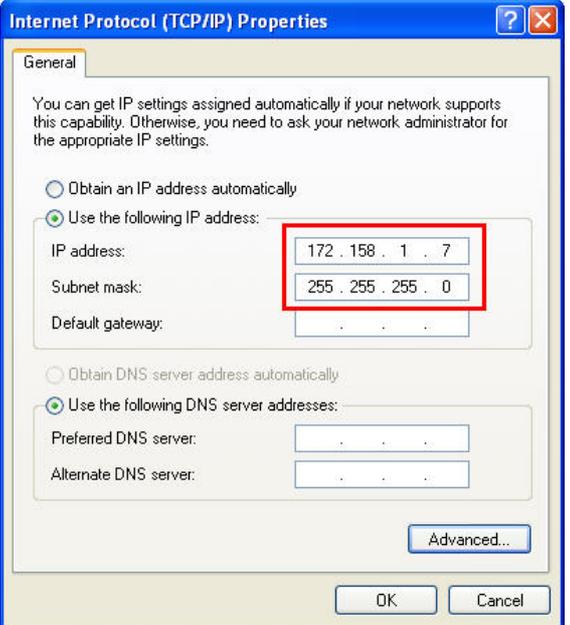
Table 4-7

Module	IP address	Device name
1.SCALANCE W788-1	172.158.1.1	W788-1-1
2.SCALANCE W788-1	172.158.1.2	W788-1-2
SCALANCE W788-2	172.158.1.3	W788-2
SCALANCE X414-3E	172.158.1.4	
SCALANCE X308-2	172.158.1.5	
Server/visualization	172.158.1.7	
SCALANCE W746-1 client	172.158.1.8	W746-1
Test PG/PC	172.158.1.9	
CP343-1 IT	172.158.1.10	

IP address of the visualization station/engineering PC

The server PC is used for engineering and visualization. The figure below shows the network setting to which you have to change the PG/PC:

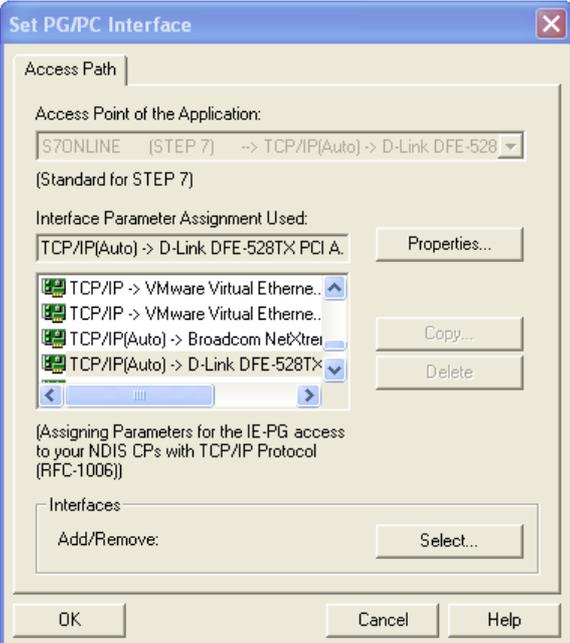
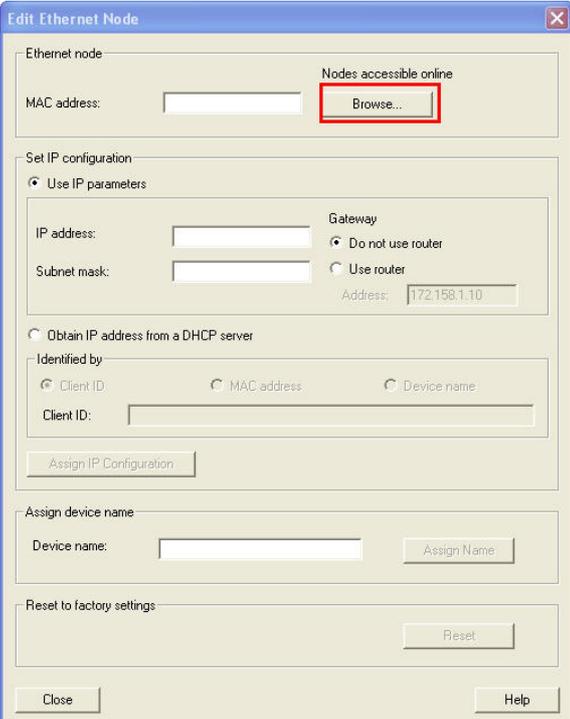
Table 4-8

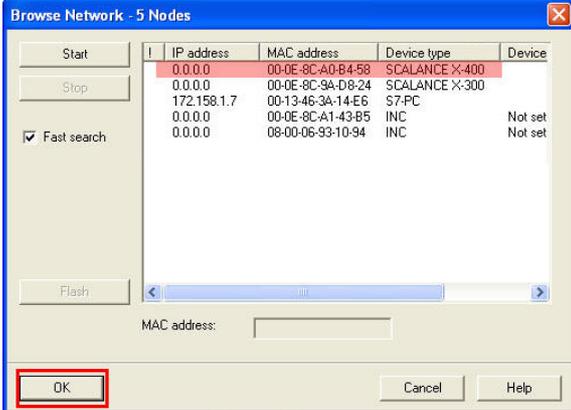
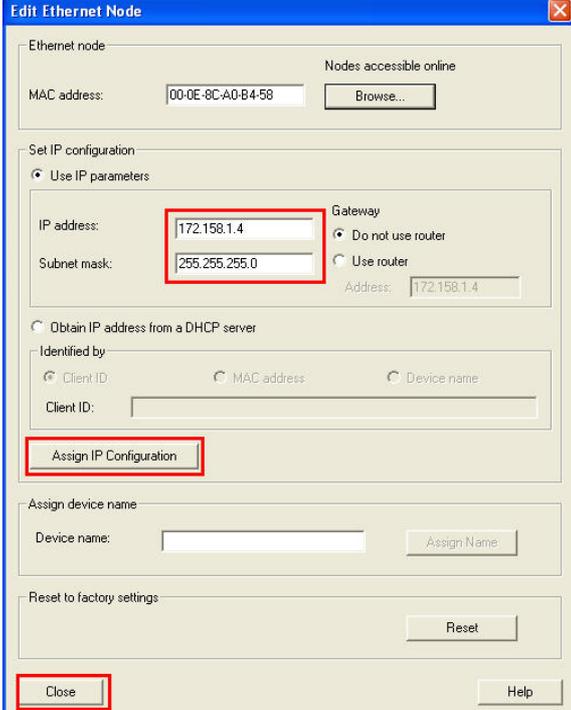
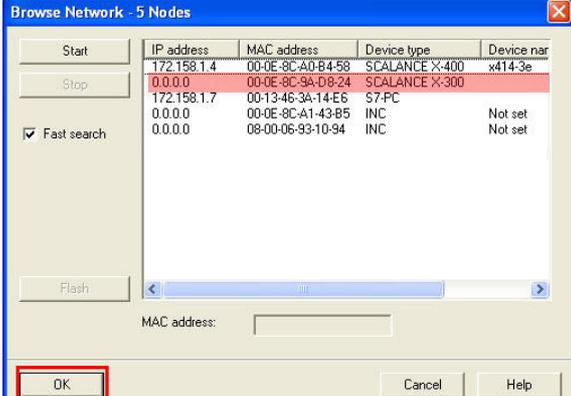
No.	Action	Comment
1.	<p>Open the Internet Protocol (TCP/IP) Properties via Start -> Settings -> Network Connection ->Local Connections.</p> <p>Select the option field Use following IP address and fill in the field as shown in the figure.</p> <p>Close the dialog boxes with "OK".</p>	

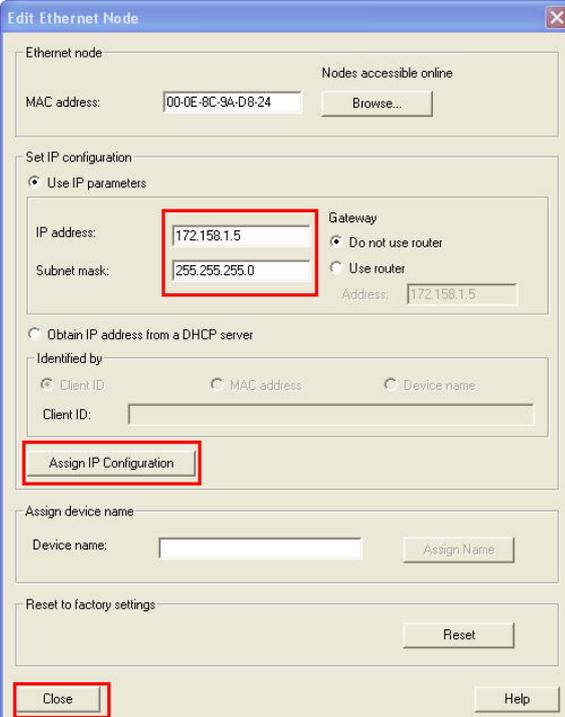
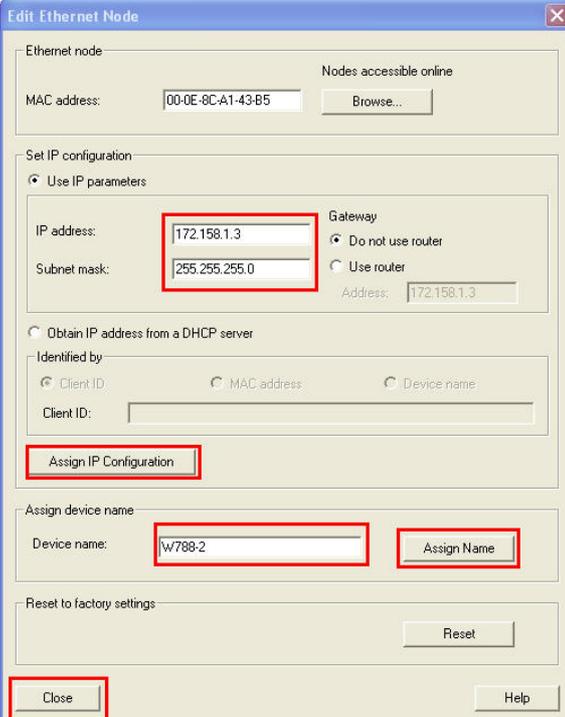
IP address of the SCALANCE X modules and access points

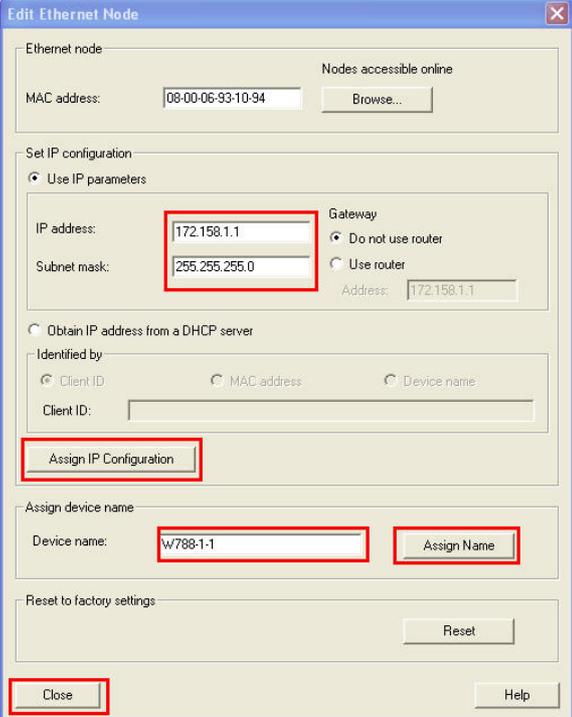
The network configuration of the SCALANCE modules can be performed using the SIMATIC MANAGER.

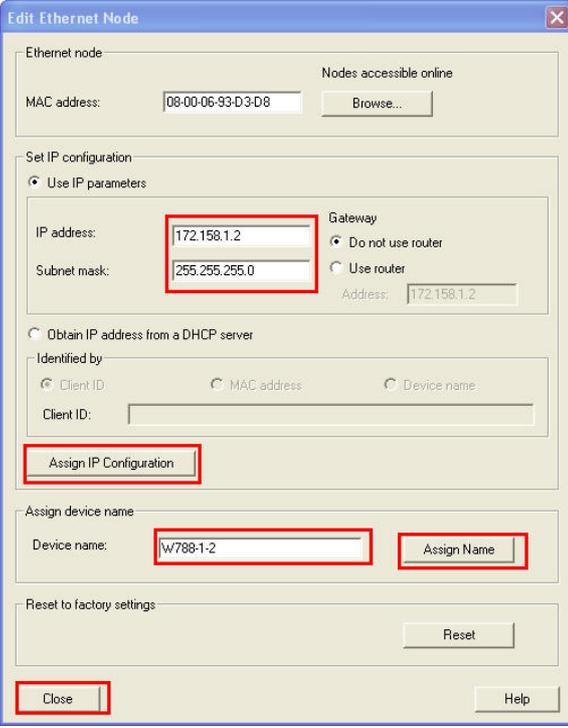
Table 4-9

No.	Action	Comment
1.	<p>Set the S7 ONLINE interface to the network card connected to the SCALANCE X308 in the SIMATIC MANAGER under Option -> Set PC/PG Interface... Click OK to close the dialog box.</p>	
2.	<p>Select the menu item PLC -> Edit Ethernet Node in the SIMATIC MANAGER. Click the Browse... button to start the search for further nodes.</p>	

No.	Action	Comment																								
3.	<p>A new dialog with nodes found in the network appears. The nodes are displayed with their IP address, MAC address and device name. Select the SCALANCE X400 and click OK.</p>	 <p>Browse Network - 5 Nodes</p> <table border="1"> <thead> <tr> <th>IP address</th> <th>MAC address</th> <th>Device type</th> <th>Device</th> </tr> </thead> <tbody> <tr> <td>0.0.0.0</td> <td>00-0E-8C-A0-B4-58</td> <td>SCALANCE X-400</td> <td></td> </tr> <tr> <td>0.0.0.0</td> <td>00-0E-8C-9A-D8-24</td> <td>SCALANCE X-300</td> <td></td> </tr> <tr> <td>172.158.1.7</td> <td>00-13-46-3A-14-E6</td> <td>S7-PC</td> <td></td> </tr> <tr> <td>0.0.0.0</td> <td>00-0E-8C-A1-43-B5</td> <td>INC</td> <td>Not set</td> </tr> <tr> <td>0.0.0.0</td> <td>08-00-06-93-10-94</td> <td>INC</td> <td>Not set</td> </tr> </tbody> </table> <p>Buttons: Start, Stop, Fast search (checked), Flash, MAC address: [], OK (highlighted), Cancel, Help.</p>	IP address	MAC address	Device type	Device	0.0.0.0	00-0E-8C-A0-B4-58	SCALANCE X-400		0.0.0.0	00-0E-8C-9A-D8-24	SCALANCE X-300		172.158.1.7	00-13-46-3A-14-E6	S7-PC		0.0.0.0	00-0E-8C-A1-43-B5	INC	Not set	0.0.0.0	08-00-06-93-10-94	INC	Not set
IP address	MAC address	Device type	Device																							
0.0.0.0	00-0E-8C-A0-B4-58	SCALANCE X-400																								
0.0.0.0	00-0E-8C-9A-D8-24	SCALANCE X-300																								
172.158.1.7	00-13-46-3A-14-E6	S7-PC																								
0.0.0.0	00-0E-8C-A1-43-B5	INC	Not set																							
0.0.0.0	08-00-06-93-10-94	INC	Not set																							
4.	<p>Enter the IP address as shown in Table 4-7 and the appropriate subnet mask. Click the Assign IP Configuration button to assign these settings to the device. Click Close to close the dialog box.</p>	 <p>Edit Ethernet Node</p> <p>Ethernet node: [] Nodes accessible online: [Browse...]</p> <p>MAC address: [00-0E-8C-A0-B4-58]</p> <p>Set IP configuration:</p> <ul style="list-style-type: none"> Use IP parameters (selected) <ul style="list-style-type: none"> IP address: [172.158.1.4] Gateway: [Do not use router] Subnet mask: [255.255.255.0] Address: [172.158.1.4] Obtain IP address from a DHCP server <p>Identified by:</p> <ul style="list-style-type: none"> Client ID (selected) MAC address Device name <p>Client ID: []</p> <p>Assign IP Configuration (highlighted)</p> <p>Assign device name:</p> <p>Device name: [] Assign Name</p> <p>Reset to factory settings:</p> <p>Reset</p> <p>Close (highlighted) Help</p>																								
5.	<p>Repeat step 2.</p> <p>The dialog box with the node found in the network opens again. The SCALANCE X414-3E is displayed with the address configured before. Now select the SCALANCE X308-2 and click OK.</p>	 <p>Browse Network - 5 Nodes</p> <table border="1"> <thead> <tr> <th>IP address</th> <th>MAC address</th> <th>Device type</th> <th>Device name</th> </tr> </thead> <tbody> <tr> <td>172.158.1.4</td> <td>00-0E-8C-A0-B4-58</td> <td>SCALANCE X-400</td> <td>x414-3e</td> </tr> <tr> <td>0.0.0.0</td> <td>00-0E-8C-9A-D8-24</td> <td>SCALANCE X-300</td> <td></td> </tr> <tr> <td>172.158.1.7</td> <td>00-13-46-3A-14-E6</td> <td>S7-PC</td> <td></td> </tr> <tr> <td>0.0.0.0</td> <td>00-0E-8C-A1-43-B5</td> <td>INC</td> <td>Not set</td> </tr> <tr> <td>0.0.0.0</td> <td>08-00-06-93-10-94</td> <td>INC</td> <td>Not set</td> </tr> </tbody> </table> <p>Buttons: Start, Stop, Fast search (checked), Flash, MAC address: [], OK (highlighted), Cancel, Help.</p>	IP address	MAC address	Device type	Device name	172.158.1.4	00-0E-8C-A0-B4-58	SCALANCE X-400	x414-3e	0.0.0.0	00-0E-8C-9A-D8-24	SCALANCE X-300		172.158.1.7	00-13-46-3A-14-E6	S7-PC		0.0.0.0	00-0E-8C-A1-43-B5	INC	Not set	0.0.0.0	08-00-06-93-10-94	INC	Not set
IP address	MAC address	Device type	Device name																							
172.158.1.4	00-0E-8C-A0-B4-58	SCALANCE X-400	x414-3e																							
0.0.0.0	00-0E-8C-9A-D8-24	SCALANCE X-300																								
172.158.1.7	00-13-46-3A-14-E6	S7-PC																								
0.0.0.0	00-0E-8C-A1-43-B5	INC	Not set																							
0.0.0.0	08-00-06-93-10-94	INC	Not set																							

No.	Action	Comment
6.	<p>Enter the IP address as shown in Table 4-7 and the appropriate subnet mask. Click the Assign IP Configuration button to assign these settings to the device.</p> <p>Click Close to close the dialog box.</p>	
7.	<p>Perform steps 2 to 3 for the SCALANCE W788-2.</p> <p>The SCALANCE W modules with the device name INC are displayed under item 3. Compare the MAC address displayed to that printed on the SCALANCE module housing in order to distinguish between the components.</p> <p>Enter the IP address as shown in Table 4-7 and the appropriate subnet mask. Click the Assign IP Configuration button to assign these settings to the device.</p> <p>Assign a device name to the SCALANCE as shown in Table 4-7 and load it to the device using the Assign Name button.</p> <p>Click Close to close the dialog box.</p>	

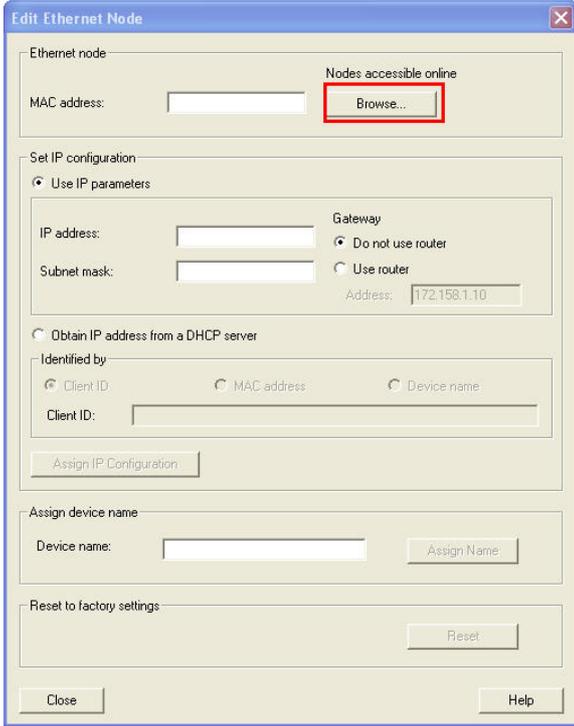
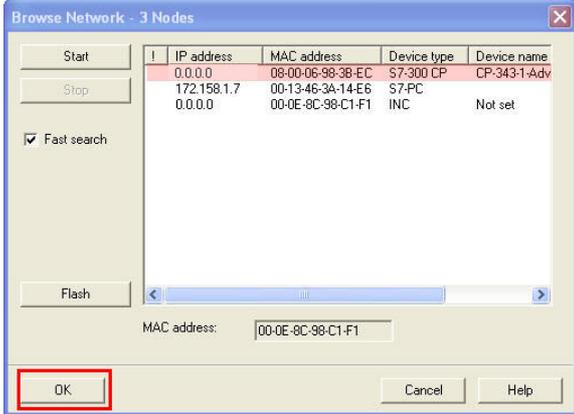
No.	Action	Comment
8.	<p>Perform steps 2 to 3 for the first SCALANCE W788-1.</p> <p>The SCALANCE W modules with the device name INC are displayed under item 3. Compare the MAC address displayed to that printed on the SCALANCE module housing in order to distinguish between the components.</p> <p>Enter the IP address as shown in Table 4-7 and the appropriate subnet mask. Click the Assign IP Configuration button to assign these settings to the device.</p> <p>Assign a device name to the SCALANCE as shown in Table 4-7 and load it to the device using the Assign Name button.</p> <p>Click Close to close the dialog box.</p>	
9.	<p>The second SCALANCE W788-1 has no Ethernet connection to the other nodes and is thus not displayed in the dialog box.</p> <p>Connect the server PC directly to the Ethernet interface of the second SCALANCE W788-1.</p>	

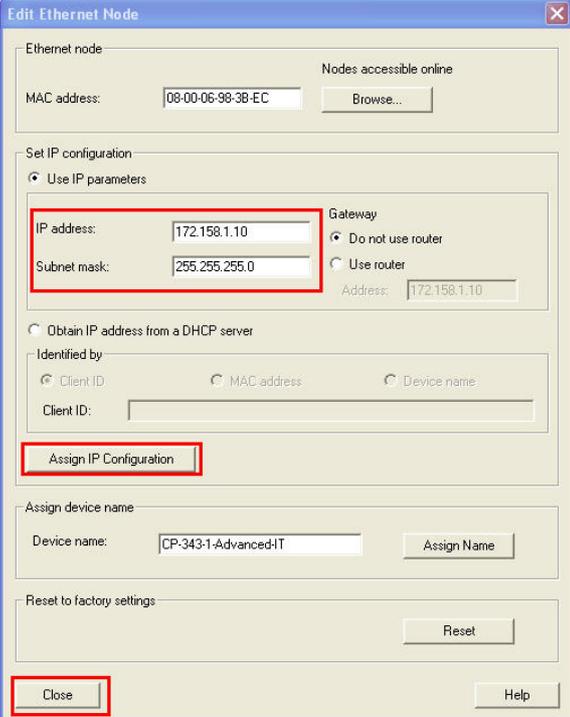
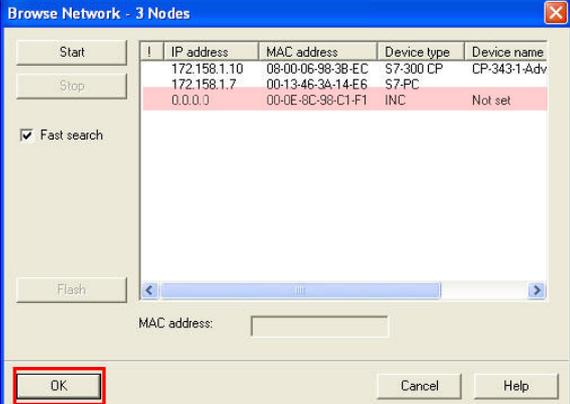
No.	Action	Comment
10.	<p>Perform steps 2 to 3 for the second SCALANCE W788-1.</p> <p>The SCALANCE W modules with the device name INC are displayed under item 3. Compare the MAC address displayed to that printed on the SCALANCE module housing in order to distinguish between the components.</p> <p>Enter the IP address as shown in Table 4-7 and the appropriate subnet mask. Click the Assign IP Configuration button to assign these settings to the device.</p> <p>Assign a device name to the SCALANCE as shown in Table 4-7 and load it to the device using the Assign Name button.</p> <p>Close the dialog box with Close. Once the IP address has been transferred, reconnect the server PC to the SCALANCE X414-3E.</p>	 <p>The screenshot shows the 'Edit Ethernet Node' dialog box with the following configuration details:</p> <ul style="list-style-type: none"> Ethernet node: MAC address: 08-00-06-93-D3-D8 Set IP configuration: <ul style="list-style-type: none"> <input checked="" type="radio"/> Use IP parameters: <ul style="list-style-type: none"> IP address: 172.158.1.2 Subnet mask: 255.255.255.0 Gateway: <input checked="" type="radio"/> Do not use router <input type="radio"/> Use router: Address: 172.158.1.2 <input type="radio"/> Obtain IP address from a DHCP server Identified by: <ul style="list-style-type: none"> <input checked="" type="radio"/> Client ID: [Empty field] <input type="radio"/> MAC address <input type="radio"/> Device name Buttons: Assign IP Configuration, Assign Name, Close, Help, Reset

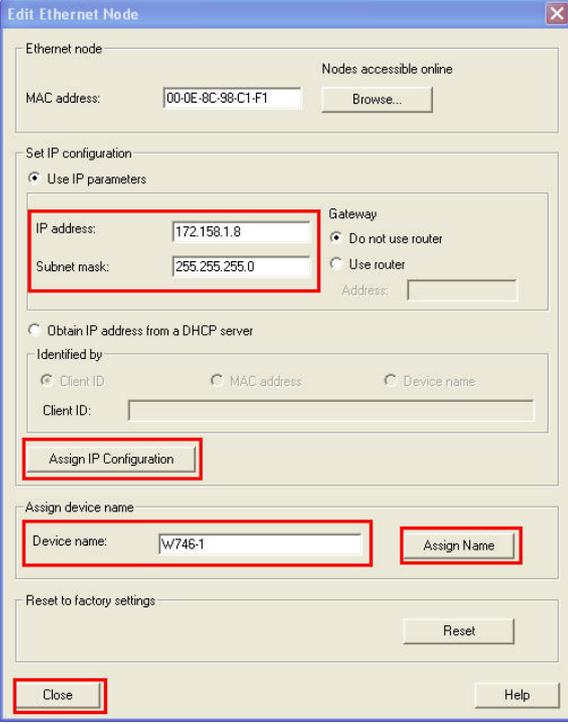
IP address of the W746-1 and CP343-1 IT WLAN clients

The network configuration of the module can be done using the SIMATIC MANAGER.

Table 4-10

No.	Action	Comment																				
1.	Connect the server PC to the SCALANCE X108.																					
2.	Select the menu item PLC -> Edit Ethernet Node in the SIMATIC MANAGER . Click the Browse... button to start the search for further nodes.																					
3.	A new dialog with nodes found in the network appears. The nodes are displayed with their IP address, MAC address and device name. Select the CP343-1 IT and click OK .	 <table border="1" data-bbox="933 1435 1348 1512"> <thead> <tr> <th>I</th> <th>IP address</th> <th>MAC address</th> <th>Device type</th> <th>Device name</th> </tr> </thead> <tbody> <tr> <td></td> <td>0.0.0.0</td> <td>08-00-06-98-38-EC</td> <td>S7-300 CP</td> <td>CP-343-1-Adv</td> </tr> <tr> <td></td> <td>172.158.1.7</td> <td>00-13-46-3A-14-E6</td> <td>S7-PC</td> <td></td> </tr> <tr> <td></td> <td>0.0.0.0</td> <td>00-0E-8C-98-C1-F1</td> <td>INC</td> <td>Not set</td> </tr> </tbody> </table>	I	IP address	MAC address	Device type	Device name		0.0.0.0	08-00-06-98-38-EC	S7-300 CP	CP-343-1-Adv		172.158.1.7	00-13-46-3A-14-E6	S7-PC			0.0.0.0	00-0E-8C-98-C1-F1	INC	Not set
I	IP address	MAC address	Device type	Device name																		
	0.0.0.0	08-00-06-98-38-EC	S7-300 CP	CP-343-1-Adv																		
	172.158.1.7	00-13-46-3A-14-E6	S7-PC																			
	0.0.0.0	00-0E-8C-98-C1-F1	INC	Not set																		

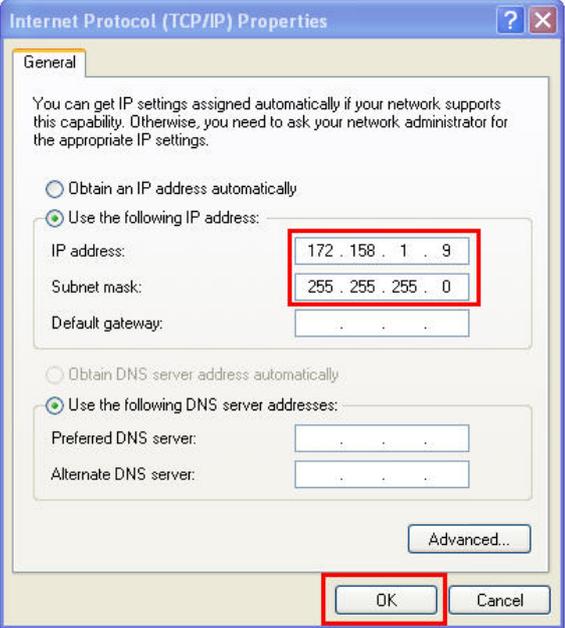
No.	Action	Comment																				
4.	<p>Enter the IP address as shown in Table 4-7 and the appropriate subnet mask. Click the Assign IP Configuration button to assign these settings to the device. Click Close to close the dialog box.</p>																					
5.	<p>Repeat step 2. The dialog box with the node found in the network opens again. The CP343-1 IT is displayed with the address configured before. Now select the SCALANCE W746-1 and click OK.</p>	 <table border="1" data-bbox="933 1176 1348 1265"> <thead> <tr> <th></th> <th>IP address</th> <th>MAC address</th> <th>Device type</th> <th>Device name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>172.158.1.10</td> <td>08-00-06-98-38-EC</td> <td>S7-300 CP</td> <td>CP-343-1-Adv</td> </tr> <tr> <td></td> <td>172.158.1.7</td> <td>00-13-46-3A-14-E6</td> <td>S7-PC</td> <td></td> </tr> <tr> <td></td> <td>0.0.0.0</td> <td>00-0E-8C-98-C1-F1</td> <td>INC</td> <td>Not set</td> </tr> </tbody> </table>		IP address	MAC address	Device type	Device name	1	172.158.1.10	08-00-06-98-38-EC	S7-300 CP	CP-343-1-Adv		172.158.1.7	00-13-46-3A-14-E6	S7-PC			0.0.0.0	00-0E-8C-98-C1-F1	INC	Not set
	IP address	MAC address	Device type	Device name																		
1	172.158.1.10	08-00-06-98-38-EC	S7-300 CP	CP-343-1-Adv																		
	172.158.1.7	00-13-46-3A-14-E6	S7-PC																			
	0.0.0.0	00-0E-8C-98-C1-F1	INC	Not set																		

No.	Action	Comment
6.	<p>Enter the IP address as shown in Table 4-7 and the appropriate subnet mask. Click the Assign IP Configuration button to assign these settings to the device. Enter the device name into the respective field as shown in table Table 4-7 and assign it to the device using the Assign Name button. Close the dialog box with OK.</p>	 <p>The screenshot shows the 'Edit Ethernet Node' dialog box. It has several sections: 'Ethernet node' with a MAC address field (00-0E-9C-98-C1-F1) and a 'Browse...' button; 'Set IP configuration' with radio buttons for 'Use IP parameters' (selected) and 'Obtain IP address from a DHCP server'. Under 'Use IP parameters', there are fields for 'IP address' (172.158.1.8) and 'Subnet mask' (255.255.255.0), and a 'Gateway' section with 'Do not use router' selected and 'Use router' as an option. Below that is an 'Identified by' section with radio buttons for 'Client ID', 'MAC address', and 'Device name', and a 'Client ID' field. At the bottom, there are 'Assign IP Configuration', 'Assign device name' (with 'Device name' field containing 'w746-1' and an 'Assign Name' button), and 'Reset to factory settings' (with a 'Reset' button). 'Close' and 'Help' buttons are at the very bottom.</p>
7.	<p>Reconnect the server PC to port 9.3 of the SCALANCE X414-3E.</p>	

IP address of the test PG/PC

The figure below shows the network setting to which you have to change the PG/PC:

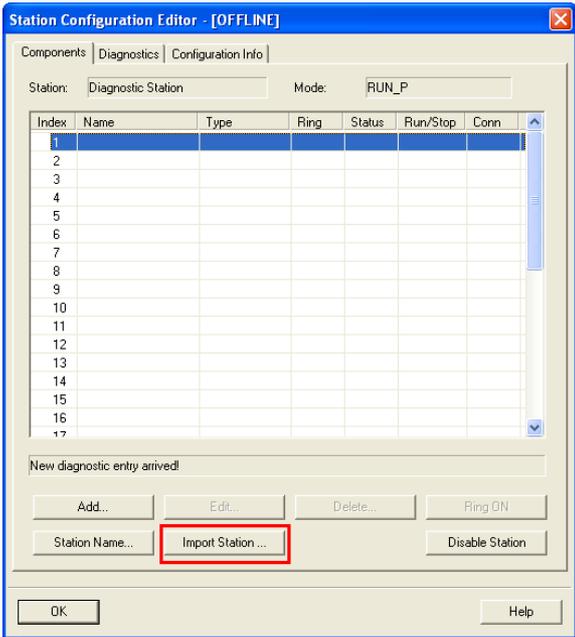
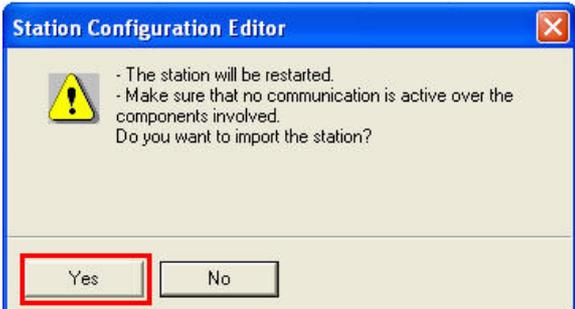
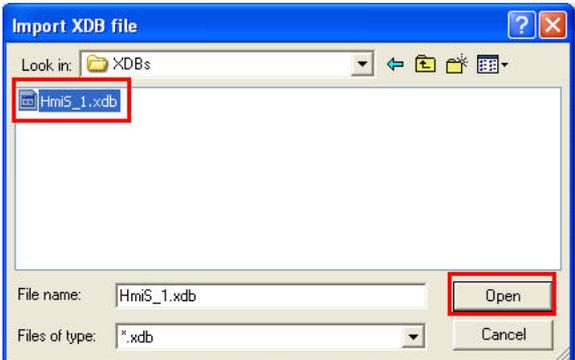
Table 4-11

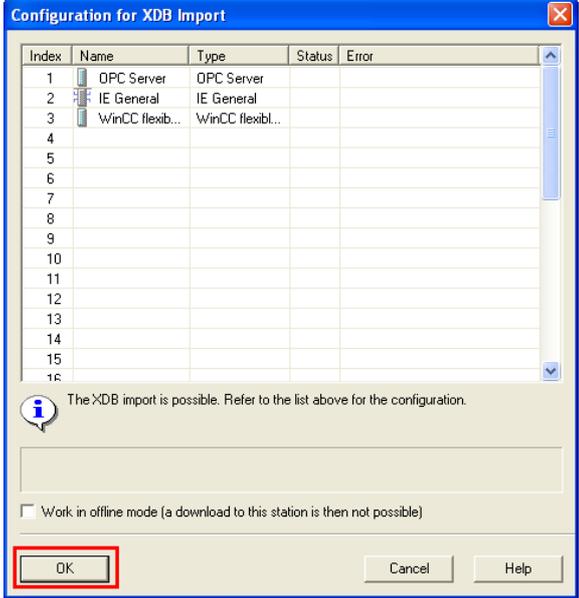
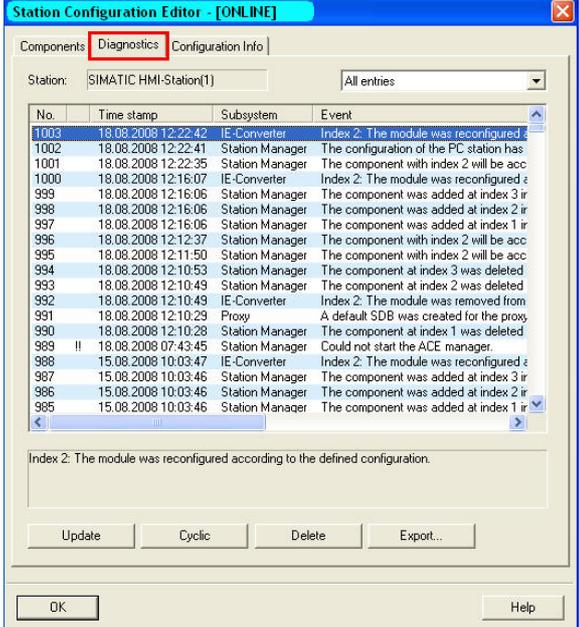
No.	Action	Comment
1.	<p>Open the Internet Protocol (TCP/IP) Properties using Start -> Settings -> Network Connection ->Local Connections.</p> <p>Select the option field Use following IP address and fill in the field as shown in the figure.</p> <p>Close the dialog box with OK.</p>	

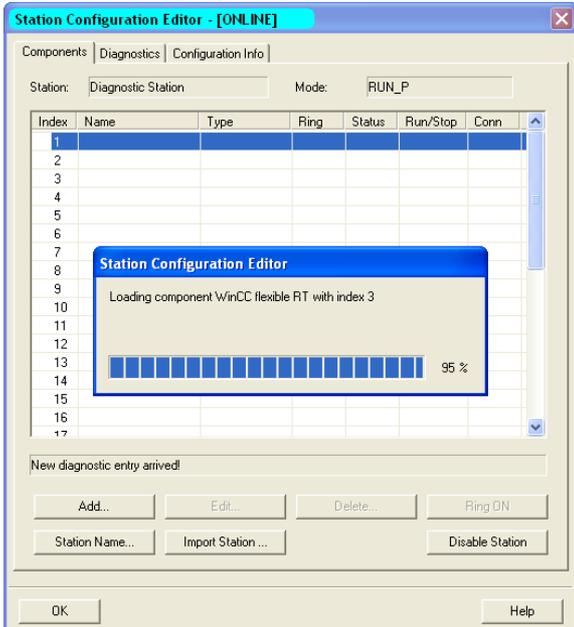
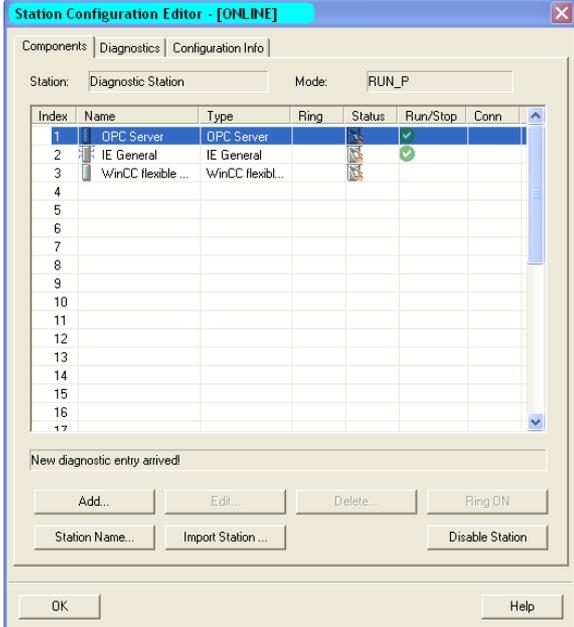
4.2.2 Configuration of the Station Configurator

The Station Configurator is configured on the server PC.

Table 4-12

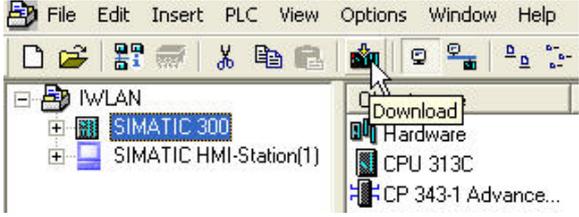
No.	Action	Comment
1.	<p>Open the Station Configurator by selecting start -> Station Configurator or by double-clicking the icon in the taskbar. Press the Import Station... button.</p>	 <p>The screenshot shows the 'Station Configuration Editor - [OFFLINE]' window. It has tabs for 'Components', 'Diagnostics', and 'Configuration Info'. The 'Station' field is set to 'Diagnostic Station' and the 'Mode' is 'RUN_P'. Below this is a table with columns: Index, Name, Type, Ring, Status, Run/Stop, and Conn. The 'Index' column contains numbers from 1 to 17. At the bottom, there are buttons for 'Add...', 'Edit...', 'Delete...', 'Ring ON', 'Station Name...', 'Import Station...', and 'Disable Station'. The 'Import Station...' button is highlighted with a red box.</p>
2.	<p>Confirm the restart of the node with Yes.</p>	 <p>The screenshot shows a warning dialog box titled 'Station Configuration Editor'. It contains a yellow warning triangle icon and the following text: '- The station will be restarted. - Make sure that no communication is active over the components involved. Do you want to import the station?'. At the bottom, there are 'Yes' and 'No' buttons. The 'Yes' button is highlighted with a red box.</p>
3.	<p>Navigate to the directory of the STEP 7 project and open the XDBs folder. Open the HmiS_1.xdb file and click Open to import the station.</p>	 <p>The screenshot shows the 'Import XDB file' dialog box. The 'Look in:' field shows the 'XDBs' folder. The file list contains 'HmiS_1.xdb', which is highlighted with a red box. At the bottom, there is a 'File name:' field containing 'HmiS_1.xdb' and an 'Open' button, which is also highlighted with a red box. There is also a 'Files of type:' dropdown set to '*.xdb' and a 'Cancel' button.</p>

No.	Action	Comment																																																																																					
4.	<p>The following dialog indicates whether the XDB file can be imported.</p> <p>If no error is displayed, confirm with the OK button.</p>	 <p>Configuration for XDB Import</p> <table border="1"> <thead> <tr> <th>Index</th> <th>Name</th> <th>Type</th> <th>Status</th> <th>Error</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>OPC Server</td> <td>OPC Server</td> <td></td> <td></td> </tr> <tr> <td>2</td> <td>IE General</td> <td>IE General</td> <td></td> <td></td> </tr> <tr> <td>3</td> <td>WinCC flexibl...</td> <td>WinCC flexibl...</td> <td></td> <td></td> </tr> <tr><td>4</td><td></td><td></td><td></td><td></td></tr> <tr><td>5</td><td></td><td></td><td></td><td></td></tr> <tr><td>6</td><td></td><td></td><td></td><td></td></tr> <tr><td>7</td><td></td><td></td><td></td><td></td></tr> <tr><td>8</td><td></td><td></td><td></td><td></td></tr> <tr><td>9</td><td></td><td></td><td></td><td></td></tr> <tr><td>10</td><td></td><td></td><td></td><td></td></tr> <tr><td>11</td><td></td><td></td><td></td><td></td></tr> <tr><td>12</td><td></td><td></td><td></td><td></td></tr> <tr><td>13</td><td></td><td></td><td></td><td></td></tr> <tr><td>14</td><td></td><td></td><td></td><td></td></tr> <tr><td>15</td><td></td><td></td><td></td><td></td></tr> <tr><td>16</td><td></td><td></td><td></td><td></td></tr> </tbody> </table> <p>The XDB import is possible. Refer to the list above for the configuration.</p> <p><input type="checkbox"/> Work in offline mode (a download to this station is then not possible)</p> <p>OK Cancel Help</p>	Index	Name	Type	Status	Error	1	OPC Server	OPC Server			2	IE General	IE General			3	WinCC flexibl...	WinCC flexibl...			4					5					6					7					8					9					10					11					12					13					14					15					16				
Index	Name	Type	Status	Error																																																																																			
1	OPC Server	OPC Server																																																																																					
2	IE General	IE General																																																																																					
3	WinCC flexibl...	WinCC flexibl...																																																																																					
4																																																																																							
5																																																																																							
6																																																																																							
7																																																																																							
8																																																																																							
9																																																																																							
10																																																																																							
11																																																																																							
12																																																																																							
13																																																																																							
14																																																																																							
15																																																																																							
16																																																																																							
5.	<p>If the XDB import is not possible, this may be remedied by restarting the computer. Diagnostic entries of the Station Configurator are displayed in the Diagnostic tab.</p>	 <p>Station Configuration Editor - [ONLINE]</p> <p>Components: Diagnostics Configuration Info</p> <p>Station: SIMATIC HMI-Station(1) All entries</p> <table border="1"> <thead> <tr> <th>No.</th> <th>Time stamp</th> <th>Subsystem</th> <th>Event</th> </tr> </thead> <tbody> <tr> <td>1003</td> <td>18.08.2008 12:22:42</td> <td>IE-Converter</td> <td>Index 2: The module was reconfigured.</td> </tr> <tr> <td>1002</td> <td>18.08.2008 12:22:41</td> <td>Station Manager</td> <td>The configuration of the PC station has</td> </tr> <tr> <td>1001</td> <td>18.08.2008 12:22:35</td> <td>Station Manager</td> <td>The component with index 2 will be acc</td> </tr> <tr> <td>1000</td> <td>18.08.2008 12:16:07</td> <td>IE-Converter</td> <td>Index 2: The module was reconfigured &</td> </tr> <tr> <td>999</td> <td>18.08.2008 12:16:06</td> <td>Station Manager</td> <td>The component was added at index 3 ir</td> </tr> <tr> <td>998</td> <td>18.08.2008 12:16:06</td> <td>Station Manager</td> <td>The component was added at index 2 ir</td> </tr> <tr> <td>997</td> <td>18.08.2008 12:16:06</td> <td>Station Manager</td> <td>The component was added at index 1 ir</td> </tr> <tr> <td>996</td> <td>18.08.2008 12:12:37</td> <td>Station Manager</td> <td>The component with index 2 will be acc</td> </tr> <tr> <td>995</td> <td>18.08.2008 12:11:50</td> <td>Station Manager</td> <td>The component with index 2 will be acc</td> </tr> <tr> <td>994</td> <td>18.08.2008 12:10:53</td> <td>Station Manager</td> <td>The component at index 3 was deleted</td> </tr> <tr> <td>993</td> <td>18.08.2008 12:10:49</td> <td>Station Manager</td> <td>The component at index 2 was deleted</td> </tr> <tr> <td>992</td> <td>18.08.2008 12:10:49</td> <td>IE-Converter</td> <td>Index 2: The module was removed from</td> </tr> <tr> <td>991</td> <td>18.08.2008 12:10:29</td> <td>Proxy</td> <td>A default SDB was created for the proxy</td> </tr> <tr> <td>990</td> <td>18.08.2008 12:10:28</td> <td>Station Manager</td> <td>The component at index 1 was deleted</td> </tr> <tr> <td>989</td> <td>18.08.2008 07:43:45</td> <td>Station Manager</td> <td>Could not start the ACE manager.</td> </tr> <tr> <td>988</td> <td>15.08.2008 10:03:47</td> <td>IE-Converter</td> <td>Index 2: The module was reconfigured &</td> </tr> <tr> <td>987</td> <td>15.08.2008 10:03:46</td> <td>Station Manager</td> <td>The component was added at index 3 ir</td> </tr> <tr> <td>986</td> <td>15.08.2008 10:03:46</td> <td>Station Manager</td> <td>The component was added at index 2 ir</td> </tr> <tr> <td>985</td> <td>15.08.2008 10:03:46</td> <td>Station Manager</td> <td>The component was added at index 1 ir</td> </tr> </tbody> </table> <p>Index 2: The module was reconfigured according to the defined configuration.</p> <p>Update Cyclic Delete Export...</p> <p>OK Help</p>	No.	Time stamp	Subsystem	Event	1003	18.08.2008 12:22:42	IE-Converter	Index 2: The module was reconfigured.	1002	18.08.2008 12:22:41	Station Manager	The configuration of the PC station has	1001	18.08.2008 12:22:35	Station Manager	The component with index 2 will be acc	1000	18.08.2008 12:16:07	IE-Converter	Index 2: The module was reconfigured &	999	18.08.2008 12:16:06	Station Manager	The component was added at index 3 ir	998	18.08.2008 12:16:06	Station Manager	The component was added at index 2 ir	997	18.08.2008 12:16:06	Station Manager	The component was added at index 1 ir	996	18.08.2008 12:12:37	Station Manager	The component with index 2 will be acc	995	18.08.2008 12:11:50	Station Manager	The component with index 2 will be acc	994	18.08.2008 12:10:53	Station Manager	The component at index 3 was deleted	993	18.08.2008 12:10:49	Station Manager	The component at index 2 was deleted	992	18.08.2008 12:10:49	IE-Converter	Index 2: The module was removed from	991	18.08.2008 12:10:29	Proxy	A default SDB was created for the proxy	990	18.08.2008 12:10:28	Station Manager	The component at index 1 was deleted	989	18.08.2008 07:43:45	Station Manager	Could not start the ACE manager.	988	15.08.2008 10:03:47	IE-Converter	Index 2: The module was reconfigured &	987	15.08.2008 10:03:46	Station Manager	The component was added at index 3 ir	986	15.08.2008 10:03:46	Station Manager	The component was added at index 2 ir	985	15.08.2008 10:03:46	Station Manager	The component was added at index 1 ir					
No.	Time stamp	Subsystem	Event																																																																																				
1003	18.08.2008 12:22:42	IE-Converter	Index 2: The module was reconfigured.																																																																																				
1002	18.08.2008 12:22:41	Station Manager	The configuration of the PC station has																																																																																				
1001	18.08.2008 12:22:35	Station Manager	The component with index 2 will be acc																																																																																				
1000	18.08.2008 12:16:07	IE-Converter	Index 2: The module was reconfigured &																																																																																				
999	18.08.2008 12:16:06	Station Manager	The component was added at index 3 ir																																																																																				
998	18.08.2008 12:16:06	Station Manager	The component was added at index 2 ir																																																																																				
997	18.08.2008 12:16:06	Station Manager	The component was added at index 1 ir																																																																																				
996	18.08.2008 12:12:37	Station Manager	The component with index 2 will be acc																																																																																				
995	18.08.2008 12:11:50	Station Manager	The component with index 2 will be acc																																																																																				
994	18.08.2008 12:10:53	Station Manager	The component at index 3 was deleted																																																																																				
993	18.08.2008 12:10:49	Station Manager	The component at index 2 was deleted																																																																																				
992	18.08.2008 12:10:49	IE-Converter	Index 2: The module was removed from																																																																																				
991	18.08.2008 12:10:29	Proxy	A default SDB was created for the proxy																																																																																				
990	18.08.2008 12:10:28	Station Manager	The component at index 1 was deleted																																																																																				
989	18.08.2008 07:43:45	Station Manager	Could not start the ACE manager.																																																																																				
988	15.08.2008 10:03:47	IE-Converter	Index 2: The module was reconfigured &																																																																																				
987	15.08.2008 10:03:46	Station Manager	The component was added at index 3 ir																																																																																				
986	15.08.2008 10:03:46	Station Manager	The component was added at index 2 ir																																																																																				
985	15.08.2008 10:03:46	Station Manager	The component was added at index 1 ir																																																																																				

No.	Action	Comment																												
6.	The PC station is configured using the data from the XDB file.	 <p>The screenshot shows the 'Station Configuration Editor - [ONLINE]' dialog box. It has tabs for 'Components', 'Diagnostics', and 'Configuration Info'. The 'Station' is set to 'Diagnostic Station' and the 'Mode' is 'RUN_P'. A table lists components with columns for Index, Name, Type, Ring, Status, Run/Stop, and Conn. A smaller dialog box is overlaid on top, titled 'Station Configuration Editor', with the message 'Loading component WinCC flexible RT with index 3' and a progress bar at 95%. At the bottom, there are buttons for 'Add...', 'Edit...', 'Delete...', 'Ring ON', 'Station Name...', 'Import Station ...', 'Disable Station', 'OK', and 'Help'.</p>																												
7.	<p>The configuration of the PC station is now complete.</p> <p>OPC Server and IE-General must be in the "Run" mode without errors.</p> <p>Close the dialog box with OK.</p>	 <p>The screenshot shows the 'Station Configuration Editor - [ONLINE]' dialog box with the same settings as above. The table now contains three rows: <table border="1" data-bbox="813 1142 1340 1478"> <thead> <tr> <th>Index</th> <th>Name</th> <th>Type</th> <th>Ring</th> <th>Status</th> <th>Run/Stop</th> <th>Conn</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>OPC Server</td> <td>OPC Server</td> <td></td> <td></td> <td>✓</td> <td></td> </tr> <tr> <td>2</td> <td>IE General</td> <td>IE General</td> <td></td> <td></td> <td>✓</td> <td></td> </tr> <tr> <td>3</td> <td>WinCC flexible ...</td> <td>WinCC flexibl...</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> The 'Run/Stop' column for the first two rows shows a green checkmark, indicating they are in the 'Run' mode. The 'OK' button is highlighted at the bottom. </p>	Index	Name	Type	Ring	Status	Run/Stop	Conn	1	OPC Server	OPC Server			✓		2	IE General	IE General			✓		3	WinCC flexible ...	WinCC flexibl...				
Index	Name	Type	Ring	Status	Run/Stop	Conn																								
1	OPC Server	OPC Server			✓																									
2	IE General	IE General			✓																									
3	WinCC flexible ...	WinCC flexibl...																												

