Security with SIMATIC NET

SCALANCE Family, CPx43-1 Advanced (V3), SOFTNET Security Client

Compendium• January 2013

Applications & Tools

Answers for industry.

SIEMENS

Siemens Industry Online Support

This entry is taken from Siemens Industry Online Support. The following link takes you directly to the download page of this document:

http://support.automation.siemens.com/WW/view/en/27043887

Caution:
The functions and solutions described in this entry are mainly limited to the realization of the automation task. In addition, please note that suitable security measures in compliance with the applicable Industrial Security standards must be taken, if your system is interconnected with other parts of the plant, the company's network or the Internet. More information can be found under entry ID 50203404.

http://support.automation.siemens.com/WW/view/en/50203404

SIEMENS

SIMATIC
Security with SIMATIC NET

Industrial Security

Warranty and Liability

Note

The application examples are not binding and do not claim to be complete regarding configuration, equipment and any eventuality. The application examples do not represent customer-specific solutions. You are responsible for ensuring that the described products are used correctly. These application examples do not relieve you of your responsibility to use sound practices in application, installation, operation and maintenance. When using these application examples, you recognize that we will not be liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these application examples at any time and without prior notice. If there are any deviations between the recommendations provided in this application example and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.

Any claims against us - based on whatever legal reason - resulting from the use of the examples, information, programs, engineering and performance data etc., described in this application example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change in the burden of proof to your disadvantage.

Preface

Objective of this application

With the increasing use of Ethernet up to the field level, security is a topic that gets more and more important also in automation engineering.

This document gives a detailed description of the topic "Industrial Security" in theory and practice.

Main contents of this document

The following main points will be discussed:

- Introduction of basic data communication and security terms important for comprehension.
- Discussion of problems of secure data transmission.
- Description of possible security scenarios with the SIMATIC NET product range.
- Description of basic principles of communication and the most important security mechanisms in theory.

Topics not covered by this application

This document is an Overview Document on Industrial Security and does not include any detailed application or configuration instructions. You can find an example configuration on the Siemens Industry Online Support web page (http://support.automation.siemens.com).

Table of Contents

1 Overview of Important Terms and Technologies

As Industrial Ethernet and PROFINET are finding their way into production, IP mechanisms and protocols, too, are advancing into the world of automation.

Note

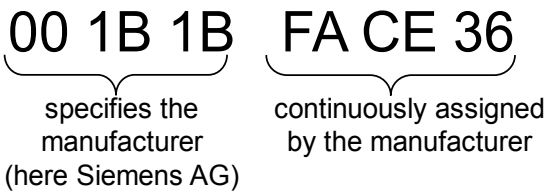
This chapter will briefly explain terms that are helpful for further understanding.

For a detailed description of these and other terms please refer to chapter 4 (Basics and Principles).

1.1 Address assignment

Each system connected to an Ethernet network is clearly specified by a MAC address. This MAC address consists of 6 bytes. The first three bytes specify the manufacturer, the last three bytes are assigned consecutively by the manufacturers. The notation is usually hexadecimal:

Figure 1-1



Each MAC address is assigned one or more IP address/es, depending on the network structure.
The IP address with IPv4 consists of 4 bytes and is represented in dotted-decimal notation (four numbers separated by dots):

The rapid increase in network-compatible devices results in the fact that the number of IP addresses enabled through IPv4 is running out.

IPv6 is to counteract this development, providing 16 bytes for the IP address. The address is represented by eight hexadecimal numbers, each separated by a colon.

Figure 1-2

IPv4: 157.234.14.87
IPv6: 2012:0dc8:89a3:08d3:1219:8f2e:aa70:7364

1.2 Transmission protocols

The protocols used in an industrial Ethernet are from the IP protocol suite. They are divided into connection-oriented TCP protocols and connectionless UDP protocols. The IP protocols owe their development to the fact that for a long time there were no official standards for integrating different computers in one network. In the early 70s, the US Department of Defense commissioned one of its departments to develop and define a communication protocol for connections and data exchange in manufacturer-independent, heterogeneous computer networks.

The package-oriented Wide Area Network Arpanet (Advanced Research Projects Agency Network) was the experimental platform used for first tests with these communication protocols. The protocol specifications were written down and published in the form of Request for Comments (RFCs).

In the early 80s, when the development was completed, the US Department of Defense declared TCP/IP as its standard communication protocol. Many of the RFCs defined were taken as military standards without changes.

The civil breakthrough of TCP/IP came with its first implementation in the 4.2BSD UNIX system. This source code was later made publicly available as PublicDomain software by the University of Berkeley. Shortly afterwards, all UNIX systems took over TCP/IP and other operating systems jumped on the bandwagon.

1.3 Firewalling

Firewalling describes the process of filtering the data traffic using information in the header of the data packet. The header includes information about the sending/receiving party, the transmission protocols used, etc., which precede the actual user data. Data traffic can be filtered according to:

- MAC addresses
- IP addresses
- Communication protocols

In addition, the syntactical correctness of the communication protocols used can be verified.

1.4 Encoding

Encrypting the data to be transmitted ensures confidentiality and integrity during data transmission. The most common encryption methods are:

- IPsec
- WPA
- SSL

For encryption, systems which are capable of encrypting and decrypting the data packets must be installed on the sending and receiving side. Such systems may be realized as standalone hardware (e.g. SCALANCE S612) or software-based (e.g. SOFTNET Security Client).

2 Risk Reduction through Security

2.1 Problem description

There are currently two major trends in industrial automation:

- wireless data transmission
- the security of networks in production

The security issue is of primary importance since industrial Ethernet solutions and numerous unsecured interfaces are on the rise. The use of standard components from information technology and the advance of Ethernet-based communication standards creates vulnerabilities unknown for the physically isolated automation systems used in the past.

2.2 Conditions and requirements

Requirements

Security requirements include:

- Data confidentiality: user data must be encrypted and protected from unauthorized access
- Node authorization: Only defined stations must participate in the data communication. Authentication is required.
- Packet identification: It must be ensured that the data packets arrive unchanged at their destination address.
- Confidentiality: Networks behind the VPN Gateways should be hidden from third parties.

Conditions of automation engineering

The specific requirements of automation engineering are:

- Taking into account effectiveness and economic efficiency through using already available infrastructure.
- Nonreactive integration: The existing network infrastructure must not be changed and existing components must not be reconfigured.
- Maintaining data security by protection from unauthorized access.
- Availability: Particularly in remote control technology it is essential that the connection between the control center and the production plant is robust, safe, and reliable.

2.3 The Siemens protection concept: “Defense in Depth”

Multi-level security concept

Increased networking and the use of proven technologies of the "Office world" in automation systems lead to increased security requirements. It is not sufficient to offer only superficial and limited protection, since attacks from outside may occur on several levels. Pronounced awareness of security is required for optimal protection. Siemens follows the "Defense in Depth" strategy in order to achieve the required security goals. The approach of this strategy is a multi-layer security model consisting of the following components:

- Plant security
- Network security
- System integrity

The advantage of this strategy is the fact that an attacker first has to break through several security mechanisms to do any damage. The security requirements of the individual layers can be taken into account.

Instruments of the "defense in depth" strategy

For the implementation of this protection concept two security instruments from the field of network security are mentionable, for example: the firewall and the VPN tunnel. A firewall is used to control data traffic. By filtering, packets can be discarded and network accesses can be blocked or granted.

VPN (IPsec) is used to secure communication against spying and manipulation.

2.3.1 The Siemens solution for plant security

Implementation of an appropriate, comprehensive security management is the basis for planning and realizing an industrial security solution.

Security management is a process mainly comprising four steps:

- Risk analysis with definition of risk reduction measures: These measures must be defined for the plant, depending on the threats and risks identified.
- Determination of guidelines and coordination of organizational measures.
- Coordination of technical measures.
- Consistent security management process with regular or event-dependent repetition of risk analysis.

2.3.2 The Siemens solution for network security

If controllers or other intelligent devices with no or minimum self-protection are located in a network segment, the only remaining option is to create a secured network environment for these devices. The easiest way to achieve this is the use of special routers or gateways. They establish security through integrated firewalls in industrial quality which also protect them. Additional security can be provided by segmenting individual sub-networks, e.g. through a cell protection concept or a demilitarized zone (DMZ).
The Siemens security solution was developed particularly for the requirements of an automation environment, in order to meet the increasing demand of network security, reduce the susceptibility to failure of the entire production plant and thus to increase its availability.

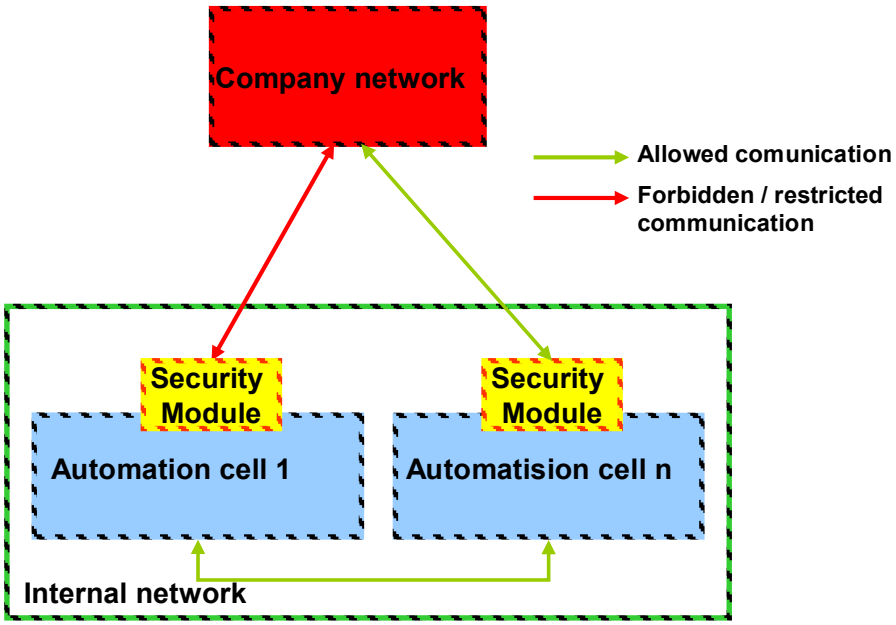
The cell protection concept

The core of this concept is to segment the automation network in terms of security and to form protected automation cells. Cells therefore are network segments which are decoupled in terms of security.

The network nodes within a cell are protected by special security modules to control the data traffic from and to the cell and to check the authorizations. Only authorized telegrams will be allowed to pass.

This can be done via VPN (Virtual Private Network) or firewall.

Figure 2-1



Advantages of the cell concept

The concept of cell protection mainly serves for protecting any devices that cannot protect themselves. Mostly, these are devices for which an upgrade with security functions would be too costly. Sometimes an upgrade is not realizable technically. Mainly smaller automation devices do not fulfill the necessary hardware requirements.

The security module protecting the complete cell secures several devices at the same time, which apart from lower costs also means lower configuration expenses.

Realtime and security

Realtime communication and security are in principle two opposing requirements. Checking the messages according to the rules or configurations costs time and performance. With the cell protection concept, both factors can be achieved simultaneously. Realtime data traffic can flow within a cell entirely unaffected by security mechanisms. Data is only checked by the security module at the cell input.

Security components

For the realization of the cell protection concept, Siemens offers security modules and software, as well as communication modules that provide integrated communication functions plus specific security functions:

- S7 Advanced Communication Processors (VPN, Firewall)
  CP443-1 Advanced and CP343-1 Advanced V3.0
- Security PC-CP (VPN, Firewall) CP1628
- GPRS/UMTS-Router (VPN, Firewall) SCALANCE M875
- Security-Module SCALANCE S V3.0
- VPN Software Client SOFTNET Security Client (V4)

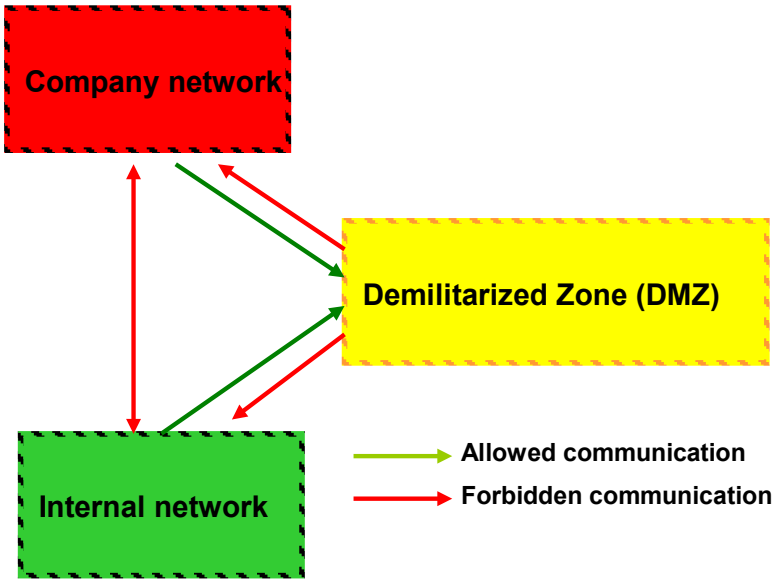
Demilitarized zone (DMZ)

The connection via a demilitarized zone (DMZ) provides an even higher level of security.

A DMZ aims at blocking the direct communication between the internal network (production network / automation cell) and the remaining company networks and the Internet through firewalls. Data can only be exchanged indirectly via an additional network isolated from the other networks (the DMZ).

This controlled data traffic enables improved protection of sensitive company data against unauthorized access and the reliable implementation of internal security guidelines for communication.

Figure 2-2



Security module

The SCALANCE S623 module is used for realizing a demilitarized zone. With its three network connections and integrated firewall, this module provides the possibility of physically separating the different networks (external, internal, and DMZ).

