Application for Communication

applications & TOOLS

Redundancy and Access Control with SCALANCE W

Configuration 12

SIEMENS

Note

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

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

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:

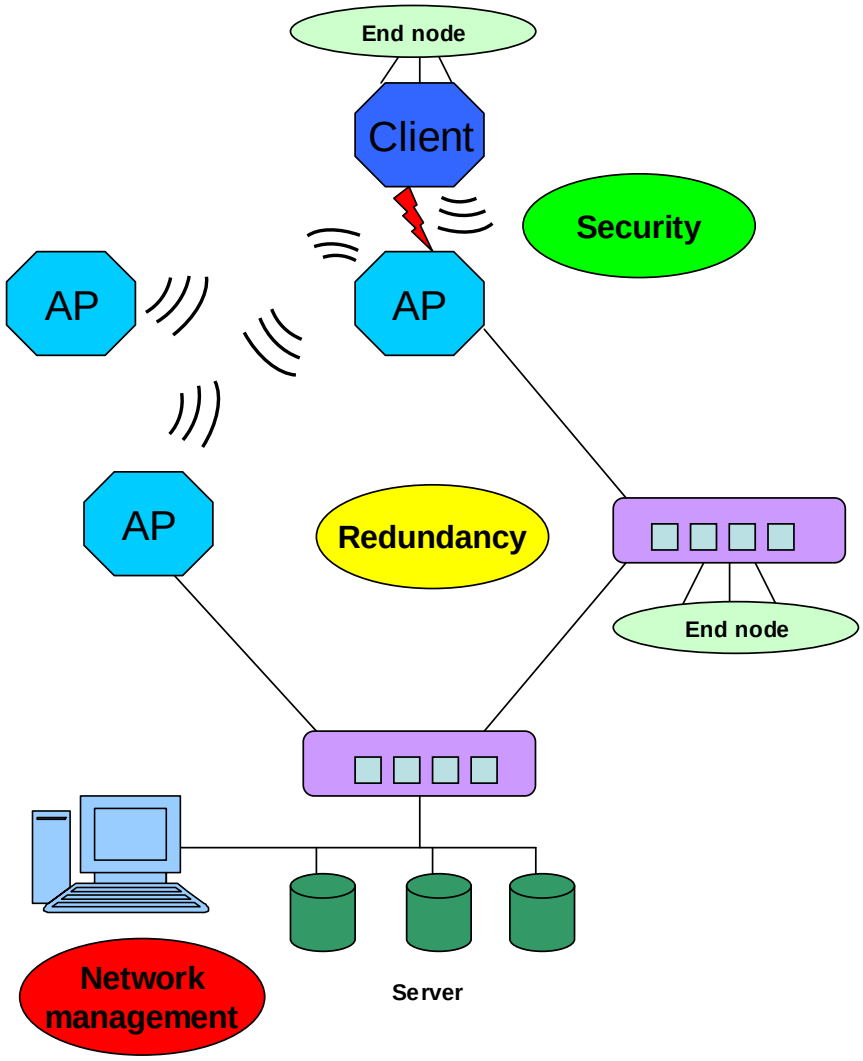
Among other things, wireless LANs provide the following advantages

- 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



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

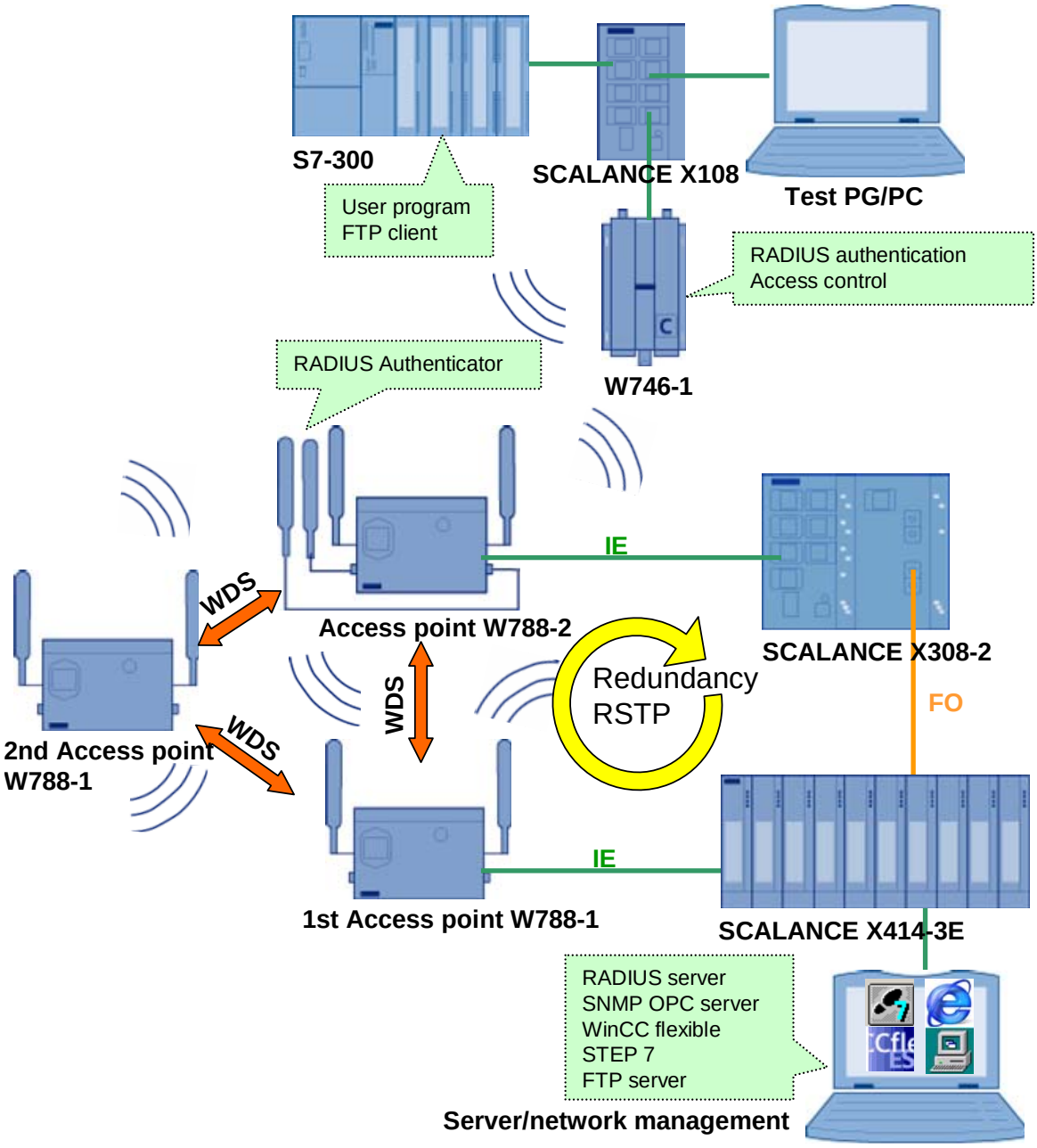
2 Automation solution

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.

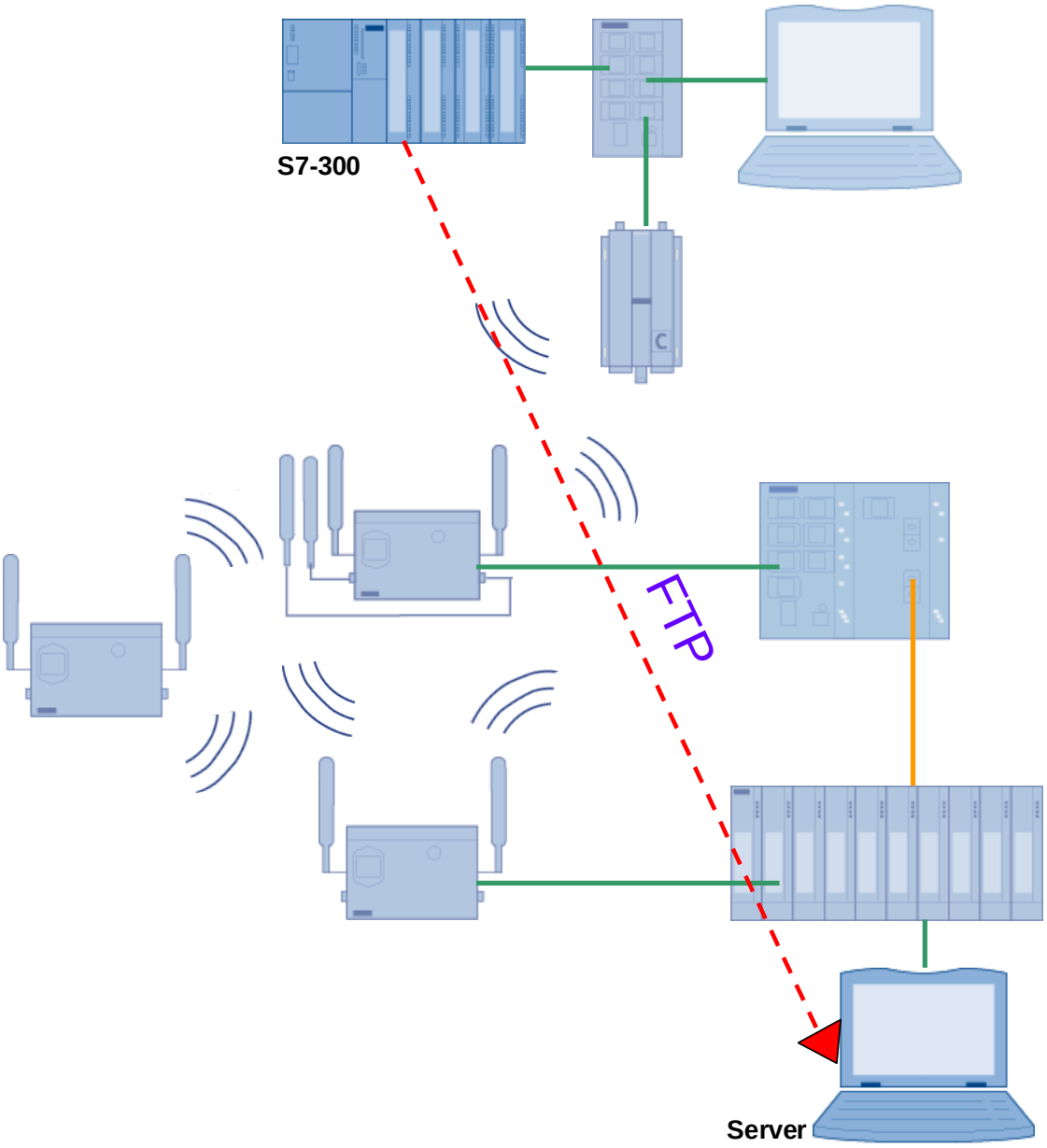
A SIMATIC S7-300 station is connected to the W746-1 client using a CP343-1 Advanced and a SCALANCE X108.

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

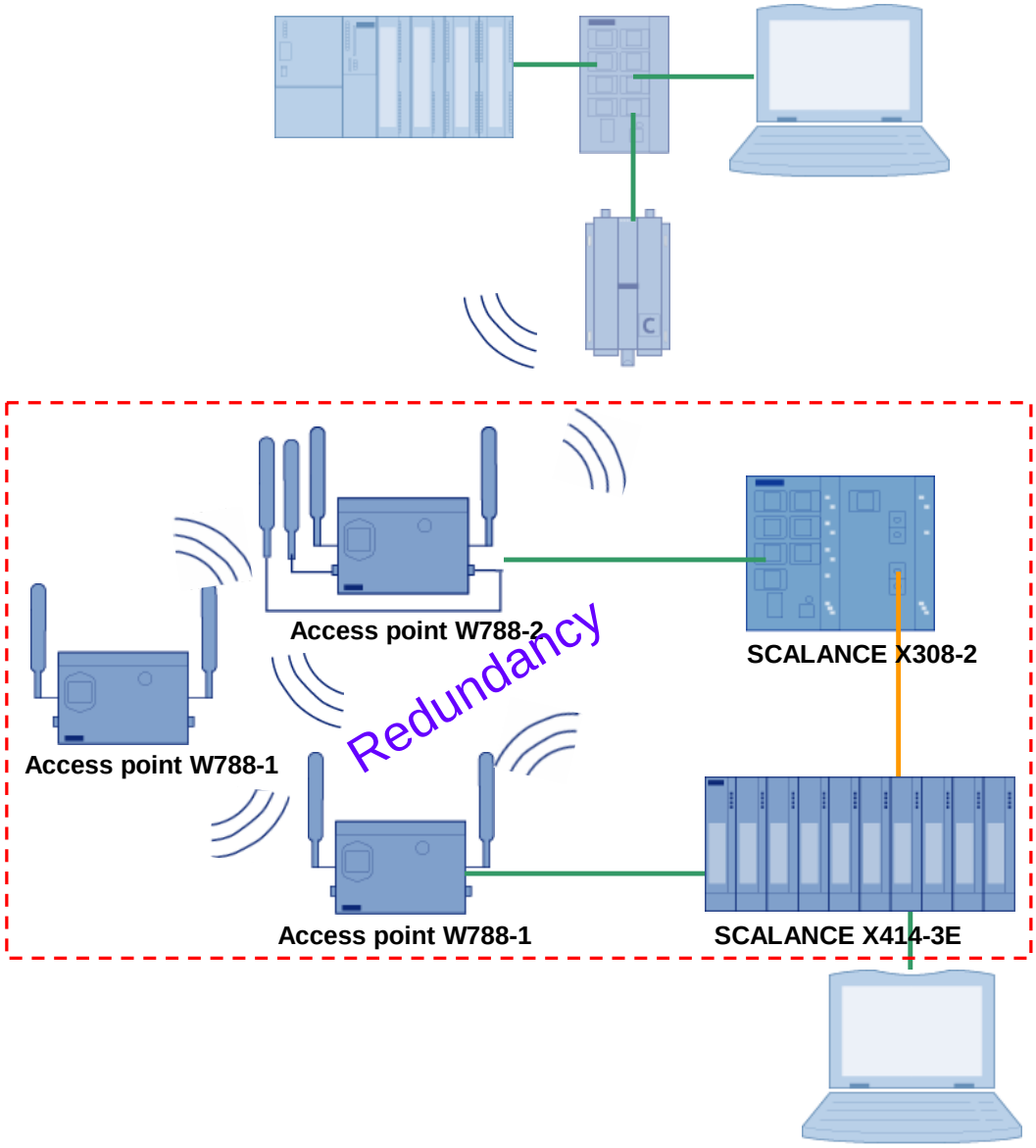


FTP data is exchanged between the S7-300 station and the server PC/PG. Once enabled, the FTP client in the CP343-1 Advanced sends a message to the FTP server every 20 seconds.

Overview of the "redundancy method"

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

Figure 2-3

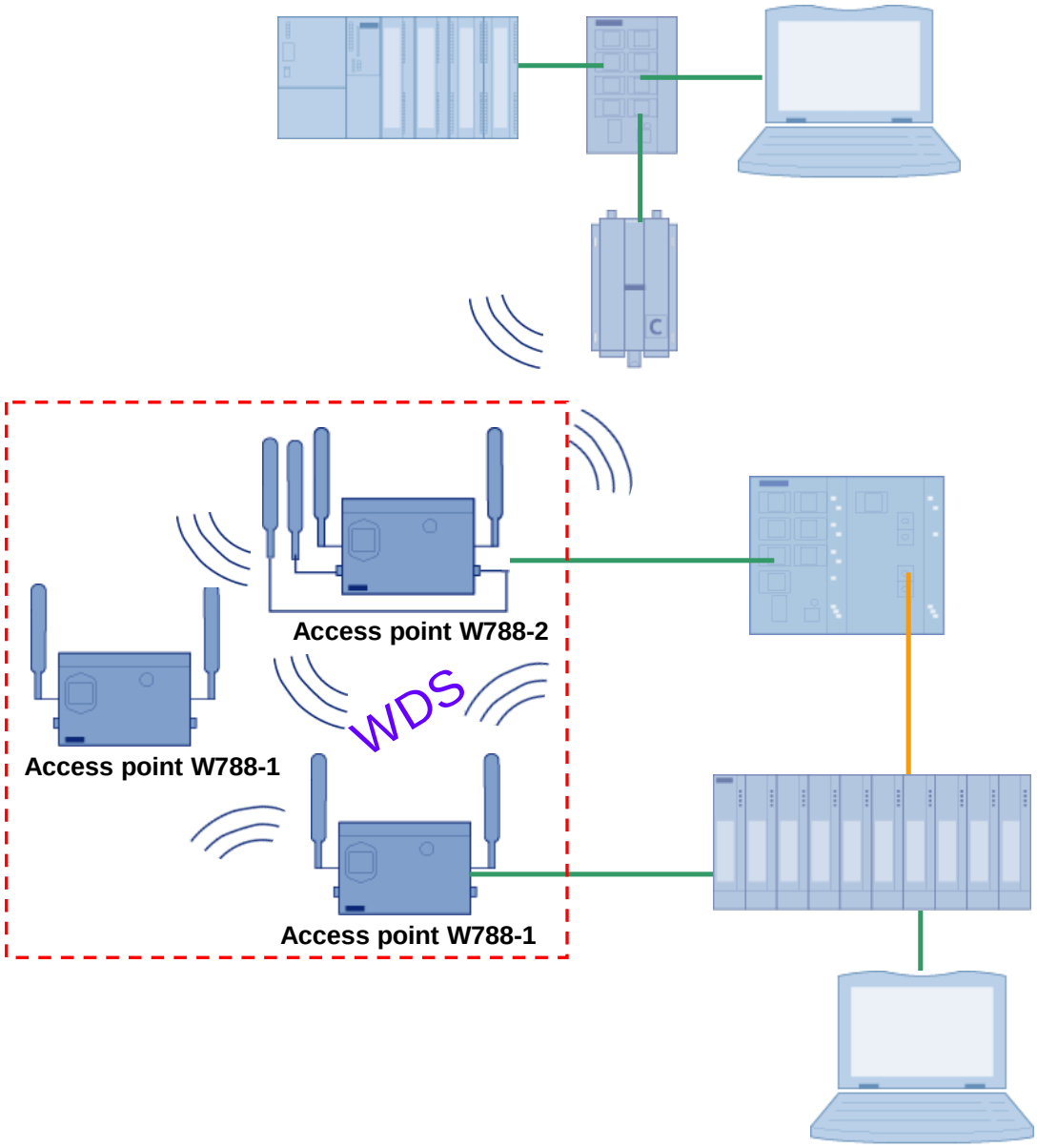


The redundancy method is configured in the two SCALANCE X modules and in the access points. The connection between the two SCALANCE X modules is configured in such a way that is used as the preferred connection.

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

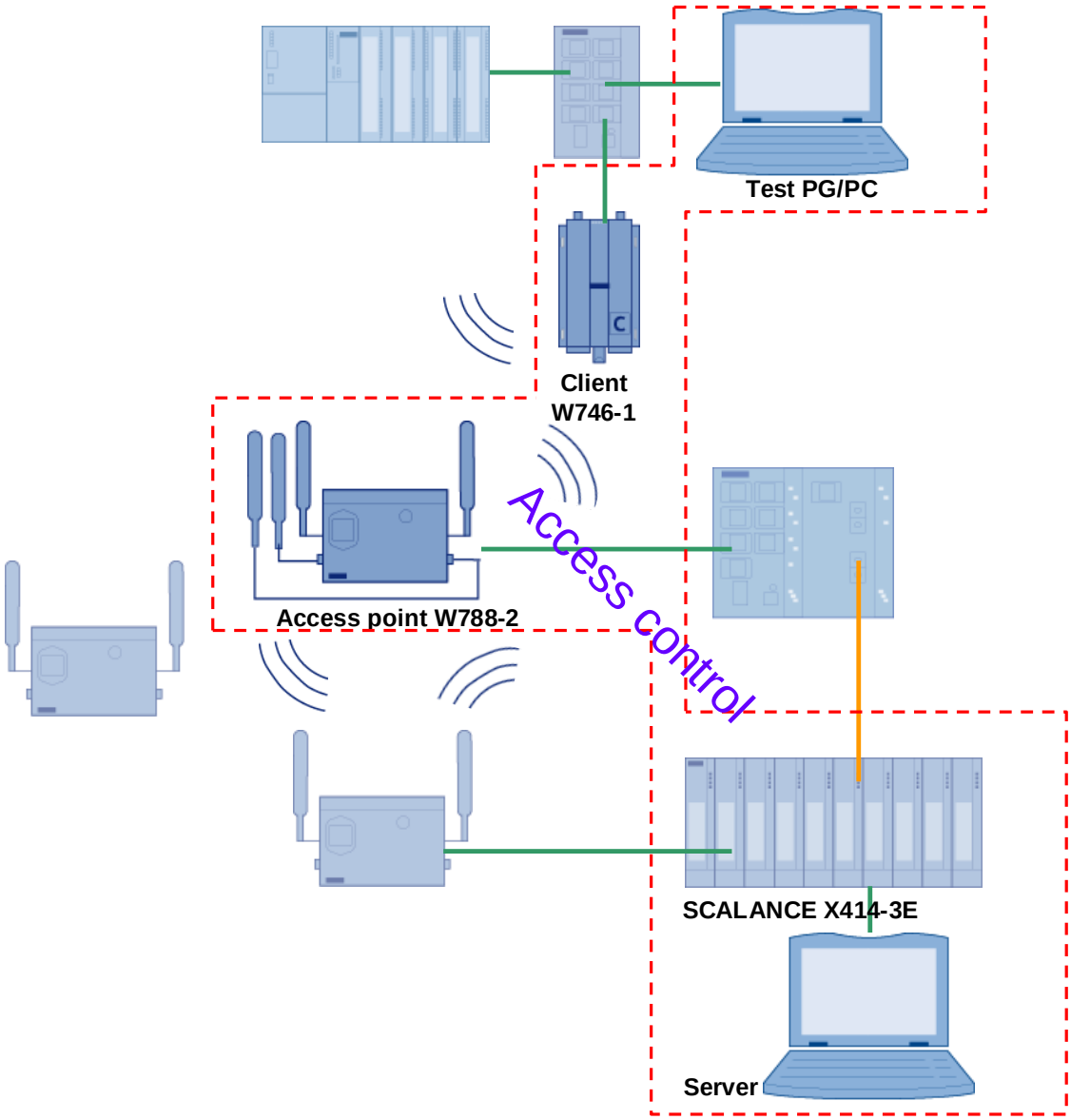


Large-area wireless networks require an appropriate infrastructure. The WDS introduced in this application is configured on all access points.

Overview of the "Access control"

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

Figure 2-5

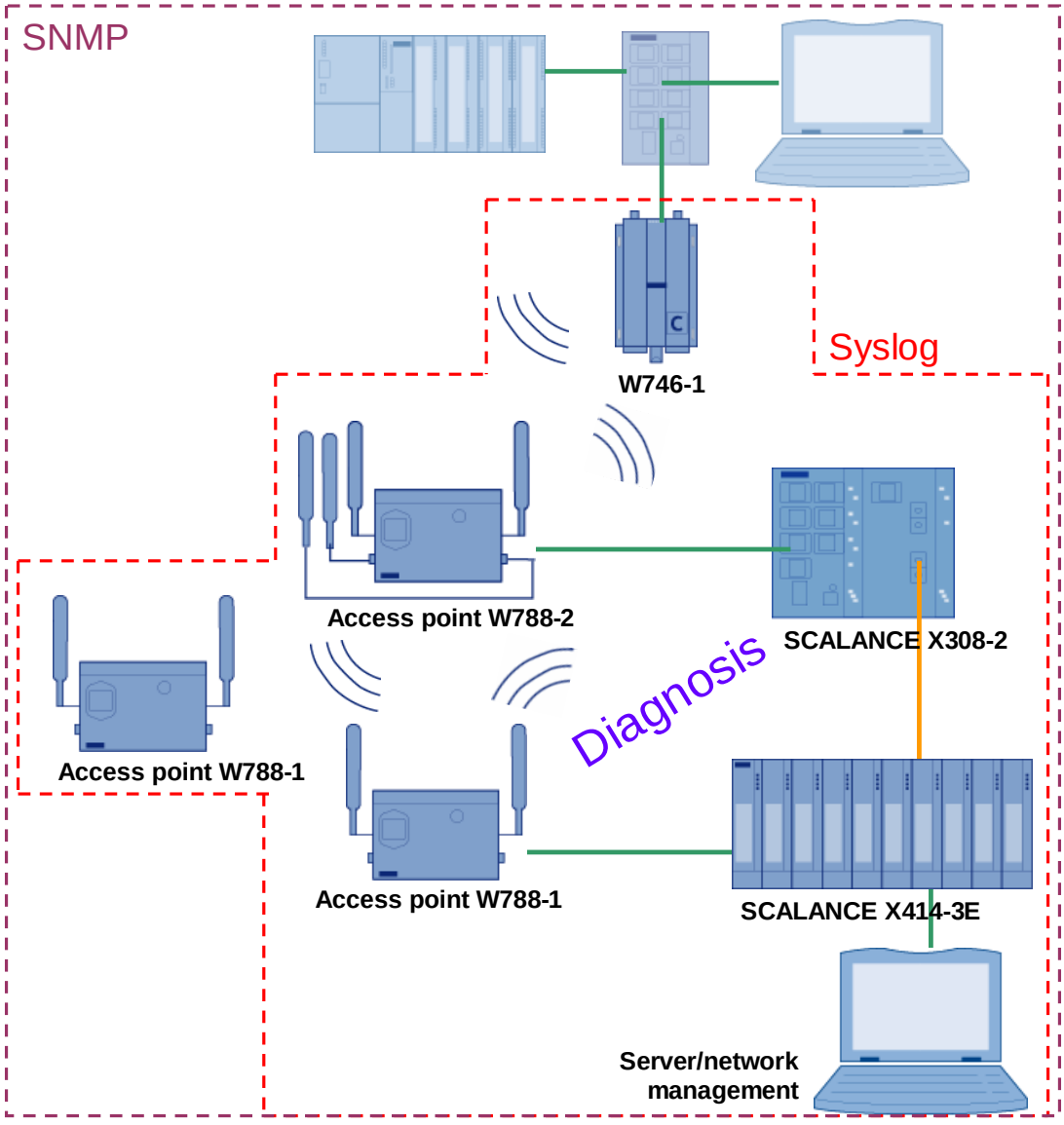


Safety aspects are very important in the use of radio technology. This is why the access control between an access point and a client/test PC/PG is demonstrated.

Overview of "diagnostic method"

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

Figure 2-6



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: • **Access rights for IP addresses** • **RADIUS** (IEEE Standard 802.1X)
Diagnostic method	The following methods are applied for the diagnosis of the network: • **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)	• All SCALANCE W • All SCALANCE X
2.	Infrastructure in IWLAN	• All W788-x access points
3.	Access control (Access Control, RADIUS) (IEEE Standard 802.1X)	• W746-1 client • W788-2 access point
4.	Diagnostic method (SNMP/Syslog) (RFC 3164/ 2821)	• 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

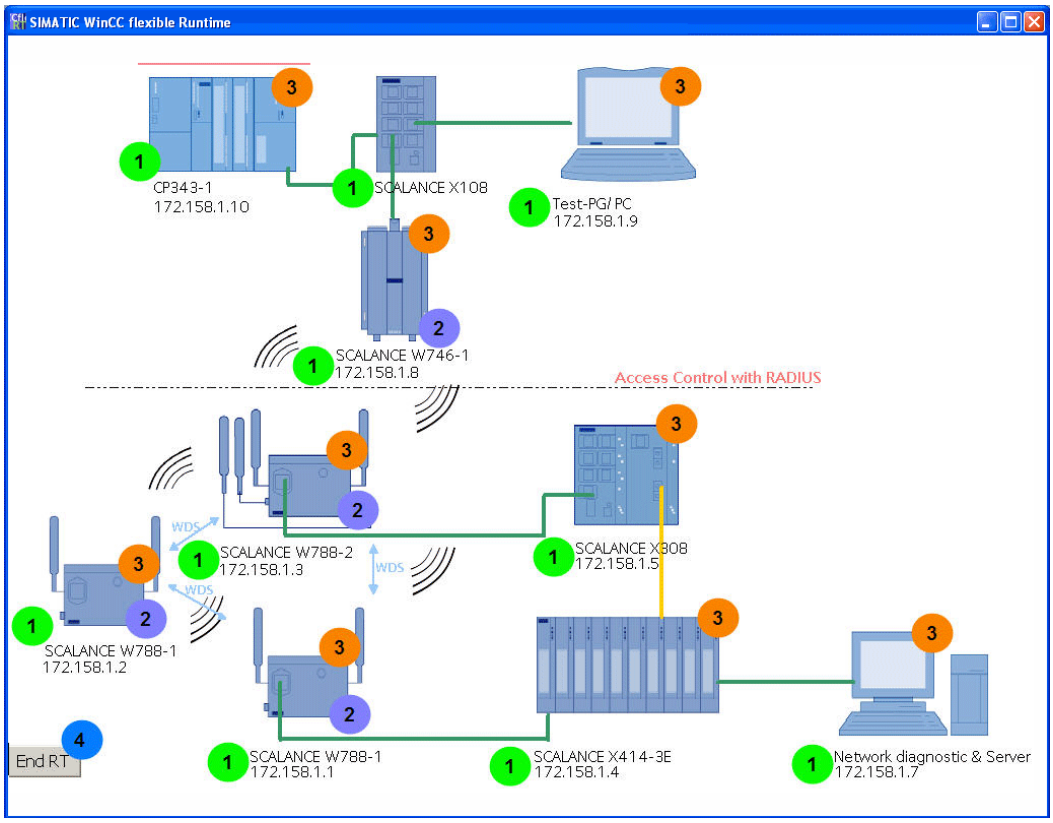


Table 2-3

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

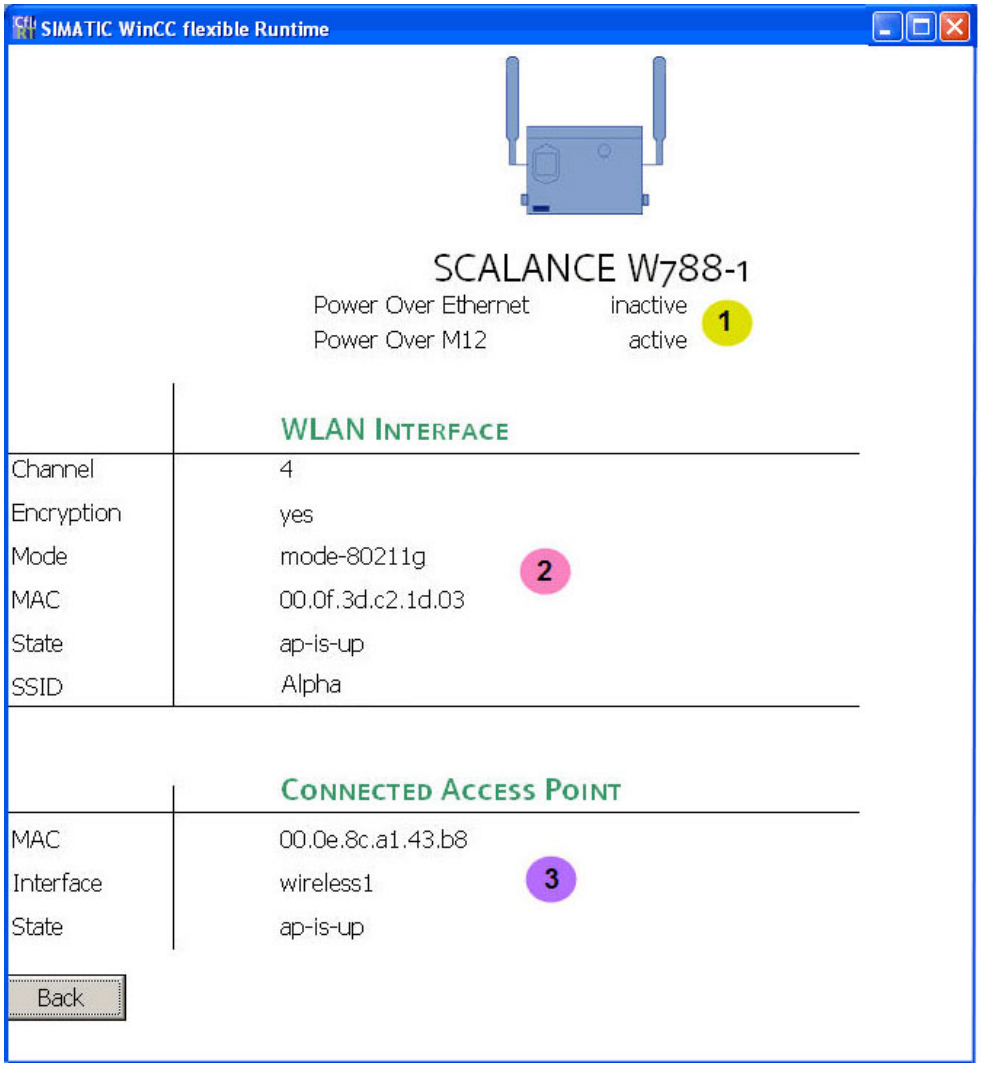


Table 2-4

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

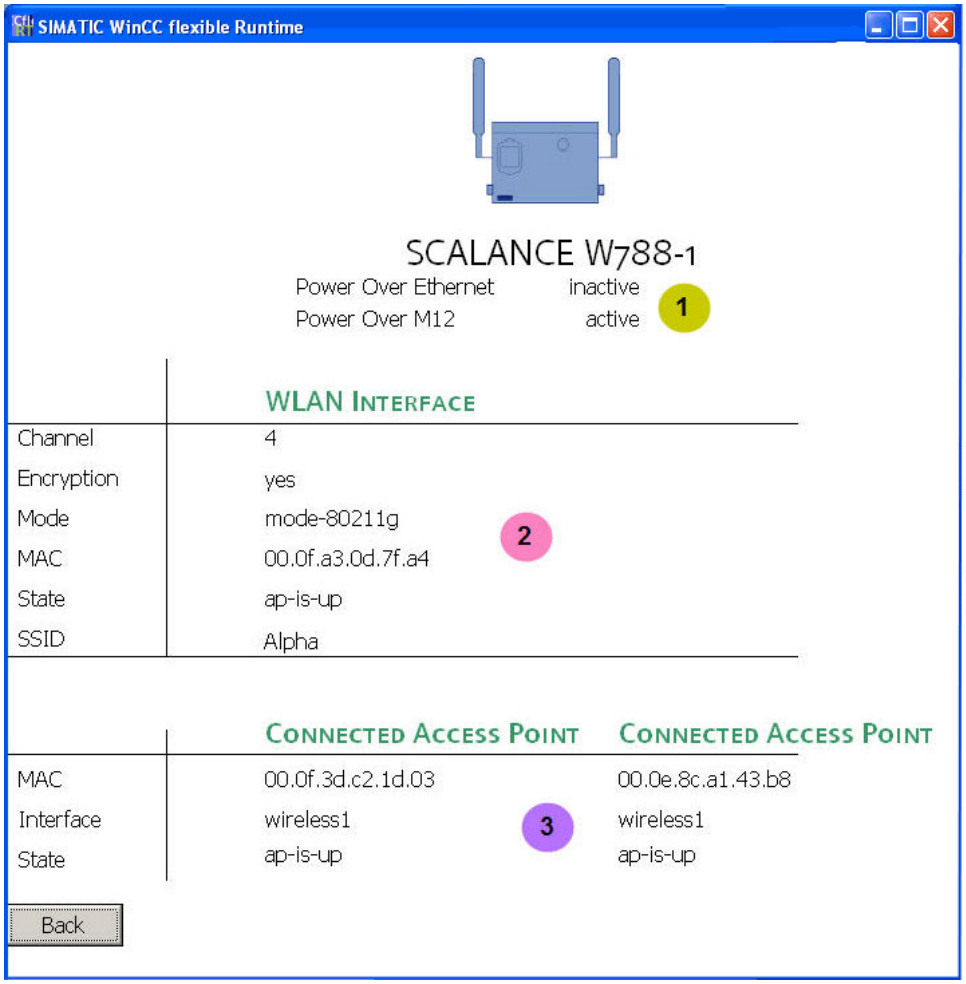


Table 2-5

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

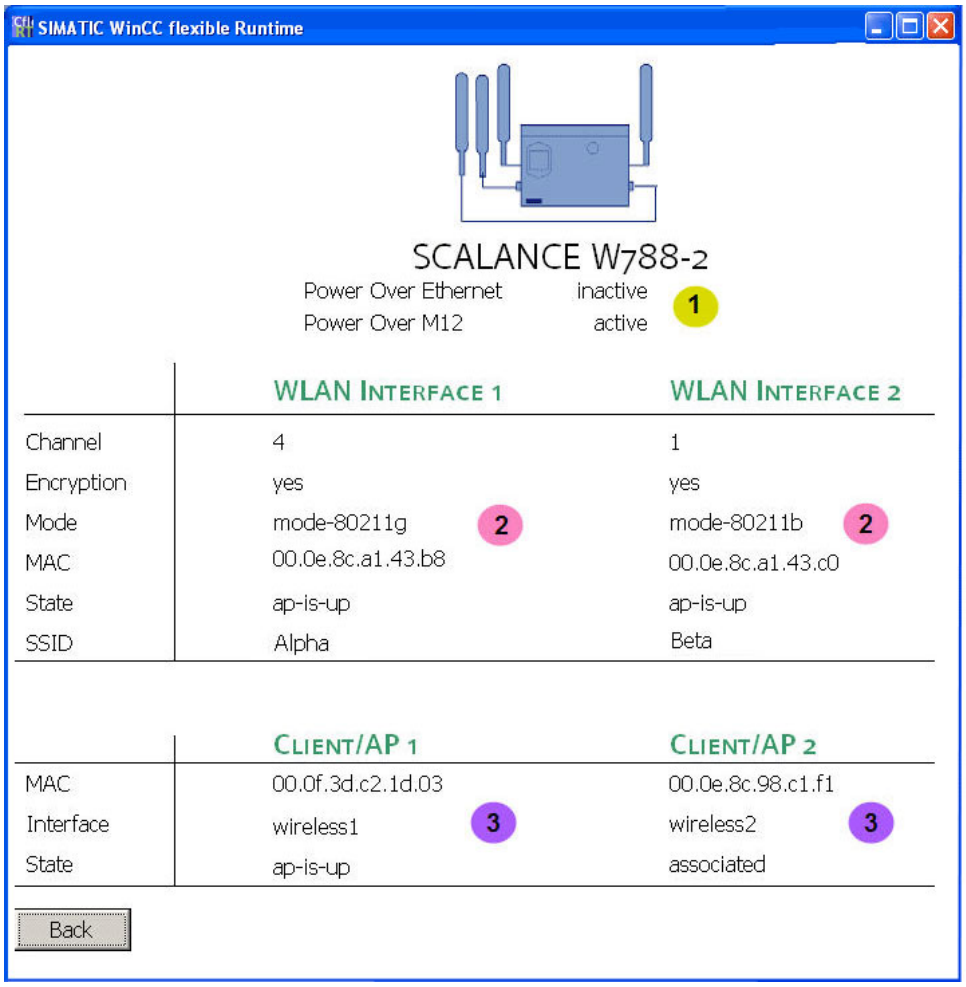


Table 2-6

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

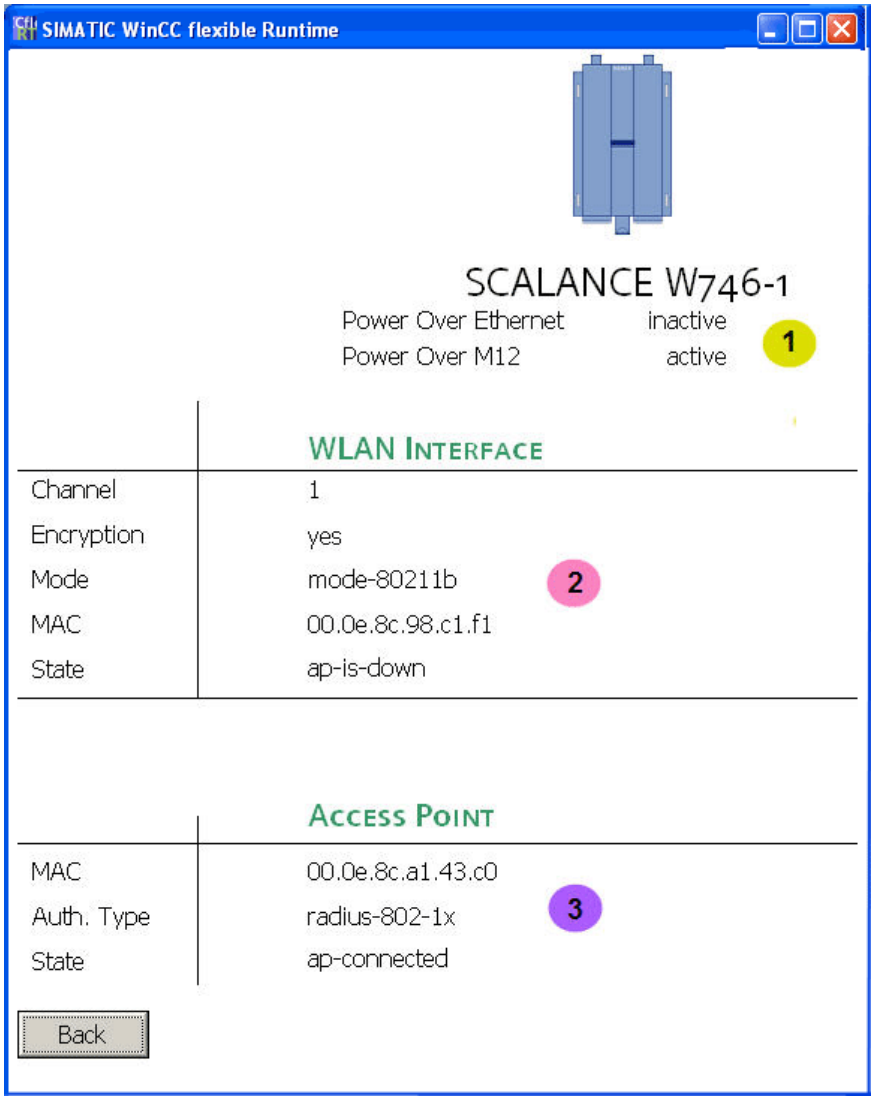


Table 2-7

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.

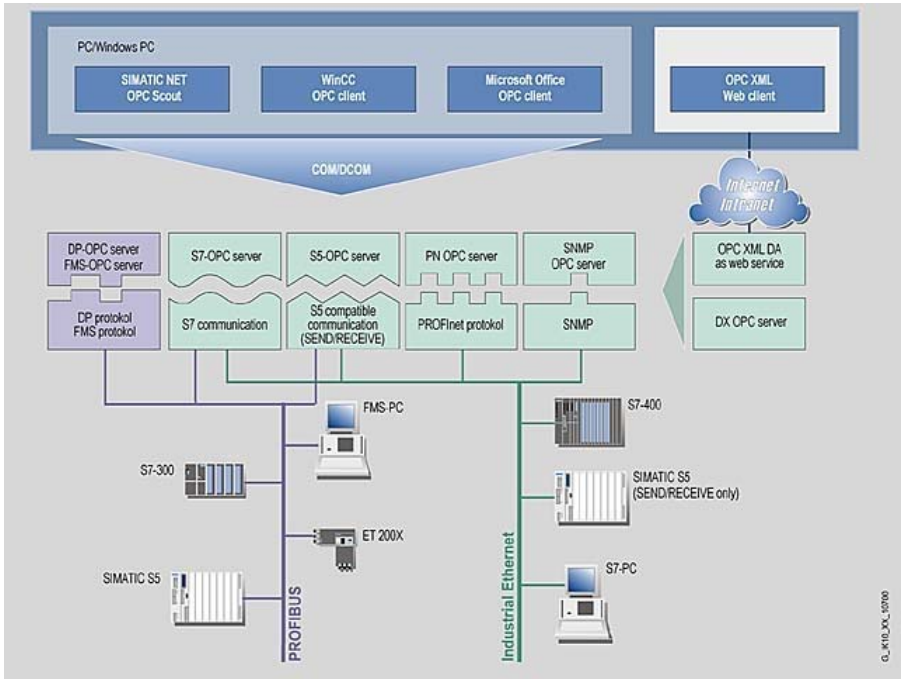
3 General principles of operation

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

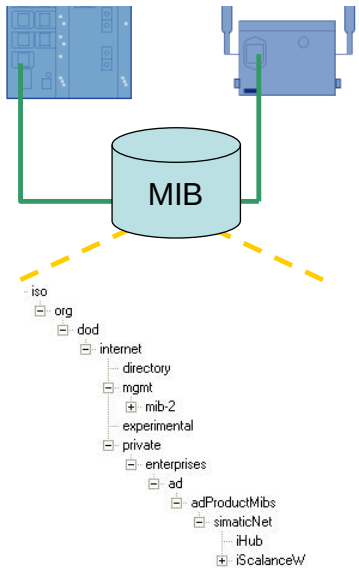
A MIB (Management Information Base) is a standardized data structure consisting of different SNMP variables, which are described by a language independent of the target system.