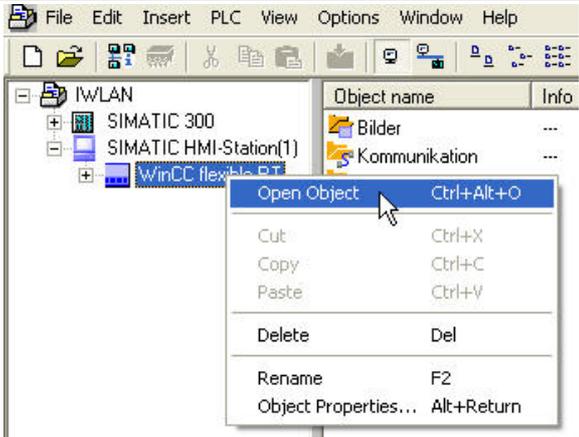
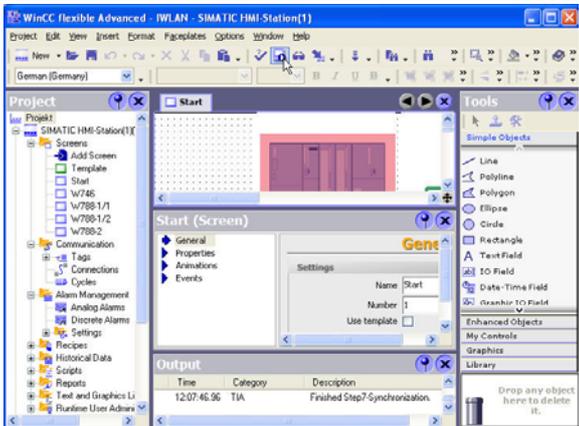
4.2.3 Load STEP 7 project

Table 4-13

No.	Action	Comment
1.	Connect the server PC to the SCALANCE X108.	
2.	Select the STEP 7 project and load it to the CPU 313C via Ethernet.	
3.	Reconnect the server PC to port 9.3 of the SCALANCE X414-3E.	

4.2.4 Start WinCC flexible Runtime

Table 4-14

No.	Action	Comment
1.	Open the SIMATIC MANAGER and the IWLAN path. Select WinCC flexible RT and open the WinCC flexible by clicking the right mouse button -> Open . WinCC flexible is opened.	
2.	Start the WinCC Runtime via Project -> Compiler -> Start Runtime or by pressing the respective icon in the toolbar.	

Note

The SCALANCE modules are not fully configured yet. This is why most of the modules are displayed red in the WINCC flexible.

Preparation in STEP 7

To be able to configure the SNMP OPC server, create an HMI station in the SIMATIC Manager, select the **WinCC flexible RT** device type and activate **S7RTM** in the **Configuration** tab of the HMI station properties.

In the hardware configuration of the HMI Station you add the network card used by you.

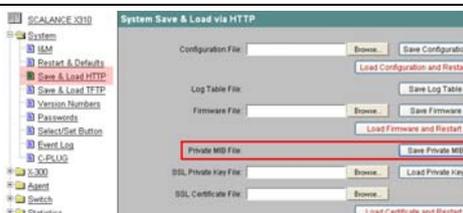
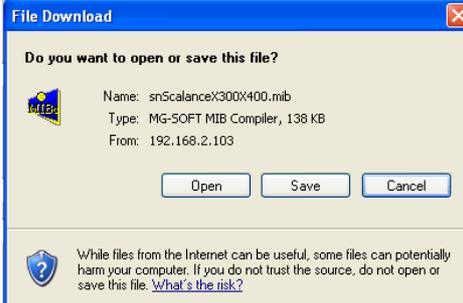
Private MIB of the SCALANCE-X300/-400 and W

To be able to use all the SNMP information provided by the SCALANCE X modules, you also need the **private MIB**.

The private MIB is equal for the SCALANCE X308-2 and X414-3E, the same applies to the SCALANCE W modules. It is thus sufficient to load only one private MIB of the SCALANCE X and W with one of the following options:

- **Web-based management (as of FW V2.3):** SCALANCE modules of the X300 series from V2.3 have a button for downloading the private MIB in the web-based management.

Table 5-1

No.	Action	Comment
1.	Open the web-based management of the SCALANCE X308-2.	http://172.158.1.5
2.	Go to the menu item system-> Save&Load http . You can load the private MIB using the Save Private MIB button.	
3.	Navigate to the directory in which you wish to save the MIB.	

- **Service&Support Portal:** [Here](#) (BID: 22015045) you can load the private MIB and one device profile. Select an MIB and extract it into a folder of your choice.

- **SCALANCE module:** You get the private MIB via web-based management by entering the following URL in a web browser (e.g., Internet Explorer):
For X300:
http://<IP address of the IE switch X-300>/snScalanceX300.mib
For X400:
http://<IP address of the IE switch X-400>/snScalanceX400.mib
For W700
http:// <IP address of the SCALANCE W>/snScalanceW.mib
Display the source text of the received page (in the menu **View -> Source text** in the Internet Explorer) and save this text, for example, as a text file under the name "**PrivateMIBX300.mib**".

Note

The standard MIBs are stored in the following directory:
<STEP7InstallationDirectory>\S7DATA\snmp\mib

Device profiles

You can either create device profiles yourself or use already existing profiles.

Device profiles that have already been prepared for all modules are located in the STEP 7 installation directory. Prepared device profiles for the SCALANCE modules already include the integration of the private MIB.

To ensure that only the SNMP variables that are actually required are loaded to the SNMP OPC server, it is useful to create an own device profile.

Note

The prepared device profiles are stored in the following directory:
<STEP7InstallationDirectory>\S7DATA\snmp\profile

5.1.1 Configuration of the SNMP OPC server

Preparation

Note

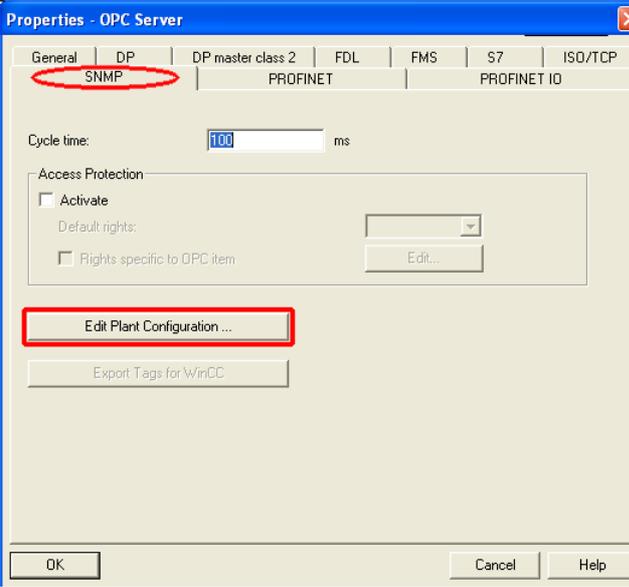
These preparatory steps are only necessary if your SIMATIC NET software is lower than V7.0 SP1.

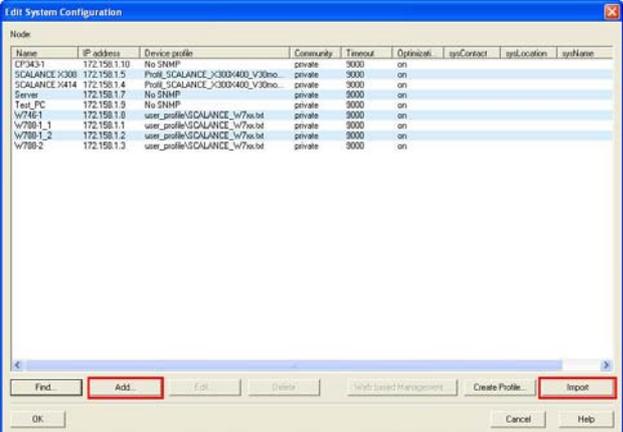
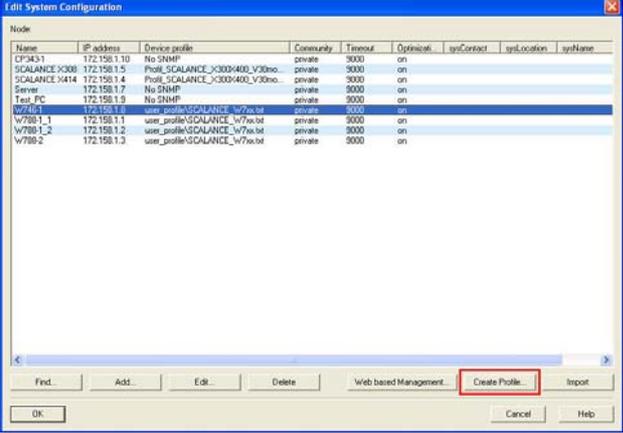
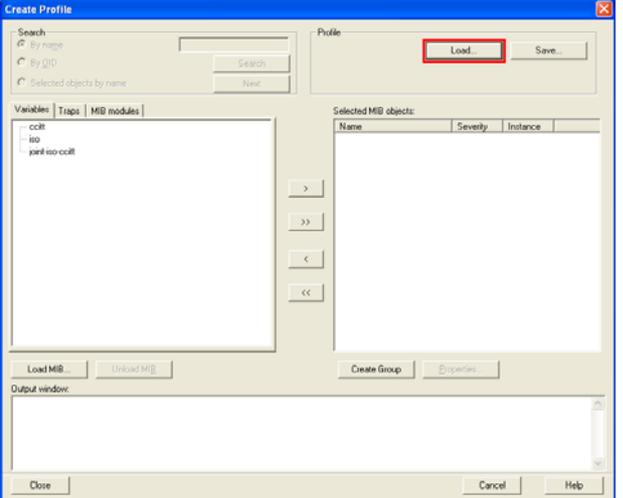
For an overview of SIMATIC software packages and versions installed on your computer, please refer to **Start->SIMATIC->Information ->Installed Software**.

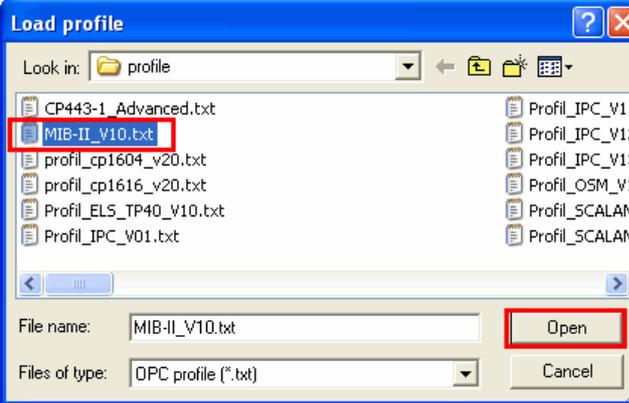
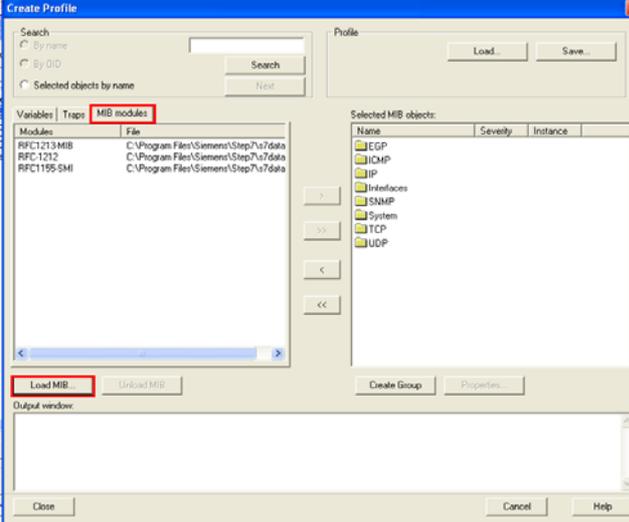
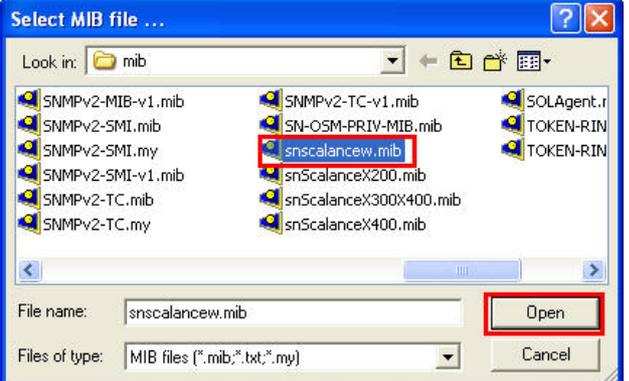
Unzip the folder with the standard MIBs and replace all files located in the MIB folder of STEP 7 **<STEP7InstallationDirectory>\S7DATA\snmp\mib** by these new standard MIBs.

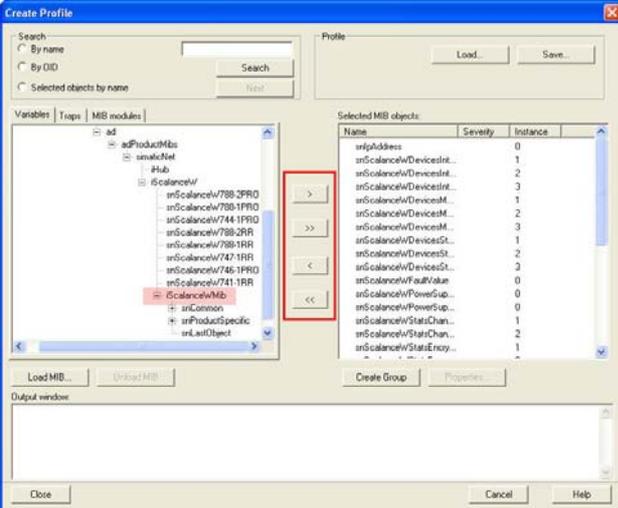
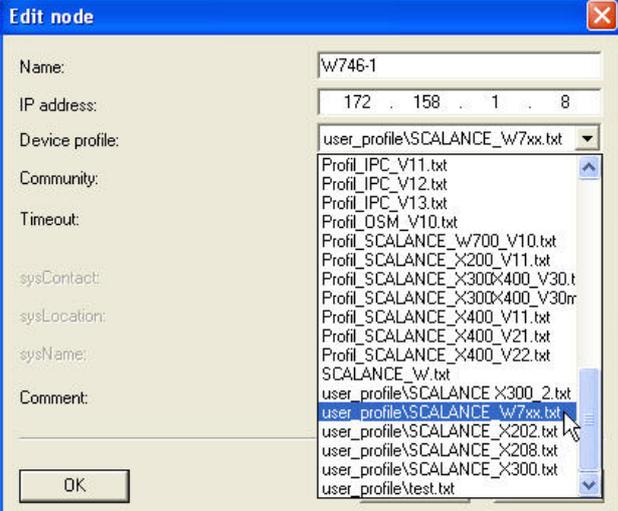
Configuration

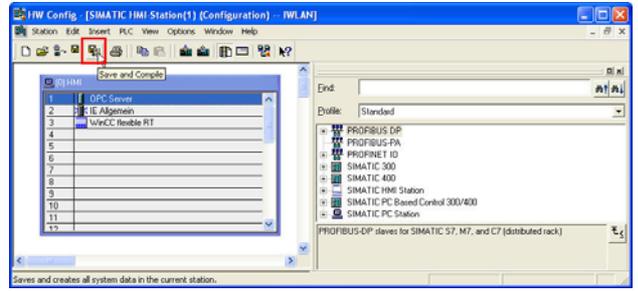
Table 5-2

No.	Action	Comment
1.	To configure the SNMP OPC server, select the HMI station in STEP 7 and open the Configuration . Open the OPC server by double-clicking its properties and select the button Edit Plant Configuration... in the SNMP tab.	

No.	Action	Comment																																																																																										
2.	In the plant configuration, import all configured network nodes with name and IP address using the Import... button. Alternatively, the devices to be monitored can also be manually entered with Add .	 <p>The screenshot shows the 'Edit System Configuration' dialog box with a table of nodes. The 'Import' button at the bottom right is highlighted with a red box.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>IP address</th> <th>Device profile</th> <th>Community</th> <th>Timeout</th> <th>Optimized</th> <th>sysContact</th> <th>sysLocation</th> <th>sysName</th> </tr> </thead> <tbody> <tr><td>CP343-1</td><td>172.158.1.10</td><td>No SNMP</td><td>private</td><td>3000</td><td>on</td><td></td><td></td><td></td></tr> <tr><td>SCALANCE X308</td><td>172.158.1.5</td><td>Profil_SCALANCE_X308-400_V30mo...</td><td>private</td><td>3000</td><td>on</td><td></td><td></td><td></td></tr> <tr><td>SCALANCE X414</td><td>172.158.1.4</td><td>Profil_SCALANCE_X308-400_V30mo...</td><td>private</td><td>3000</td><td>on</td><td></td><td></td><td></td></tr> <tr><td>Server</td><td>172.158.1.7</td><td>No SNMP</td><td>private</td><td>3000</td><td>on</td><td></td><td></td><td></td></tr> <tr><td>Test_PC</td><td>172.158.1.9</td><td>No SNMP</td><td>private</td><td>3000</td><td>on</td><td></td><td></td><td></td></tr> <tr><td>W788-1</td><td>172.158.1.8</td><td>user_profile_SCALANCE_w788.tst</td><td>private</td><td>3000</td><td>on</td><td></td><td></td><td></td></tr> <tr><td>W788-1-1</td><td>172.158.1.1</td><td>user_profile_SCALANCE_w788.tst</td><td>private</td><td>3000</td><td>on</td><td></td><td></td><td></td></tr> <tr><td>W788-1-2</td><td>172.158.1.2</td><td>user_profile_SCALANCE_w788.tst</td><td>private</td><td>3000</td><td>on</td><td></td><td></td><td></td></tr> <tr><td>W788-2</td><td>172.158.1.3</td><td>user_profile_SCALANCE_w788.tst</td><td>private</td><td>3000</td><td>on</td><td></td><td></td><td></td></tr> </tbody> </table>	Name	IP address	Device profile	Community	Timeout	Optimized	sysContact	sysLocation	sysName	CP343-1	172.158.1.10	No SNMP	private	3000	on				SCALANCE X308	172.158.1.5	Profil_SCALANCE_X308-400_V30mo...	private	3000	on				SCALANCE X414	172.158.1.4	Profil_SCALANCE_X308-400_V30mo...	private	3000	on				Server	172.158.1.7	No SNMP	private	3000	on				Test_PC	172.158.1.9	No SNMP	private	3000	on				W788-1	172.158.1.8	user_profile_SCALANCE_w788.tst	private	3000	on				W788-1-1	172.158.1.1	user_profile_SCALANCE_w788.tst	private	3000	on				W788-1-2	172.158.1.2	user_profile_SCALANCE_w788.tst	private	3000	on				W788-2	172.158.1.3	user_profile_SCALANCE_w788.tst	private	3000	on			
Name	IP address	Device profile	Community	Timeout	Optimized	sysContact	sysLocation	sysName																																																																																				
CP343-1	172.158.1.10	No SNMP	private	3000	on																																																																																							
SCALANCE X308	172.158.1.5	Profil_SCALANCE_X308-400_V30mo...	private	3000	on																																																																																							
SCALANCE X414	172.158.1.4	Profil_SCALANCE_X308-400_V30mo...	private	3000	on																																																																																							
Server	172.158.1.7	No SNMP	private	3000	on																																																																																							
Test_PC	172.158.1.9	No SNMP	private	3000	on																																																																																							
W788-1	172.158.1.8	user_profile_SCALANCE_w788.tst	private	3000	on																																																																																							
W788-1-1	172.158.1.1	user_profile_SCALANCE_w788.tst	private	3000	on																																																																																							
W788-1-2	172.158.1.2	user_profile_SCALANCE_w788.tst	private	3000	on																																																																																							
W788-2	172.158.1.3	user_profile_SCALANCE_w788.tst	private	3000	on																																																																																							
3.	Select the device to assign a separate SNMP device profile to the devices to be monitored. Use the Create Profile... button to open the corresponding dialog box.	 <p>The screenshot shows the 'Edit System Configuration' dialog box with the same table as above. The 'Create Profile...' button at the bottom right is highlighted with a red box.</p>																																																																																										
4.	With Load you can load a prepared profile.	 <p>The screenshot shows the 'Create Profile' dialog box. The 'Load...' button is highlighted with a red box.</p>																																																																																										

No.	Action	Comment
5.	<p>Load the MIB-II_V10.txt profile as a basis for creating a profile for a SCALANCE X module. This profile is located in the STEP 7 installation directory in the S7DATA/snmp/profile folder.</p>	
6.	<p>As soon as the profile has been loaded, change to the MIB modules tab. To be able to use the SCALANCE module-specific SNMP variables, reload its private MIB. To do this, click the Load MIB... button.</p>	
7.	<p>Navigate to the directory in which you have stored the private MIB of the SCALANCE, select the file and open it. The private MIB is loaded (here the SCALANCE W MIB).</p>	

No.	Action	Comment
8.	<p>Navigate to the Variables tab, for example, to private/.../iScalanceW/iScalanceWMib. Search the tree for the variables you need for SNMP monitoring. You can use the arrows to add or remove individual or several variables of your choice from the selection.</p>	
9.	<p>Store this newly created profile under any name in the STEP 7 installation directory in the S7DATA/snmp/user_profile folder and close the Create Profile dialog box.</p>	
10.	<p>You can now select the newly created profile as a device profile for the SCALANCE module and use it. To do this, select and double-click the device. You can select the created profile or existing profiles in the Edit node dialog.</p>	

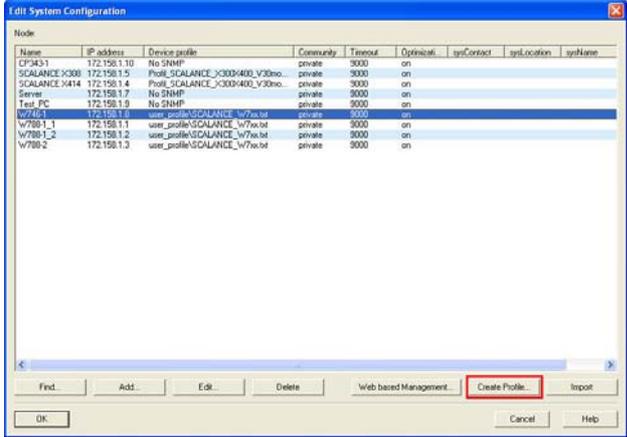
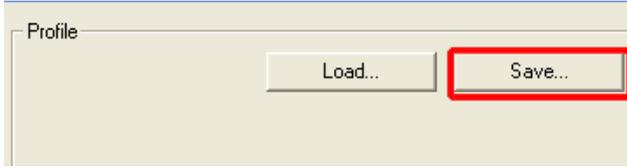
No.	Action	Comment
11.	After closing the dialog boxes with OK and clicking the Save and compile button for the station, the configuration of the SNMP OPC server is complete and the station can be loaded.	

5.1.2 Changing the existing SCALANCE device profiles

Once the device profiles have been created as a text file, they are only stored in the **S7DATA/snmp/user_profile** folder of the **STEP 7 installation directory** and not in the STEP 7 project directory. The XDB file generated after saving and compiling the HMI station contains the necessary information.

If you do not want to change the SNMP variables of this application, you need the text file used. The code folder included in the delivery contains the device profiles of the two SCALANCE modules as a text file.

Table 5-3

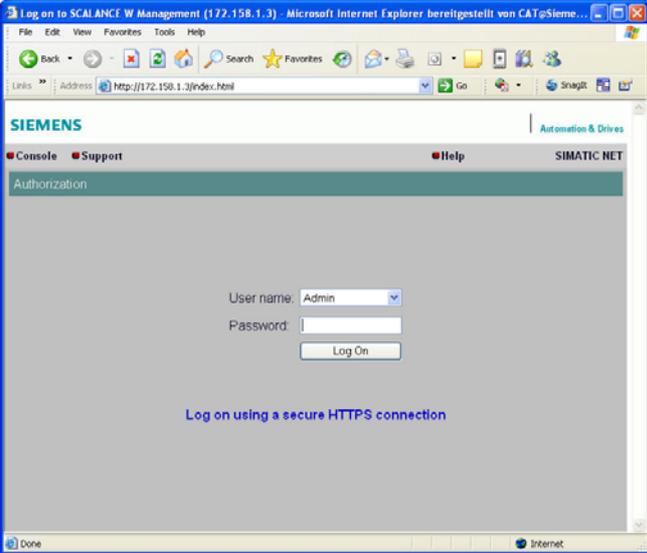
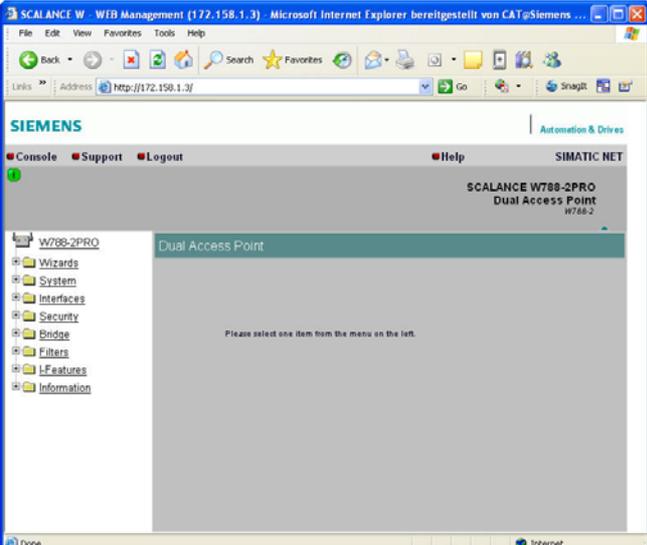
No.	Action	Comment
1.	Save the device profiles in your STEP 7 installation directory in the S7DATA/snmp/user_profile folder.	
2.	To change the device profiles, select the HMI station in STEP 7 and open the Configuration . Open the OPC Server properties and select the Edit Plant Configuration... button in the SNMP tab.	
3.	Select a SCALANCE. Use the Create Profile... button to open the dialog box required for the change.	
5.	Change the device profile as desired and save it. Close the dialog box by clicking OK.	
6.	After saving and compiling the station, the SNMP OPC server has been configured and the station can be loaded.	

5.2 Web-based management

The SCALANCE switches are configured using web-based management.

Note When using the web-based management, no proxy sever must be set in the connection properties of the internet browser.

Table 5-4

No.	Action	Comment
1.	Open an internet browser, for example Internet Explorer or Firefox, and enter the following address: http://<IP address of the SCALANCE> .	
2.	Enter the user name and password. Click the Log On button in order to log on.	The default settings are: User: admin Password: admin
3.	The web-based management opens.	

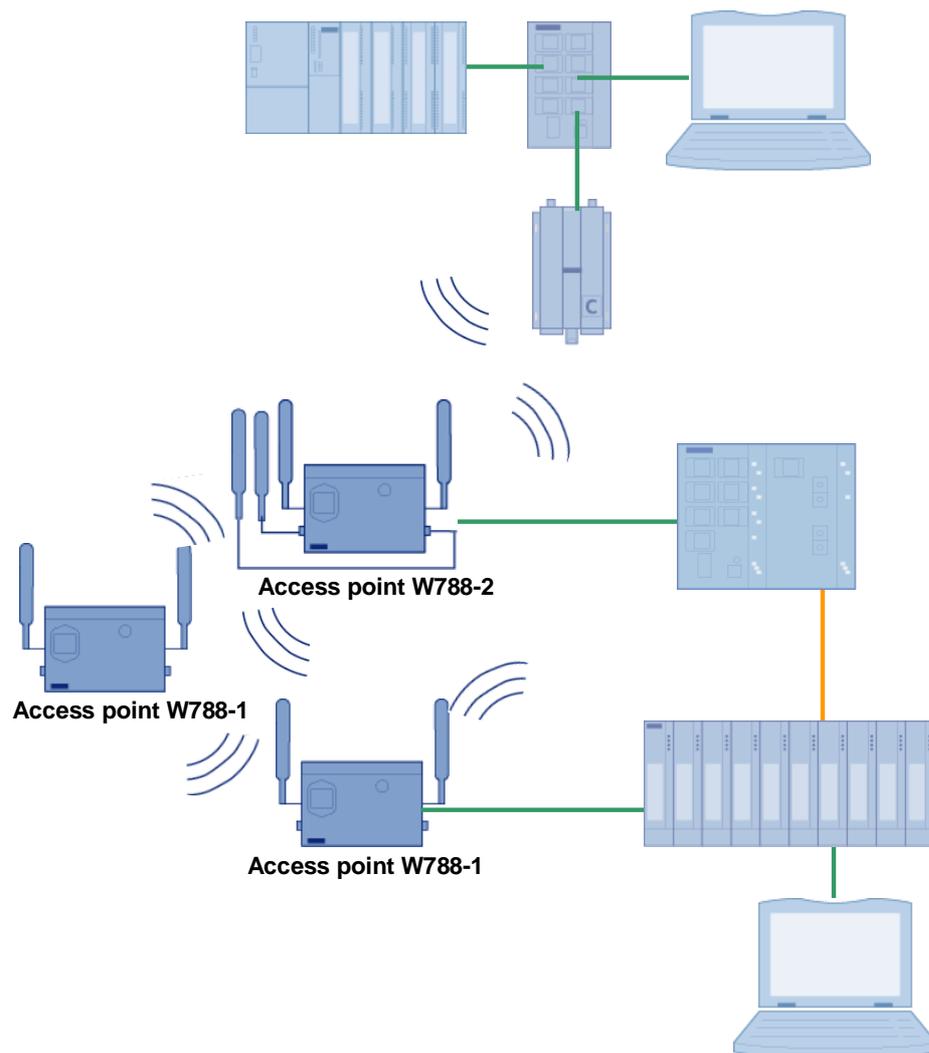
Note

The Internet Explorer of Win2003 Server is installed with high security settings. It might be possible that the web-based management pages of the SCALANCE modules and the configuration page of the FTP server cannot be displayed. To prevent these pages from being blocked, you can turn off the high security settings under **Start->Settings->Control Panel->Add or Remove Programs->Add/Remove Windows Components->Internet Explorer Enhanced Security Configuration** by removing the tick or clicking **Next>**.

5.3 Standard configuration of the SCALANCE W modules

The web-based management of the SCALANCE W modules offers several wizards that provide help for the WLAN connection settings.

Figure 5-2



5.3.1 Wizards of the SCALANCE W788-2

This wizard can be used to make basic settings:

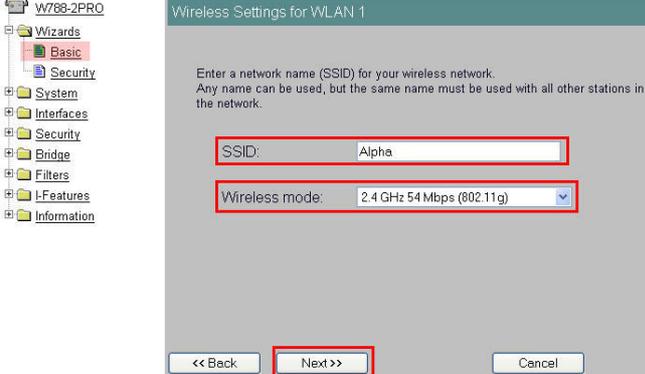
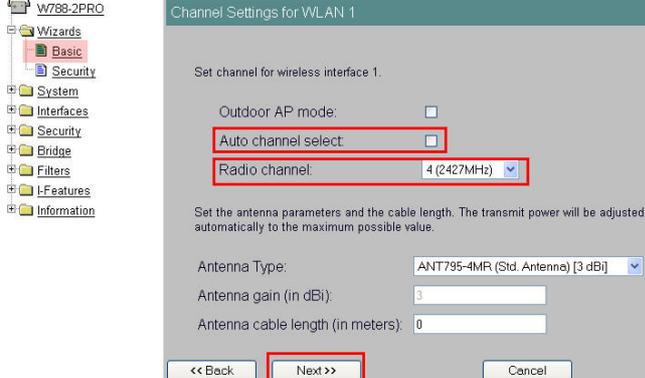
- Configuration of the radio networks
- Security settings

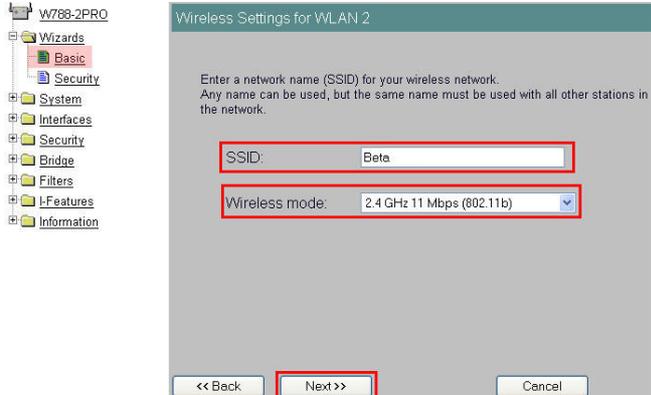
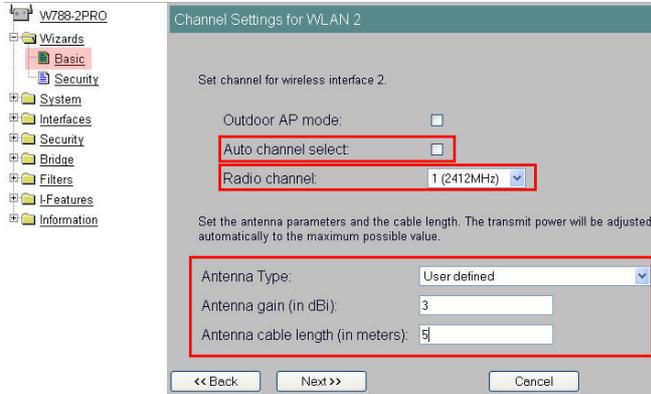
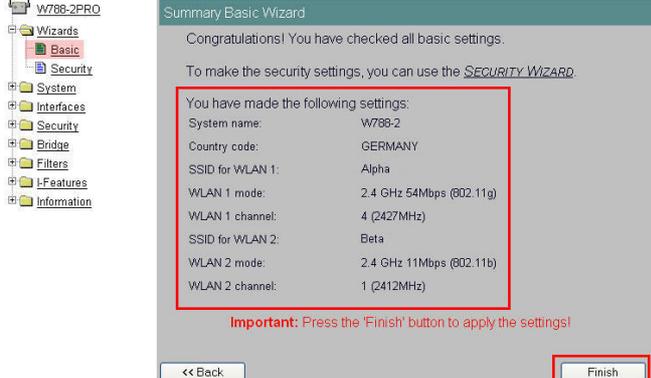
The following agreement is made for the SCALANCE W788-2 interfaces:

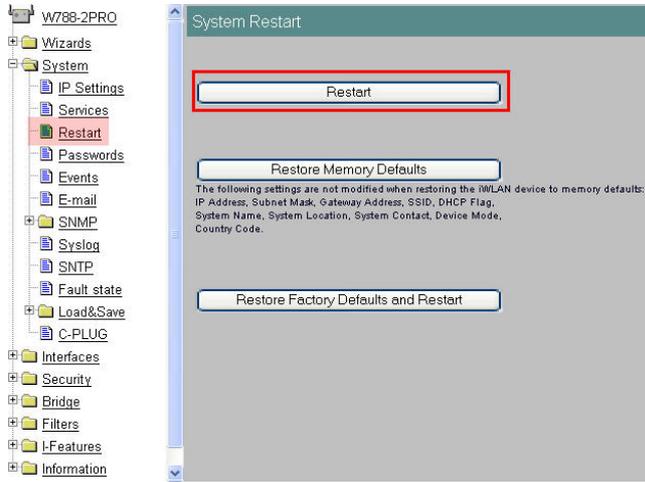
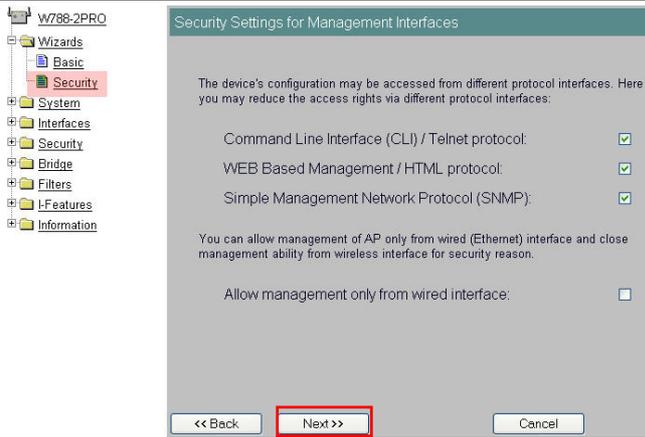
- WLAN interface 1 for the WDS function.
- WLAN interface 2 for the connection to the W746-1.

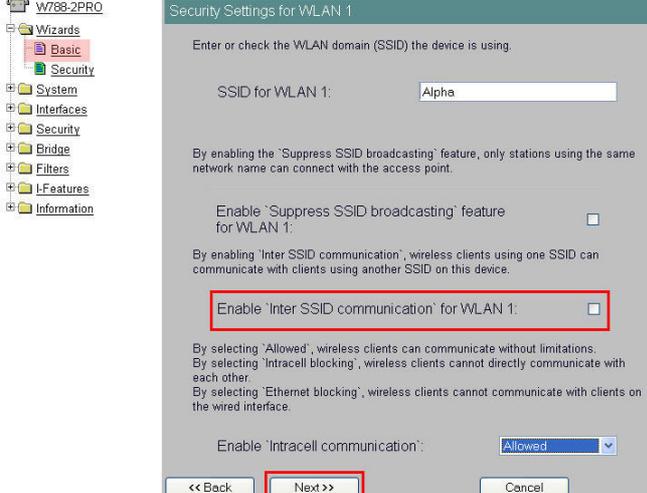
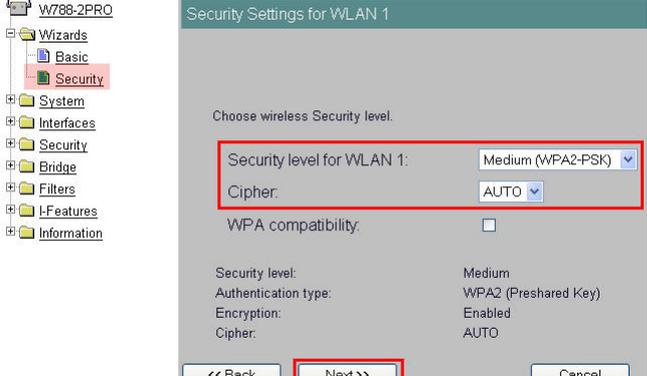
Table 5-5

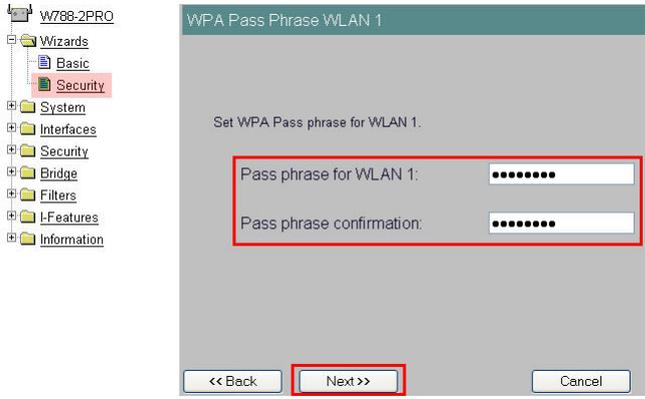
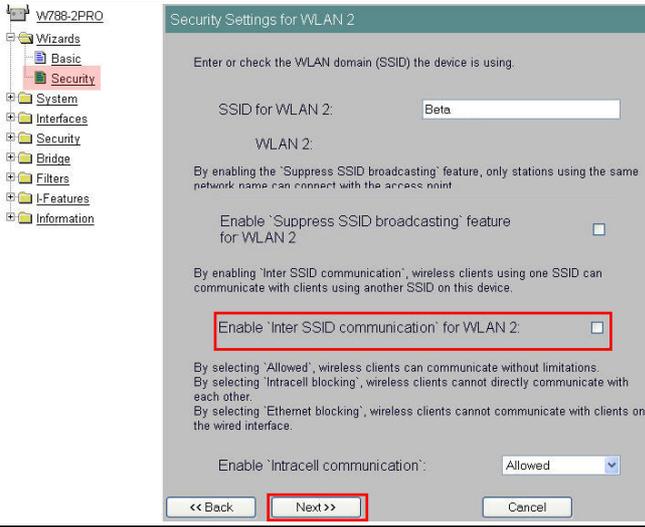
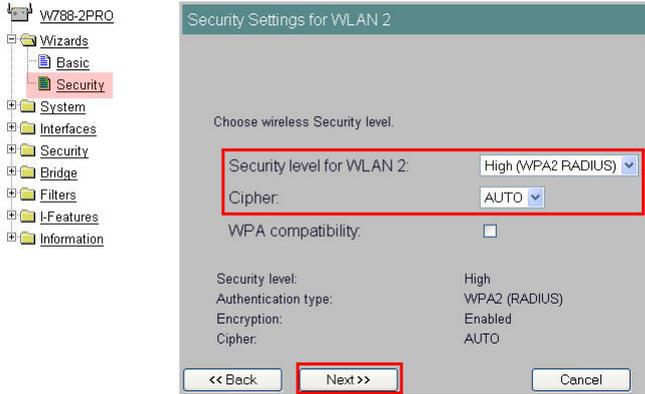
No.	Action	Comment
1.	Open the web-based management for the SCALANCE W788-2.	http://172.158.1.3
2.	Click Wizards -> Basic in the navigation bar. You can skip the first dialog box with the IP address by clicking Next .	
3.	You have already transferred the system name to the module via the SIMATIC MANAGER. Go to the next window here.	