2.3.3 The Siemens solution for system integrity

In order to maintain the system integrity, it is important to minimize the vulnerabilities in PC systems and in the control level. Siemens meets this requirement with the following solutions:

- Use of antivirus and whitelisting software
- Maintenance and update processes
- User authentication for machine or plant operators
- Integrated access protection mechanisms in automation components
- Protection of the program code through know-how protection, copy protection, and assignment of passwords

3 Possible Scenarios for Data Protection

This chapter will show a selection of security scenarios that can all be realized with the products of the SIMATIC NET product range.

Each security scenario will describe the corresponding **application** and a **practical solution approach** with security components.

These scenarios can be divided into the following main categories:

- Restricting communication in plants
- Secure data communication via unsecured networks
- Secure communication via WLAN

3.1 Node restriction on S7 controls

Network topology

Figure 3-1

Fehler! Es ist nicht möglich, durch die Bearbeitung von Feldfunktionen Objekte zu erstellen.

Application

The S7 controller is connected to a network via an Ethernet CP. This network has several nodes. But only some nodes should be allowed access to the S7 controller.

Problem

The network itself does not have a protection mechanism against unauthorized access to the S7 station. Therefore, the S7 station can be accessed from any configuration station using STEP 7 and its configuration can be changed. This unauthorized access could lead to the S7 station being sabotaged.

Possible solutions using SIMATIC NET components

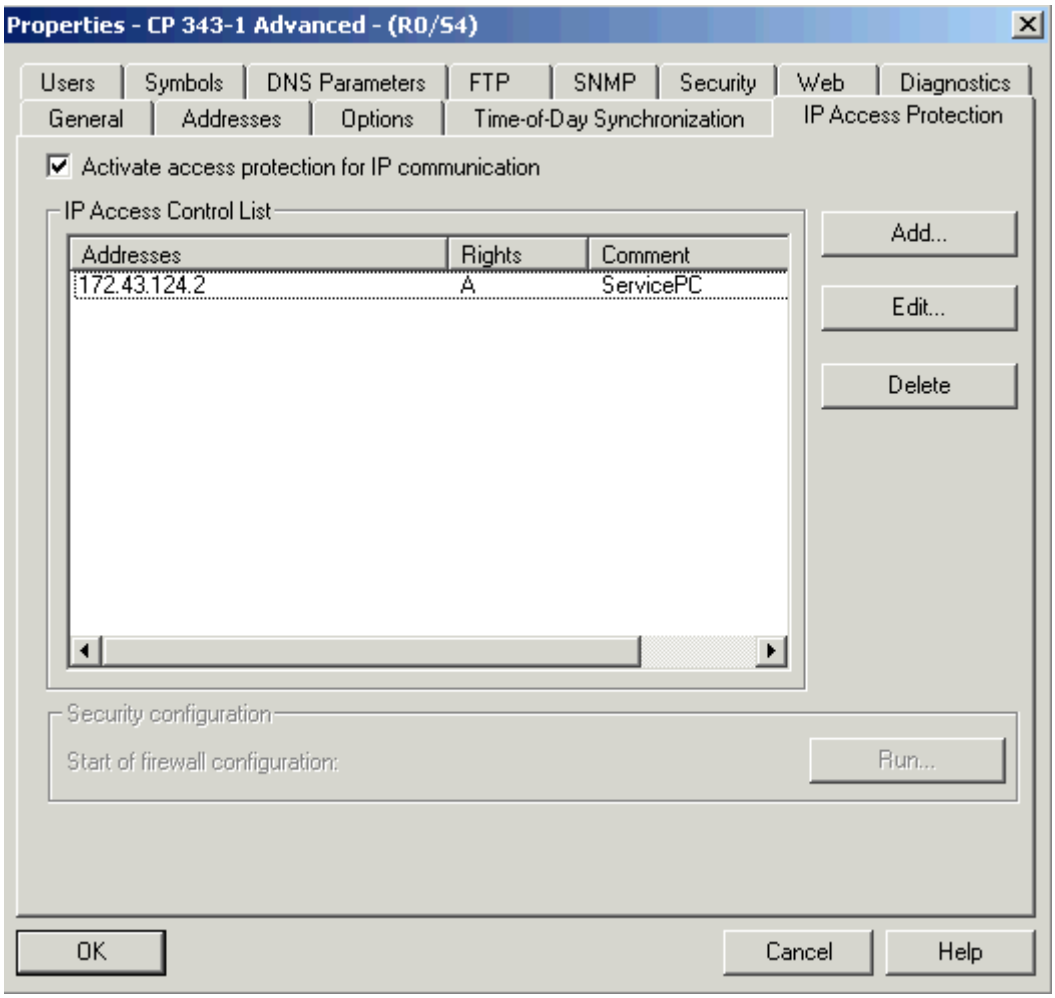
There are several possible solutions:

- Protection in the end device through access protection
- Protection through a firewall
- Protection through segmentation using VLANs
- Protection through authentication

3.1.1 Protection in the end device

Solution approach

Figure 3-2



Description

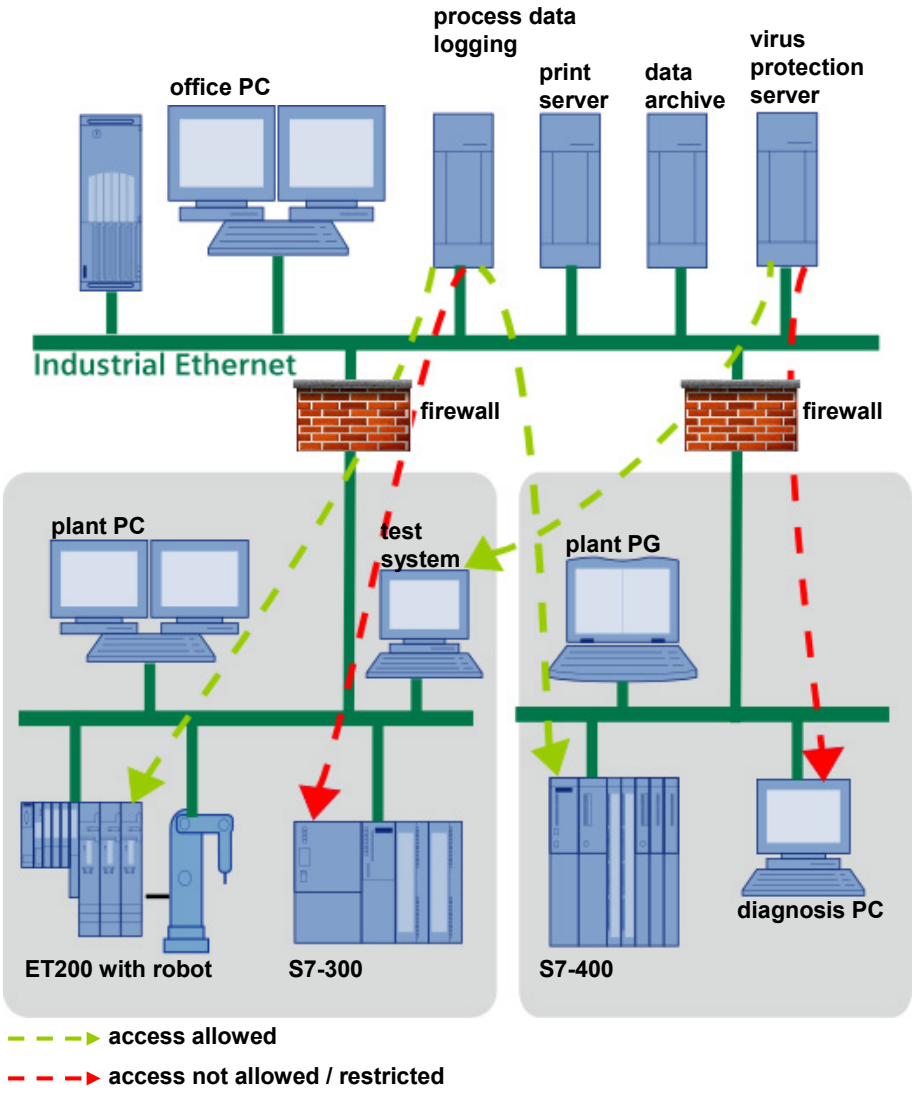
To prevent unauthorized access to a S7 station, an **Ethernet communication processor** (e.g. CP343-1) is used for network connection on the S7 side. These CPs can be configured to permit selected IP addresses only to access the S7 station via Ethernet.

The required configuration is made via the STEP 7 HW Config in the CP properties. The IP access protection tab contains an editable list where all IP addresses can be entered which are allowed to access the S7 station.

3.1.2 Protection through a firewall

Solution scheme

Figure 3-3



Description

A firewall can basically filter incoming and outgoing data packets with regard to selected criteria. All products of the **SCALANCE S** and **SCALANCE M** family and the **security communication modules** provide this function.
Both the receiver and the sender address may be used as a criterion for the firewall in order to prevent access to the S7 controllers. The firewall will only let the data packets pass to the S7 controller if the rule for forwarding has been configured accordingly. If they do not match, the packet will be rejected.

The fire wall rules of the SCALANCE S family and the security communication module will be created using the Security Configuration Tool (SCT) and may be defined as follows:

- globally
- locally
- user-defined (only SCALANCE S V3 or higher)

Local rule sets are assigned to one module each and are directly defined in the properties dialog.

Global firewall rules are defined outside the modules on project level, which provides the advantage that rules applying to several modules must only be configured once. Via drag & drop, the global firewall rules are simply assigned to the module they are applicable to.

Global firewall rules can be defined for:

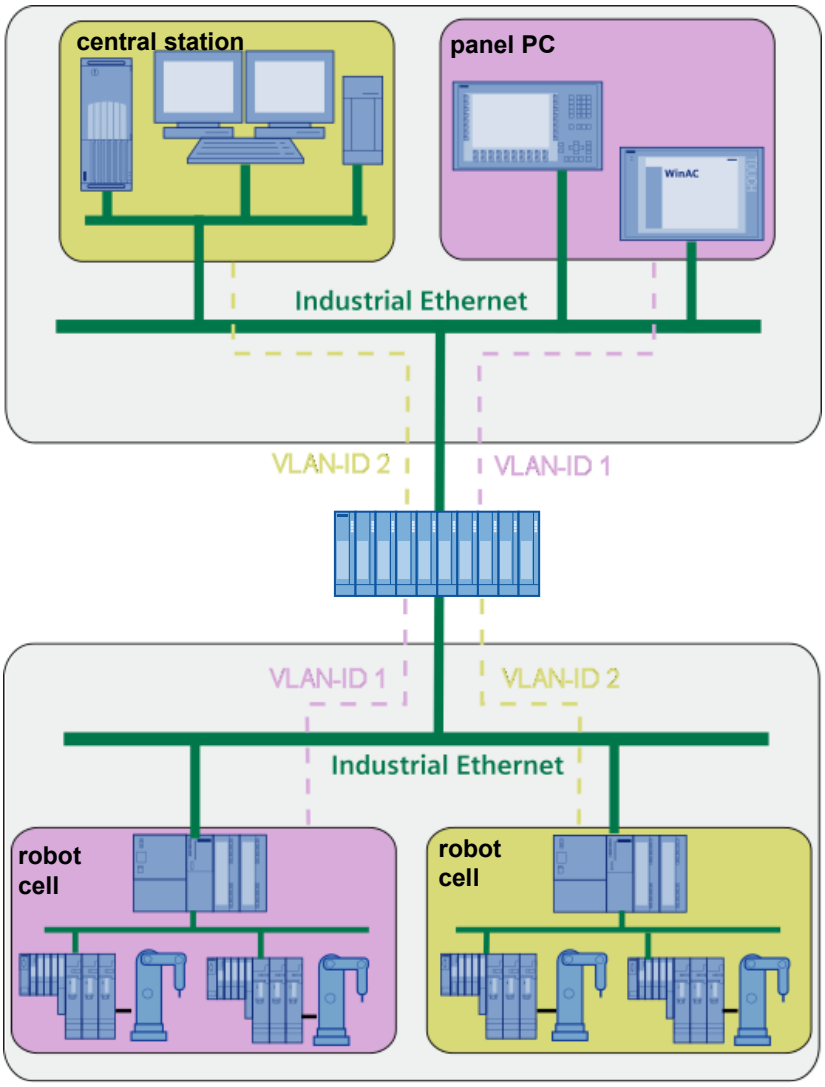
- IP rule sets
- MAC rule sets

For the **user-defined firewall** the rule sets can be assigned to one or more users and then to individual security modules, providing the option to make accesses subject to successful user authentication. For authentication, the user can log on to SCALANCE S V3 on a web page. After successful log-on the firewall rule set assigned to this user will be activated.