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

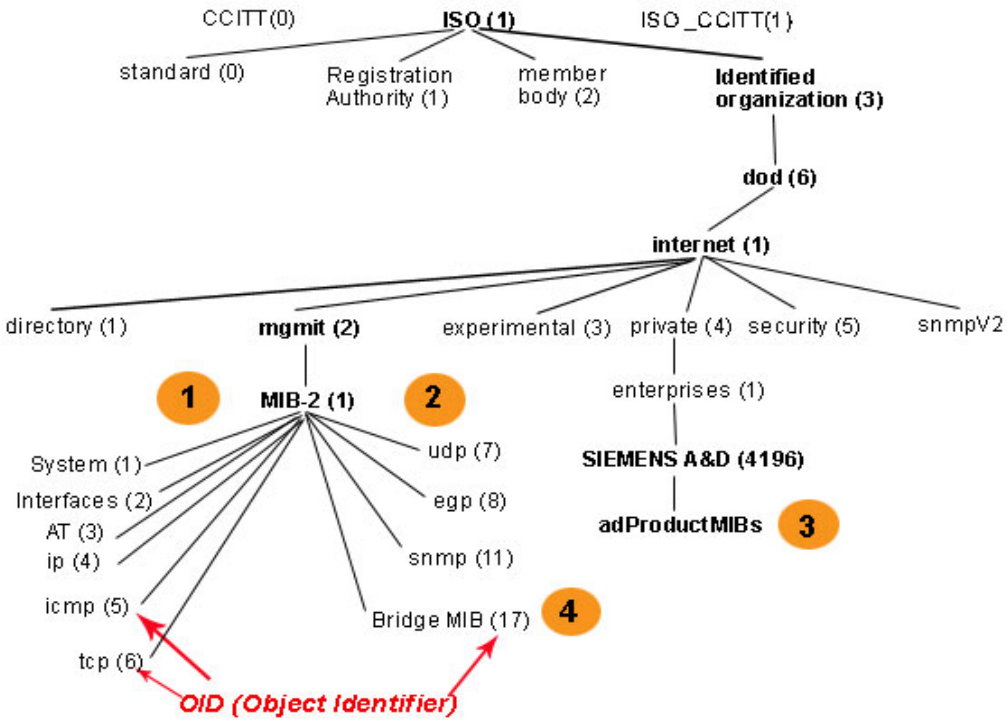
4 Bridge MIB

• 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

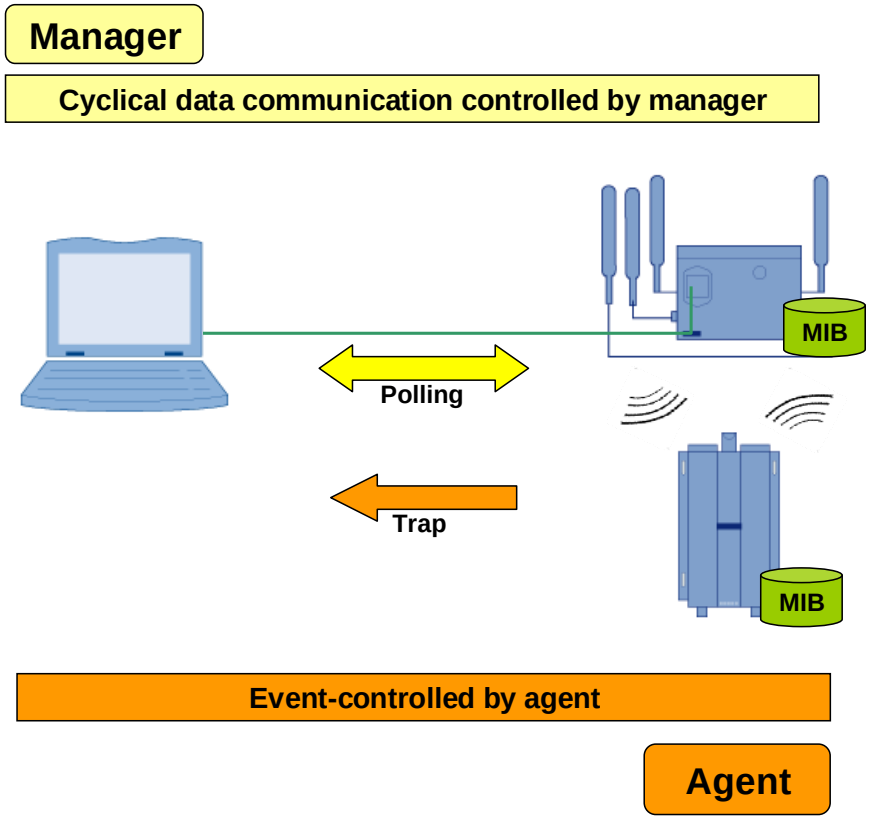


The OID (Object Identifier) describes the address of the MIB object. The address of standardized MIB objects is set by default. Private MIB objects are always stored in the "Enterprise" directory. The manufacturer is responsible for the addresses in this structure. The only requirement is to register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

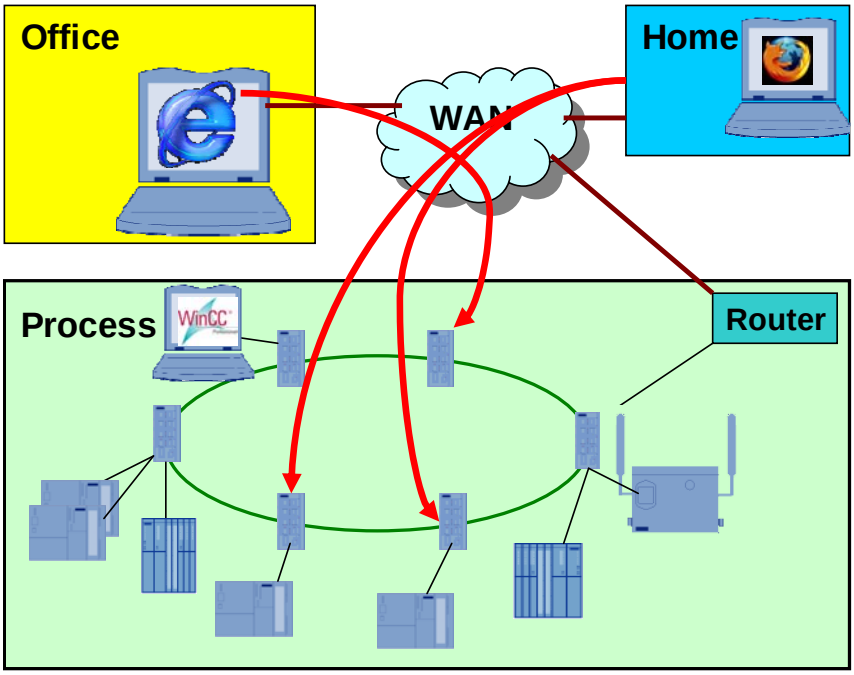
Note The prepared device profiles are located in the following directory:

<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.

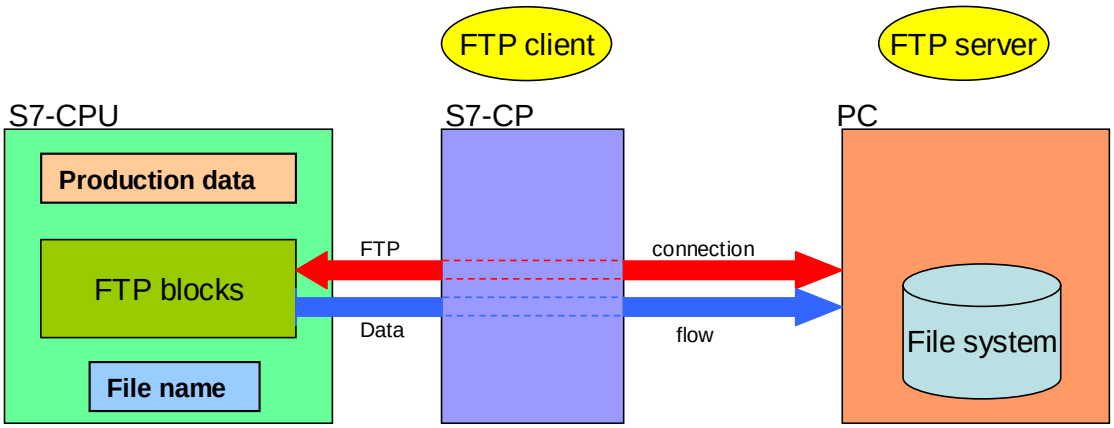
Figure 3-6

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

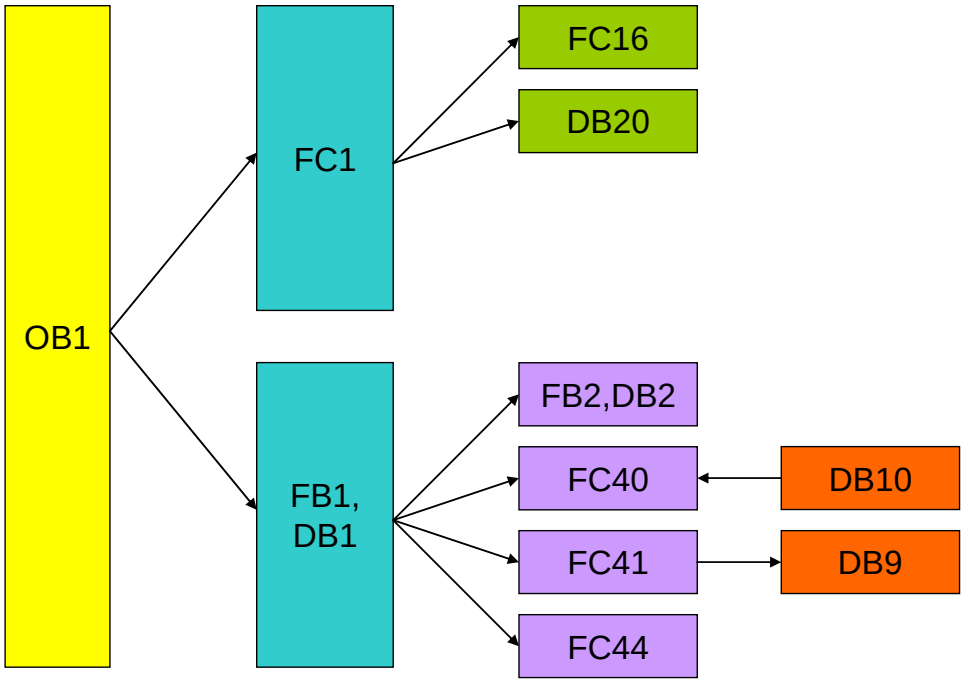


Table 3-2

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.

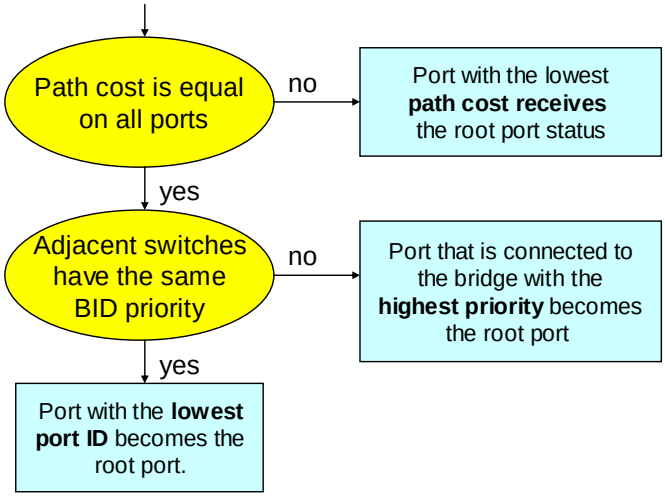
Process sequence

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

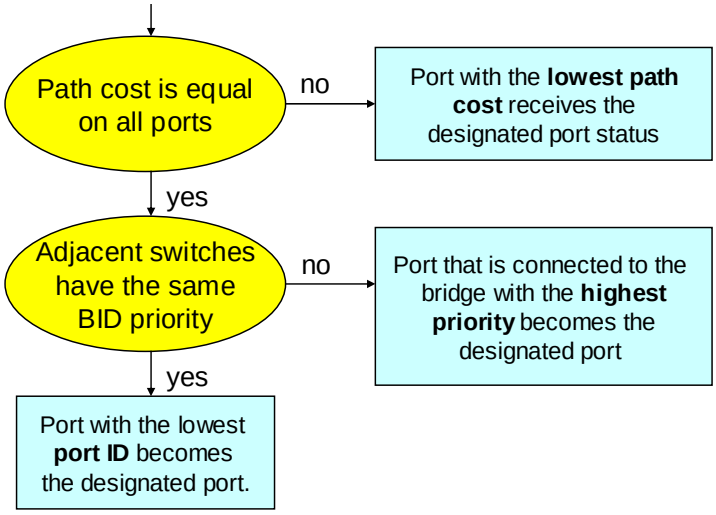
The path cost is the reciprocal value of the bandwidth of a switch port: 1000/line capacitance in Mbps.

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.

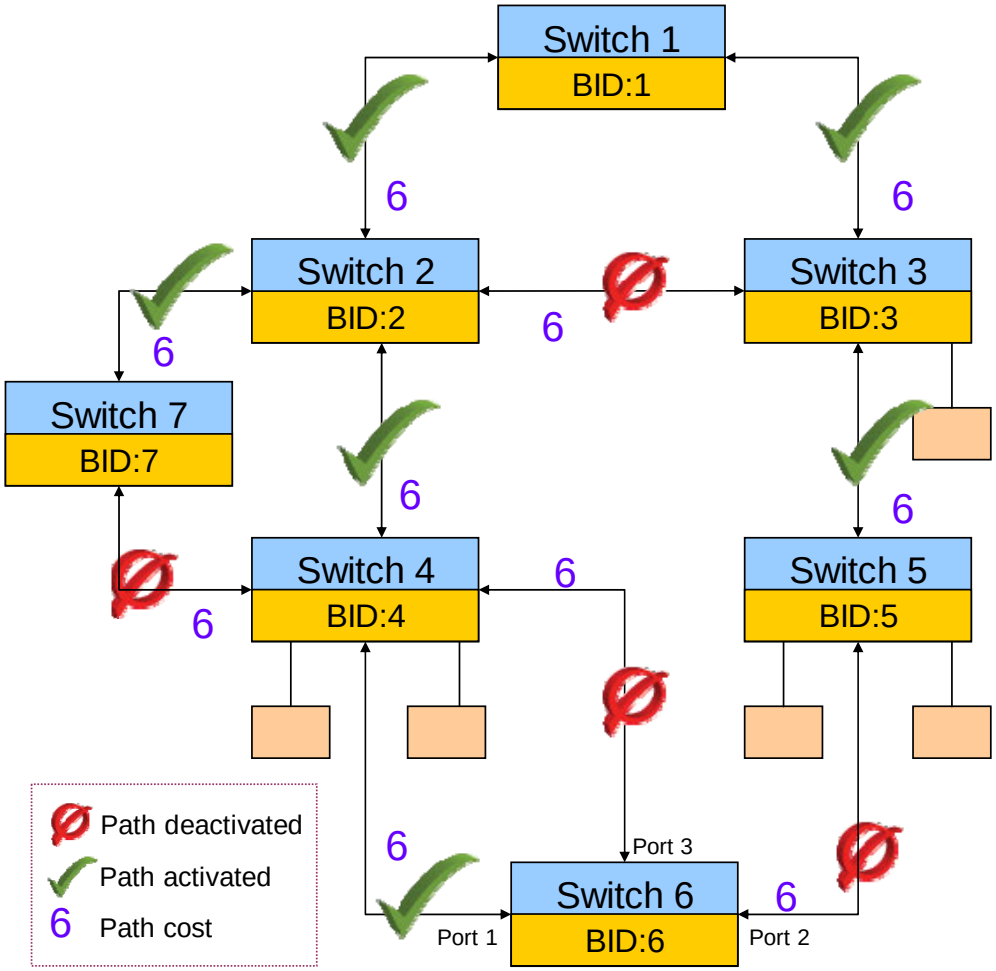
Rapid spanning tree

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



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

Table 3-3

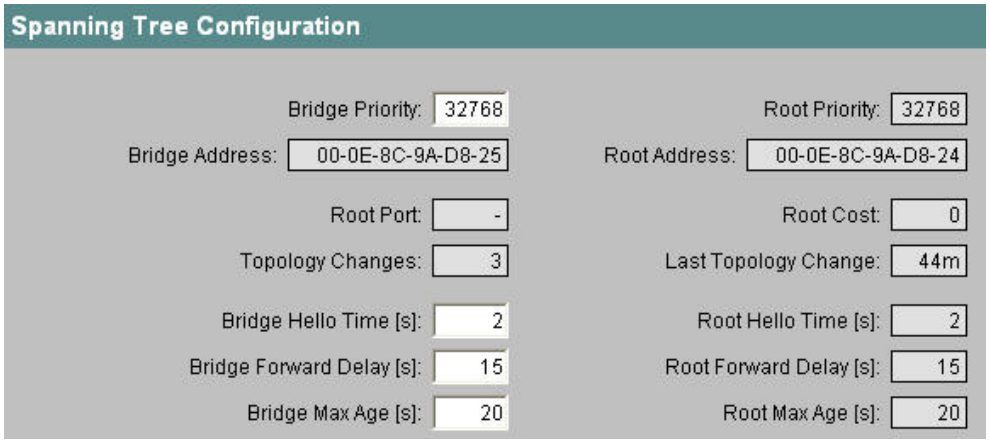
Step	Action	Note
1.	Switch 1 is declared the root bridge.	Switch 1 has the lowest bridge ID.
2.	The path between switch 2 and switch 3 is deactivated.	The path cost between switch 2 (or 3) and switch 1 using this path is higher. The path cost between switch 2 (or 3) and switch 1 is 6. The path cost between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

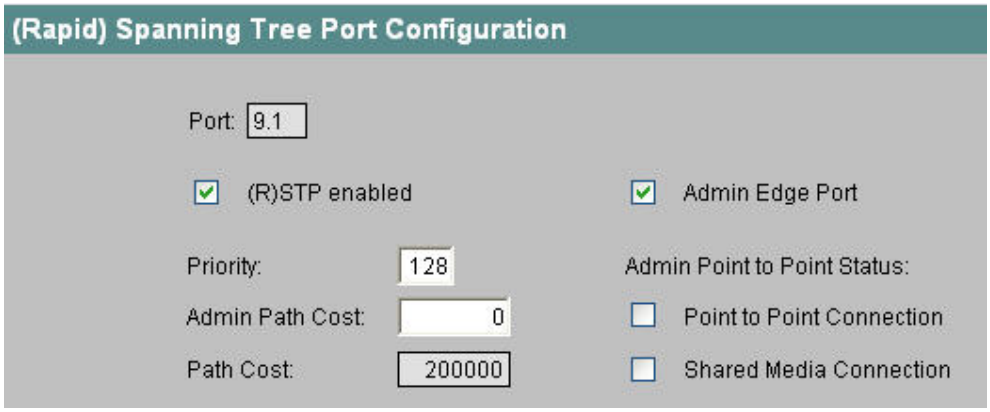


Table 3-5

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: • 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: • 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).

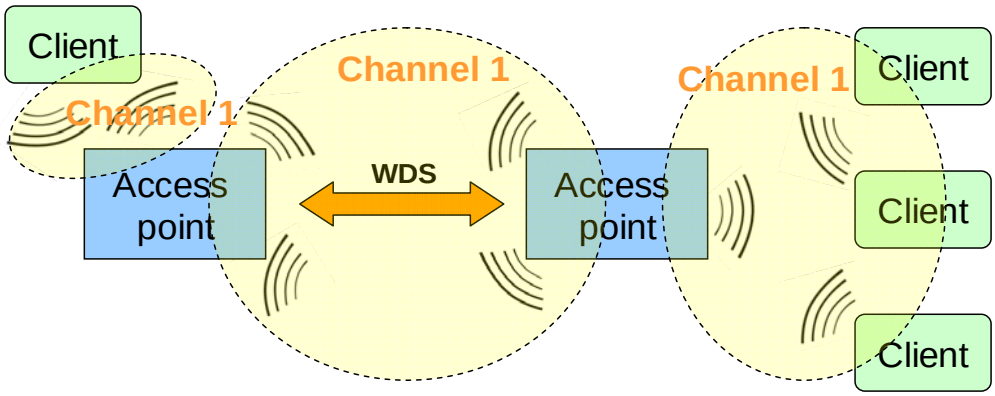
Wireless Distribution System (WDS)

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

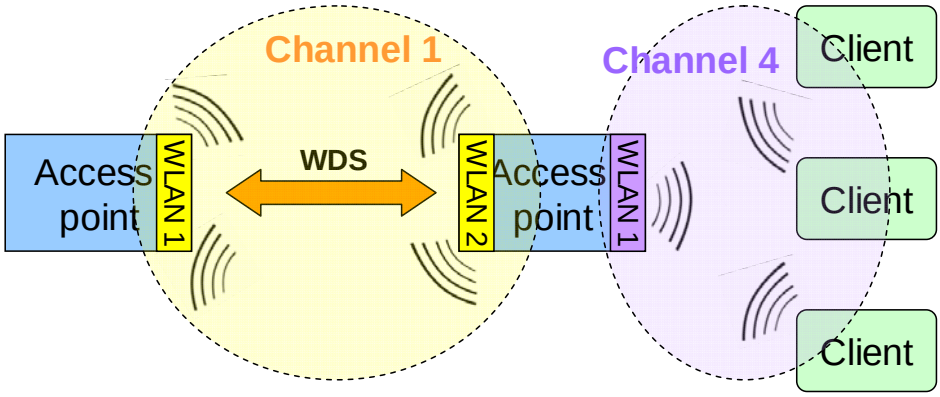


Restrictions

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

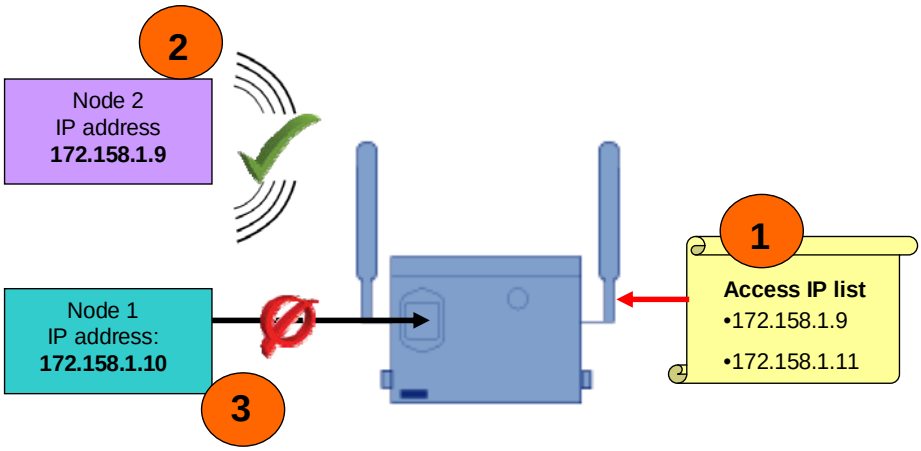


Table 3-7

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

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

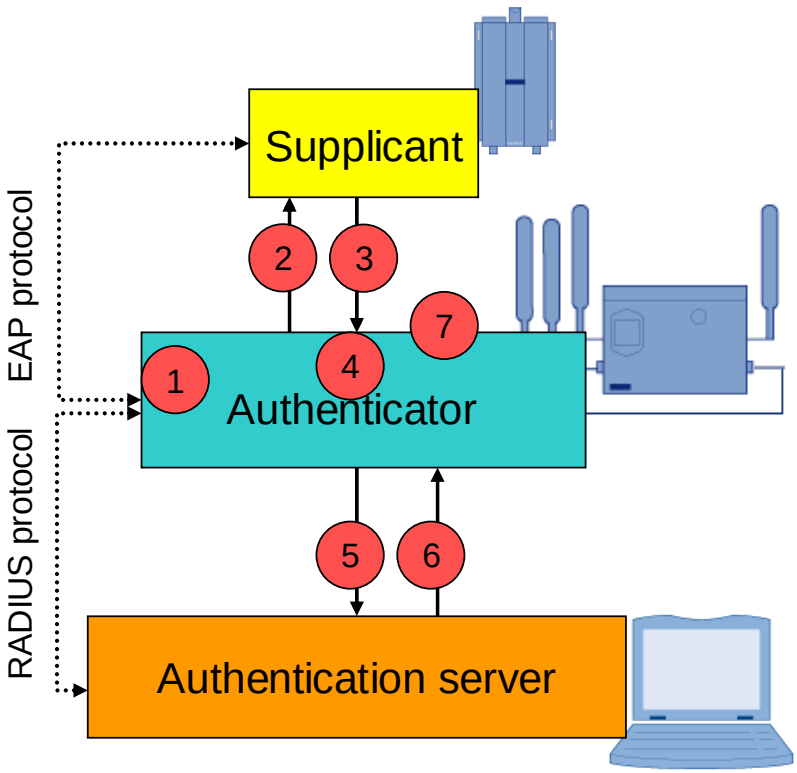


Table 3-9

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

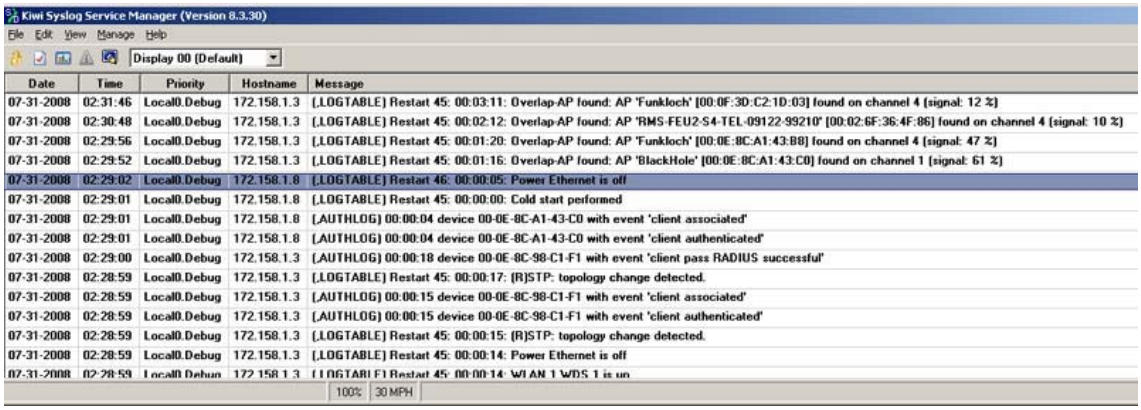
If a configured event occurs, the SCALANCE components automatically generate a Syslog message and send it to the Syslog server.

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



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).

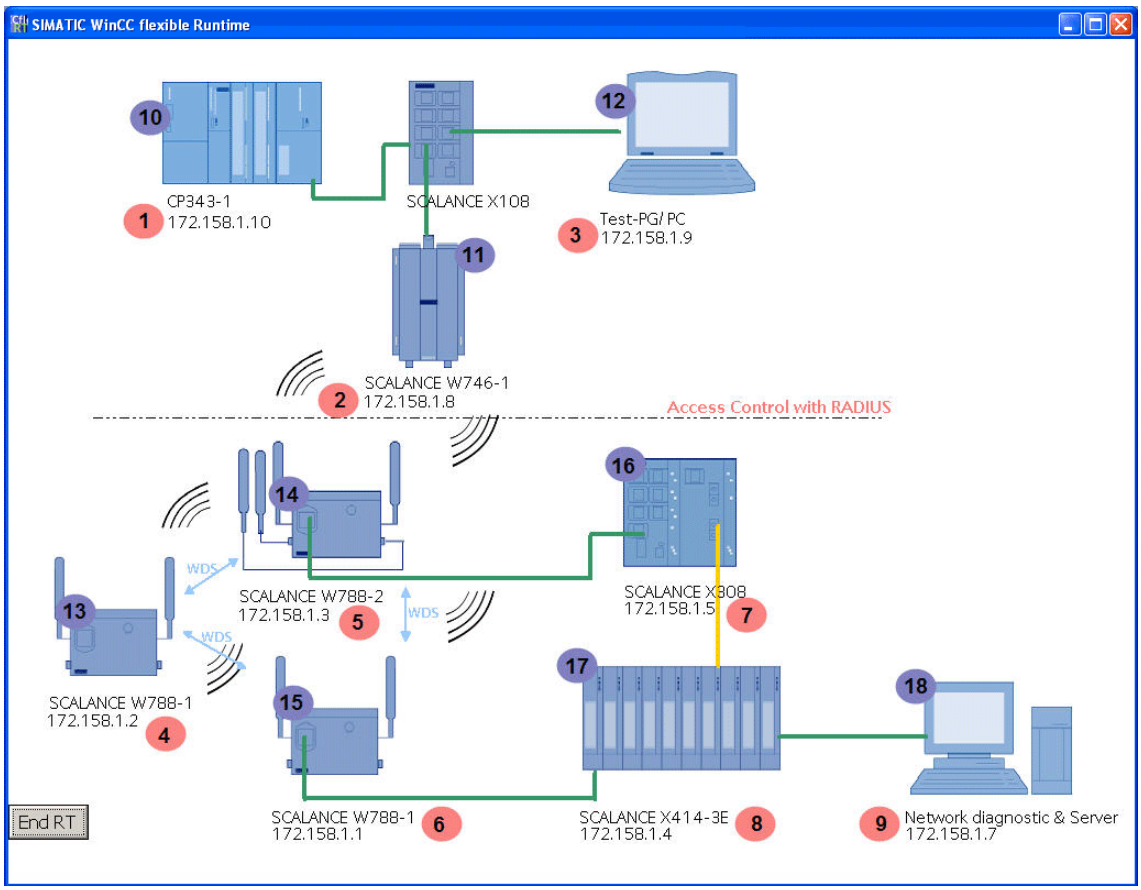
OPC variable

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



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:

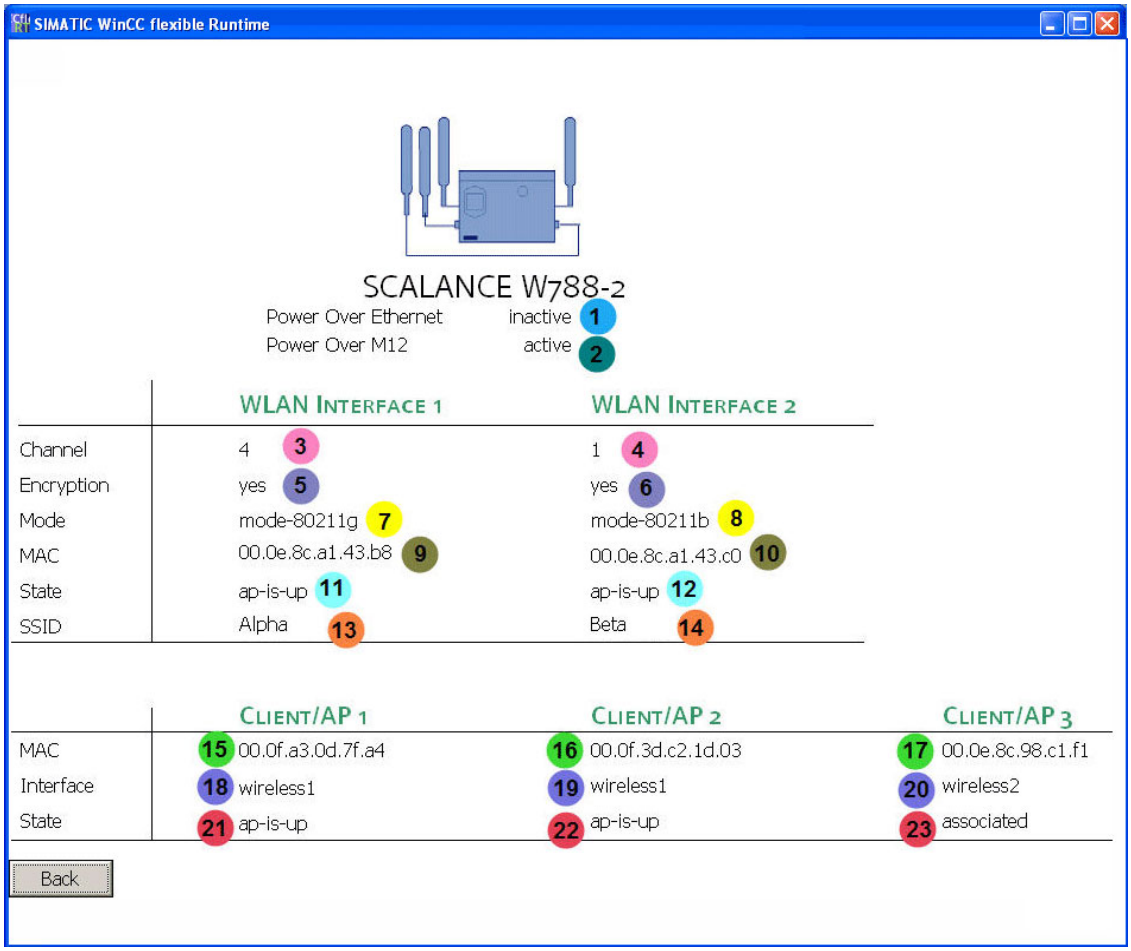
Table 3-11

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



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

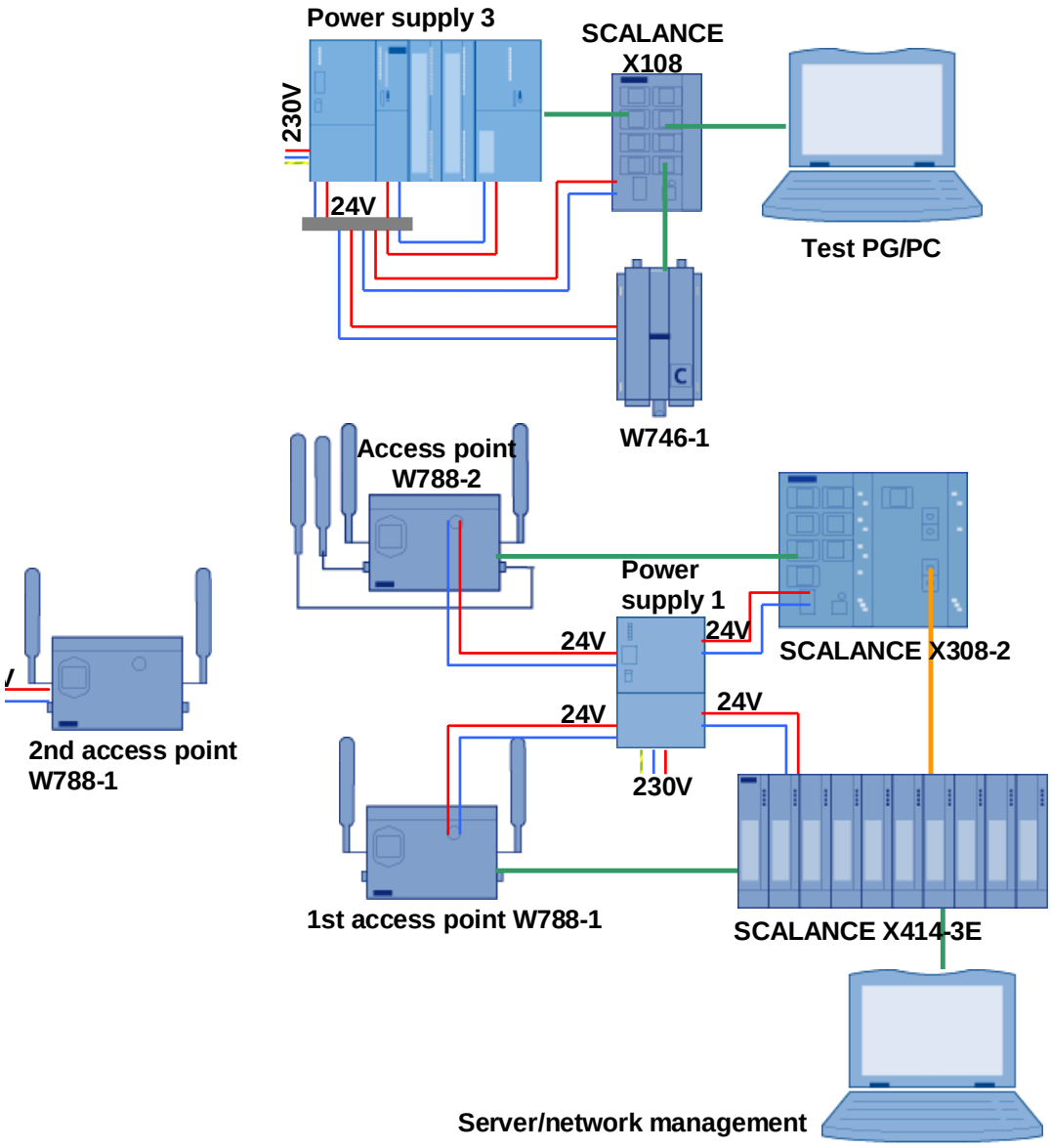
Table 4-2

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.

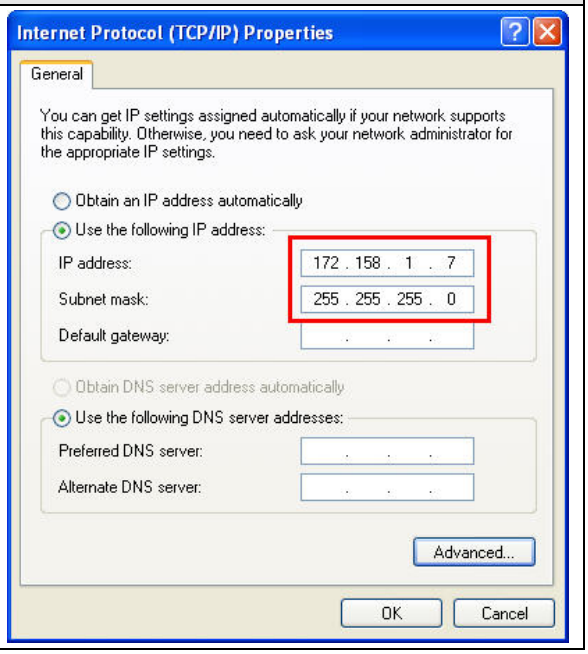
Table 4-7

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:

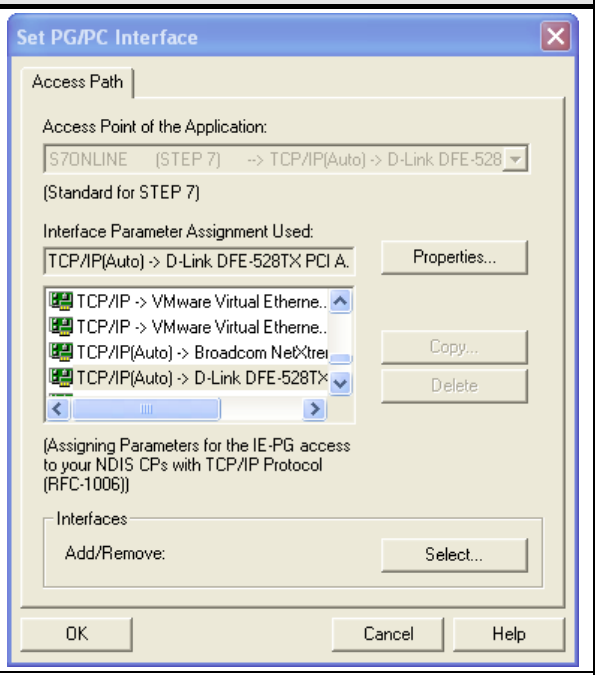
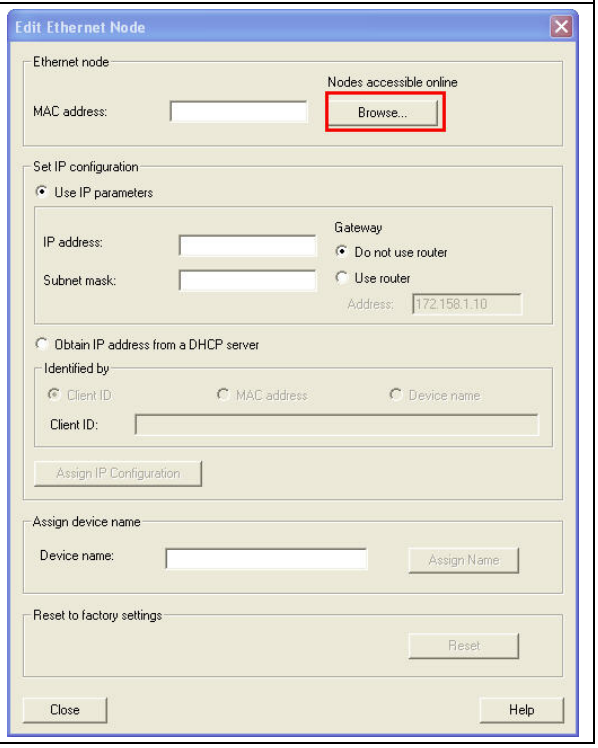
Table 4-8

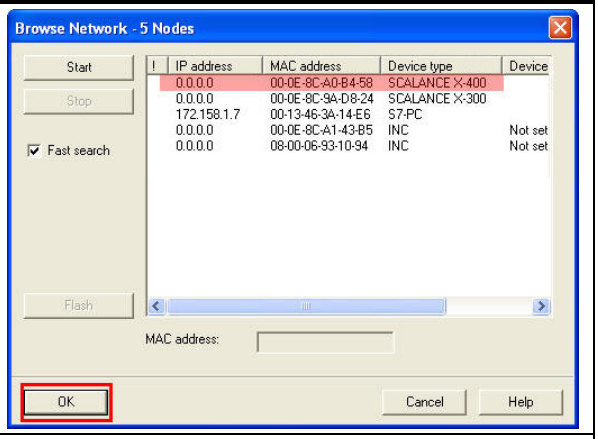
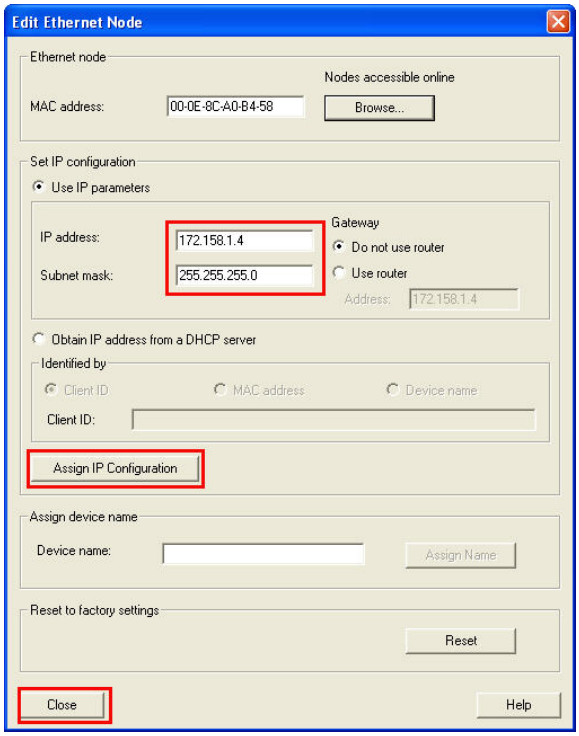
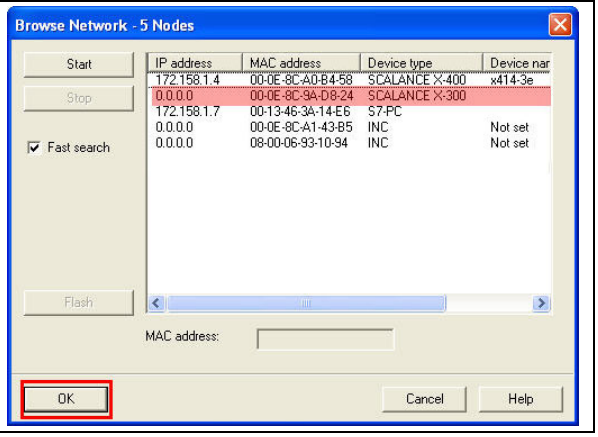
No.	Action	Comment
1.	Open the **Internet Protocol (TCP/IP) Properties** via **`Start -> Settings -> Network Connection ->Local Connections.`** Select the option field **Use following IP address** and fill in the field as shown in the figure. Close the dialog boxes with "OK".	