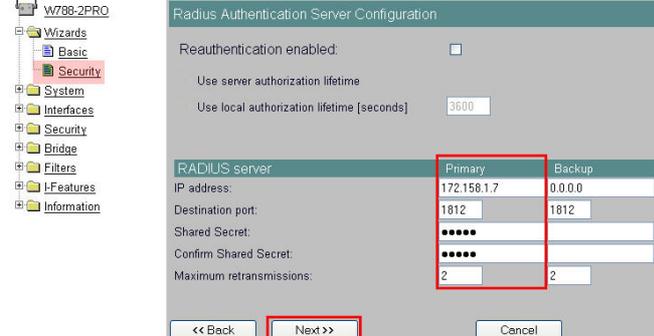
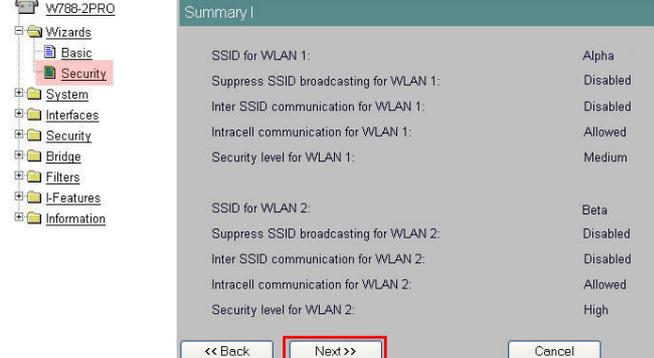
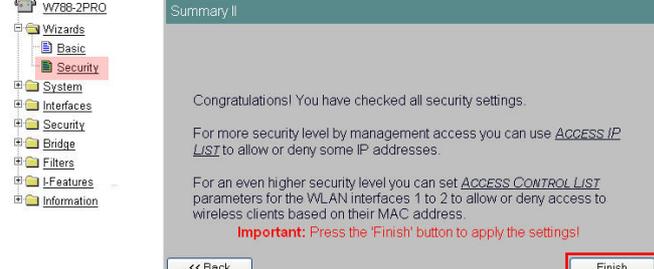
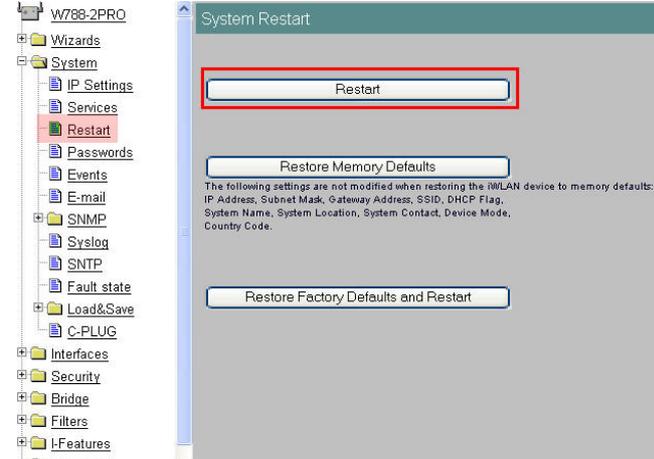
No.	Action	Comment
4.	Select GERMANY as a country code and go to the next step with Next .	 <p>The screenshot shows a configuration window titled 'Country code'. It contains a text prompt 'Please choose your country code.' and a dropdown menu labeled 'Country code:' with 'GERMANY' selected. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'. The 'Next >>' button is highlighted with a red rectangular box.</p>
5.	Enter the name for radio network 1 under SSID . Select 2.4 GHz 54 Mbps (802.11g) as Wireless Mode . Confirm the entry with Next .	 <p>The screenshot shows a configuration window titled 'Wireless Settings for WLAN 1'. It contains a text prompt 'Enter a network name (SSID) for your wireless network.' and a text input field labeled 'SSID:' containing 'Alpha'. Below it is a dropdown menu labeled 'Wireless mode:' set to '2.4 GHz 54 Mbps (802.11g)'. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'. The 'Next >>' button is highlighted with a red rectangular box.</p>
6.	Deactivate Auto Channel select in the next dialog box and select Radio Channel 4 instead. Click Next to go to the next configuration window.	 <p>The screenshot shows a configuration window titled 'Channel Settings for WLAN 1'. It contains a text prompt 'Set channel for wireless interface 1.' and several options. The 'Auto channel select' checkbox is unchecked. The 'Radio channel' dropdown menu is set to '4 (2427MHz)'. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'. The 'Next >>' button is highlighted with a red rectangular box.</p>

No.	Action	Comment
7.	Repeat steps 5 and 6 for the second interface. Enter the name for radio network 2 under SSID . Select 2.4 GHz 11 Mbps (802.11b) as Wireless Mode . Confirm the entry with Next .	 <p>Wireless Settings for WLAN 2</p> <p>Enter a network name (SSID) for your wireless network. Any name can be used, but the same name must be used with all other stations in the network.</p> <p>SSID: <input type="text" value="Beta"/></p> <p>Wireless mode: <input type="text" value="2.4 GHz 11 Mbps (802.11b)"/></p> <p><< Back Next >> Cancel</p>
8.	Deactivate Auto Channel select also for the second interface in the next step and select Radio Channel 1 instead. Click Next to go to the next configuration window.	 <p>Channel Settings for WLAN 2</p> <p>Set channel for wireless interface 2.</p> <p>Outdoor AP mode: <input type="checkbox"/></p> <p>Auto channel select: <input type="checkbox"/></p> <p>Radio channel: <input type="text" value="1 (2412MHz)"/></p> <p>Set the antenna parameters and the cable length. The transmit power will be adjusted automatically to the maximum possible value.</p> <p>Antenna Type: <input type="text" value="User defined"/></p> <p>Antenna gain (in dBi): <input type="text" value="3"/></p> <p>Antenna cable length (in meters): <input type="text" value="5"/></p> <p><< Back Next >> Cancel</p>
9.	Once the Basic Wizard is complete, an overview of the parameters entered is displayed. Exit the wizard with Finish to accept all settings.	 <p>Summary Basic Wizard</p> <p>Congratulations! You have checked all basic settings.</p> <p>To make the security settings, you can use the <i>SECURITY WIZARD</i>.</p> <p>You have made the following settings:</p> <ul style="list-style-type: none"> System name: W768-2 Country code: GERMANY SSID for WLAN 1: Alpha WLAN 1 mode: 2.4 GHz 54Mbps (802.11g) WLAN 1 channel: 4 (2427MHz) SSID for WLAN 2: Beta WLAN 2 mode: 2.4 GHz 11Mbps (802.11b) WLAN 2 channel: 1 (2412MHz) <p>Important: Press the 'Finish' button to apply the settings!</p> <p><< Back Finish</p>

No.	Action	Comment
10.	<p>Restart the SCALANCE W788-2 by clicking system- > Restart. Log on to the web-based management again after the restart.</p> <p>The Basic Wizard is thus complete. The radio networks have been configured.</p>	
11.	<p>The security settings are made in the next steps. Open the Security Wizard by clicking wizards-> security. On the first page, you can change the administrator password for the web-based management. Skip this setting with Next.</p>	
12.	<p>Do not change the default settings in the next step and proceed with Next.</p>	

No.	Action	Comment
13.	Change the write permission of SNMP variables into public and click Next to go to the next configuration.	 <p>Security Settings for SNMP Protocol</p> <p>Set the SNMPv1 community string to protect your device from the unauthorized access over SNMPv1.</p> <p>You can forbid to use SNMPv1 protocol for configuration.</p> <p>Write community string: <input type="text" value="public"/></p> <p>SNMPv1/v2 read only: <input checked="" type="checkbox"/></p> <p><< Back Next >> Cancel</p>
14.	Deactivate the function that clients with different SSID can communicate with each other. The next window appears after clicking Next .	 <p>Security Settings for WLAN 1</p> <p>Enter or check the WLAN domain (SSID) the device is using.</p> <p>SSID for WLAN 1: <input type="text" value="Alpha"/></p> <p>By enabling the 'Suppress SSID broadcasting' feature, only stations using the same network name can connect with the access point.</p> <p>Enable 'Suppress SSID broadcasting' feature for WLAN 1: <input type="checkbox"/></p> <p>By enabling 'Inter SSID communication', wireless clients using one SSID can communicate with clients using another SSID on this device.</p> <p>Enable 'Inter SSID communication' for WLAN 1: <input type="checkbox"/></p> <p>By selecting 'Allowed', wireless clients can communicate without limitations. By selecting 'Intracell blocking', wireless clients cannot directly communicate with each other. By selecting 'Ethernet blocking', wireless clients cannot communicate with clients on the wired interface.</p> <p>Enable 'Intracell communication': <input type="text" value="Allowed"/></p> <p><< Back Next >> Cancel</p>
15.	Select Medium (WPA2-PSK) and Cipher AUTO as a security level for interface 1. Click Next to go to the next step.	 <p>Security Settings for WLAN 1</p> <p>Choose wireless Security level.</p> <p>Security level for WLAN 1: <input type="text" value="Medium (WPA2-PSK)"/></p> <p>Cipher: <input type="text" value="AUTO"/></p> <p>WPA compatibility: <input type="checkbox"/></p> <p>Security level: Medium Authentication type: WPA2 (Preshared Key) Encryption: Enabled Cipher: AUTO</p> <p><< Back Next >> Cancel</p>

No.	Action	Comment
16.	<p>Define a key for encoding the network. Confirm the key a second time.</p> <p>Note: Note the key because it is required for configuring the other access points. Click Next to go to the next step.</p>	
17.	<p>Steps 14-16 are now repeated for the second WLAN interface.</p> <p>Deactivate the function that clients with different SSID can communicate with each other. The next window appears after clicking Next.</p>	
18.	<p>Select High (WPA2-RADIUS) and Cipher AUTO as a security level for interface 2. Click Next to go to the next step.</p>	

No.	Action	Comment																		
19.	Enter the the IP address of the server PC as the primary RADIUS server . Define a secret admin password and confirm this password a second time. Click Next to display an overview of the security settings.	 <p>RADIUS Authentication Server Configuration</p> <p>Reauthentication enabled: <input type="checkbox"/></p> <p>Use server authorization lifetime</p> <p>Use local authorization lifetime [seconds] <input type="text" value="3600"/></p> <table border="1"> <thead> <tr> <th>RADIUS server</th> <th>Primary</th> <th>Backup</th> </tr> </thead> <tbody> <tr> <td>IP address:</td> <td>172.158.1.7</td> <td>0.0.0.0</td> </tr> <tr> <td>Destination port:</td> <td>1812</td> <td>1812</td> </tr> <tr> <td>Shared Secret:</td> <td>.....</td> <td></td> </tr> <tr> <td>Confirm Shared Secret:</td> <td>.....</td> <td></td> </tr> <tr> <td>Maximum retransmissions:</td> <td>2</td> <td>2</td> </tr> </tbody> </table> <p><< Back Next >> Cancel</p>	RADIUS server	Primary	Backup	IP address:	172.158.1.7	0.0.0.0	Destination port:	1812	1812	Shared Secret:		Confirm Shared Secret:		Maximum retransmissions:	2	2
RADIUS server	Primary	Backup																		
IP address:	172.158.1.7	0.0.0.0																		
Destination port:	1812	1812																		
Shared Secret:																			
Confirm Shared Secret:																			
Maximum retransmissions:	2	2																		
20.	You can exit the Security Wizard with Next .	 <p>Summary I</p> <p>SSID for WLAN 1: Alpha</p> <p>Suppress SSID broadcasting for WLAN 1: Disabled</p> <p>Inter SSID communication for WLAN 1: Disabled</p> <p>Intracell communication for WLAN 1: Allowed</p> <p>Security level for WLAN 1: Medium</p> <p>SSID for WLAN 2: Beta</p> <p>Suppress SSID broadcasting for WLAN 2: Disabled</p> <p>Inter SSID communication for WLAN 2: Disabled</p> <p>Intracell communication for WLAN 2: Allowed</p> <p>Security level for WLAN 2: High</p> <p><< Back Next >> Cancel</p>																		
21.	Close the Security Wizard with Finish .	 <p>Summary II</p> <p>Congratulations! You have checked all security settings.</p> <p>For more security level by management access you can use ACCESS_IP LIST to allow or deny some IP addresses.</p> <p>For an even higher security level you can set ACCESS_CONTROL LIST parameters for the WLAN interfaces 1 to 2 to allow or deny access to wireless clients based on their MAC address.</p> <p>Important: Press the 'Finish' button to apply the settings!</p> <p><< Back Finish</p>																		
22.	Restart the SCALANCE W788-2 by clicking System-> Restart .	 <p>System Restart</p> <p>Restart</p> <p>Restore Memory Defaults</p> <p>The following settings are not modified when restoring the WLAN device to memory defaults: IP Address, Subnet Mask, Gateway Address, SSID, DHCP Flag, System Name, System Location, System Contact, Device Mode, Country Code.</p> <p>Restore Factory Defaults and Restart</p>																		

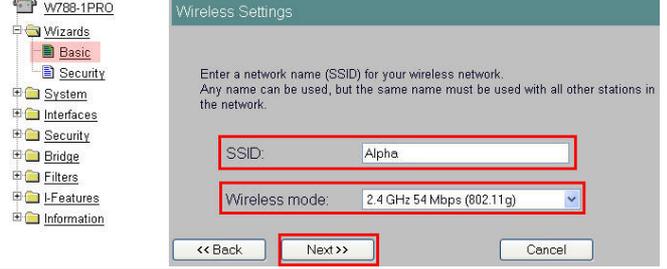
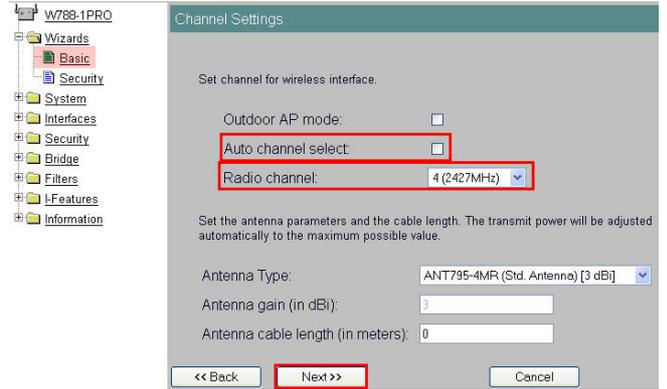
No.	Action	Comment
23.	Navigate to system-> SNMP and enter private under read community string . Confirm with Set Values .	

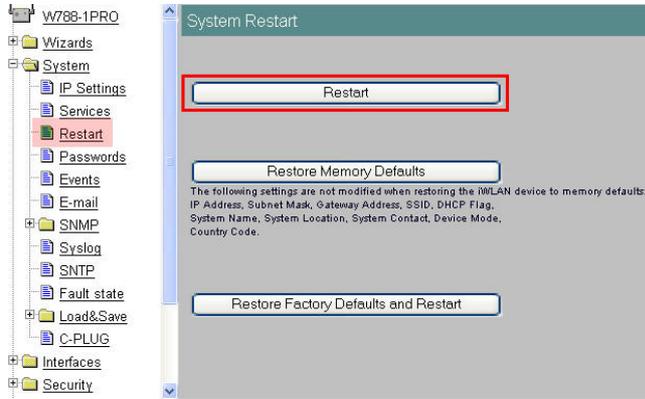
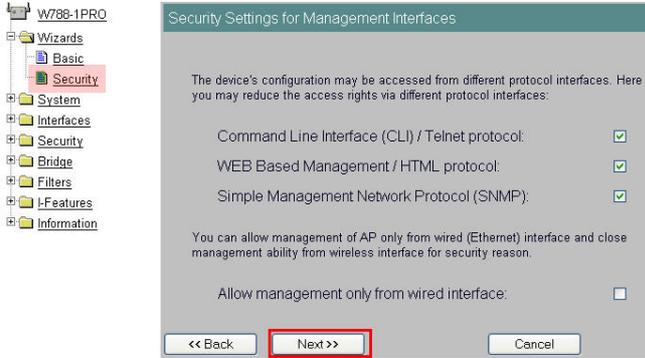
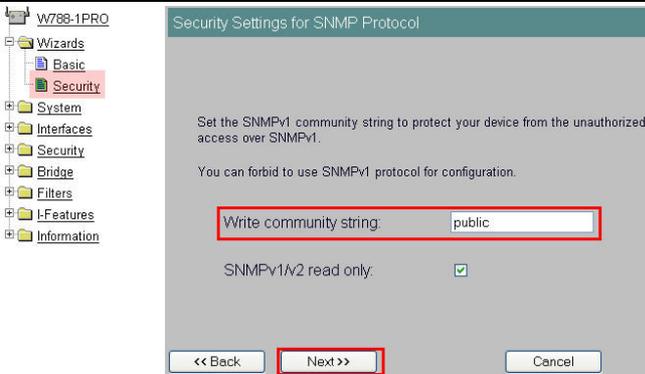
5.3.2 Wizards of both SCALANCE W788-1

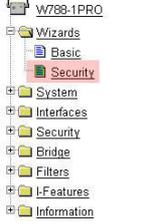
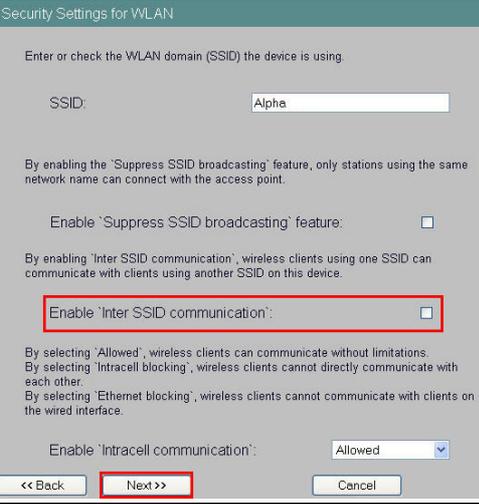
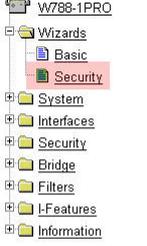
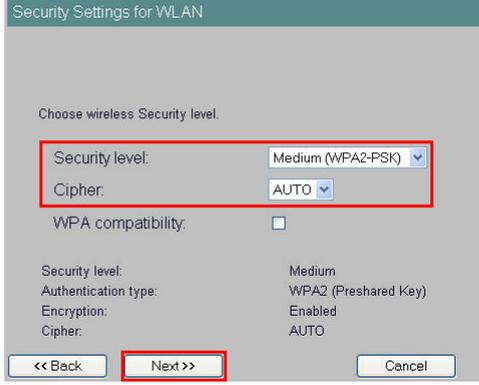
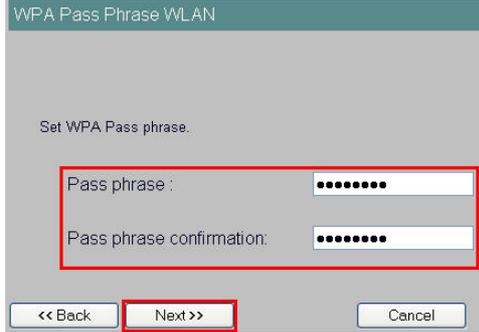
Both SCALANCE W788-1 are configured with identical settings. Only the system name and the IP addresses are different.

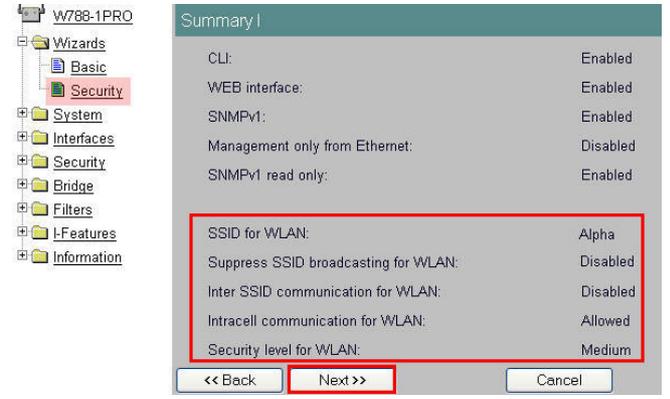
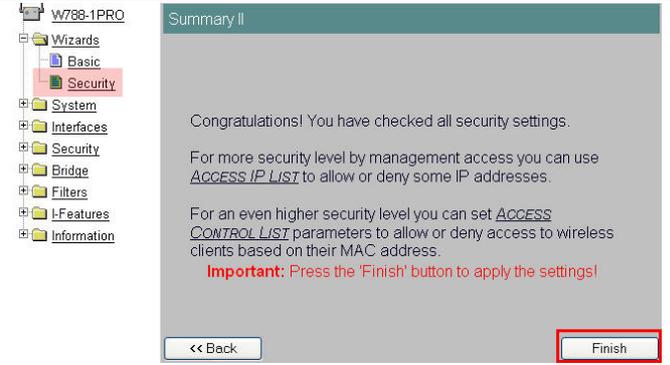
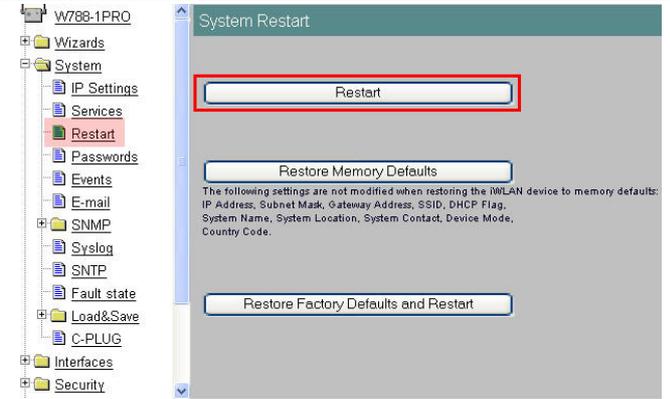
Table 5-6

No.	Action	Comment
1.	Open the web-based management for the first SCALANCE W788-1.	http://172.158.1.1
2.	Click Wizards -> Basic in the navigation bar. You can skip the first dialog box with the IP address by clicking Next .	
3.	You have already transferred the system name to the module via the SIMATIC MANAGER. Go to the next window here.	

No.	Action	Comment
4.	Select GERMANY as a country code and go to the next step with Next .	
5.	Enter the radio network name you have selected for WLAN interface 1 of the SCALANCE W788-2 under SSID . Select 2.4 GHz 54 Mbps (802.11g) as Wireless Mode . Confirm the entry with Next and follow the next step.	
6.	Deactivate Auto Channel select and select Radio Channel 4 instead. Click Next to go to the next configuration window.	
7.	Once the Basic Wizard is complete, an overview of the parameters entered is displayed. Exit the wizard with Finish to accept all settings.	

No.	Action	Comment
8.	<p>Restart the SCALANCE W788-2 by clicking system ->Restart. Log on to the web-based management again after the restart.</p> <p>The Basic Wizard is thus complete.</p>	
9.	<p>The security settings are now made in the next steps. Open the Security Wizard by clicking wizards->security. On the first page, you can change the administrator password for the web-based management. Skip this setting with Next.</p>	
10.	<p>Do not change the default settings in the next step and proceed with Next.</p>	
11.	<p>Change the write permission of SNMP variables into public and click Next to go to the next configuration.</p>	

No.	Action	Comment	
12.	<p>Deactivate the function that clients with different SSID can communicate with each other. The next window appears after clicking Next.</p>		
13.	<p>Select Medium (WPA2-PSK) and Cipher AUTO as a security level. Click Next to go to the next step.</p>		
14.	<p>Under Network encoding, enter the key you have defined for interface 1 of the SCALANCE W788-2 (Table 5-5, line 16). Confirm the key a second time. Click Next to go to the next step.</p>		

No.	Action	Comment																				
15.	You can exit the Security Wizard with Next .	 <p>Summary I</p> <table border="1"> <tr><td>CLI:</td><td>Enabled</td></tr> <tr><td>WEB interface:</td><td>Enabled</td></tr> <tr><td>SNMPv1:</td><td>Enabled</td></tr> <tr><td>Management only from Ethernet:</td><td>Disabled</td></tr> <tr><td>SNMPv1 read only:</td><td>Enabled</td></tr> <tr><td>SSID for WLAN:</td><td>Alpha</td></tr> <tr><td>Suppress SSID broadcasting for WLAN:</td><td>Disabled</td></tr> <tr><td>Inter SSID communication for WLAN:</td><td>Disabled</td></tr> <tr><td>Intracell communication for WLAN:</td><td>Allowed</td></tr> <tr><td>Security level for WLAN:</td><td>Medium</td></tr> </table> <p><< Back Next >> Cancel</p>	CLI:	Enabled	WEB interface:	Enabled	SNMPv1:	Enabled	Management only from Ethernet:	Disabled	SNMPv1 read only:	Enabled	SSID for WLAN:	Alpha	Suppress SSID broadcasting for WLAN:	Disabled	Inter SSID communication for WLAN:	Disabled	Intracell communication for WLAN:	Allowed	Security level for WLAN:	Medium
CLI:	Enabled																					
WEB interface:	Enabled																					
SNMPv1:	Enabled																					
Management only from Ethernet:	Disabled																					
SNMPv1 read only:	Enabled																					
SSID for WLAN:	Alpha																					
Suppress SSID broadcasting for WLAN:	Disabled																					
Inter SSID communication for WLAN:	Disabled																					
Intracell communication for WLAN:	Allowed																					
Security level for WLAN:	Medium																					
16.	Close the Security Wizard with Finish .	 <p>Summary II</p> <p>Congratulations! You have checked all security settings.</p> <p>For more security level by management access you can use <u>ACCESS IP LIST</u> to allow or deny some IP addresses.</p> <p>For an even higher security level you can set <u>ACCESS CONTROL LIST</u> parameters to allow or deny access to wireless clients based on their MAC address.</p> <p>Important: Press the 'Finish' button to apply the settings!</p> <p><< Back Finish</p>																				
17.	Restart the SCALANCE W788-1 by clicking System-> Restart .	 <p>System Restart</p> <p>Restart</p> <p>Restore Memory Defaults</p> <p>The following settings are not modified when restoring the WLAN device to memory defaults: IP Address, Subnet Mask, Gateway Address, SSID, DHCP Flag, System Name, System Location, System Contact, Device Mode, Country Code.</p> <p>Restore Factory Defaults and Restart</p>																				

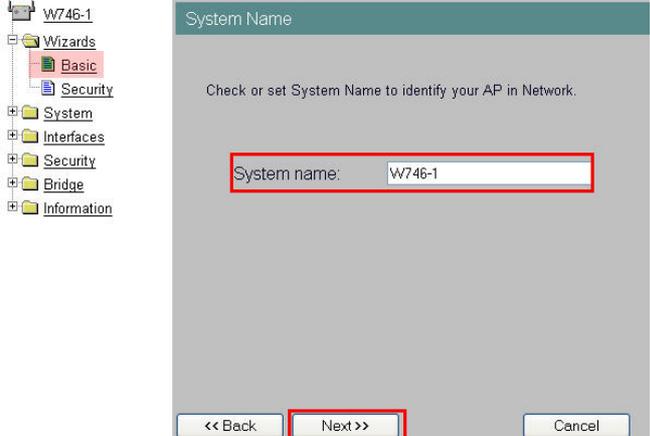
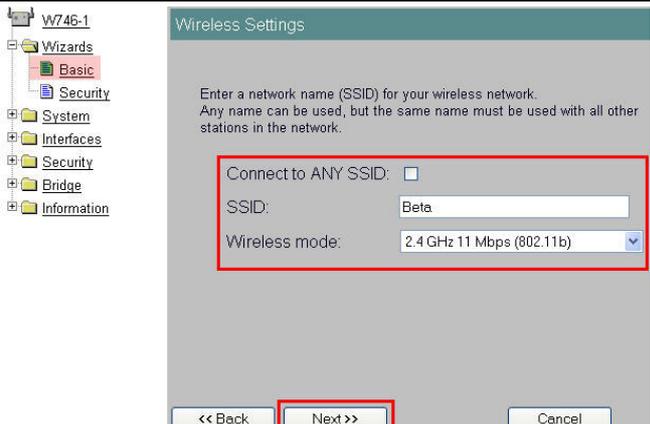
No.	Action	Comment
18.	Navigate to system-> SNMP and enter private under read community string . Confirm with Set Values .	

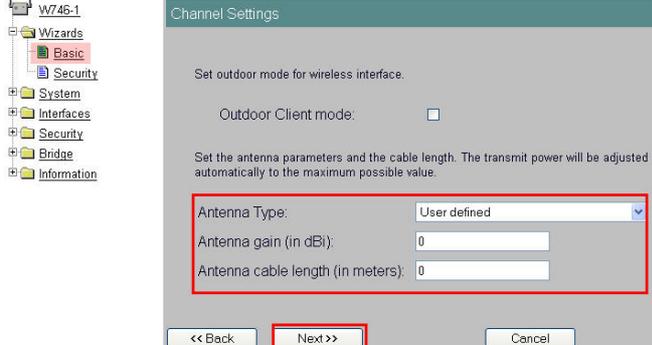
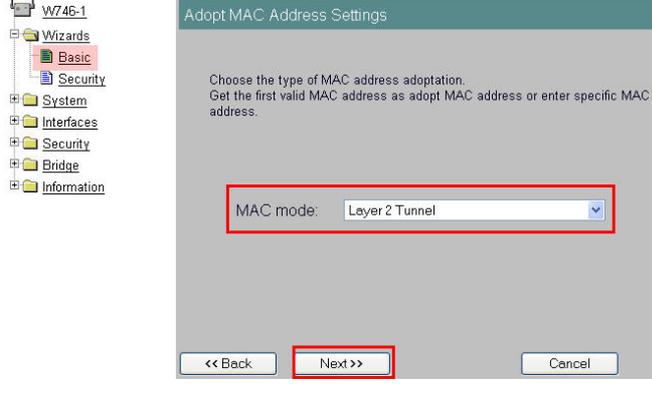
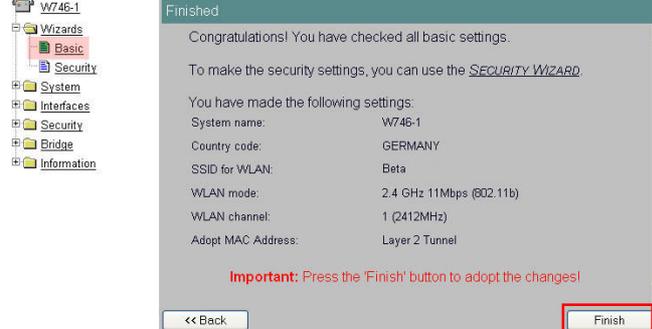
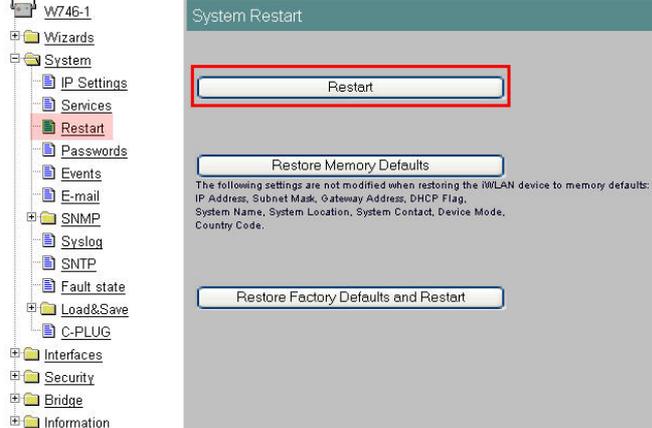
Note Configure the second SCALANCE W788-1 in the same way. For this purpose, connect the server PC directly to the Ethernet interface of the second SCALANCE W788-1.

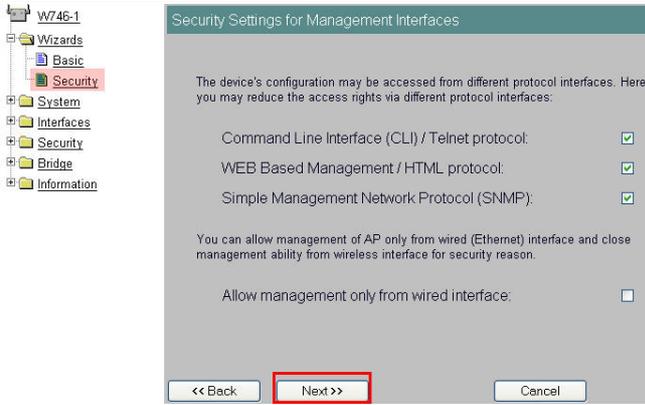
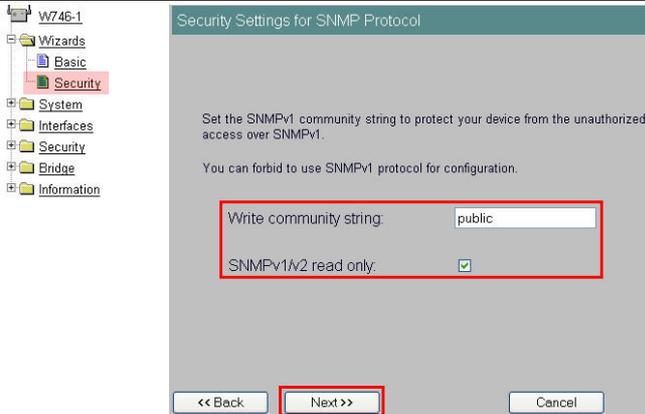
5.3.3 Wizards of the SCALANCE W746-1

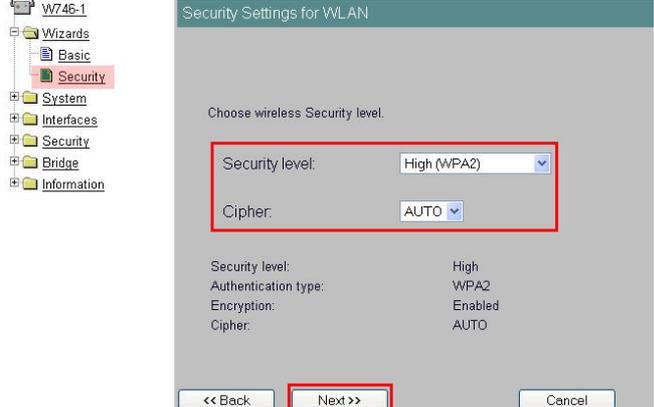
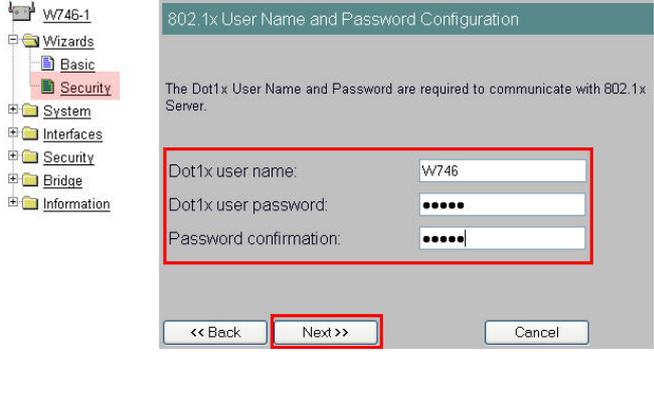
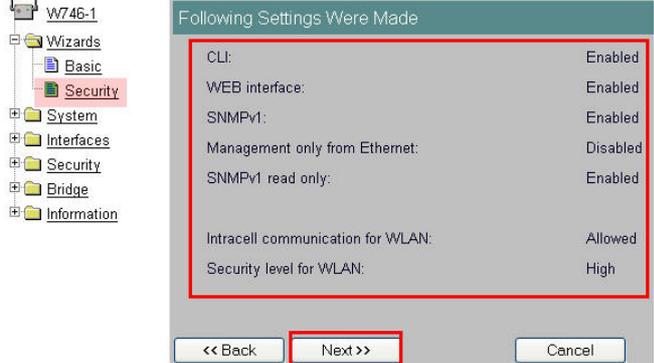
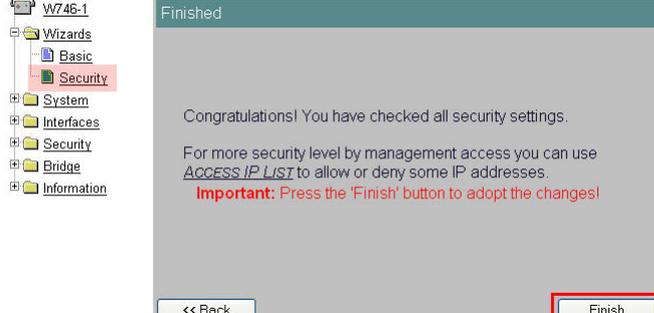
Table 5-7

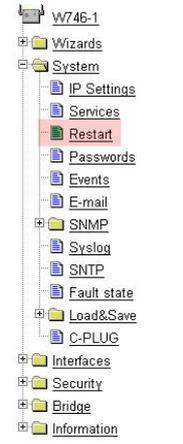
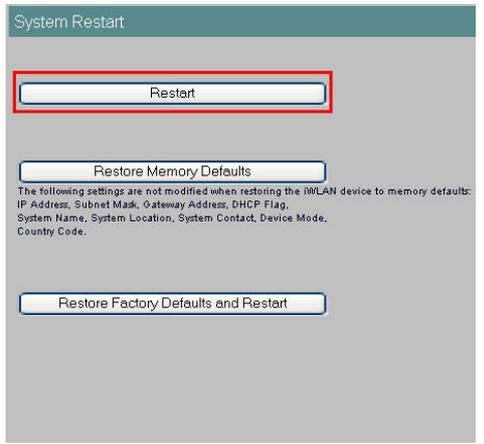
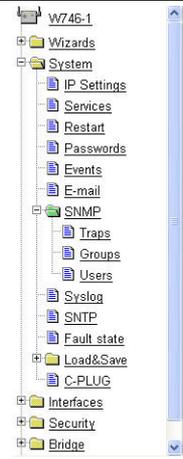
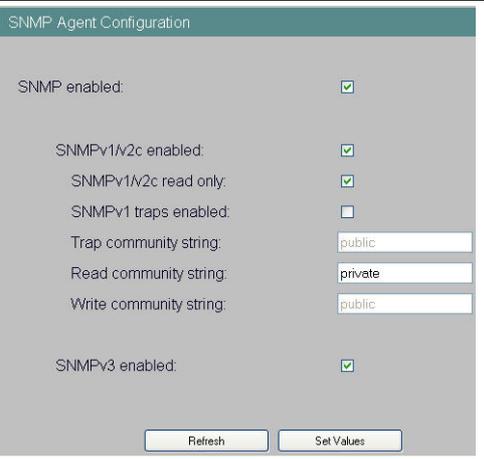
No.	Action	Comment
1.	Connect the server PC to the SCALANCE X108.	
2.	Open the web-based management for the SCALANCE W746-1.	http://172.158.1.8
3.	Click wizards -> Basic in the navigation bar. You can skip the first dialog box with the IP address by clicking Next .	

No.	Action	Comment
4.	You have already transferred the system name to the module via the SIMATIC MANAGER. Go to the next window here.	 <p>The screenshot shows the 'System Name' configuration window. The title bar reads 'System Name'. Below the title, there is a text box with the instruction: 'Check or set System Name to identify your AP in Network.' The 'System name' field contains the text 'W746-1'. At the bottom of the window, there are three buttons: '<< Back', 'Next >>', and 'Cancel'. The 'Next >>' button is highlighted with a red rectangular box.</p>
5.	Select GERMANY as a country code and go to the next step with Next .	 <p>The screenshot shows the 'Country code' configuration window. The title bar reads 'Country code'. Below the title, there is a text box with the instruction: 'Please choose your country code.' The 'Country code' dropdown menu is set to 'GERMANY'. At the bottom of the window, there are three buttons: '<< Back', 'Next >>', and 'Cancel'. The 'Next >>' button is highlighted with a red rectangular box.</p>
6.	Deactivate the function that enables the connection to all SSIDs. Enter the radio network name you have selected for WLAN interface 2 of the SCALANCE W788-2 under SSID (Table 5-5, line 7). Select 2.4 GHz 11 Mbps (802.11b) as Wireless Mode . Confirm the entry with Next .	 <p>The screenshot shows the 'Wireless Settings' configuration window. The title bar reads 'Wireless Settings'. Below the title, there is a text box with the instruction: 'Enter a network name (SSID) for your wireless network. Any name can be used, but the same name must be used with all other stations in the network.' There are three main settings: 'Connect to ANY SSID' (checkbox, unchecked), 'SSID' (text field, 'Beta'), and 'Wireless mode' (dropdown menu, '2.4 GHz 11 Mbps (802.11b)'). At the bottom of the window, there are three buttons: '<< Back', 'Next >>', and 'Cancel'. The 'Next >>' button is highlighted with a red rectangular box.</p>

No.	Action	Comment
7.	Select the antenna you have installed on the W746-1 from the selection box. If your antenna is not displayed in the list or you have not installed an antenna, select User defined . Click Next to go to the next configuration window.	
8.	For reasons of accessibility, all devices that are connected to the Ethernet interface of the W746-1 need a MAC address. If more than one node is installed downstream the SCALANCE W746-1 - as with this configuration -, the Layer 2 Tunneling function can be used. Select Layer 2 Tunnel as a MAC mode. Click Next to go to the final step.	
9.	Once the Basic Wizard is complete, an overview of the parameters entered is displayed. Exit the wizard with Finish to accept all settings.	
10.	Restart the SCALANCE W746-1 by clicking System > Restart . Log on to the web-based management again after the restart. The Basic Wizard is thus complete.	

No.	Action	Comment
11.	The security settings are made in the next steps. Open the Security Wizard by clicking wizards-> security . On the first page, you can change the administrator password for the web-based management. Skip this setting with Next .	
12.	Do not change the default settings in the next step and proceed with Next .	
13.	Change the write permission of SNMP variables into public and click Next to go to the next configuration.	

No.	Action	Comment														
14.	Select High (WPA2) and Cipher AUTO as a security level . Click Next to go to the next step.	 <p>Security Settings for WLAN</p> <p>Choose wireless Security level.</p> <p>Security level: High (WPA2)</p> <p>Cipher: AUTO</p> <p>Security level: High Authentication type: WPA2 Encryption: Enabled Cipher: AUTO</p> <p><< Back Next >> Cancel</p>														
15.	Enter a user name (here: W746) and a password (here: RADIUS_Authentication) which the SCALANCE can use to log on to the RADIUS server. Note: Note the user name and password for the configuration of the RADIUS server. Click Next to go to the next step.	 <p>802.1x User Name and Password Configuration</p> <p>The Dot1x User Name and Password are required to communicate with 802.1x Server.</p> <p>Dot1x user name: W746</p> <p>Dot1x user password:</p> <p>Password confirmation:</p> <p><< Back Next >> Cancel</p>														
16.	You can exit the Security Wizard with Next .	 <p>Following Settings Were Made</p> <table border="1"> <tr><td>CLI:</td><td>Enabled</td></tr> <tr><td>WEB interface:</td><td>Enabled</td></tr> <tr><td>SNMPv1:</td><td>Enabled</td></tr> <tr><td>Management only from Ethernet:</td><td>Disabled</td></tr> <tr><td>SNMPv1 read only:</td><td>Enabled</td></tr> <tr><td>Intracell communication for WLAN:</td><td>Allowed</td></tr> <tr><td>Security level for WLAN:</td><td>High</td></tr> </table> <p><< Back Next >> Cancel</p>	CLI:	Enabled	WEB interface:	Enabled	SNMPv1:	Enabled	Management only from Ethernet:	Disabled	SNMPv1 read only:	Enabled	Intracell communication for WLAN:	Allowed	Security level for WLAN:	High
CLI:	Enabled															
WEB interface:	Enabled															
SNMPv1:	Enabled															
Management only from Ethernet:	Disabled															
SNMPv1 read only:	Enabled															
Intracell communication for WLAN:	Allowed															
Security level for WLAN:	High															
17.	Close the Security Wizard with Finish .	 <p>Finished</p> <p>Congratulations! You have checked all security settings.</p> <p>For more security level by management access you can use <u>ACCESS IP LIST</u> to allow or deny some IP addresses.</p> <p>Important: Press the 'Finish' button to adopt the changes!</p> <p><< Back Finish</p>														

No.	Action	Comment	
18.	Restart the SCALANCE W746-1 by clicking system -> Restart .		
19.	Navigate to system -> SNMP and enter private under read community string . Confirm with Set Values .		
20.	Reconnect the server PC to port 9.3 of the SCALANCE X414-3E.		

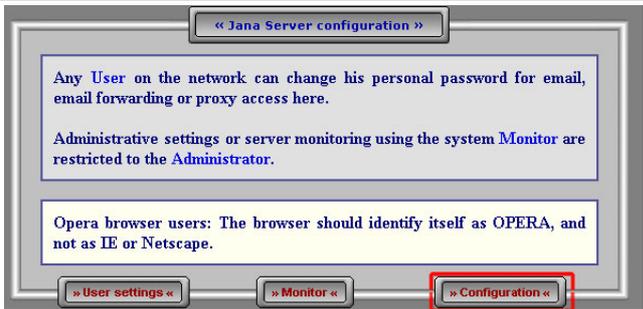
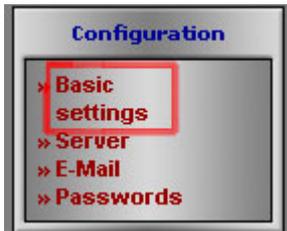
5.4 Configuration of the FTP server

The configuration of the FTP server is demonstrated using the JanaServer freeware tool.

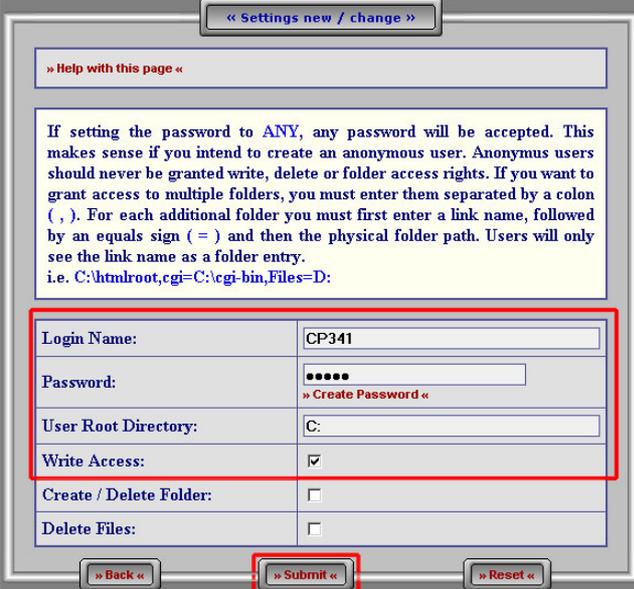
Note

The Internet Explorer of the Win2003 operating system has high security settings and the configuration page of the JanaServer might be blocked. Enter the HTML address of the configuration page into the list of trusted pages.