3.1.3 Protection through “segmentation”

Solution scheme

Figure 3-4



Description

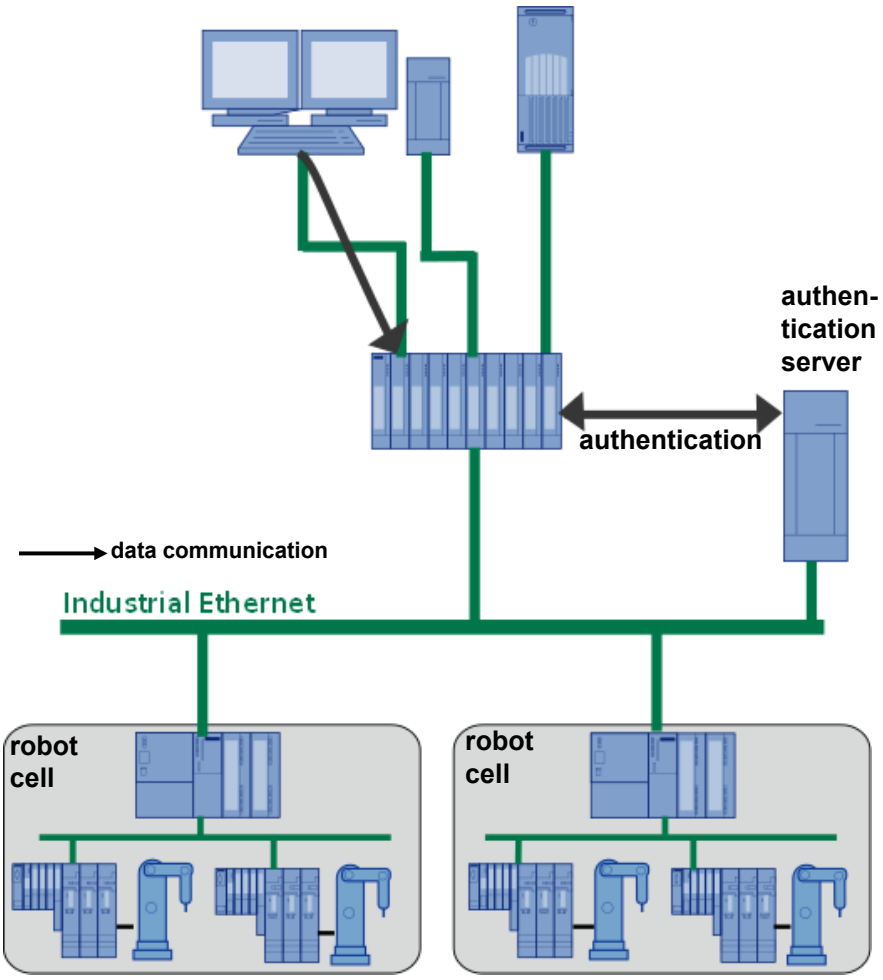
Another way of protecting against unauthorized accesses to an S7 controller is the use of VLANs. The switches **SCALANCE X-300, X-400** and **X-500** allow for a corresponding configuration.

This method uses the web-based management to assign a VLAN ID to the individual ports of a switch. Communication will then only be possible within a VLAN (ports with the same VLAN ID). This means that both the configuration station and the S7 station must be on switch ports with the same VLAN ID.

3.1.4 Protection through authentication

Solution scheme

Figure 3-5



Description

The **SCALANCE switches** of the **X-300, X-400, and X-500** series support **IEEE 802.1x.** This standard is a method for authentication in networks.

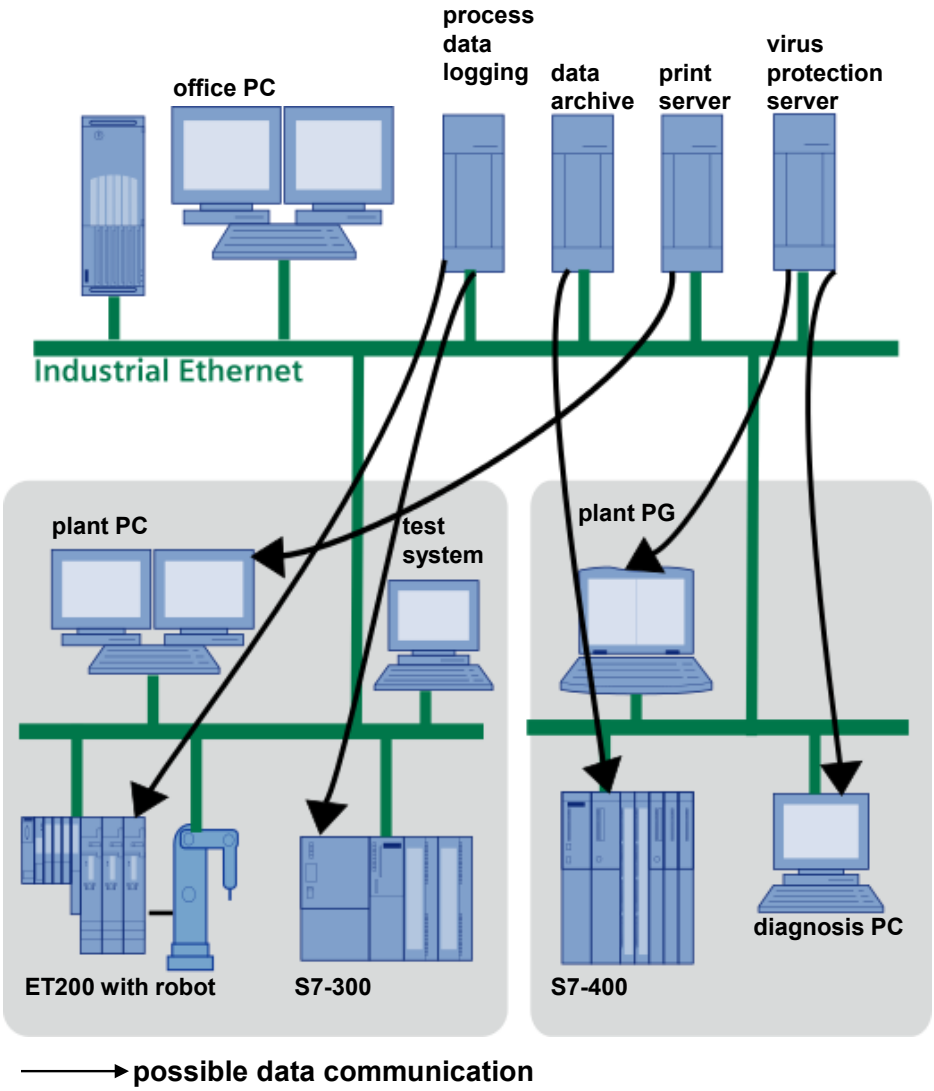
The RADIUS concept is based on an external authentication server, so that access to the network for end devices in the robot cell can be restricted via the IE switch.

Via the web-based management, each port in the IE switch can be assigned to perform an authentication process for defined end devices. The IE switch uses an authentication server (RADIUS server) to verify the log-on data transmitted by the end device. If these data match the data stored on the RADIUS server, the end device is granted access to the network behind the switch via this port; if not, access will be denied.
This standard requires both the RADIUS server and the end device to support the EAP (Extensive Authentication Protocol).

3.2 Communication restrictions for plants / single devices

Network topology

Figure 3-6



Application

A network involves several nodes with different functions.

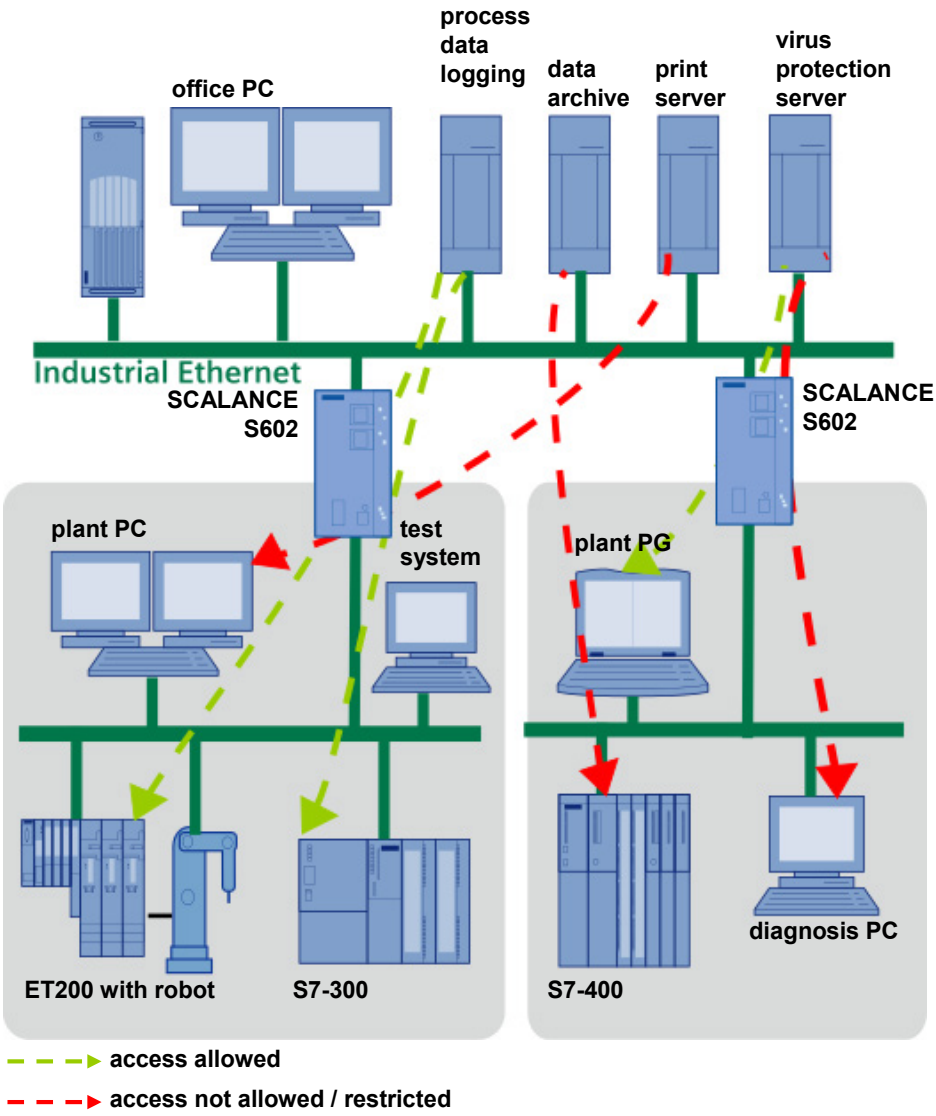
Each single device or cell, by means of a fire wall, shall be capable of restricting access to that device or internal devices, so that only certain applications are available to selected nodes.

Problem

The different functionalities are often bound to specific protocols (e.g. the S7 protocol for the S7 configuration, DCP for IP address assignment, HTTP for web-based management). The problem here is that there is no filtering for certain protocols within the network and therefore all nodes can access any application.

Possible solution using SIMATIC NET components

Figure 3-7



The **SCALANCE S602** module can be used for cell protection in this case, besides the SCALANCE S612, S623 security modules and security CPs. It provides the same **firewall functionality** as the modules mentioned, but it does not have VPN functionality.

The SCALANCE S is used as the connection point of the cell with the remaining network. A filter is configured for the protocol to be blocked in order to prevent certain protocols from spreading throughout the entire network, restricting them instead to the relevant cell.

With a filter on PROFINET-DCP (for identifying all PROFINET nodes), for example, only the nodes within the cell (and not the nodes of the remaining network) will be displayed.

3.3 Bandwidth restriction

Application

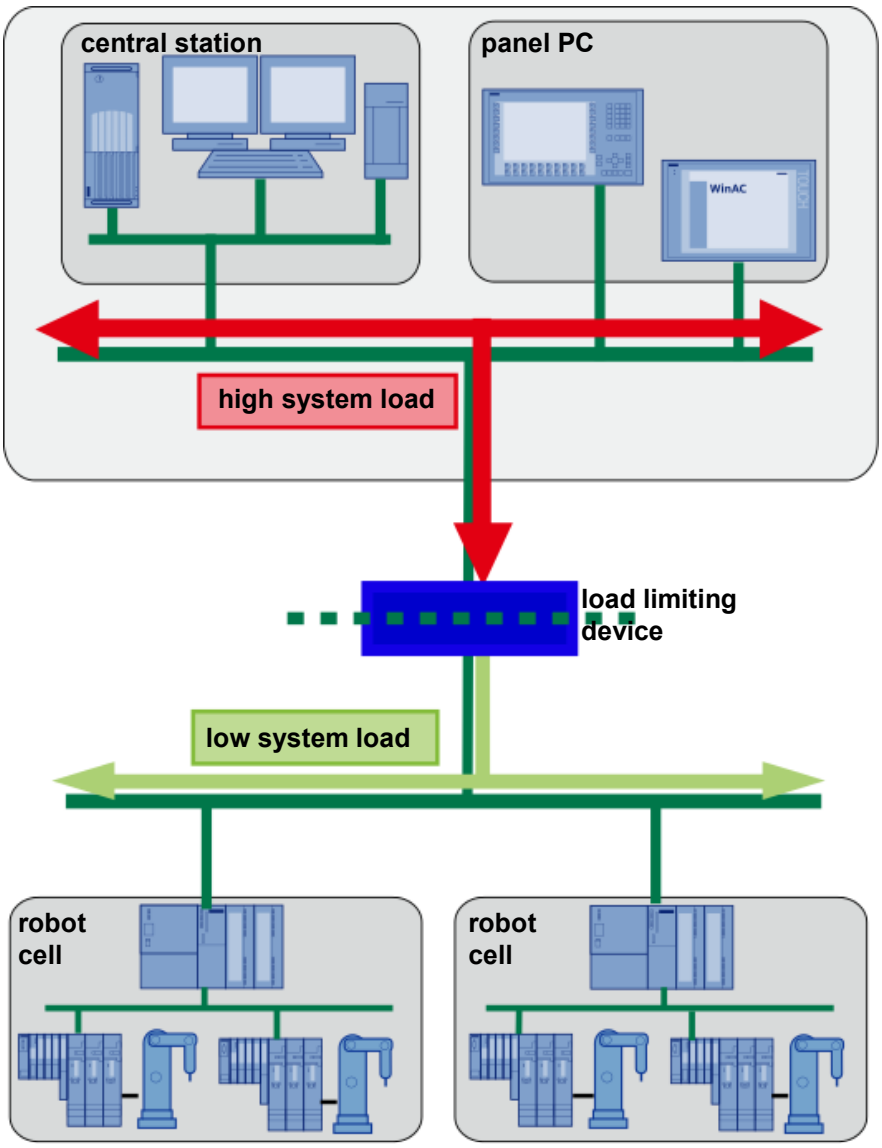
Frequently, multiple automation cells are interconnected through a higher-level network. A system load occurring in that network (e.g. broadcast storm) shall have no impact on the individual stations.