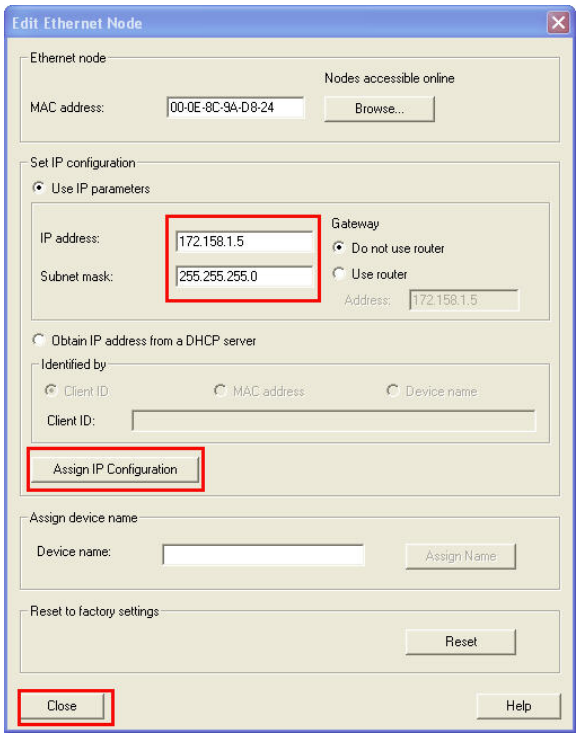
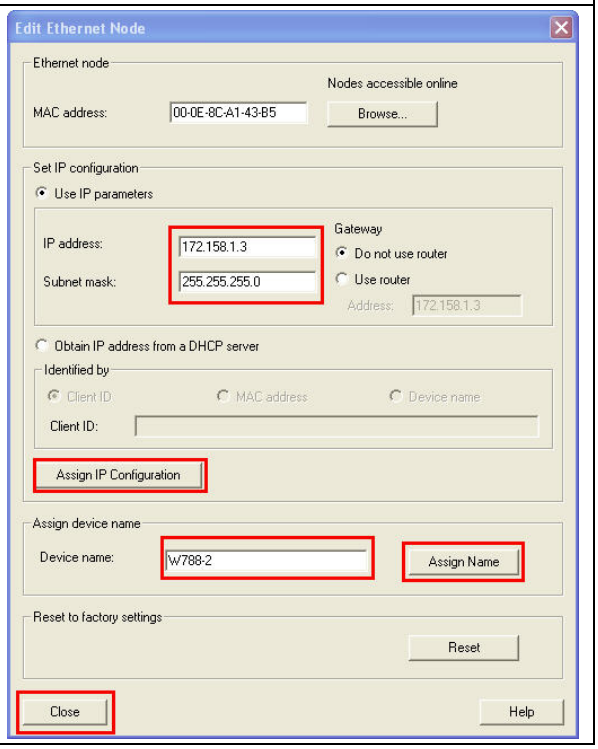
IP address of the SCALANCE X modules and access points

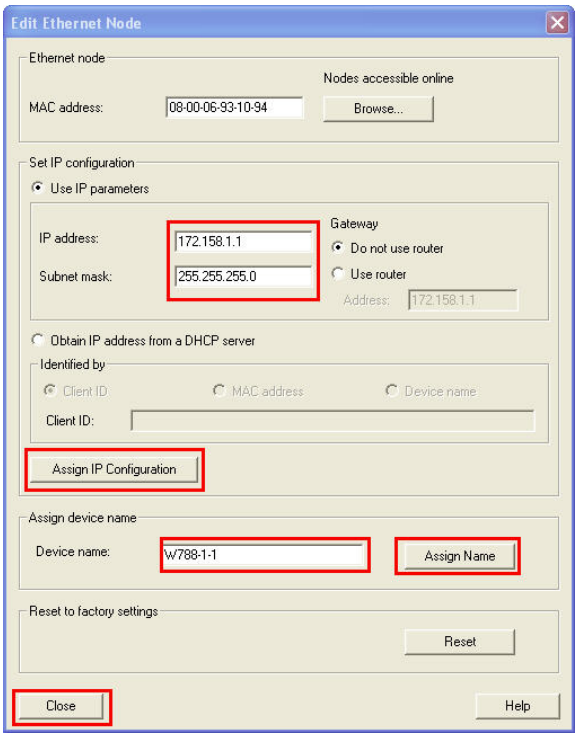
The network configuration of the SCALANCE modules can be performed using the SIMATIC MANAGER.

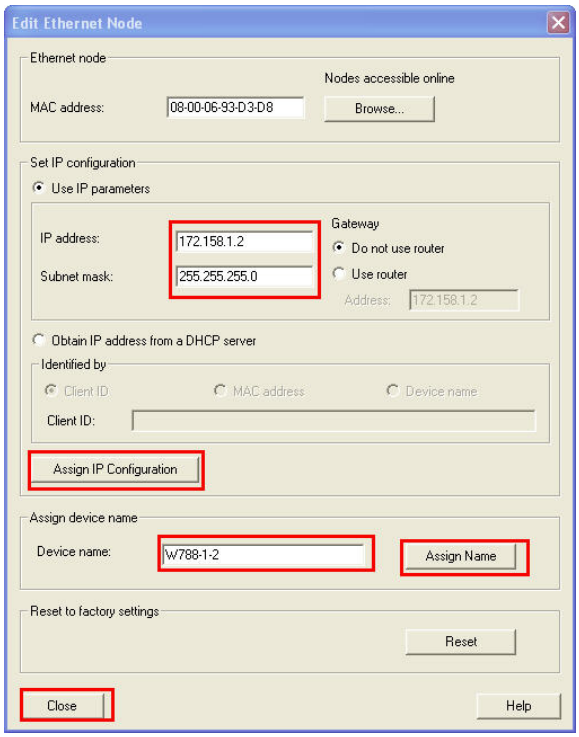
Table 4-9

No.	Action	Comment
1.	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.	
2.	Select the menu item **`PLC -> Edit Ethernet Node`** in the **SIMATIC MANAGER**. Click the **Browse…** button to start the search for further nodes.	

No.	Action	Comment
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 **SCALANCE X400** and click **OK**.	
4.	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.	
5.	Repeat step 2. 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**.	

No.	Action	Comment
6.	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.	
7.	Perform steps 2 to 3 for the **SCALANCE W788-2**. 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. 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. Assign a device name to the SCALANCE as shown in Table 4-7 and load it to the device using the **Assign Name** button. Click **Close** to close the dialog box.	

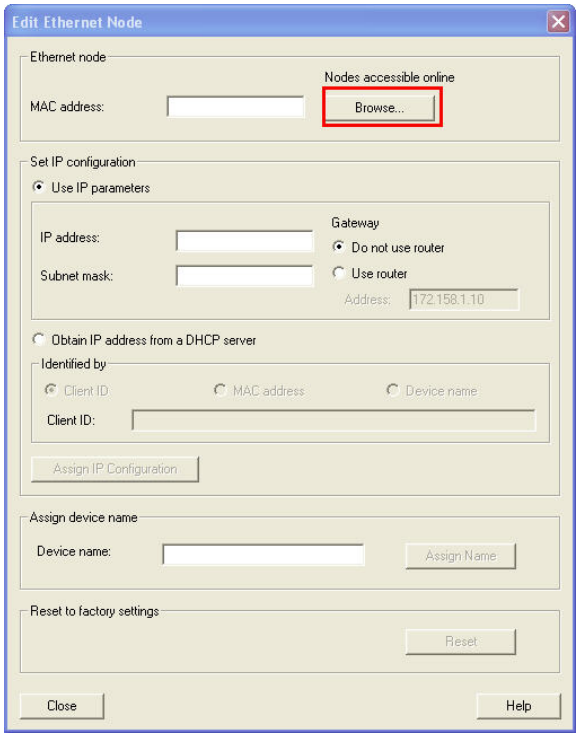
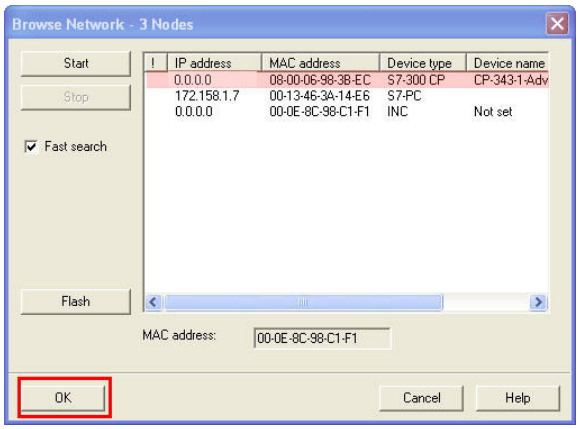
No.	Action	Comment
8.	Perform steps 2 to 3 for the **first SCALANCE W788-1**. The SCALANCE W modules with the device name **INC** are displayed under item 3. Compare the MAC address displayed to that printed on the SCALANCE module housing in order to distinguish between the components. Enter the IP address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

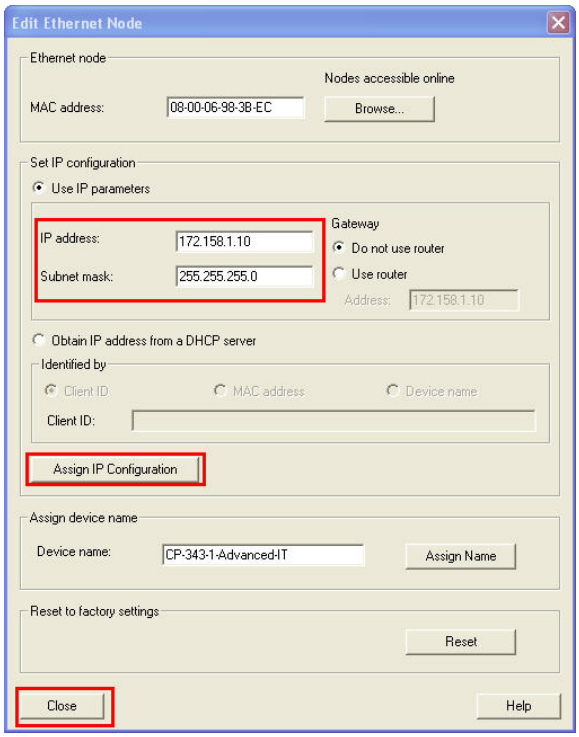
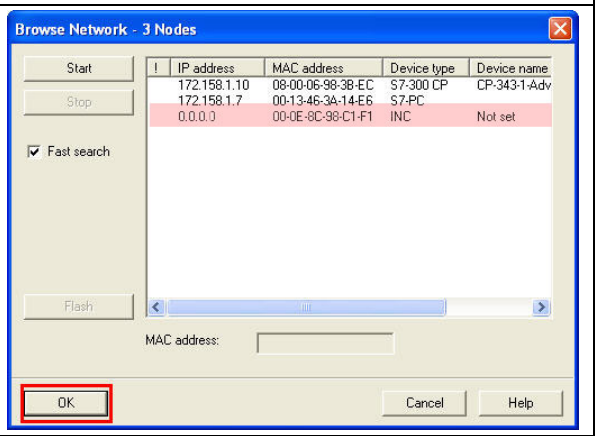
No.	Action	Comment
10.	Perform steps 2 to 3 for the **second SCALANCE W788-1**. The SCALANCE W modules with the device name **INC** are displayed under item 3. Compare the MAC address displayed to that printed on the SCALANCE module housing in order to distinguish between the components. Enter the IP 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. Assign a device name to the SCALANCE as shown in Table 4-7 and load it to the device using the **Assign Name** button. Close the dialog box with **Close**. Once the IP address has been transferred, reconnect the server PC to the SCALANCE X414-3E.	

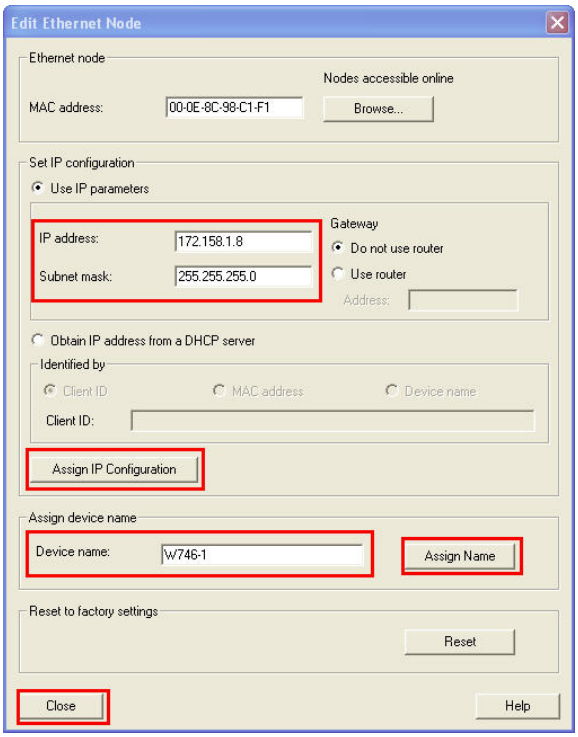
IP address of the W746-1 and CP343-1 IT WLAN clients

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**.	

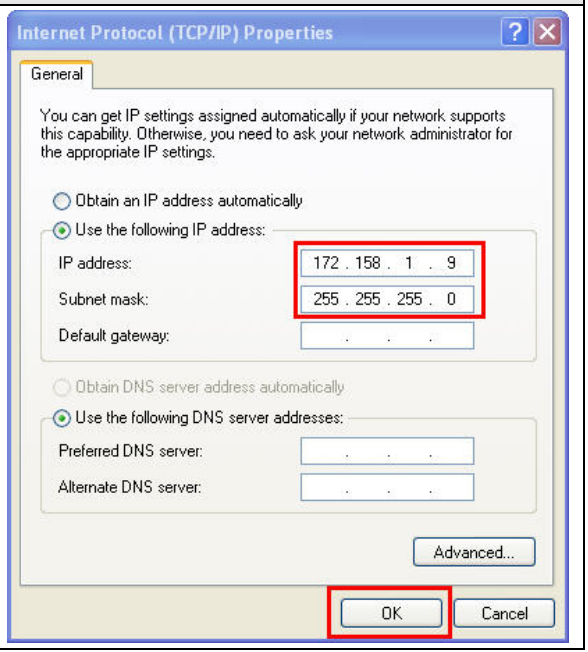
No.	Action	Comment
4.	Enter the IP address as shown in Table 4-7 and the appropriate subnet mask. Click the **Assign IP Configuration** button to assign these settings to the device. Click **Close** to close the dialog box.	
5.	Repeat step 2. The dialog box with the node found in the network opens again. The CP343-1 IT is displayed with the address configured before. Now select the **SCALANCE W746-1** and click **OK**.	

No.	Action	Comment
6.	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**.	
7.	Reconnect the server PC to port 9.3 of the SCALANCE X414-3E.	

IP address of the test PG/PC

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

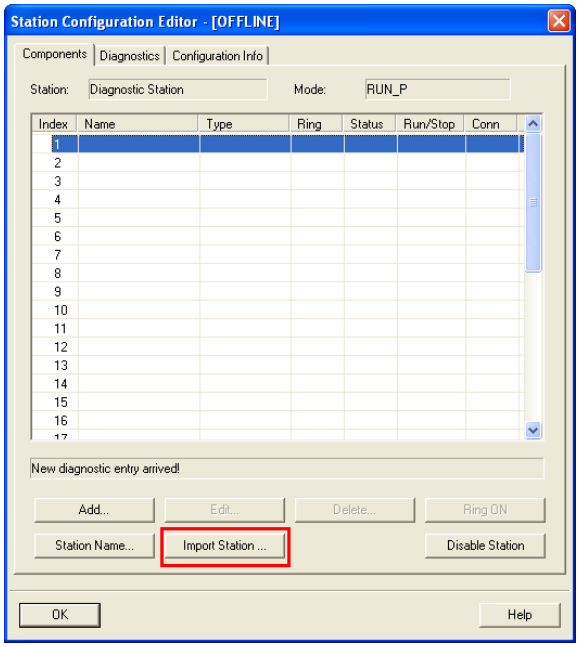
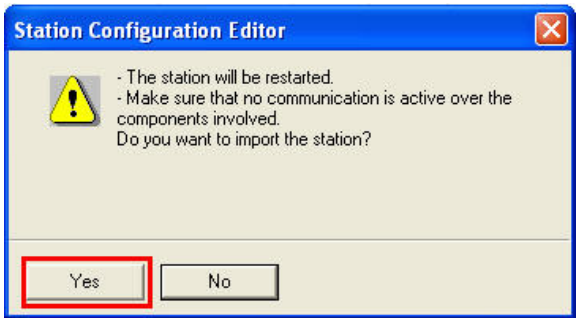
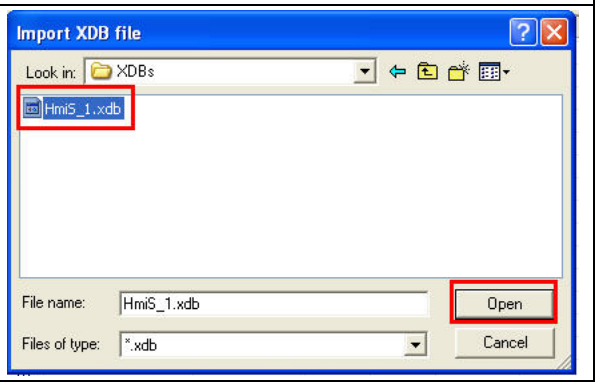
Table 4-11

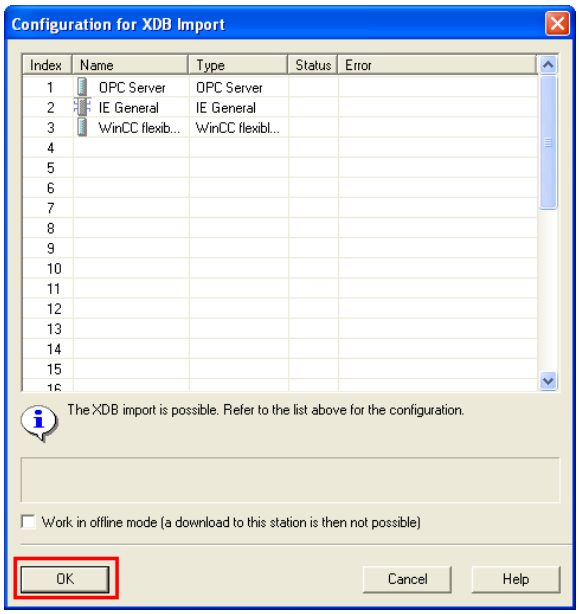
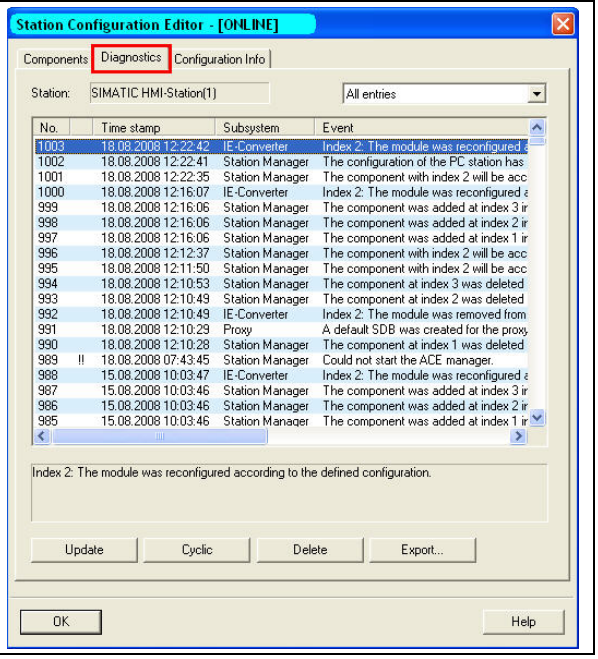
No.	Action	Comment
1.	Open the **Internet Protocol (TCP/IP) Properties** using **`Start -> Settings -> Network Connection ->Local Connections.`** Select the option field **Use following IP address** and fill in the field as shown in the figure. Close the dialog box with **OK**.	

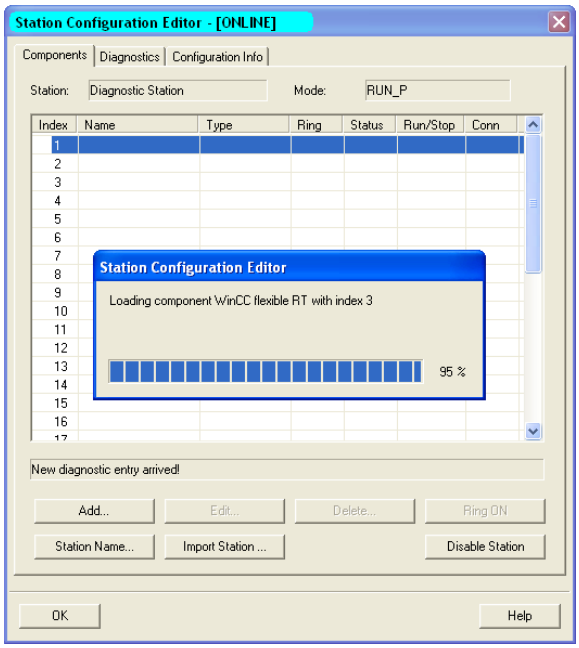
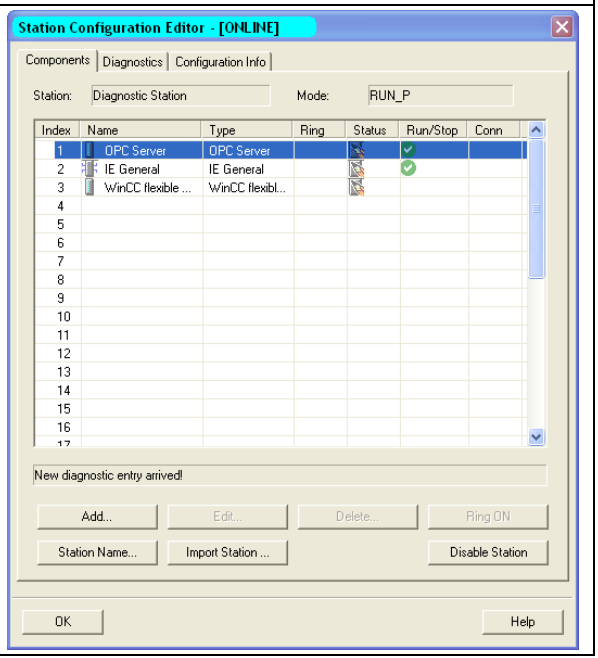
4.2.2 Configuration of the Station Configurator

The Station Configurator is configured on the server PC.

Table 4-12

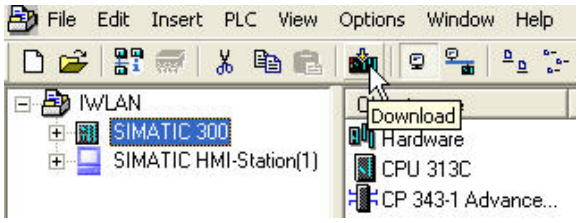
No.	Action	Comment
1.	Open the Station Configurator by selecting **`Start -> Station Configurator`** or by double-clicking the icon in the taskbar. Press the **Import Station...** button.	
2.	Confirm the restart of the node with **Yes**.	
3.	Navigate to the directory of the STEP 7 project and open the **XDBs** folder. Open the **HmiS_1.xdb** file and click **Open** to import the station.	

No.	Action	Comment
4.	The following dialog indicates whether the XDB file can be imported. If no error is displayed, confirm with the **OK** button.	
5.	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.	

No.	Action	Comment
6.	The PC station is configured using the data from the XDB file.	
7.	The configuration of the PC station is now complete. OPC Server and IE-General must be in the "Run" mode without errors. Close the dialog box with **OK**.	

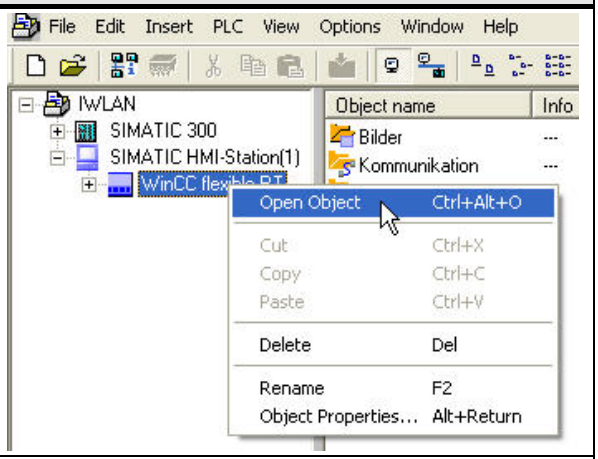
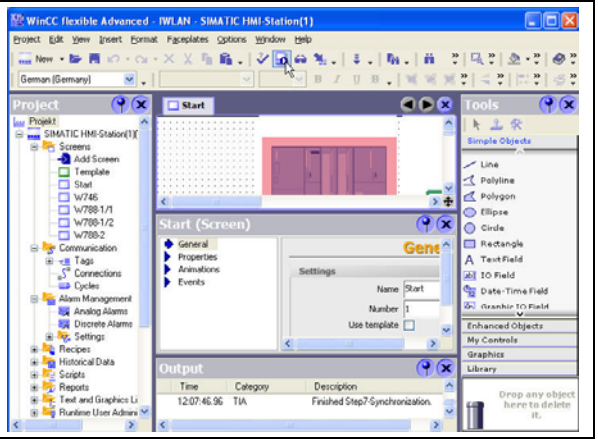
4.2.3 Load STEP 7 project

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.

5 Configuration

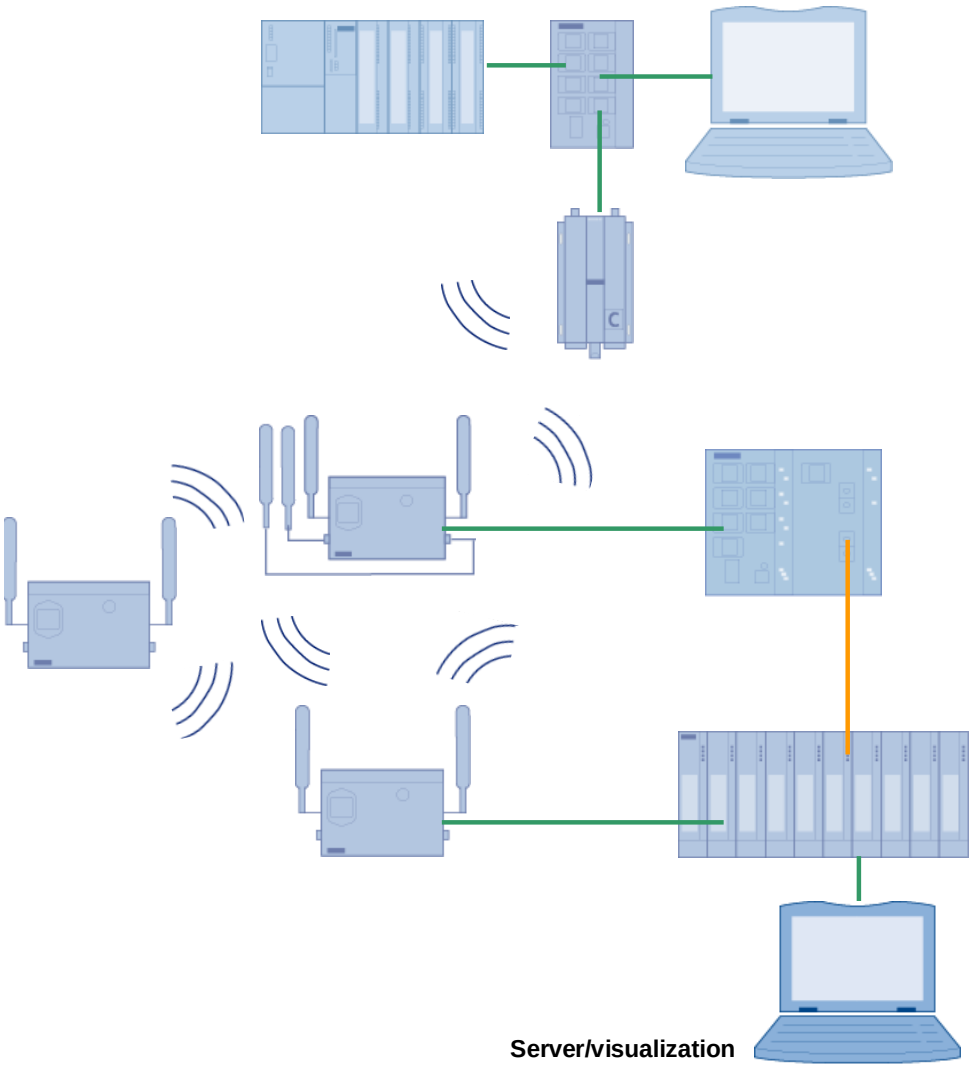
This chapter shows the necessary steps for the configuration of the SCALANCE modules and the software.

5.1 Configuration of the SNMP OPC server

Note The SNMP OPC server has already been configured in the provided code. Section 5.1 only serves for providing information.

The SNMP OPC server is configured on the server PC that is also used for visualization.

Figure 5-1



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.

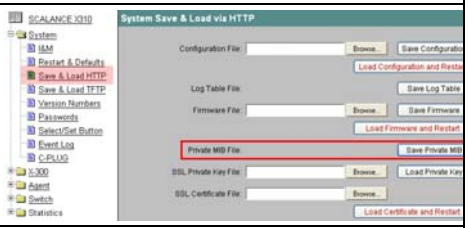
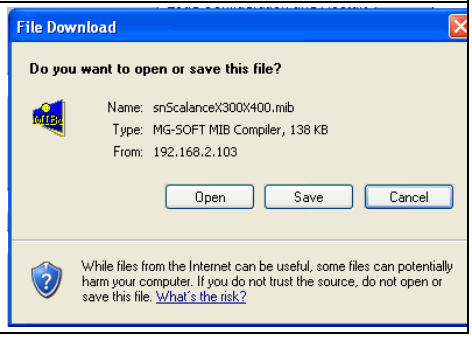
Private MIB of the SCALANCE-X300/-400 and W

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

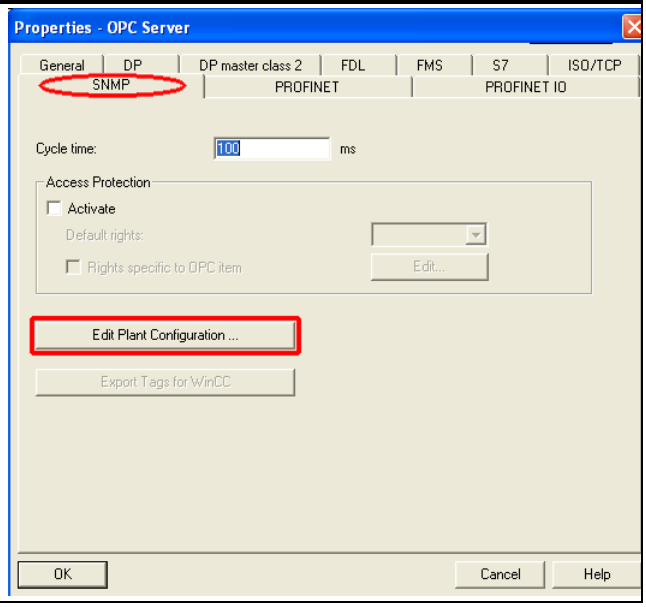
These preparatory steps are only necessary if your SIMATIC NET software is lower than V7.0 SP1.

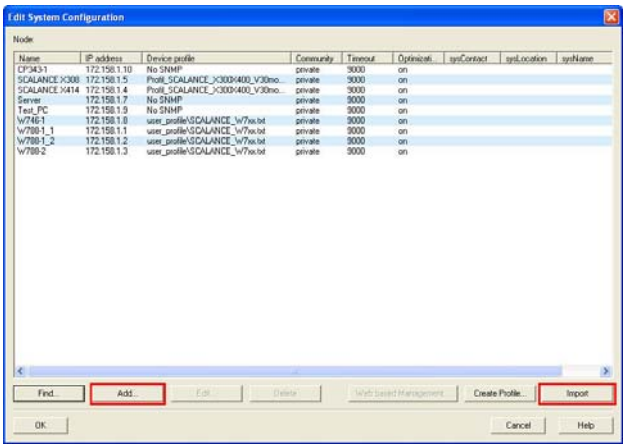
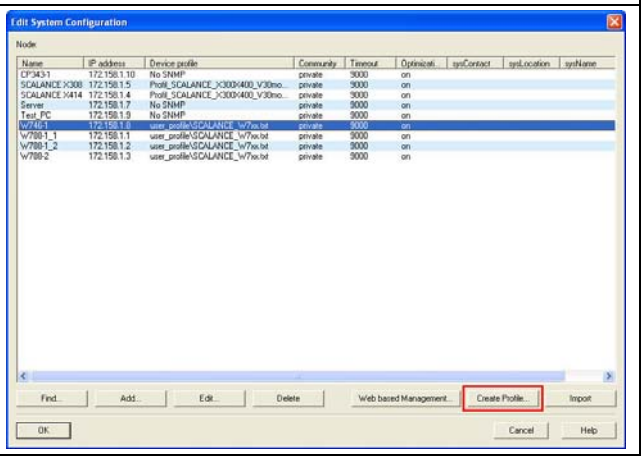
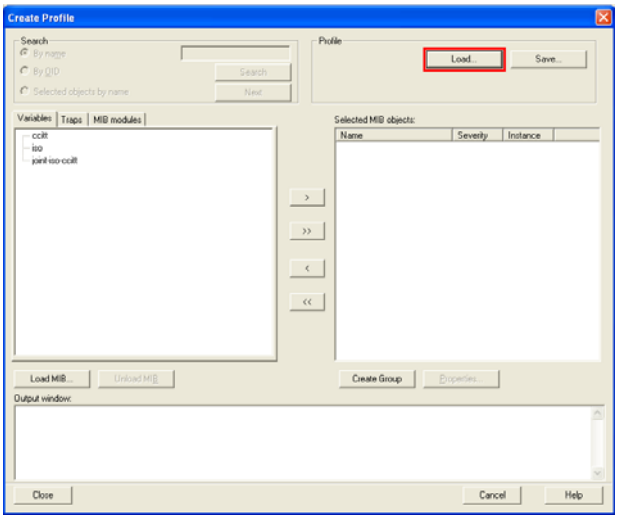
For an overview of SIMATIC software packages and versions installed on your computer, please refer to **`Start->SIMATIC->Information ->Installed Software`**.

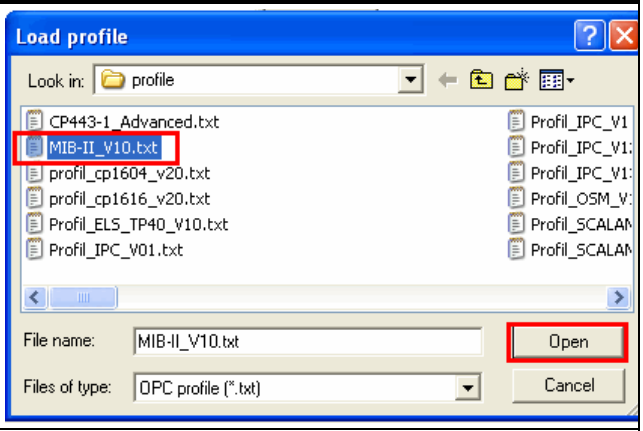
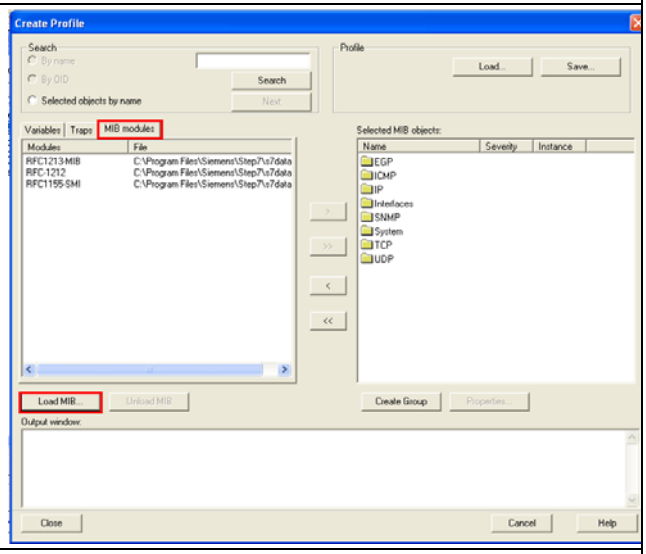
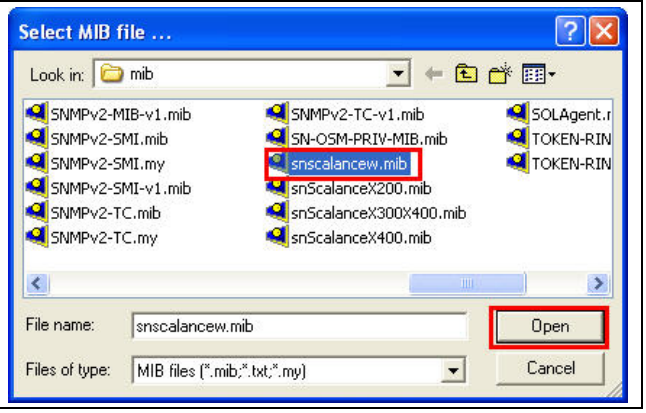
Unzip the folder with the standard MIBs and replace all files located in the MIB folder of STEP 7 **<STEP7InstallationDirectory>\S7DATA\snmp\mib** by these new standard MIBs.

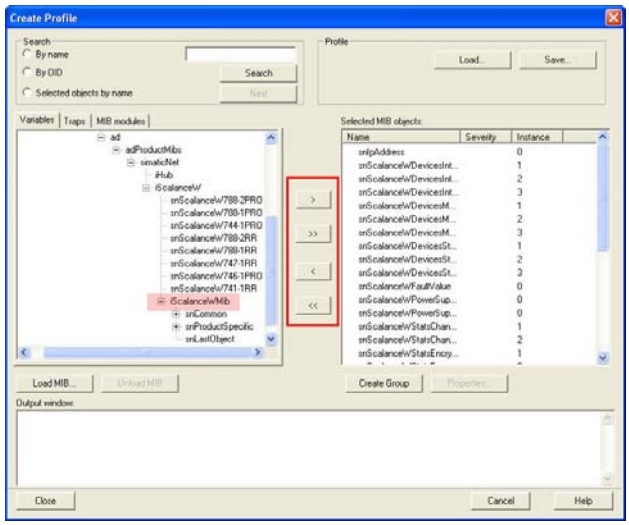
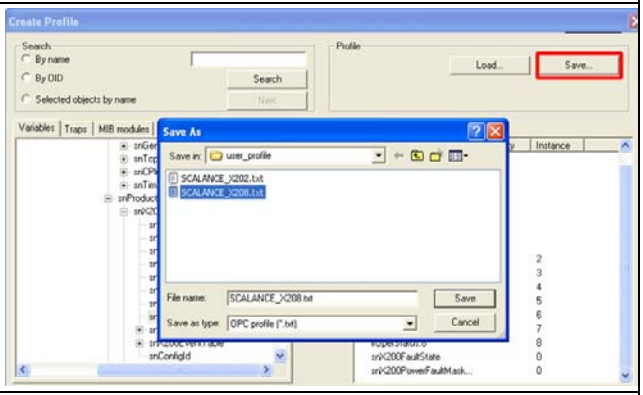
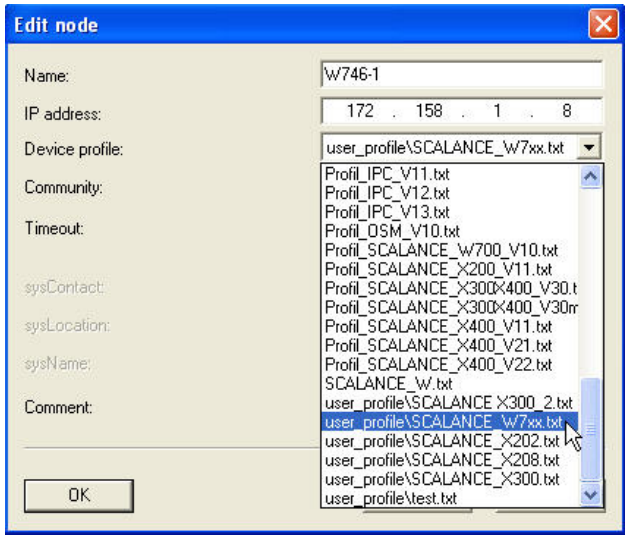
Configuration

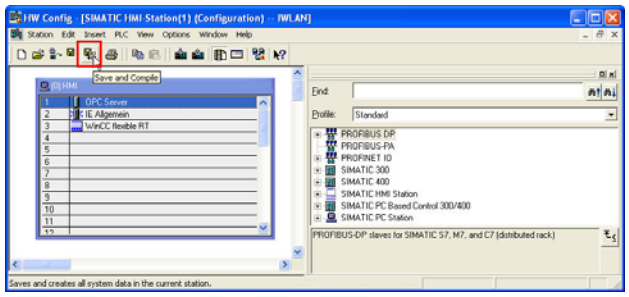
Table 5-2

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**.	
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.	
4.	With **Load** you can load a prepared profile.	

No.	Action	Comment
5.	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.	
6.	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.	
7.	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).	

No.	Action	Comment
8.	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.	
9.	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.	
10.	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.	

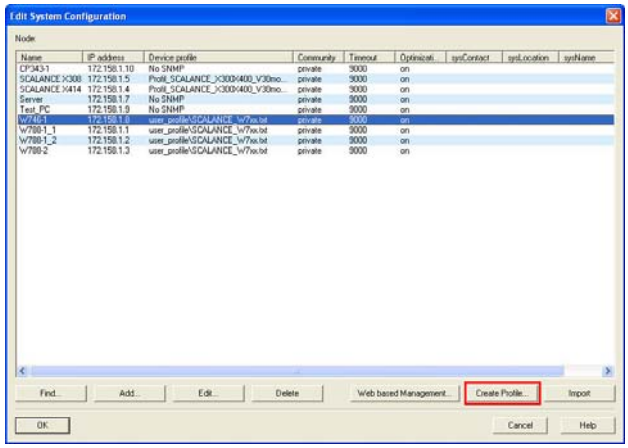
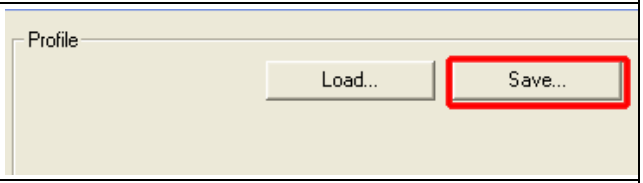
No.	Action	Comment
11.	After closing the dialog boxes with **OK** and clicking the **Save and compile** button for the station, the configuration of the SNMP OPC server is complete and the station can be loaded.	