Table 5-8

No.	Action	Comment
1.	Start the configuration page of the JanaServer by clicking Start->Programs->JanaServer 2->Administration.	
2.	Click Configuration.	
3.	Select the menu item Basic Settings in the Configuration navigation box.	
4.	Click the submenu IP addresses in the Basic Settings menu item.	

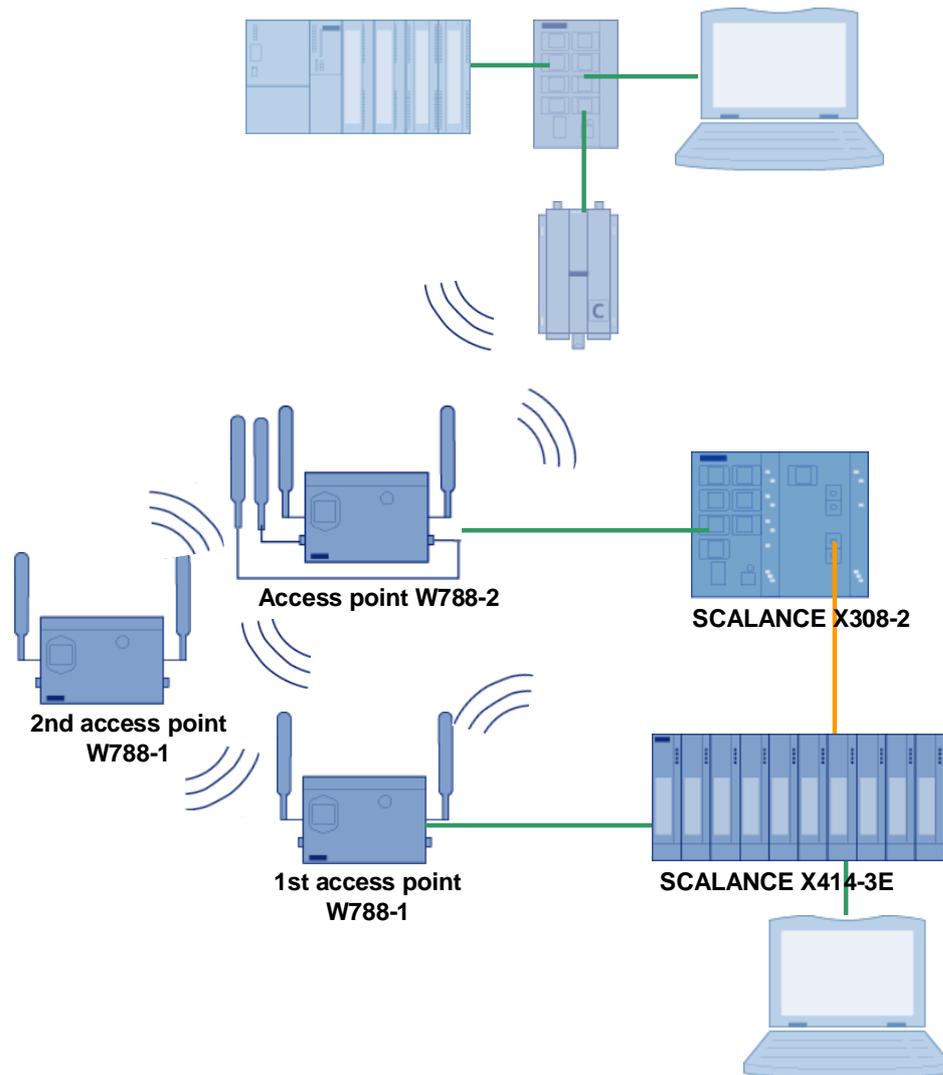
No.	Action	Comment																		
5.	Enter the additional IP address 172.158.1.7 under Settings of IP Addresses . The IP addresses are separated by commas. Confirm with Submit .																			
6.	Activate the FTP-Server both for the Local host (127.0.0.) and the PC (172.158.1.7). Scroll down the HTML page and accept your setting with Submit .	<table border="1" data-bbox="751 1084 1326 1285"> <thead> <tr> <th>Function</th> <th>127.0.0.1</th> <th>172.158.1.7</th> </tr> </thead> <tbody> <tr> <td>Http / Ftp Proxy</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Http Server</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>SSL Http Server</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr style="border: 2px solid red;"> <td>Ftp Server</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>SSL Ftp-Server</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Function	127.0.0.1	172.158.1.7	Http / Ftp Proxy	<input type="checkbox"/>	<input type="checkbox"/>	Http Server	<input type="checkbox"/>	<input type="checkbox"/>	SSL Http Server	<input type="checkbox"/>	<input type="checkbox"/>	Ftp Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SSL Ftp-Server	<input type="checkbox"/>	<input type="checkbox"/>
Function	127.0.0.1	172.158.1.7																		
Http / Ftp Proxy	<input type="checkbox"/>	<input type="checkbox"/>																		
Http Server	<input type="checkbox"/>	<input type="checkbox"/>																		
SSL Http Server	<input type="checkbox"/>	<input type="checkbox"/>																		
Ftp Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>																		
SSL Ftp-Server	<input type="checkbox"/>	<input type="checkbox"/>																		
7.	Restart the PC.																			
8.	Navigate to Server in the Navigation box Home .																			

No.	Action	Comment
9.	Finally click FTP server in the Navigation box Server .	
10.	Scroll down the web site to the end and create a new user with New under FTP Server User .	
11.	<p>Enter CP341 as a Login Name and admin as a password. You can enter the Path where the file of the CP343-1 IT is to be filed under User Root Directory. (Here: C:\). Provide the user with write permissions. Confirm your entry with Submit.</p> <p>Note: The login data for the user are stored in the DB10 data block and can be opened and edited using the SIMATIC MANAGER.</p>	
12.	Restart the PC.	

5.5 Configuration of the redundancy method RSTP

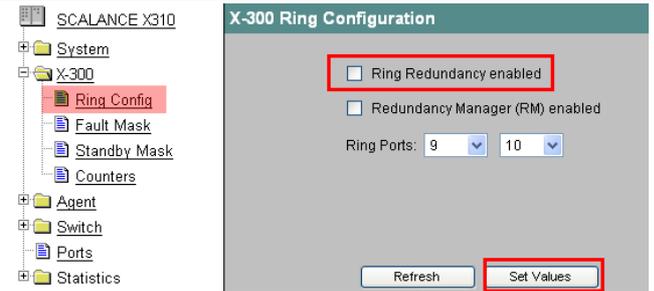
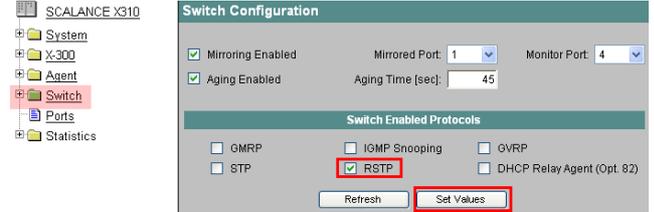
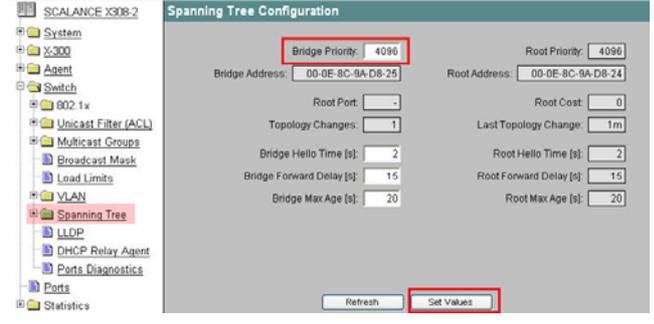
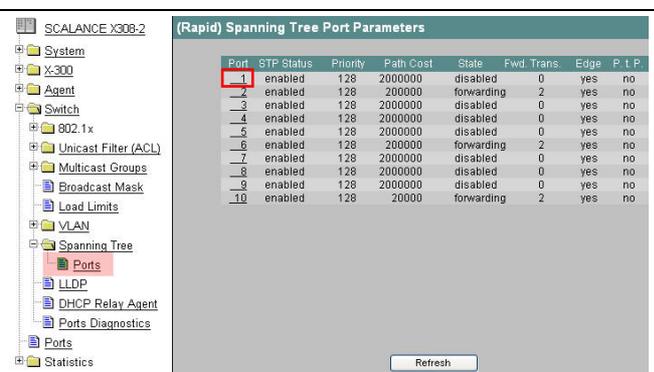
The **rapid spanning tree** function is configured in **all** SCALANCE X modules and access points.

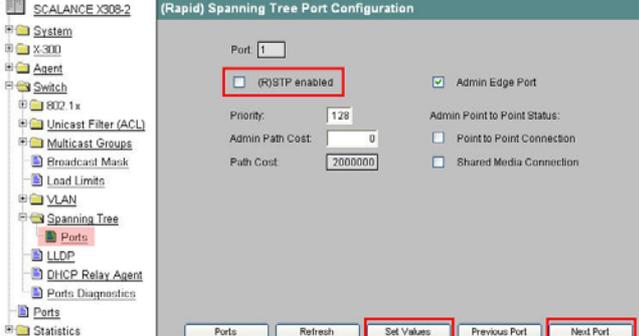
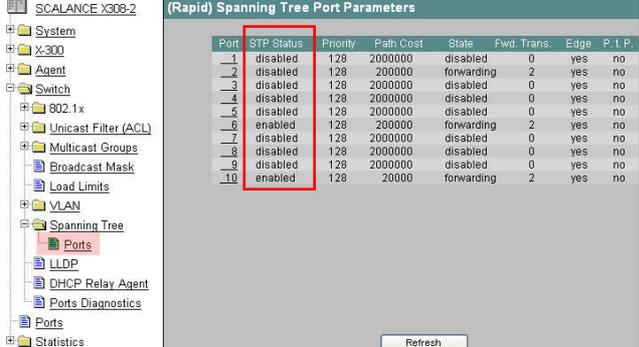
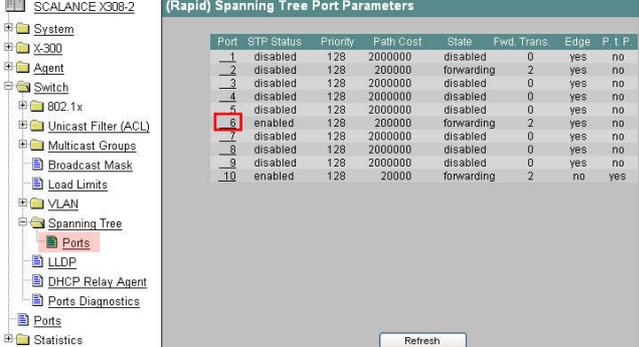
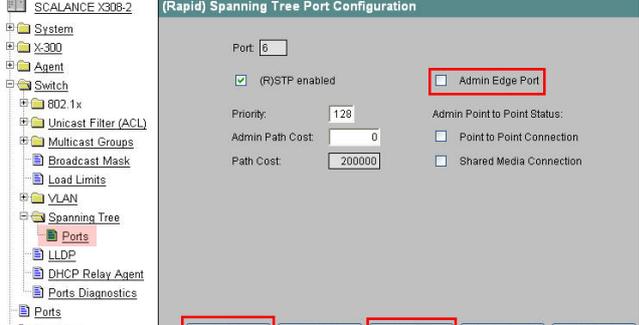
Figure 5-3



RSTP in SCALANCE X308-2

Table 5-9

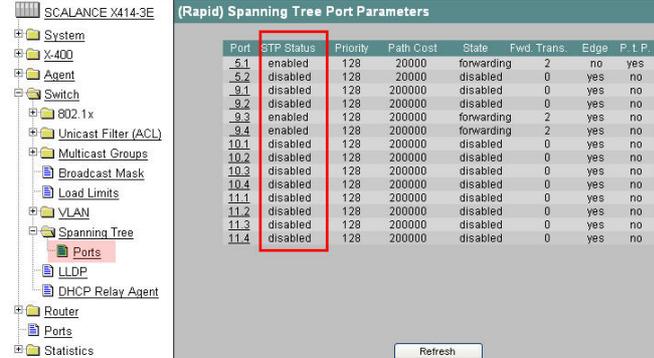
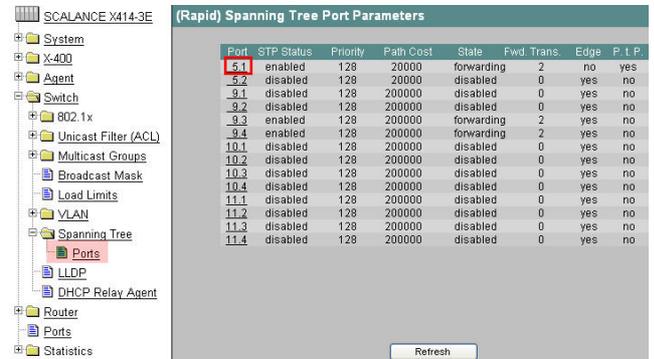
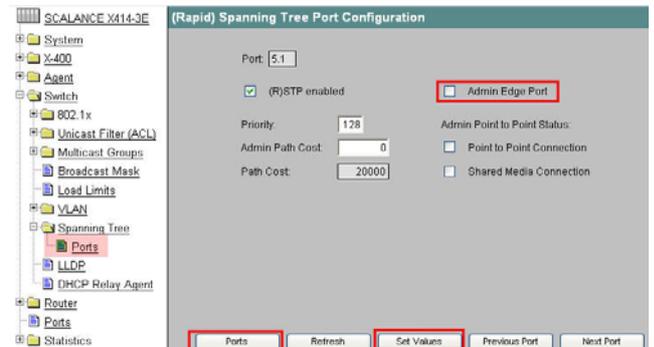
No.	Action	Comment																																																																																								
1.	Open the web-based management for the SCALANCE X308-2.	http://172.158.1.5																																																																																								
2.	For the rapid spanning tree protocol, the ring redundancy must be switched off in the SCALANCE. Navigate to X-300->Ring Config and switch off the ring redundancy. Confirm the action with Set Values .																																																																																									
3.	Click Switch in the navigation bar. Activate RSTP and confirm your selection with Set Values .																																																																																									
4.	You can change the bridge priority under Switch->Spanning Tree . The switch with the lowest bridge ID becomes the root bridge . Change the value to 4096 . This ensures that the SCALANCE X308-2 becomes the root bridge. Save the settings with Set Values .																																																																																									
5.	Only the RSTP ports are to be used in this application. For an overview table of the individual ports, refer to switch->Spanning Tree->Ports . All ports that are not needed must not use RSTP either. First of all, click port 1.	 <table border="1"> <thead> <tr> <th>Port</th> <th>STP Status</th> <th>Priority</th> <th>Path Cost</th> <th>State</th> <th>Fwd. Trans.</th> <th>Edge</th> <th>P. I. P.</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>enabled</td> <td>128</td> <td>2000000</td> <td>disabled</td> <td>0</td> <td>yes</td> <td>no</td> </tr> <tr> <td>2</td> <td>enabled</td> <td>128</td> <td>2000000</td> <td>forwarding</td> <td>2</td> <td>yes</td> <td>no</td> </tr> <tr> <td>3</td> <td>enabled</td> <td>128</td> <td>2000000</td> <td>disabled</td> <td>0</td> <td>yes</td> <td>no</td> </tr> <tr> <td>4</td> <td>enabled</td> <td>128</td> <td>2000000</td> <td>disabled</td> <td>0</td> <td>yes</td> <td>no</td> </tr> <tr> <td>5</td> <td>enabled</td> <td>128</td> <td>2000000</td> <td>disabled</td> <td>0</td> <td>yes</td> <td>no</td> </tr> <tr> <td>6</td> <td>enabled</td> <td>128</td> <td>2000000</td> <td>forwarding</td> <td>2</td> <td>yes</td> <td>no</td> </tr> <tr> <td>7</td> <td>enabled</td> <td>128</td> <td>2000000</td> <td>disabled</td> <td>0</td> <td>yes</td> <td>no</td> </tr> <tr> <td>8</td> <td>enabled</td> <td>128</td> <td>2000000</td> <td>disabled</td> <td>0</td> <td>yes</td> <td>no</td> </tr> <tr> <td>9</td> <td>enabled</td> <td>128</td> <td>2000000</td> <td>disabled</td> <td>0</td> <td>yes</td> <td>no</td> </tr> <tr> <td>10</td> <td>enabled</td> <td>128</td> <td>200000</td> <td>forwarding</td> <td>2</td> <td>yes</td> <td>no</td> </tr> </tbody> </table>	Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P. I. P.	1	enabled	128	2000000	disabled	0	yes	no	2	enabled	128	2000000	forwarding	2	yes	no	3	enabled	128	2000000	disabled	0	yes	no	4	enabled	128	2000000	disabled	0	yes	no	5	enabled	128	2000000	disabled	0	yes	no	6	enabled	128	2000000	forwarding	2	yes	no	7	enabled	128	2000000	disabled	0	yes	no	8	enabled	128	2000000	disabled	0	yes	no	9	enabled	128	2000000	disabled	0	yes	no	10	enabled	128	200000	forwarding	2	yes	no
Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P. I. P.																																																																																			
1	enabled	128	2000000	disabled	0	yes	no																																																																																			
2	enabled	128	2000000	forwarding	2	yes	no																																																																																			
3	enabled	128	2000000	disabled	0	yes	no																																																																																			
4	enabled	128	2000000	disabled	0	yes	no																																																																																			
5	enabled	128	2000000	disabled	0	yes	no																																																																																			
6	enabled	128	2000000	forwarding	2	yes	no																																																																																			
7	enabled	128	2000000	disabled	0	yes	no																																																																																			
8	enabled	128	2000000	disabled	0	yes	no																																																																																			
9	enabled	128	2000000	disabled	0	yes	no																																																																																			
10	enabled	128	200000	forwarding	2	yes	no																																																																																			

No.	Action	Comment																																																																																								
6.	Deactivate the RSTP for this port and confirm with Set Values . Upon clicking the Next Port button, the same window as for port 2 appears automatically. Deactivate the RSTP for all ports that are not used, i.e. all except for port 6 and 10.																																																																																									
7.	The port table shows what port is activated or deactivated for RSTP.	 <table border="1" data-bbox="879 775 1350 943"> <thead> <tr> <th>Port</th> <th>STP Status</th> <th>Priority</th> <th>Path Cost</th> <th>State</th> <th>Fwd. Trans.</th> <th>Edge</th> <th>P. T. P.</th> </tr> </thead> <tbody> <tr><td>1</td><td>disabled</td><td>128</td><td>2000000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>2</td><td>disabled</td><td>128</td><td>200000</td><td>forwarding</td><td>2</td><td>yes</td><td>no</td></tr> <tr><td>3</td><td>disabled</td><td>128</td><td>2000000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>4</td><td>disabled</td><td>128</td><td>2000000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>5</td><td>disabled</td><td>128</td><td>2000000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>6</td><td>enabled</td><td>128</td><td>200000</td><td>forwarding</td><td>2</td><td>yes</td><td>no</td></tr> <tr><td>7</td><td>disabled</td><td>128</td><td>2000000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>8</td><td>disabled</td><td>128</td><td>2000000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>9</td><td>disabled</td><td>128</td><td>2000000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10</td><td>enabled</td><td>128</td><td>200000</td><td>forwarding</td><td>2</td><td>yes</td><td>no</td></tr> </tbody> </table>	Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P. T. P.	1	disabled	128	2000000	disabled	0	yes	no	2	disabled	128	200000	forwarding	2	yes	no	3	disabled	128	2000000	disabled	0	yes	no	4	disabled	128	2000000	disabled	0	yes	no	5	disabled	128	2000000	disabled	0	yes	no	6	enabled	128	200000	forwarding	2	yes	no	7	disabled	128	2000000	disabled	0	yes	no	8	disabled	128	2000000	disabled	0	yes	no	9	disabled	128	2000000	disabled	0	yes	no	10	enabled	128	200000	forwarding	2	yes	no
Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P. T. P.																																																																																			
1	disabled	128	2000000	disabled	0	yes	no																																																																																			
2	disabled	128	200000	forwarding	2	yes	no																																																																																			
3	disabled	128	2000000	disabled	0	yes	no																																																																																			
4	disabled	128	2000000	disabled	0	yes	no																																																																																			
5	disabled	128	2000000	disabled	0	yes	no																																																																																			
6	enabled	128	200000	forwarding	2	yes	no																																																																																			
7	disabled	128	2000000	disabled	0	yes	no																																																																																			
8	disabled	128	2000000	disabled	0	yes	no																																																																																			
9	disabled	128	2000000	disabled	0	yes	no																																																																																			
10	enabled	128	200000	forwarding	2	yes	no																																																																																			
8.	Since port 6 and 10 are connected to another SCALANCE, the tick for the end node must be removed for these ports. Click port 6 in the port table.																																																																																									
9.	Deactivate the Admin Edge Port and confirm with Set Values . Click Port to get back to the port table. Repeat the procedure for port 10 .																																																																																									

RSTP in the SCALANCE X414-3E

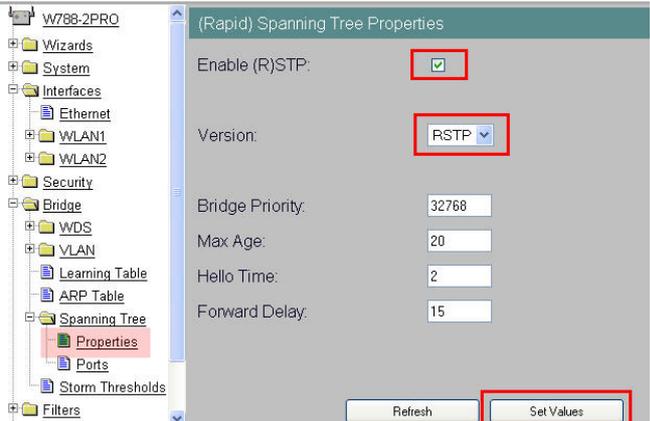
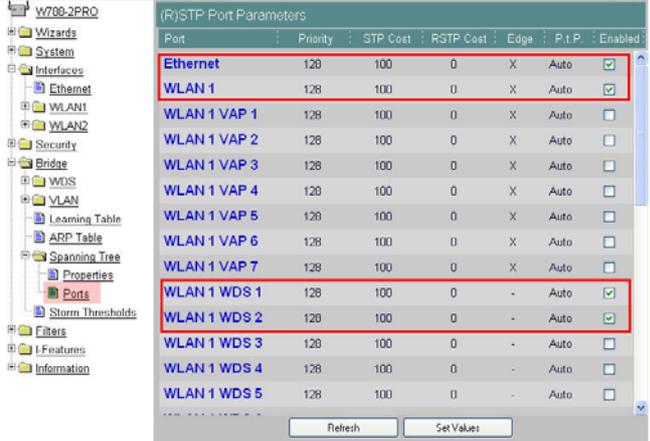
Table 5-10

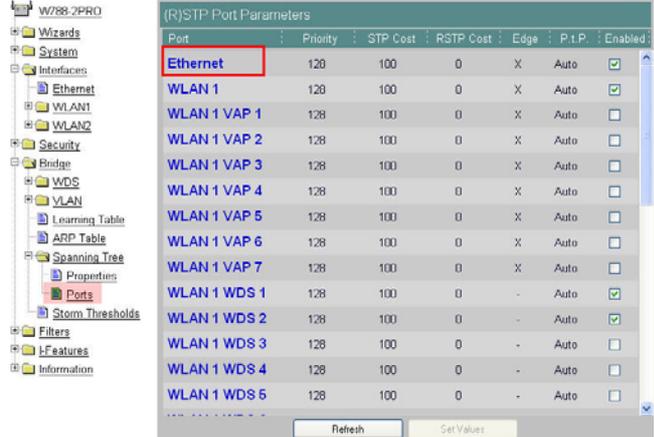
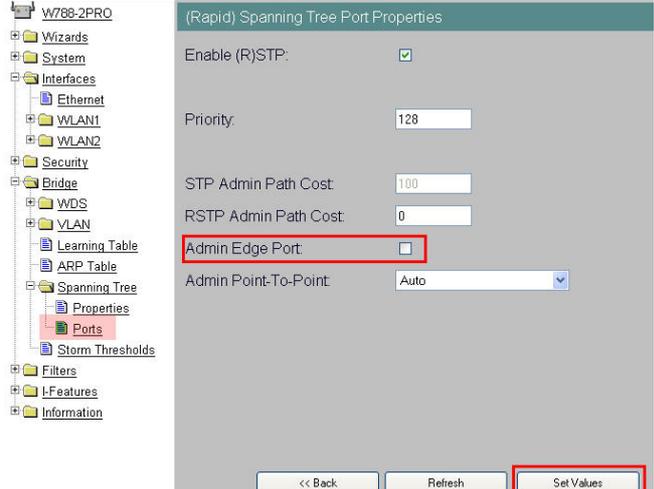
No.	Action	Comment																																																																																																																																																						
1.	Set the DIP switch on the SCALANCE X414-3E to the position shown to the right. The DIP switches are located in module 4.	RM → Off STBY → Off R1 → On R2 → On																																																																																																																																																						
2.	After changing the DIP switch, the SCALANCE must be restarted. Briefly switch the voltage supply of the SCALANCE X414-3E off and switch it on again.																																																																																																																																																							
3.	Open the web-based management for the SCALANCE X414-3E.	http://172.158.1.4																																																																																																																																																						
4.	Click Switch in the navigation bar. Activate RSTP and confirm your selection with Set Values .																																																																																																																																																							
5.	Only the RSTP ports are to be used in this application. For an overview table of the individual ports, refer to Switch-> Spanning Tree ->Ports . All ports that are not needed must not use RSTP either. First of all, click port 5.2.	<table border="1"> <thead> <tr> <th>Port</th> <th>STP Status</th> <th>Priority</th> <th>Path Cost</th> <th>State</th> <th>Fwd Trans.</th> <th>Edge</th> <th>P</th> <th>T</th> <th>P</th> </tr> </thead> <tbody> <tr><td>5.1</td><td>enabled</td><td>128</td><td>20000</td><td>forwarding</td><td>2</td><td>no</td><td>yes</td><td>no</td><td>no</td></tr> <tr><td>5.2</td><td>enabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>9.1</td><td>enabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>9.2</td><td>enabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>9.3</td><td>enabled</td><td>128</td><td>200000</td><td>forwarding</td><td>2</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>9.4</td><td>enabled</td><td>128</td><td>200000</td><td>forwarding</td><td>2</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>10.1</td><td>enabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>10.2</td><td>enabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>10.3</td><td>enabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>10.4</td><td>enabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>11.1</td><td>enabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>11.2</td><td>enabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>11.3</td><td>enabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> <tr><td>11.4</td><td>enabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td><td>no</td><td>no</td></tr> </tbody> </table>	Port	STP Status	Priority	Path Cost	State	Fwd Trans.	Edge	P	T	P	5.1	enabled	128	20000	forwarding	2	no	yes	no	no	5.2	enabled	128	20000	disabled	0	yes	no	no	no	9.1	enabled	128	200000	disabled	0	yes	no	no	no	9.2	enabled	128	200000	disabled	0	yes	no	no	no	9.3	enabled	128	200000	forwarding	2	yes	no	no	no	9.4	enabled	128	200000	forwarding	2	yes	no	no	no	10.1	enabled	128	200000	disabled	0	yes	no	no	no	10.2	enabled	128	200000	disabled	0	yes	no	no	no	10.3	enabled	128	200000	disabled	0	yes	no	no	no	10.4	enabled	128	200000	disabled	0	yes	no	no	no	11.1	enabled	128	200000	disabled	0	yes	no	no	no	11.2	enabled	128	200000	disabled	0	yes	no	no	no	11.3	enabled	128	200000	disabled	0	yes	no	no	no	11.4	enabled	128	200000	disabled	0	yes	no	no	no
Port	STP Status	Priority	Path Cost	State	Fwd Trans.	Edge	P	T	P																																																																																																																																															
5.1	enabled	128	20000	forwarding	2	no	yes	no	no																																																																																																																																															
5.2	enabled	128	20000	disabled	0	yes	no	no	no																																																																																																																																															
9.1	enabled	128	200000	disabled	0	yes	no	no	no																																																																																																																																															
9.2	enabled	128	200000	disabled	0	yes	no	no	no																																																																																																																																															
9.3	enabled	128	200000	forwarding	2	yes	no	no	no																																																																																																																																															
9.4	enabled	128	200000	forwarding	2	yes	no	no	no																																																																																																																																															
10.1	enabled	128	200000	disabled	0	yes	no	no	no																																																																																																																																															
10.2	enabled	128	200000	disabled	0	yes	no	no	no																																																																																																																																															
10.3	enabled	128	200000	disabled	0	yes	no	no	no																																																																																																																																															
10.4	enabled	128	200000	disabled	0	yes	no	no	no																																																																																																																																															
11.1	enabled	128	200000	disabled	0	yes	no	no	no																																																																																																																																															
11.2	enabled	128	200000	disabled	0	yes	no	no	no																																																																																																																																															
11.3	enabled	128	200000	disabled	0	yes	no	no	no																																																																																																																																															
11.4	enabled	128	200000	disabled	0	yes	no	no	no																																																																																																																																															
6.	Deactivate RSTP for this port and confirm with Set Values . Upon clicking the Next Port button, the same window is displayed automatically for port 9.1. Deactivate RSTP for all ports that are not used, i.e. for all except for ports 5.1, 9.3 and 9.4.																																																																																																																																																							

No.	Action	Comment																																																																																																																								
7.	The port table shows what port is activated or deactivated for RSTP.	 <p>(Rapid) Spanning Tree Port Parameters</p> <table border="1"> <thead> <tr> <th>Port</th> <th>STP Status</th> <th>Priority</th> <th>Path Cost</th> <th>State</th> <th>Fwd. Trans.</th> <th>Edge</th> <th>P.t.P.</th> </tr> </thead> <tbody> <tr><td>5.1</td><td>enabled</td><td>128</td><td>20000</td><td>forwarding</td><td>2</td><td>no</td><td>yes</td></tr> <tr><td>5.2</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>9.1</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>9.2</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>9.3</td><td>enabled</td><td>128</td><td>200000</td><td>forwarding</td><td>2</td><td>yes</td><td>no</td></tr> <tr><td>9.4</td><td>enabled</td><td>128</td><td>200000</td><td>forwarding</td><td>2</td><td>yes</td><td>no</td></tr> <tr><td>10.1</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.2</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.3</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.4</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.1</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.2</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.3</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.4</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> </tbody> </table>	Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P.t.P.	5.1	enabled	128	20000	forwarding	2	no	yes	5.2	disabled	128	20000	disabled	0	yes	no	9.1	disabled	128	200000	disabled	0	yes	no	9.2	disabled	128	200000	disabled	0	yes	no	9.3	enabled	128	200000	forwarding	2	yes	no	9.4	enabled	128	200000	forwarding	2	yes	no	10.1	disabled	128	200000	disabled	0	yes	no	10.2	disabled	128	200000	disabled	0	yes	no	10.3	disabled	128	200000	disabled	0	yes	no	10.4	disabled	128	200000	disabled	0	yes	no	11.1	disabled	128	200000	disabled	0	yes	no	11.2	disabled	128	200000	disabled	0	yes	no	11.3	disabled	128	200000	disabled	0	yes	no	11.4	disabled	128	200000	disabled	0	yes	no
Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P.t.P.																																																																																																																			
5.1	enabled	128	20000	forwarding	2	no	yes																																																																																																																			
5.2	disabled	128	20000	disabled	0	yes	no																																																																																																																			
9.1	disabled	128	200000	disabled	0	yes	no																																																																																																																			
9.2	disabled	128	200000	disabled	0	yes	no																																																																																																																			
9.3	enabled	128	200000	forwarding	2	yes	no																																																																																																																			
9.4	enabled	128	200000	forwarding	2	yes	no																																																																																																																			
10.1	disabled	128	200000	disabled	0	yes	no																																																																																																																			
10.2	disabled	128	200000	disabled	0	yes	no																																																																																																																			
10.3	disabled	128	200000	disabled	0	yes	no																																																																																																																			
10.4	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.1	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.2	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.3	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.4	disabled	128	200000	disabled	0	yes	no																																																																																																																			
8.	Since port 5.1 and 9.3 are connected to another SCALANCE, the tick for the end node must be removed for these ports. Click port 5.1 in the port table.	 <p>(Rapid) Spanning Tree Port Parameters</p> <table border="1"> <thead> <tr> <th>Port</th> <th>STP Status</th> <th>Priority</th> <th>Path Cost</th> <th>State</th> <th>Fwd. Trans.</th> <th>Edge</th> <th>P.t.P.</th> </tr> </thead> <tbody> <tr><td>5.1</td><td>enabled</td><td>128</td><td>20000</td><td>forwarding</td><td>2</td><td>no</td><td>yes</td></tr> <tr><td>5.2</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>9.1</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>9.2</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>9.3</td><td>disabled</td><td>128</td><td>200000</td><td>forwarding</td><td>2</td><td>yes</td><td>no</td></tr> <tr><td>9.4</td><td>enabled</td><td>128</td><td>200000</td><td>forwarding</td><td>2</td><td>yes</td><td>no</td></tr> <tr><td>10.1</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.2</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.3</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.4</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.1</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.2</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.3</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.4</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> </tbody> </table>	Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P.t.P.	5.1	enabled	128	20000	forwarding	2	no	yes	5.2	disabled	128	20000	disabled	0	yes	no	9.1	disabled	128	200000	disabled	0	yes	no	9.2	disabled	128	200000	disabled	0	yes	no	9.3	disabled	128	200000	forwarding	2	yes	no	9.4	enabled	128	200000	forwarding	2	yes	no	10.1	disabled	128	200000	disabled	0	yes	no	10.2	disabled	128	200000	disabled	0	yes	no	10.3	disabled	128	200000	disabled	0	yes	no	10.4	disabled	128	200000	disabled	0	yes	no	11.1	disabled	128	200000	disabled	0	yes	no	11.2	disabled	128	200000	disabled	0	yes	no	11.3	disabled	128	200000	disabled	0	yes	no	11.4	disabled	128	200000	disabled	0	yes	no
Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P.t.P.																																																																																																																			
5.1	enabled	128	20000	forwarding	2	no	yes																																																																																																																			
5.2	disabled	128	20000	disabled	0	yes	no																																																																																																																			
9.1	disabled	128	200000	disabled	0	yes	no																																																																																																																			
9.2	disabled	128	200000	disabled	0	yes	no																																																																																																																			
9.3	disabled	128	200000	forwarding	2	yes	no																																																																																																																			
9.4	enabled	128	200000	forwarding	2	yes	no																																																																																																																			
10.1	disabled	128	200000	disabled	0	yes	no																																																																																																																			
10.2	disabled	128	200000	disabled	0	yes	no																																																																																																																			
10.3	disabled	128	200000	disabled	0	yes	no																																																																																																																			
10.4	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.1	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.2	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.3	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.4	disabled	128	200000	disabled	0	yes	no																																																																																																																			
9.	Deactivate the Admin Edge Port and confirm with Set Values . Click Port to get back to the port table. Repeat the procedure for port 9.3.	 <p>(Rapid) Spanning Tree Port Configuration</p> <p>Port: 5.1</p> <p><input checked="" type="checkbox"/> (R)STP enabled <input type="checkbox"/> Admin Edge Port</p> <p>Priority: 128 Admin Point to Point Status:</p> <p>Admin Path Cost: 0 <input type="checkbox"/> Point to Point Connection</p> <p>Path Cost: 20000 <input type="checkbox"/> Shared Media Connection</p> <p>Buttons: Port, Refresh, Set Values, Previous Port, Next Port</p>																																																																																																																								

RSTP in the SCALANCE W

Table 5-11

No.	Action	Comment																																																																																																									
1.	Open the web-based management for the SCALANCE W788-2.	http://172.158.1.3																																																																																																									
2.	Click Bridge->Spanning Tree->Properties in the navigation bar. Activate RSTP , select RSTP as a version and confirm your selection with Set Values .																																																																																																										
3.	<p>Only the RSTP ports are to be used in this application. For an overview table of the individual ports, refer to Bridge-> Spanning Tree ->Ports. All ports that are not needed must not use RSTP either. Deactivate all boxes except for</p> <ul style="list-style-type: none"> • Ethernet, • WLAN 1, • WLAN 1 • WDS 1, • WLAN 1 • WDS 2, • WLAN 2 • Redundancy. <p>Confirm with Set Values.</p>	 <table border="1" data-bbox="871 1055 1369 1487"> <thead> <tr> <th>Port</th> <th>Priority</th> <th>STP Cost</th> <th>RSTP Cost</th> <th>Edge</th> <th>P. I.P.</th> <th>Enabled</th> </tr> </thead> <tbody> <tr><td>Ethernet</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>WLAN 1</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 1</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 2</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 3</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 4</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 5</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 6</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 7</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 WDS 1</td><td>128</td><td>100</td><td>0</td><td>-</td><td>Auto</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>WLAN 1 WDS 2</td><td>128</td><td>100</td><td>0</td><td>-</td><td>Auto</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>WLAN 1 WDS 3</td><td>128</td><td>100</td><td>0</td><td>-</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 WDS 4</td><td>128</td><td>100</td><td>0</td><td>-</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 WDS 5</td><td>128</td><td>100</td><td>0</td><td>-</td><td>Auto</td><td><input type="checkbox"/></td></tr> </tbody> </table>	Port	Priority	STP Cost	RSTP Cost	Edge	P. I.P.	Enabled	Ethernet	128	100	0	X	Auto	<input checked="" type="checkbox"/>	WLAN 1	128	100	0	X	Auto	<input checked="" type="checkbox"/>	WLAN 1 VAP 1	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 2	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 3	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 4	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 5	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 6	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 7	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 WDS 1	128	100	0	-	Auto	<input checked="" type="checkbox"/>	WLAN 1 WDS 2	128	100	0	-	Auto	<input checked="" type="checkbox"/>	WLAN 1 WDS 3	128	100	0	-	Auto	<input type="checkbox"/>	WLAN 1 WDS 4	128	100	0	-	Auto	<input type="checkbox"/>	WLAN 1 WDS 5	128	100	0	-	Auto	<input type="checkbox"/>
Port	Priority	STP Cost	RSTP Cost	Edge	P. I.P.	Enabled																																																																																																					
Ethernet	128	100	0	X	Auto	<input checked="" type="checkbox"/>																																																																																																					
WLAN 1	128	100	0	X	Auto	<input checked="" type="checkbox"/>																																																																																																					
WLAN 1 VAP 1	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 2	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 3	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 4	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 5	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 6	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 7	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 WDS 1	128	100	0	-	Auto	<input checked="" type="checkbox"/>																																																																																																					
WLAN 1 WDS 2	128	100	0	-	Auto	<input checked="" type="checkbox"/>																																																																																																					
WLAN 1 WDS 3	128	100	0	-	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 WDS 4	128	100	0	-	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 WDS 5	128	100	0	-	Auto	<input type="checkbox"/>																																																																																																					

No.	Action	Comment																																																																																																									
4.	<p>Since the Ethernet, WLAN 1, WLAN 1 WDS 1, WLAN 1 WDS 2 and WLAN 2 ports are connected to another SCALANCE, the tick for the end node must be removed for these ports. Click the Ethernet port in the port table.</p>	 <p>The screenshot shows a tree view on the left with 'Ports' selected. The main area displays a table titled '(R)STP Port Parameters' with the following data:</p> <table border="1"> <thead> <tr> <th>Port</th> <th>Priority</th> <th>STP Cost</th> <th>RSTP Cost</th> <th>Edge</th> <th>P. t. P.</th> <th>Enabled</th> </tr> </thead> <tbody> <tr><td>Ethernet</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>WLAN 1</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 1</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 2</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 3</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 4</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 5</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 6</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 VAP 7</td><td>128</td><td>100</td><td>0</td><td>X</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 WDS 1</td><td>128</td><td>100</td><td>0</td><td>-</td><td>Auto</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>WLAN 1 WDS 2</td><td>128</td><td>100</td><td>0</td><td>-</td><td>Auto</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>WLAN 1 WDS 3</td><td>128</td><td>100</td><td>0</td><td>-</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 WDS 4</td><td>128</td><td>100</td><td>0</td><td>-</td><td>Auto</td><td><input type="checkbox"/></td></tr> <tr><td>WLAN 1 WDS 5</td><td>128</td><td>100</td><td>0</td><td>-</td><td>Auto</td><td><input type="checkbox"/></td></tr> </tbody> </table>	Port	Priority	STP Cost	RSTP Cost	Edge	P. t. P.	Enabled	Ethernet	128	100	0	X	Auto	<input checked="" type="checkbox"/>	WLAN 1	128	100	0	X	Auto	<input checked="" type="checkbox"/>	WLAN 1 VAP 1	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 2	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 3	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 4	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 5	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 6	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 VAP 7	128	100	0	X	Auto	<input type="checkbox"/>	WLAN 1 WDS 1	128	100	0	-	Auto	<input checked="" type="checkbox"/>	WLAN 1 WDS 2	128	100	0	-	Auto	<input checked="" type="checkbox"/>	WLAN 1 WDS 3	128	100	0	-	Auto	<input type="checkbox"/>	WLAN 1 WDS 4	128	100	0	-	Auto	<input type="checkbox"/>	WLAN 1 WDS 5	128	100	0	-	Auto	<input type="checkbox"/>
Port	Priority	STP Cost	RSTP Cost	Edge	P. t. P.	Enabled																																																																																																					
Ethernet	128	100	0	X	Auto	<input checked="" type="checkbox"/>																																																																																																					
WLAN 1	128	100	0	X	Auto	<input checked="" type="checkbox"/>																																																																																																					
WLAN 1 VAP 1	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 2	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 3	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 4	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 5	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 6	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 VAP 7	128	100	0	X	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 WDS 1	128	100	0	-	Auto	<input checked="" type="checkbox"/>																																																																																																					
WLAN 1 WDS 2	128	100	0	-	Auto	<input checked="" type="checkbox"/>																																																																																																					
WLAN 1 WDS 3	128	100	0	-	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 WDS 4	128	100	0	-	Auto	<input type="checkbox"/>																																																																																																					
WLAN 1 WDS 5	128	100	0	-	Auto	<input type="checkbox"/>																																																																																																					
5.	<p>Deactivate the Admin Edge Port and confirm with Set Values. Repeat the procedure for ports WLAN 1, WLAN 1 WDS 1, WLAN 1 WDS 2 and WLAN 2.</p>	 <p>The screenshot shows the '(Rapid) Spanning Tree Port Properties' dialog box. The 'Admin Edge Port' checkbox is unchecked and highlighted with a red box. The 'Set Values' button at the bottom right is also highlighted with a red box.</p>																																																																																																									

Copyright © Siemens AG 2008 All rights reserved
30805917_SCALANCE_W_OFFICE_DOKU_v10_en.doc

Repeat the procedure for both SCALANCE W788-1. Please note that these modules are only equipped with one WLAN interface, i.e. they do not have a WLAN 2 port. **Enable RSTP** only for **Ethernet, WLAN 1, WLAN 1 WDS 1** and **WLAN 1 WDS 2**, and deactivate **Admin Edge Port** on these ports.

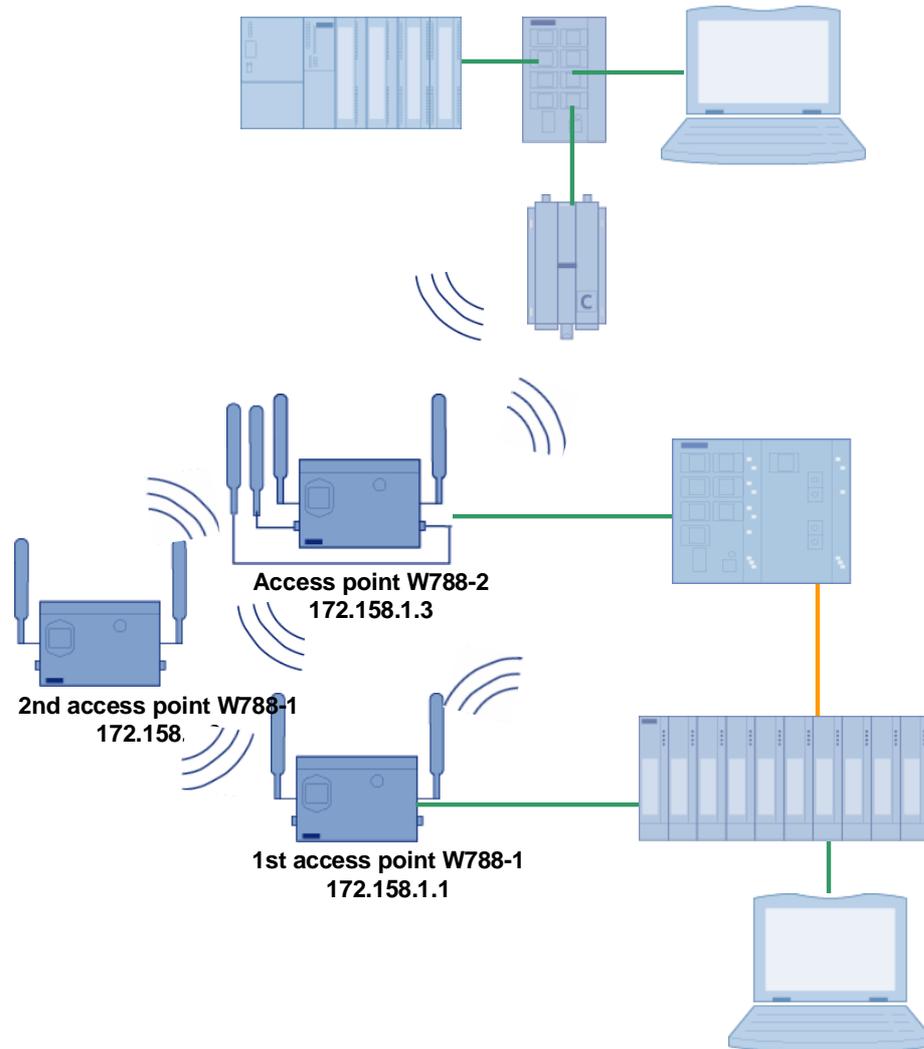
Note

To be able to configure the second SCALANCE W788-1, the server must be connected directly to the Ethernet port of the access point. After the configuration is complete, reconnect the server to the SCALANCE X414-3E.

5.6 Configuration of WDS

The WDS function is configured in all SCALANCE W78x modules.