Problem

Usually, the network itself does not have any filter functions for such overload conditions. As a consequence, a broadcast storm, for instance, will be forwarded to all cells, causing the connections between all communication partners within that cell to be aborted. Data exchange will come to a stop.

Possible solutions using SIMATIC NET components

Figure 3-8

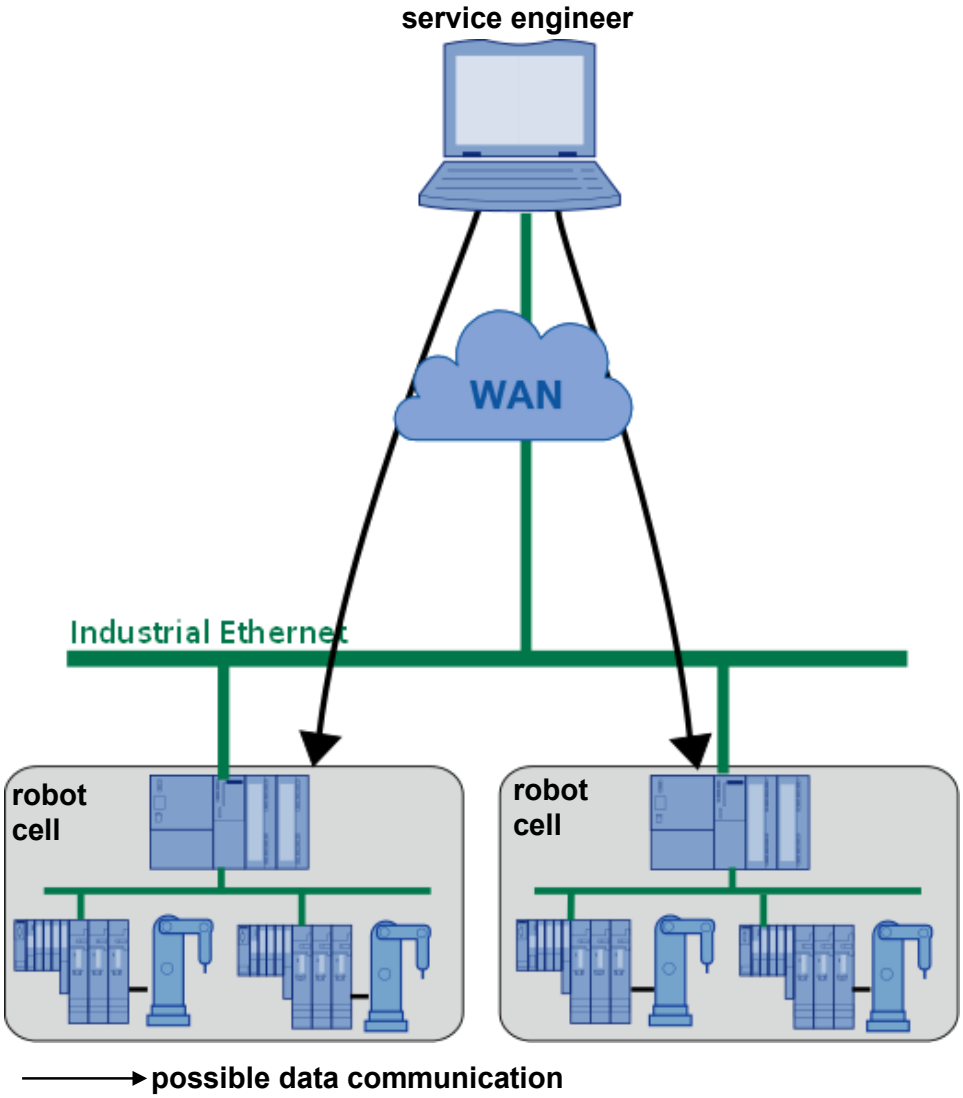


The easiest way to prevent network loads from spreading is to install a **load limiting device** at the connecting point between a cell and the network. A load limiting device can be either a **SCALANCE X-300, X-400,** or **X-500** switch, a **SCALANCE S** module or a **security CP** with activated bandwidth limitation. If, with this setting, a high load occurs in a network, data exchange can continue without difficulties or restrictions within the cell.

3.4 Secure remote access via Internet

Network topology

Figure 3-9



Application

Service engineers frequently need to connect to a production network from a remote location in order to remotely access the stations (e.g. S7, etc.) connected in the network. Once connected to the network, the service engineer can, for instance, load new programs into an S7 controller or update the firmware.

Since a higher performance is expected today, an Internet connection via DSL line is preferred to a modem solution via analog dial-up line. With a DSL line, technicians around the world can connect to a production network at lower costs than with the modem solution.

Problem

Two data security aspects are of major interest in this scenario: Firstly, it is important to encrypt data transmitted over the Internet to protect them against unauthorized access. Secondly, it is essential that only the service staff is given access to the system.

Possible solutions using SIMATIC NET components

The Siemens product portfolio offers the following security components for this purpose:

- Security Modules SCALANCE S612 and S623
- SOFTNET Security client (SSC) software
- PLC-CPs (CPx43-1 Advanced V3)
- PC-CP1628
- SCALANCE M875 UMTS router

All components are VPN-capable and can establish secure connections using IPsec.

Via the joint configuration software **Security Configuration Tool**, the modules can be configured such that they represent the end points of a joint VPN (Virtual Private Network) tunnel.

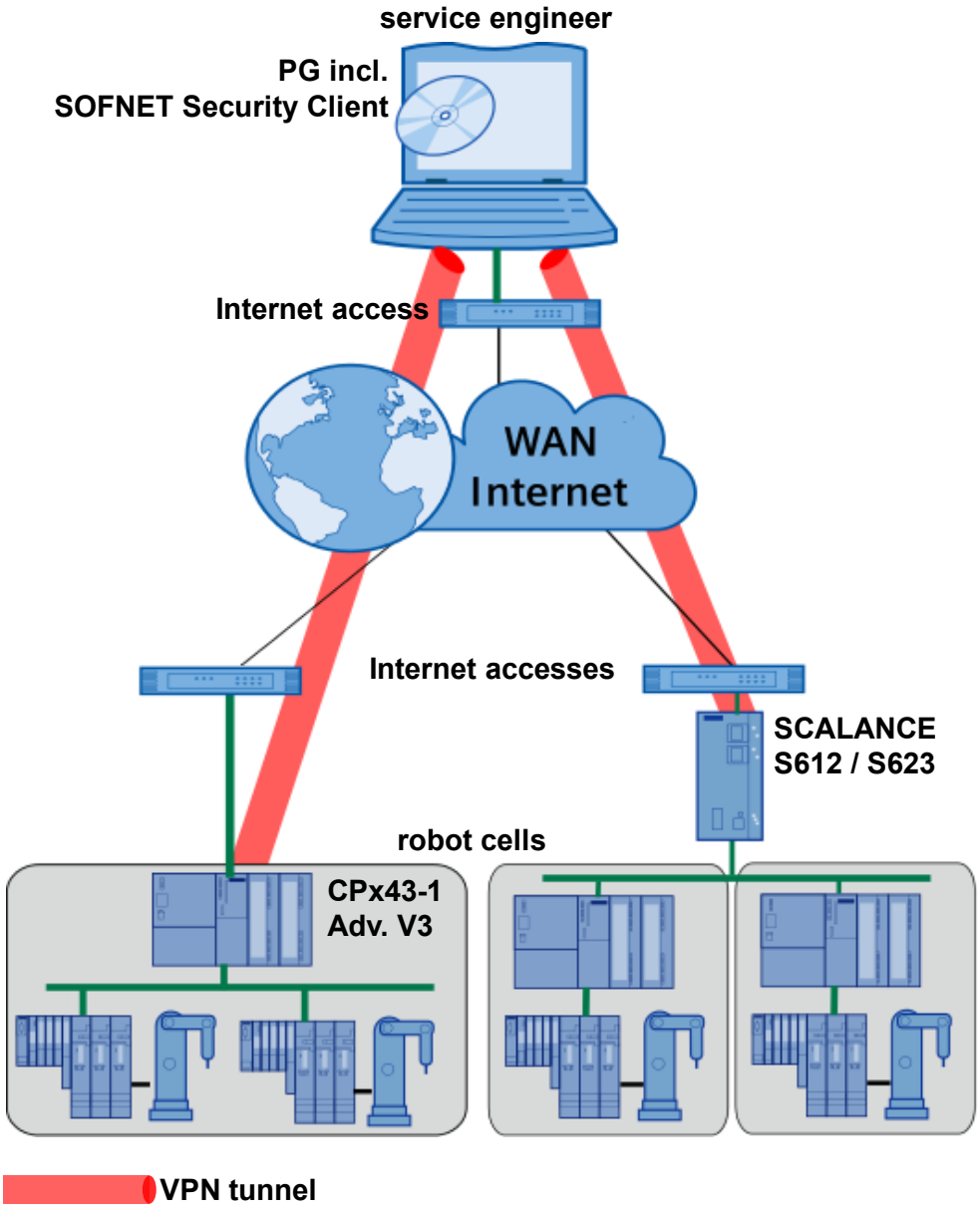
The remote access to an automation network by a service engineer, taking into account the above-mentioned data security aspects, is **software-based** with the SSC on the engineer's side and **hardware-based** with one of the modules mentioned above on the plant side.

After setting up a VPN connection with the peer on the automation side, a service engineer can access any device in the automation network, for example to load a new parameterization to an S7 station using STEP 7.

3.4.1 Access to a system with DSL broadband connection

Solution scheme

Figure 3-10



Description

If the system has a **DSL connection**, the following modules can be used on the service PC in combination with a SOFTNET Security Client:

- Use of a SCALANCE S612 or S623.
- Use of a security CP.

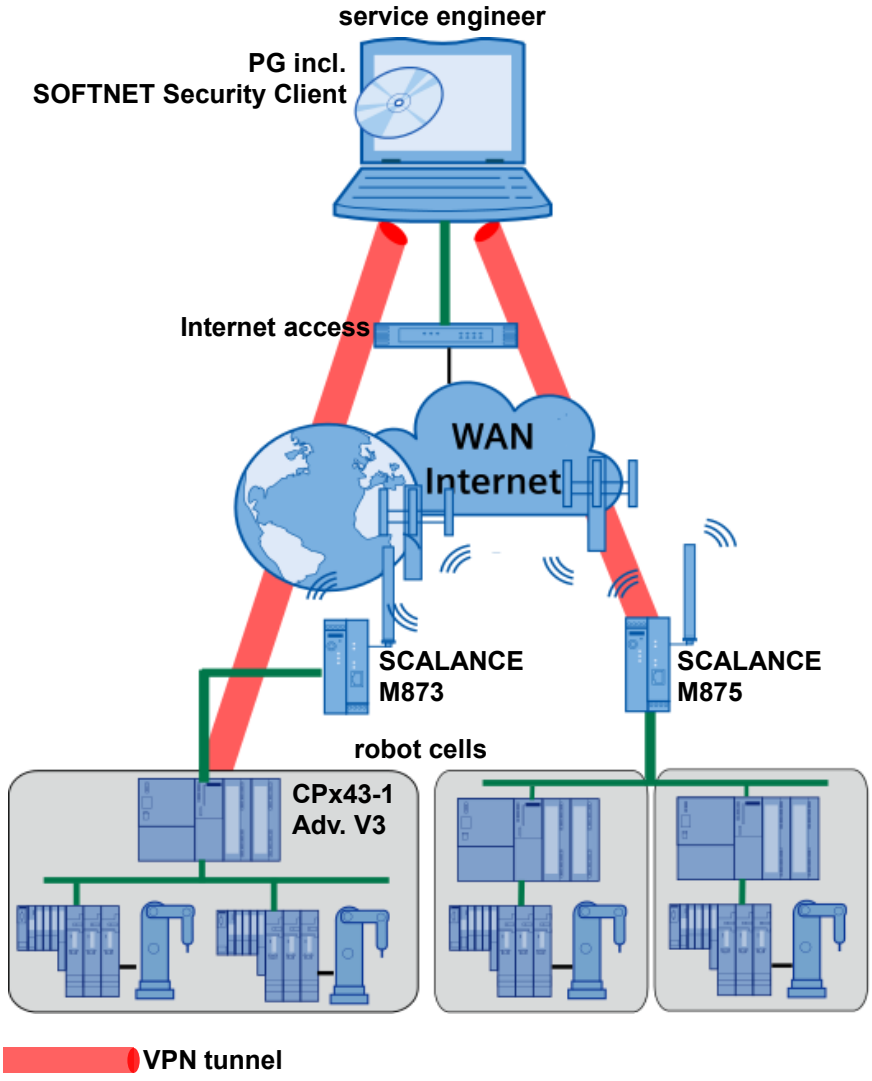
The SOFTNET Security Client is the active node in this configuration, i.e. it initiates the tunnel build-up to the SCALANCE S module or CP1628 / CPx43-1 Advanced V3 on the network side. The advantage is the fact that a service engineer can log on to the system from any location in the world without having to know his current IP address (**dynamic WAN IP address**).

The automation network comprises a SCALANCE S (S612, S623) or a CP1628 / CPx43-1 Advanced V3 which protects and terminates the IPSec tunnel. These modules are connected to the Internet via an appropriate access. The access point in the network is realized via a **static WAN IP address** or via a **registered FQDN** (Fully Qualified Domain Name) at a service provider for dynamic DNS (only in combination with SCALANCE S). Using this address or name, the SOFTNET Security Client can establish a connection to the peer on the Internet.