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

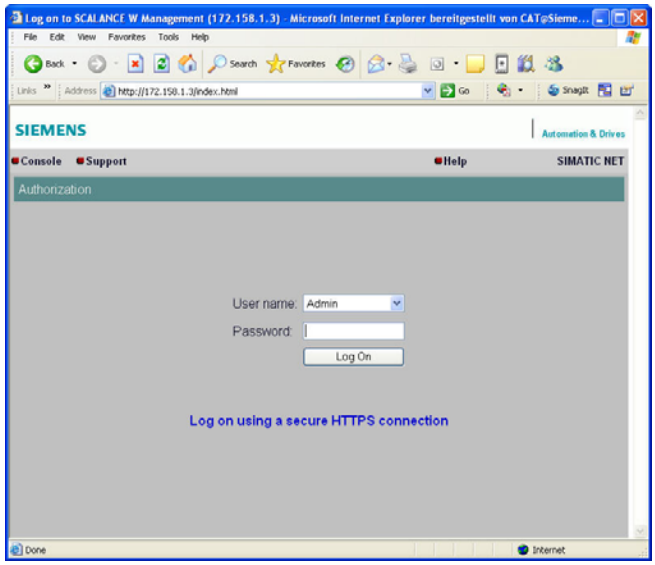
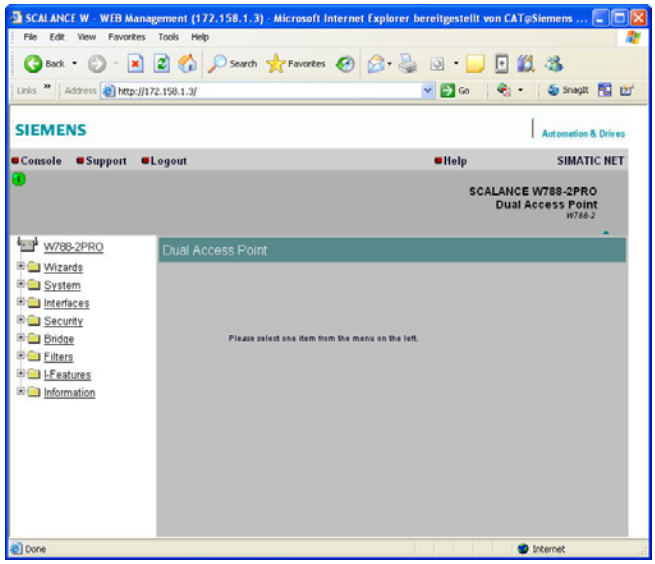
No.	Action	Comment
1.	Save the device profiles in your **STEP 7 installation directory** in the **S7DATA/snmp/user_profile** folder.	
2.	To change the device profiles, select the HMI station in STEP 7 and open the **Configuration**. Open the OPC Server properties and select the **Edit Plant Configuration…** 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

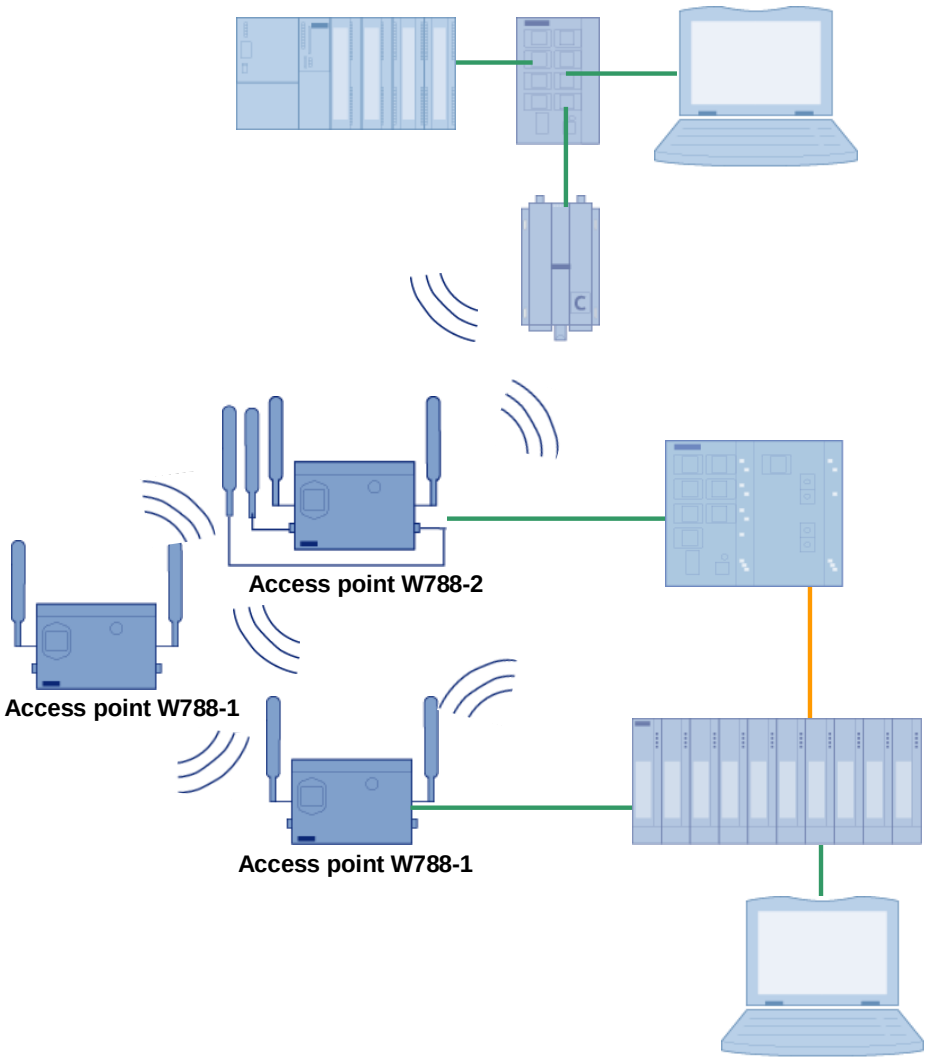
No.	Action	Comment
1.	Open an internet browser, for example Internet Explorer or Firefox, and enter the following address: **http://<IP address of the SCALANCE>**.	
2.	Enter the user name and password. Click the **Log On** button in order to log on.	The default settings are: User: admin Password: admin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

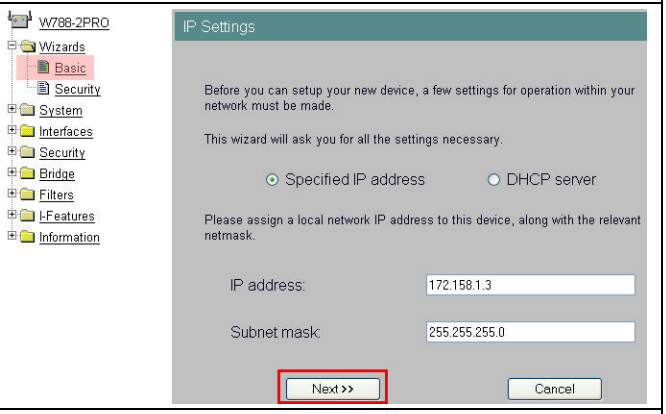
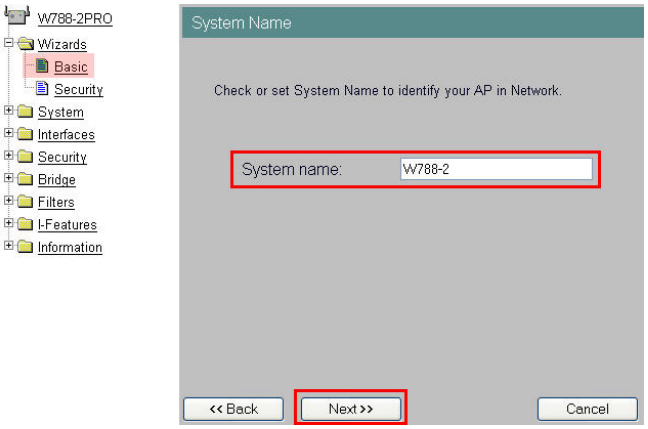
This wizard can be used to make basic settings:

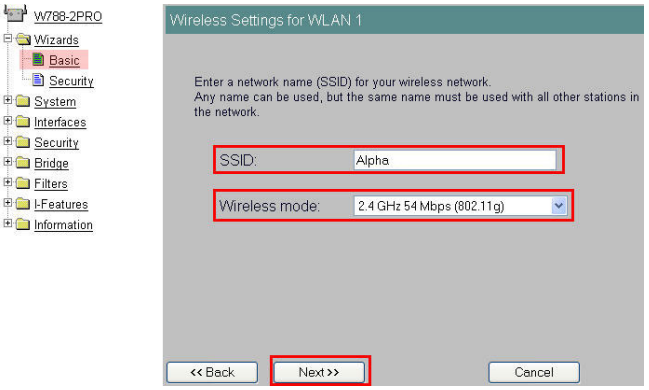
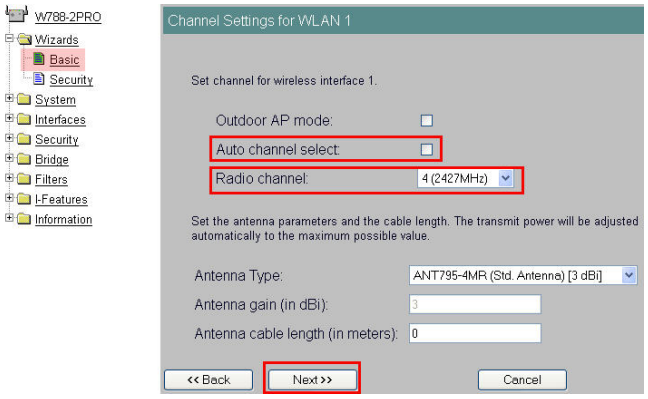
- Configuration of the radio networks
- Security settings

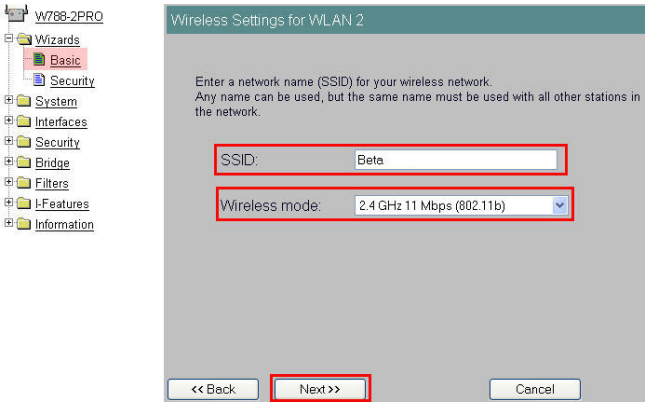
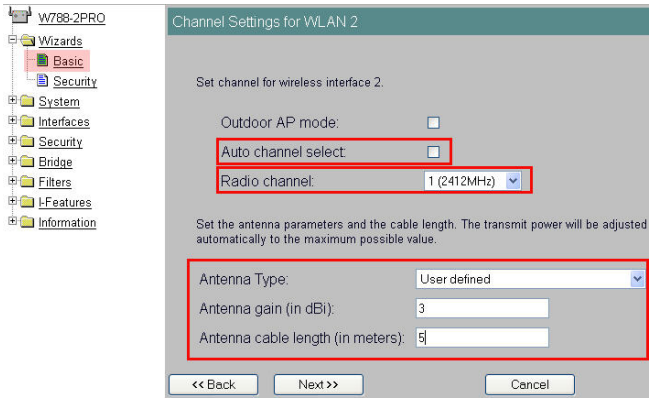
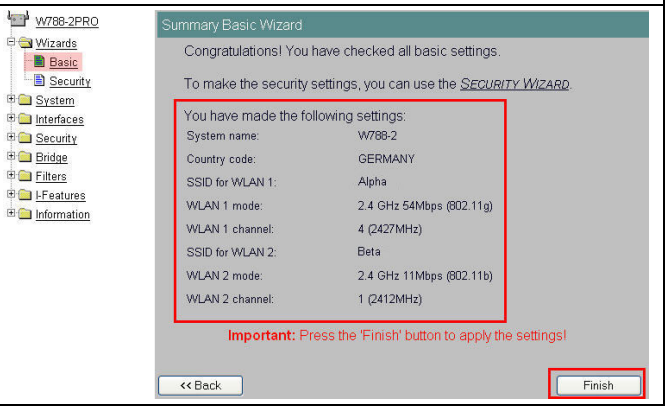
The following agreement is made for the SCALANCE W788-2 interfaces:

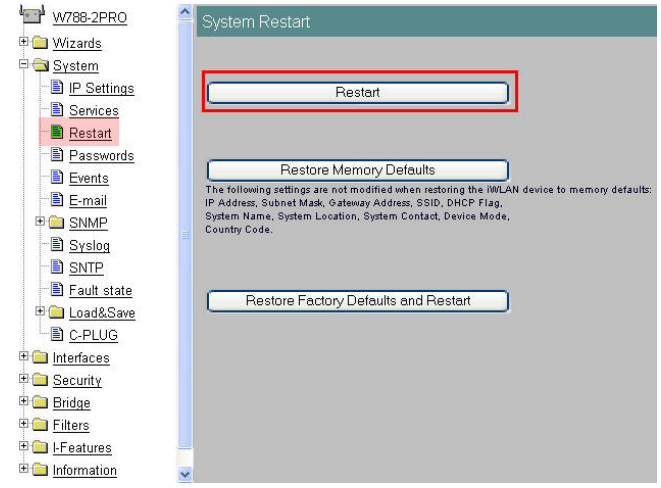
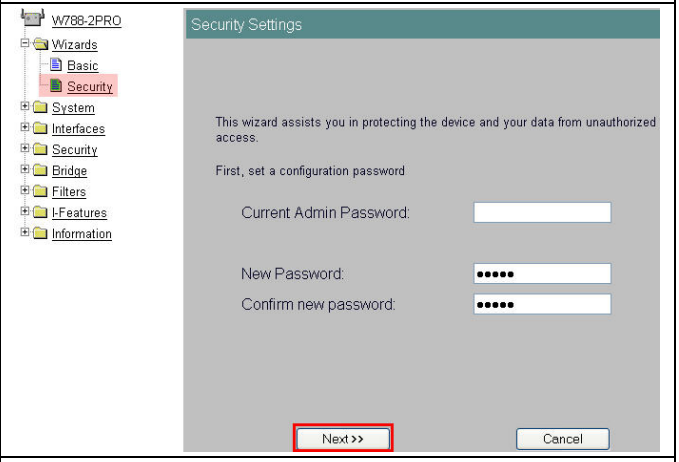
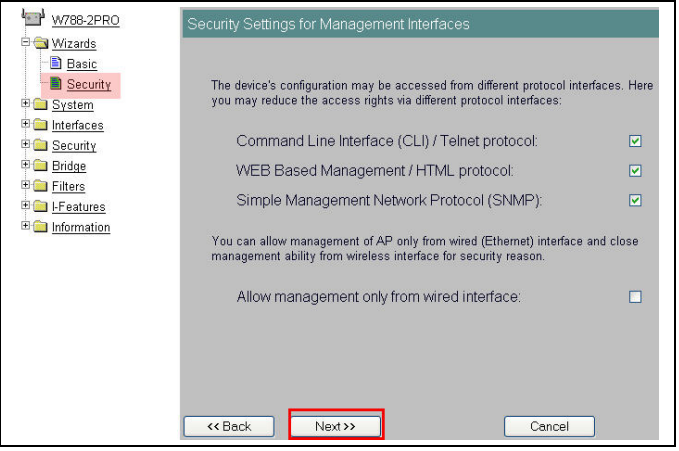
- WLAN interface 1 for the WDS function.
- WLAN interface 2 for the connection to the W746-1.

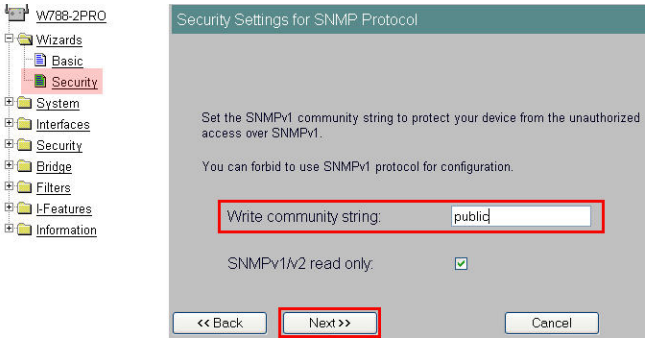
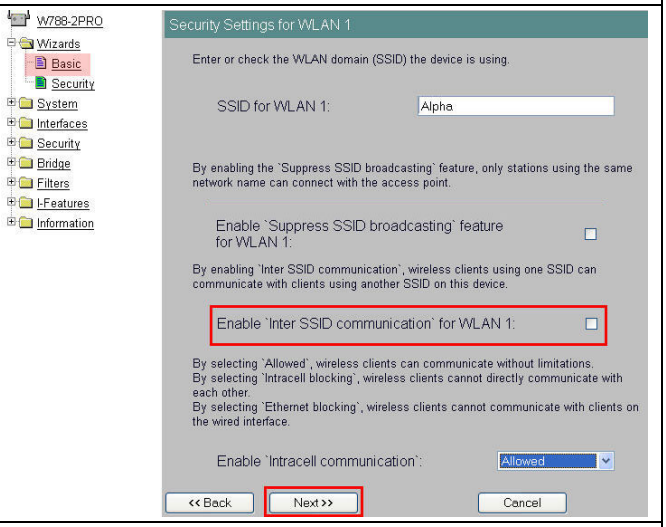
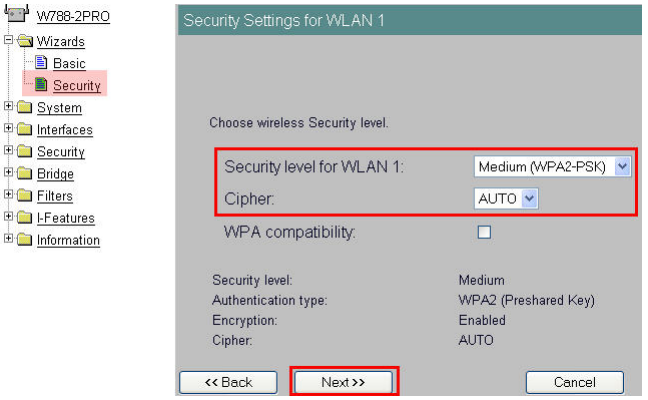
Table 5-5

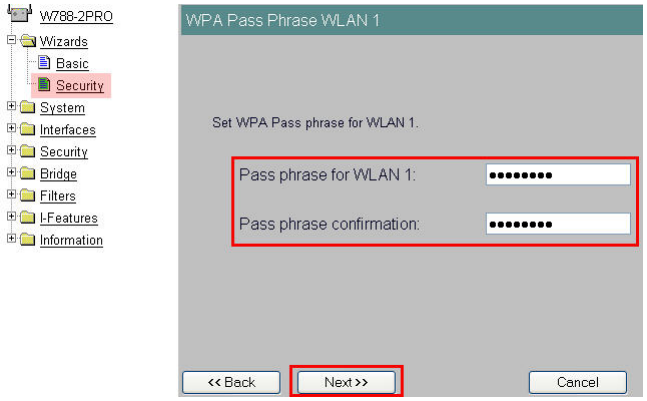
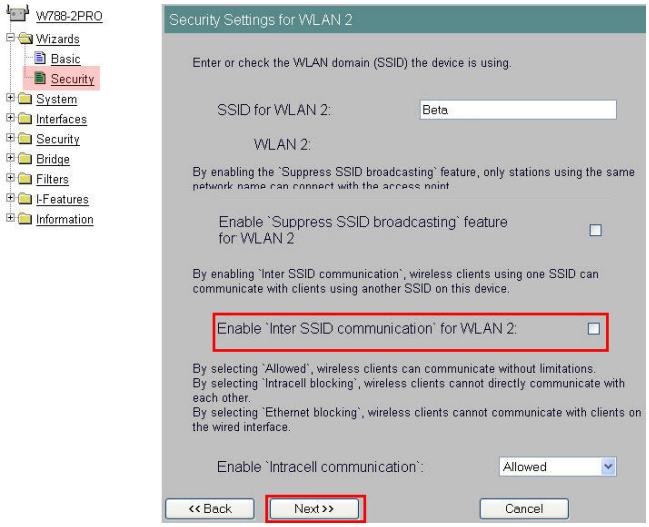
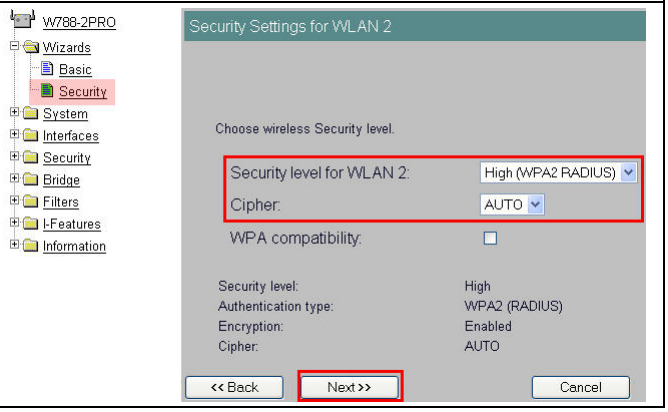
No.	Action	Comment
1.	Open the web-based management for the SCALANCE W788-2.	http://172.158.1.3
2.	Click **`Wizards -> Basic`** in the navigation bar. You can skip the first dialog box with the IP address by clicking **Next**.	
3.	You have already transferred the system name to the module via the SIMATIC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

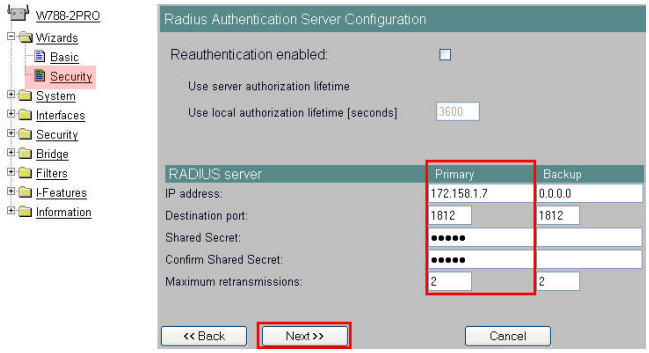
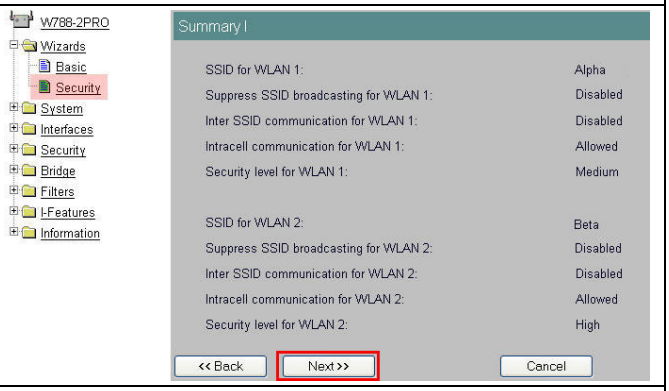
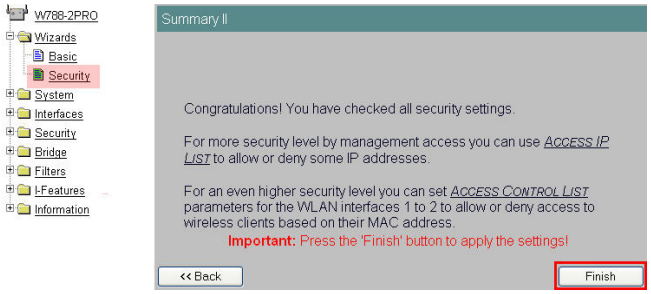
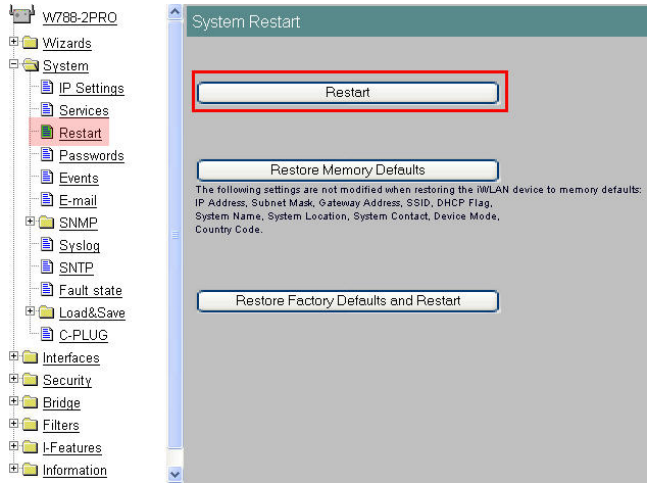
No.	Action	Comment
4.	Select **GERMANY** as a country code and go to the next step with **Next**.	
5.	Enter the name for radio network 1 under **SSID**. Select **2.4 GHz 54 Mbps (802.11g)** as **Wireless Mode**. Confirm the entry with **Next**.	
6.	Deactivate **Auto Channel select** in the next dialog box and select **Radio Channel 4** instead. Click **Next** to go to the next configuration window.	

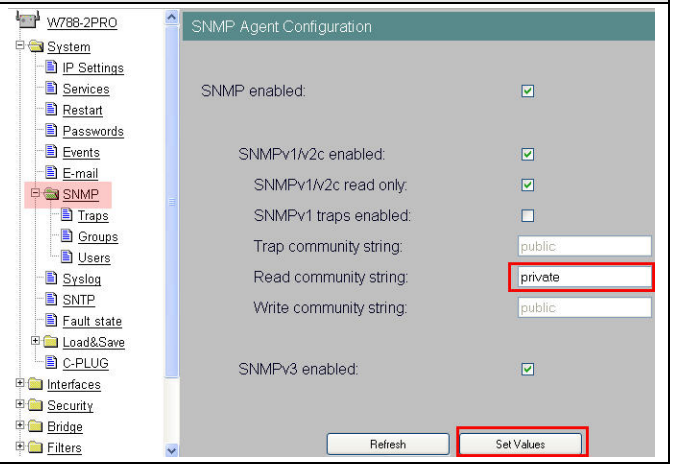
No.	Action	Comment
7.	Repeat steps 5 and 6 for the second interface. Enter the name for radio network 2 under **SSID**. Select **2.4 GHz 11 Mbps (802.11b)** as **Wireless Mode**. Confirm the entry with **Next**.	
8.	Deactivate **Auto Channel select** also for the second interface in the next step and select **Radio Channel 1** instead. Click **Next** to go to the next configuration window.	
9.	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
10.	Restart the SCALANCE W788-2 by clicking **System-> Restart**. Log on to the web-based management again after the restart. The Basic Wizard is thus complete. The radio networks have been configured.	
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**.	

No.	Action	Comment
13.	Change the write permission of SNMP variables into **public** and click **Next** to go to the next configuration.	
14.	**Deactivate** the function that clients with different SSID can communicate with each other. The next window appears after clicking **Next**.	
15.	Select **Medium (WPA2-PSK)** and **Cipher AUTO** as a **security level** for interface 1. Click **Next** to go to the next step.	

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

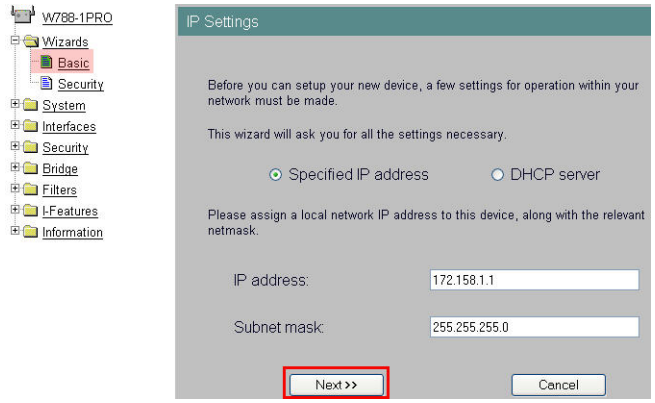
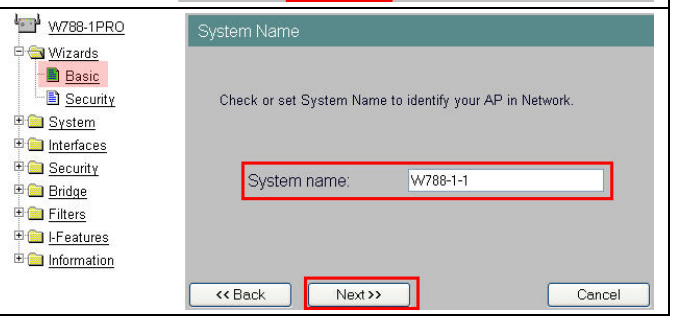
No.	Action	Comment
19.	Enter the the IP address of the **server PC** as the **primary RADIUS server**. Define a **secret admin password** and confirm this password a second time. Click **Next** to display an overview of the security settings.	
20.	You can exit the Security Wizard with **Next**.	
21.	Close the Security Wizard with **Finish**.	
22.	Restart the SCALANCE W788-2 by clicking **`System-> Restart`**.	

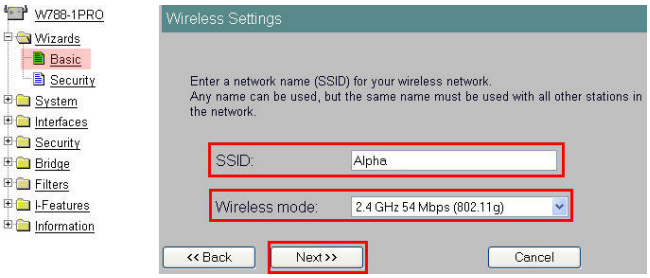
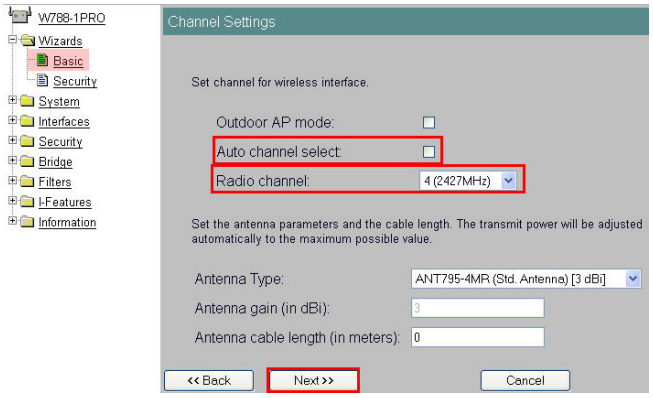
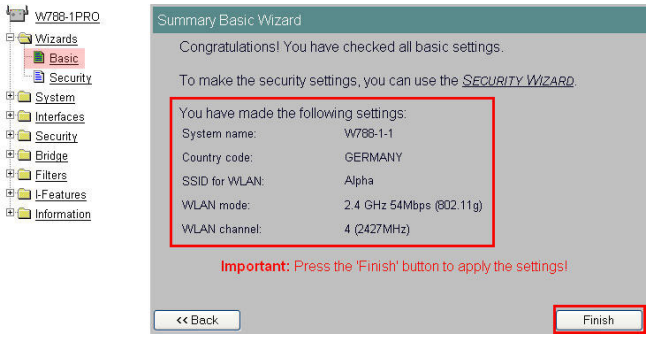
No.	Action	Comment
23.	Navigate to **System-> SNMP** and enter **private** under **read community string**. Confirm with **Set Values**.	

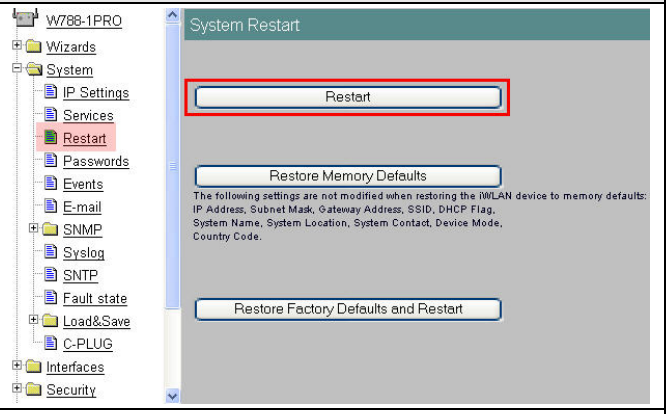
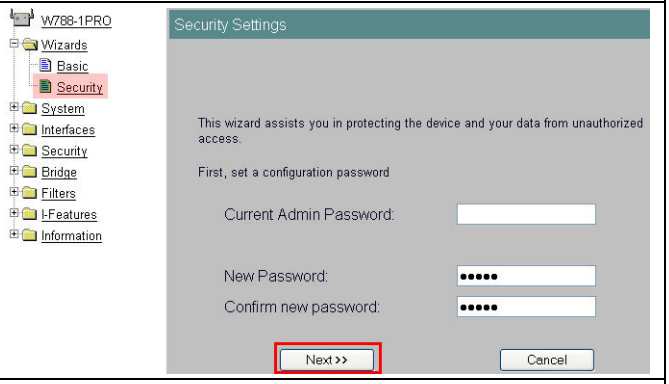
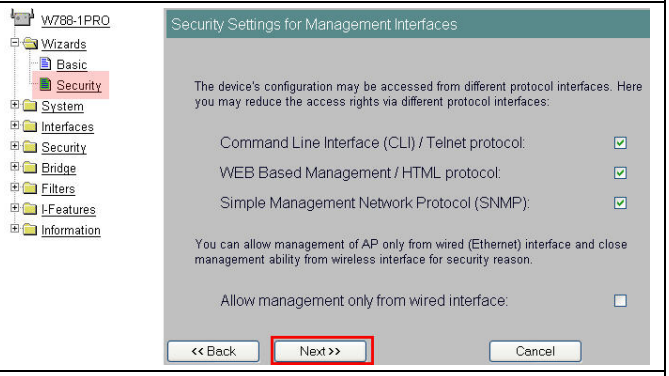
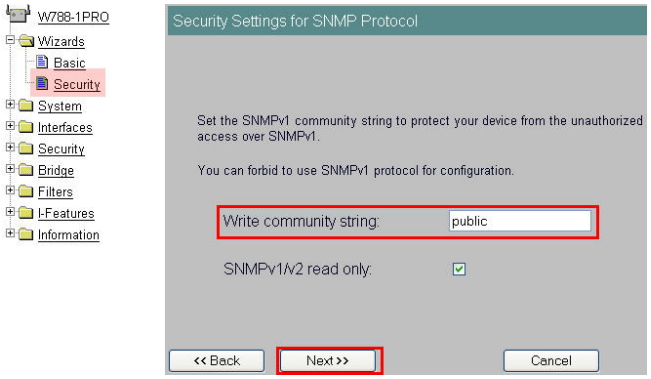
5.3.2 Wizards of both SCALANCE W788-1

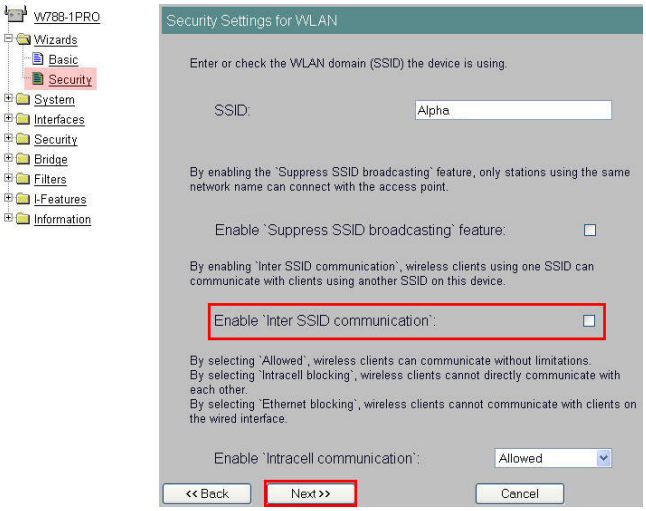
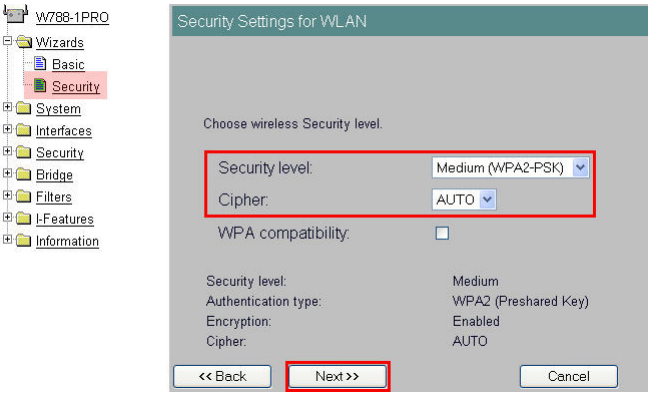
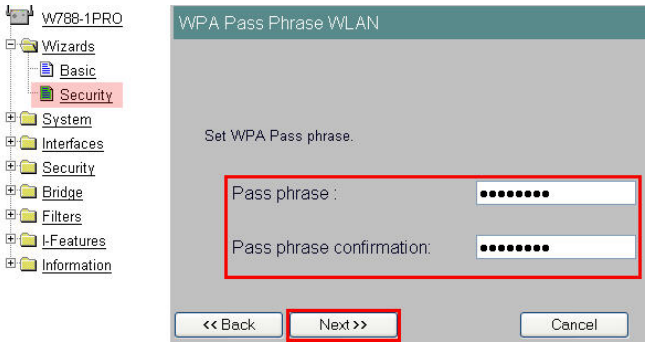
Both SCALANCE W788-1 are configured with identical settings. Only the system name and the IP addresses are different.

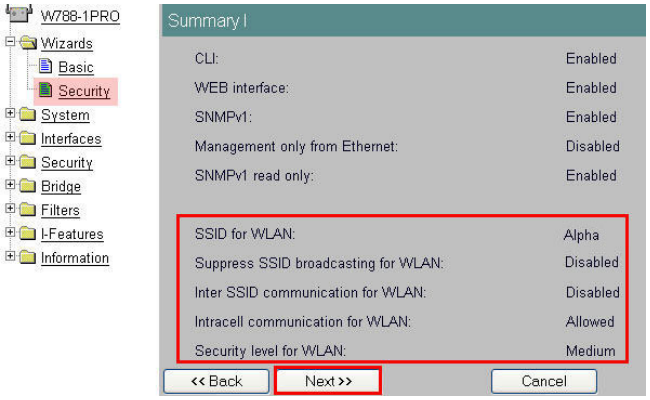
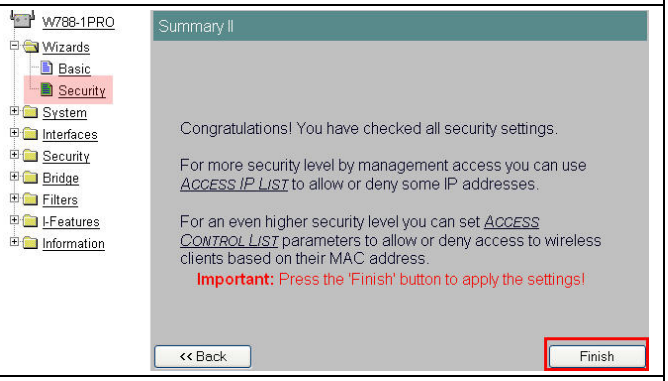
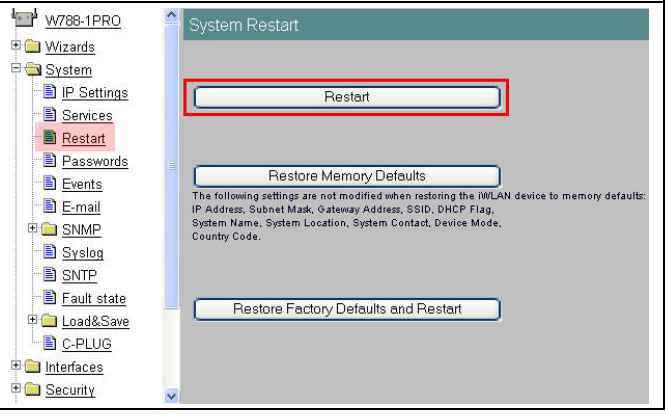
Table 5-6

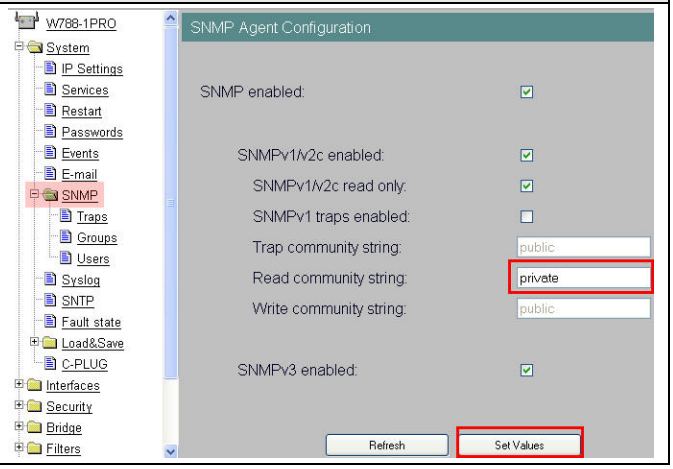
No.	Action	Comment
1.	Open the web-based management for the first SCALANCE W788-1.	http://172.158.1.1
2.	Click **Wizards -> Basic** in the navigation bar. You can skip the first dialog box with the IP address by clicking **Next**.	
3.	You have already transferred the system name to the module via the 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.	Restart the SCALANCE W788-2 by clicking **System ->Restart**. Log on to the web-based management again after the restart. The Basic Wizard is thus complete.	
9.	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**.	
10.	Do not change the default settings in the next step and proceed with **Next**.	
11.	Change the write permission of SNMP variables into **public** and click **Next** to go to the next configuration.	

No.	Action	Comment
12.	**Deactivate** the function that clients with different SSID can communicate with each other. The next window appears after clicking **Next**.	
13.	Select **Medium (WPA2-PSK)** and **Cipher AUTO** as a **security level**. Click **Next** to go to the next step.	
14.	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.	

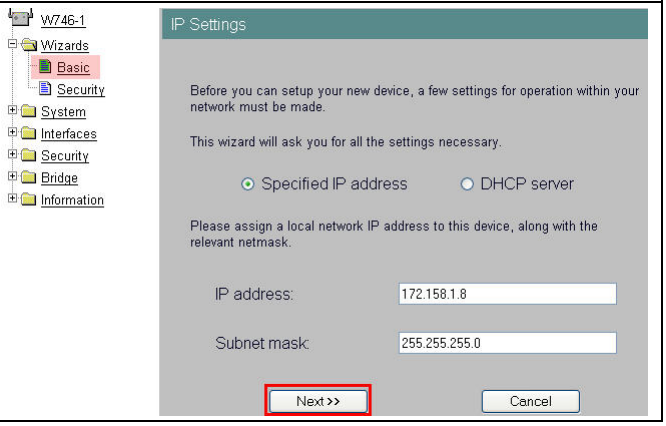
No.	Action	Comment
15.	You can exit the Security Wizard with **Next**.	
16.	Close the Security Wizard with **Finish**.	
17.	Restart the SCALANCE W788-1 by clicking **System-> Restart**.	

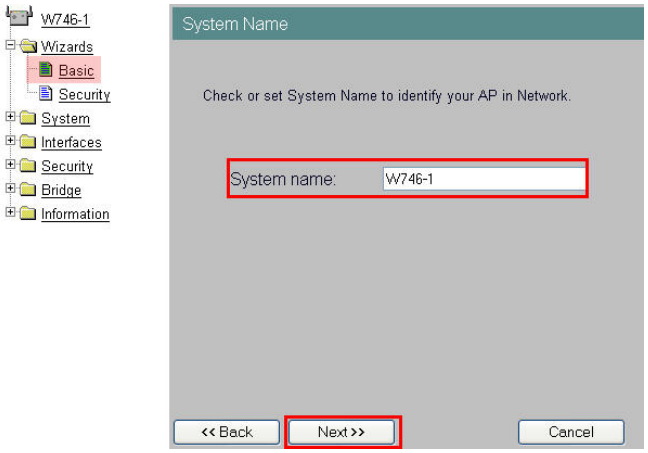
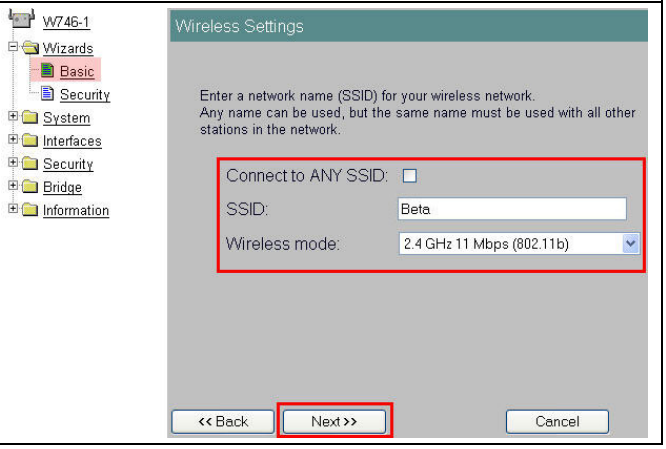
No.	Action	Comment
18.	Navigate to **System-> SNMP** and enter **private** under **read community string**. Confirm with **Set Values**.	

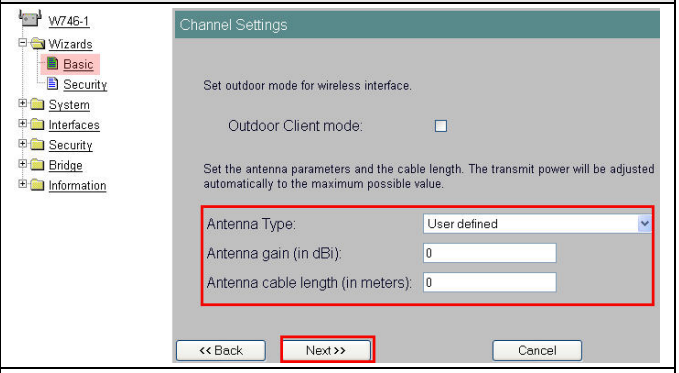
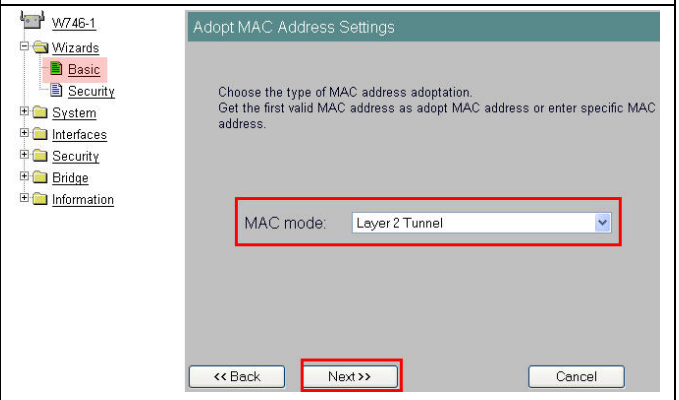
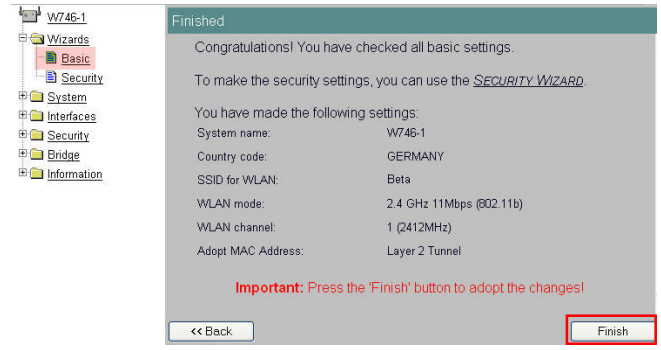
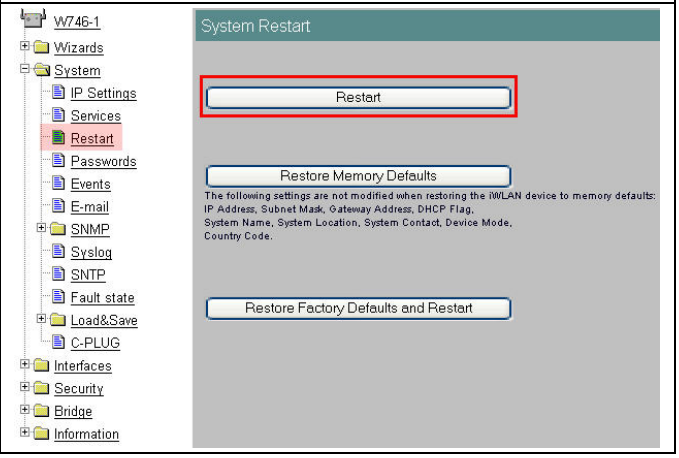
Note Configure the second SCALANCE W788-1 in the same way. For this purpose, connect the server PC directly to the Ethernet interface of the second SCALANCE W788-1.