Figure 5-4

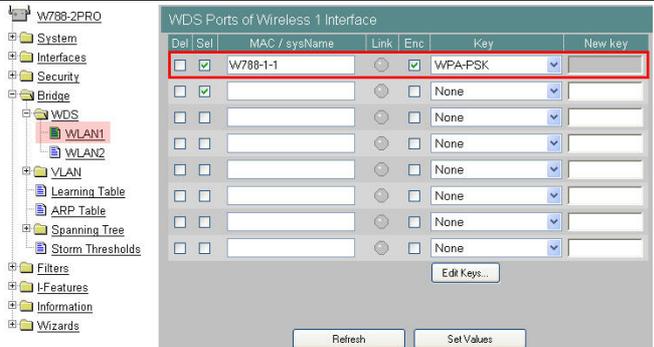
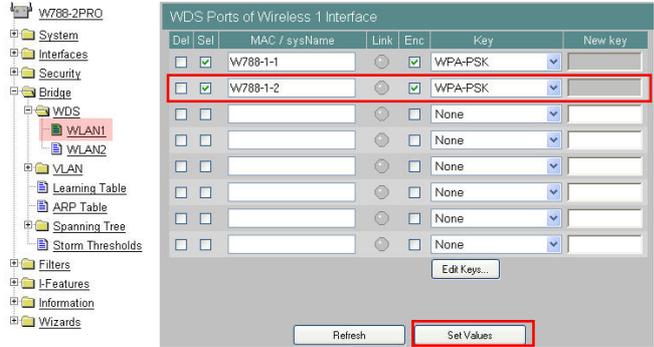


5.6.1 WDS in the SCALANCE W788-2

The SCALANCE W788-2 must establish a WDS connection to the following components using the first WLAN interface:

- First SCALANCE W788-1 (device name: W788-1-1)
- Second SCALANCE W788-1 (device name: W788-1-2)

Table 5-12

No.	Action	Comment
1.	Open the web-based management for the SCALANCE W788-2.	http://172.158.1.3
2.	Click Bridge-> WDS->WLAN1 in the navigation bar. Enter the device name of the first SCALANCE W788-1 in the first line. Tick Sel (Select) and Enc (Encryption). Select WPA-PSK as a key.	
3.	Enter the device name of the second SCALANCE W788-1 in the second line. Tick Sel (Select) and Enc (Encryption). Select WPA-PSK as a key. Confirm your entry with Set Values .	

5.6.2 WDS in the first SCALANCE W788-1

The SCALANCE W788-1 is expected to establish a WDS connection to the following components:

- SCALANCE W788-2 (device name: W788-2)
- Second SCALANCE W788-1 (device name: W788-1-2)

Table 5-13

No.	Action	Comment
1.	Open the web-based management for the SCALANCE W788-1.	http://172.158.1.1
2.	Click Bridge-> wds in the navigation bar. Enter the device name of the SCALANCE W788-2 in the first line. Tick Sel (Select) and Enc (Encryption). Select WPA-PSK as a key.	
3.	Enter the device name of the second SCALANCE W788-1 in the second line. Tick Sel (Select) and Enc (Encryption). Select WPA-PSK as a key. Confirm your entry with Set Values .	

5.6.3 WDS in the second SCALANCE W788-1

The SCALANCE W788-1 is expected to establish a WDS connection to the following components:

- SCALANCE W788-2 (device name: W788-2)
- First SCALANCE W788-1 (device name: W788-1-1)

Note

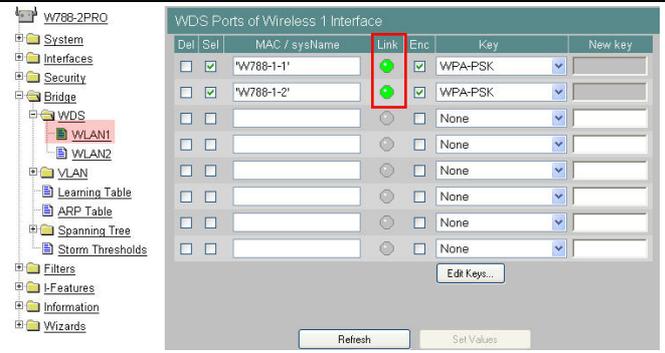
To be able to configure the second SCALANCE W788-1, the server must be connected directly to the Ethernet port of the access point. After the configuration is complete, reconnect the server to the SCALANCE X414-3E.

Table 5-14

No.	Action	Comment
1.	Open the web-based management for the SCALANCE W788-1.	http://172.158.1.2
2.	Click Bridge-> WDS in the navigation bar. Enter the device name of the SCALANCE W788-2 in the first line. Tick Sel (Select) and Enc (Encryption). Select WPA-PSK as a key.	
3.	Enter the device name of the first SCALANCE W788-1 in the second line. Tick Sel (Select) and Enc (Encryption). Select WPA-PSK as a key. Confirm your entry with Set Values .	

5.6.4 WDS link check

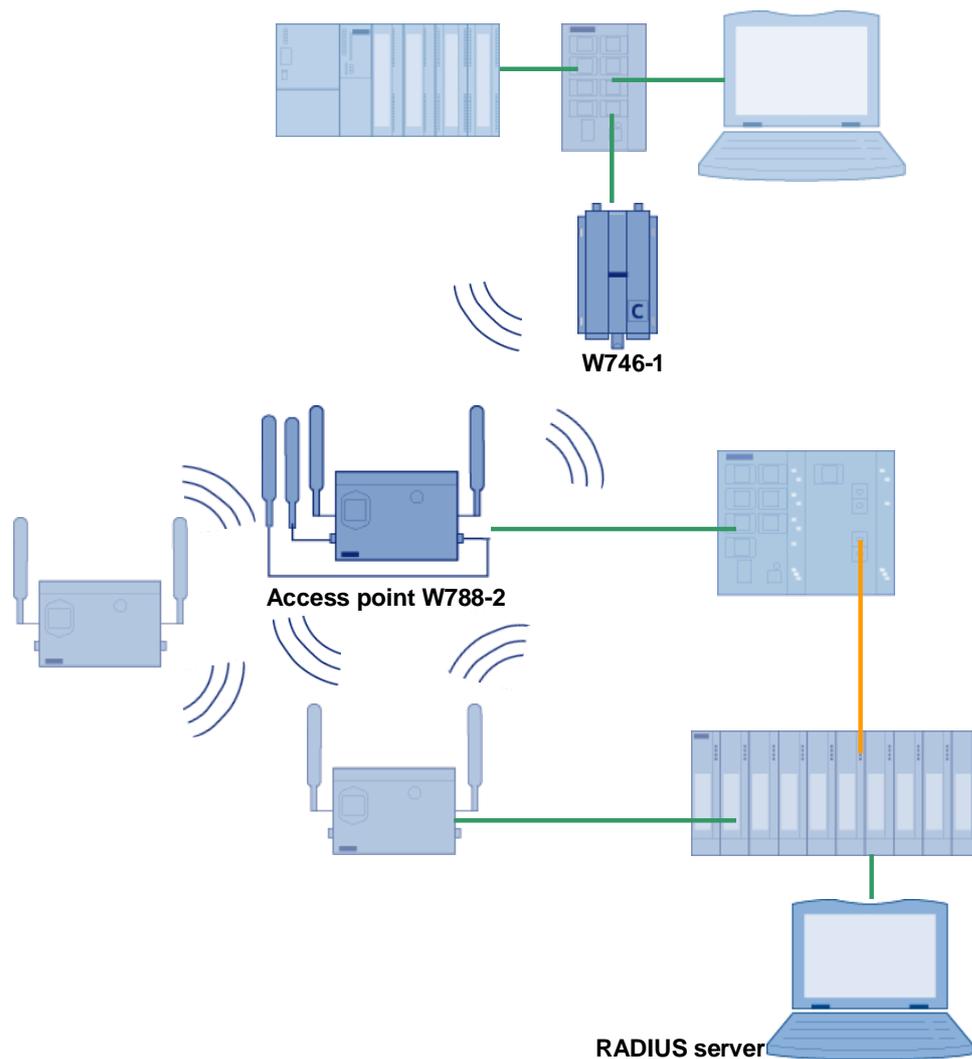
Table 5-15

No.	Action	Comment																																																															
1.	Connect the server PC to port 9.3 of the SCALANCE X414-3E.																																																																
2.	Open, for example, the web-based management for the SCALANCE W788-2.	http://172.158.1.3																																																															
3.	Click Bridge-> WDS->WLAN1 in the navigation bar. As soon as a WDS connection to the partners has been established, the link button lights up green.	 <p>The screenshot shows the 'WDS Ports of Wireless 1 Interface' configuration page. On the left is a navigation tree with 'WDS' expanded to 'WLAN1'. The main area contains a table with columns: Del, Sel, MAC / sysName, Link, Enc, Key, and New key. The 'Link' column for the entry 'W788-1-2' has a green plus sign icon, indicating a successful connection. Other entries have greyed-out link icons.</p> <table border="1"> <thead> <tr> <th>Del</th> <th>Sel</th> <th>MAC / sysName</th> <th>Link</th> <th>Enc</th> <th>Key</th> <th>New key</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>'W788-1-1'</td> <td></td> <td><input checked="" type="checkbox"/></td> <td>WPA-PSK</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>'W788-1-2'</td> <td></td> <td><input checked="" type="checkbox"/></td> <td>WPA-PSK</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> <td></td> <td><input type="checkbox"/></td> <td>None</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> <td></td> <td><input type="checkbox"/></td> <td>None</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> <td></td> <td><input type="checkbox"/></td> <td>None</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> <td></td> <td><input type="checkbox"/></td> <td>None</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> <td></td> <td><input type="checkbox"/></td> <td>None</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> <td></td> <td><input type="checkbox"/></td> <td>None</td> <td></td> </tr> </tbody> </table>	Del	Sel	MAC / sysName	Link	Enc	Key	New key	<input type="checkbox"/>	<input checked="" type="checkbox"/>	'W788-1-1'		<input checked="" type="checkbox"/>	WPA-PSK		<input type="checkbox"/>	<input checked="" type="checkbox"/>	'W788-1-2'		<input checked="" type="checkbox"/>	WPA-PSK		<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None		<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None		<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None		<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None		<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None		<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None	
Del	Sel	MAC / sysName	Link	Enc	Key	New key																																																											
<input type="checkbox"/>	<input checked="" type="checkbox"/>	'W788-1-1'		<input checked="" type="checkbox"/>	WPA-PSK																																																												
<input type="checkbox"/>	<input checked="" type="checkbox"/>	'W788-1-2'		<input checked="" type="checkbox"/>	WPA-PSK																																																												
<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None																																																												
<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None																																																												
<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None																																																												
<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None																																																												
<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None																																																												
<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	None																																																												

5.7 Configuration of the access control

On the one hand, an access list is created in the SCALANCE W746-1 for the access control. On the other hand, a RADIUS server is set up in the Win2003 server operating system and the components involved are configured.

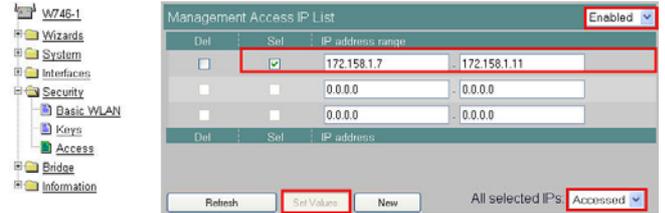
Figure 5-5



5.7.1 Access rights for IP addresses

By means of defining access rights, only specific IP addresses are allowed to access the SCALANCE module management.

Table 5-16

No.	Action	Comment
1.	Connect the server PC to the SCALANCE X108.	
2.	Open the web-based management for the SCALANCE W746-1.	http://172.158.1.8
3.	Navigate to security->Access .	
4.	Enter the IP range 172.158.1.7-172.158.1.11 . Select Set and Accessed for all IP addresses. Set the IP address range to Enable . Confirm your entry with Set Values .	

5.7.2 RADIUS server in Win2003 server

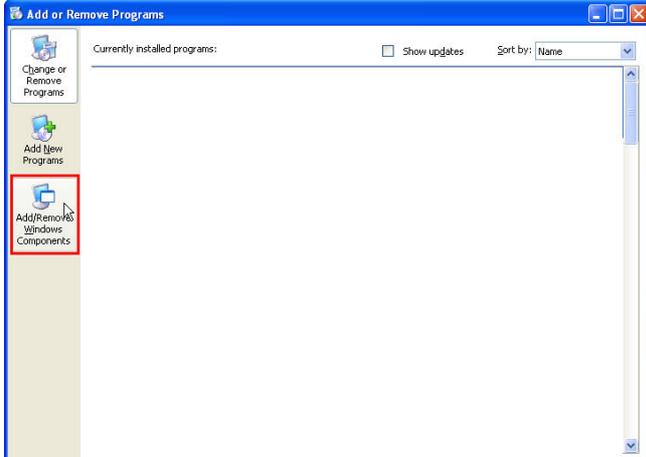
Install the IAS

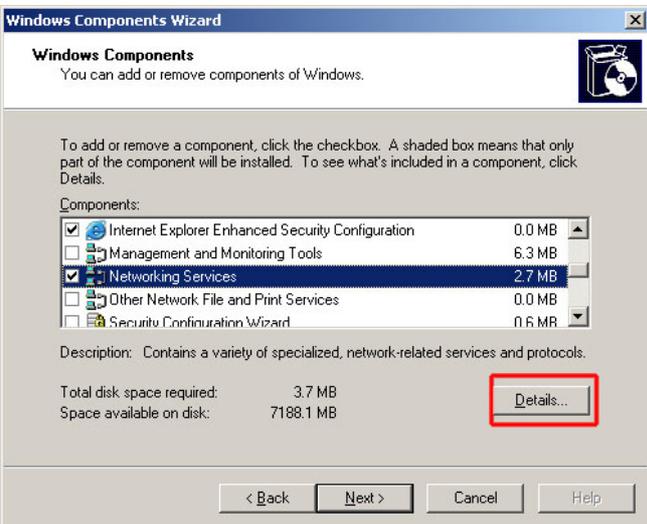
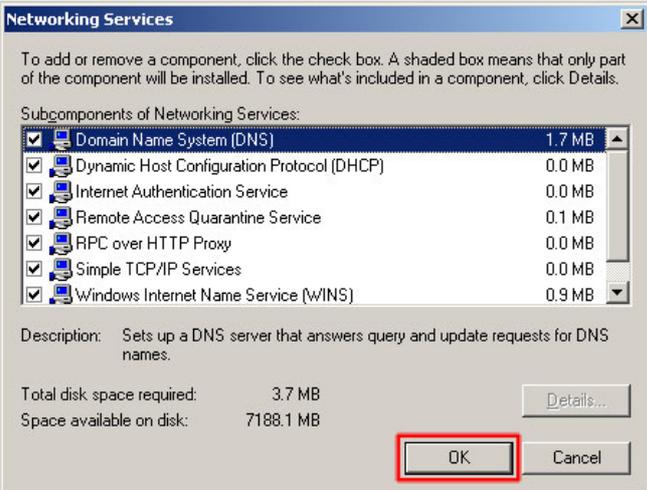
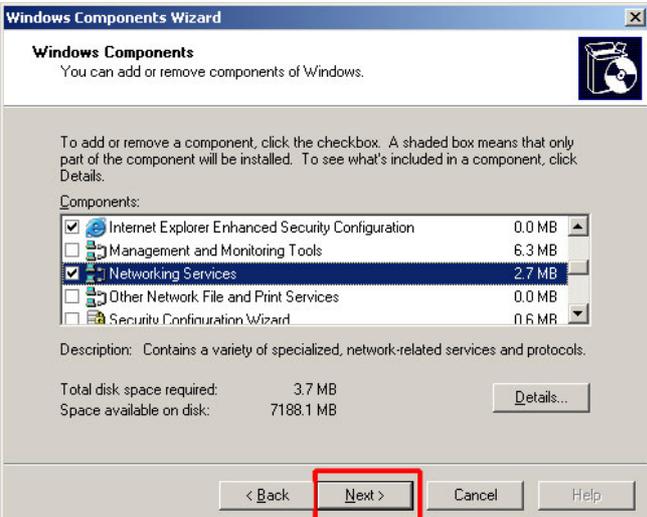
The IAS (Internet Authentication Server) is included in the Win2003 installation CD and must be installed as a new component in the operating system.

Note

You need the installation CD of Windows Server 2003 for installing the IAS.

Table 5-17

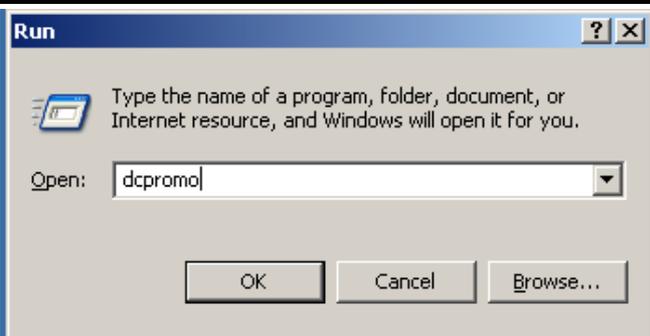
No.	Action	Comment
1.	Open the control panel by pressing Start-> Settings-> ControlPanel . Double-click Add or Remove Programs .	
2.	Select Add/ Remove Windows Components .	

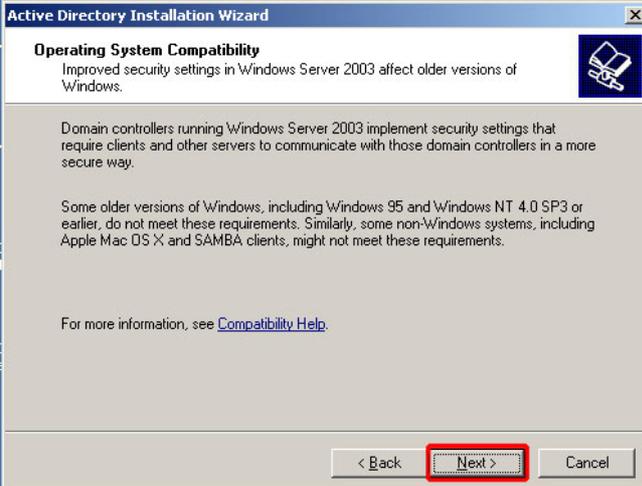
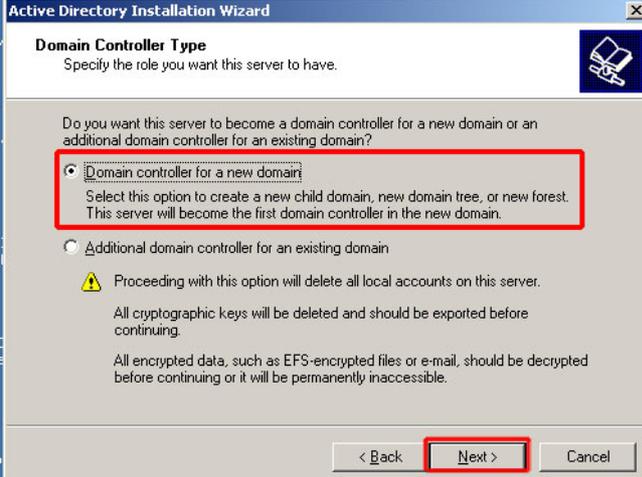
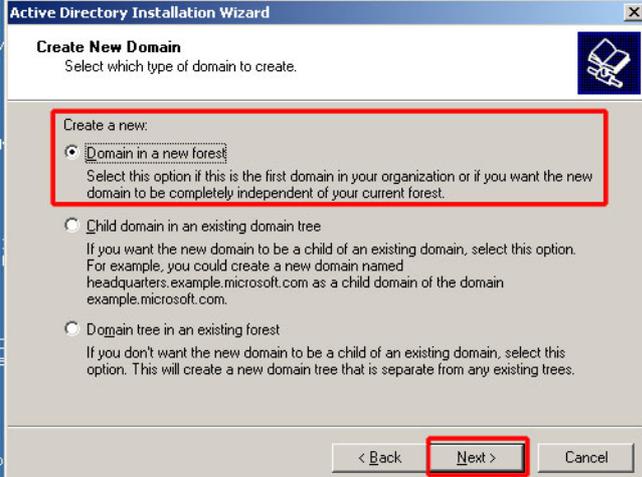
No.	Action	Comment
3.	<p>Scroll to Networking Services in the selection list. Tick this component and have the details displayed by clicking Details...</p>	 <p>The screenshot shows the 'Windows Components Wizard' window. The 'Networking Services' component is selected in the list, and its details are displayed below. The 'Details...' button is highlighted with a red box.</p>
4.	<p>Make sure you have selected all subcomponents. Then click OK.</p>	 <p>The screenshot shows the 'Networking Services' subcomponents list. All subcomponents are checked, and the 'OK' button is highlighted with a red box.</p>
5.	<p>Click Next> to start the installation of the new Windows component. Follow the instructions of the installation wizard.</p> <p>Once the installation is complete, the IAS has been installed on your computer.</p>	 <p>The screenshot shows the 'Windows Components Wizard' window. The 'Networking Services' component is selected, and the 'Next >' button is highlighted with a red box.</p>

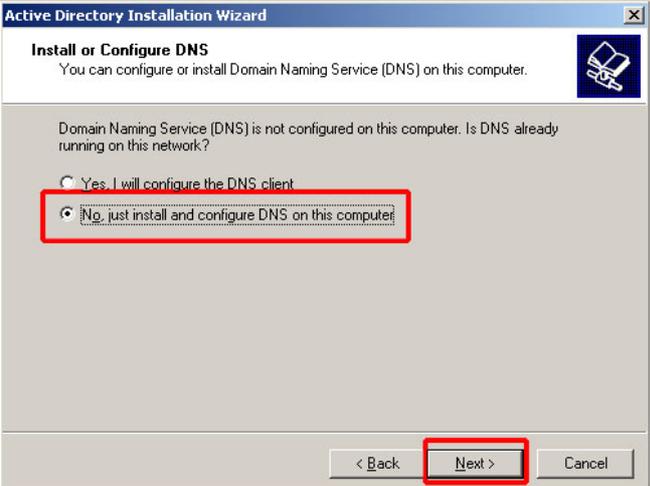
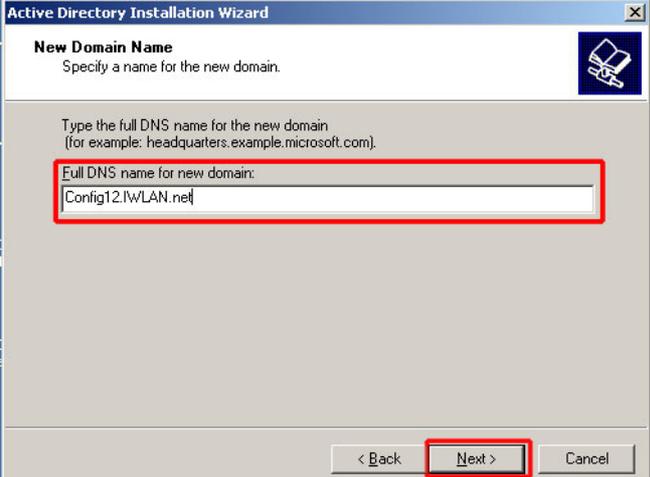
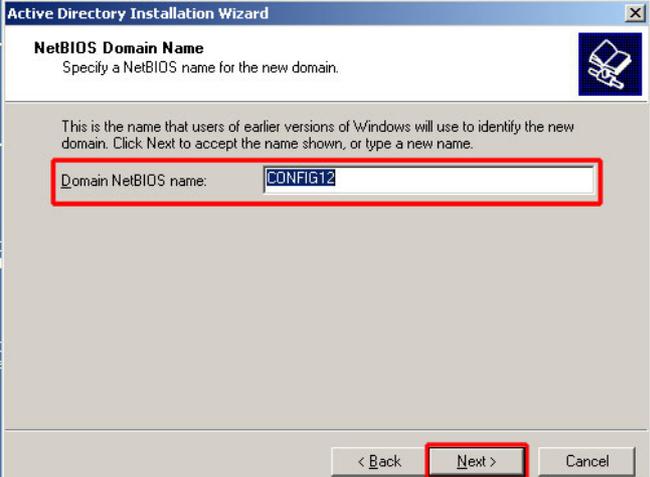
No.	Action	Comment
6.	During the installation of IAS you may be asked for the winsctrs.dll file.	This file is included in the installation CD, however, the file name is WINSCTRS.DL_ . If you cannot find the file, we recommend using the Windows search via Start->Search->For Files or Folders . Enter winsctrs.dl* as a file name and search your CD-Rom drive.

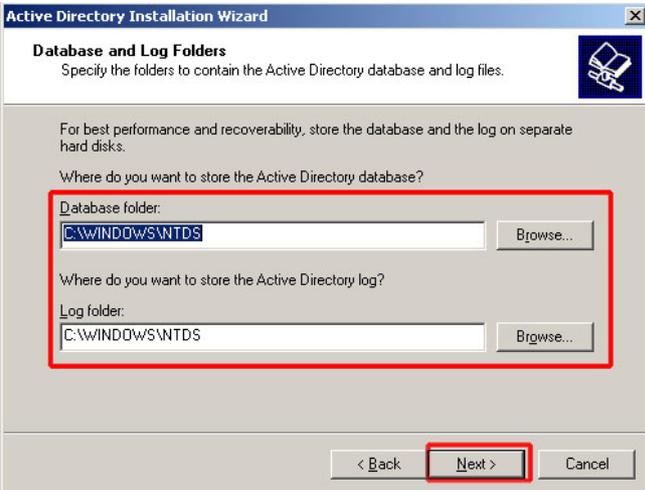
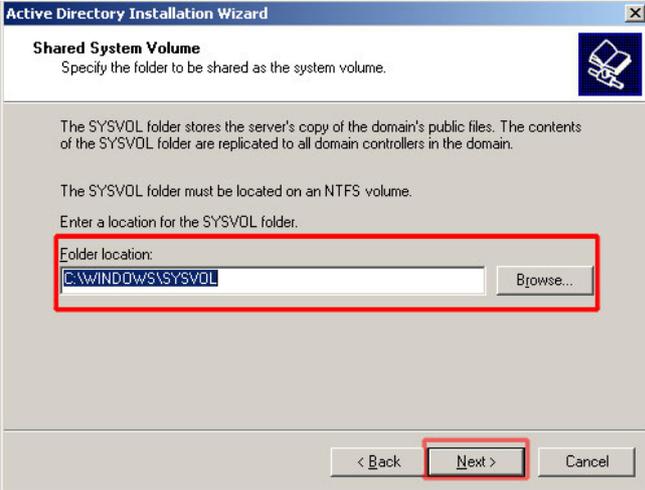
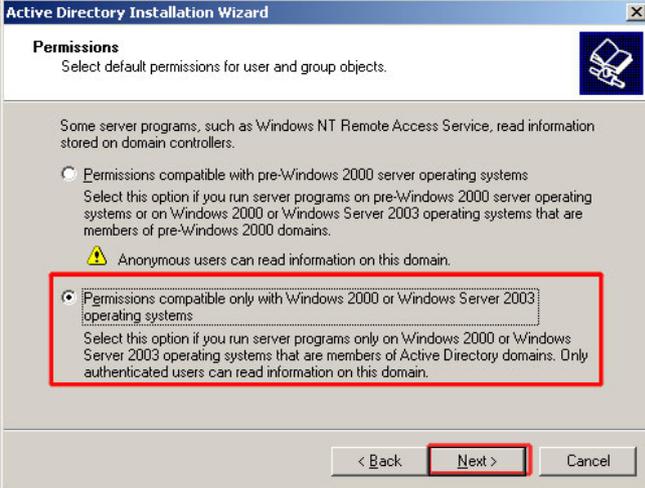
Set up an Active Directory

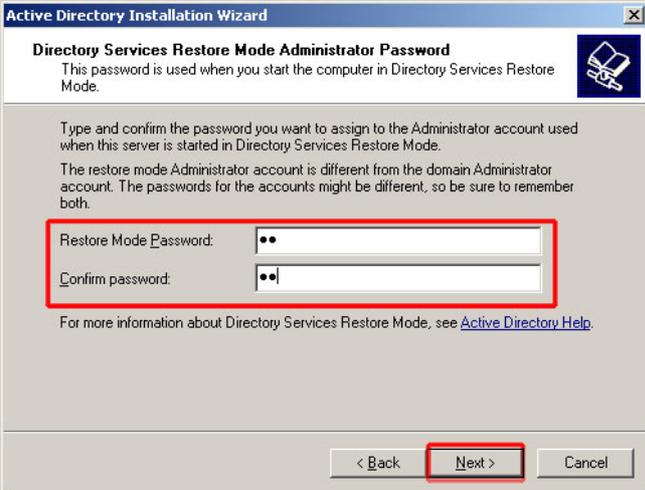
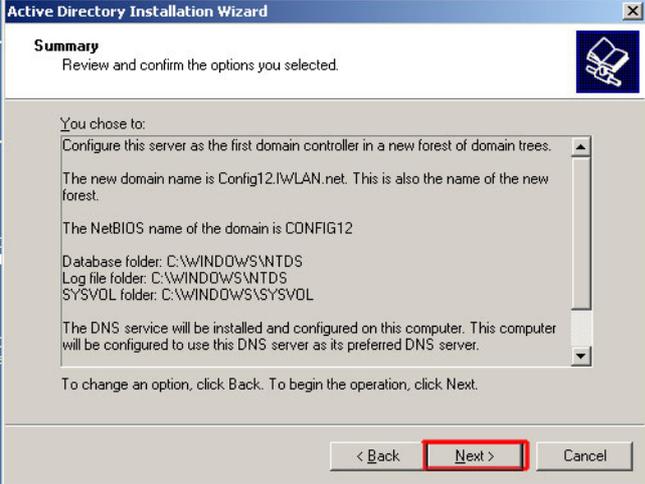
Table 5-18

No.	Action	Comment
1.	Open the command window by clicking Start-> Run... Enter the command dcpromo and confirm with OK .	
2.	The Active Directory Installation Wizard is started. Click Next to go to the next step.	

No.	Action	Comment
3.	Skip the next window with Next> .	 <p>Active Directory Installation Wizard</p> <p>Operating System Compatibility Improved security settings in Windows Server 2003 affect older versions of Windows.</p> <p>Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.</p> <p>Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 or earlier, do not meet these requirements. Similarly, some non-Windows systems, including Apple Mac OS X and SAMBA clients, might not meet these requirements.</p> <p>For more information, see Compatibility Help.</p> <p>< Back Next > Cancel</p>
4.	As you want to create a new domain, the server is expected to become a domain controller for a new domain. Click Next> .	 <p>Active Directory Installation Wizard</p> <p>Domain Controller Type Specify the role you want this server to have.</p> <p>Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?</p> <p><input checked="" type="radio"/> Domain controller for a new domain Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.</p> <p><input type="radio"/> Additional domain controller for an existing domain</p> <p> Proceeding with this option will delete all local accounts on this server. All cryptographic keys will be deleted and should be exported before continuing. All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.</p> <p>< Back Next > Cancel</p>
5.	Do not change the default setting when selecting the domain type . Confirm with Next> .	 <p>Active Directory Installation Wizard</p> <p>Create New Domain Select which type of domain to create.</p> <p>Create a new:</p> <p><input checked="" type="radio"/> Domain in a new forest Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.</p> <p><input type="radio"/> Child domain in an existing domain tree If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.</p> <p><input type="radio"/> Domain tree in an existing forest If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.</p> <p>< Back Next > Cancel</p>

No.	Action	Comment
6.	Select that the DNS server is to be installed and click Next> .	 <p>Active Directory Installation Wizard</p> <p>Install or Configure DNS You can configure or install Domain Naming Service (DNS) on this computer.</p> <p>Domain Naming Service (DNS) is not configured on this computer. Is DNS already running on this network?</p> <p><input type="radio"/> Yes, I will configure the DNS client</p> <p><input checked="" type="radio"/> No, just install and configure DNS on this computer</p> <p>< Back Next > Cancel</p>
7.	Enter a DNS name for the new domain. (Here: Config12.IWLAN.net) Click Next> to go to the next step. Note: The action Next> causes a longer waiting period until the next step is called.	 <p>Active Directory Installation Wizard</p> <p>New Domain Name Specify a name for the new domain.</p> <p>Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).</p> <p>Full DNS name for new domain: Config12.IWLAN.net</p> <p>< Back Next > Cancel</p>
8.	A name is already suggested as NetBIOS name . Click Next> to accept the name or enter a new name.	 <p>Active Directory Installation Wizard</p> <p>NetBIOS Domain Name Specify a NetBIOS name for the new domain.</p> <p>This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.</p> <p>Domain NetBIOS name: CONFIG12</p> <p>< Back Next > Cancel</p>

No.	Action	Comment
9.	If necessary, you can use this step to change the path under which the database or log file is to be saved by Active Directory. Click Next to go to the next step.	 <p>The screenshot shows the 'Active Directory Installation Wizard' window, 'Database and Log Folders' step. It prompts the user to specify folders for the database and log files. The 'Database folder' and 'Log folder' fields are both set to 'C:\WINDOWS\NTDS'. The 'Next >' button is highlighted with a red box.</p>
10.	A copy of the public services server of the domain is saved in the SYSVOL folder. The folder must be on one of the NTFS volumes. Enter a path for the folder or leave the name that is suggested. Click Next to go to the next step.	 <p>The screenshot shows the 'Active Directory Installation Wizard' window, 'Shared System Volume' step. It prompts the user to specify the folder to be shared as the system volume. The 'Folder location' field is set to 'C:\WINDOWS\SYSVOL'. The 'Next >' button is highlighted with a red box.</p>
11.	Define the authorizations for the users and group objects. The default setting was left unchanged here. Click Next to go to the next step.	 <p>The screenshot shows the 'Active Directory Installation Wizard' window, 'Permissions' step. It prompts the user to select default permissions for user and group objects. Two options are shown: 'Permissions compatible with pre-Windows 2000 operating systems' (unselected) and 'Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems' (selected). The selected option is highlighted with a red box. The 'Next >' button is also highlighted with a red box.</p>

No.	Action	Comment
12.	<p>Enter an administrator password. You will need this password if you start your computer in the "Restore directory services" mode. Click Next>.</p>	
13.	<p>A summary is displayed. Confirm the installation of the domain with Next>. Note: The action Next> is followed by a longer waiting period.</p>	
14.	<p>The Active Directory has now been installed on your computer. Exit the wizard with Finish.</p>	

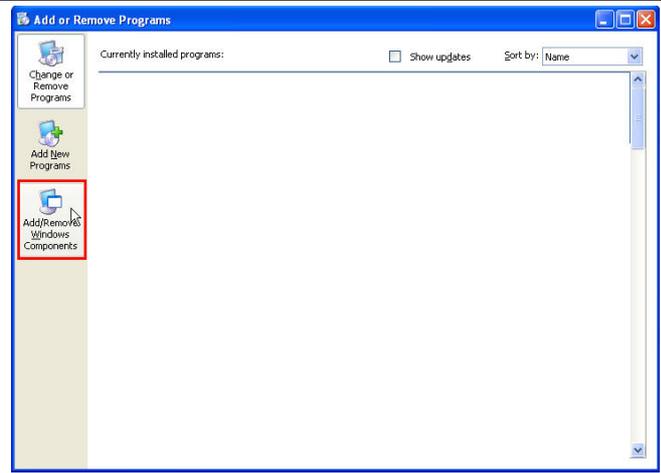
No.	Action	Comment
15.	Restart your computer to make the changes effective.	

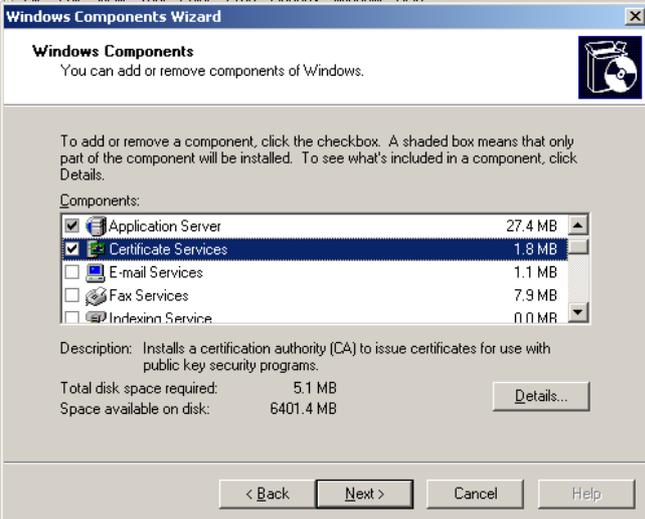
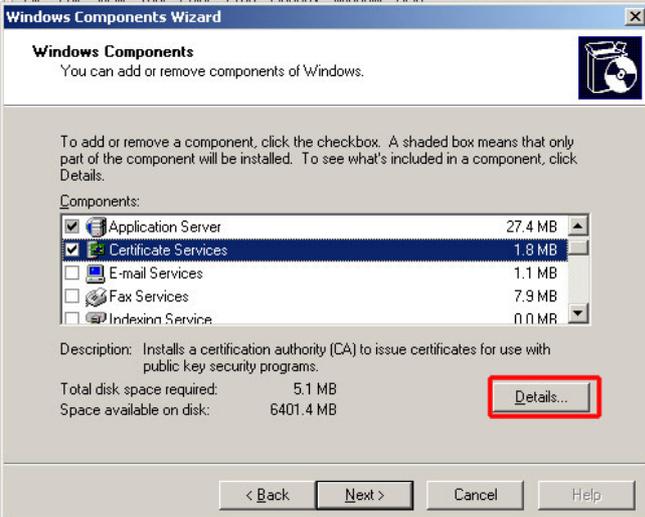
Note From now on, log on to this domain (**here: Config12.IWLAN.net**) when restarting your computer.

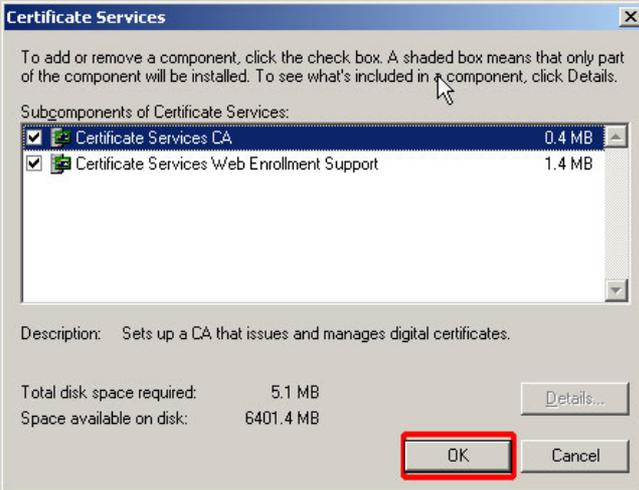
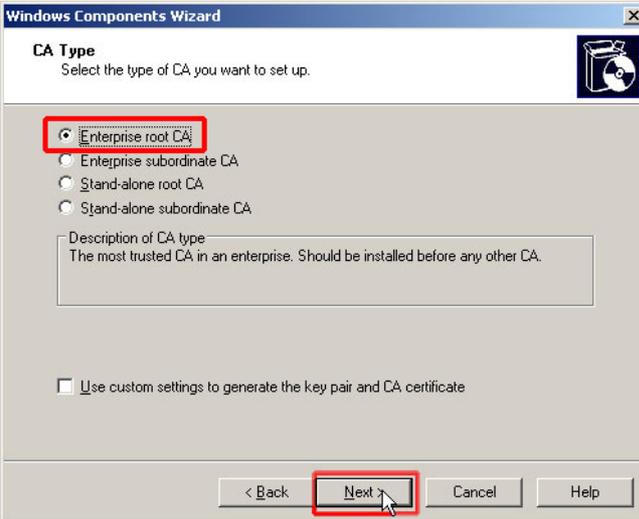
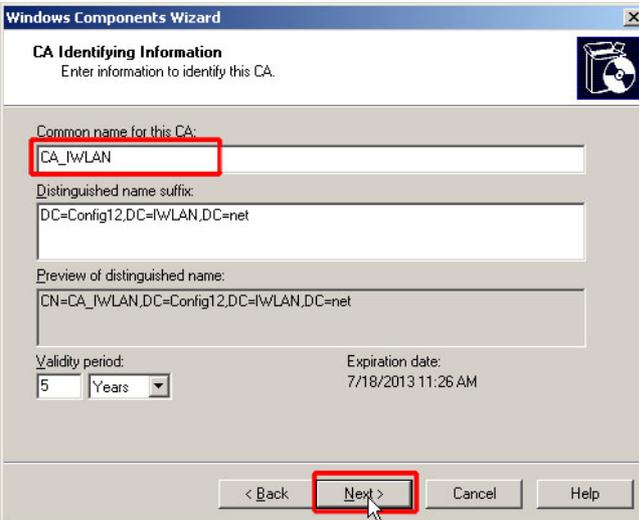
Install a certification authority

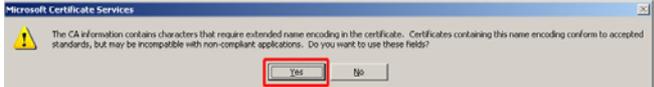
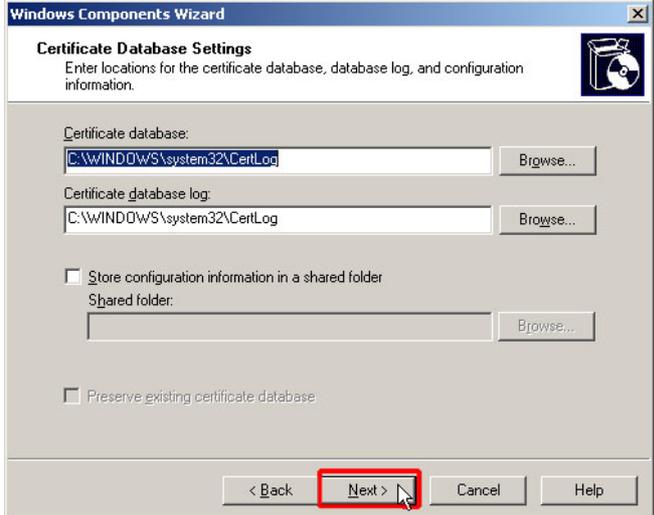
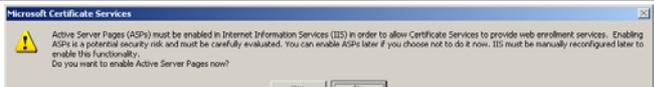
The certification authority is required to create certificates.

Table 5-19

No.	Action	Comment
1.	Open the control panel by pressing Start-> Settings->ControlPanel . Double-click Add or Remove Programs .	
2.	Select Add/ Remove Windows Components .	

No.	Action	Comment
3.	Scroll to Certificate Services in the selection list. Tick this component.	 <p>The screenshot shows the 'Windows Components Wizard' window. The 'Certificate Services' component is selected in the list, which is highlighted with a blue background. The list also includes 'Application Server' (27.4 MB), 'E-mail Services' (1.1 MB), 'Fax Services' (7.9 MB), and 'Indexing Service' (0.0 MB). Below the list, the description for Certificate Services is shown: 'Installs a certification authority (CA) to issue certificates for use with public key security programs.' The total disk space required is 5.1 MB, and the space available on disk is 6401.4 MB. The 'Details...' button is visible at the bottom right of the component details section.</p>
4.	A warning appears. Confirm this warning with Yes .	 <p>The screenshot shows a warning dialog box titled 'Microsoft Certificate Services'. The text inside reads: 'After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?'. The 'Yes' button is highlighted with a red box.</p>
5.	Click Details... to have the details displayed.	 <p>This screenshot is identical to the one in step 3, but the 'Details...' button at the bottom right of the component details section is highlighted with a red box.</p>

No.	Action	Comment						
6.	<p>Make sure you have selected all subcomponents. Then click OK to close the dialog box.</p> <p>Click Next to go to the next step.</p>	 <p>Certificate Services</p> <p>To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.</p> <p>Subcomponents of Certificate Services:</p> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td>Certificate Services CA</td> <td>0.4 MB</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>Certificate Services Web Enrollment Support</td> <td>1.4 MB</td> </tr> </table> <p>Description: Sets up a CA that issues and manages digital certificates.</p> <p>Total disk space required: 5.1 MB Space available on disk: 6401.4 MB</p> <p>Buttons: Details..., OK, Cancel</p>	<input checked="" type="checkbox"/>	Certificate Services CA	0.4 MB	<input checked="" type="checkbox"/>	Certificate Services Web Enrollment Support	1.4 MB
<input checked="" type="checkbox"/>	Certificate Services CA	0.4 MB						
<input checked="" type="checkbox"/>	Certificate Services Web Enrollment Support	1.4 MB						
7.	<p>Select Root certification authority of the company as a certification authority type. Click Next to go to the next step.</p>	 <p>Windows Components Wizard</p> <p>CA Type Select the type of CA you want to set up.</p> <p><input checked="" type="radio"/> Enterprise root CA <input type="radio"/> Enterprise subordinate CA <input type="radio"/> Stand-alone root CA <input type="radio"/> Stand-alone subordinate CA</p> <p>Description of CA type The most trusted CA in an enterprise. Should be installed before any other CA.</p> <p><input type="checkbox"/> Use custom settings to generate the key pair and CA certificate</p> <p>Buttons: < Back, Next >, Cancel, Help</p>						
8.	<p>Enter a name for the certification authority (here: CA_IWLAN) and click Next> to go to the next step.</p>	 <p>Windows Components Wizard</p> <p>CA Identifying Information Enter information to identify this CA.</p> <p>Common name for this CA: <input type="text" value="CA_IWLAN"/></p> <p>Distinguished name suffix: DC=Config12,DC=IWLAN,DC=net</p> <p>Preview of distinguished name: CN=CA_IWLAN,DC=Config12,DC=IWLAN,DC=net</p> <p>Validity period: 5 Years Expiration date: 7/18/2013 11:26 AM</p> <p>Buttons: < Back, Next >, Cancel, Help</p>						

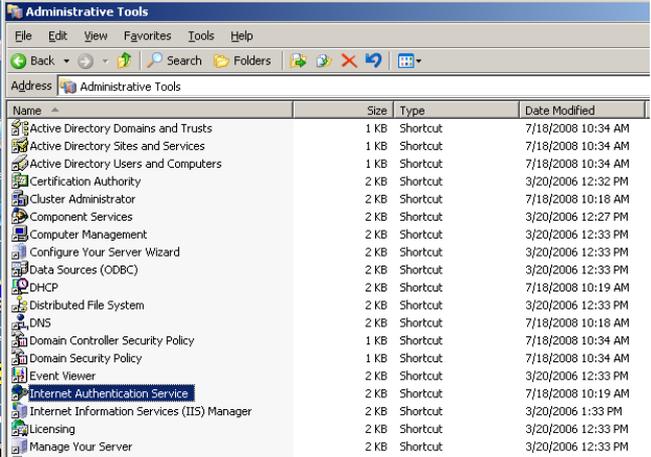
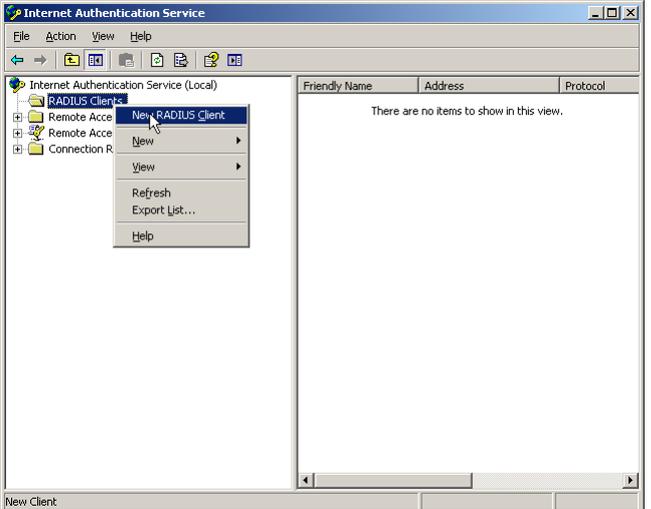
No.	Action	Comment
9.	Confirm the warning that special characters might not be compatible with Yes .	
10.	Enter a new path for the certification database or leave the suggested path. Click Next> .	
11.	Confirm the note with Yes . The components are configured.	
12.	During the installation of the CA you may be asked for the certenc.dll file.	This file is included in the installation CD, however the file name is CERTENC.DL_. If you cannot find the file, we recommend using the Windows search via Start->Search->For Files or Folders . Enter certenc.dl* as a file name and search your CD-Rom drive.
13.	If required, confirm the next note with Yes .	