3.4.2 Access to a system accessible via the mobile phone network

Solution scheme

Figure 3-11



Description

If the system is located in a place that is hard to reach or if there is no DSL connection with a static IP address, the system can be connected via the mobile phone network. With this method, the following modules can be used on the service PC in combination with a SOFTNET Security Client:

- SCALANCE M875 UMTS router
- CPx43-1 Advanced V3 or CP1628
- SCALANCE S612 / S623 with SCALANCE M873 to access the mobile phone network

The SOFTNET Security Client initiates the tunnel build-up to the security modules on the system side. The service engineer can therefore log on to the system from any location in the world without having to know his current IP address (**dynamic WAN IP address**).

A SCALANCE M875, SCALANCE S612 / S623 or Security-CP V3 / CP1628 in connection with a SCALANCE M873 is integrated into the automation network as the peer to the IPsec tunnel.

These modules will dial into the mobile phone network and establish a connection to the Internet. The access point in the network is realized via a static WAN IP address or via a registered FQDN (Fully Qualified Domain Name) at a service provider for dynamic DNS (only in combination with SCALANCE S). Using this address or name, the SOFTNET Security Client can establish a connection to the peer on the Internet.

3.5 Secure data communication between system components

3.5.1 Data communication via Internet

Network topology

Figure 3-12

Fehler! Es ist nicht möglich, durch die Bearbeitung von Feldfunktionen Objekte zu erstellen.

Application

Plant components networked around the globe or remote access via WAN to single devices from a central station, e.g. for diagnosis, are quite common today. Exchanging sensitive manufacturing data, important production data, or confidential data, etc. among plant components and/or with the central station are part of everyday routine. Secure communication is therefore essential.

Problem

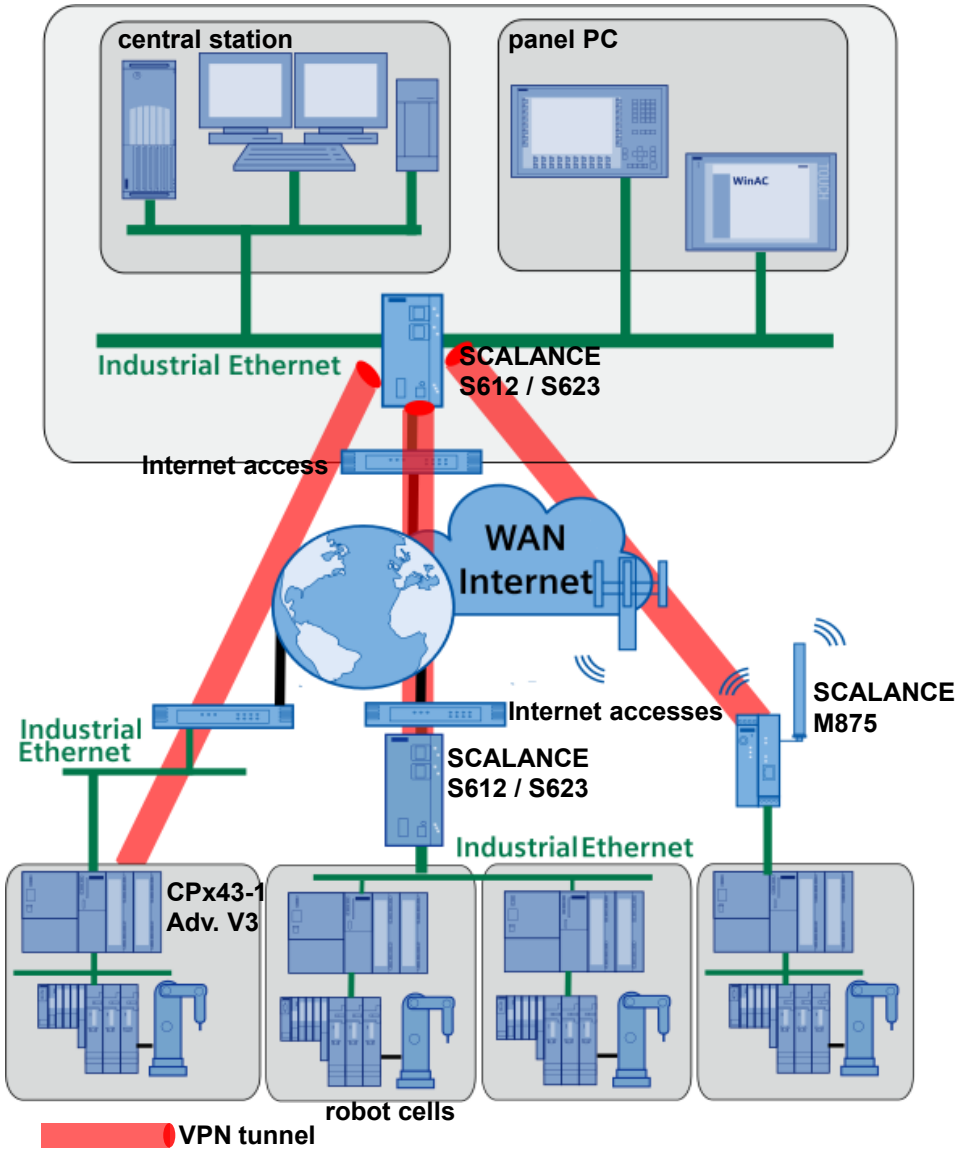
The Internet is an unsecure transmission channel:

- Incorrect PC settings and lacking security updates cause vulnerabilities, opening the way for viruses, trojans, or worms.
- Non-encrypted data can easily be intercepted or manipulated.
- Data is temporarily buffered.
- Unnoticed hacker attacks from outside.

An unprotected internet connection can cause entire plant parts to be sabotaged or to fail.

Possible solution using SIMATIC NET components

Figure 3-13



Description

Static VPN connections are established to enable secure communication between distributed plants. To achieve this, each cell is equipped with one VPN-capable security module with internet access.

The following security modules are suitable for this scenario:

- Security Modules SCALANCE S (S612, S623)
- PLC-CPs (CPx43-1 Advanced V3) with security functionality
- PC-CP1628 with security functionality
- UMTS router SCALANCE M with security functionality

Through the Security Configuration Tool configuration software, all **security modules** will be configured such that they will represent the end points of a joint central security module.

One module in this configuration will be configured as an active node, i.e. it will initiate the tunnel build-up to the other SCALANCE S modules. The active module only needs a **dynamic IP address**.

The other modules are passive, terminating the IPSec tunnel for the automation network in which they are located. The access point will be realized via a static WAN IP address or via a registered FQDN (Fully Qualified Domain Name) at a service provider for dynamic DNS.

As the connection is being established, the active side will then establish a VPN connection to all modules configured as passive. After that, the individual networks/cells will behave as though they were part of a common network.

This means that FTP connections, for instance, can be parameterized and operated as usual. Furthermore, a service engineer can connect to one of the cells in order to access all devices in this cell (e.g. for diagnosing devices using NCM).

The following table shows the possible VPN combinations for the use of the security modules:

Table 3-1

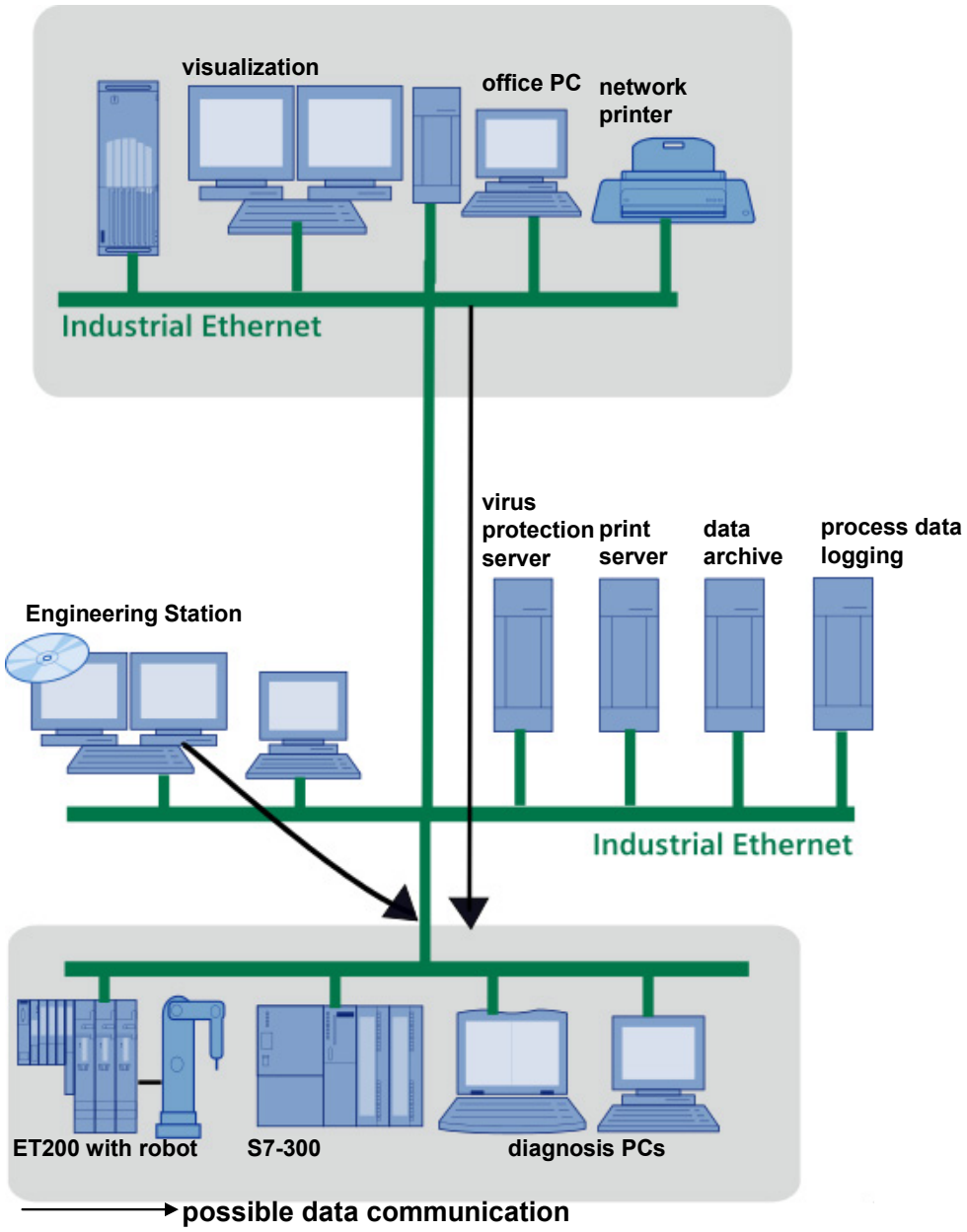
		Passive		
		SCALANCE S612 / S623	**CPx43-1 Advanced V3 / CP1628**	**SCALANCE M875**
Active	**SCALANCE S612 / S623**	OK	OK	OK
	CPx43-1 Advanced V3 CP1628	OK	OK	OK
	SCALANCE M875	OK*	OK	OK*

* dynamic DNS names can be used.

3.5.2 Data communication via LAN

Network topology

Figure 3-14



Application

In an up-to-date company network, the office and automation networks are interconnected.

Exchanging sensitive manufacturing data, important production data, or confidential data, etc. between the automation network and the central station is part of the daily routine.

Problem

If the connection of the two networks is not secured, confidential production data might be transmitted to the office network without being controlled and might be viewed or modified by third parties.

Possible solution using SIMATIC NET components

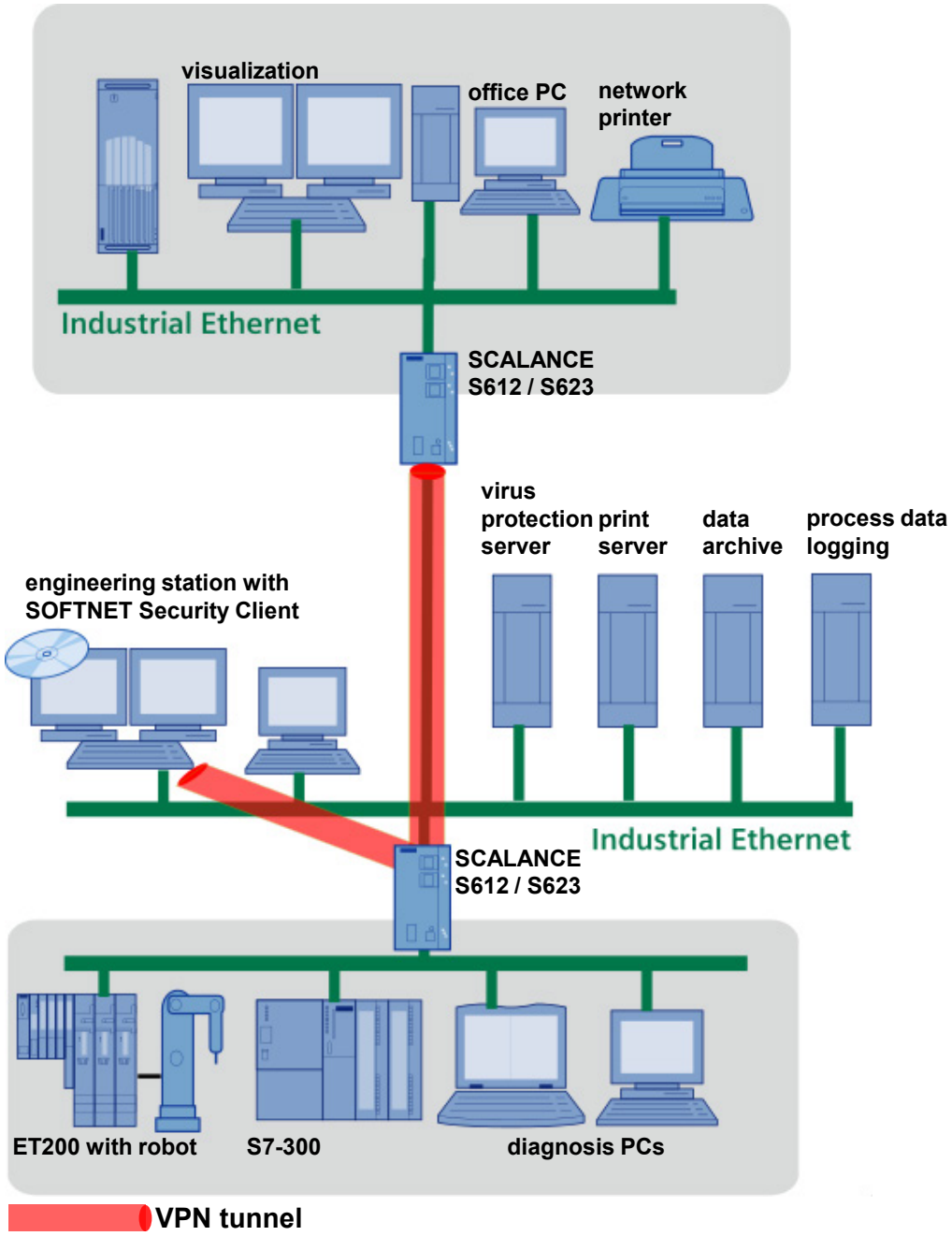
There are two possible solutions:

- Protection through a secure communication channel.
- Protection through DMZ.
- Protection through a firewall for regulating data traffic (see chapter 3.1.2 and 3.2).