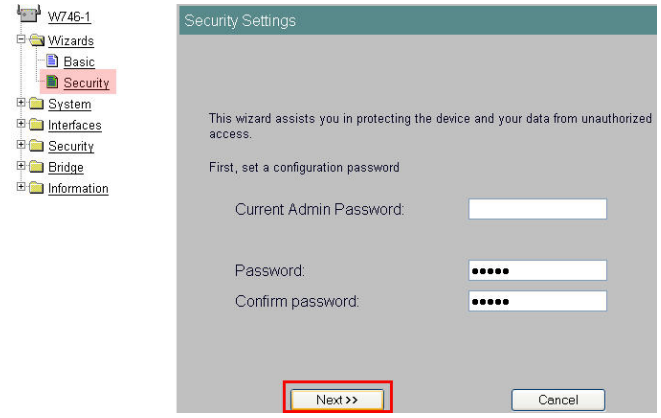
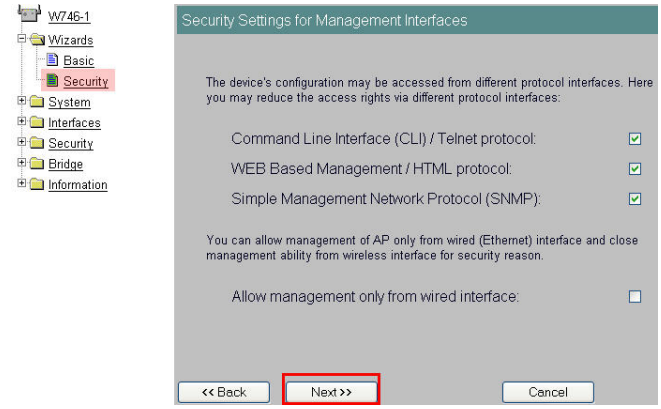
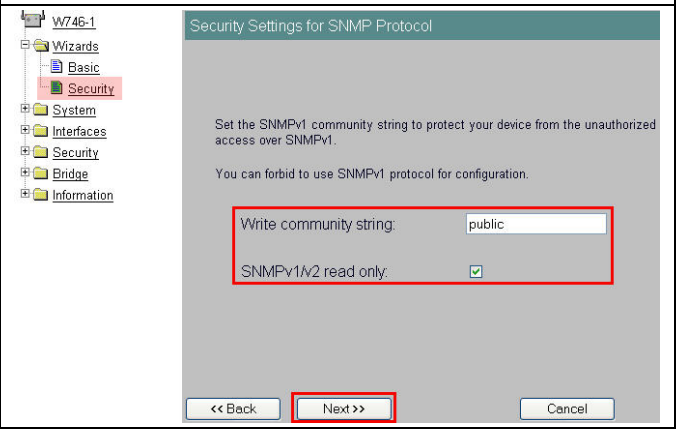
5.3.3 Wizards of the SCALANCE W746-1

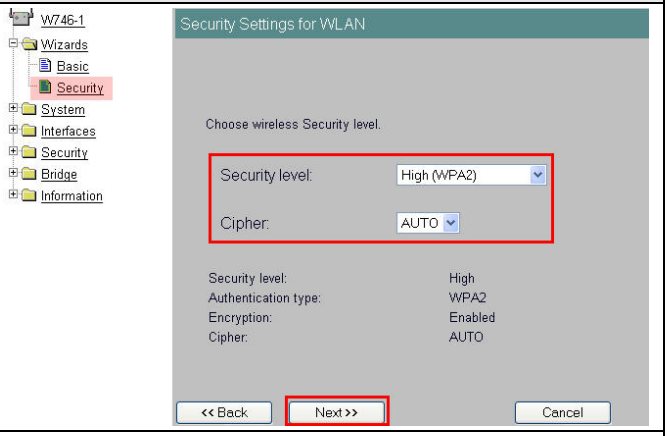
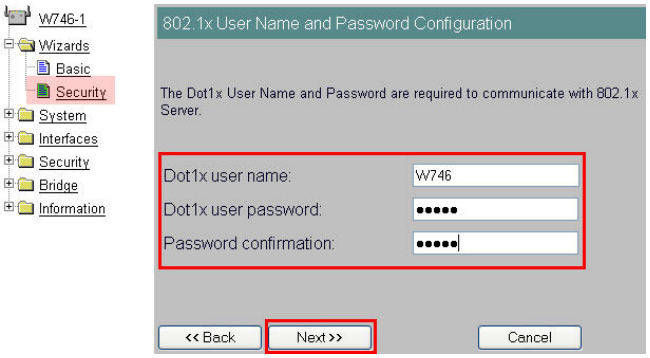
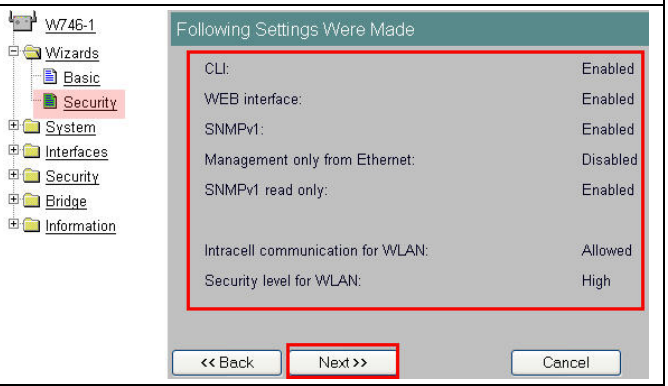
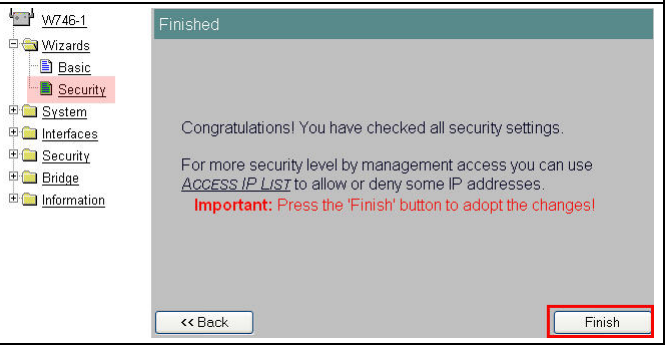
Table 5-7

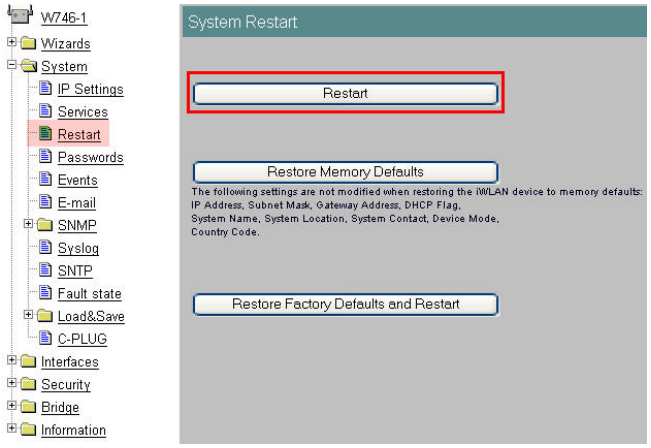
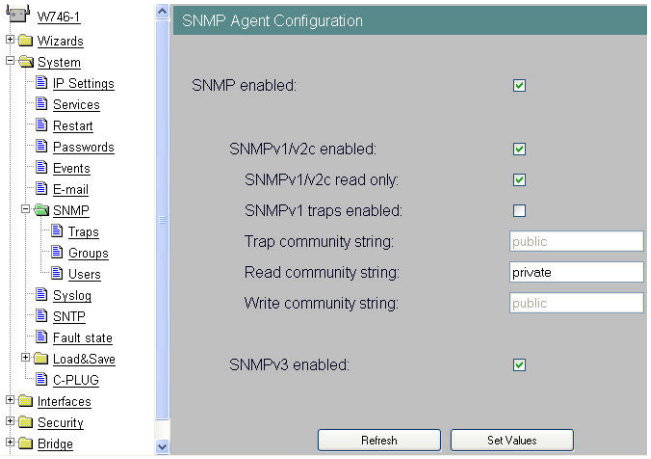
No.	Action	Comment
1.	Connect the server PC to the SCALANCE X108.	
2.	Open the web-based management for the SCALANCE W746-1.	http://172.158.1.8
3.	Click **Wizards -> Basic** in the navigation bar. You can skip the first dialog box with the IP address by clicking **Next**.	

No.	Action	Comment
4.	You have already transferred the system name to the module via the SIMATIC MANAGER. Go to the next window here.	
5.	Select **GERMANY** as a country code and go to the next step with **Next**.	
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**.	

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.	
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 configu-ration of the RADIUS server. Click **Next** to go to the next step.	
16.	You can exit the Security Wizard with **Next**.	
17.	Close the Security Wizard with **Finish**.	

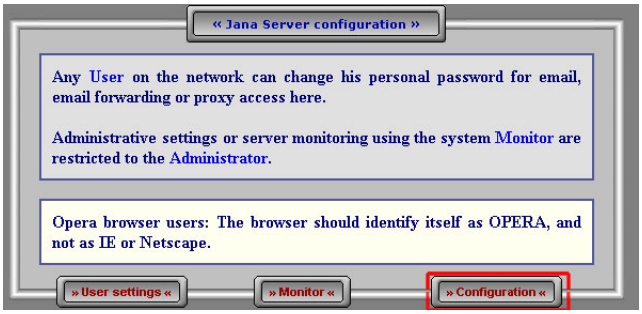
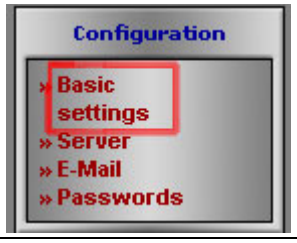
No.	Action	Comment
18.	Restart the SCALANCE W746-1 by clicking **System ->Restart**.	
19.	Navigate to **System-> SNMP** and enter **private** under **read community string**. Confirm with **Set Values**.	
20.	Reconnect the server PC to port 9.3 of the SCALANCE X414-3E.	

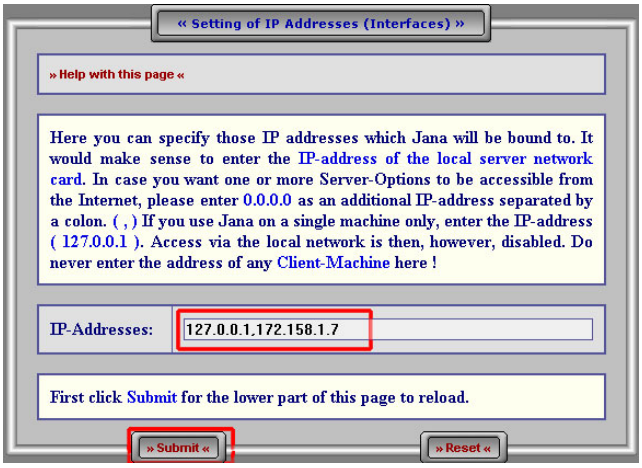
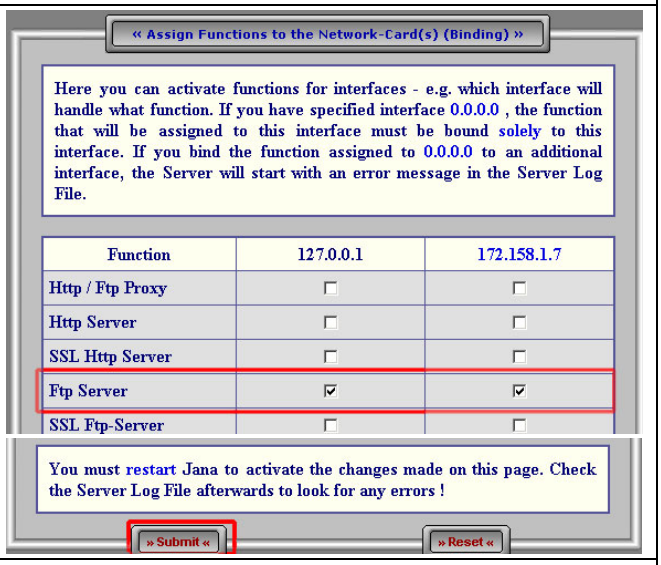
5.4 Configuration of the FTP server

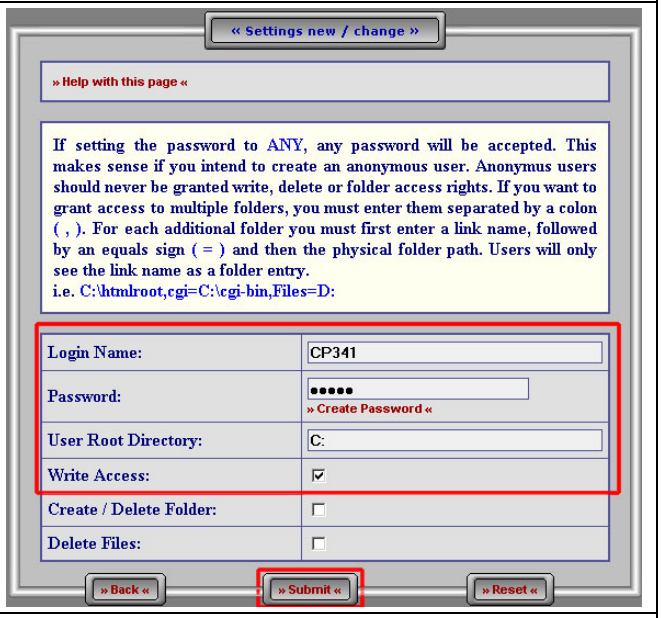
The configuration of the FTP server is demonstrated using the JanaServer freeware tool.

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.	

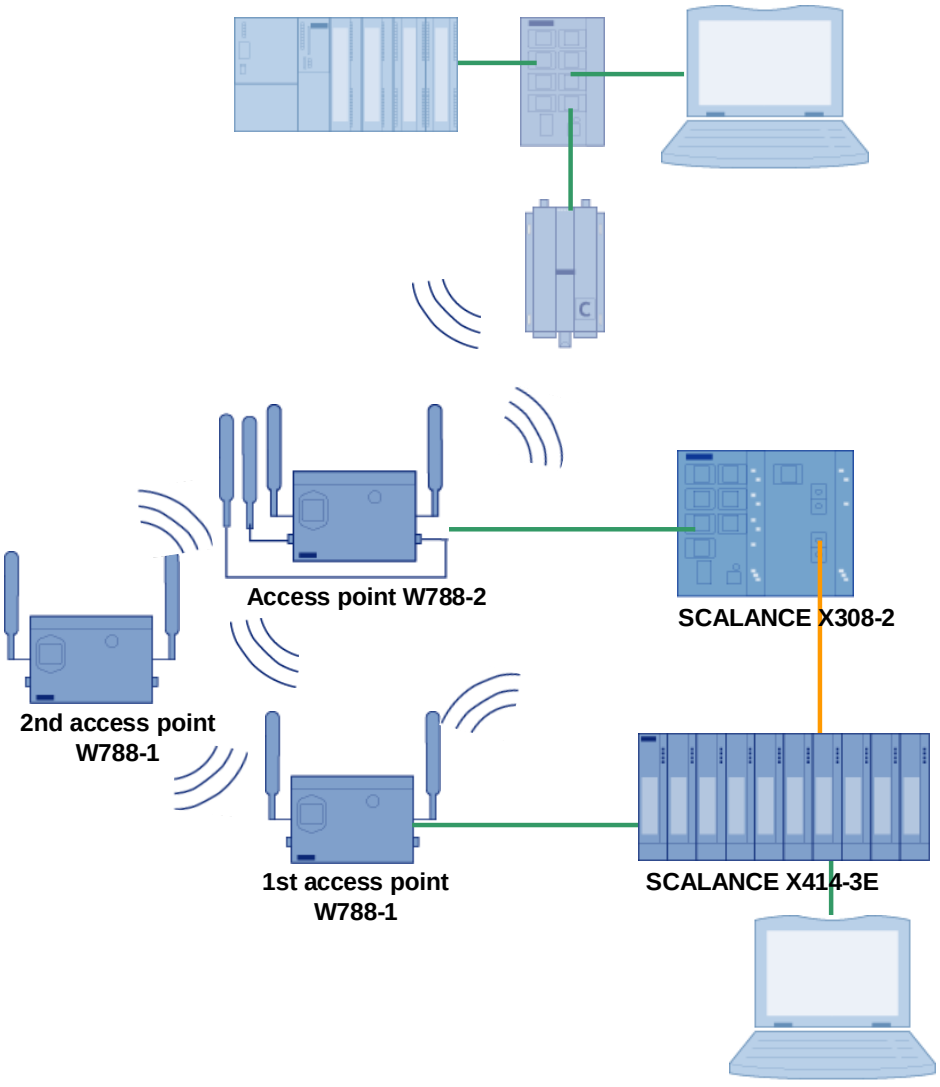
No.	Action	Comment
5.	Enter the additional IP address **172.158.1.7** under **Settings of IP Addresses**. The IP addresses are separated by commas. Confirm with **Submit**.	
6.	**Activate** the **FTP-Server** both for the **Local host** (127.0.0.) and the **PC** (172.158.1.7). Scroll down the HTML page and accept your setting with **Submit**.	
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.	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**. **Note**: The login data for the user are stored in the DB10 data block and can be opened and edited using the SIMATIC MANAGER.	
12.	Restart the PC.	

5.5 Configuration of the redundancy method RSTP

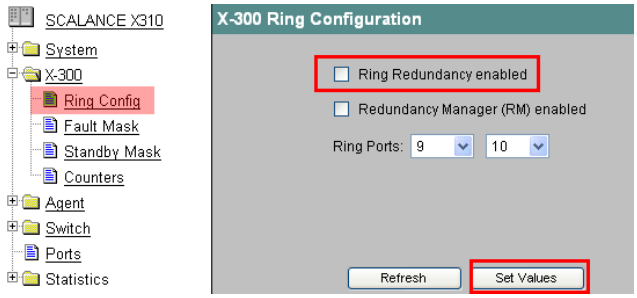
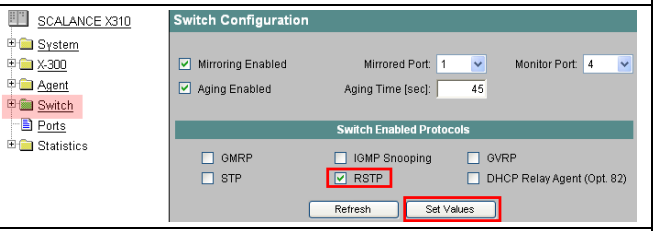
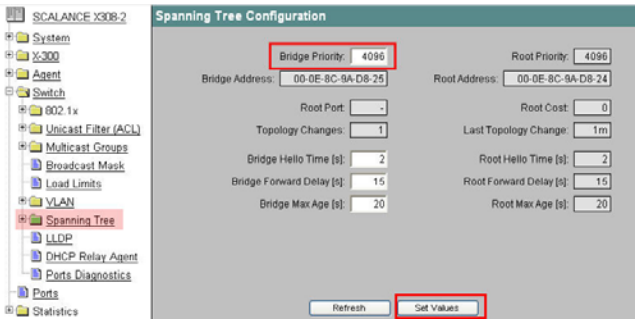
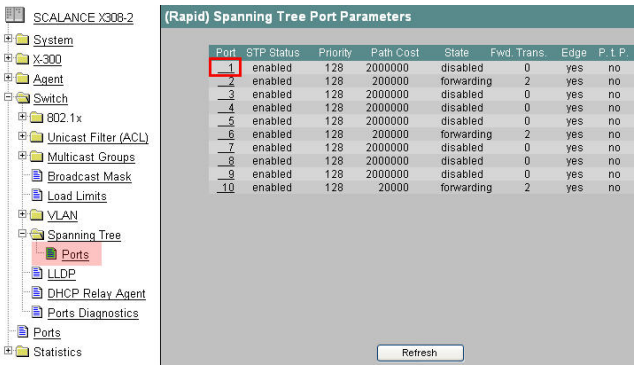
The **rapid spanning tree** function is configured in **all** SCALANCE X modules and access points.

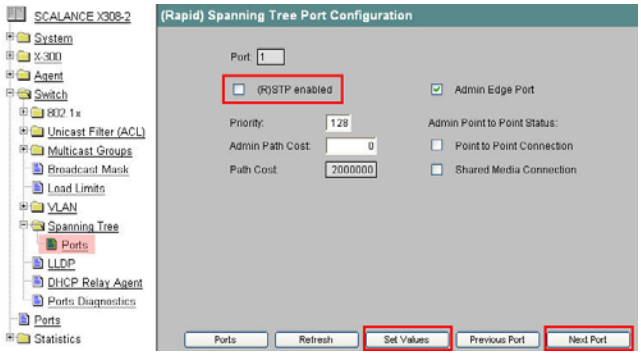
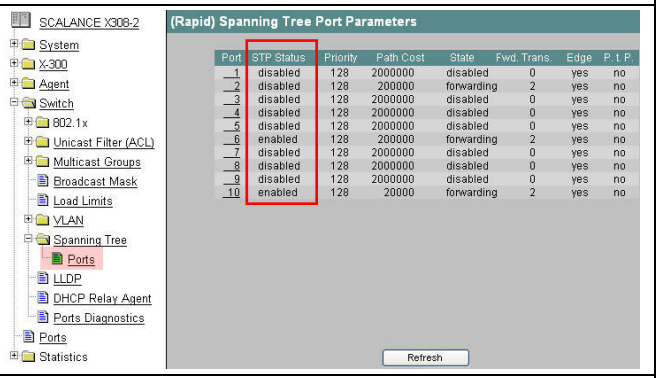
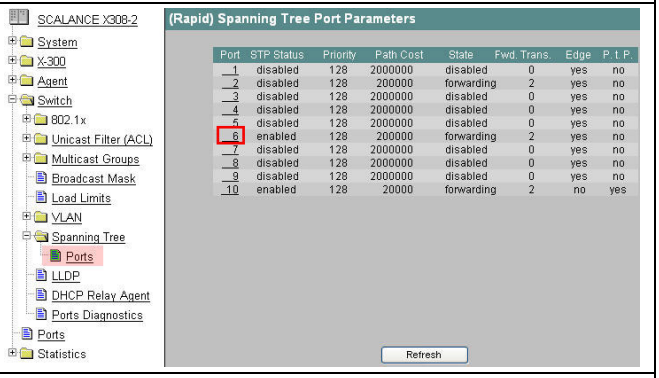
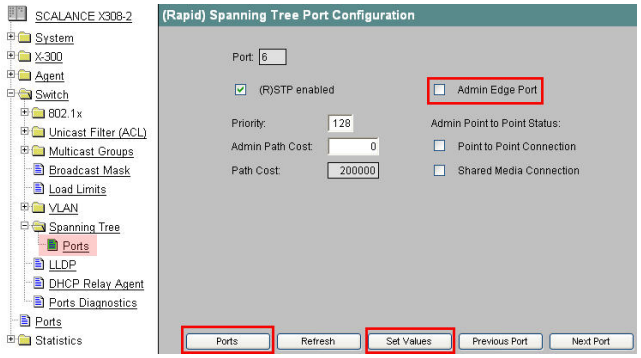
Figure 5-3



RSTP in SCALANCE X308-2

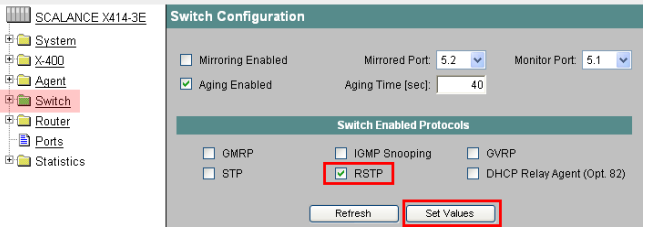
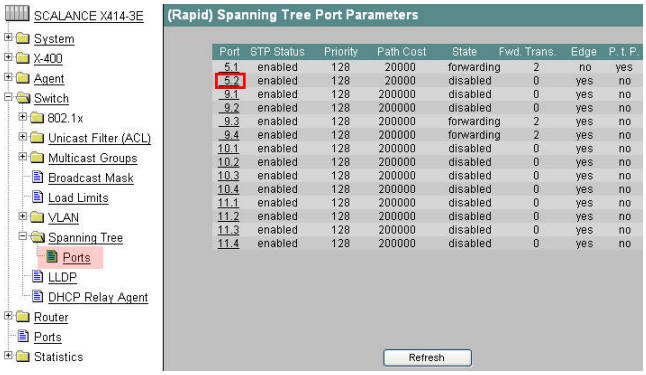
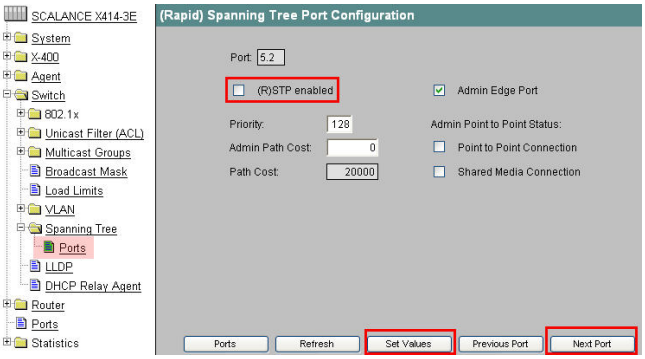
Table 5-9

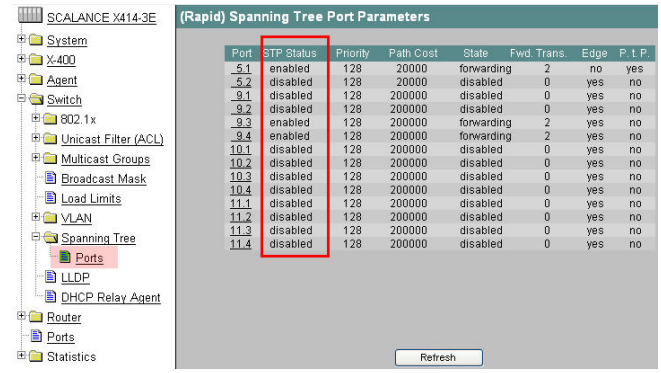
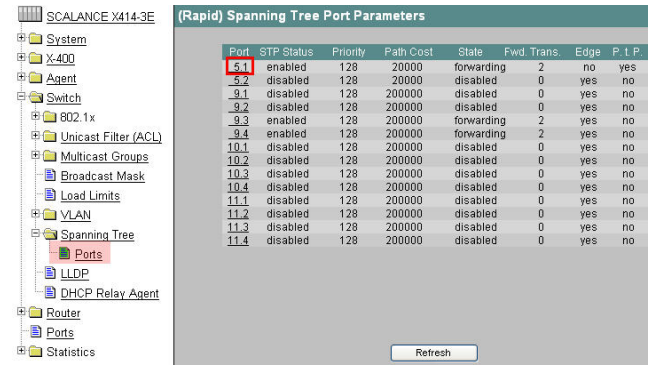
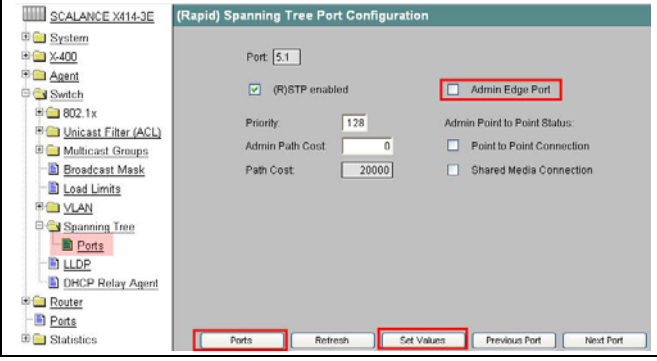
No.	Action	Comment
1.	Open the web-based management for the SCALANCE X308-2.	http://172.158.1.5
2.	For the rapid spanning tree protocol, the ring redundancy must be switched off in the SCALANCE. Navigate to **`X-300->Ring Config`** and switch off the ring redundancy. Confirm the action with **Set Values**.	
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.	

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.	
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

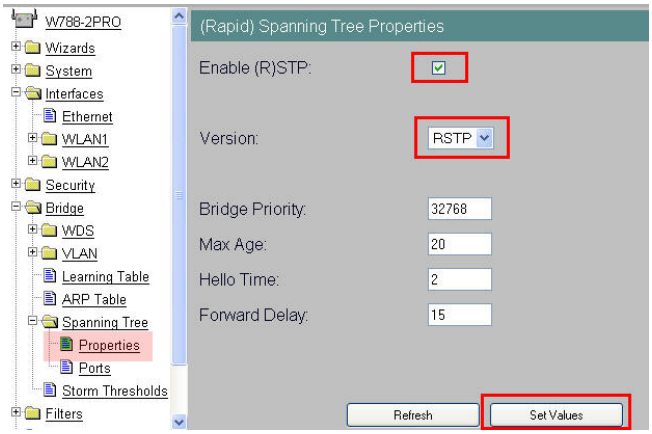
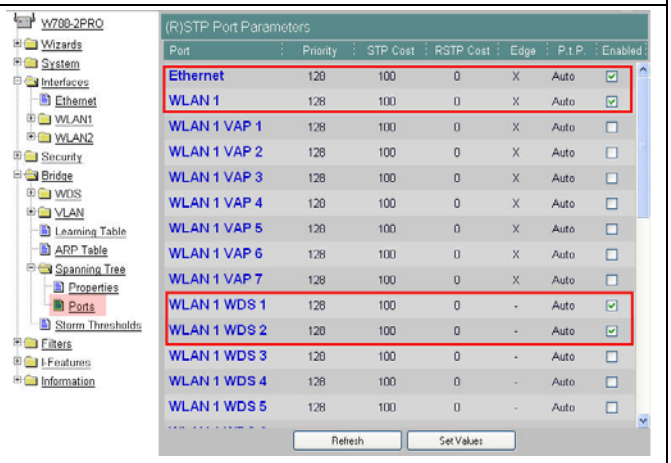
Table 5-10

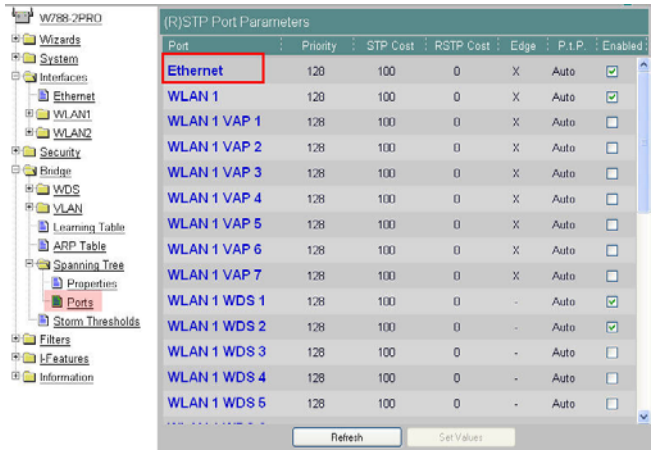
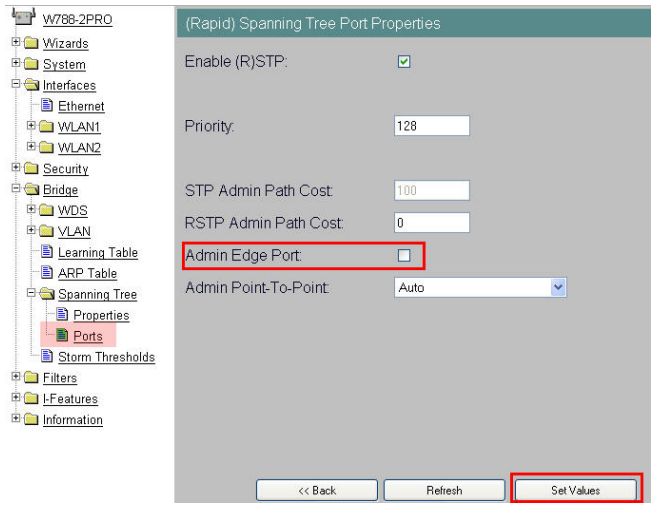
No.	Action	Comment
1.	Set the DIP switch on the SCALANCE X414-3E to the position shown to the right. The DIP switches are located in module 4.	RM ➔ Off STBY ➔ Off R1 ➔ On R2 ➔ On
2.	After changing the DIP switch, the SCALANCE must be restarted. Briefly switch the voltage supply of the SCALANCE X414-3E 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.	
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.	
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.	
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.	

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.	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 • **Ethernet,** • **WLAN 1,** • **WLAN 1** • **WDS 1,** • **WLAN 1** • **WDS 2,** • **WLAN 2** • **Redundancy**. Confirm with **Set Values**.	

No.	Action	Comment
4.	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.	
5.	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**.	

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.

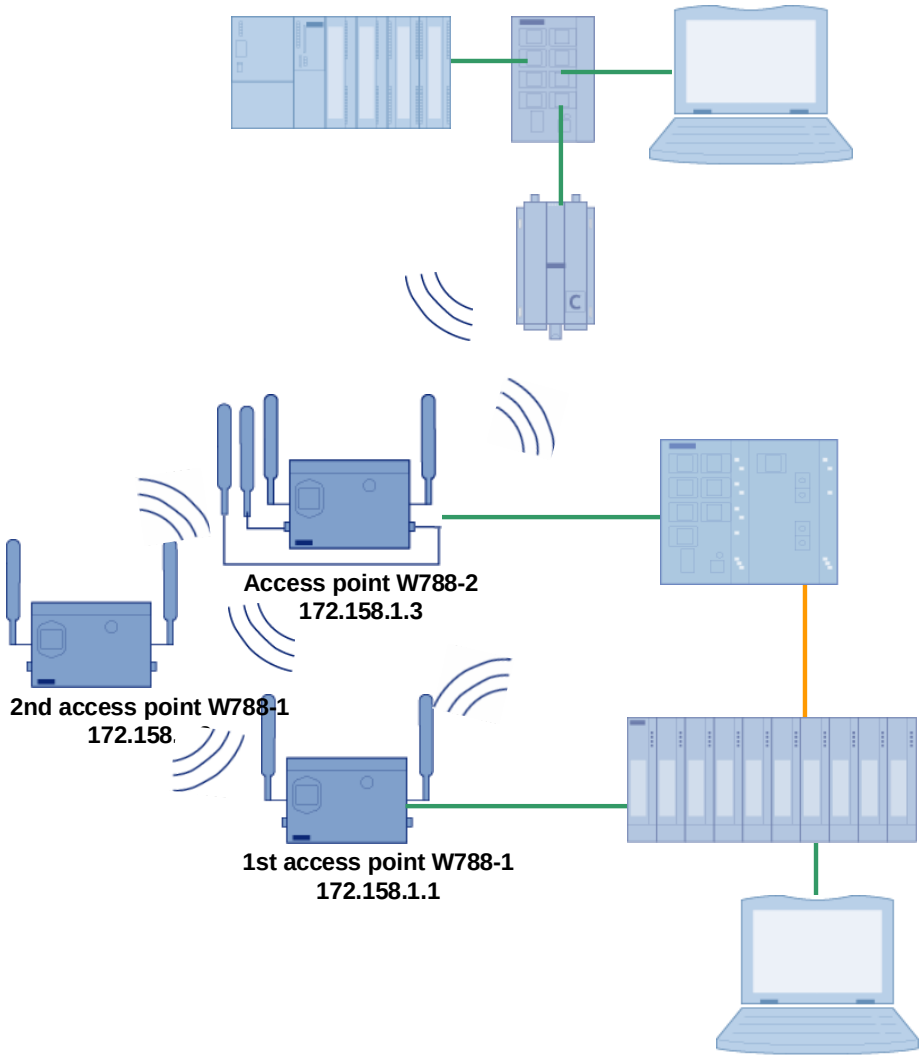
Note

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

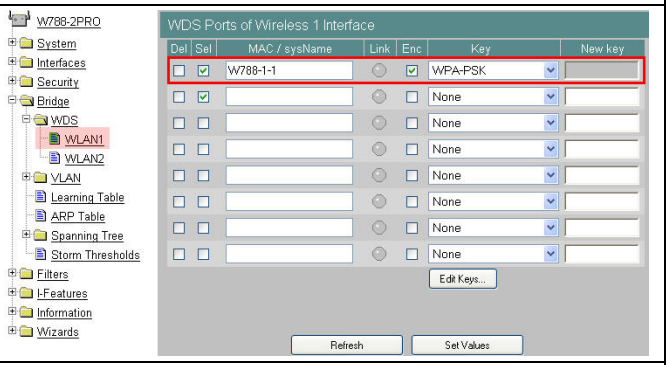
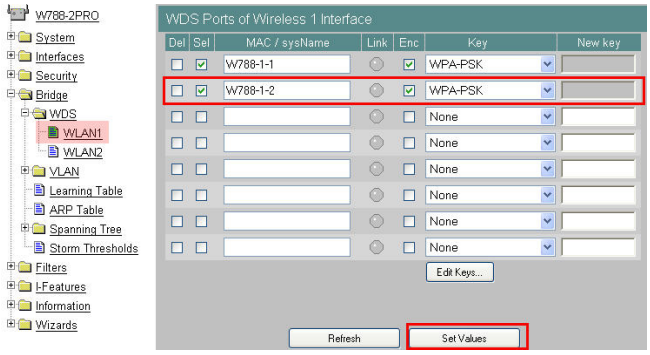


5.6.1 WDS in the SCALANCE W788-2

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

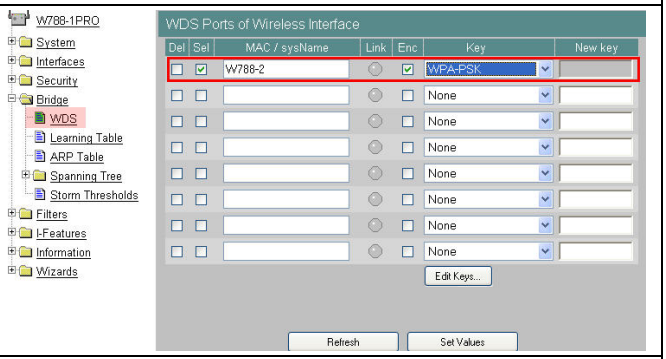
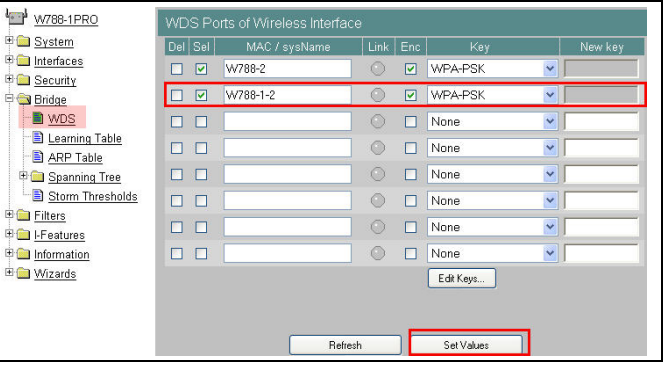
No.	Action	Comment
1.	Open the web-based management for the SCALANCE W788-2.	http://172.158.1.3
2.	Click **`Bridge-> WDS->WLAN1`** in the navigation bar. Enter the **device name of the first SCALANCE W788-1** in the first line. Tick **Sel** (Select) and **Enc** (Encryption). Select **WPA-PSK** as a key.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

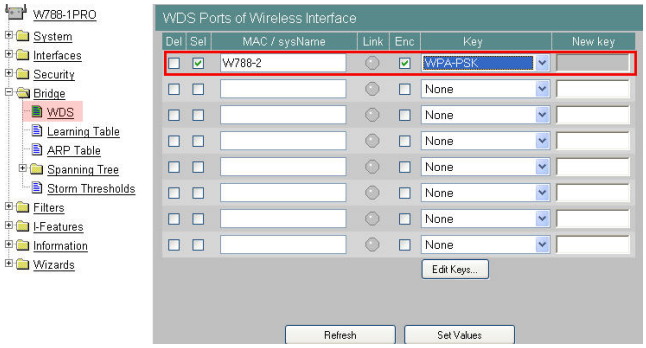
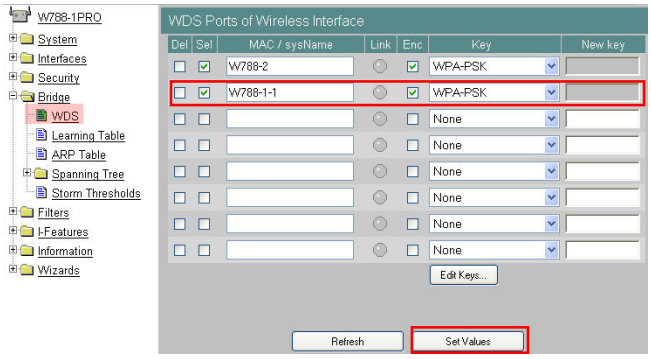
5.6.3 WDS in the second SCALANCE W788-1

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)

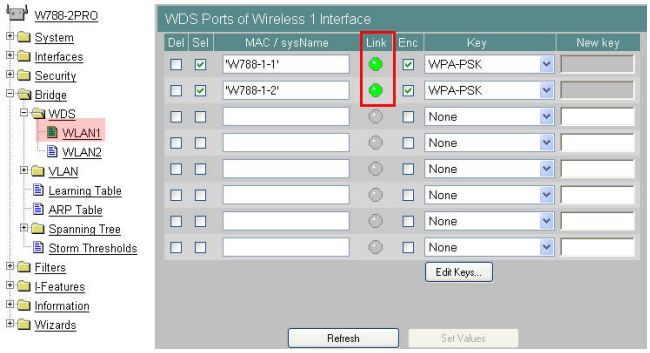
Note To be able to configure the second SCALANCE W788-1, the server must be connected directly to the Ethernet port of the access point. After the configuration is complete, reconnect the server to the SCALANCE X414-3E.

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

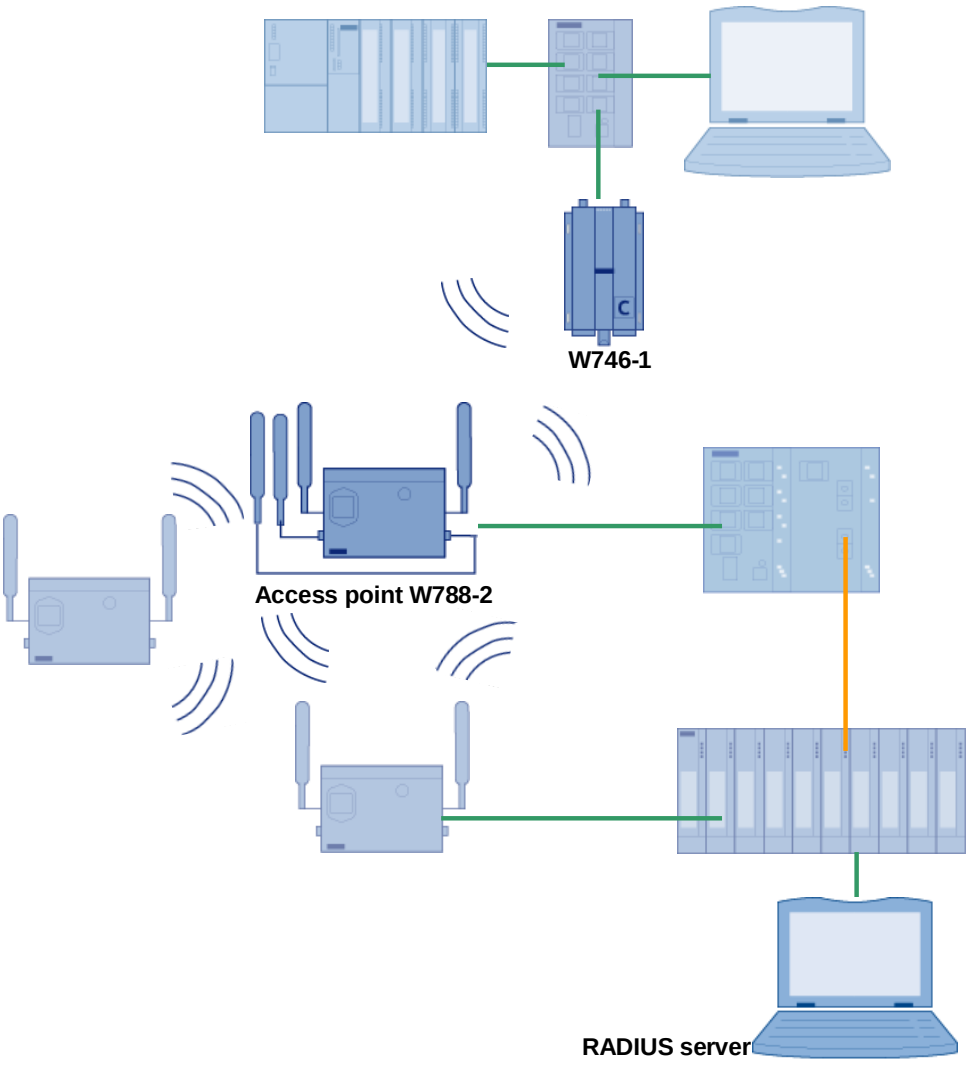
Table 5-15

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.	

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.

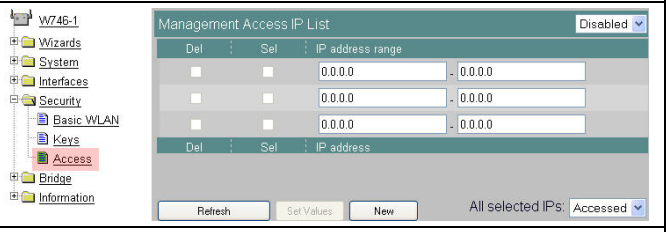
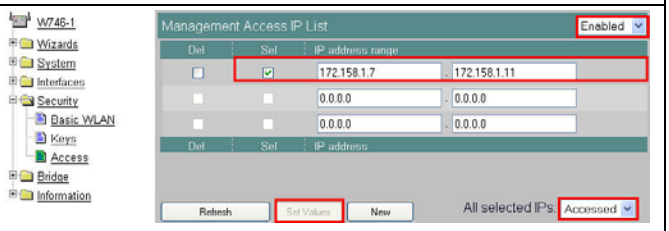
Figure 5-5



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 **Sel** and **Accessed** for all IP addresses. Set the IP address range to **Enable.** Confirm your entry with **Set Values**.	