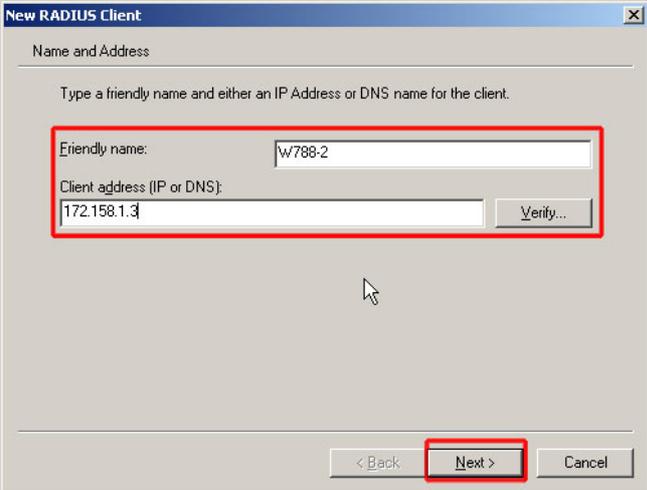
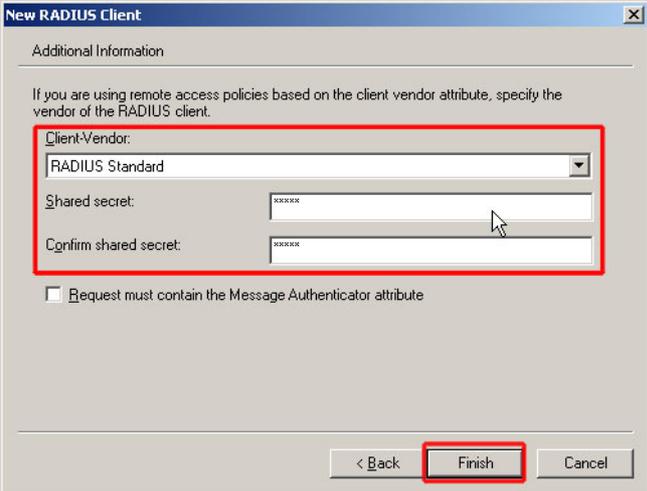
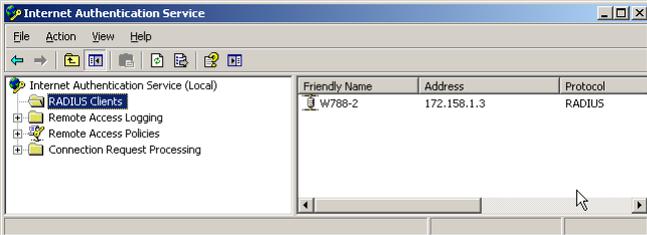
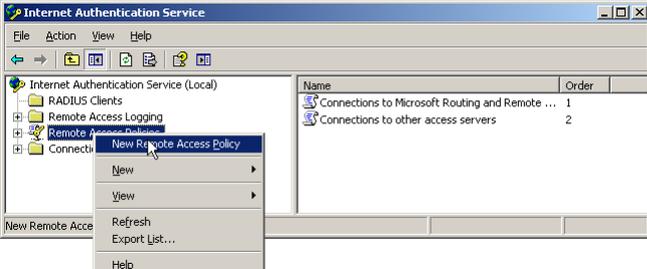
No.	Action	Comment
14.	Exit the wizard with Finish .	 <p>The screenshot shows a Windows dialog box titled "Windows Components Wizard" with the subtitle "Completing the Windows Components Wizard". The main text reads: "You have successfully completed the Windows Components Wizard." Below this, it says: "To close this wizard, click Finish." At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Help". The "Finish" button is highlighted with a red rectangular box, and a mouse cursor is pointing at it.</p>

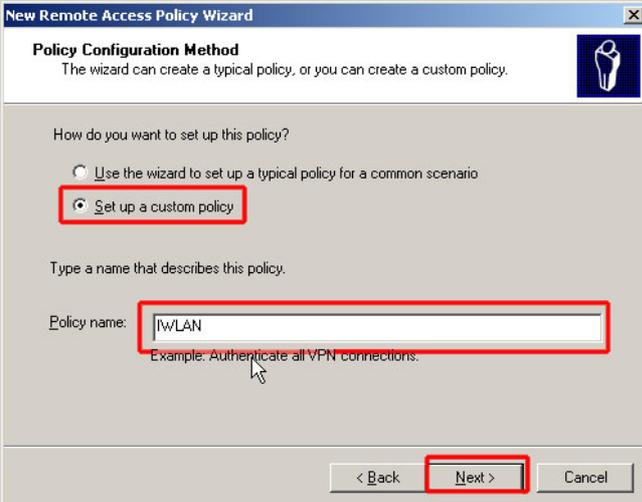
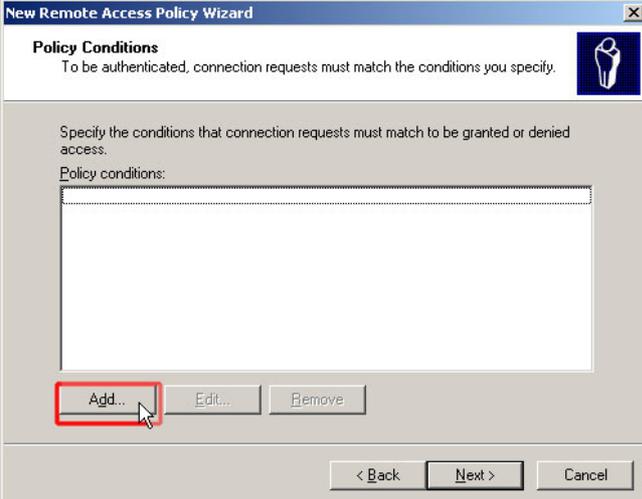
Configure the IAS

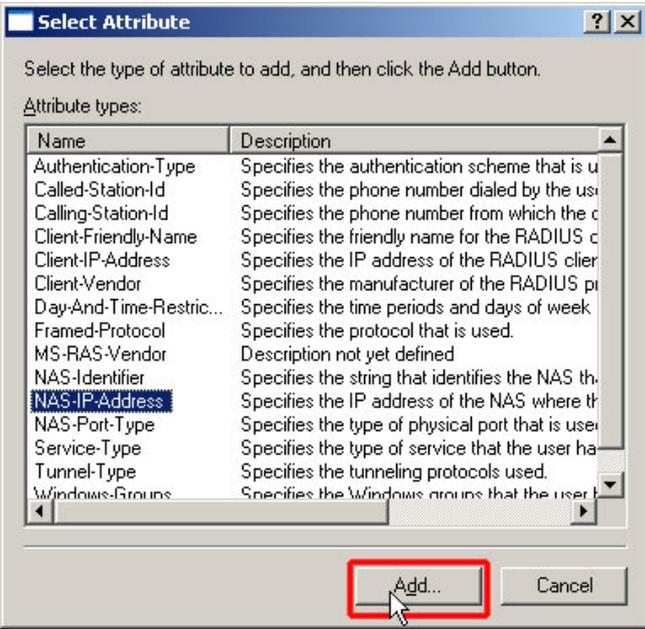
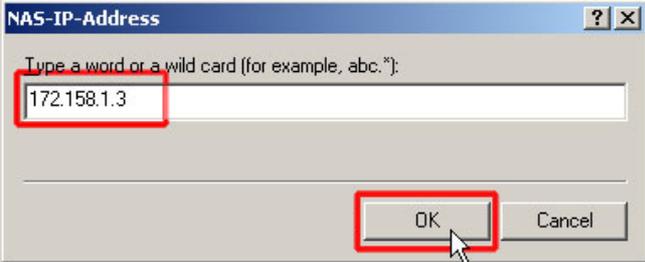
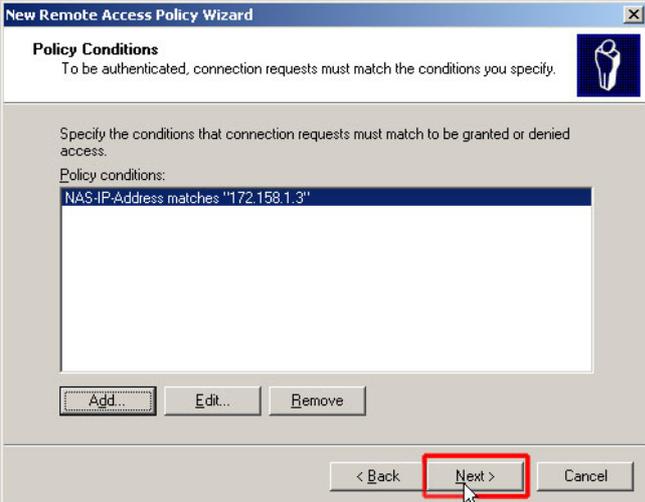
During the next steps, the Internet Authentication Service is configured in such a way that the SCALANCE W746 cannot log on to the SCALANCE W788-2 until it has authenticated itself on the IAS with the correct password.

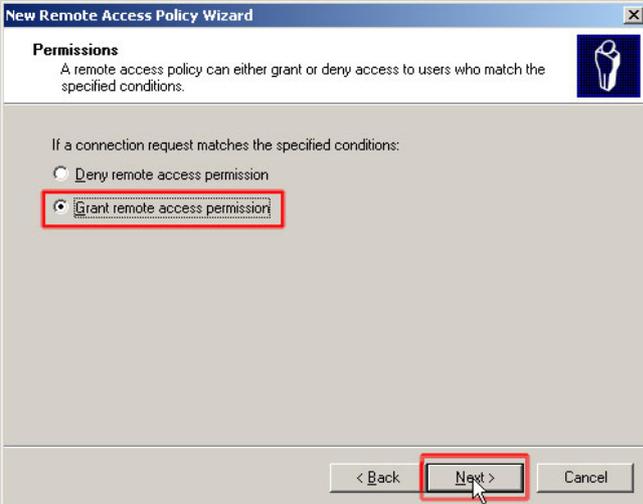
Table 5-20

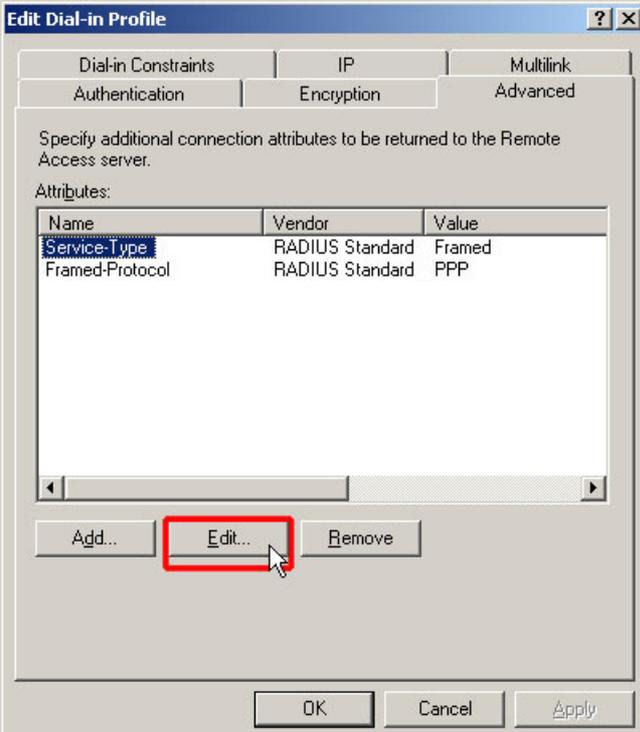
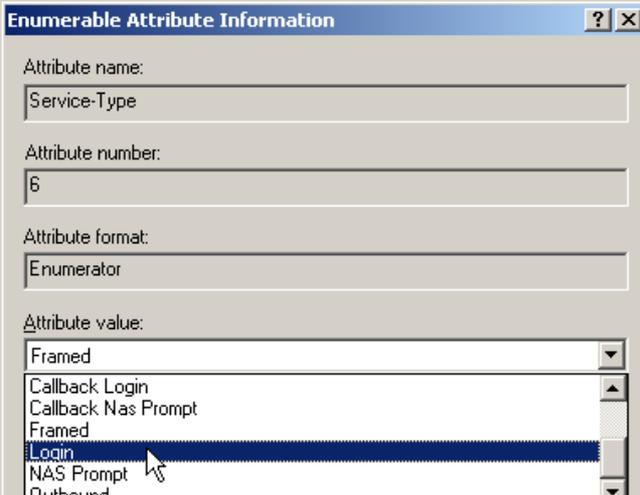
No.	Action	Comment
1.	<p>Open the management by pressing Start->Settings->ControlPanel->Administrative Tools. Double-click Internet Authentication Service.</p>	
2.	<p>A new window opens. Select RADIUS clients and create a new RADIUS client using the right mouse button -> New RADIUS client.</p>	

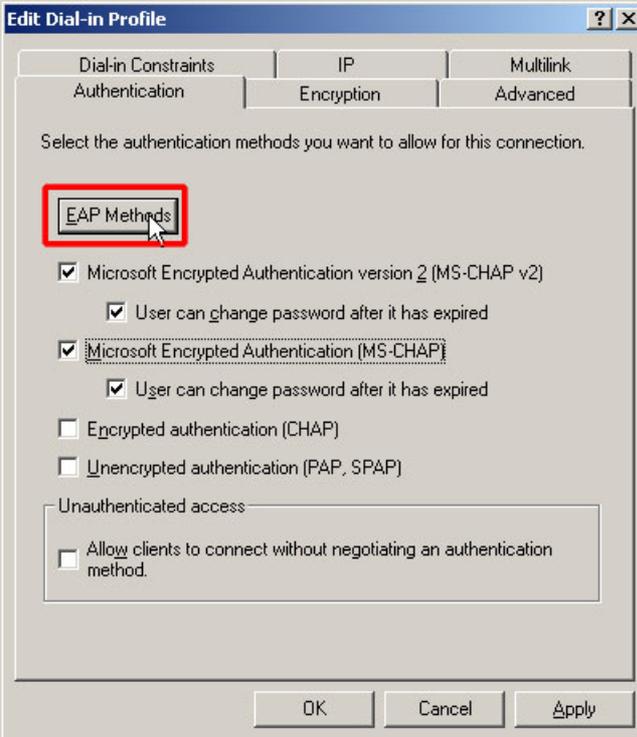
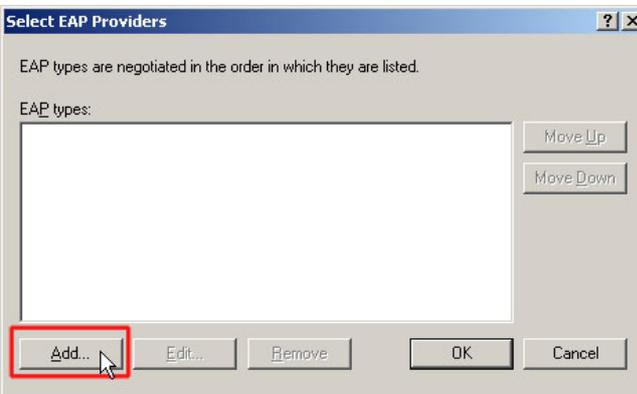
No.	Action	Comment
3.	Enter a name for the RADIUS client (here: W788-2) and the IP address 172.158.1.3 of the SCALANCE W788-2 that functions as authenticator. Click Next> .	
4.	Select RADIUS Standard as a client manufacturer and, as a common key, enter the key you have assigned in the SCALANCE W788-2 during the RADIUS configuration (Table 5-5 line 19). (Here: admin). Close the dialog box with Finish .	
5.	A new RADIUS client has been created.	
6.	Select Remote Access Policies and create a new policy using the right mouse button-> New Remote Access Policy .	

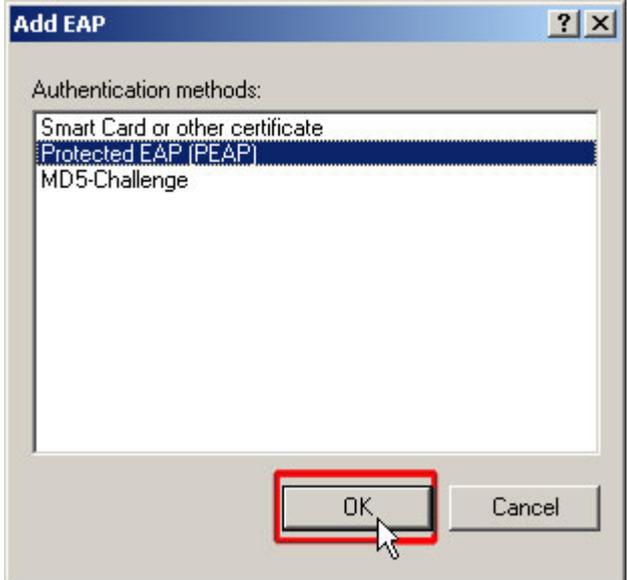
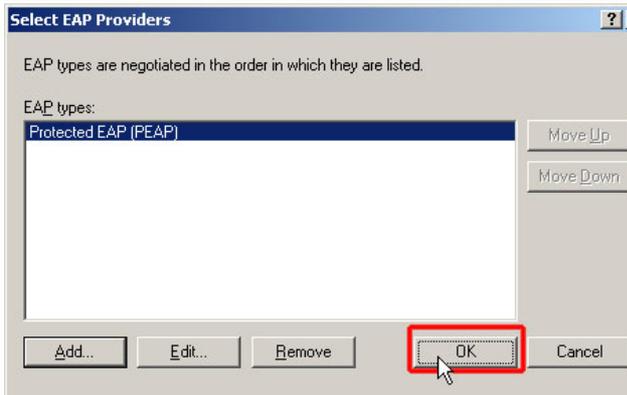
No.	Action	Comment
7.	The wizard for new RAS policies opens. In the next step, select that you want to create a user-defined policy and enter a name . Click Next> .	
8.	Add a new policy condition with Add....	

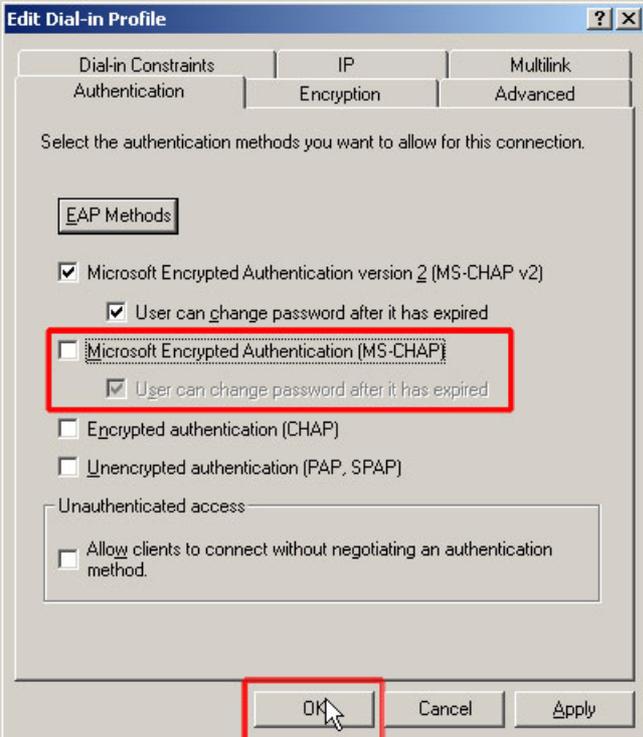
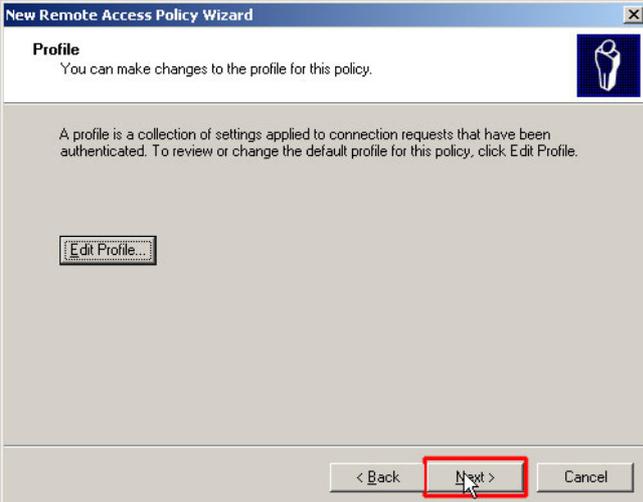
No.	Action	Comment																																
9.	Select NAS IP Address from the catalog and mark the line. Accept the attribute with Add....	 <p>Select Attribute</p> <p>Select the type of attribute to add, and then click the Add button.</p> <p>Attribute types:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Authentication-Type</td> <td>Specifies the authentication scheme that is u</td> </tr> <tr> <td>Called-Station-Id</td> <td>Specifies the phone number dialed by the us</td> </tr> <tr> <td>Calling-Station-Id</td> <td>Specifies the phone number from which the c</td> </tr> <tr> <td>Client-Friendly-Name</td> <td>Specifies the friendly name for the RADIUS c</td> </tr> <tr> <td>Client-IP-Address</td> <td>Specifies the IP address of the RADIUS clie</td> </tr> <tr> <td>Client-Vendor</td> <td>Specifies the manufacturer of the RADIUS p</td> </tr> <tr> <td>Day-And-Time-Restic...</td> <td>Specifies the time periods and days of week</td> </tr> <tr> <td>Framed-Protocol</td> <td>Specifies the protocol that is used.</td> </tr> <tr> <td>MS-RAS-Vendor</td> <td>Description not yet defined</td> </tr> <tr> <td>NAS-Identifier</td> <td>Specifies the string that identifies the NAS th</td> </tr> <tr> <td>NAS-IP-Address</td> <td>Specifies the IP address of the NAS where th</td> </tr> <tr> <td>NAS-Port-Type</td> <td>Specifies the type of physical port that is use</td> </tr> <tr> <td>Service-Type</td> <td>Specifies the type of service that the user ha</td> </tr> <tr> <td>Tunnel-Type</td> <td>Specifies the tunneling protocols used.</td> </tr> <tr> <td>Windows-Groups</td> <td>Specifies the Windows groups that the user t</td> </tr> </tbody> </table> <p>Add... Cancel</p>	Name	Description	Authentication-Type	Specifies the authentication scheme that is u	Called-Station-Id	Specifies the phone number dialed by the us	Calling-Station-Id	Specifies the phone number from which the c	Client-Friendly-Name	Specifies the friendly name for the RADIUS c	Client-IP-Address	Specifies the IP address of the RADIUS clie	Client-Vendor	Specifies the manufacturer of the RADIUS p	Day-And-Time-Restic...	Specifies the time periods and days of week	Framed-Protocol	Specifies the protocol that is used.	MS-RAS-Vendor	Description not yet defined	NAS-Identifier	Specifies the string that identifies the NAS th	NAS-IP-Address	Specifies the IP address of the NAS where th	NAS-Port-Type	Specifies the type of physical port that is use	Service-Type	Specifies the type of service that the user ha	Tunnel-Type	Specifies the tunneling protocols used.	Windows-Groups	Specifies the Windows groups that the user t
Name	Description																																	
Authentication-Type	Specifies the authentication scheme that is u																																	
Called-Station-Id	Specifies the phone number dialed by the us																																	
Calling-Station-Id	Specifies the phone number from which the c																																	
Client-Friendly-Name	Specifies the friendly name for the RADIUS c																																	
Client-IP-Address	Specifies the IP address of the RADIUS clie																																	
Client-Vendor	Specifies the manufacturer of the RADIUS p																																	
Day-And-Time-Restic...	Specifies the time periods and days of week																																	
Framed-Protocol	Specifies the protocol that is used.																																	
MS-RAS-Vendor	Description not yet defined																																	
NAS-Identifier	Specifies the string that identifies the NAS th																																	
NAS-IP-Address	Specifies the IP address of the NAS where th																																	
NAS-Port-Type	Specifies the type of physical port that is use																																	
Service-Type	Specifies the type of service that the user ha																																	
Tunnel-Type	Specifies the tunneling protocols used.																																	
Windows-Groups	Specifies the Windows groups that the user t																																	
10.	Enter the IP address of the SCALANCE W788-2 (172.158.1.3) and confirm with OK .	 <p>NAS-IP-Address</p> <p>Type a word or a wild card (for example, abc.*):</p> <p>172.158.1.3</p> <p>OK Cancel</p>																																
11.	The policy has been created. Click Next> .	 <p>New Remote Access Policy Wizard</p> <p>Policy Conditions To be authenticated, connection requests must match the conditions you specify.</p> <p>Specify the conditions that connection requests must match to be granted or denied access.</p> <p>Policy conditions:</p> <p>NAS-IP-Address matches "172.158.1.3"</p> <p>Add... Edit... Remove</p> <p>< Back Next > Cancel</p>																																

No.	Action	Comment
12.	<p>If a query corresponds to this policy, access is to be granted.</p> <p>Click Next to go to the next step.</p>	 <p>New Remote Access Policy Wizard</p> <p>Permissions A remote access policy can either grant or deny access to users who match the specified conditions.</p> <p>If a connection request matches the specified conditions:</p> <p><input type="radio"/> Deny remote access permission</p> <p><input checked="" type="radio"/> Grant remote access permission</p> <p>< Back Next > Cancel</p>
13.	<p>Click Profile to go to the policy settings.</p>	 <p>New Remote Access Policy Wizard</p> <p>Profile You can make changes to the profile for this policy.</p> <p>A profile is a collection of settings applied to connection requests that have been authenticated. To review or change the default profile for this policy, click Edit Profile.</p> <p>Edit Profile...</p> <p>< Back Next > Cancel</p>

No.	Action	Comment									
14.	Change to the Advanced tab. Select Service Type and click Edit .	 <p>Edit Dial-in Profile</p> <p>Dial-in Constraints IP Multilink Authentication Encryption Advanced</p> <p>Specify additional connection attributes to be returned to the Remote Access server.</p> <p>Attributes:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Vendor</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Service-Type</td> <td>RADIUS Standard</td> <td>Framed</td> </tr> <tr> <td>Framed-Protocol</td> <td>RADIUS Standard</td> <td>PPP</td> </tr> </tbody> </table> <p>Add... Edit... Remove</p> <p>OK Cancel Apply</p>	Name	Vendor	Value	Service-Type	RADIUS Standard	Framed	Framed-Protocol	RADIUS Standard	PPP
Name	Vendor	Value									
Service-Type	RADIUS Standard	Framed									
Framed-Protocol	RADIUS Standard	PPP									
15.	Select Login as an attribute value and confirm with OK .	 <p>Enumerable Attribute Information</p> <p>Attribute name: Service-Type</p> <p>Attribute number: 6</p> <p>Attribute format: Enumerator</p> <p>Attribute value:</p> <ul style="list-style-type: none"> Framed Callback Login Callback Nas Prompt Framed Login NAS Prompt Outbound 									

No.	Action	Comment
16.	Change to the Authentication tab. Click EAP Methods .	 <p>Edit Dial-in Profile</p> <p>Dial-in Constraints IP Multilink Authentication Encryption Advanced</p> <p>Select the authentication methods you want to allow for this connection.</p> <p>EAP Methods</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Microsoft Encrypted Authentication version 2 (MS-CHAP v2) <ul style="list-style-type: none"> <input checked="" type="checkbox"/> User can change password after it has expired <input checked="" type="checkbox"/> Microsoft Encrypted Authentication (MS-CHAP) <ul style="list-style-type: none"> <input checked="" type="checkbox"/> User can change password after it has expired <input type="checkbox"/> Encrypted authentication (CHAP) <input type="checkbox"/> Unencrypted authentication (PAP, SPAP) <p>Unauthenticated access</p> <ul style="list-style-type: none"> <input type="checkbox"/> Allow clients to connect without negotiating an authentication method. <p>OK Cancel Apply</p>
17.	Add new EAP types with Add...	 <p>Select EAP Providers</p> <p>EAP types are negotiated in the order in which they are listed.</p> <p>EAP types:</p> <p>Move Up Move Down</p> <p>Add... Edit... Remove OK Cancel</p>

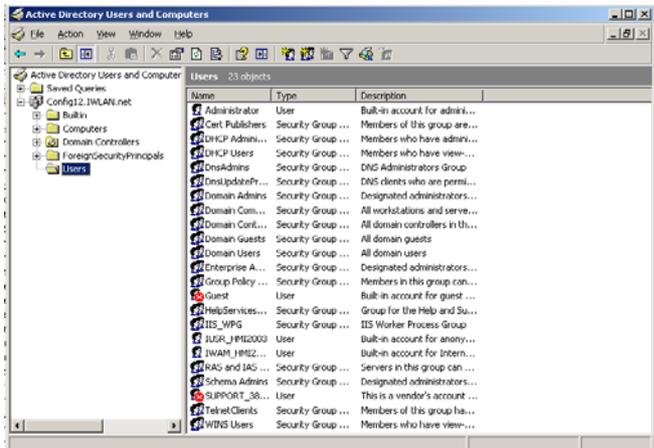
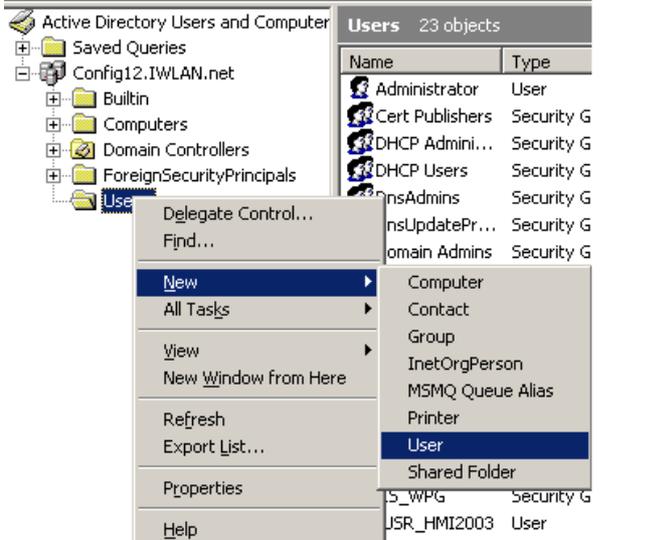
No.	Action	Comment
18.	Select Protected EAP (PEAP) as an authentication method. Click OK to accept the settings.	
19.	The authentication method has been included in the list. Close the dialog box with OK .	

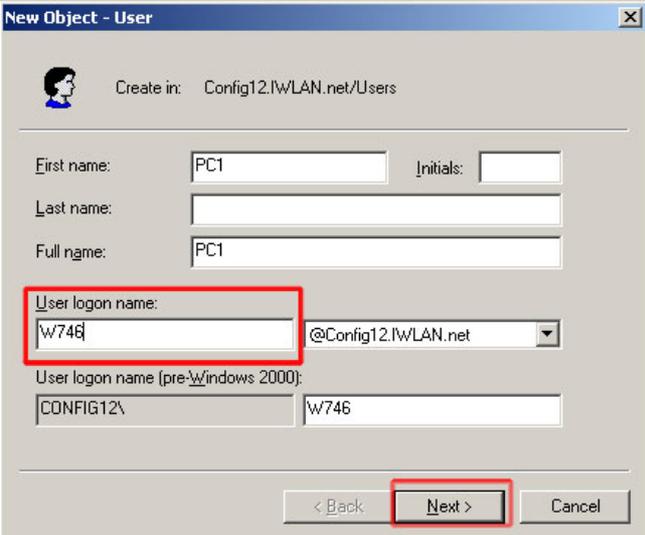
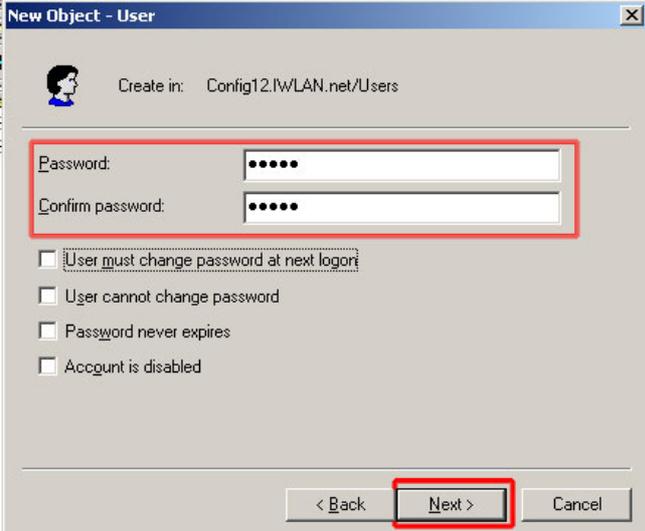
No.	Action	Comment
20.	Deactivate the MS-CHAP and close the dialog box with OK .	
21.	You are asked whether you want to view help on the authentication topic. Click No .	
22.	Click Next> .	

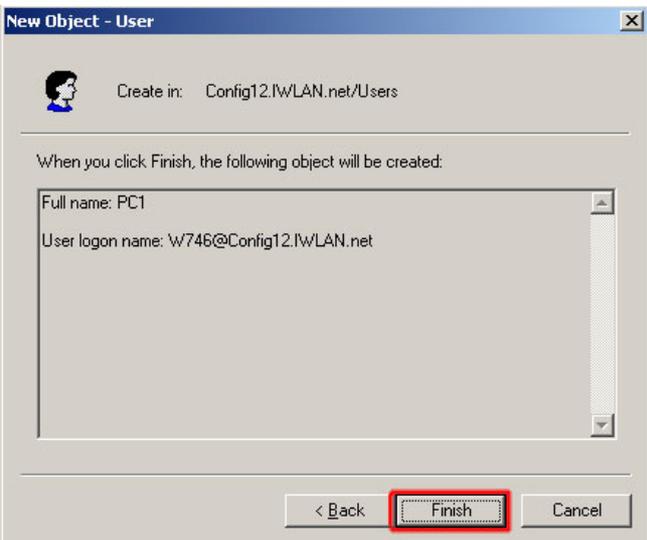
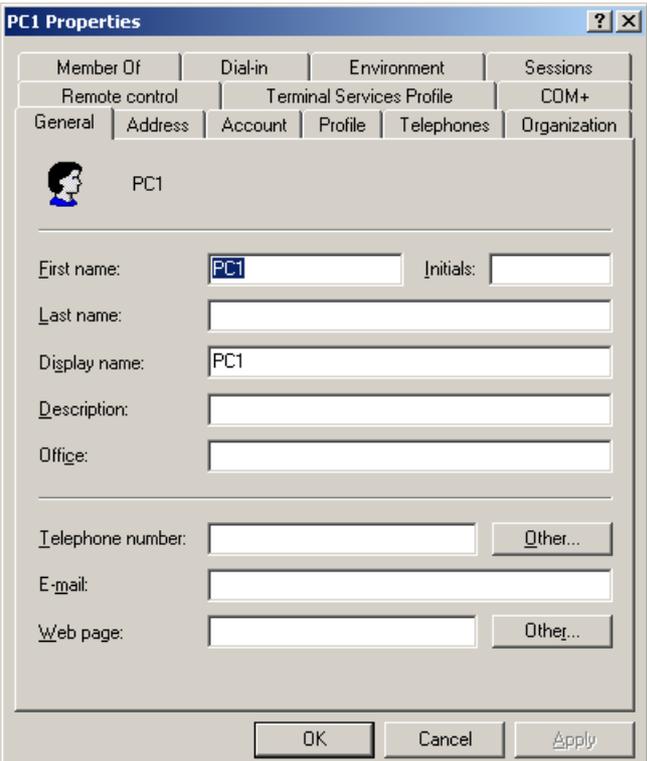
No.	Action	Comment
23.	Close the wizard with Finish .	
24.	Select the Internet Authentication Service and register it using the right mouse button -> Register Server in Active Directory .	
25.	Confirm the following note with OK .	
26.	Confirm the following note with OK .	

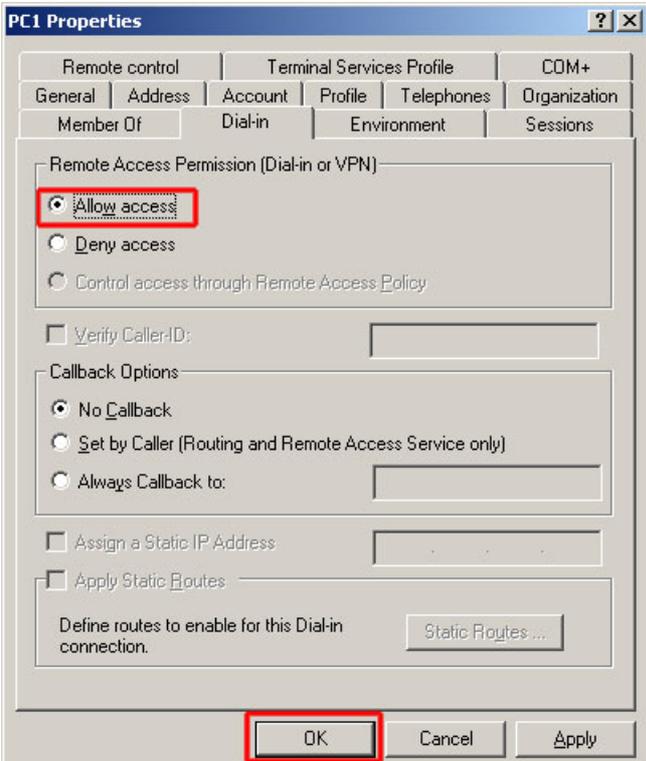
Create a user

Table 5-21

No.	Action	Comment
1.	Open the management by pressing Start->Settings->ControlPanel->Administrative Tools . Double-click Active Directory Users and Computers .	
2.	A new window opens. Select the Users folder that is in the domain created. (See Table 5-18) Here: Config12.IWLAN.net	
3.	Select the Users folder and create a new user using the right mouse button -> New->User .	

No.	Action	Comment
4.	<p>Enter name and first name. As a user login name, assign the name you have defined in the RADIUS configuration of the SCALANCE W746-1 (Table 5-7 line 15). (Here: W746) Click Next>.</p>	 <p>The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is 'Config12.IWLAN.net/Users'. The 'First name' field contains 'PC1'. The 'Last name' field is empty. The 'Full name' field contains 'PC1'. The 'User logon name' field contains 'w746' and the domain dropdown is '@Config12.IWLAN.net'. The 'User logon name (pre-Windows 2000)' field contains 'CONFIG12\' and the password field contains 'w746'. The 'Next >' button is highlighted with a red box.</p>
5.	<p>As a password, assign the password you have defined in the RADIUS configuration of the SCALANCE W746-1 (Table 5-7 line 15). (Here: RADIUS_Authentication) Deselect the first checkbox. Then click Next>.</p>	 <p>The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is 'Config12.IWLAN.net/Users'. The 'Password' and 'Confirm password' fields are filled with dots. The 'User must change password at next logon' checkbox is unchecked. The 'User cannot change password' checkbox is unchecked. The 'Password never expires' checkbox is unchecked. The 'Account is disabled' checkbox is unchecked. The 'Next >' button is highlighted with a red box.</p>

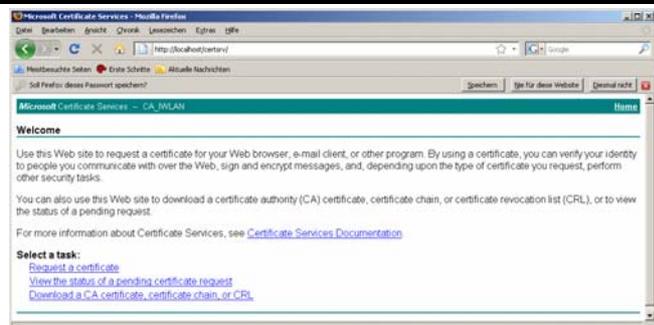
No.	Action	Comment
6.	Complete the creation of a new user with Finish .	
7.	Select the newly created user in the user list and double-click. The Properties dialog box opens.	

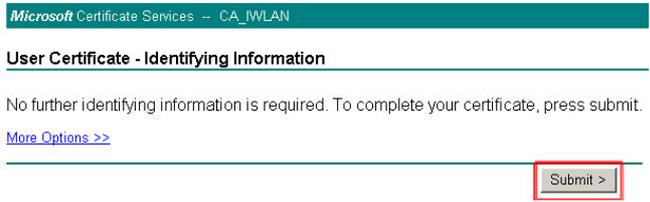
No.	Action	Comment
8.	Change to the Dial-In tab. Enable the access for this user. Close the dialog box with OK .	 <p>The screenshot shows the 'PC1 Properties' dialog box with the 'Dial-in' tab selected. Under 'Remote Access Permission (Dial-in or VPN)', the 'Allow access' radio button is selected and circled in red. Below it are 'Deny access' and 'Control access through Remote Access Policy' options. Under 'Callback Options', 'No Callback' is selected. At the bottom, the 'OK' button is also circled in red.</p>

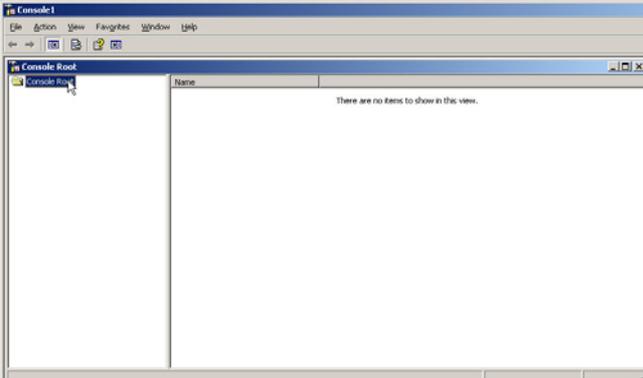
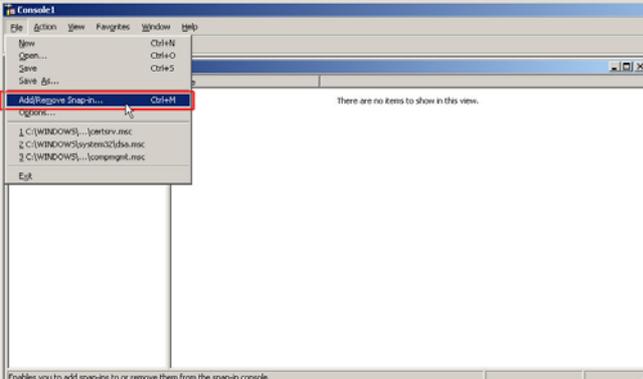
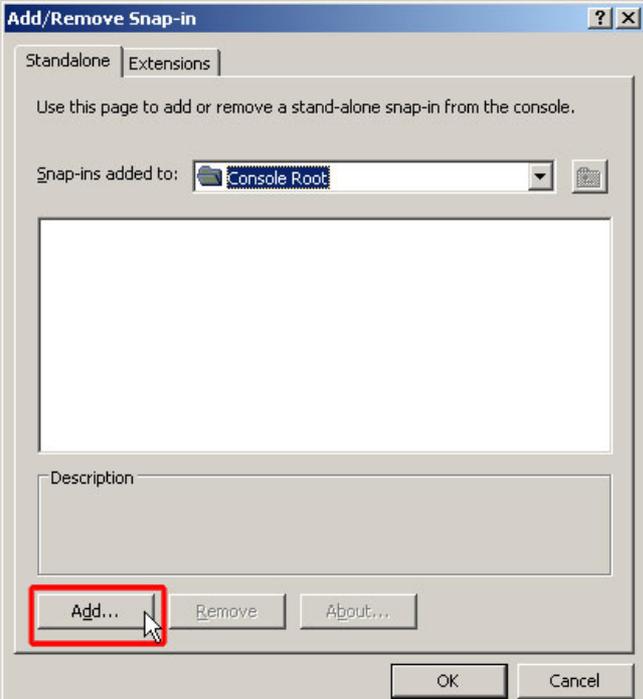
Create certificates

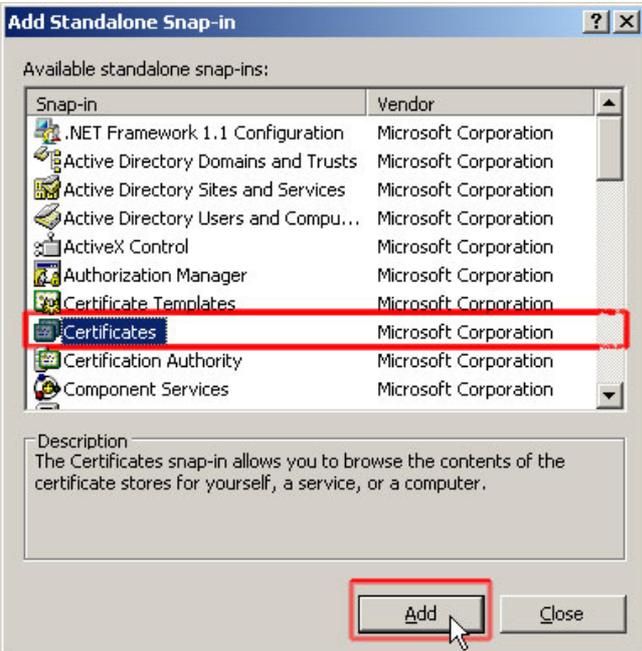
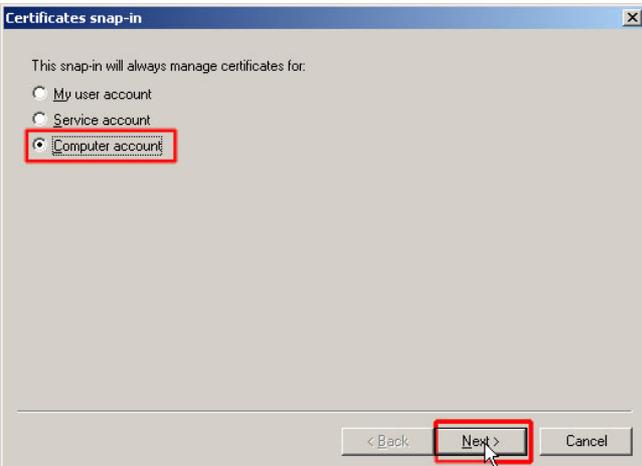
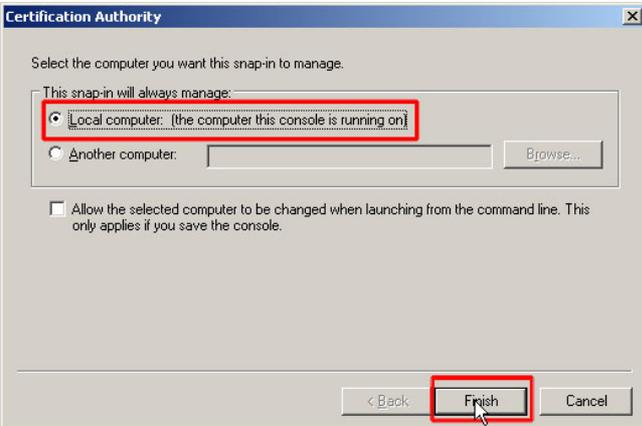
The certificates are used to authenticate the RADIUS server and the client. The certificates are stored on a page in the file system of the Win2003 server and are also loaded to the SCALANCE W746-1 configuration.