3.5.2.1 Protection through a secure communication channel

Solution scheme

Figure 3-15



Description

Communication between the automation cell and the central station is accomplished via an exclusive corporate network. Static VPN connections are established to enable secure communication. For this purpose, each site has a VPN-capable security module.

The following security modules are suitable for this scenario:

- Security Modules SCALANCE S (S612, S623)
- SOFTNET Security Client software
- PLC-CPs (CPx43-1 Advanced V3) with security functionality
- PC-CP (CP1628) with security functionality

Through the Security Configuration Tool configuration software, all **security modules** will be configured such that they will represent the end points of a joint VPN tunnel.

One module in this configuration will be configured as an active node, i.e. it will initiate the tunnel build-up to the other modules.

The other modules are passive, terminating the IPSec tunnel for the automation network in which they are located.

As the connection is being established, the active side will then establish a VPN connection to all security modules configured as passive. After that, the individual networks will behave as though they were part of a common network.

This means that S7 connections, for instance, can be parameterized and operated as usual. Furthermore, a service engineer can connect to one of the cells in the network in order to access all devices in this cell (e.g. for diagnosing devices using NCM).

The following table shows the possible VPN combinations for the use of the security modules:

Table 3-2

		Automation cell	
		SCALANCE S612 / S623	**CPx43-1 Advanced V3**
Company network	**SOFTNET Security Client**	OK*	OK
	CP1628	OK	OK
	SCALANCE S612 / S623	OK	OK

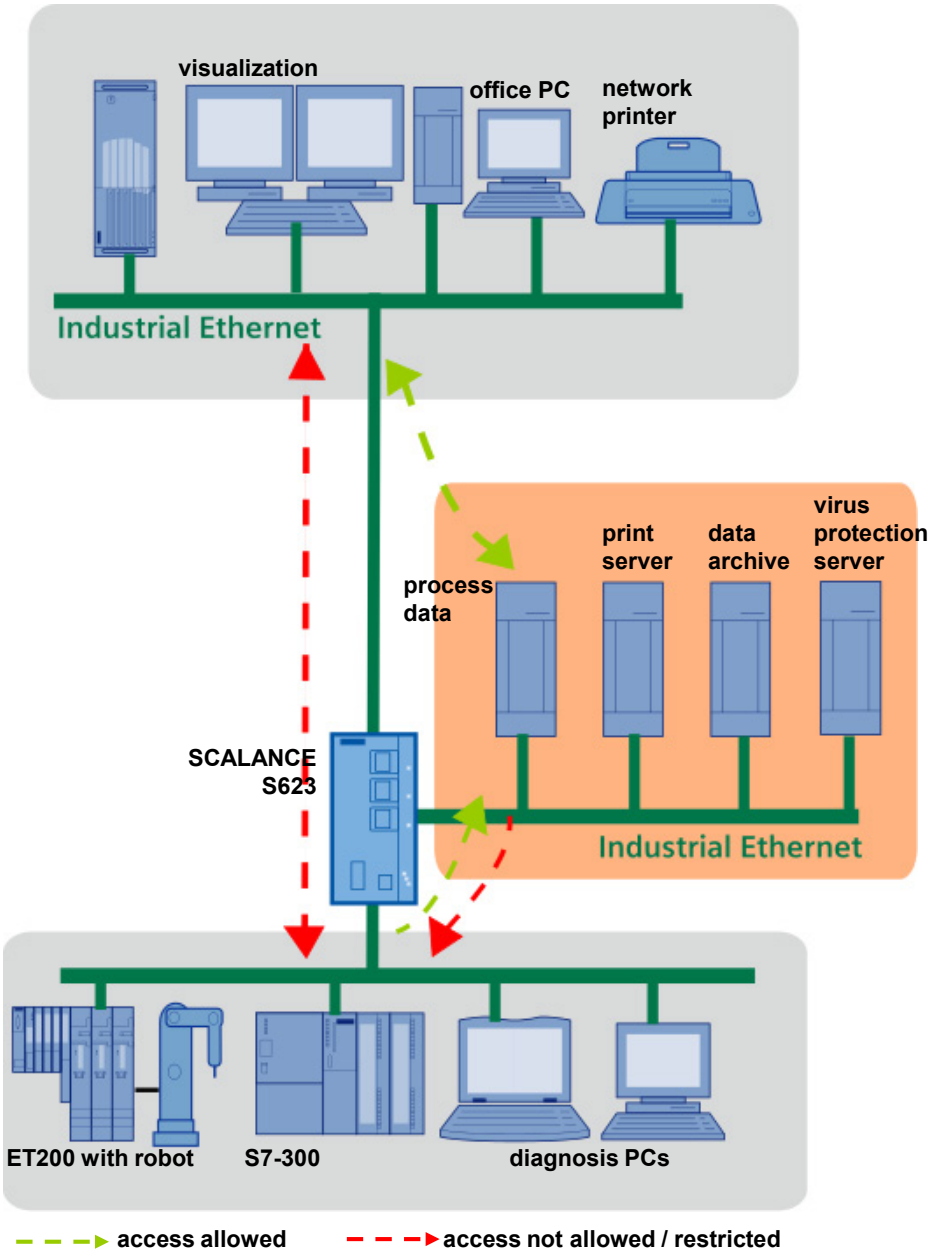
* dynamic DNS names can be used.

The difference to the "Node restriction on S7 controllers" scenario (chapter 3.1) is that in this case an entire automation cell is protected against unauthorized access via the VPN tunnel and not one S7 controller only is protected via the CP. The data transmitted via the tunnel are encrypted.

3.5.2.2 Protection through DMZ

Solution scheme

Figure 3-16



Description

With its three network connections, the SCALANCE S623 provides the possibility of establishing a demilitarized zone and physically separating the different networks (external, internal, and DMZ).

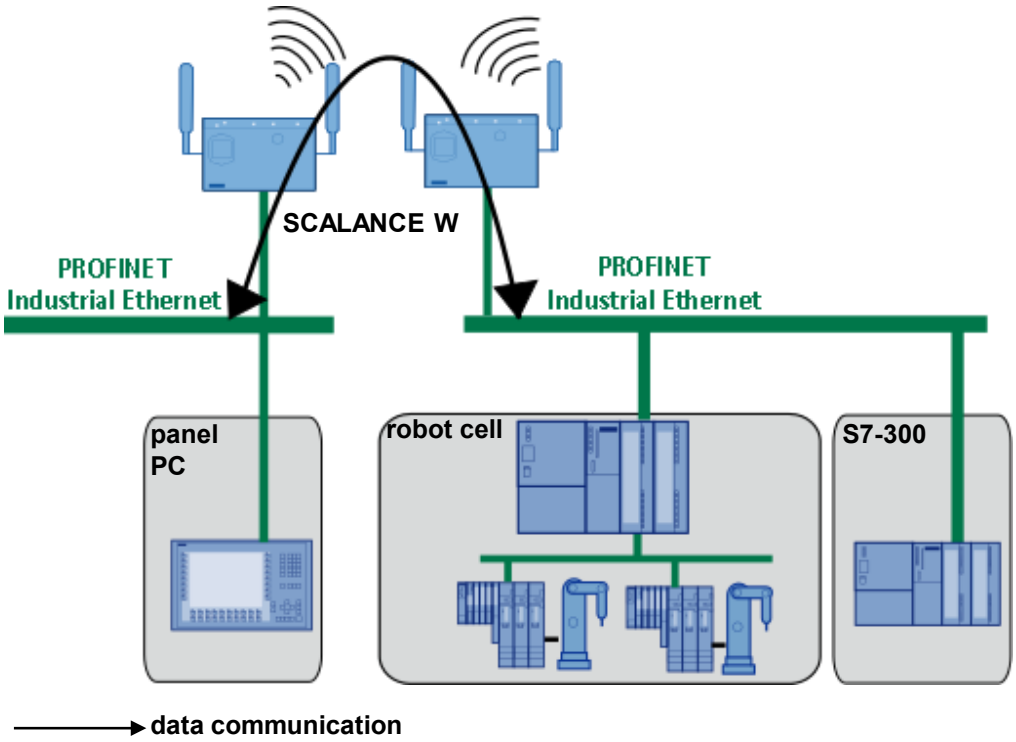
Network nodes, that should be accessible both from the internal and the external network, will be integrated into the DMZ and will thus be isolated against other networks. This controlled separation enables the network nodes to access required

data even though they have no direct access to the single devices within the protected automation cell (internal network).
The separation follows defined firewall rules.

3.6 WLAN scenarios with SCALANCE W

Network topology

Figure 3-17



Application

Plant components which are difficult to access or areas where extreme conditions prevail (high temperature, rough environment etc.) are connected via a radio field. Secret, sensitive data is exchanged via industrial wireless LAN. Data security aspects shall also be taken into account for this type of transmission.

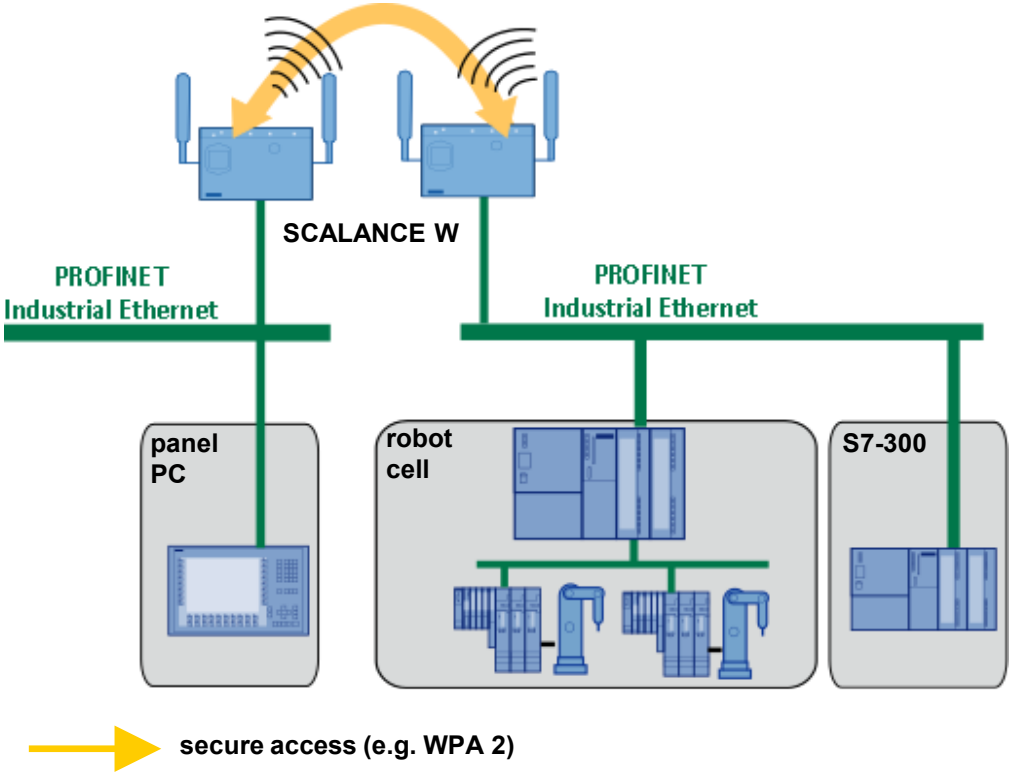
Problem

The radio network does not provide any protection features against unauthorized access. An unprotected radio network bears the risk that unauthorized persons can log on to the WLAN and sabotage other terminal equipment.

To ensure data security, the WLAN components must have appropriate protection features.