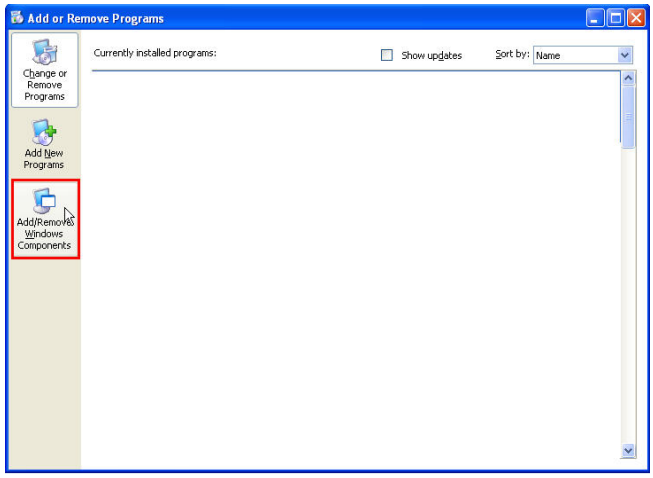
5.7.2 RADIUS server in Win2003 server

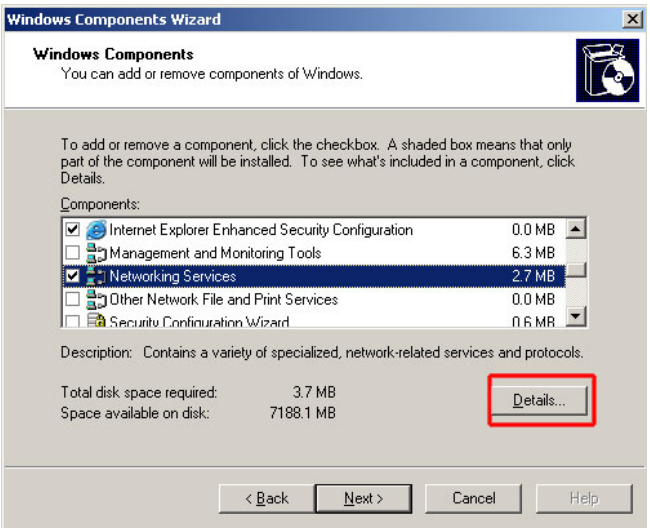
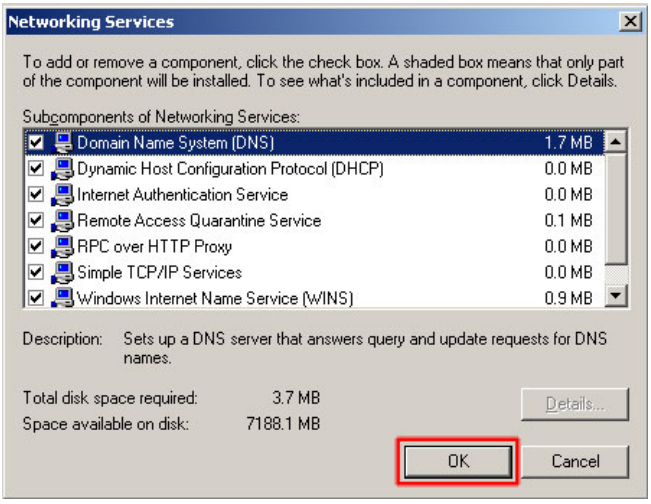
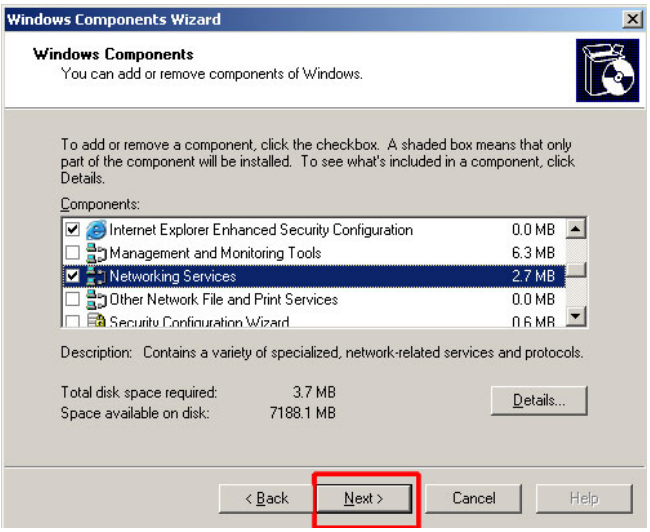
Install the IAS

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

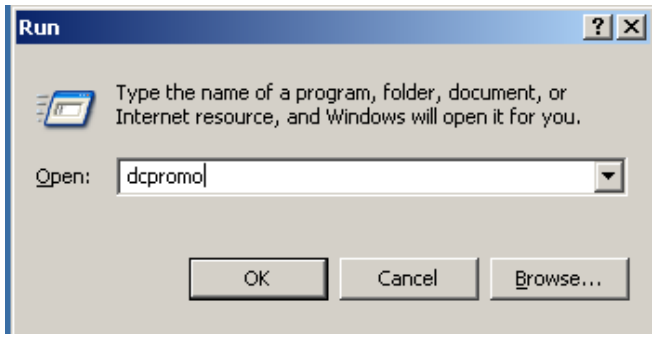
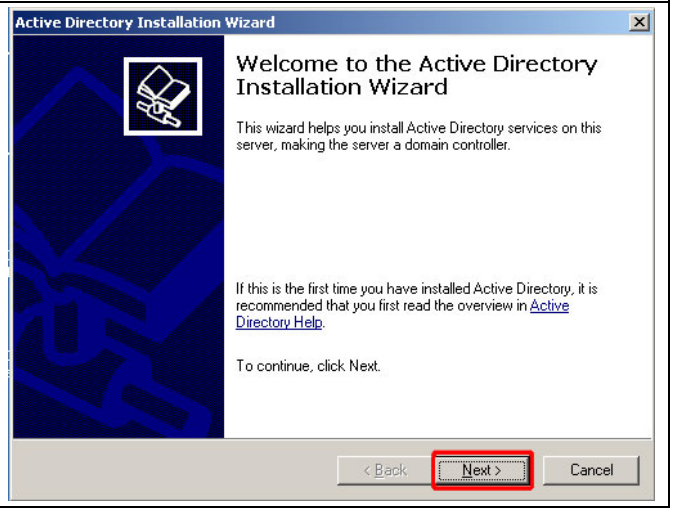
No.	Action	Comment
1.	Open the control panel by pressing **`Start-> Settings-> ControlPanel`**. Double-click **Add or Remove Programs**.	
2.	Select **Add/ Remove Windows Components**.	

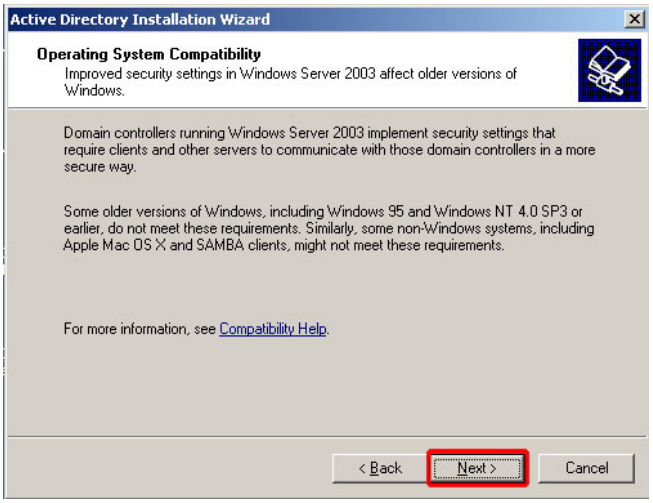
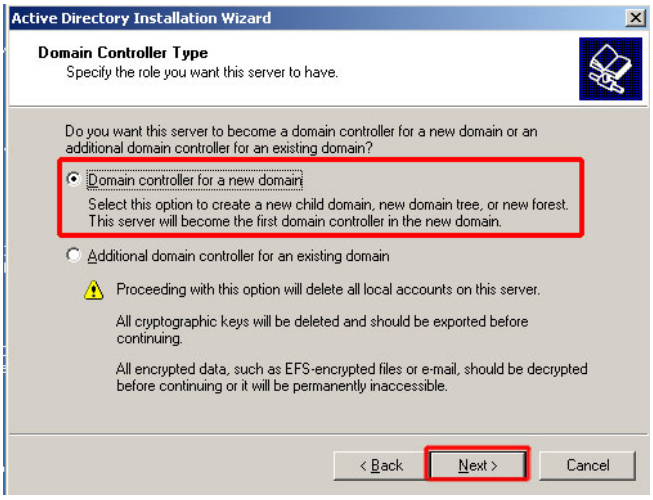
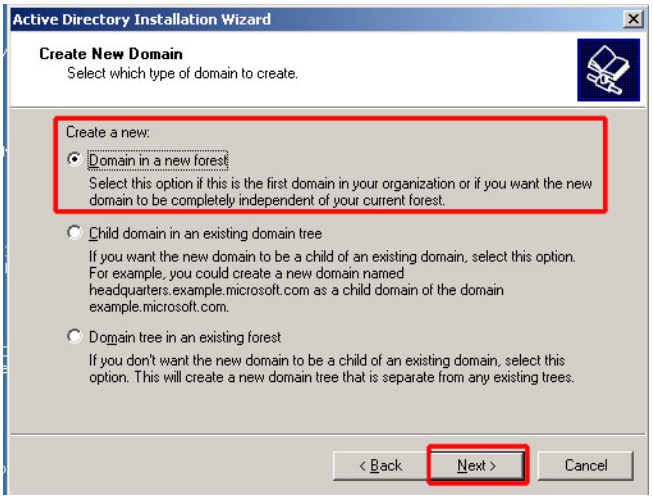
No.	Action	Comment
3.	Scroll to **Networking Services** in the selection list. Tick this component and have the details displayed by clicking **Details...**.	
4.	Make sure you have selected all subcomponents. Then click **OK**.	
5.	Click **Next>** to start the installation of the new Windows component. Follow the instructions of the installation wizard. Once the installation is complete, the IAS has been installed on your computer.	

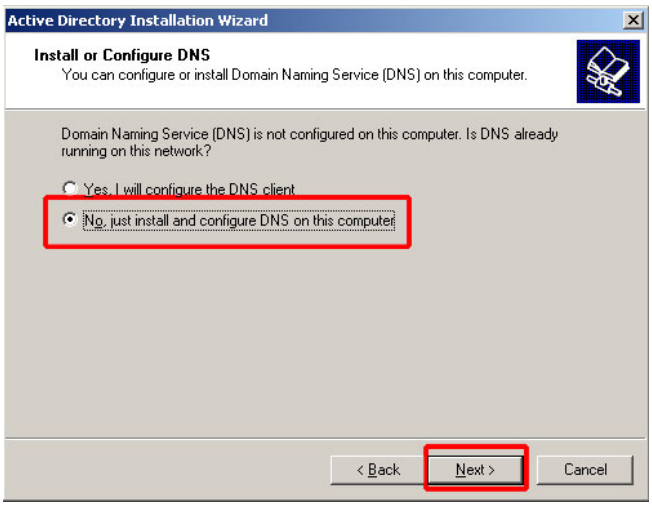
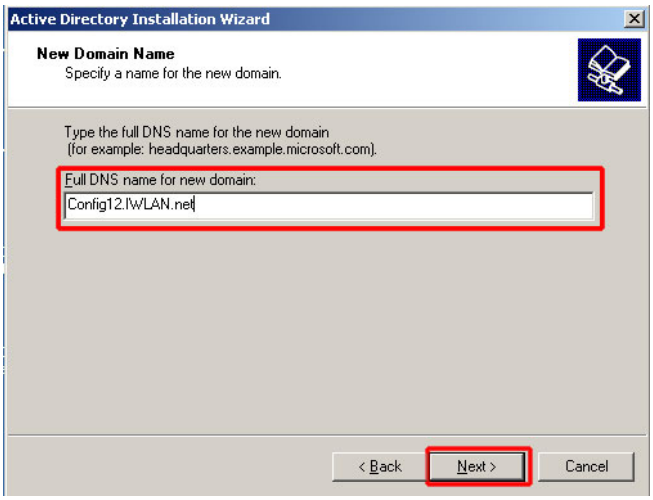
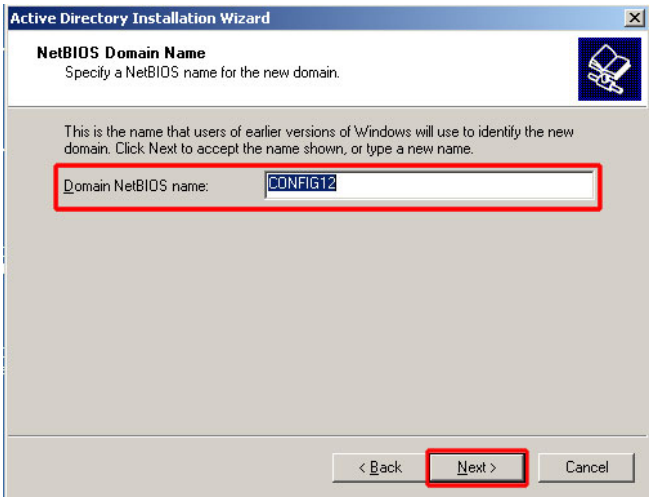
No.	Action	Comment
6.	During the installation of IAS you may be asked for the **winsctrs.dll** file.	This file is included in the installation CD, however, the file name is **WINSCTRS.DL_**. If you cannot find the file, we recommend using the Windows search via **`Start->Search->For Files or Folders`**.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

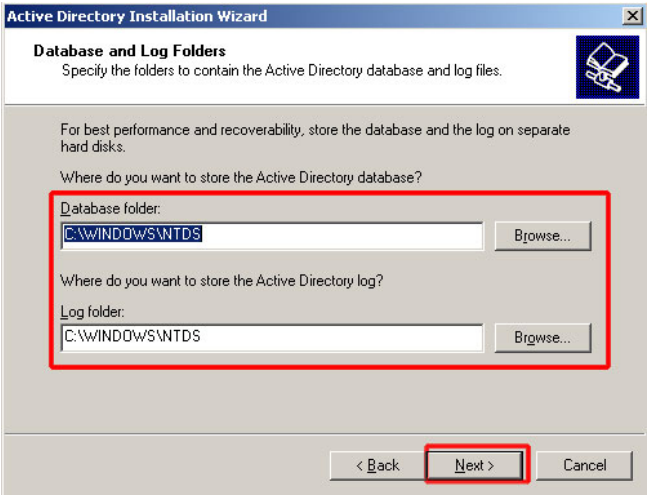
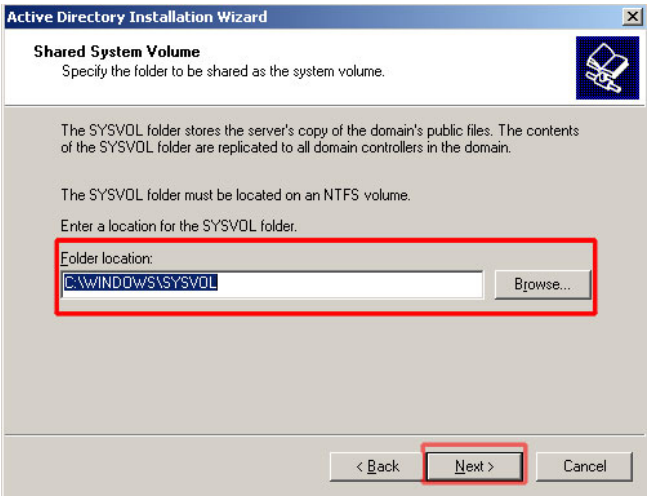
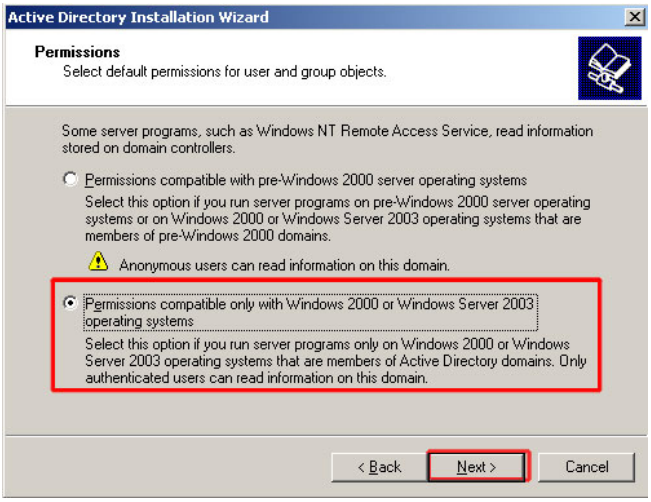
Set up an Active Directory

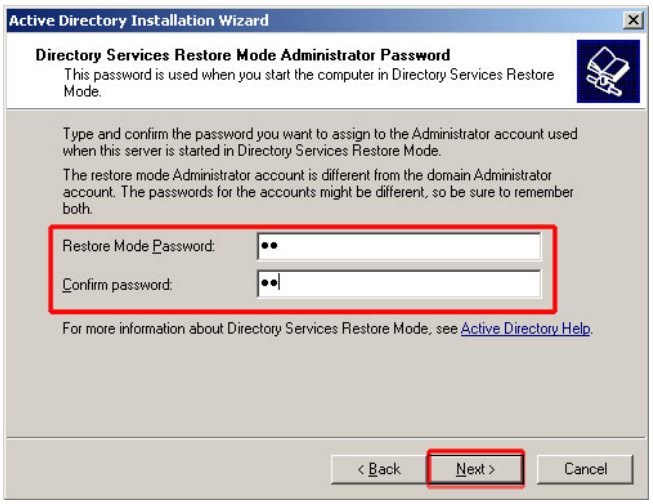
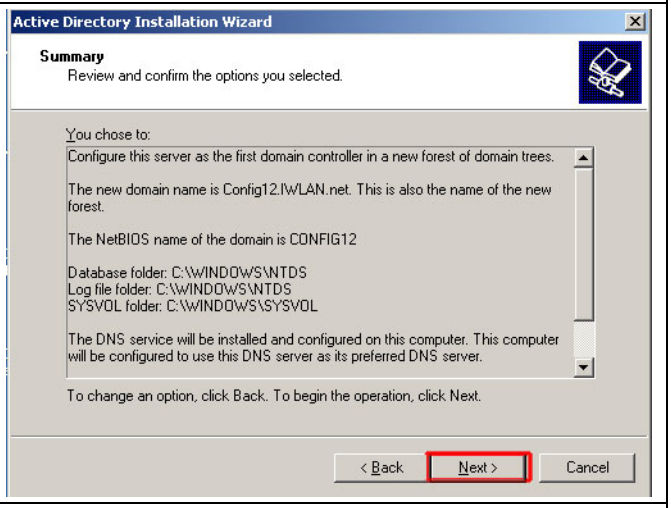
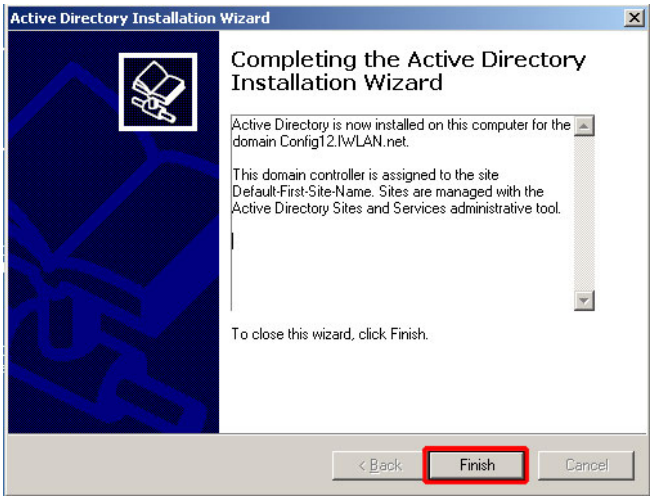
Table 5-18

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>**.	
4.	As you want to create a new domain, the server is expected to become a **domain controller** for a new domain. Click **Next>**.	
5.	Do not change the default setting when selecting the **domain type**. Confirm with **Next>**.	

No.	Action	Comment
6.	Select that the DNS server is to be installed and click **Next>**.	
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.	
8.	A name is already suggested as **NetBIOS name**. Click **Next>** to accept the name or enter a new name.	

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.	
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.	
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.	

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

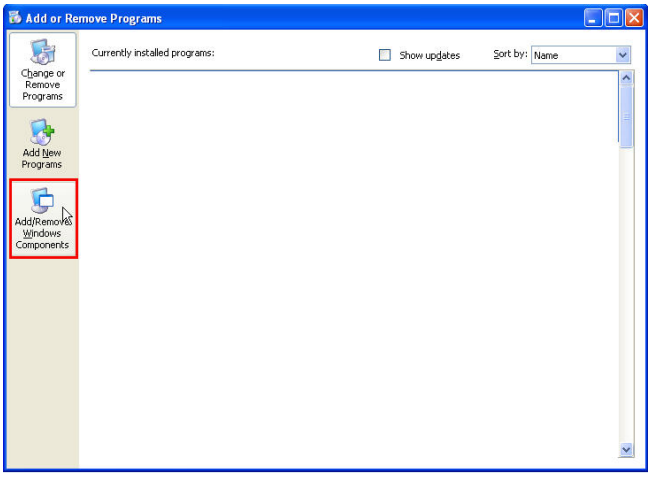
No.	Action	Comment
15.	Restart your computer to make the changes effective.	

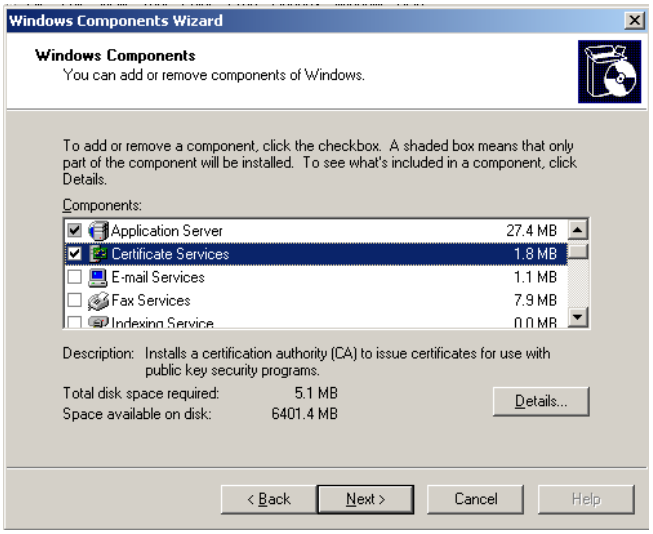
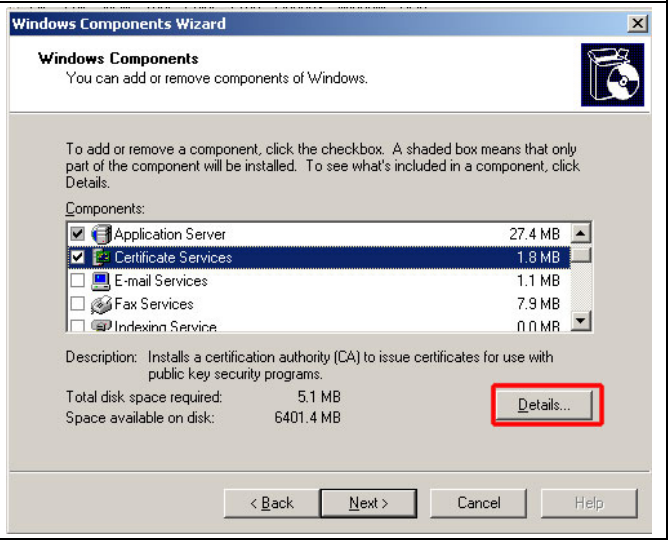
Note From now on, log on to this domain (**here**: **Config12.IWLAN.net**) when restarting your computer.

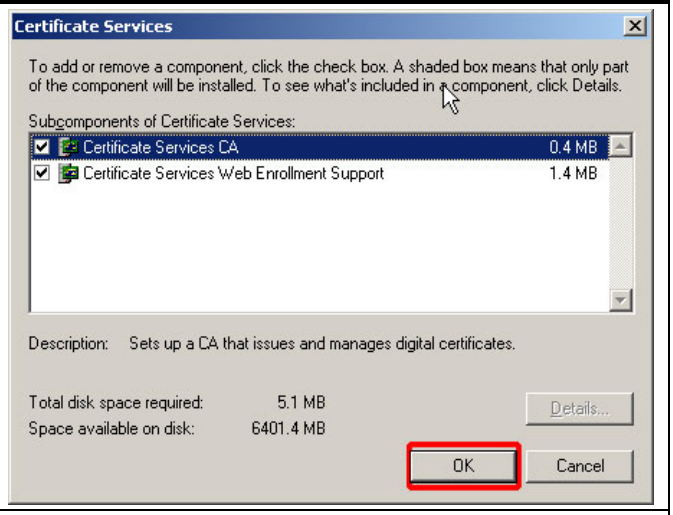
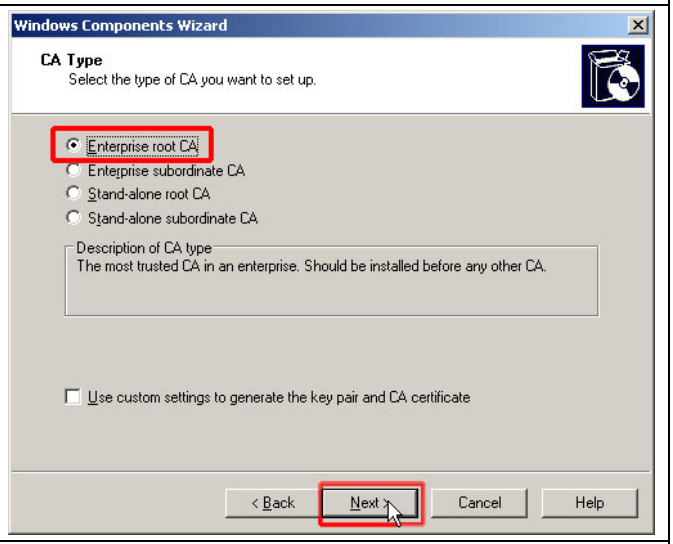
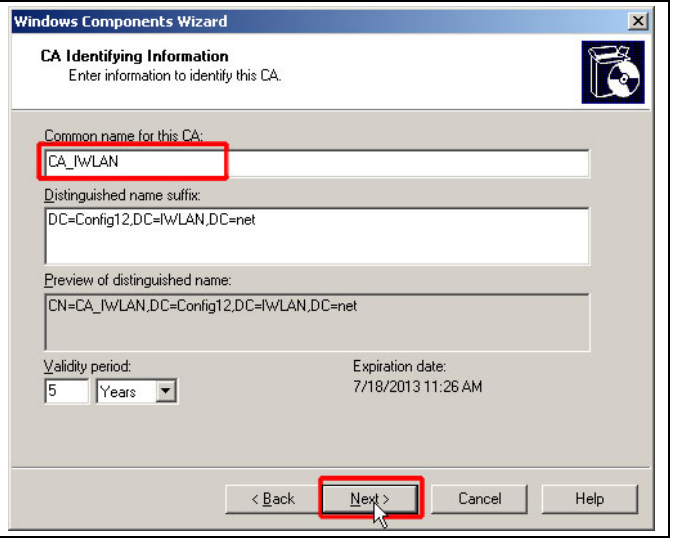
Install a certification authority

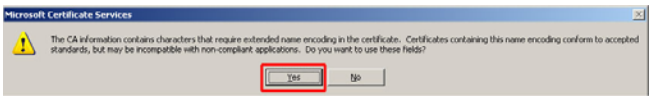
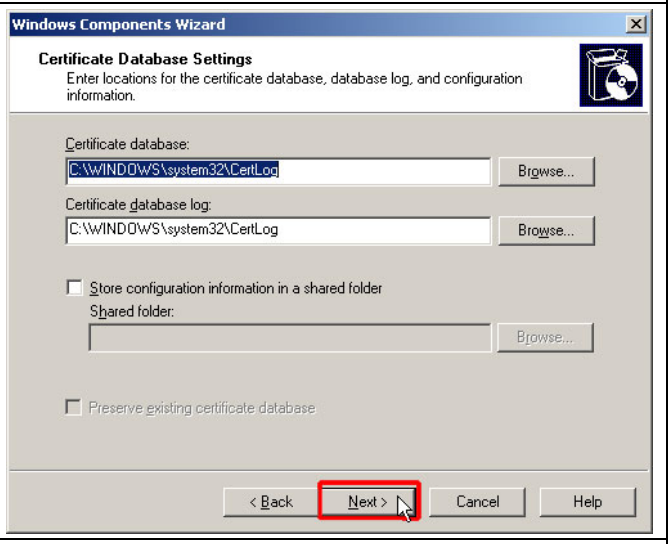
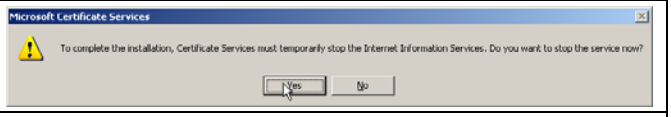
The certification authority is required to create certificates.

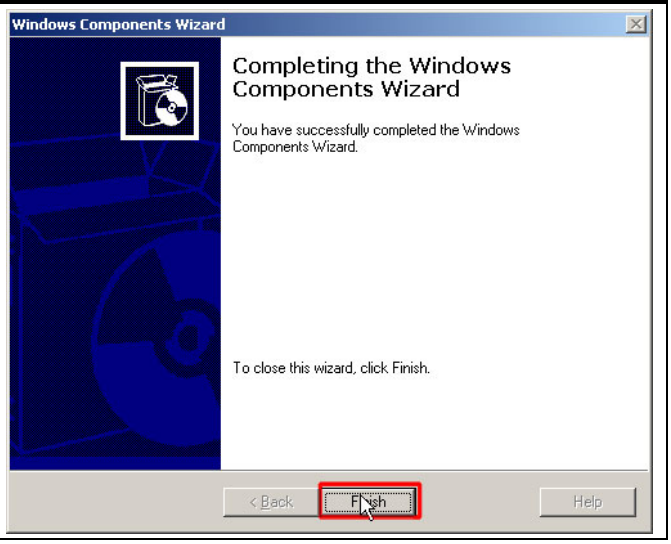
Table 5-19

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.	
4.	A warning appears. Confirm this warning with **Yes**.	
5.	Click **Details…** to have the details displayed.	

No.	Action	Comment
6.	Make sure you have selected all subcomponents. Then click **OK** to close the dialog box. Click **Next** to go to the next step.	
7.	Select **Root certification authority of the company** as a certification authority type. Click **Next** to go to the next step.	
8.	Enter a **name for the certification authority** (**here**: **CA_IWLAN**) and click **Next>** to go to the next step.	

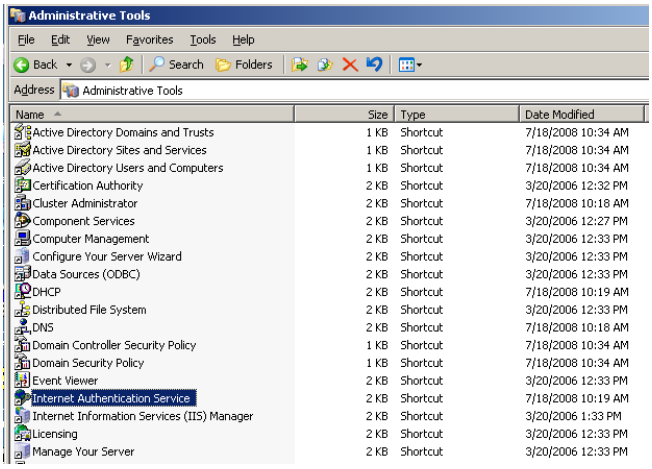
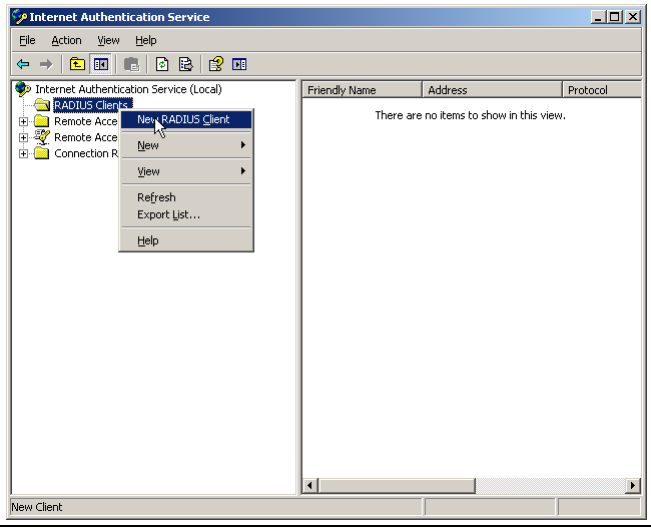
No.	Action	Comment
9.	Confirm the warning that special characters might not be compatible with **Yes**.	
10.	Enter a new path for the certification database or leave the suggested path. Click **Next>**.	
11.	Confirm the note with **Yes**. The components are configured.	
12.	During the installation of 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**.	

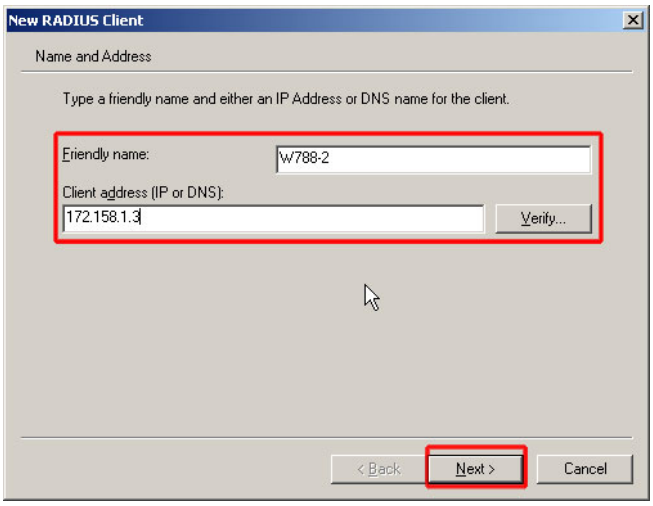
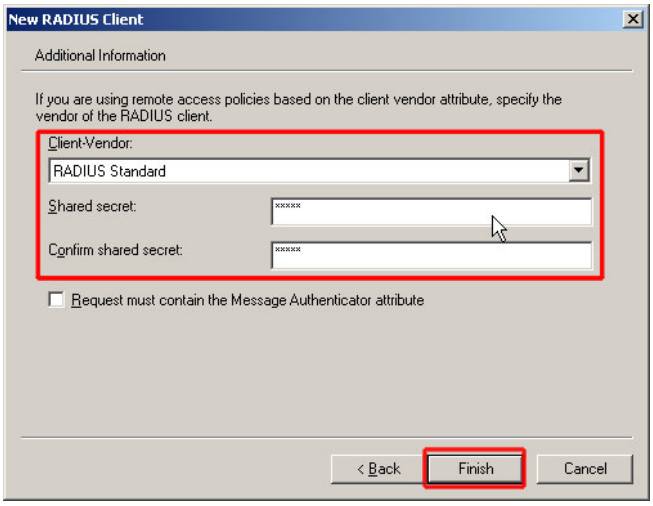
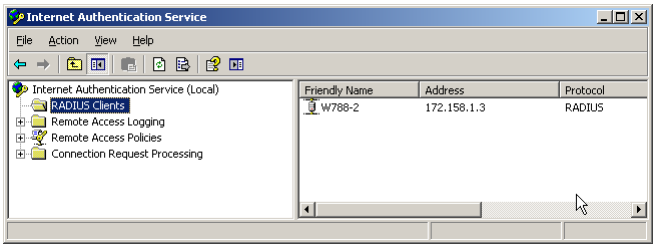
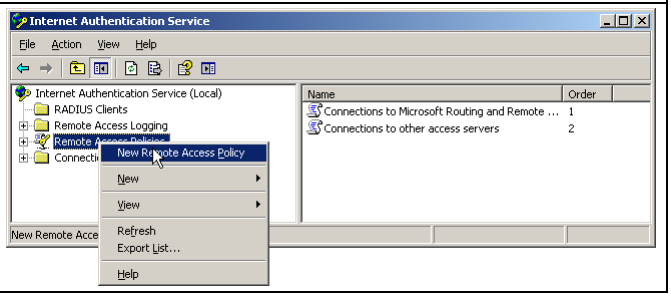
No.	Action	Comment
14.	Exit the wizard with **Finish**.	

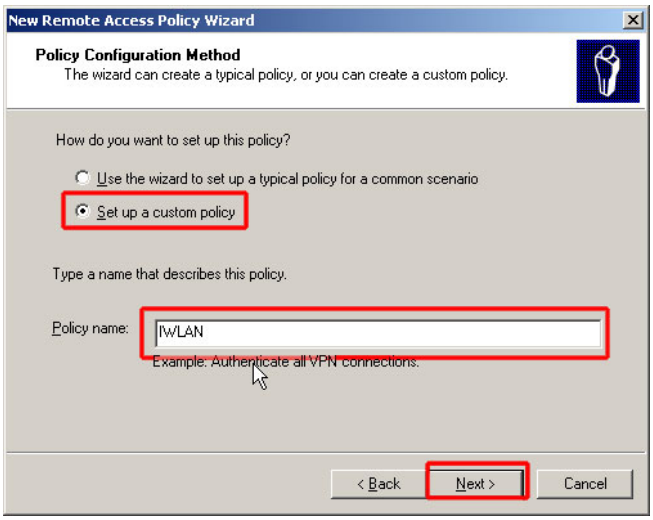
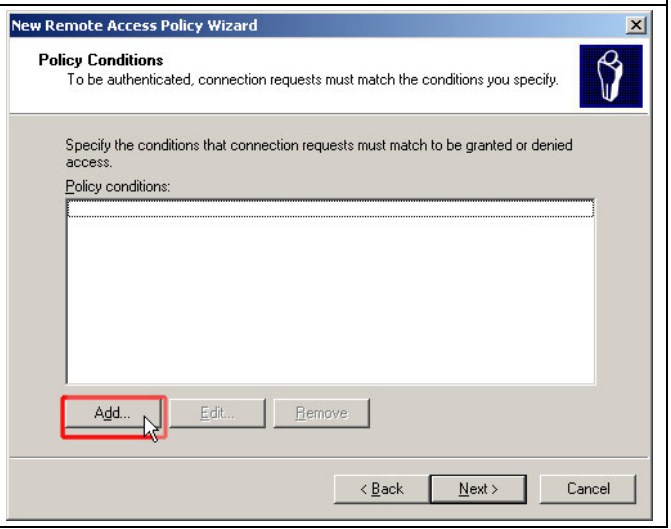
Configure the IAS

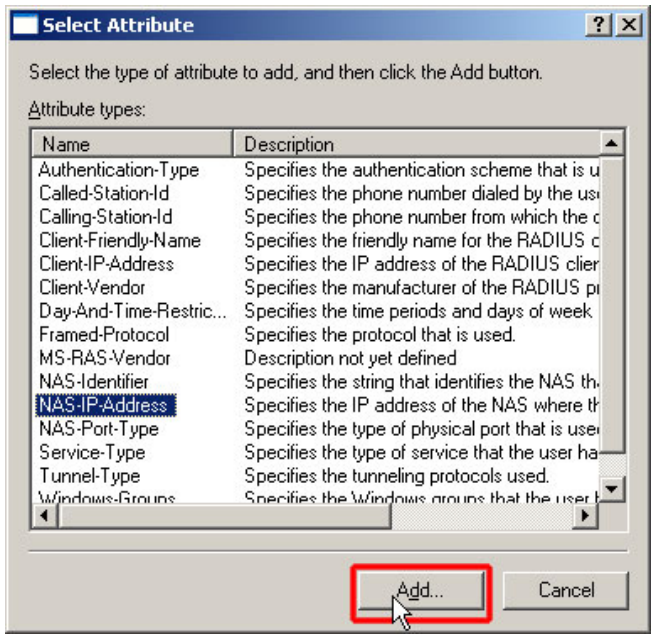
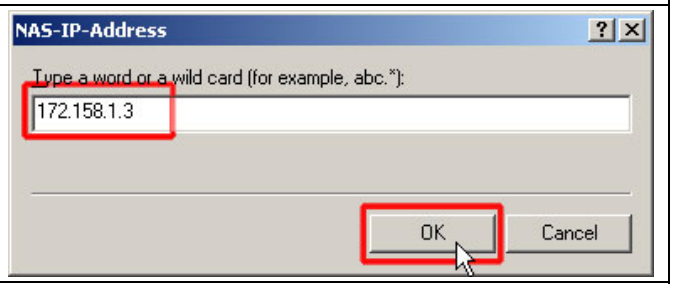
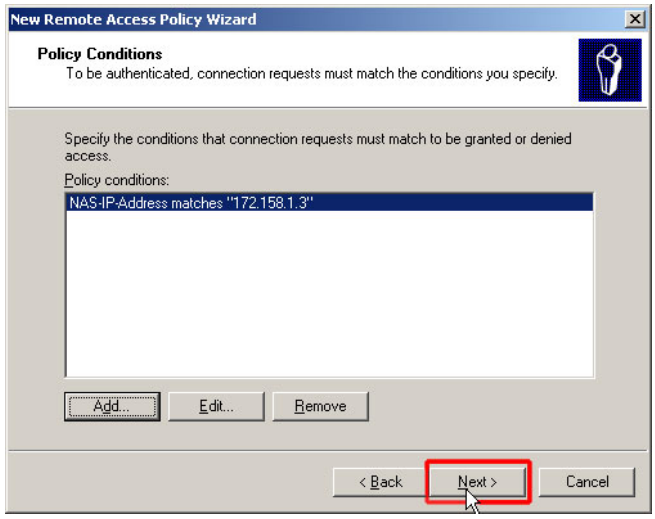
During the next steps, the Internet Authentication Service is configured in such a way that the SCALANCE W746 cannot log on to the SCALANCE W788-2 until it has authenticated itself on the IAS with the correct password.

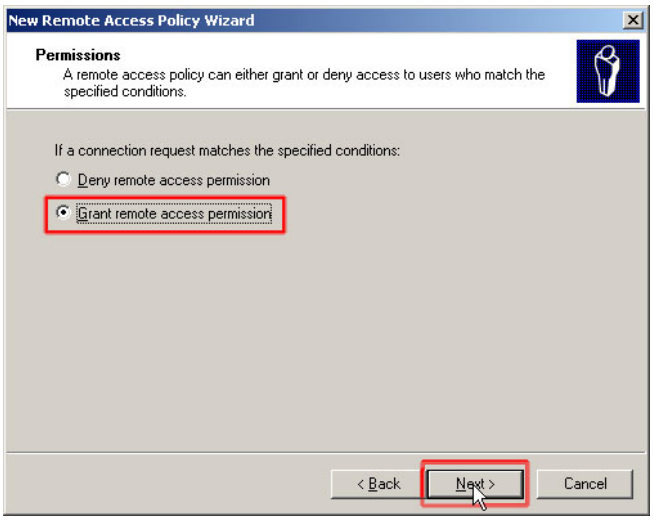
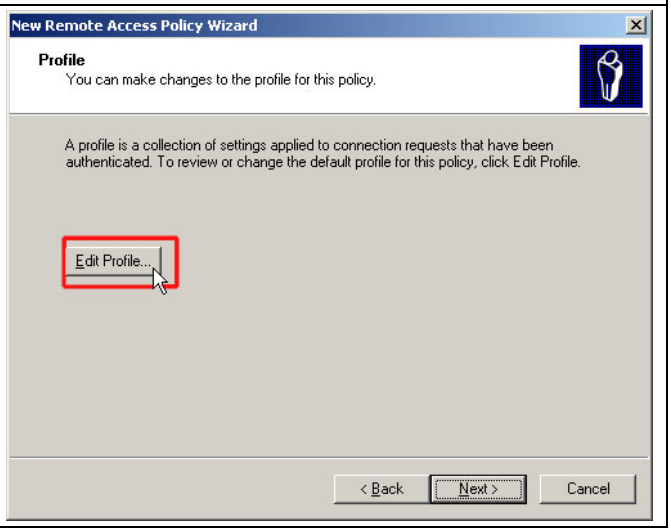
Table 5-20

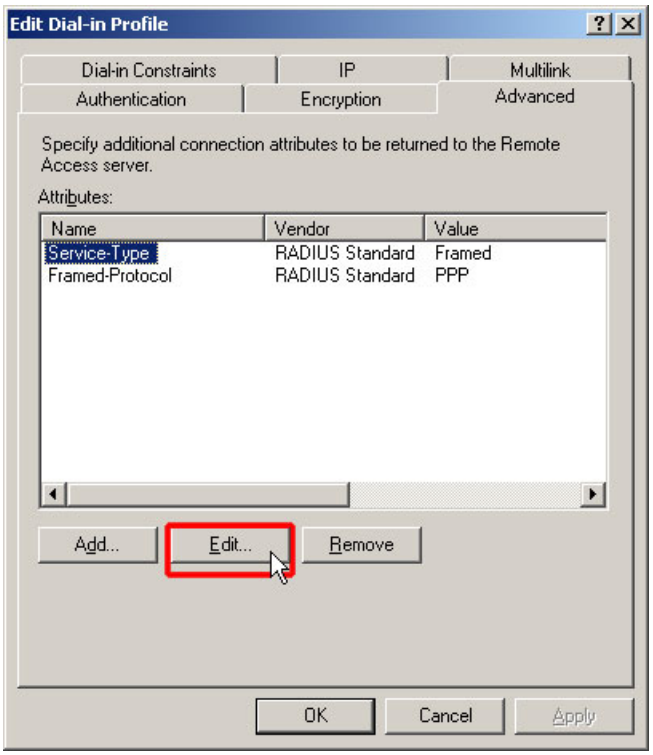
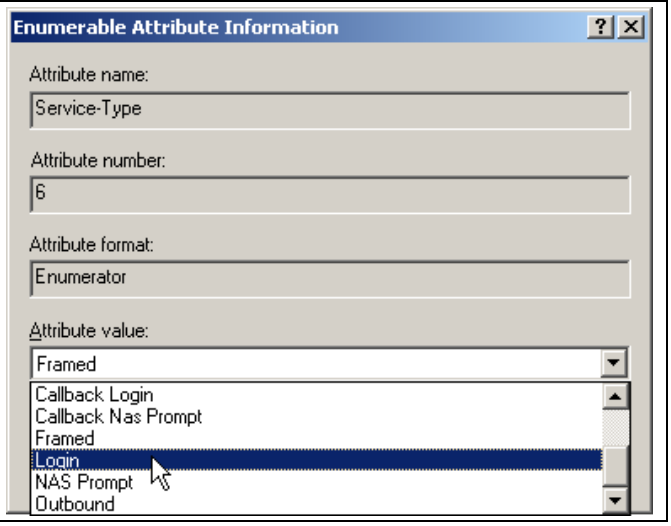
No.	Action	Comment
1.	Open the management by pressing **`Start-> Settings- >ControlPanel-> Administrative Tools`**. Double-click **Internet Authentication Service**.	
2.	A new window opens. Select **RADIUS clients** and create a new RADIUS client using the **`right mouse button -> New RADIUS client`**.	