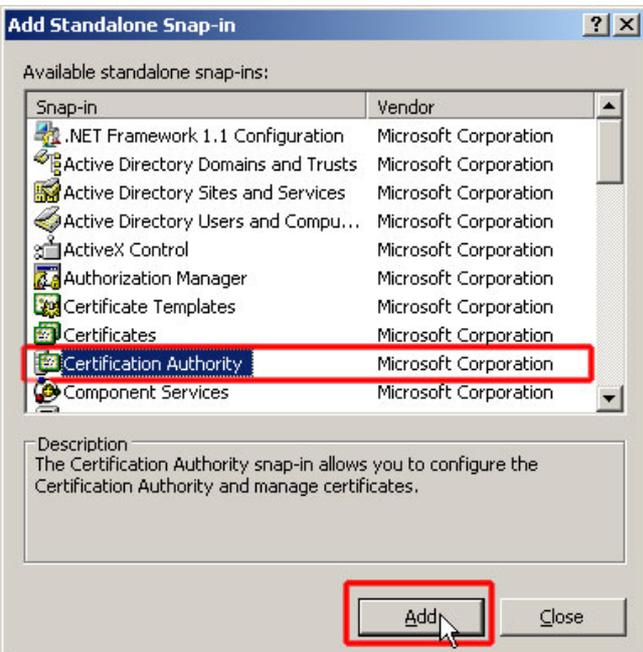
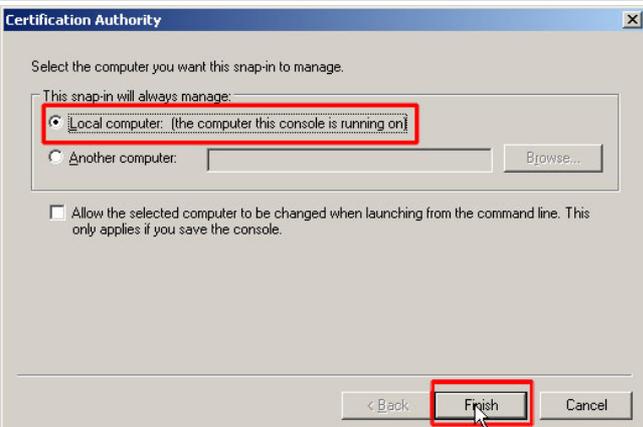
Table 5-22

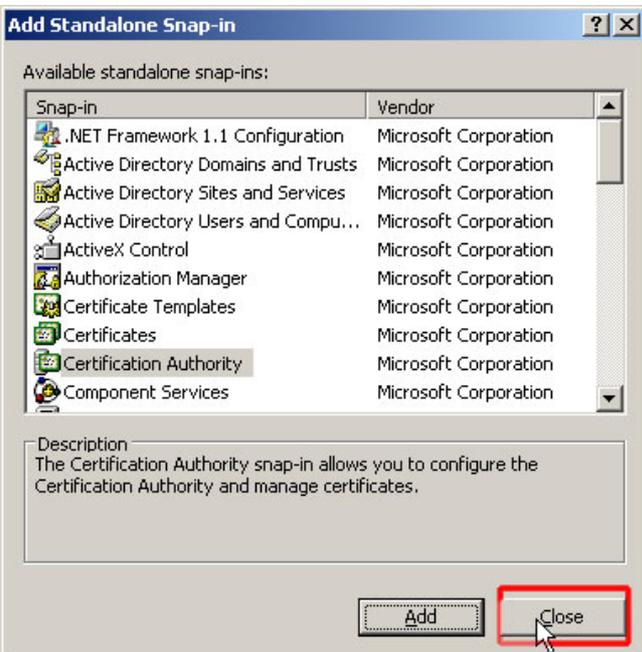
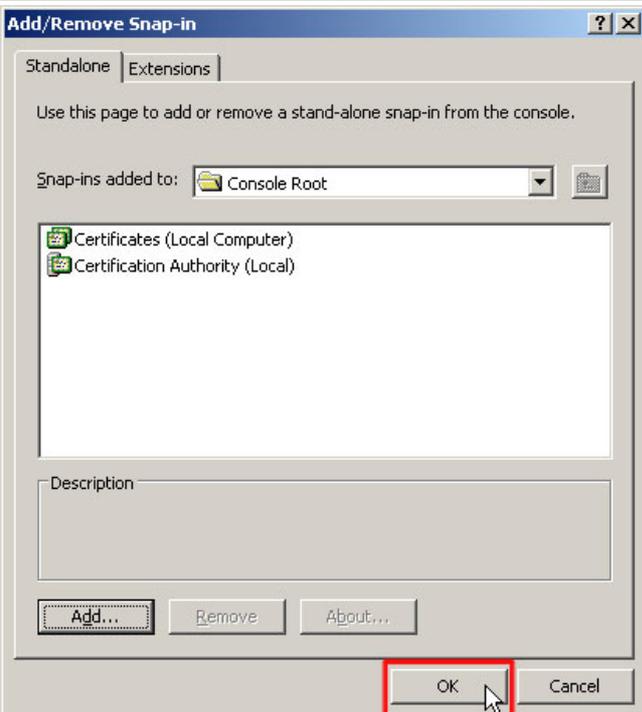
No.	Action	Comment
1.	Open a web browser and enter http://localhost/certsrv into the address field. Click Request a certificate .	 <p>The screenshot shows a web browser window displaying the Microsoft Certificate Services website. The address bar shows 'http://localhost/certsrv'. The page content includes a 'Welcome' message and a 'Select a task:' section where the 'Request a certificate' link is highlighted.</p>

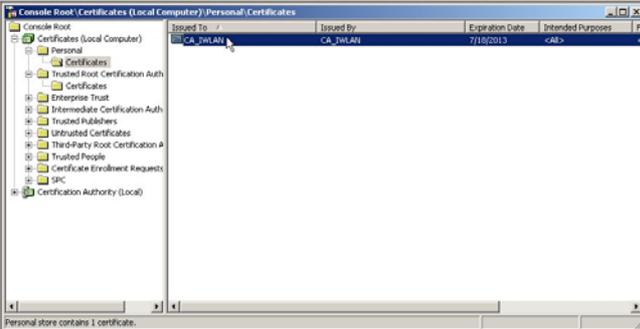
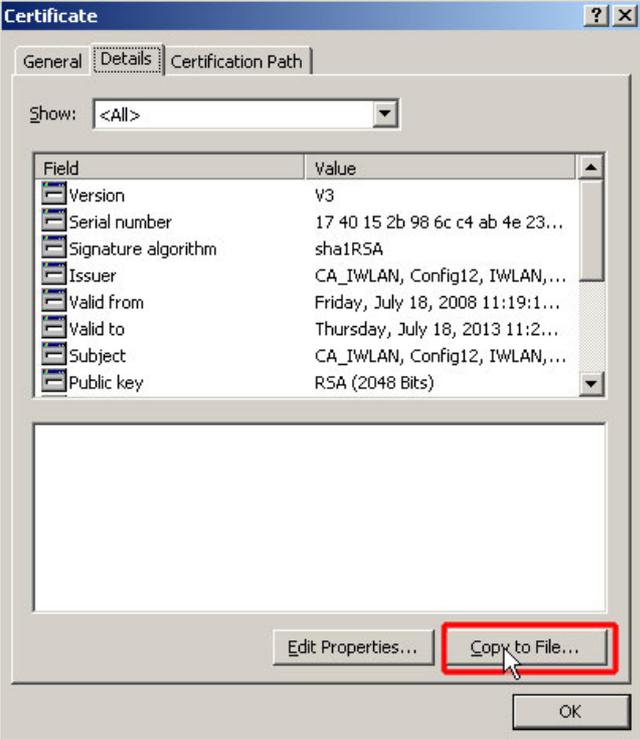
No.	Action	Comment
2.	Click User Certificate .	 <p><i>Microsoft</i> Certificate Services -- CA_IWLAN</p> <h3>Request a Certificate</h3> <p>Select the certificate type:</p> <p>User Certificate</p> <p>Or, submit an advanced certificate request.</p>
3.	Click Submit .	 <p><i>Microsoft</i> Certificate Services -- CA_IWLAN</p> <h3>User Certificate - Identifying Information</h3> <p>No further identifying information is required. To complete your certificate, press submit.</p> <p>More Options >></p> <p><input type="button" value="Submit >"/></p>
4.	Confirm the warning that a new certificate has been requested with Yes .	 <p>Potential Scripting Violation</p> <p>This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?</p> <p><input type="button" value="Yes"/> <input type="button" value="No"/></p>
5.	Click Install this certificate .	 <p><i>Microsoft</i> Certificate Services -- CA_IWLAN</p> <h3>Certificate Issued</h3> <p>The certificate you requested was issued to you.</p> <p> Install this certificate</p>
6.	Confirm the warning that a new certificate is installed on your computer with Yes .	 <p>Potential Scripting Violation</p> <p>This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on the computer and gain access to your data. Do you want this program to add the certificates now? Click Yes if you trust the Web site. Otherwise, click No.</p> <p><input type="button" value="Yes"/> <input type="button" value="No"/></p>
7.	A new certificate has been created. Restart your computer to make all changes effective.	
8.	Open the command window by clicking start-> Run.... Enter mmc as a command and click OK .	

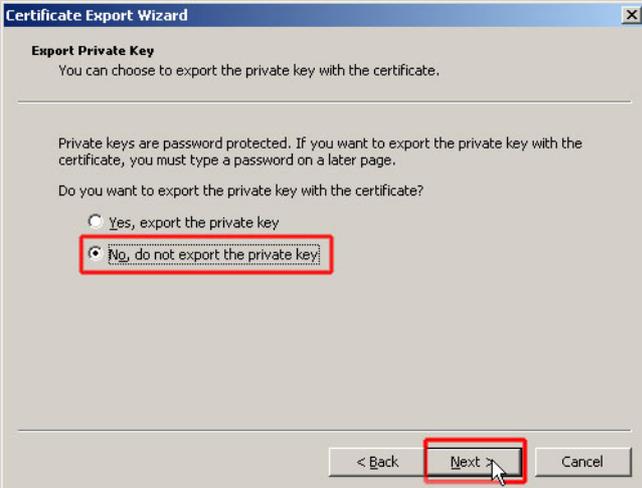
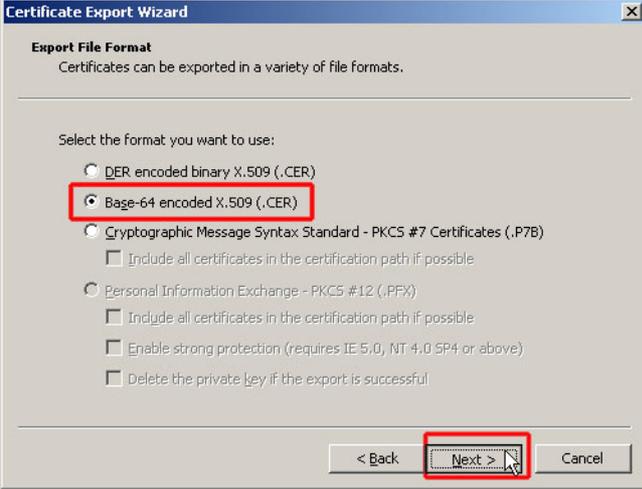
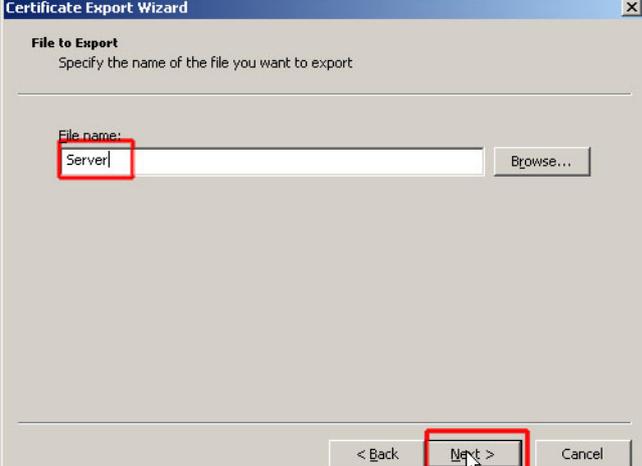
No.	Action	Comment
9.	A new console window opens.	 <p>The screenshot shows the 'Console' application window. The 'Console Root' folder is selected in the left pane, and the right pane displays the message 'There are no items to show in this view.'</p>
10.	Select the Console Root folder and add new attributes using File->Add/Remove Snap In...	 <p>The screenshot shows the 'Console' application window with the 'File' menu open. The 'Add/Remove Snap-in...' option is highlighted, and the keyboard shortcut 'Ctrl+H' is visible next to it.</p>
11.	A new dialog box opens. Click Add....	 <p>The screenshot shows the 'Add/Remove Snap-in' dialog box. The 'Standalone' tab is selected. The 'Snap-ins added to:' field contains 'Console Root'. The 'Add...' button is highlighted with a red box.</p>

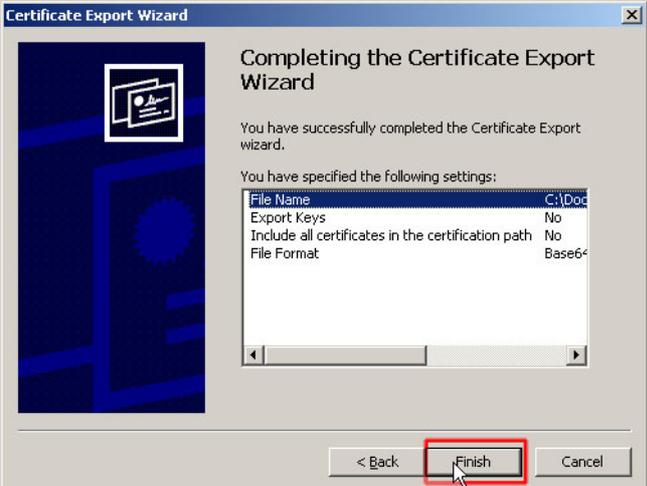
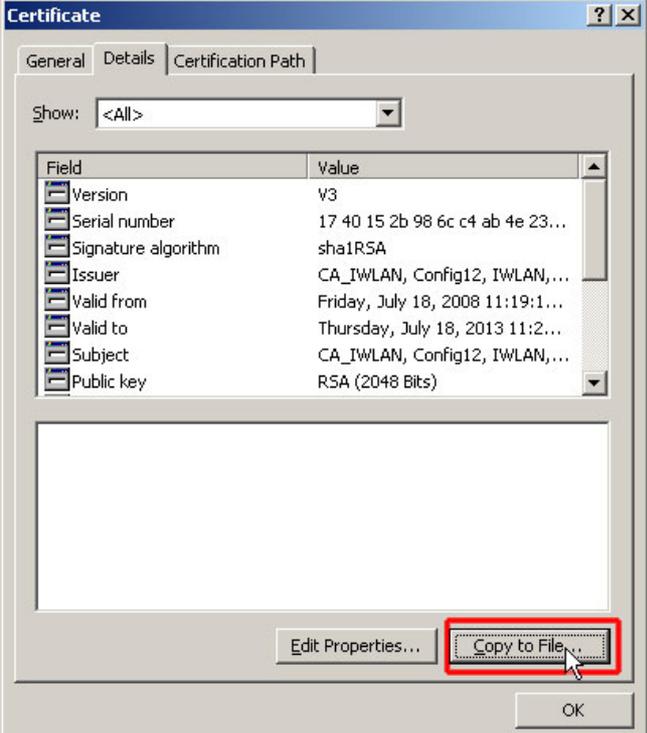
No.	Action	Comment
12.	Select Certificates from the list and click Add .	 <p>The screenshot shows the 'Add Standalone Snap-in' dialog box. It contains a list of available snap-ins with columns for 'Snap-in' and 'Vendor'. The 'Certificates' snap-in is selected and highlighted with a red box. Below the list is a description: 'The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.' At the bottom right, the 'Add' button is highlighted with a red box.</p>
13.	To view the certificates of the computer, select Computer account . Click Next> .	 <p>The screenshot shows the 'Certificates snap-in' dialog box. It asks 'This snap-in will always manage certificates for:' with three radio button options: 'My user account', 'Service account', and 'Computer account'. The 'Computer account' option is selected and highlighted with a red box. At the bottom right, the 'Next >' button is highlighted with a red box.</p>
14.	Select the local computer and close the dialog box with Finish .	 <p>The screenshot shows the 'Certification Authority' dialog box. It asks 'Select the computer you want this snap-in to manage.' Below this, it says 'This snap-in will always manage:' with two radio button options: 'Local computer: [the computer this console is running on]' and 'Another computer:'. The 'Local computer' option is selected and highlighted with a red box. At the bottom right, the 'Finish' button is highlighted with a red box.</p>

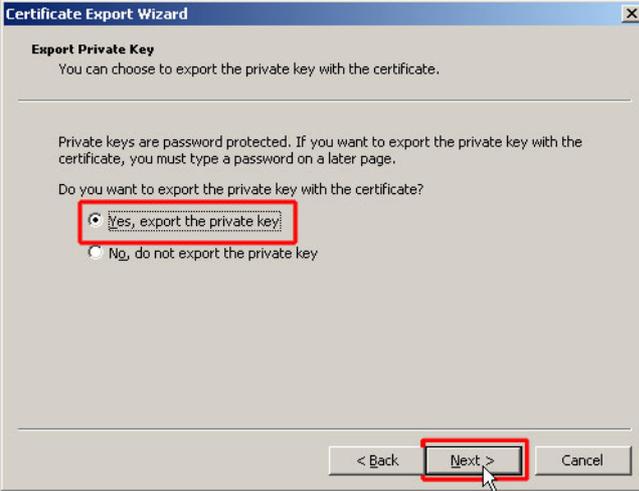
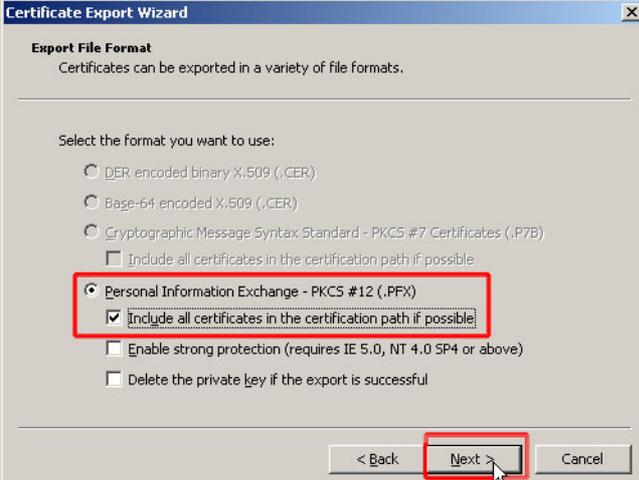
No.	Action	Comment
15.	The list with the possible snap-ins is displayed again. Select Certification Authority and click Add .	 <p>The screenshot shows the 'Add Standalone Snap-in' dialog box. It features a list of available snap-ins with columns for 'Snap-in' and 'Vendor'. The 'Certification Authority' snap-in is highlighted with a red box. Below the list is a description: 'The Certification Authority snap-in allows you to configure the Certification Authority and manage certificates.' At the bottom right, the 'Add' button is highlighted with a red box, and a mouse cursor is pointing at it.</p>
16.	Select the local computer and close the dialog box with Finish .	 <p>The screenshot shows the 'Certification Authority' dialog box. It prompts the user to 'Select the computer you want this snap-in to manage.' Under the heading 'This snap-in will always manage:', the 'Local computer: [the computer this console is running on]' radio button is selected and highlighted with a red box. There is also an 'Another computer:' field with a 'Browse...' button. At the bottom, the 'Finish' button is highlighted with a red box, and a mouse cursor is pointing at it.</p>

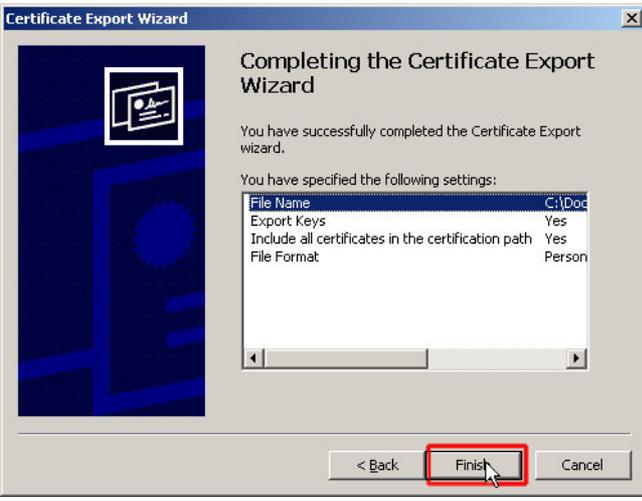
No.	Action	Comment
17.	Close the list with the snap-ins that are available with Close .	 <p>The screenshot shows the 'Add Standalone Snap-in' dialog box. It features a table of available snap-ins with columns for 'Snap-in' and 'Vendor'. The 'Certification Authority' snap-in is selected. Below the table is a description field. At the bottom right, the 'Close' button is highlighted with a red rectangular box.</p>
18.	Close the dialog box with OK .	 <p>The screenshot shows the 'Add/Remove Snap-in' dialog box with the 'Standalone' tab selected. It displays a list of installed snap-ins under the 'Console Root'. The 'OK' button at the bottom right is highlighted with a red rectangular box.</p>

No.	Action	Comment																		
19.	<p>Select the newly created certificate of the CA_IWLAN certification authority under Certificates->Personal->Certificates and double-click.</p>	 <p>The screenshot shows the 'Certificates (Local Computer)' window with the 'Personal' store selected. Under 'Certificates', a certificate issued by 'CA_IWLAN' is visible. The 'Issued To' field is highlighted.</p>																		
20.	<p>The certificate properties appear. Change to the Details tab. A server certificate is exported first. Click Copy to File.</p>	 <p>The screenshot shows the 'Certificate' dialog box with the 'Details' tab selected. The 'Field' and 'Value' table is visible:</p> <table border="1" data-bbox="754 891 1331 1137"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Version</td> <td>V3</td> </tr> <tr> <td>Serial number</td> <td>17 40 15 2b 98 6c c4 ab 4e 23...</td> </tr> <tr> <td>Signature algorithm</td> <td>sha1RSA</td> </tr> <tr> <td>Issuer</td> <td>CA_IWLAN, Config12, IWLAN,...</td> </tr> <tr> <td>Valid from</td> <td>Friday, July 18, 2008 11:19:1...</td> </tr> <tr> <td>Valid to</td> <td>Thursday, July 18, 2013 11:2...</td> </tr> <tr> <td>Subject</td> <td>CA_IWLAN, Config12, IWLAN,...</td> </tr> <tr> <td>Public key</td> <td>RSA (2048 Bits)</td> </tr> </tbody> </table> <p>The 'Copy to File...' button is highlighted with a red box.</p>	Field	Value	Version	V3	Serial number	17 40 15 2b 98 6c c4 ab 4e 23...	Signature algorithm	sha1RSA	Issuer	CA_IWLAN, Config12, IWLAN,...	Valid from	Friday, July 18, 2008 11:19:1...	Valid to	Thursday, July 18, 2013 11:2...	Subject	CA_IWLAN, Config12, IWLAN,...	Public key	RSA (2048 Bits)
Field	Value																			
Version	V3																			
Serial number	17 40 15 2b 98 6c c4 ab 4e 23...																			
Signature algorithm	sha1RSA																			
Issuer	CA_IWLAN, Config12, IWLAN,...																			
Valid from	Friday, July 18, 2008 11:19:1...																			
Valid to	Thursday, July 18, 2013 11:2...																			
Subject	CA_IWLAN, Config12, IWLAN,...																			
Public key	RSA (2048 Bits)																			
21.	<p>The Certificate Export Wizard opens. Click Next to go to the next step.</p>	 <p>The screenshot shows the 'Certificate Export Wizard' window with the 'Welcome to the Certificate Export Wizard' screen. The 'Next >' button is highlighted with a red box.</p>																		

No.	Action	Comment
22.	The private key is not to be exported. Tick the appropriate box. Click Next >.	 <p>Certificate Export Wizard</p> <p>Export Private Key You can choose to export the private key with the certificate.</p> <p>Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.</p> <p>Do you want to export the private key with the certificate?</p> <p><input type="radio"/> Yes, export the private key</p> <p><input checked="" type="radio"/> No, do not export the private key</p> <p>< Back Next > Cancel</p>
23.	The certificate is to be Base-64 encoded . Click Next to go to the next step.	 <p>Certificate Export Wizard</p> <p>Export File Format Certificates can be exported in a variety of file formats.</p> <p>Select the format you want to use:</p> <p><input type="radio"/> DER encoded binary X.509 (.CER)</p> <p><input checked="" type="radio"/> Base-64 encoded X.509 (.CER)</p> <p><input type="radio"/> Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)</p> <p><input type="checkbox"/> Include all certificates in the certification path if possible</p> <p><input type="radio"/> Personal Information Exchange - PKCS #12 (.PFX)</p> <p><input type="checkbox"/> Include all certificates in the certification path if possible</p> <p><input type="checkbox"/> Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)</p> <p><input type="checkbox"/> Delete the private key if the export is successful</p> <p>< Back Next > Cancel</p>
24.	To differentiate between the certificates, enter Server as a file name. Go to Browse... if you want to change the storage path. Click Next >.	 <p>Certificate Export Wizard</p> <p>File to Export Specify the name of the file you want to export</p> <p>File name: <input type="text" value="Server"/> Browse...</p> <p>< Back Next > Cancel</p>

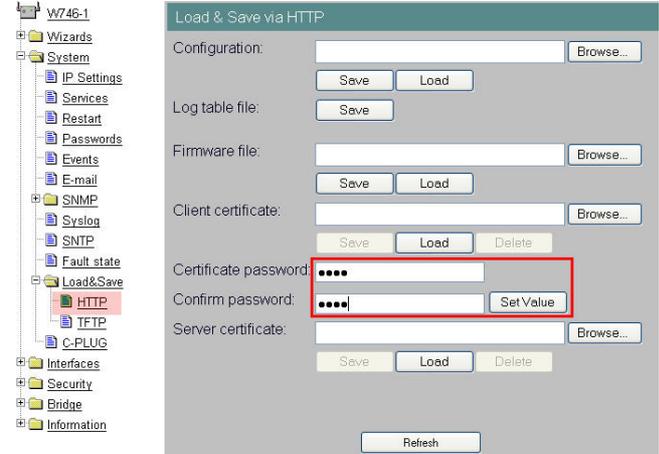
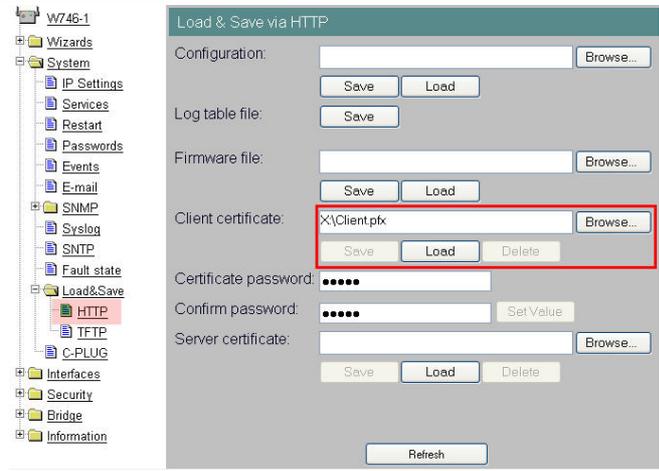
No.	Action	Comment																		
25.	<p>Exit the Certificate Export Wizard with Finish.</p> <p>The path under which the certificate has been stored is displayed under File Name.</p>																			
26.	<p>Then the certificate is downloaded for the client. Click Copy to File again.</p>	 <table border="1" data-bbox="751 1055 1326 1301"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Version</td> <td>V3</td> </tr> <tr> <td>Serial number</td> <td>17 40 15 2b 98 6c c4 ab 4e 23...</td> </tr> <tr> <td>Signature algorithm</td> <td>sha1RSA</td> </tr> <tr> <td>Issuer</td> <td>CA_IWLAN, Config12, IWLAN,...</td> </tr> <tr> <td>Valid from</td> <td>Friday, July 18, 2008 11:19:1...</td> </tr> <tr> <td>Valid to</td> <td>Thursday, July 18, 2013 11:2...</td> </tr> <tr> <td>Subject</td> <td>CA_IWLAN, Config12, IWLAN,...</td> </tr> <tr> <td>Public key</td> <td>RSA (2048 Bits)</td> </tr> </tbody> </table>	Field	Value	Version	V3	Serial number	17 40 15 2b 98 6c c4 ab 4e 23...	Signature algorithm	sha1RSA	Issuer	CA_IWLAN, Config12, IWLAN,...	Valid from	Friday, July 18, 2008 11:19:1...	Valid to	Thursday, July 18, 2013 11:2...	Subject	CA_IWLAN, Config12, IWLAN,...	Public key	RSA (2048 Bits)
Field	Value																			
Version	V3																			
Serial number	17 40 15 2b 98 6c c4 ab 4e 23...																			
Signature algorithm	sha1RSA																			
Issuer	CA_IWLAN, Config12, IWLAN,...																			
Valid from	Friday, July 18, 2008 11:19:1...																			
Valid to	Thursday, July 18, 2013 11:2...																			
Subject	CA_IWLAN, Config12, IWLAN,...																			
Public key	RSA (2048 Bits)																			

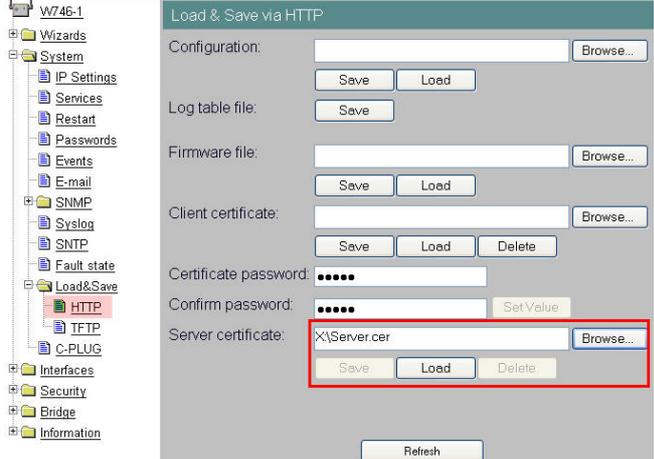
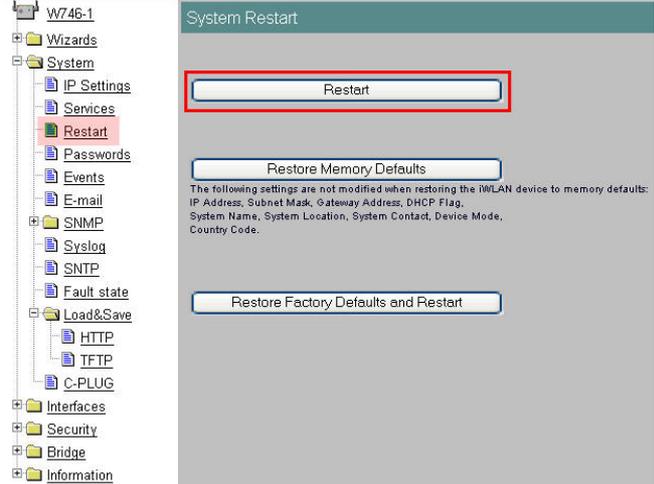
No.	Action	Comment
27.	The Certificate Export Wizard opens again. Click Next to go to the next step.	 <p>Certificate Export Wizard</p> <p>Welcome to the Certificate Export Wizard</p> <p>This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.</p> <p>A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.</p> <p>To continue, click Next.</p> <p>< Back Next > Cancel</p>
28.	You can now select whether the private key is to be exported as well. Click Next> .	 <p>Certificate Export Wizard</p> <p>Export Private Key</p> <p>You can choose to export the private key with the certificate.</p> <p>Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.</p> <p>Do you want to export the private key with the certificate?</p> <p><input checked="" type="radio"/> Yes, export the private key</p> <p><input type="radio"/> No, do not export the private key</p> <p>< Back Next > Cancel</p>
29.	Only one format is allowed for the export file. Activate the first checkbox and deactivate the checkbox in the middle. Click Next to go to the next step.	 <p>Certificate Export Wizard</p> <p>Export File Format</p> <p>Certificates can be exported in a variety of file formats.</p> <p>Select the format you want to use:</p> <p><input type="radio"/> DER, encoded binary X.509 (.CER)</p> <p><input type="radio"/> Base-64 encoded X.509 (.CER)</p> <p><input type="radio"/> Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)</p> <p><input type="checkbox"/> Include all certificates in the certification path if possible</p> <p><input checked="" type="radio"/> Personal Information Exchange - PKCS #12 (.PFX)</p> <p><input checked="" type="checkbox"/> Include all certificates in the certification path if possible</p> <p><input type="checkbox"/> Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)</p> <p><input type="checkbox"/> Delete the private key if the export is successful</p> <p>< Back Next > Cancel</p>

No.	Action	Comment
30.	<p>Enter the password to be used to protect the private key. (Here: W746)</p> <p>Note: Note this password because it will be required for uploading the certificates to the SCALANCE W746-1.</p>	
31.	<p>Enter Client as a file name to make it easier to differentiate between the certificates. Go to Browse... if you want to change the storage path. Click Next>.</p>	
32.	<p>Close the Certificate Export Wizard with Finish. The path under which the certificate has been stored is displayed under File Name.</p>	
33.	<p>Close the certificate properties with OK.</p>	

Load certificates to W746-1

Table 5-23

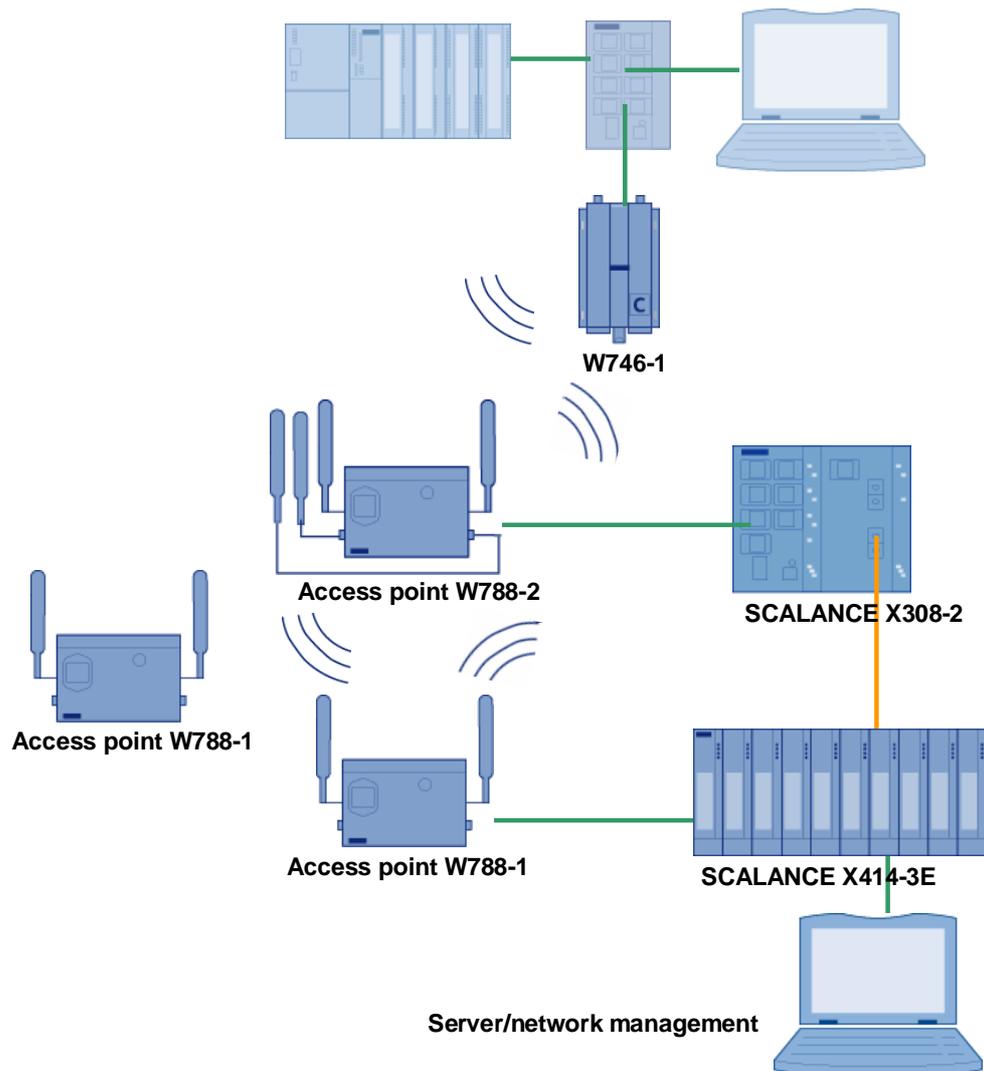
No.	Action	Comment
1.	Connect the server PC to the SCALANCE X108.	
2.	Open the web-based management for the SCALANCE W746-1 and log on.	http://172.158.1.8
3.	Navigate to system->Load&Save->http . Enter the password you have assigned for the private key (Table 5-22 line 30) (Here: W746). Click Set Values .	
4.	Click Browse... under Client certificate to navigate to the path where you have stored the certificates (Table 5-22). Open the Client certificate and load it by clicking Load .	

No.	Action	Comment
5.	Click Browse... under Server certificate to navigate to the path where you have stored the certificates you just exported (Table 5-22). Open the Server certificate and load it by clicking Load .	
6.	Go to the Restart menu item and restart the SCALANCE.	
7.	Log on again after restarting. Navigate to security->Basic WLAN . The size of the loaded certificates is displayed in bytes.	
8.	Connect the server PC to the SCALANCE X414-3E. From now on, you can start the web-based management of the SCALANCE W746-2 also using the SCALANCE W788-2.	

5.8 Syslog messages

The **Syslog** function is configured in **all** SCALANCE X modules and access points.

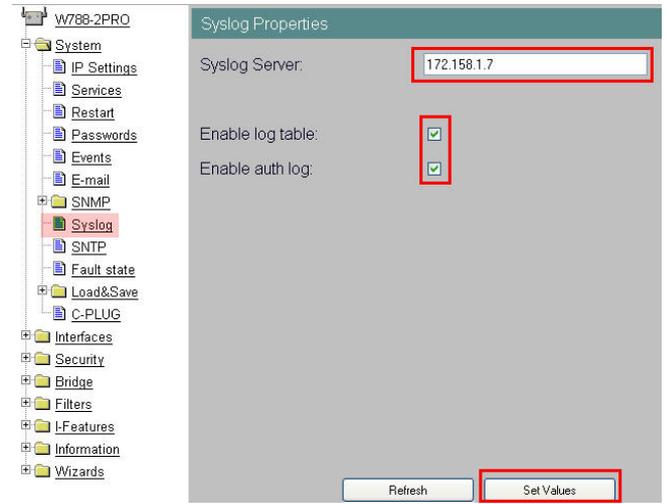
Figure 5-6



Settings on the SCALANCE W

The table below shows the necessary configuration steps on the SCALANCE W788-2. The other SCALANCE W modules are configured analogously.

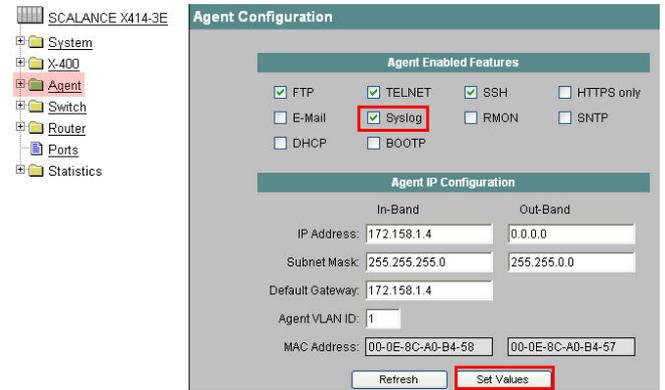
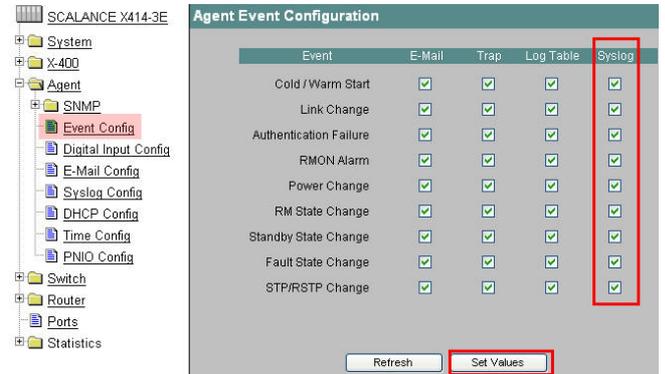
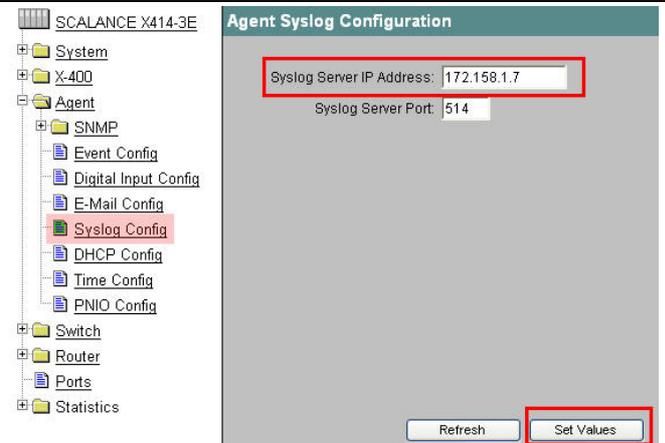
Table 5-24

No.	Action	Comment
9.	Open the web-based management for the SCALANCE W788-2.	http://172.158.1.3
10.	Navigate to System->syslog . Enter the Syslog Server (172.158.1.7) and activate both checkboxes. Accept the settings with Set Values .	

Note Configure the other SCALANCE W in the same way.

Settings on the SCALANCE X

The following table shows the necessary configuration steps on the SCALANCE X414-3E. The other SCALANCE X modules are configured analogously.

No.	Action	Comment
1.	Open the web-based management for the SCALANCE X414-3E	http://172.158.1.4
2.	Navigate to Agent and activate Syslog. Accept the settings with Set Values .	
3.	Change to the Event Config subitem and activate the messages you want to have displayed via Syslog. Accept your settings with Set Values .	
4.	Change to the Syslog Config submenu. Enter the Syslog Server (172.158.1.7) . Accept the settings with Set Values .	

Note Configure the SCALANCE X308-2 in the same way.

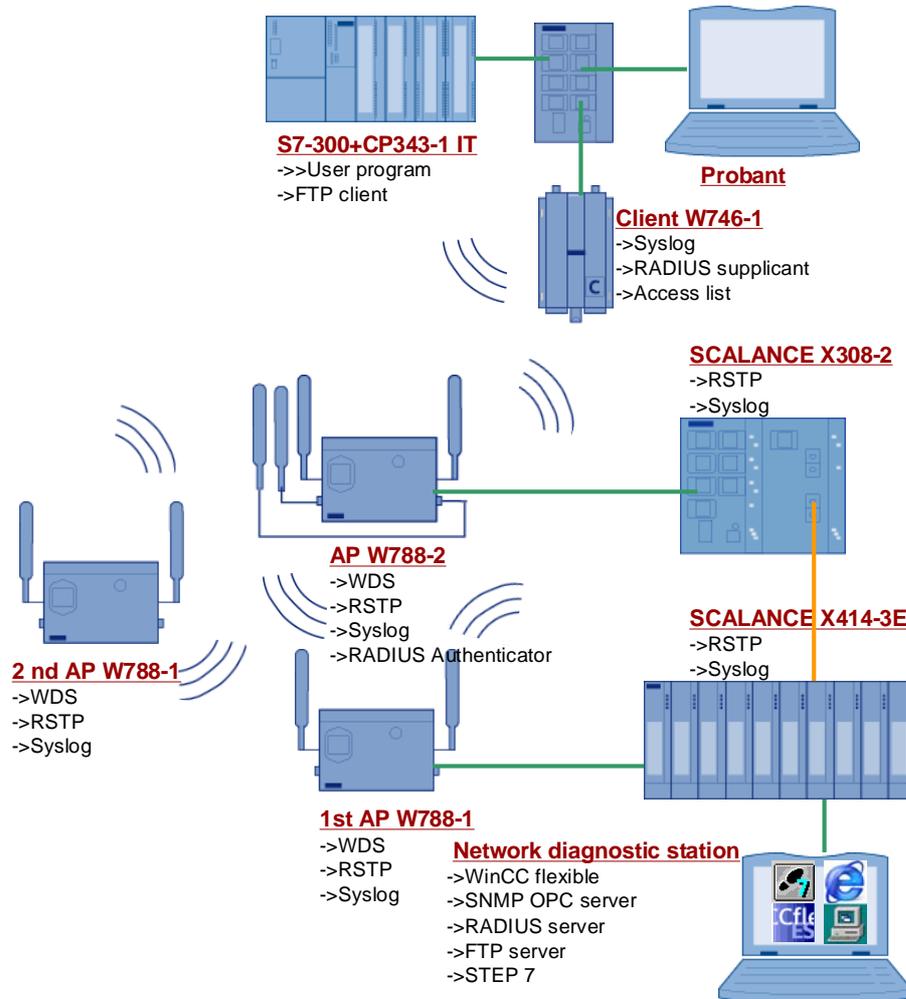
Configuring the Syslog server

Kiwi Syslog Daemon is used as a Syslog server. This program can be started without special configuration. It listens for Syslog messages on port 514 and provides these as a plain text message.

6 Operating scenarios in the sample network

Overview of the entire network

Figure 6-1



Copyright © Siemens AG 2008 All rights reserved
30805917_SCALANCE_W_OFFICE_DOKU_v10_en.doc

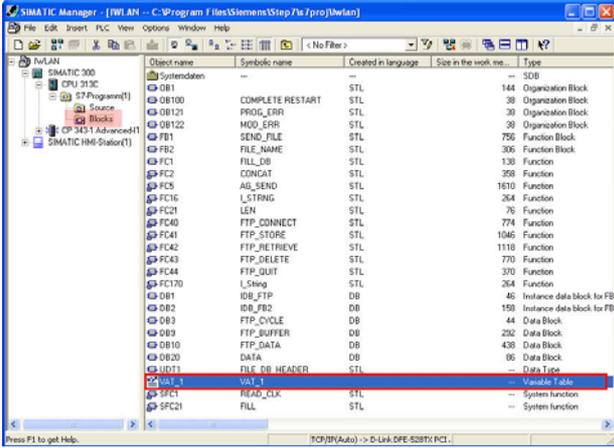
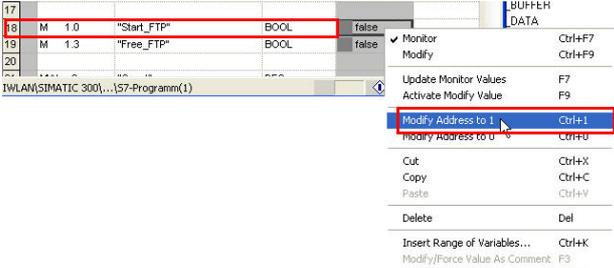
Preparation

Start or open all programs that have been installed for this application on the server.