Possible solution using SIMATIC NET components

Figure 3-18



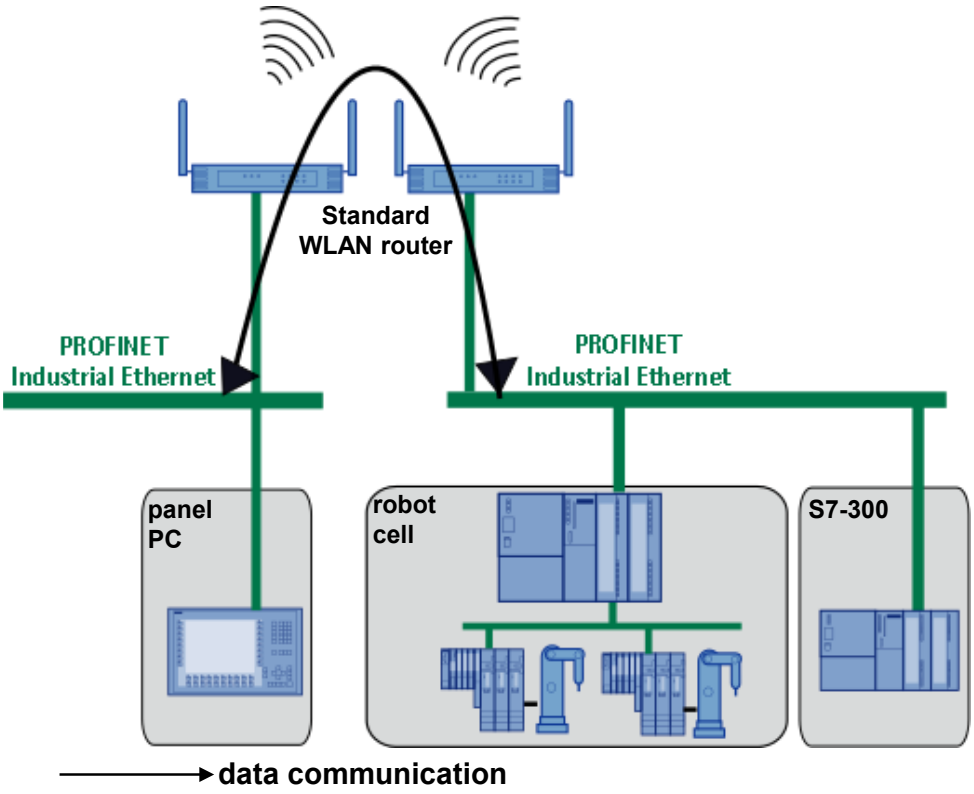
Besides their robust design, the **SCALANCE W** products also provide **effective mechanisms for data security**. Any data to be transmitted will be encrypted and thus protected against spying, interception, and manipulation.

The access points and WLAN clients will be configured via the web-based management.

3.7 WLAN scenario with non-secure components

Network topology

Figure 3-19



Application

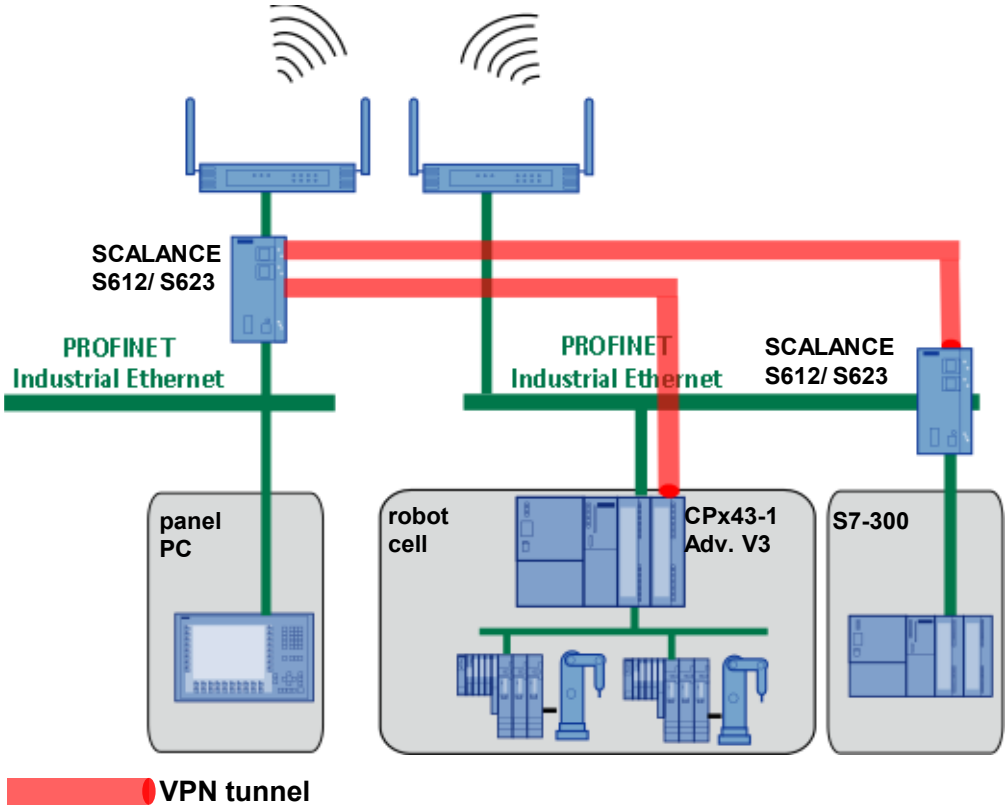
Not every WLAN infrastructure is equipped with the necessary security mechanisms. In most cases it is not possible to completely rebuild the WLAN infrastructure. Therefore, the security mechanisms must be retrofitted by extending the existing network. Data security aspects shall also be observed with an existing radio network.

Problem

It is not trivial to expand an existing radio network. It must be guaranteed that the new modules can be integrated without difficulty and without causing any disturbances. If this is not the case, the system might be unstable. As a consequence, all existing modules will have to be reconfigured, which implies additional costs and expenditure.

Possible solution using SIMATIC NET components

Figure 3-20



In order to create a protected and secure data link, a static VPN connection will be established between distributed plants, A security module (e.g. SCALANCE S612 or S623 or CPx43-1 Advanced V3) being additionally integrated in every subsystem.

The advantage of this proceeding is the fact that there is no need to reconfigure the already existing WLAN access points.

Through the Security Configuration Tool configuration software, the newly integrated security modules will be configured such that they will represent the end points of a joint VPN tunnel.

4 Basics and Principles

4.1 Basics of Ethernet and the IP protocol suite

4.1.1 OSI model (7-layer model)

The OSI (Open System Interconnection) model was developed by the International Organization for Standardization (ISO) and is the theoretical basis for data transmission in networks.

The model describes the way data is transmitted between two computer systems. Data transmission is divided into seven layers, each layer being assigned a certain task to fulfill autonomously.

Figure 4-1

7	Application layer
6	Presentation layer
5	Session layer
4	Transport layer
3	Network layer
2	Data link layer
1	Physical layer

Due to this modular design, specific program parts of individual layers can be exchanged as desired. This offers the possibility to develop programs which are independent of the hardware used, which is a considerable advantage over a monolithic solution.

For instance, it is possible to communicate with another computer via WLAN, via a modem connection, via the serial interface, or via industrial Ethernet using the same TELNET application.

The TELNET program (OSI Layer 7) operates independently of the physical line. It merely passes the data packets on to the TCP layer (OSI layer 4) or receives data packets from this layer.

4.1.2 System addressing (MAC and IP address)

Every network node of an IP-based Ethernet network is characterized by

- its unique MAC address specified by the hardware and
- an IP address assigned to it.

A subnet mask provides the information about the address range of its IP subnet.

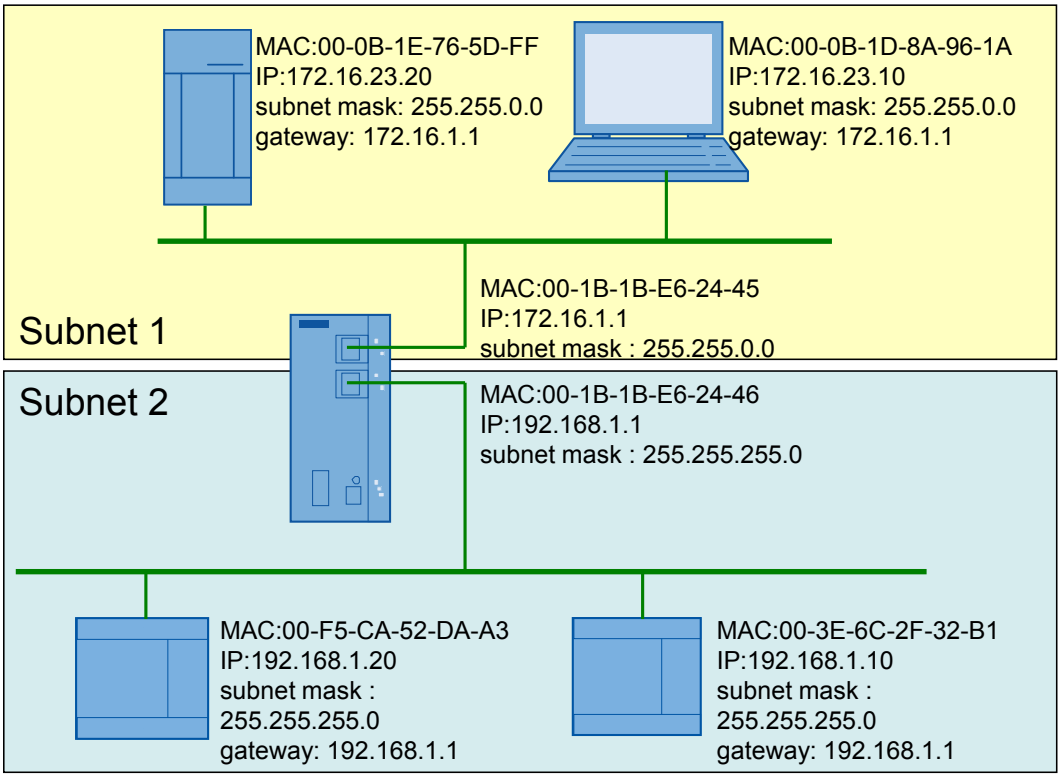
If several subnets are defined in a network, the node is also informed about which addresses (systems) to use in order to reach the network nodes in other subnets.

These systems located at the subnet transitions are referred to as routers.

The following components from the SCALANCE product range can be used as routers:

- SCALANCE S modules (S602, S612, S623)
- SCALANCE X414-3E as layer 3 router

Figure 4-2



4.1.3 Address resolution with ARP

The Address Resolution Protocol (ARP) maps a MAC address to an IP address. Every network node has its table with this mapping. The following table shows an example of the ARP address resolution:

Table 4-1

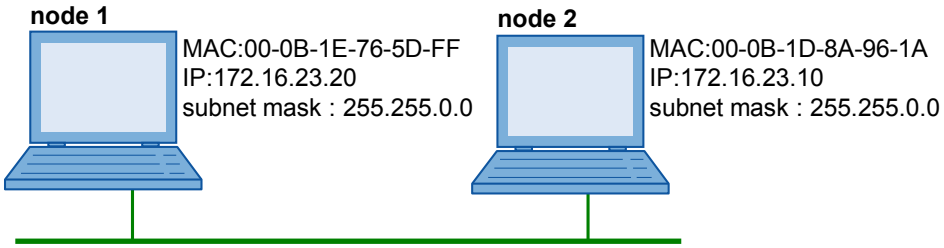
IP Address	Mac Address	Type
146.254.249.1	00-07-b4-00-00-02	dynamic
146.254.249.2	00-09-7b-9e-f1-8a	dynamic
146.254.249.3	00-09-7b-e0-a0-0a	dynamic

All assignments learned via the ARP are saved as ‘dynamic’. It is also possible to define ‘static’ entries manually.

Example 1: Address resolution in the same subnet:

Node 1 wants to send data to node 2:

Figure 4-3



Process:

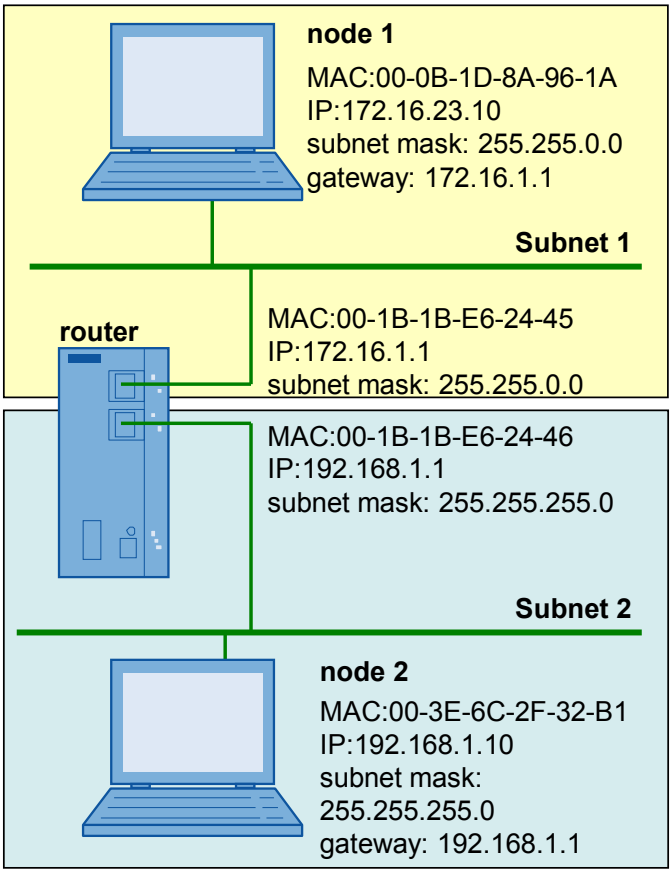
Table 4-2

Step	Functional sequence
1.	Node 1 sends the following to all others in the subnet (via broadcast address 172.16.255.255): "Who has IP address 172.16.23.10?"
2.	Computer 2 identifies this to be its IP address and responds: „The MAC address to 172.16.23.10 is 00-0B-1D-8A-96-1A“.
3.	The connection between node 1 and 2 can now be established.

Example 2: Address resolution beyond subnet limits:

If node 1 wants to establish a connection to a system outside its own subnet, address resolution will be a bit more difficult since a router is installed at the transition between the subnets.