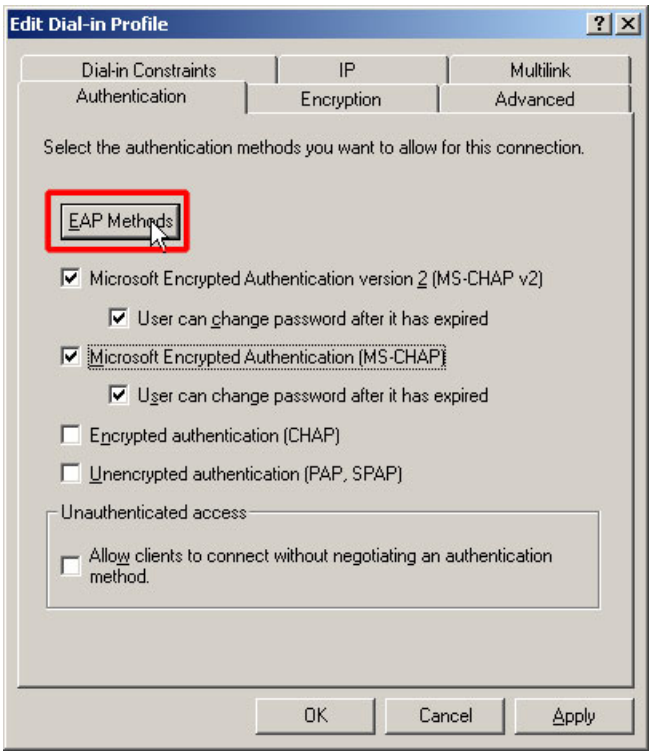
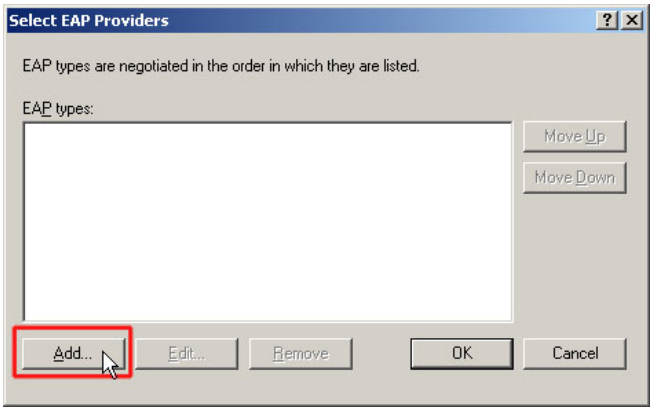
No.	Action	Comment
3.	Enter a name for the RADIUS client (**here**: **W788-2**) and the **IP address 172.158.1.3** of the SCALANCE W788-2 that functions as authenticator. Click **Next>**.	
4.	Select **RADIUS Standard** as a client manufacturer and, as a common key, enter **the key** you have assigned 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`**.	

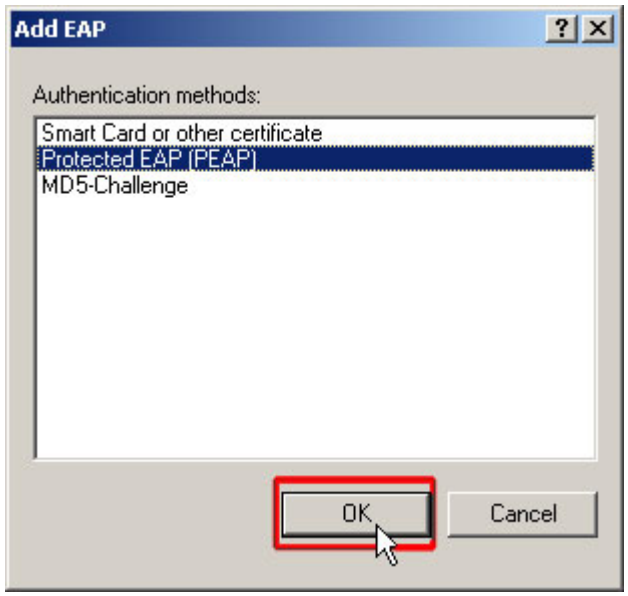
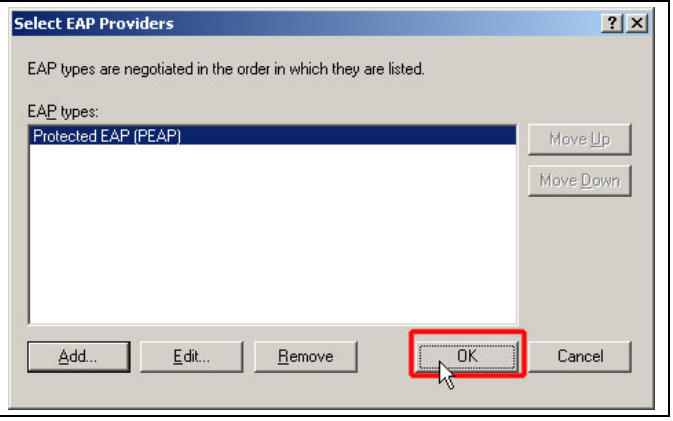
No.	Action	Comment
7.	The wizard for new RAS policies opens. In the next step, select that you want to create a **user-defined policy** and enter a **name**. Click **Next>**.	
8.	Add a new policy condition with **Add…**.	

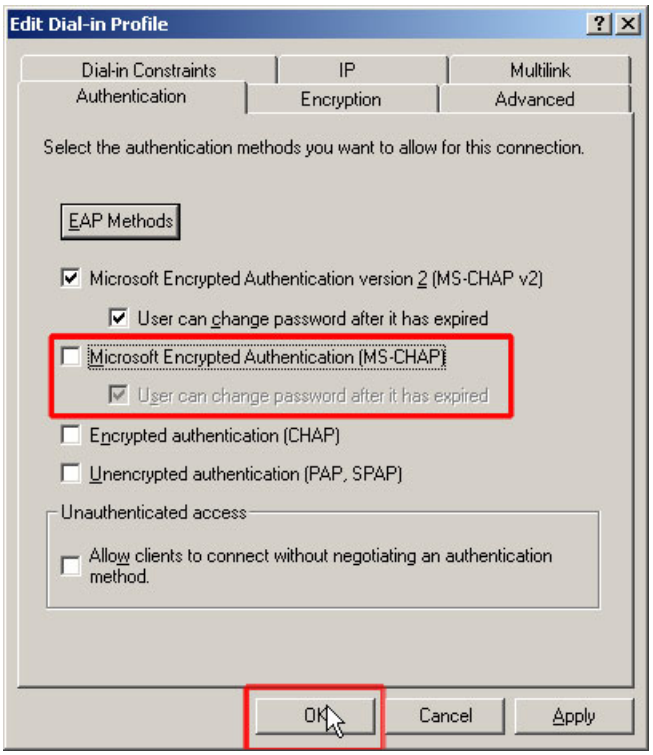
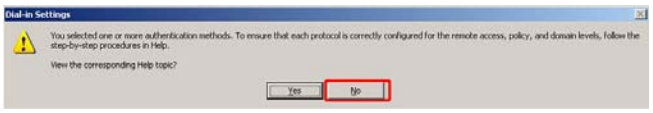
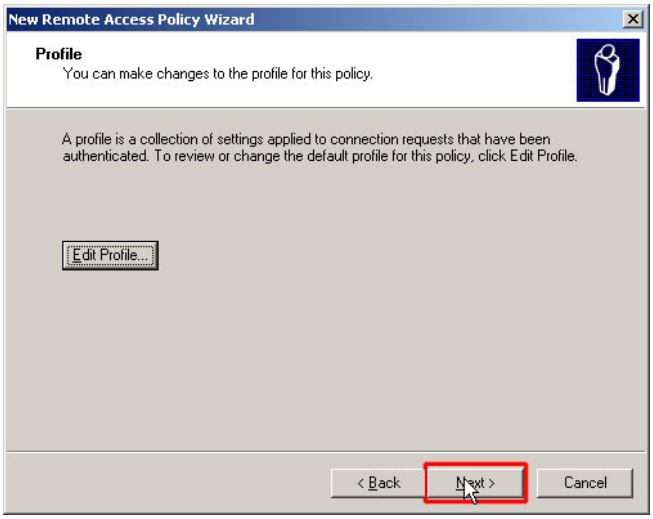
No.	Action	Comment
9.	Select **NAS IP Address** from the catalog and mark the line. Accept the attribute with **Add…**.	
10.	Enter the IP address of the SCALANCE W788-2 (**172.158.1.3**) and confirm with **OK**.	
11.	The policy has been created. Click **Next>**.	

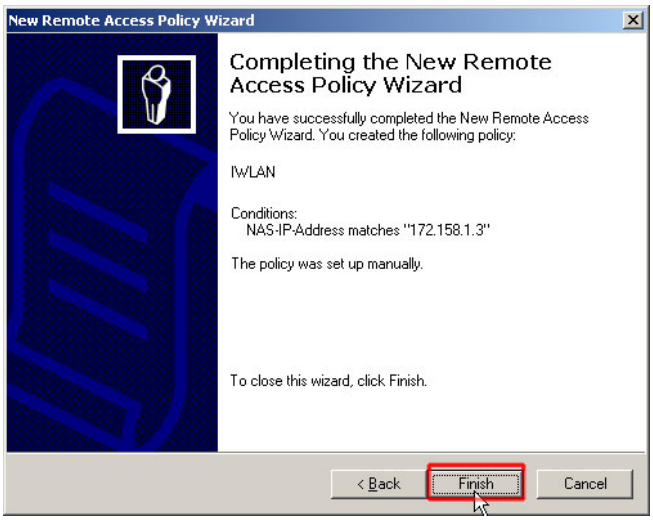
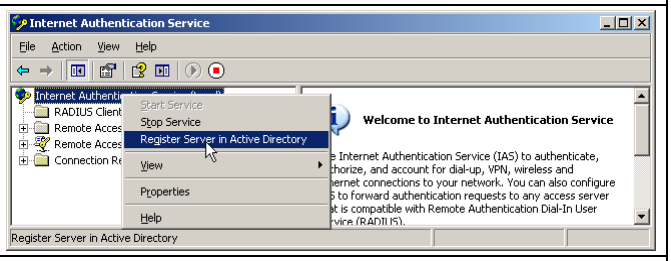
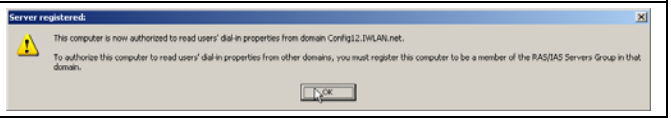
No.	Action	Comment
12.	If a query corresponds to this policy, **access is to be granted**. Click **Next** to go to the next step.	
13.	Click **Profile** to go to the policy settings.	

No.	Action	Comment
14.	Change to the **Advanced** tab. Select **Service Type** and click **Edit**.	
15.	Select **Login** as an attribute value and confirm with **OK**.	

No.	Action	Comment
16.	Change to the **Authentication** tab**.** Click **EAP Methods**.	
17.	Add new EAP types with **Add...**.	

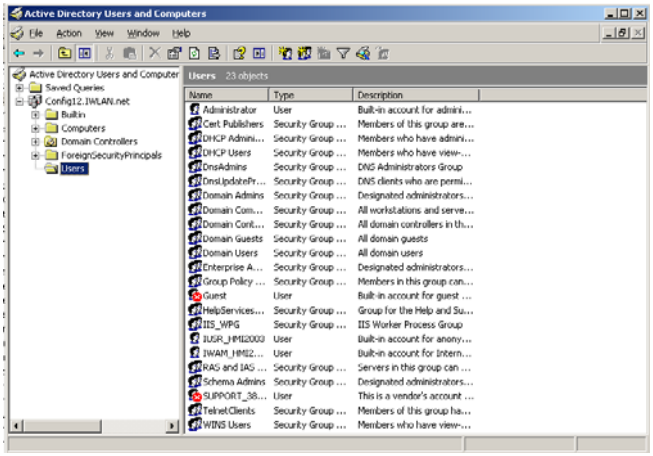
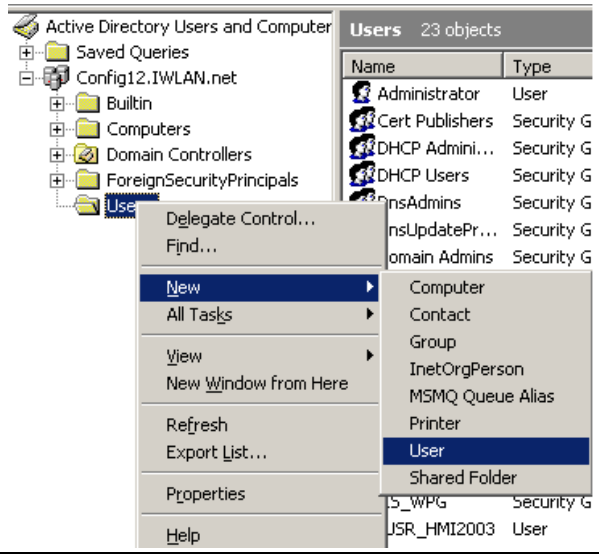
No.	Action	Comment
18.	Select **Protected EAP (PEAP)** as an authentication method. Click **OK** to accept the settings.	
19.	The authentication method has been included in the list. Close the dialog box with **OK**.	

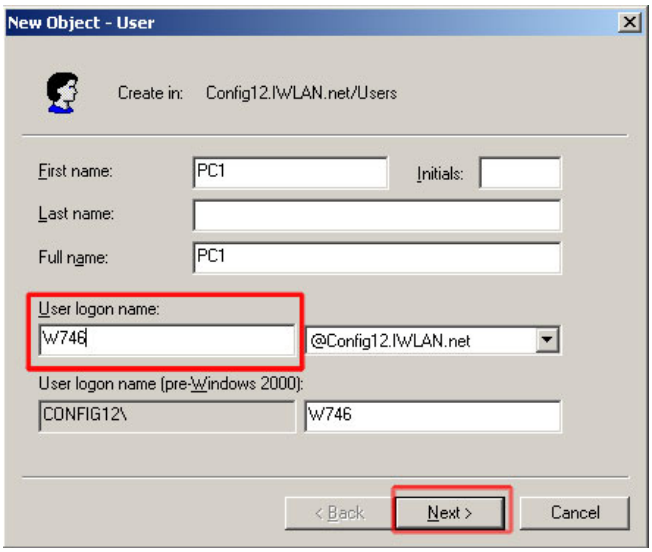
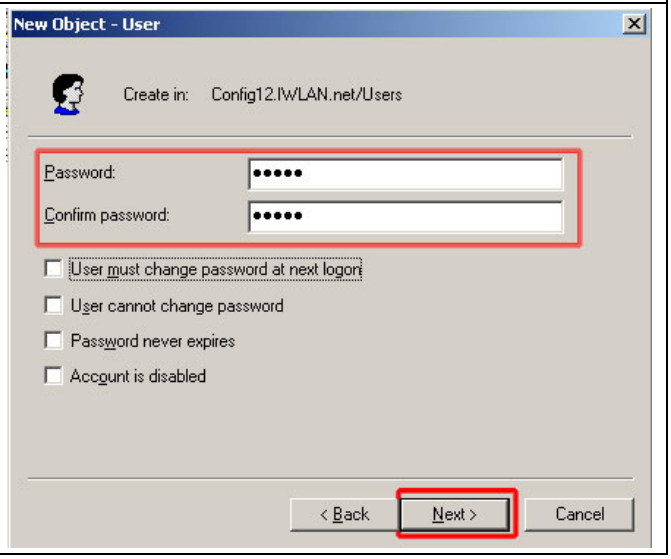
No.	Action	Comment
20.	Deactivate the **MS-CHAP** and close the dialog box with **OK**.	
21.	You are asked whether you want to view help on the authentication topic. Click **No**.	
22.	Click **Next>**.	

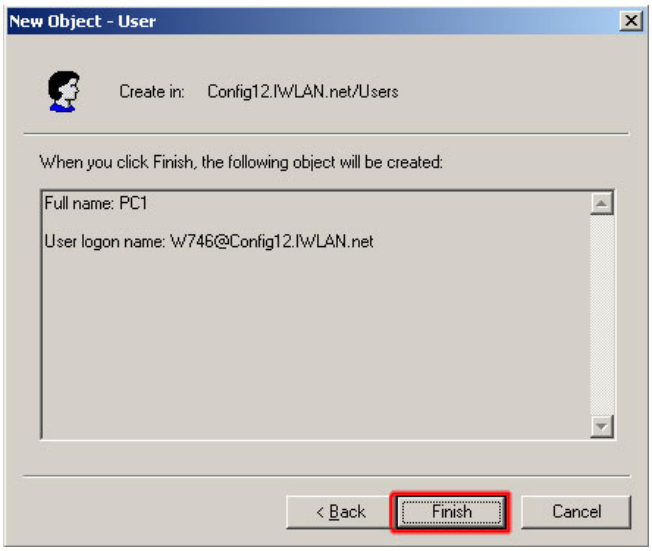
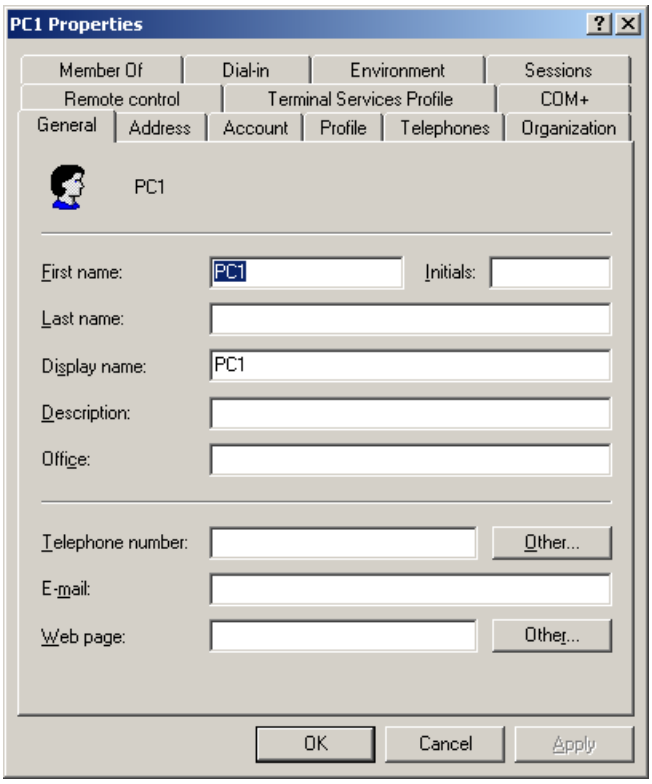
No.	Action	Comment
23.	Close the wizard with **Finish**.	
24.	Select the Internet Authentication Service and register it using the **`right mouse button -> Register Server in Active Directory`**.	
25.	Confirm the following note with **OK**.	
26.	Confirm the following note with **OK**.	

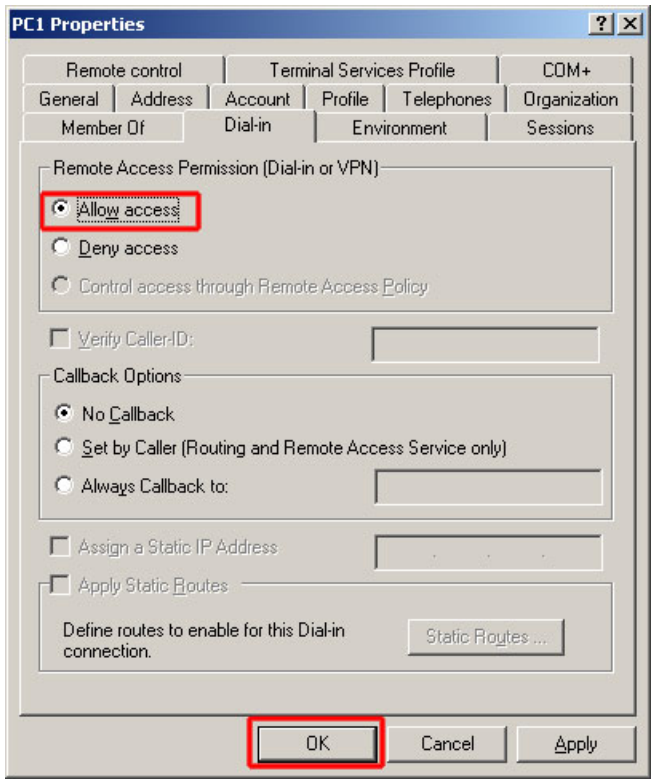
Create a user

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.	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>**.	
5.	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>**.	

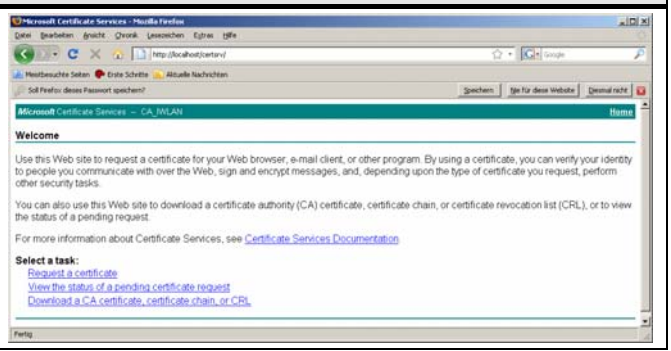
No.	Action	Comment
6.	Complete the creation of a new user with **Finish**.	
7.	Select the newly created user in the user list and double-click. The **Properties** dialog box opens.	

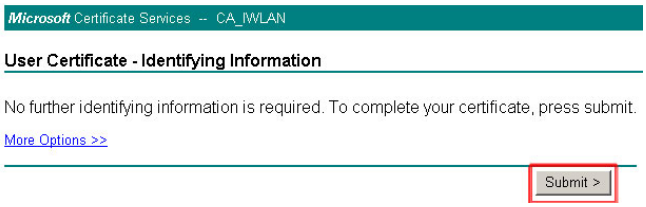
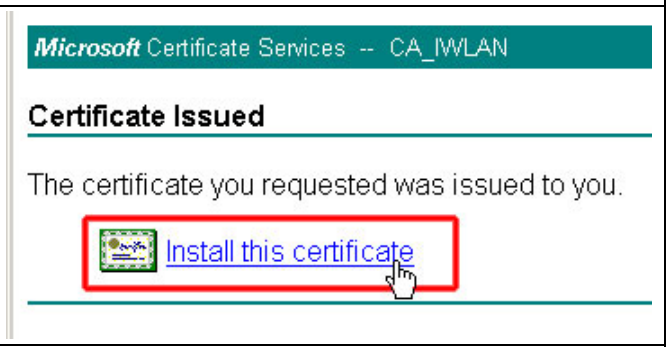
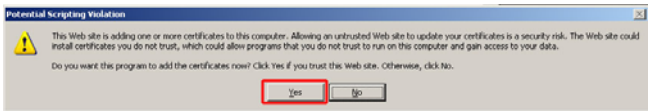
No.	Action	Comment
8.	Change to the **Dial-In** tab. Enable the access for this user. Close the dialog box with **OK**.	

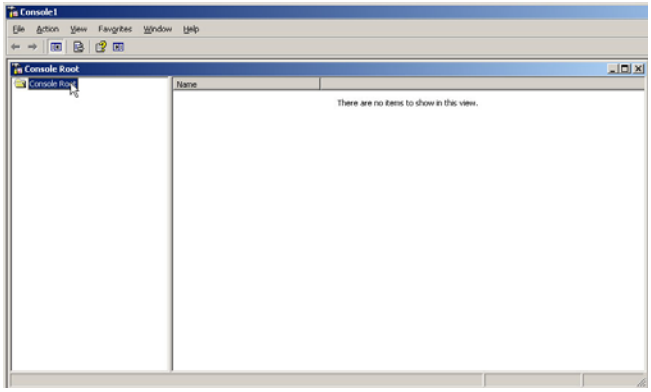
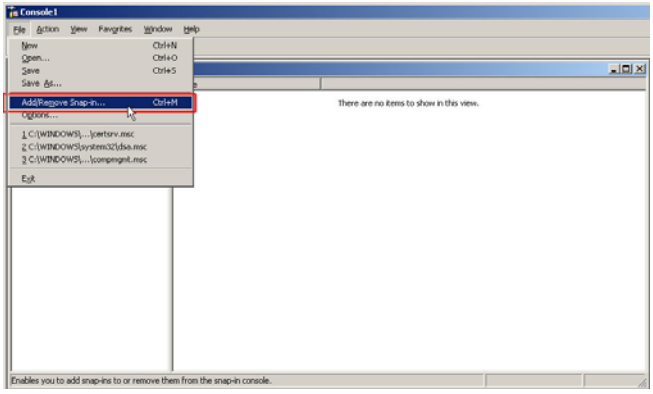
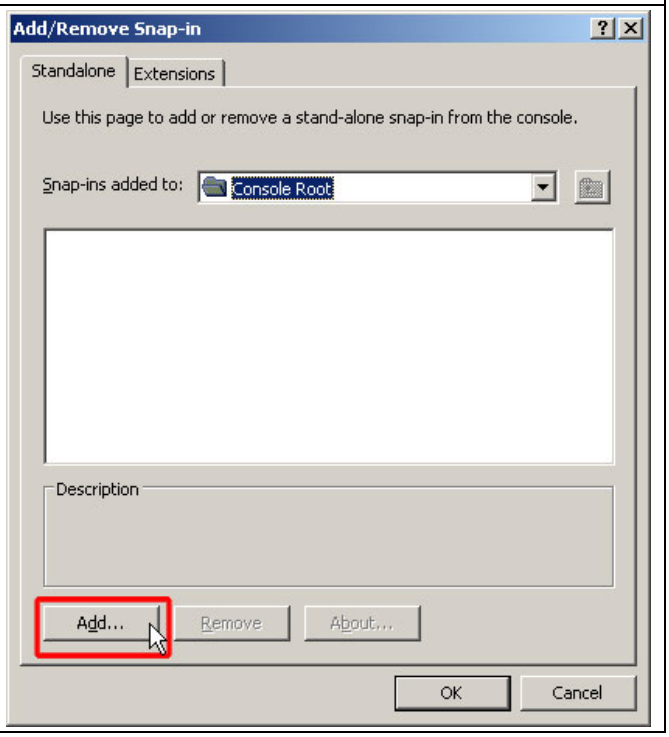
Create certificates

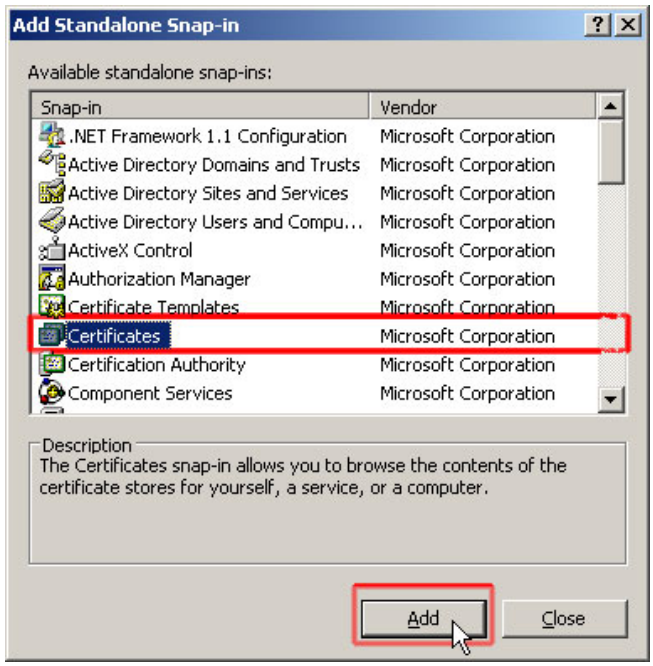
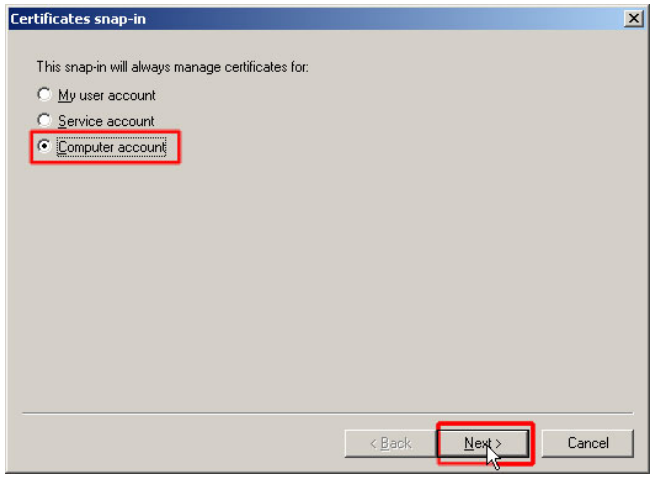
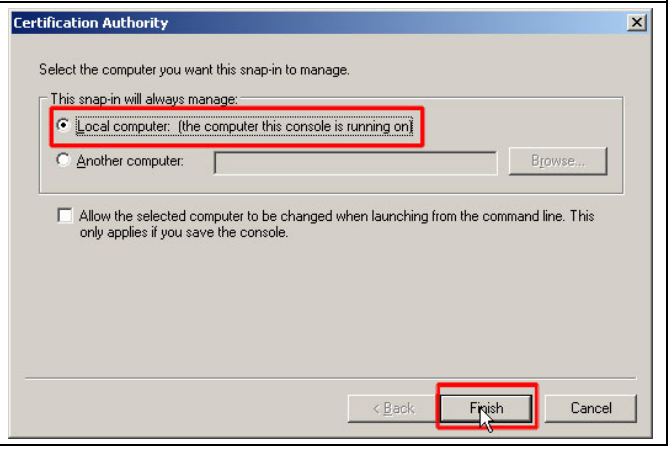
The certificates are used to authenticate the RADIUS server and the client. The certificates are stored on a page in the file system of the Win2003 server and are also loaded to the SCALANCE W746-1 configuration.

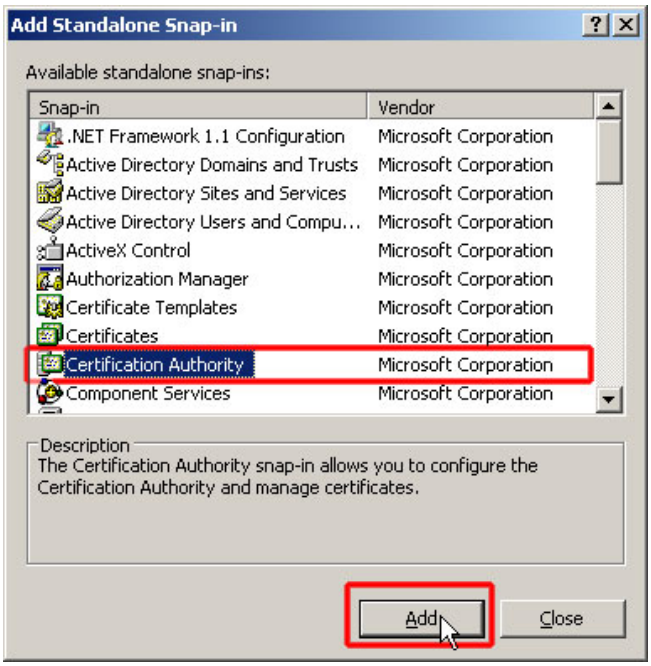
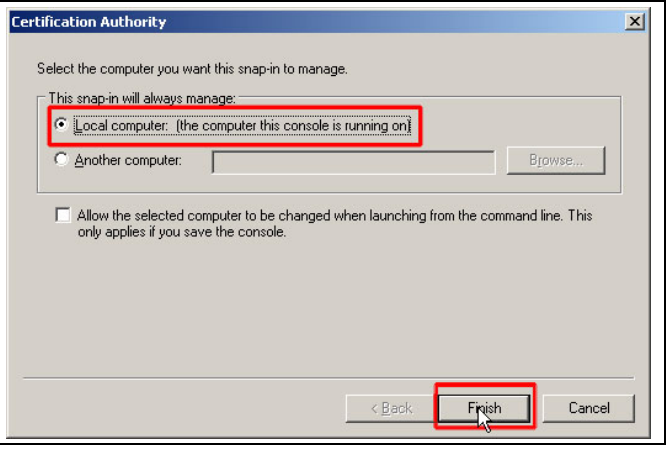
Table 5-22

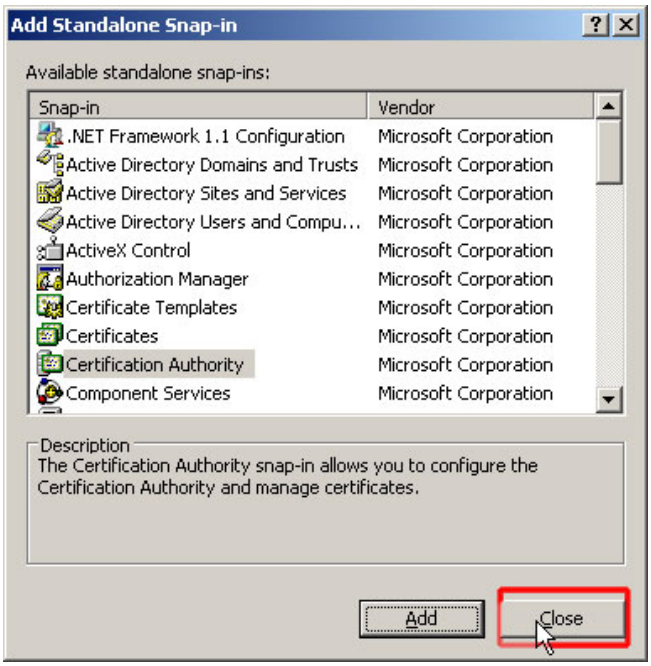
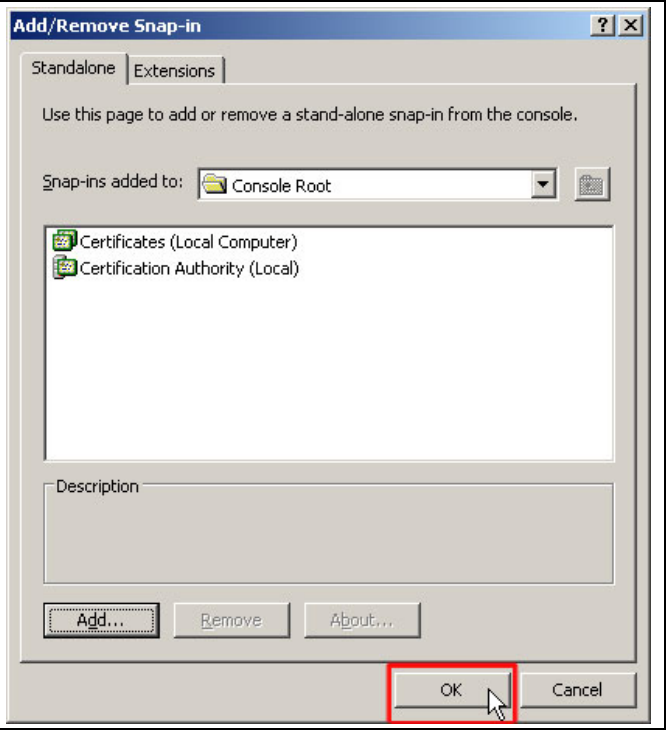
No.	Action	Comment
1.	Open a web browser and enter http://localhost/certsrv into the address field. Click **Request a certificate**.	

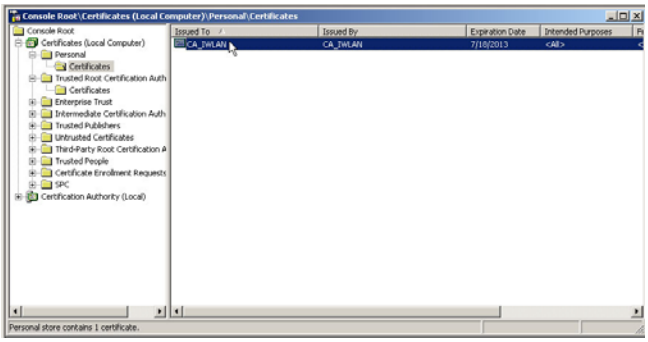
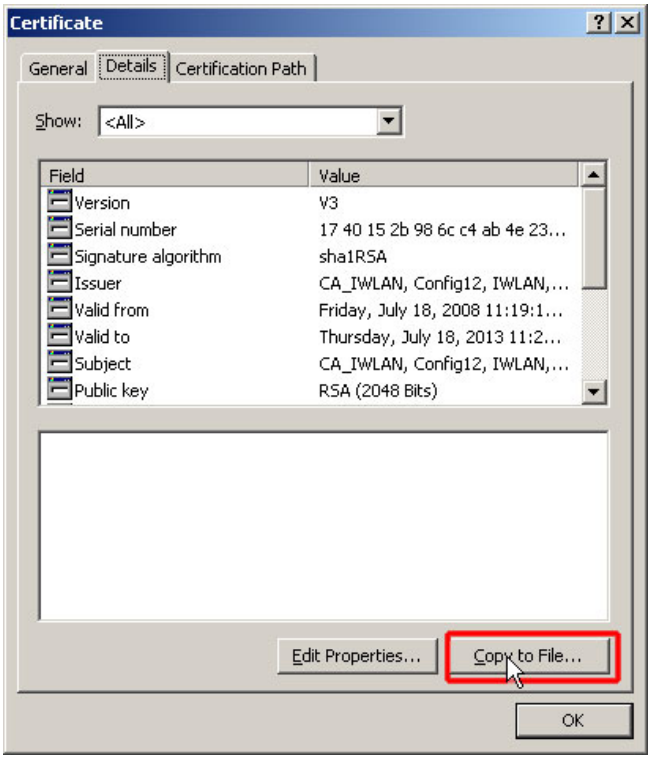
No.	Action	Comment
2.	Click **User Certificate**.	
3.	Click **Submit**.	
4.	Confirm the warning that a new certificate has been requested with **Yes**.	
5.	Click **Install this certificate**.	
6.	Confirm the warning that a new certificate is installed on your computer with **Yes**.	
7.	A new certificate 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**.	

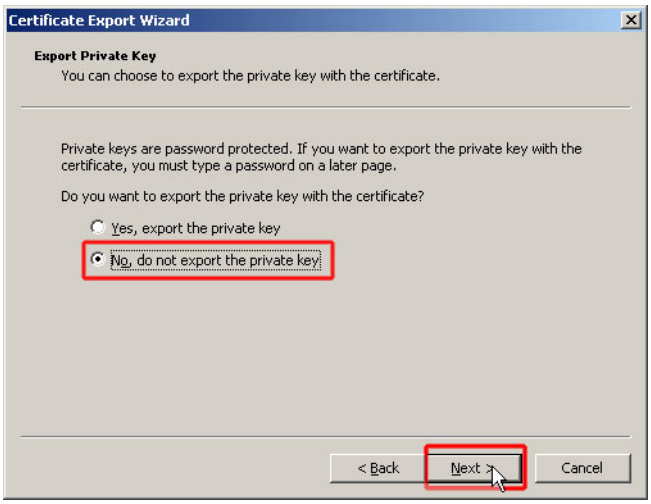
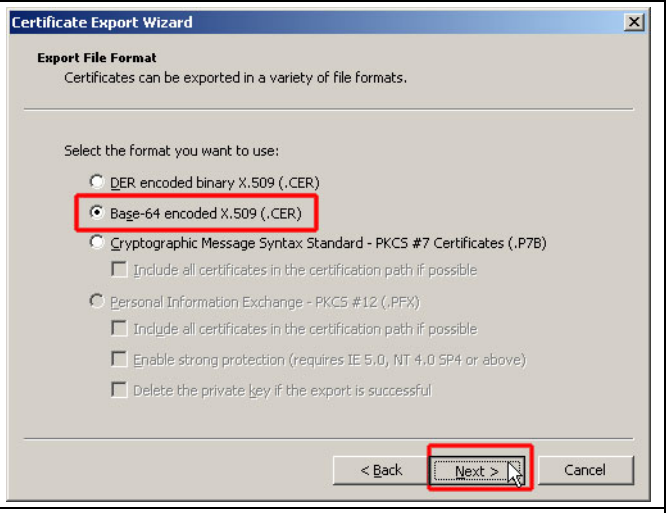
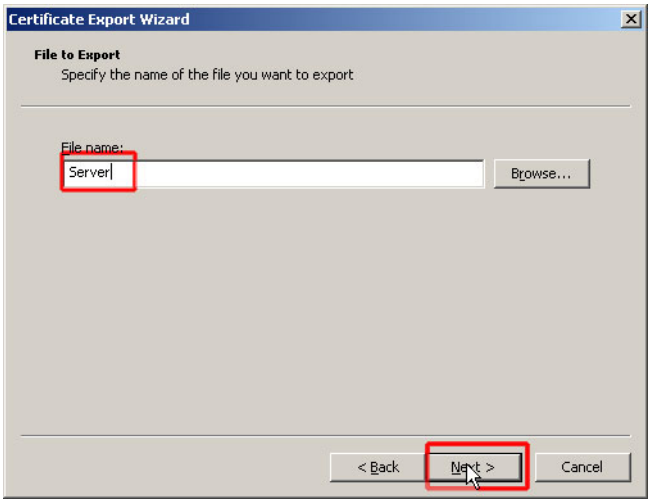
No.	Action	Comment
9.	A new console window opens.	
10.	Select the **Console Root** folder and add new attributes using **`File->Add/Remove Snap In...`**.	
11.	A new dialog box opens. Click **Add...**.	

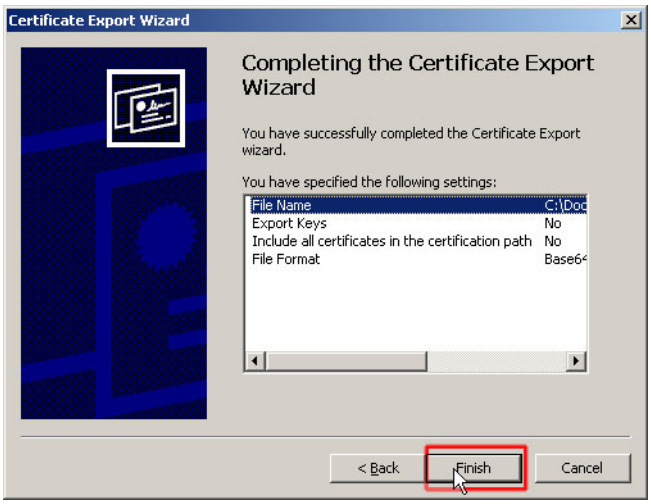
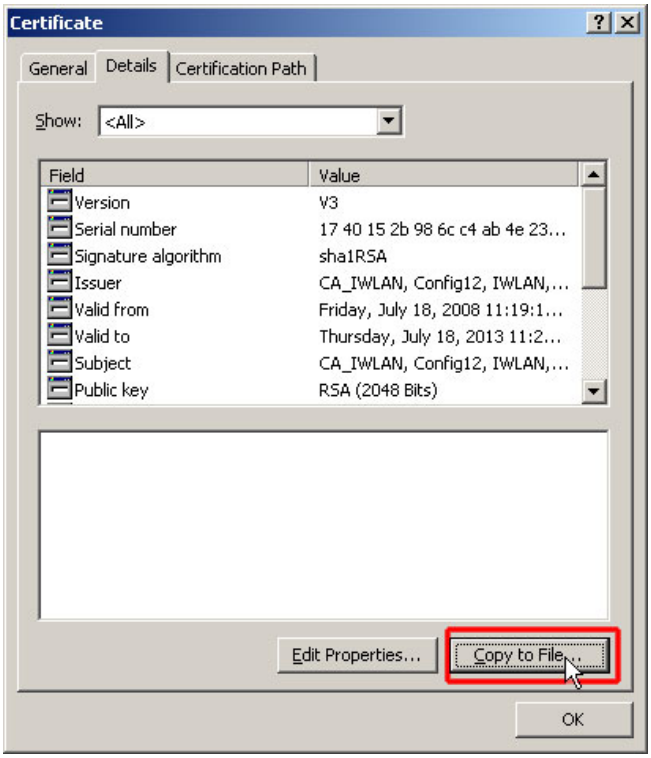
No.	Action	Comment
12.	Select **Certificates** from the list and click **Add**.	
13.	To view the certificates of the computer, select **Computer account**. Click **Next>**.	
14.	Select the **local computer** and close the dialog box with **Finish**.	