- JanaServer with **Start->Programs->JanaServer 2->JanaAdmin**
- Syslog software with **Start->Programs>Kiwi Enterprises->Kiwi Syslog Daemon->Kiwi Syslog Daemon**

6.1 FTP scenario

Table 6-1

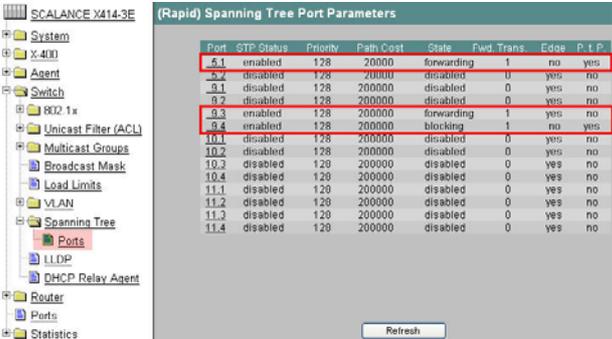
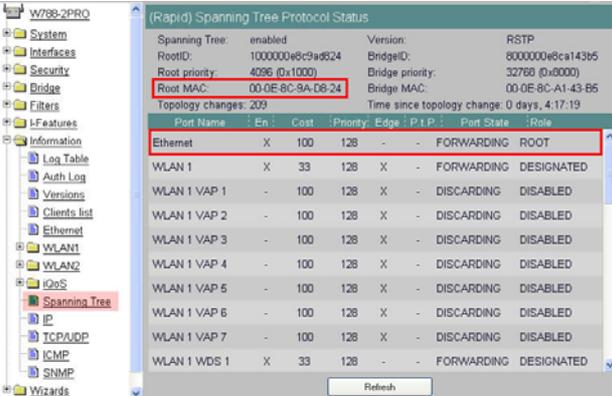
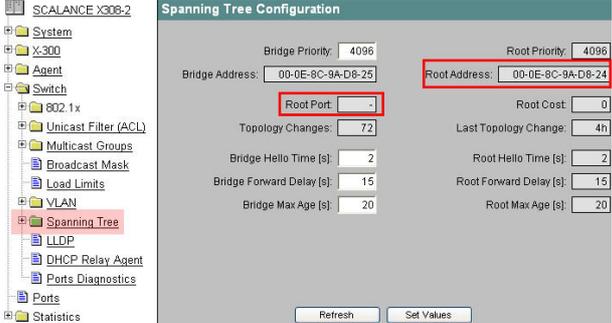
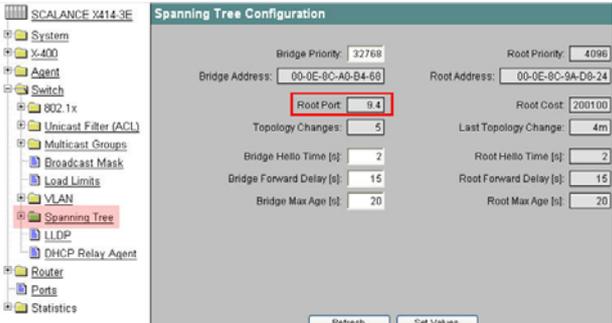
No.	Action	Comment
1.	<p>Open the SIMATIC MANAGER and the IWLAN STEP 7 project. Navigate to SIMATIC 300->CPU 313C->S7-Program->Blocks and double-click the variables table VAR1.</p>	
2.	<p>Use your right mouse button to click the status of line 18 (M1.0) and change the status to 1. This starts the cyclical FTP transfer.</p>	
3.	<p>During the first FTP transfer, a file is created in the directory C:\ on the server PC. This file is cyclically updated by new values.</p>	

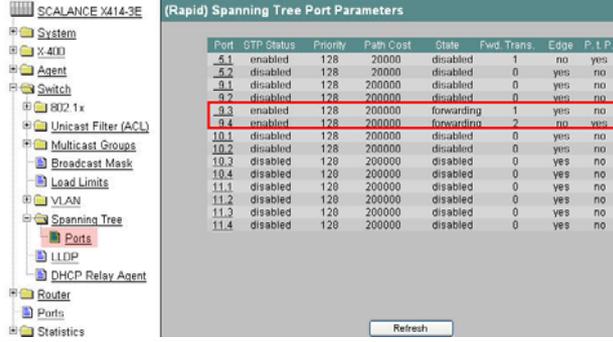
6.2 Redundancy scenario

As soon as the topology of the network changes, the RSTP function is activated. This scenario shows the option of testing and reporting RSTP.

Table 6-2

No.	Action	Comment
1.	<p>By setting the priority in the SCALANCE X308-2 this module is forced to become the root bridge.</p> <p>Open the web-based management of the SCALANCE X308-2 (172.158.1.5) and navigate to Switch-> Spanning Tree.</p> <p>Here you can see the MAC address of the root bridge and the root port. Since this module is the root bridge itself, there is no root port.</p>	<p>The screenshot shows the 'Spanning Tree Configuration' page for SCALANCE X308-2. The 'Root Address' field is highlighted with a red box and contains the value '00-0E-8C-9A-D8-24'. The 'Root Port' field is also highlighted with a red box and contains the value '5.1'. Other fields include Bridge Priority (4096), Root Priority (4096), Bridge Address (00-0E-8C-9A-D8-25), Topology Changes (72), Last Topology Change (4h), Bridge Hello Time (2s), Root Hello Time (2s), Bridge Forward Delay (15s), Root Forward Delay (15s), Bridge Max Age (20s), and Root Max Age (20s).</p>
2.	<p>Under Switch-> Spanning Tree->Ports you can see which ports are blocked or enabled.</p>	<p>The screenshot shows the '(Rapid) Spanning Tree Port Parameters' table for SCALANCE X308-2. The table has columns: Port, STP Status, Priority, Path Cost, State, Fwd. Trans., Edge, P, I, P. Ports 6 and 10 are highlighted with red boxes. Port 6 is 'enabled' and in 'forwarding' state. Port 10 is 'enabled' and in 'forwarding' state. Other ports (1-5, 7-9) are 'disabled'.</p>
3.	<p>Open the web-based management of the SCALANCE X414-3E (172.158.1.4) and navigate to Switch-> Spanning Tree.</p> <p>Here you can see the MAC address of the root bridge (SCALANCE 308-2) and the root port.</p>	<p>The screenshot shows the 'Spanning Tree Configuration' page for SCALANCE X414-3E. The 'Root Address' field is highlighted with a red box and contains the value '00-0E-8C-9A-D8-24'. The 'Root Port' field is also highlighted with a red box and contains the value '5.1'. Other fields include Bridge Priority (32768), Root Priority (4096), Bridge Address (00-0E-8C-A0-B4-68), Topology Changes (4), Last Topology Change (5h), Bridge Hello Time (2s), Root Hello Time (2s), Bridge Forward Delay (15s), Root Forward Delay (15s), Bridge Max Age (20s), and Root Max Age (20s).</p>

No.	Action	Comment																																																																																																																								
4.	Under Switch-> Spanning Tree->Ports you can see which ports are blocked or enabled.	 <table border="1" data-bbox="898 389 1358 728"> <thead> <tr> <th>Port</th> <th>STP Status</th> <th>Priority</th> <th>Path Cost</th> <th>State</th> <th>Fwd. Trans</th> <th>Edges</th> <th>P. T. P.</th> </tr> </thead> <tbody> <tr><td>5.1</td><td>enabled</td><td>128</td><td>20000</td><td>forwarding</td><td>1</td><td>no</td><td>yes</td></tr> <tr><td>5.2</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>9.1</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>9.2</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>9.3</td><td>enabled</td><td>128</td><td>20000</td><td>forwarding</td><td>1</td><td>yes</td><td>no</td></tr> <tr><td>9.4</td><td>enabled</td><td>128</td><td>20000</td><td>blocking</td><td>1</td><td>no</td><td>yes</td></tr> <tr><td>10.1</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.2</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.3</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.4</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.1</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.2</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.3</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.4</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> </tbody> </table>	Port	STP Status	Priority	Path Cost	State	Fwd. Trans	Edges	P. T. P.	5.1	enabled	128	20000	forwarding	1	no	yes	5.2	disabled	128	20000	disabled	0	yes	no	9.1	disabled	128	20000	disabled	0	yes	no	9.2	disabled	128	20000	disabled	0	yes	no	9.3	enabled	128	20000	forwarding	1	yes	no	9.4	enabled	128	20000	blocking	1	no	yes	10.1	disabled	128	20000	disabled	0	yes	no	10.2	disabled	128	20000	disabled	0	yes	no	10.3	disabled	128	20000	disabled	0	yes	no	10.4	disabled	128	20000	disabled	0	yes	no	11.1	disabled	128	20000	disabled	0	yes	no	11.2	disabled	128	20000	disabled	0	yes	no	11.3	disabled	128	20000	disabled	0	yes	no	11.4	disabled	128	20000	disabled	0	yes	no
Port	STP Status	Priority	Path Cost	State	Fwd. Trans	Edges	P. T. P.																																																																																																																			
5.1	enabled	128	20000	forwarding	1	no	yes																																																																																																																			
5.2	disabled	128	20000	disabled	0	yes	no																																																																																																																			
9.1	disabled	128	20000	disabled	0	yes	no																																																																																																																			
9.2	disabled	128	20000	disabled	0	yes	no																																																																																																																			
9.3	enabled	128	20000	forwarding	1	yes	no																																																																																																																			
9.4	enabled	128	20000	blocking	1	no	yes																																																																																																																			
10.1	disabled	128	20000	disabled	0	yes	no																																																																																																																			
10.2	disabled	128	20000	disabled	0	yes	no																																																																																																																			
10.3	disabled	128	20000	disabled	0	yes	no																																																																																																																			
10.4	disabled	128	20000	disabled	0	yes	no																																																																																																																			
11.1	disabled	128	20000	disabled	0	yes	no																																																																																																																			
11.2	disabled	128	20000	disabled	0	yes	no																																																																																																																			
11.3	disabled	128	20000	disabled	0	yes	no																																																																																																																			
11.4	disabled	128	20000	disabled	0	yes	no																																																																																																																			
5.	To trace the RSTP status in the access points, open the web-based management (e.g., 172.158.1.3) and navigate to Information->Spanning Tree .	 <table border="1" data-bbox="898 741 1358 1137"> <thead> <tr> <th>Port Name</th> <th>En</th> <th>Cost</th> <th>Priority</th> <th>Edge</th> <th>P. T. P.</th> <th>Port State</th> <th>Role</th> </tr> </thead> <tbody> <tr><td>Ethernet</td><td>X</td><td>100</td><td>128</td><td>-</td><td>-</td><td>FORWARDING</td><td>ROOT</td></tr> <tr><td>WLAN 1</td><td>X</td><td>33</td><td>128</td><td>X</td><td>-</td><td>FORWARDING</td><td>DESIGNATED</td></tr> <tr><td>WLAN 1 VAP 1</td><td>-</td><td>100</td><td>128</td><td>X</td><td>-</td><td>DISCARDING</td><td>DISABLED</td></tr> <tr><td>WLAN 1 VAP 2</td><td>-</td><td>100</td><td>128</td><td>X</td><td>-</td><td>DISCARDING</td><td>DISABLED</td></tr> <tr><td>WLAN 1 VAP 3</td><td>-</td><td>100</td><td>128</td><td>X</td><td>-</td><td>DISCARDING</td><td>DISABLED</td></tr> <tr><td>WLAN 1 VAP 4</td><td>-</td><td>100</td><td>128</td><td>X</td><td>-</td><td>DISCARDING</td><td>DISABLED</td></tr> <tr><td>WLAN 1 VAP 5</td><td>-</td><td>100</td><td>128</td><td>X</td><td>-</td><td>DISCARDING</td><td>DISABLED</td></tr> <tr><td>WLAN 1 VAP 6</td><td>-</td><td>100</td><td>128</td><td>X</td><td>-</td><td>DISCARDING</td><td>DISABLED</td></tr> <tr><td>WLAN 1 VAP 7</td><td>-</td><td>100</td><td>128</td><td>X</td><td>-</td><td>DISCARDING</td><td>DISABLED</td></tr> <tr><td>WLAN 1 WDS 1</td><td>X</td><td>33</td><td>128</td><td>-</td><td>-</td><td>FORWARDING</td><td>DESIGNATED</td></tr> </tbody> </table>	Port Name	En	Cost	Priority	Edge	P. T. P.	Port State	Role	Ethernet	X	100	128	-	-	FORWARDING	ROOT	WLAN 1	X	33	128	X	-	FORWARDING	DESIGNATED	WLAN 1 VAP 1	-	100	128	X	-	DISCARDING	DISABLED	WLAN 1 VAP 2	-	100	128	X	-	DISCARDING	DISABLED	WLAN 1 VAP 3	-	100	128	X	-	DISCARDING	DISABLED	WLAN 1 VAP 4	-	100	128	X	-	DISCARDING	DISABLED	WLAN 1 VAP 5	-	100	128	X	-	DISCARDING	DISABLED	WLAN 1 VAP 6	-	100	128	X	-	DISCARDING	DISABLED	WLAN 1 VAP 7	-	100	128	X	-	DISCARDING	DISABLED	WLAN 1 WDS 1	X	33	128	-	-	FORWARDING	DESIGNATED																																
Port Name	En	Cost	Priority	Edge	P. T. P.	Port State	Role																																																																																																																			
Ethernet	X	100	128	-	-	FORWARDING	ROOT																																																																																																																			
WLAN 1	X	33	128	X	-	FORWARDING	DESIGNATED																																																																																																																			
WLAN 1 VAP 1	-	100	128	X	-	DISCARDING	DISABLED																																																																																																																			
WLAN 1 VAP 2	-	100	128	X	-	DISCARDING	DISABLED																																																																																																																			
WLAN 1 VAP 3	-	100	128	X	-	DISCARDING	DISABLED																																																																																																																			
WLAN 1 VAP 4	-	100	128	X	-	DISCARDING	DISABLED																																																																																																																			
WLAN 1 VAP 5	-	100	128	X	-	DISCARDING	DISABLED																																																																																																																			
WLAN 1 VAP 6	-	100	128	X	-	DISCARDING	DISABLED																																																																																																																			
WLAN 1 VAP 7	-	100	128	X	-	DISCARDING	DISABLED																																																																																																																			
WLAN 1 WDS 1	X	33	128	-	-	FORWARDING	DESIGNATED																																																																																																																			
6.	Remove the SC plug from port 5.1 of the SCALANCE X414-3E.	The path created can no longer be used and the components must be reorganized.																																																																																																																								
7.	Open the web-based management of the SCALANCE X308-2 (172.158.1.5) and navigate to Switch-> Spanning Tree . The SCALANCE X308-2 is still the root bridge because the priority has not changed.																																																																																																																									
8.	Open the web-based management of the SCALANCE X414-3E (172.158.1.4) and navigate to Switch-> Spanning Tree . The root port has changed.																																																																																																																									

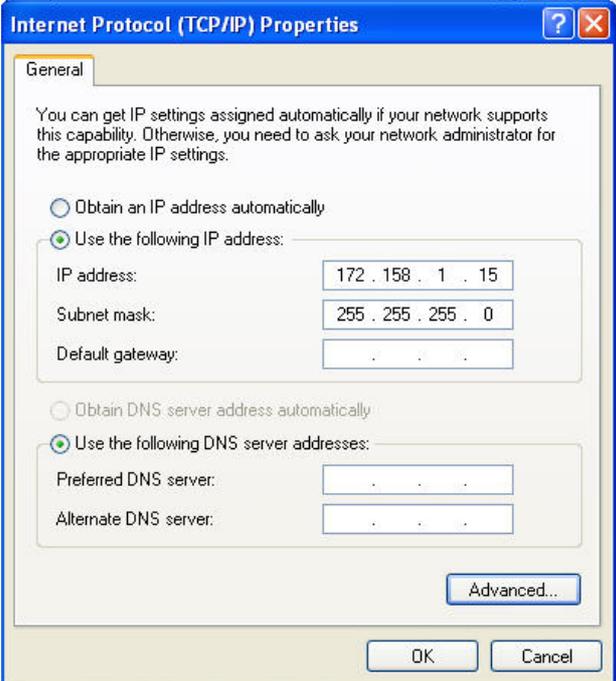
No.	Action	Comment																																																																																																																								
9.	You can see under switch->Spanning Tree->Ports that the port that was blocked before is now active.	 <table border="1" data-bbox="900 405 1353 734"> <thead> <tr> <th>Port</th> <th>STP Status</th> <th>Priority</th> <th>Path Cost</th> <th>State</th> <th>Fwd. Trans.</th> <th>Edge</th> <th>P. T. P.</th> </tr> </thead> <tbody> <tr><td>8.1</td><td>enabled</td><td>128</td><td>20000</td><td>disabled</td><td>1</td><td>no</td><td>yes</td></tr> <tr><td>8.2</td><td>disabled</td><td>128</td><td>20000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>8.1</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>8.2</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>8.3</td><td>enabled</td><td>128</td><td>200000</td><td>forwarding</td><td>1</td><td>yes</td><td>no</td></tr> <tr><td>8.4</td><td>enabled</td><td>128</td><td>200000</td><td>forwarding</td><td>2</td><td>no</td><td>yes</td></tr> <tr><td>10.1</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.2</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.3</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>10.4</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.1</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.2</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.3</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> <tr><td>11.4</td><td>disabled</td><td>128</td><td>200000</td><td>disabled</td><td>0</td><td>yes</td><td>no</td></tr> </tbody> </table>	Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P. T. P.	8.1	enabled	128	20000	disabled	1	no	yes	8.2	disabled	128	20000	disabled	0	yes	no	8.1	disabled	128	200000	disabled	0	yes	no	8.2	disabled	128	200000	disabled	0	yes	no	8.3	enabled	128	200000	forwarding	1	yes	no	8.4	enabled	128	200000	forwarding	2	no	yes	10.1	disabled	128	200000	disabled	0	yes	no	10.2	disabled	128	200000	disabled	0	yes	no	10.3	disabled	128	200000	disabled	0	yes	no	10.4	disabled	128	200000	disabled	0	yes	no	11.1	disabled	128	200000	disabled	0	yes	no	11.2	disabled	128	200000	disabled	0	yes	no	11.3	disabled	128	200000	disabled	0	yes	no	11.4	disabled	128	200000	disabled	0	yes	no
Port	STP Status	Priority	Path Cost	State	Fwd. Trans.	Edge	P. T. P.																																																																																																																			
8.1	enabled	128	20000	disabled	1	no	yes																																																																																																																			
8.2	disabled	128	20000	disabled	0	yes	no																																																																																																																			
8.1	disabled	128	200000	disabled	0	yes	no																																																																																																																			
8.2	disabled	128	200000	disabled	0	yes	no																																																																																																																			
8.3	enabled	128	200000	forwarding	1	yes	no																																																																																																																			
8.4	enabled	128	200000	forwarding	2	no	yes																																																																																																																			
10.1	disabled	128	200000	disabled	0	yes	no																																																																																																																			
10.2	disabled	128	200000	disabled	0	yes	no																																																																																																																			
10.3	disabled	128	200000	disabled	0	yes	no																																																																																																																			
10.4	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.1	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.2	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.3	disabled	128	200000	disabled	0	yes	no																																																																																																																			
11.4	disabled	128	200000	disabled	0	yes	no																																																																																																																			
10.	A short message about the topology change is passed on to the Syslog server.																																																																																																																									

6.3 Access control scenario

Access control

The access list protects the management of the SCALANCE W746-1 against unwanted access.

Table 6-3

No.	Action	Comment
1.	Connect the test PG/PC to the SCALANCE X108 and open the web-based management of the SCALANCE W746-1. Since the text PG/PC (172.158.1.9) has an IP address that is enabled in the IP range of the SCALANCE W746-1 module, the PC is allowed to access the management.	
2.	Change the IP address of the test PG/PC. Open the Internet Protocol (TCP/IP) Properties using Start -> Settings -> Network Connection -> Local Connections . Select the option field Use the following IP address and fill in the fields as shown in the figure. Close the dialog box with OK .	

No.	Action	Comment
3.	Since the IP address is now outside the configured address range, the access to the web-based management is denied.	

RADIUS

The RADIUS function is used to protect a network against unauthorized access by third persons. In this application, the SCALANCE W746-1 can only log on to the access point W788-2, once the module has successfully authenticated on the RADIUS server.

Table 6-4

No.	Action	Comment
1.	Turn on the server PC that also runs the RADIUS server and connect all components to each other (see Figure 2-1).	
2.	Use the freeware tool Wireshark to view the protocol communication between the modules. The SCALANCE W746-1 sends a query with the configured login name and password to the SCALANCE W788-2, which passes on this message to the RADIUS server. Login name: W746 Password: RADIUS_Authentication	<pre> RADIUS Protocol Code: Access-Request (1) Packet identifier: 0x9 (9) Length: 225 Authenticator: 5AFE33Cd209d7Ad850B11D302F7C1A7A Attribute Value Pairs AVP: l=18 t=Message-Authenticator(80): 6157325A76977EE1FC297115CE2A6578 AVP: l=6 t=Service-Type(6): Framed-User (2) AVP: l=7 t=User-Name(1): W746\000 User-Name: w746 AVP: l=6 t=Framed-MTU(12): 1488 AVP: l=25 t=State(24): 178A02BF000001370001AC9E010700000003165C07B700 AVP: l=29 t=Called-Station-Id(30): 00-0E-8C-A1-43-C0:BlackHole AVP: l=19 t=Calling-Station-Id(31): 00-0E-8C-98-C1-F1 AVP: l=8 t=NAS-Identifier(32): W788-2 AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19) AVP: l=24 t=Connect-Info(77): CONNECT 54Mbps 802.11a AVP: l=31 t=EAP-Message(79) Last segment [1] AVP: l=6 t=NAS-IP-Address(4): 172.158.1.3 AVP: l=6 t=NAS-Port(5): 1 AVP: l=14 t=NAS-Port-Id(87): STA port # 1 </pre>

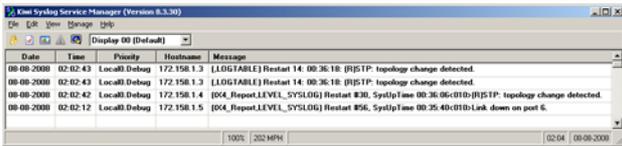
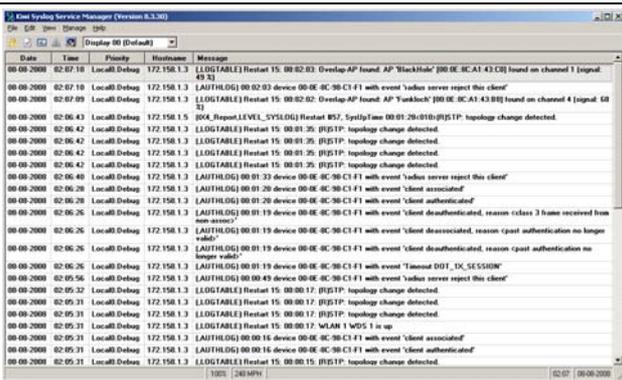
No.	Action	Comment
3.	<p>Since a user with this data has been created in the RADIUS server, the SCALANCE W746-1 is allowed to access the network.</p>	<pre> RADIUS Protocol Code: Access-Accept (2) Packet identifier: 0xa (10) Length: 271 Authenticator: 1EFF7CDBEC95BE67DB44A5122DD11A5B [This is a response to a request in frame 344] [Time from request: 0.002818000 seconds] Attribute Value Pairs AVP: l=6 t=Framed-Protocol(7): PPP(1) AVP: l=6 t=Service-type(6): Login-User(1) Service-type: Login-User (1) AVP: l=6 t=EAP-Message(79) Last Segment [1] AVP: l=32 t=Class(25): 538505C5000001370001AC9E010701C8F8A679C96D040000... AVP: l=16 t=Vendor-Specific(26) v=Microsoft(311) AVP: l=51 t=Vendor-Specific(26) v=Microsoft(311) AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311) AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311) AVP: l=18 t=Message-Authenticator(80): DEB7690122D45FE658595267089190AB </pre>
4.	<p>As soon as you exit the RADIUS server (e.g., by shutting the computer down) and restart the SCALANCE W788-2, the SCALANCE W746-1 has no longer access to the network.</p>	

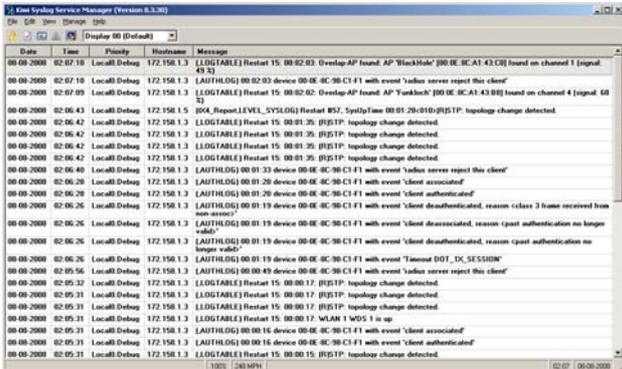
6.4 Diagnosis scenario

This chapter illustrates how the Syslog functions and SNMP variables in the SCALANCE can be used for diagnosis.

Syslog

Table 6-5

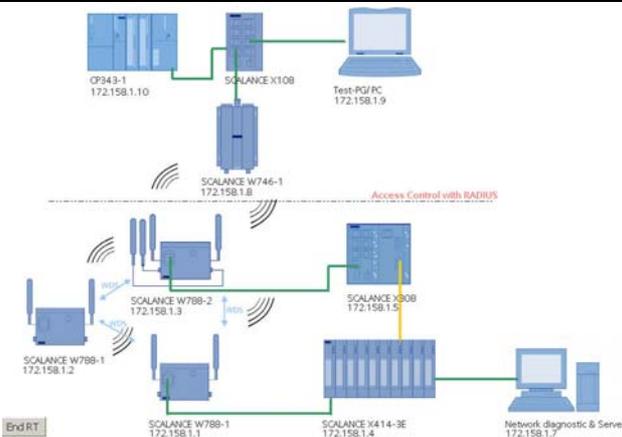
No.	Action	Comment
1.	Disconnect the cable from one port of the SCALANCE X308-2 or the SCALANCE X414-3E. The link down is transmitted as a short message to the server. If the topology is also changed by this, a Syslog message is sent to the server.	 <p>The screenshot shows a Syslog Service Manager window with a table of log entries. The entries include: <ul style="list-style-type: none"> 08-09-2008 02:02:43 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 14: 00:36:18 (RIS:TP) topology change detected. 08-09-2008 02:02:43 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 14: 00:36:18 (RIS:TP) topology change detected. 08-09-2008 02:02:42 Local0 Debug 172.158.1.4 [04_Report.LEVEL_SYSLOG] Restart #30: SyslogTime 00:36:06:010(RIS:TP) topology change detected. 08-09-2008 02:02:12 Local0 Debug 172.158.1.5 [04_Report.LEVEL_SYSLOG] Restart #36: SyslogTime 00:35:40:010(Link down on port 6). </p>
2.	Restart the SCALANCE by briefly switching the power supply off and back on. As soon as the SCALANCE reboots, a Syslog message is sent.	 <p>The screenshot shows a Syslog Service Manager window with a table of log entries. The entries include: <ul style="list-style-type: none"> 08-09-2008 02:02:18 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:02:03: Overlap-AP found: AP 'BlackHole' [00:0E:8C:A1:43:C8] found on channel 1 [signal: 49.5] 08-09-2008 02:02:18 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:02:03: device 00:0E:8C:90:C3:F1 with event 'radius server reject this client' 08-09-2008 02:02:09 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:02:02: Overlap-AP found: AP 'Yanblack' [00:0E:8C:A1:43:8E] found on channel 4 [signal: 68.5] 08-09-2008 02:06:43 Local0 Debug 172.158.1.5 [04_Report.LEVEL_SYSLOG] Restart #52: SyslogTime 00:01:20:010(RIS:TP) topology change detected. 08-09-2008 02:06:42 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:01:20 (RIS:TP) topology change detected. 08-09-2008 02:06:42 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:01:20 (RIS:TP) topology change detected. 08-09-2008 02:06:42 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:01:20 (RIS:TP) topology change detected. 08-09-2008 02:06:40 Local0 Debug 172.158.1.3 (AUTHLOG) 00:01:33 device 00:0E:8C:90:C3:F1 with event 'radius server reject this client' 08-09-2008 02:06:28 Local0 Debug 172.158.1.3 (AUTHLOG) 00:01:20 device 00:0E:8C:90:C3:F1 with event 'blind associated' 08-09-2008 02:06:28 Local0 Debug 172.158.1.3 (AUTHLOG) 00:01:20 device 00:0E:8C:90:C3:F1 with event 'blind authenticated' 08-09-2008 02:06:26 Local0 Debug 172.158.1.3 (AUTHLOG) 00:01:19 device 00:0E:8C:90:C3:F1 with event 'blind deauthenticated, reason: class 3 have received from non access' 08-09-2008 02:06:26 Local0 Debug 172.158.1.3 (AUTHLOG) 00:01:19 device 00:0E:8C:90:C3:F1 with event 'blind deauthenticated, reason: guest authentication no longer valid' 08-09-2008 02:06:26 Local0 Debug 172.158.1.3 (AUTHLOG) 00:01:19 device 00:0E:8C:90:C3:F1 with event 'timed out: DIS_SESSION' 08-09-2008 02:05:56 Local0 Debug 172.158.1.3 (AUTHLOG) 00:00:49 device 00:0E:8C:90:C3:F1 with event 'radius server reject this client' 08-09-2008 02:05:32 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:00:17 (RIS:TP) topology change detected. 08-09-2008 02:05:31 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:00:17 (RIS:TP) topology change detected. 08-09-2008 02:05:31 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:00:17 (RIS:TP) topology change detected. 08-09-2008 02:05:31 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:00:17 (RIS:TP) topology change detected. 08-09-2008 02:05:31 Local0 Debug 172.158.1.3 (AUTHLOG) 00:00:16 device 00:0E:8C:90:C3:F1 with event 'blind associated' 08-09-2008 02:05:31 Local0 Debug 172.158.1.3 (AUTHLOG) 00:00:16 device 00:0E:8C:90:C3:F1 with event 'blind authenticated' 08-09-2008 02:05:31 Local0 Debug 172.158.1.3 (LOGTABLE) Restart 15: 00:00:15 (RIS:TP) topology change detected. </p>
3.	Open the web-based management of any SCALANCE and log on using a wrong password. The Syslog server receives a message that an IP address with a wrong password attempts to access the management.	 <p>The screenshot shows a Syslog Service Manager window with a table of log entries. The entry includes: <ul style="list-style-type: none"> 08-09-2008 02:08:52 Local0 Debug 172.158.1.1 (LOGTABLE) Restart 16: 00:03:20: Authentication Failure: Failed web password from 172.158.1.7 </p>

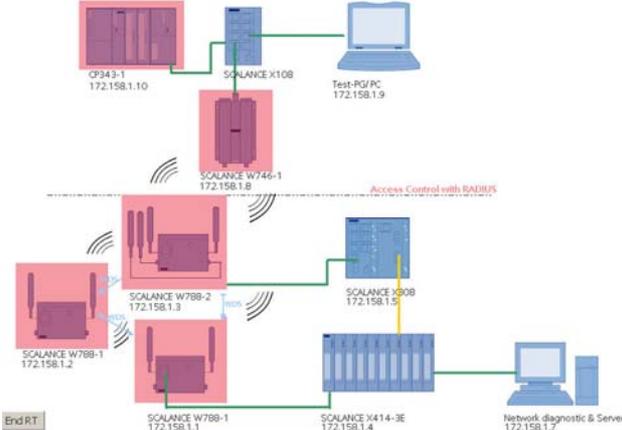
No.	Action	Comment
4.	If a SCALANCE finds several radio networks within its environment, it sends a message to the server.	 <p>The screenshot shows a log window titled 'Log by using WinCC flexible (Version 6.3.30)'. The log contains several entries with columns for Date, Time, Priority, Hostname, and Message. Key messages include: 'Development-AP found AP "BlackHole" [00:0E:8C:A1:43:C0] found on channel 1 [signal: 49.9]', 'device 00:0E:8C:90:C3:F1 with event "radius server reject this client"', 'Development-AP found AP "YunBlack" [00:0E:8C:A1:43:B0] found on channel 4 [signal: 60.3]', 'SysUpTime 00:01:20:010:[RIS1P]: topology change detected', 'topology change detected', 'device 00:0E:8C:90:C3:F1 with event "radius server reject this client"', 'client associated', 'device 00:0E:8C:90:C3:F1 with event "found authenticated"', 'device 00:0E:8C:90:C3:F1 with event "found deauthenticated, reason: class 3 have received from non-serve"', 'device 00:0E:8C:90:C3:F1 with event "found deauthenticated, reason: cpast authentication no longer valid"', 'device 00:0E:8C:90:C3:F1 with event "Timeout DOT_IC_SESSION"', 'device 00:0E:8C:90:C3:F1 with event "radius server reject this client"', 'topology change detected', 'topology change detected', 'WLAN 1 WDS 1 is up', 'device 00:0E:8C:90:C3:F1 with event "found associated"', and 'device 00:0E:8C:90:C3:F1 with event "found authenticated"'. The log ends with 'topology change detected'.</p>

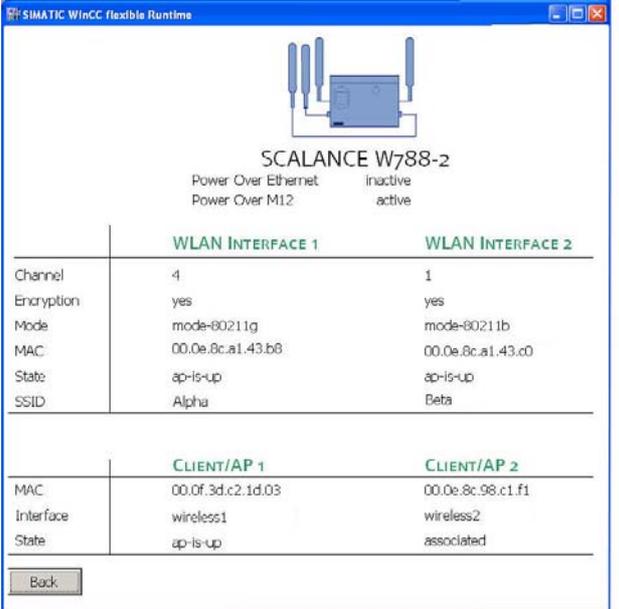
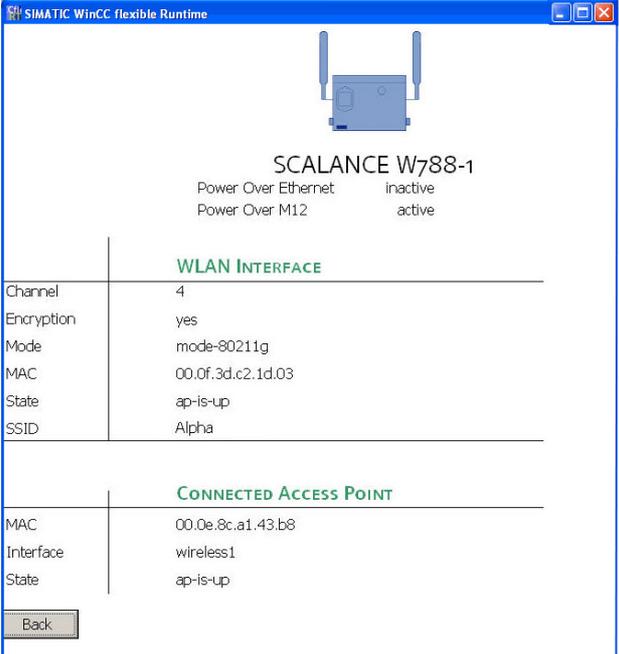
Network visualization

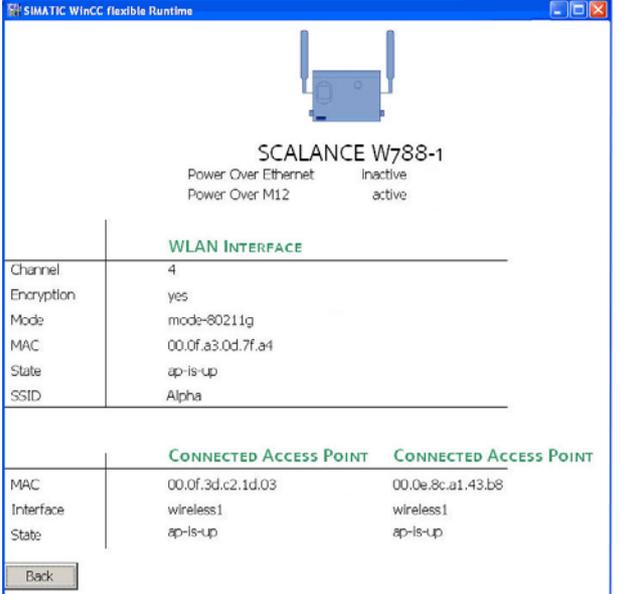
The network visualization feature via WinCC flexible can be used to display and monitor components.

Table 6-6

No.	Action	Comment
1.	Start the WinCC flexible as described in chapter 4.2.4.	
2.	The general overview shows the status of the network in WinCC flexible.	 <p>The diagram illustrates a network topology. At the top left, a device labeled 'CP343-1 172.158.1.10' is connected to 'SCALANCE X108'. This SCALANCE X108 is connected to a 'Test-PC/FC 172.158.1.9'. Below this, 'SCALANCE W746-1 172.158.1.B' is connected to the X108. A red dashed line labeled 'Access Control with RADIUS' separates this section from the one below. Below the line, 'SCALANCE W788-2 172.158.1.3' is connected to 'SCALANCE X808 172.158.1.5'. To the left, 'SCALANCE W788-1 172.158.1.2' is connected to the W788-2. At the bottom, 'SCALANCE W788-1 172.158.1.1' is connected to 'SCALANCE X414-3E 172.158.1.4'. This X414-3E is connected to a 'Network diagnostic & Server 172.158.1.7'. A small box labeled 'End RT' is located at the bottom left of the diagram.</p>

No.	Action	Comment																				
3.	<p>Remove port 6 from the SCALANCE X308-2. First of all, the modules displayed red are no longer available. Only after the topology has changed and an alternative path (i.e. via port 9.4 of the SCALANCE X414-3E) has been found, the connection has been re-established. The reorganization process can take some seconds.</p>																					
4.	<p>Clicking the SCALANCE W746-1 opens the information page. Data on the own WLAN interface and on the connected access point is displayed here.</p>	 <p style="text-align: center;">SCALANCE W746-1</p> <p style="text-align: center;">Power Over Ethernet inactive Power Over M12 active</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="text-align: center; color: green;">WLAN INTERFACE</th> </tr> </thead> <tbody> <tr> <td style="width: 30%;">Channel</td> <td>1</td> </tr> <tr> <td>Encryption</td> <td>yes</td> </tr> <tr> <td>Mode</td> <td>mode-80211b</td> </tr> <tr> <td>MAC</td> <td>00.0e.8c.98.c1.f1</td> </tr> <tr> <td>State</td> <td>ap-is-down</td> </tr> </tbody> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="text-align: center; color: green;">ACCESS POINT</th> </tr> </thead> <tbody> <tr> <td style="width: 30%;">MAC</td> <td>00.0e.8c.a1.43.c0</td> </tr> <tr> <td>Auth. Type</td> <td>wpa2</td> </tr> <tr> <td>State</td> <td>ap-connected</td> </tr> </tbody> </table>	WLAN INTERFACE		Channel	1	Encryption	yes	Mode	mode-80211b	MAC	00.0e.8c.98.c1.f1	State	ap-is-down	ACCESS POINT		MAC	00.0e.8c.a1.43.c0	Auth. Type	wpa2	State	ap-connected
WLAN INTERFACE																						
Channel	1																					
Encryption	yes																					
Mode	mode-80211b																					
MAC	00.0e.8c.98.c1.f1																					
State	ap-is-down																					
ACCESS POINT																						
MAC	00.0e.8c.a1.43.c0																					
Auth. Type	wpa2																					
State	ap-connected																					

No.	Action	Comment																																												
5.	Return to the overall view and click the SCALANCE W788-2. A new window opens and displays information on the WLAN interfaces.	 <table border="1" data-bbox="743 394 1362 1003"> <thead> <tr> <th colspan="2"></th> <th>WLAN INTERFACE 1</th> <th>WLAN INTERFACE 2</th> </tr> </thead> <tbody> <tr> <td>Channel</td> <td></td> <td>4</td> <td>1</td> </tr> <tr> <td>Encryption</td> <td></td> <td>yes</td> <td>yes</td> </tr> <tr> <td>Mode</td> <td></td> <td>mode-80211g</td> <td>mode-80211b</td> </tr> <tr> <td>MAC</td> <td></td> <td>00.0e.8c.a1.43.b8</td> <td>00.0e.8c.a1.43.c0</td> </tr> <tr> <td>State</td> <td></td> <td>ap-is-up</td> <td>ap-is-up</td> </tr> <tr> <td>SSID</td> <td></td> <td>Alpha</td> <td>Beta</td> </tr> </tbody> </table> <table border="1" data-bbox="743 846 1362 952"> <thead> <tr> <th colspan="2"></th> <th>CLIENT/AP 1</th> <th>CLIENT/AP 2</th> </tr> </thead> <tbody> <tr> <td>MAC</td> <td></td> <td>00.0f.3d.c2.1d.03</td> <td>00.0e.8c.98.c1.f1</td> </tr> <tr> <td>Interface</td> <td></td> <td>wireless1</td> <td>wireless2</td> </tr> <tr> <td>State</td> <td></td> <td>ap-is-up</td> <td>associated</td> </tr> </tbody> </table>			WLAN INTERFACE 1	WLAN INTERFACE 2	Channel		4	1	Encryption		yes	yes	Mode		mode-80211g	mode-80211b	MAC		00.0e.8c.a1.43.b8	00.0e.8c.a1.43.c0	State		ap-is-up	ap-is-up	SSID		Alpha	Beta			CLIENT/AP 1	CLIENT/AP 2	MAC		00.0f.3d.c2.1d.03	00.0e.8c.98.c1.f1	Interface		wireless1	wireless2	State		ap-is-up	associated
		WLAN INTERFACE 1	WLAN INTERFACE 2																																											
Channel		4	1																																											
Encryption		yes	yes																																											
Mode		mode-80211g	mode-80211b																																											
MAC		00.0e.8c.a1.43.b8	00.0e.8c.a1.43.c0																																											
State		ap-is-up	ap-is-up																																											
SSID		Alpha	Beta																																											
		CLIENT/AP 1	CLIENT/AP 2																																											
MAC		00.0f.3d.c2.1d.03	00.0e.8c.98.c1.f1																																											
Interface		wireless1	wireless2																																											
State		ap-is-up	associated																																											
6.	Return to the overall view and click the first SCALANCE W788-1. A new window opens and displays information on the WLAN interfaces.	 <table border="1" data-bbox="743 1021 1362 1675"> <thead> <tr> <th colspan="2"></th> <th>WLAN INTERFACE</th> </tr> </thead> <tbody> <tr> <td>Channel</td> <td></td> <td>4</td> </tr> <tr> <td>Encryption</td> <td></td> <td>yes</td> </tr> <tr> <td>Mode</td> <td></td> <td>mode-80211g</td> </tr> <tr> <td>MAC</td> <td></td> <td>00.0f.3d.c2.1d.03</td> </tr> <tr> <td>State</td> <td></td> <td>ap-is-up</td> </tr> <tr> <td>SSID</td> <td></td> <td>Alpha</td> </tr> </tbody> </table> <table border="1" data-bbox="743 1503 1362 1630"> <thead> <tr> <th colspan="2"></th> <th>CONNECTED ACCESS POINT</th> </tr> </thead> <tbody> <tr> <td>MAC</td> <td></td> <td>00.0e.8c.a1.43.b8</td> </tr> <tr> <td>Interface</td> <td></td> <td>wireless1</td> </tr> <tr> <td>State</td> <td></td> <td>ap-is-up</td> </tr> </tbody> </table>			WLAN INTERFACE	Channel		4	Encryption		yes	Mode		mode-80211g	MAC		00.0f.3d.c2.1d.03	State		ap-is-up	SSID		Alpha			CONNECTED ACCESS POINT	MAC		00.0e.8c.a1.43.b8	Interface		wireless1	State		ap-is-up											
		WLAN INTERFACE																																												
Channel		4																																												
Encryption		yes																																												
Mode		mode-80211g																																												
MAC		00.0f.3d.c2.1d.03																																												
State		ap-is-up																																												
SSID		Alpha																																												
		CONNECTED ACCESS POINT																																												
MAC		00.0e.8c.a1.43.b8																																												
Interface		wireless1																																												
State		ap-is-up																																												

No.	Action	Comment												
7.	Return to the overall view and click the second SCALANCE W788-1. A new window opens and displays information on the WLAN interfaces.	 <p>The screenshot shows a window titled 'SIMATIC WinCC flexible Runtime' displaying the configuration for a SCALANCE W788-1 device. At the top, there is a device icon and the text 'SCALANCE W788-1'. Below this, it shows 'Power Over Ethernet' as 'inactive' and 'Power Over M12' as 'active'. A section titled 'WLAN INTERFACE' contains the following details:</p> <table border="1"> <tr><td>Channel</td><td>4</td></tr> <tr><td>Encryption</td><td>yes</td></tr> <tr><td>Mode</td><td>mode-80211g</td></tr> <tr><td>MAC</td><td>00.0f.a3.0d.7f.a4</td></tr> <tr><td>State</td><td>ap-is-up</td></tr> <tr><td>SSID</td><td>Alpha</td></tr> </table> <p>Below the WLAN interface section, there are two columns for 'CONNECTED ACCESS POINT'. The first column shows a MAC address of 00.0f.3d.c2.1d.03 and an interface of wireless1. The second column shows a MAC address of 00.0e.8c.a1.43.b8 and an interface of wireless1. Both access points are in the 'ap-is-up' state. A 'Back' button is located at the bottom left of the window.</p>	Channel	4	Encryption	yes	Mode	mode-80211g	MAC	00.0f.a3.0d.7f.a4	State	ap-is-up	SSID	Alpha
Channel	4													
Encryption	yes													
Mode	mode-80211g													
MAC	00.0f.a3.0d.7f.a4													
State	ap-is-up													
SSID	Alpha													

Appendix and Bibliography

7 Glossary

Table 7-1

Term	Description
WDS	Wireless Distribution Service ; radio network consisting of several access points.
MIB	Management Information Base ; a tree structure containing all the data relevant for network management with SNMP.
SNMP	Simple Network Management Protocol ; standardized protocol for transporting network management information.
RADIUS	Remote Authentication Dial-In User Service ; protocol for authentication, authorization and accounting of users in a network.
RSTP	Rapid Spanning Tree Protocol ; protocol for switching off redundant paths in meshed networks.
Syslog	Protocol; transmitting of messages to a Syslog server in a network.
SSID	Service Set Identifier ; name of the radio network

8 Bibliography

Internet links

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

Table 8-1

	Topic	Title
\1\	Reference to this article	http://support.automation.siemens.com/WW/view/de/30805917
\2\	Siemens I IA Customer Support	http://support.automation.siemens.com
\3\	SCALANCE X Manual	SIMATIC NET Industrial Ethernet Switches SCALANCE X-300 SCALANCE X-400 Configuration Manual (BID: 19625108)
\4\	SCALANCE W78x Manual	SIMATIC NET SCALANCE W784-1xx / SCALANCE W74x-1 Operating Manual (BID: 27094182)
	SCALANCE W Manual	SIMATIC NET SCALANCE W788-xPRO/RR und SCALANCE W74x-1PRO/RR Operating Manual (BID: 28529396)

9 History

Table 9-1 History

Version	Date	Modification
V1.0	04.09.2008	First issue