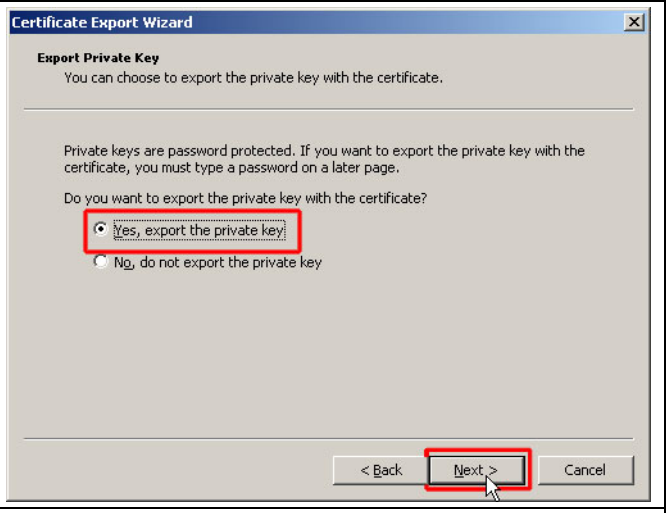
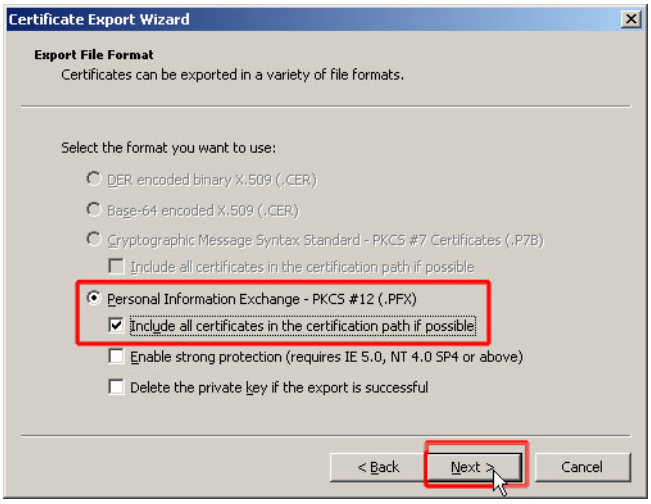
No.	Action	Comment
15.	The list with the possible snap-ins is displayed again. Select **Certification Authority** and click **Add**.	
16.	Select the **local computer** and close the dialog box with **Finish**.	

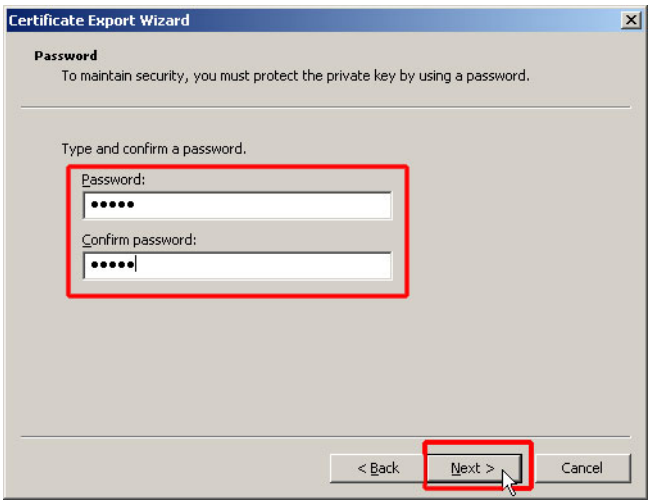
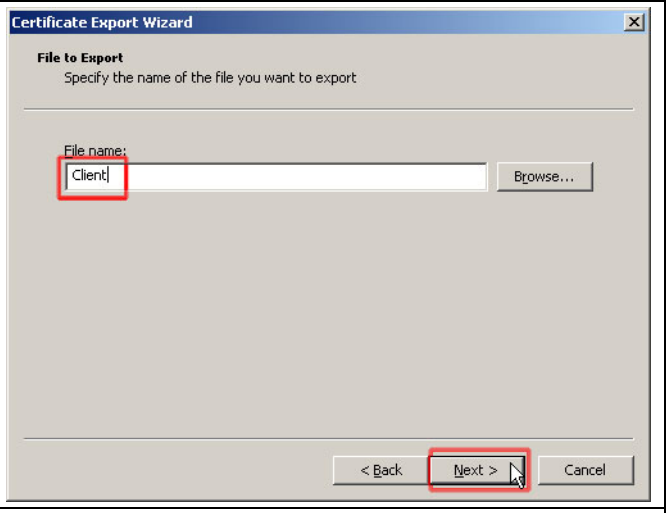
No.	Action	Comment
17.	Close the list with the snap-ins that are available with **Close**.	
18.	Close the dialog box with **OK**.	

No.	Action	Comment
19.	Select the newly created certificate of the **CA_IWLAN** certification authority under **`Certificates-> Personal-> Certificates`** and double-click.	
20.	The certificate properties appear. Change to the **Details** tab. A server certificate is exported first. Click **Copy to File**.	
21.	The Certificate Export Wizard opens. Click **Next** to go to the next step.	

No.	Action	Comment
22.	The private key is not to be exported. Tick the appropriate box. Click **Next>**.	
23.	The certificate is to be **Base-64 encoded**. Click **Next** to go to the next step.	
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>**.	

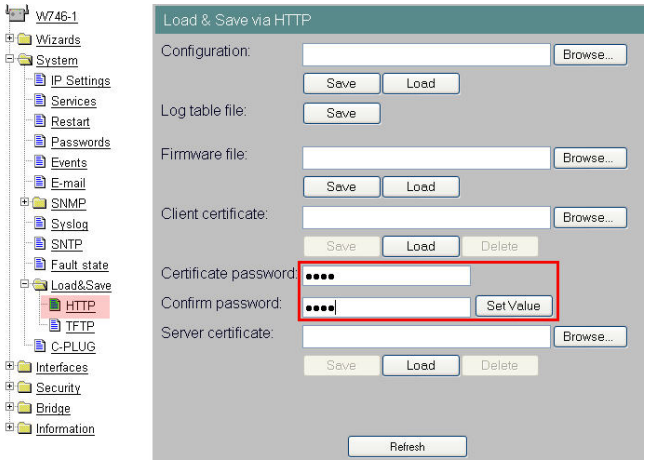
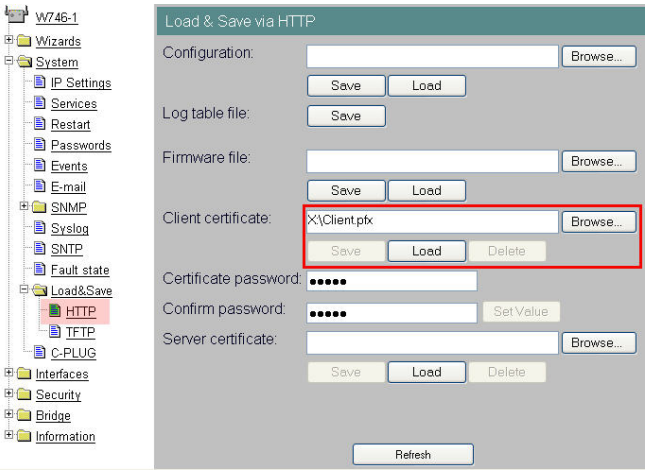
No.	Action	Comment
25.	Exit the Certificate Export Wizard with **Finish**. The path under which the certificate has been stored is displayed under **File Name**.	
26.	Then the certificate is downloaded for the client. Click **Copy to File** again.	

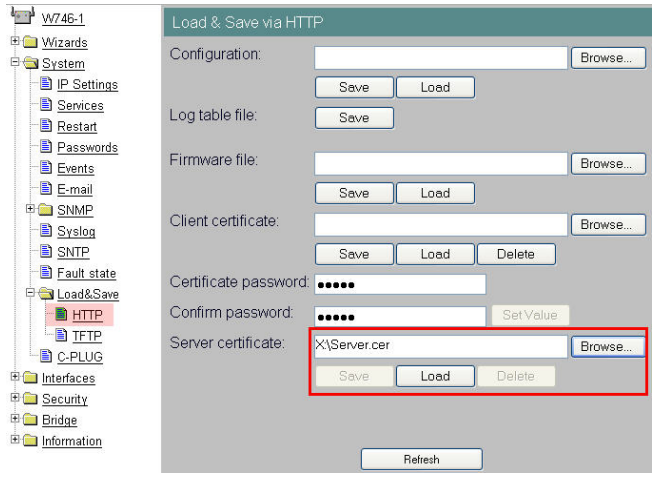
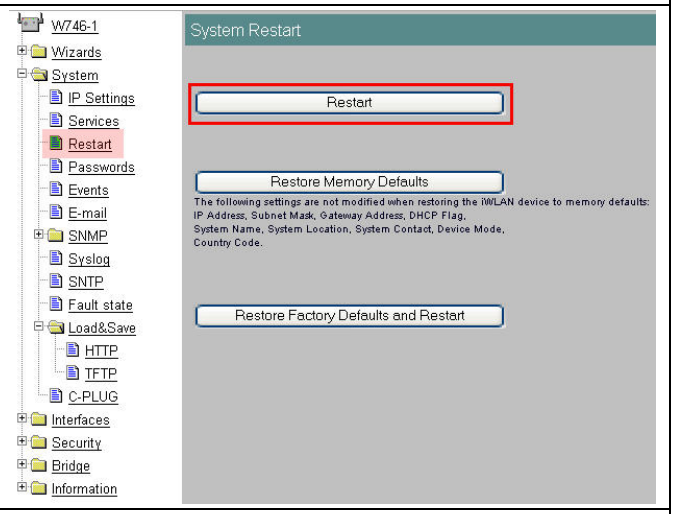
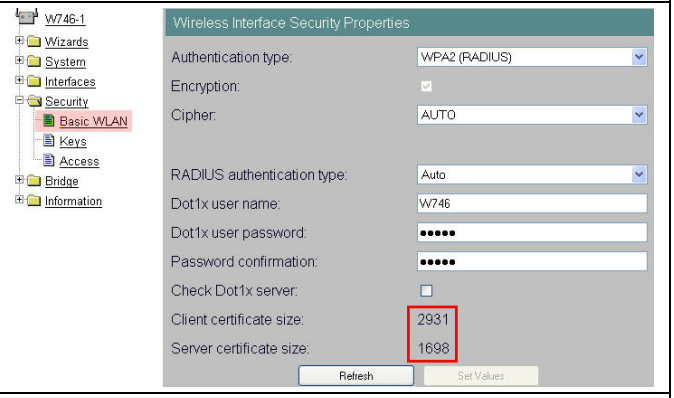
No.	Action	Comment
27.	The Certificate Export Wizard opens again. Click **Next** to go to the next step.	
28.	You can now select whether the private key is to be exported as well. Click **Next>**.	
29.	Only one format is allowed for the export file. Activate the first checkbox and deactivate the checkbox in the middle. Click **Next** to go to the next step.	

No.	Action	Comment
30.	Enter the password to be used to protect the private key. (Here: **W746**) **Note**: Note this password because it will be required for uploading the certificates to the SCALANCE W746-1.	
31.	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>**.	
32.	Close the Certificate Export Wizard with **Finish**. The path under which the certificate has been stored is displayed under **File Name**.	
33.	Close the certificate properties with **OK**.	

Load certificates to W746-1

Table 5-23

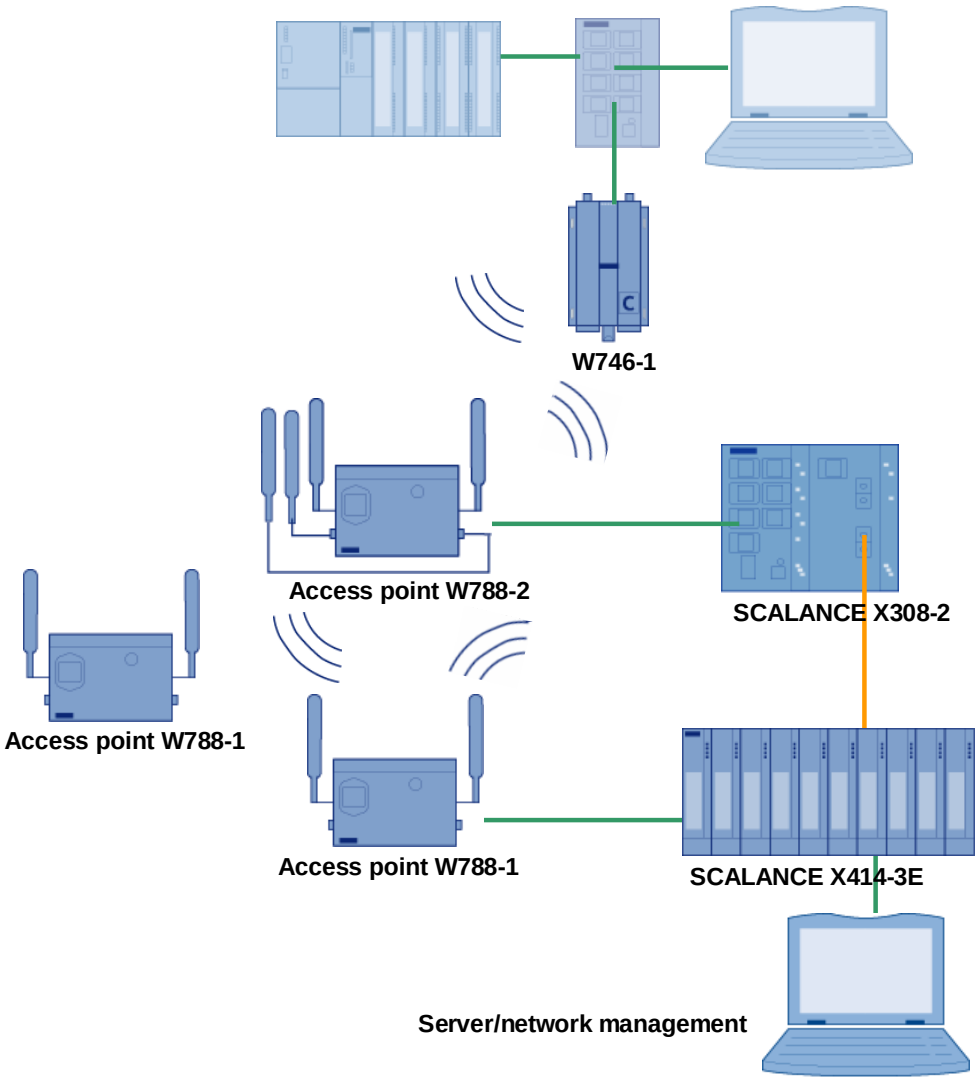
No.	Action	Comment
1.	Connect the server PC to the SCALANCE X108.	
2.	Open the web-based management for the SCALANCE W746-1 and log on.	http://172.158.1.8
3.	Navigate to **System-> Load&Save->http**. Enter the password you have assigned for the private key (Table 5-22 line 30) (Here: **W746**). Click **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.

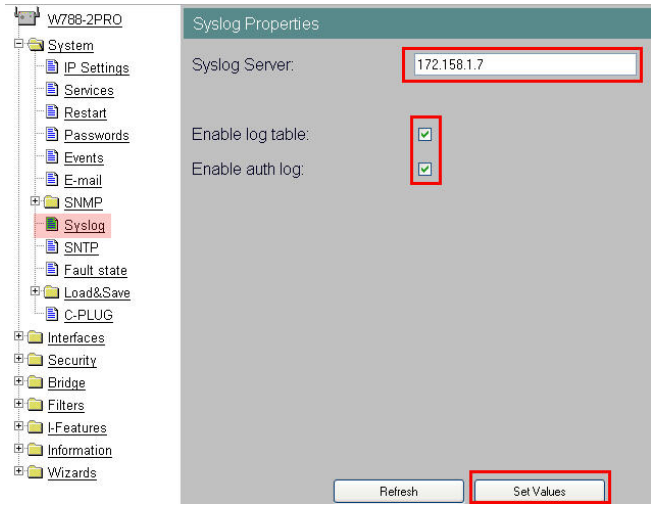
Figure 5-6



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.

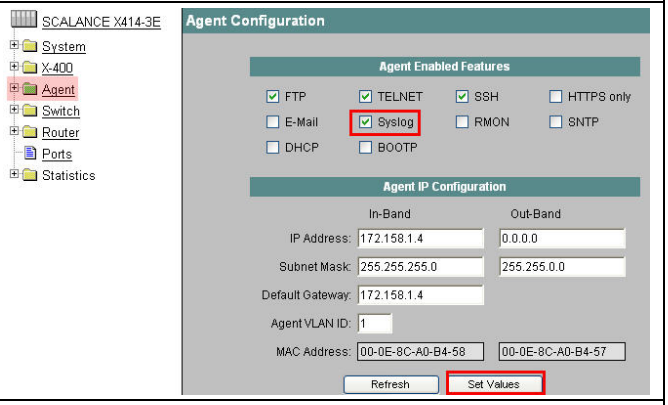
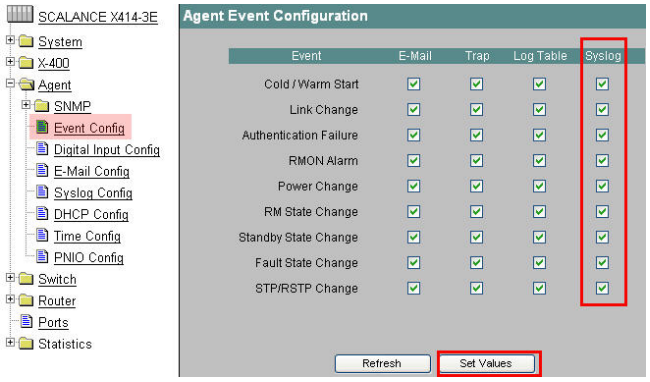
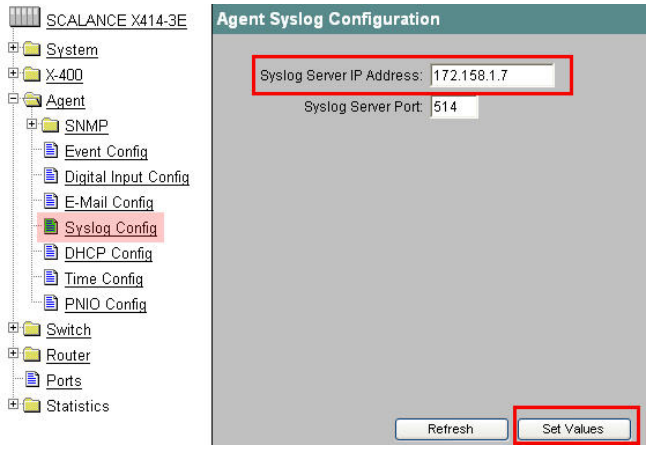
Table 5-24

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.

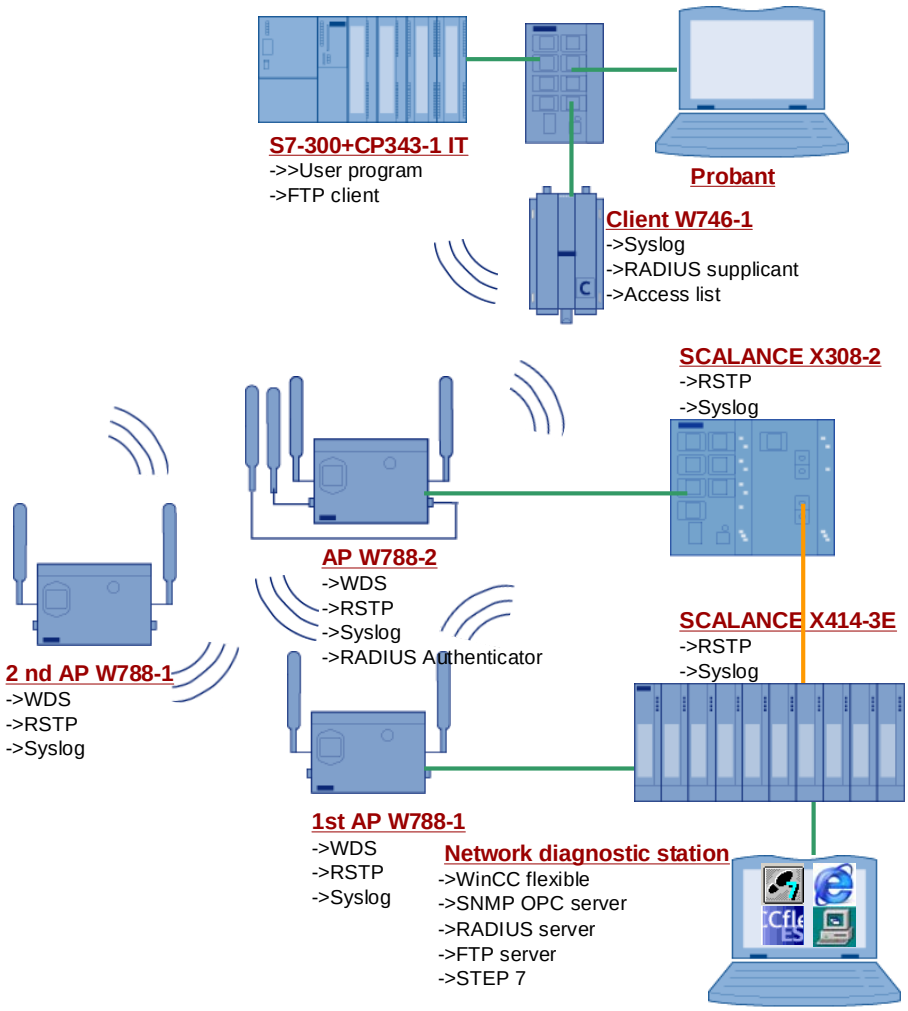
Configuring the Syslog server

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



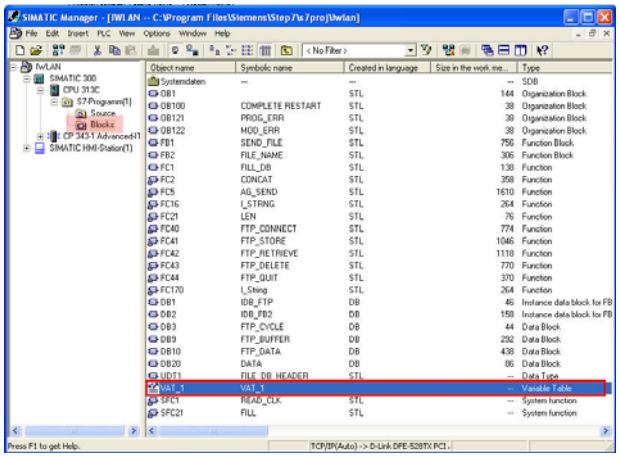
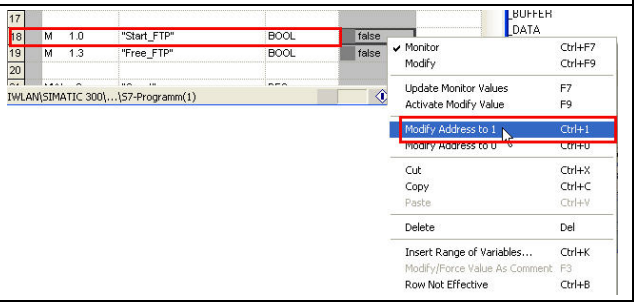
Preparation

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

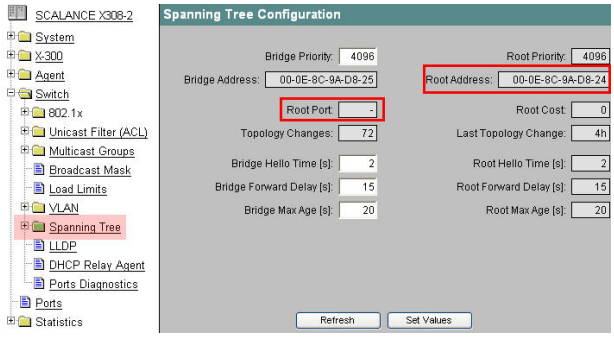
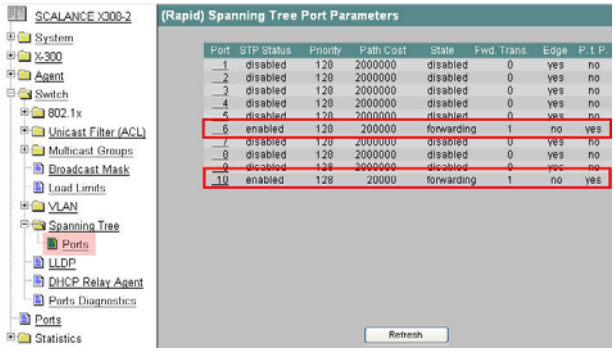
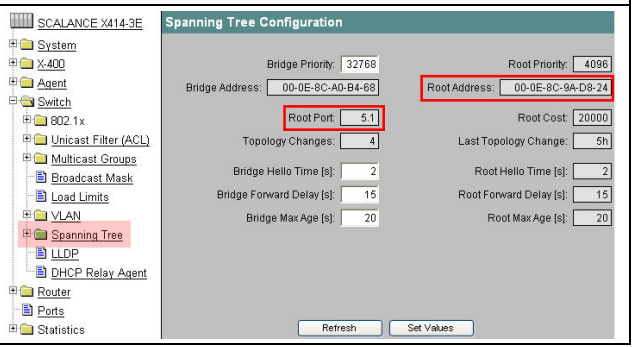
Table 6-1

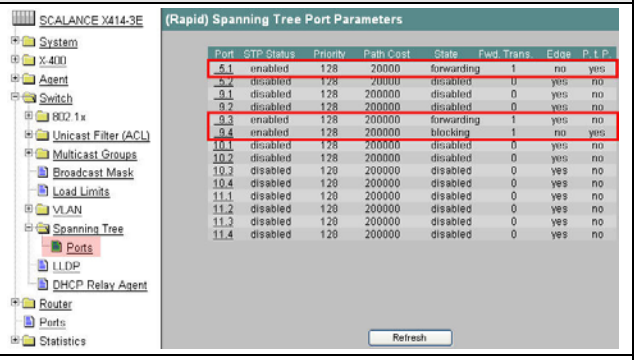
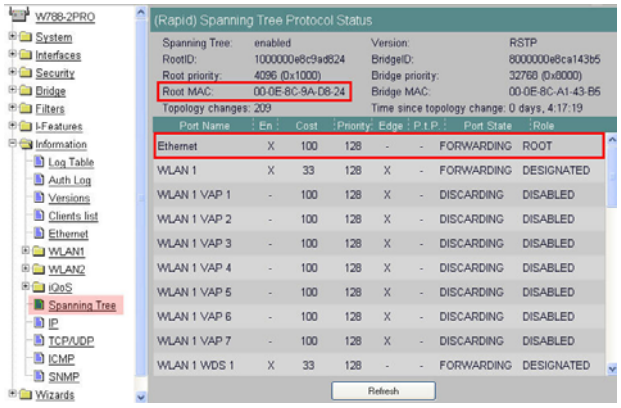
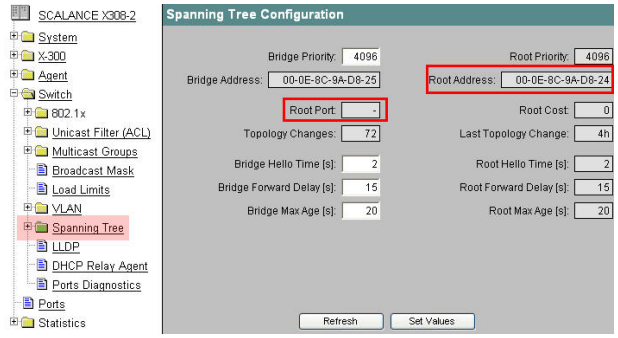
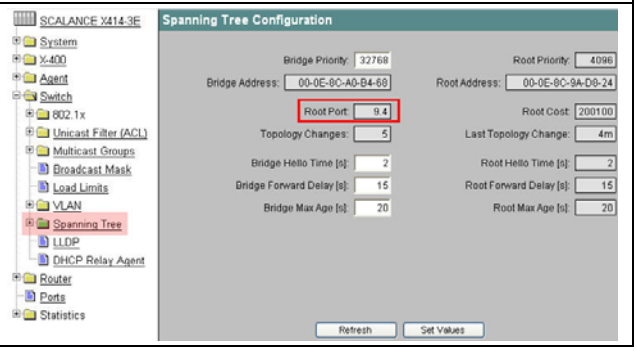
No.	Action	Comment
1.	Open the **SIMATIC MANAGER** and the **IWLAN** STEP 7 project. Navigate to **`SIMATIC 300->CPU 313C->S7-Program->Blocks`** and double-click the variables table **`VAR1`**.	
2.	Use your **right mouse button** to click the status of **line 18** (**M1.0**) and change the **status to 1**. This starts the cyclical FTP transfer.	
3.	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.	

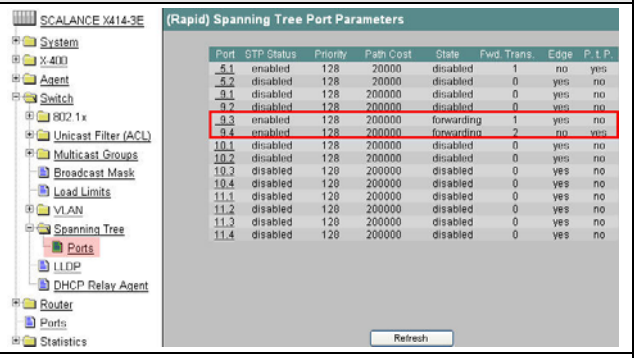
6.2 Redundancy scenario

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.	By setting the priority in the SCALANCE X308-2 this module is forced to become the root bridge. Open the web-based management of the SCALANCE X308-2 (172.158.1.5) and navigate to **Switch-> Spanning Tree**. 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.	
2.	Under **Switch-> Spanning Tree->Ports** you can see which ports are blocked or enabled.	
3.	Open the web-based management of the SCALANCE X414-3E (172.158.1.4) and navigate to **Switch-> Spanning Tree**. Here you can see the MAC address of the root bridge (SCALANCE 308-2) and the root port.	

No.	Action	Comment
4.	Under **Switch-> Spanning Tree->Ports** you can see which ports are blocked or enabled.	
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**.	
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.**	

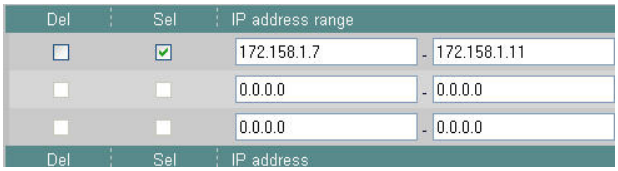
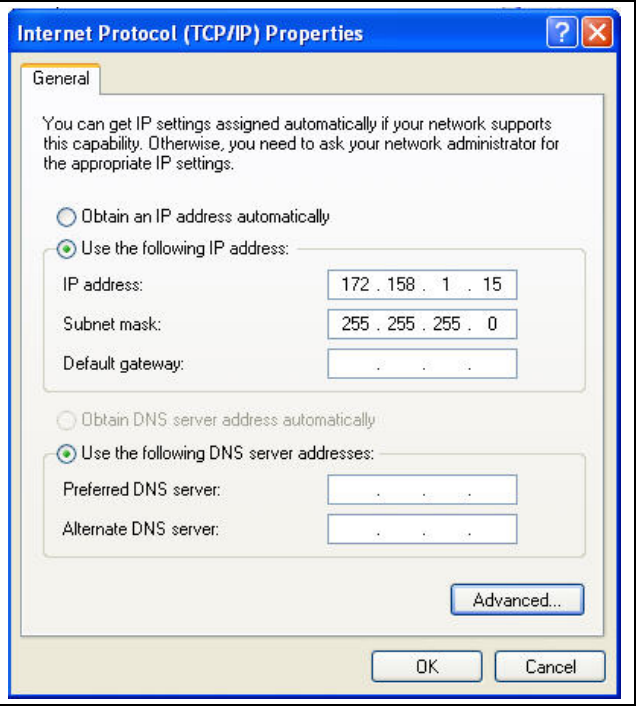
No.	Action	Comment
9.	You can see under **Switch-> Spanning Tree->Ports** that the port that was blocked before is now active.	
10.	A short message about the topology change is passed on to the Syslog server.	

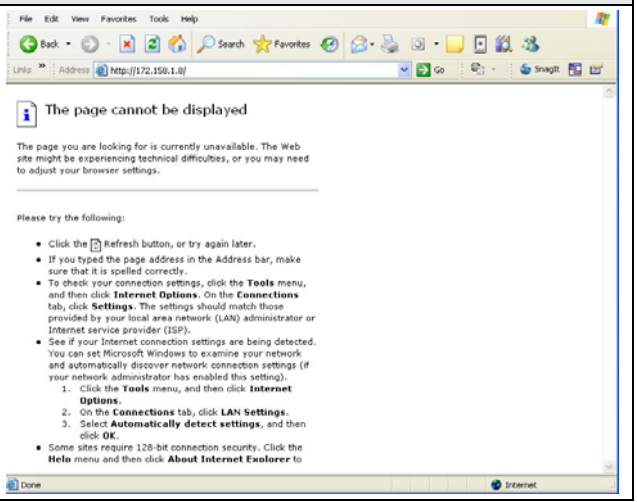
6.3 Access control scenario

Access control

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

Table 6-3

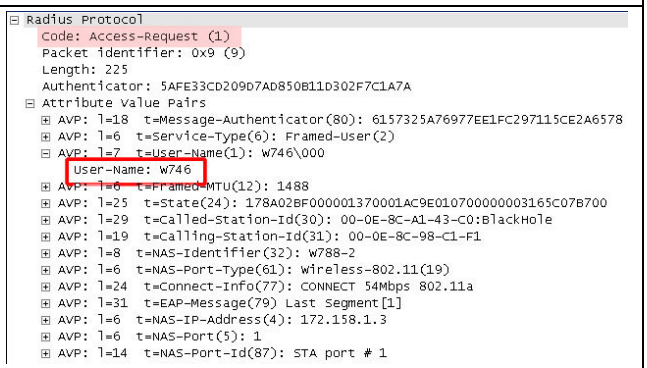
No.	Action	Comment
1.	Connect the test PG/PC to the SCALANCE X108 and open the web-based management of the SCALANCE W746-1. Since the text PG/PC (172.158.1.9) has an IP address that is enabled in the IP range of the SCALANCE W746-1 module, the PC is allowed to access the management.	
2.	Change the IP 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.	

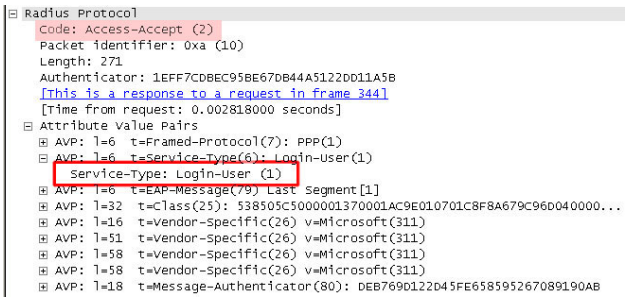
RADIUS

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	

Configuration 12 Article ID: 30805917

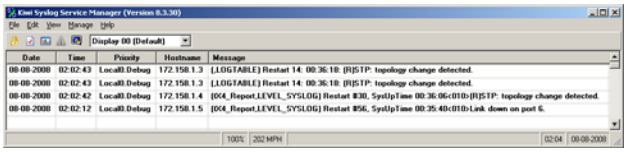
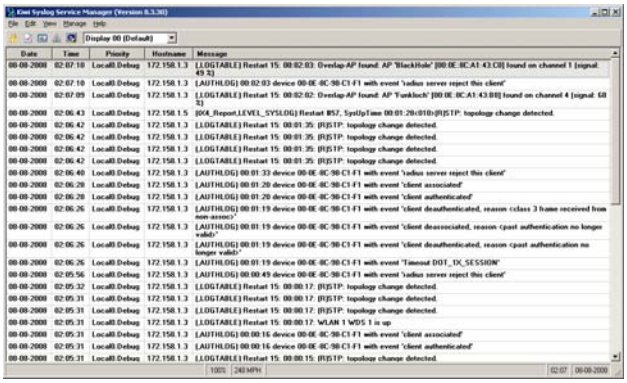
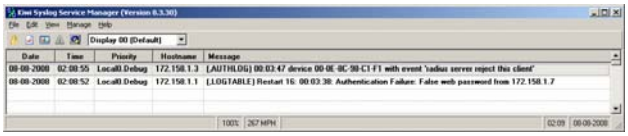
No.	Action	Comment
3.	Since a user with this data has been created in the RADIUS server, the SCALANCE W746-1 is allowed to access the network.	
4.	As soon as you exit the RADIUS server (e.g., by shutting the computer down) and restart the SCALANCE W788-2, the SCALANCE W746-1 has no longer access to the network.	

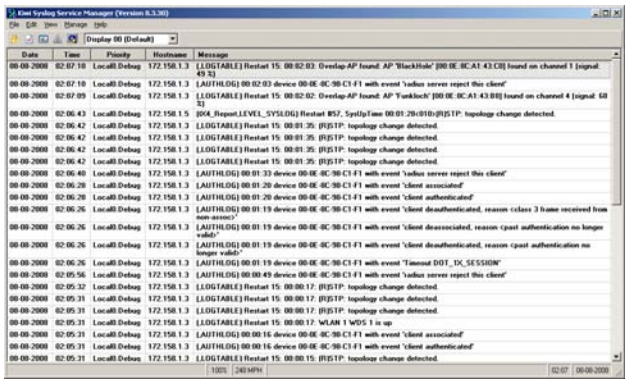
6.4 Diagnosis scenario

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

Syslog

Table 6-5

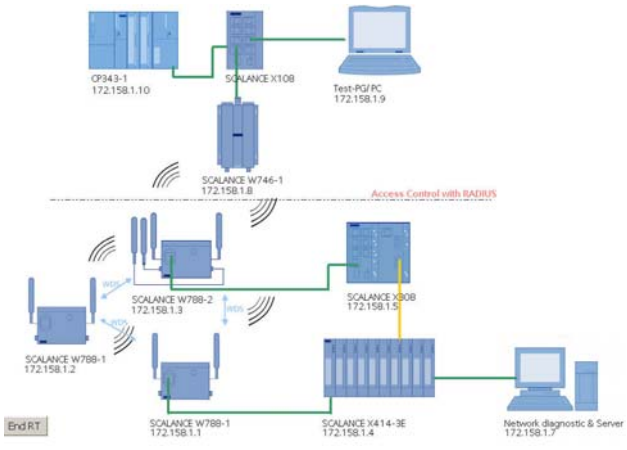
No.	Action	Comment
1.	Disconnect the cable from one port of the SCALANCE X308-2 or the SCALANCE X414-3E. The link down is transmitted as a short message to the server. If the topology is also changed by this, a Syslog message is sent to the server.	
2.	Restart the SCALANCE by briefly switching the power supply off and back on. As soon as the SCALANCE reboots, a Syslog message is sent.	
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.	

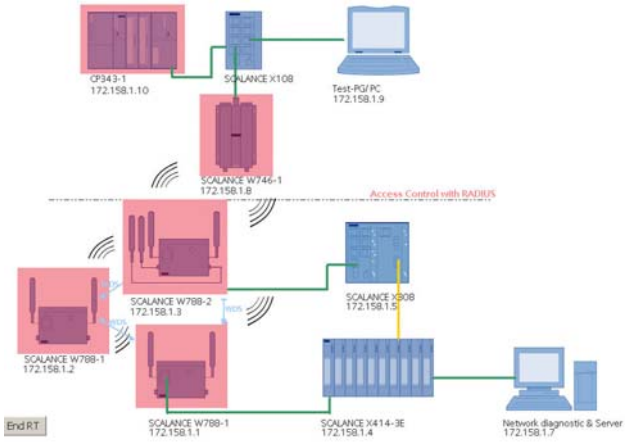
No.	Action	Comment
4.	If a SCALANCE finds several radio networks within its environment, it sends a message to the server.	

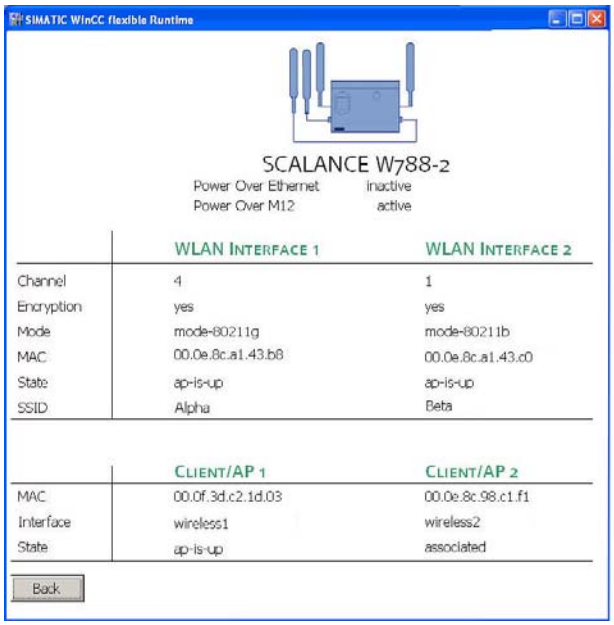
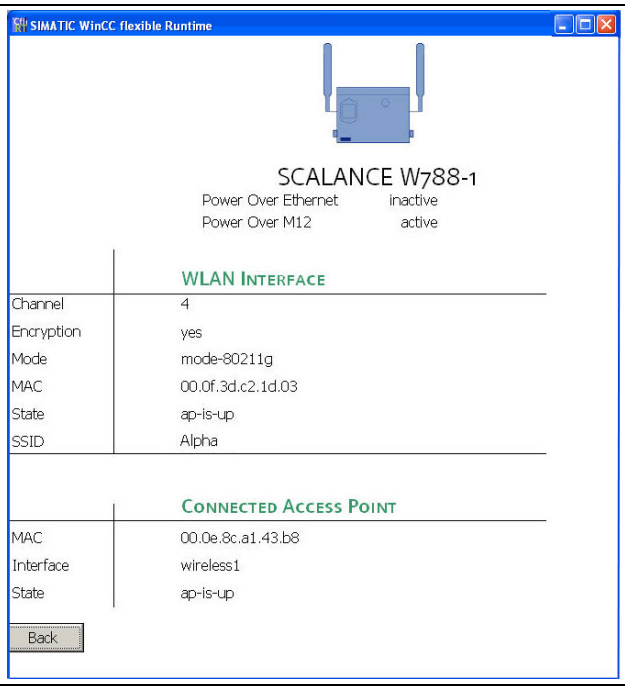
Network visualization

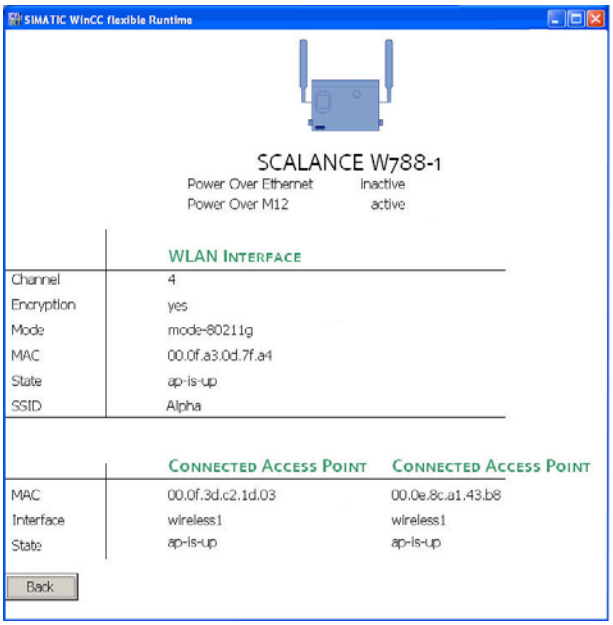
The network visualization feature via WinCC flexible can be used to display and monitor components.

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.	

No.	Action	Comment
3.	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.	
4.	Clicking the SCALANCE W746-1 opens the information page. Data on the own WLAN interface and on the connected access point is displayed here.	 SCALANCE W746-1 Power Over Ethernet inactive Power Over M12 active **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.	
6.	Return to the overall view and click the first SCALANCE W788-1. A new window opens and displays information on the WLAN interfaces.	

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.	

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