Figure 4-4



Sequence

Table 4-3

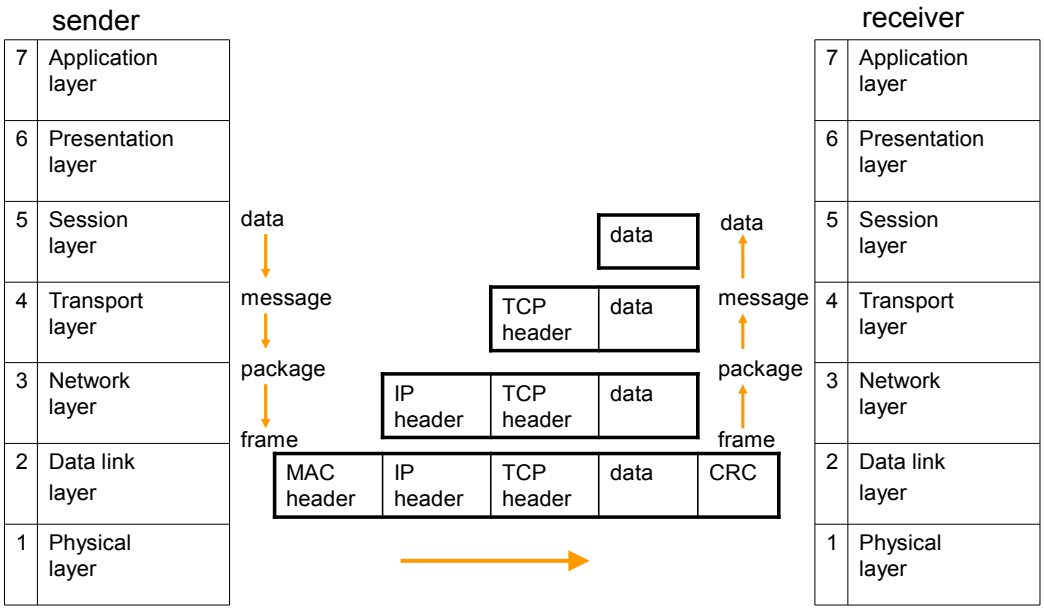
Step	Functional sequence
1.	From the combination of its own IP address and subnet mask, node 1 realizes that node 2 is located in a different subnet.
2.	The routing table of node 1 includes an entry specifying that the subnet in which node 2 is located can be reached via IP address 172.16.1.1.
3.	Node 1 therefore sends the following ARP request to 172.16.1.1: "Who has IP address 172.16.1.1?"
4.	Node 1 receives the following response from the router: "MAC address to 172.16.1.1 is 00-1B-1B-E6-24-45."
5.	Then node 1 sends the first packet intended for node 2 to the router (here: SCALANCE S602).
6.	The router identifies the data packet to be intended for node 2. Its routing table shows that it is directly connected to the corresponding subnet.
7.	Thus it sends an ARP request to the subnet of node 2: "Who has IP address 192.168.1.10?"

Step	Functional sequence
8.	Node 2 responds: "MAC address to 192.168.1.10 is 00-3E-6C-2F-32-B1."
9.	Address resolution in the reverse direction is done accordingly. In this case, however, node 2 requires an entry in its routing table that it can reach the subnet of node 1 via address 192.168.1.1.1.

4.1.4 Structure of a data packet

Data are transmitted in "packets". These packets are created by the relevant protocols in the individual OSI layers adding transmission-related information to the actual data to be transmitted. This additional information is referred to as header:

Figure 4-5



The individual headers, which the sending side adds when sending the data, are evaluated layer by layer on the receiving end until the data is available to the application at the top layers.

4.1.5 Formation of subnets and routing

The formation of subnets and routing, meaning data forwarding across subnet limits, are assigned to **OSI layer 3**.

The creation of subnets requires a subnet ID and a subnet mask. The lowest IP address is used as subnet ID. The number of IP addresses contained in the subnet from the subnet ID on is defined by the subnet mask.

Example:

A company consists of four manufacturing units with 30 controllers each. These units are to be mapped as subnets in one overall network. The overall network is assigned the address range 192.168.1.0 – 192.168.1.255:

Table 4-4

	Subnet ID	Address range network nodes	Broadcast address	Corresponding subnet mask
Unit 1	192.168.1.0	192.168.1.1 to 192.168.1.30	192.168.1.31	255.255.255.224
Unit 2	192.168.1.32	192.168.1.33 to 192.168.1.62	192.168.1.63	255.255.255.224
Unit 3	192.168.1.64	192.168.1.65 to 192.168.1.94	192.168.1.95	255.255.255.224
Unit 4	192.168.1.96	192.168.1.97 to 192.168.1.126	192.168.1.127	255.255.255.224

The highest IP address in a subnet (**192.168.1.31** for unit 1) must not be assigned to any network node. This address is referred to as **broadcast address** and is used as collective address for all IP addresses in the subnet. If data is sent to this highest IP address, then all nodes on the subnet are the receivers.

4.1.6 The TCP protocol

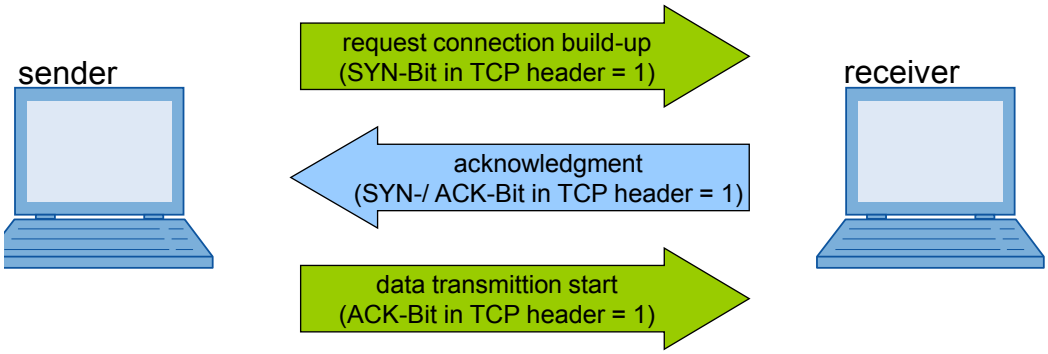
TCP as a part of the IP protocol suite is assigned to **OSI layer 4** (transport layer). Every TCP/IP data link has a sender and a receiver. In the IP protocol suite, TCP is a **connection-oriented** protocol that controls the data traffic and will take measures in the event of data loss.

The TCP's task is to split the data stream of the different applications, add a header and forward it for transmission to the Internet Protocol (IP) on OSI layer 3 (network layer). On the receiving side, TCP will sort the data and put them back together to a data stream. TCP will identify lost packets and request them again. On the transport layer, sending and receiving side are in permanent contact with each other. Although it is rather a virtual connection, control messages are exchanged continuously during data transmission. The Ethernet CP supports the socket interface (e.g. Winsock.dll) to TCP/IP that is available on virtually every end system (PC or external system) with the SEND/RECEIVE interface via TCP connections.

A TCP connection is established and closed using the 3-way handshake:

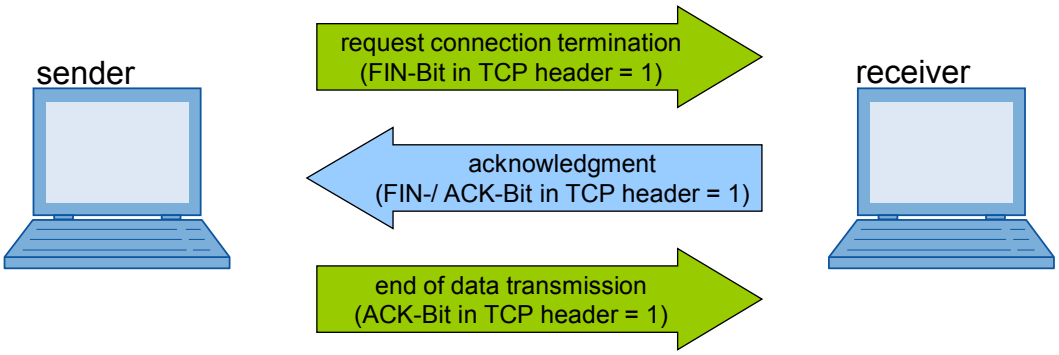
Establishing a TCP connection:

Figure 4-6



Closing a TCP connection:

Figure 4-7



4.1.7 The UDP protocol

As TCP, UDP is also assigned to **OSI layer 4** (transport layer). Unlike TCP, UDP is a **connectionless protocol**; it will not send acknowledgements for packets that have arrived. Some features such as data flow control or protocol-controlled re-requesting of lost data packets are omitted, making UDP faster. Therefore, UDP is better suited for data transmissions such as video streaming where lost data packets do not matter. UDP is also used as a simple transport protocol if higher-layer protocols (in OSI layers 5-7) carry out error-checking.

4.1.8 Port addressing

A port number, associated with an application or service, is included in every TCP or UDP data packet. This application or service will monitor the assigned port and will receive the data from TCP or UDP.

Port numbers start with 1 and are each assigned to a specific application up to number 1024. All higher port numbers - up to a maximum of 65535 - can be used freely by other programs.

Ports from 2000 on are available for STEP 7 connection configuration.

This port structure enables several applications to simultaneously establish connections to several communication partners via the network.

Application examples

The following table shows some examples for the assignment of an application to the corresponding port.

Table 4-5

Application	Transport protocol	Port number
FTP (data exchange)	TCP	20
FTP (control data)	TCP	21
SSH	TCP	22
TELNET	TCP	23
SMTP (e-mail)	TCP	25
DNS (name resolution)	UDP	53
HTTP	TCP	80
ISO_TSAP (SIMATIC Manager)	TCP	102
HTTPS (SSL)	TCP	443

4.2 Basic principles of wireless data transmission

The advantage of wireless data transmission is the fact that no physical lines are needed between the communication partners. It is therefore possible to remotely retrieve data from plants or production plants that are difficult to reach and where no fixed connection can be made, without big installation effort.

The system via WLAN / UMTS / GSM is maintenance-free (since there are no physical lines) and it can also be used in rough industrial environments without problems.

Wireless LAN (WLAN) is suitable for data transmission within a company network.

For data transmission via public networks, there are currently two systems to mention:

- Data transmission via GPRS or EDGE
- Data transmission via UMTS

The following chapters will explain how wireless communication works and the differences between the systems.

4.2.1 Wireless LAN radio technology

WLAN designates a radio technology according to the IEEE 802.11 standard. Data is naturally not transmitted via an Ethernet cable, but via radio waves in the 2.4 GHz or 5 GHz frequency range.

Until today, the IEEE 802.11 standard has continuously been developed, new versions being marked by additional lower-case letters (e.g. IEEE 802.11b).

Without much installation effort, WLAN offers more mobility, saves the wiring, and avoids system downtimes due to cable failures.

WLAN technology

WLAN is a network which actually replaces the Ethernet cable by radio communication. The most basic differences can be found on the physical layer (layer 1) since the data is transmitted through the air by means of electromagnetic waves, different modulation and encoding procedures being defined depending on the standard.

Data transfer rate with WLAN

The original standard IEEE 802.11 provides for data transfer rates of 1-2 Mbit/s. This standard has been further developed in order to meet the continuous demand for bandwidth. IEEE 802.11b already operates at 11 Mbit/s, IEEE 802.11a at up to 54 Mbit/s and as the next WLAN generation IEEE 802.11n at up to 600 Mbit/s.

4.2.2 Radio systems GPRS and EDGE

GPRS (General Packet Radio Service) and EDGE (Enhanced Data Rates for GSM Evolution) are mobile wireless technologies for fast data transmission and are based on the existing GSM network (**G**lobal **S**ystem for **M**obile Communications). They were developed mainly for accessing IP-based networks such as the Internet.

GSM technology

The frequency band of the GSM network is divided into several channels which in turn are split in eight cyclically recurring user channels (time slots). Payload can be transferred in these time slots.

The transmission of signals via defined frequency bands requires modulating (changing) the signals. In this case the useful signal to be transferred is multiplied with a carrier frequency. Through the modulation the useful signal is shifted to a higher frequency range.

GSM is connection-oriented, i.e. a continuous bearer channel (time slot) is reserved for the entire data transmission phase, irrespective of whether this channel is used for the data transmission or whether the entire capacity is used.

GPRS technology

GPRS is a packet-oriented procedure. For data transmission, no transmission channel is permanently reserved but it uses the free time slots of the GSM network in order to forward the packets through the network.

On the transmission side, the message is divided into individual packets, each including additional information (packet sequence, receiver address) and sent through the network independent of each other. The receiver's job is then to store the packets temporarily and to sort them in the correct order.

Different encoding procedures (coding schemes / CS) for error correction and different types of modulation are available for data transmission.

Data rate for GPRS

Several time slots can be combined with each other in order to obtain higher data rates during transmission. A maximum of five time slots are bundled for one device through the highest multi-slot class (class 12), i.e. a maximum of five channels in total can be used for uplink and downlink at the same time (e.g. 3 channels for uplink and 2 for downlink or 1 for uplink and 4 for downlink, see Table 4-6).

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

Table 4-6

Downlink	Uplink
1	4
2	3
3	2
4	1

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

On the one hand this is due to the fact that the number of parallel usable GSM channels varies depending on network load and capability of the mobile device. On the other hand, the data rate is adjusted to the quality of the radio network through channel coding (coding schemes). For GPRS, the data rate in the individual GSM channel is fixed to 13.4 kbit/s (CS2) as a standard.

EGPRS / EDGE

The **E**nhanced **G**eneral **P**acket **R**adio **S**ervice (also referred to as **EDGE**, **E**nhanced **D**ata **R**ates for **G**SM **E**volution) is an expansion of GPRS. EGPRS uses a different, more efficient modulation method (8-PSK) than GPRS does. This means that with EGPRS the data rate can be accelerated up to four times.

Data rate for EGPRS

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

In practice, however, this theoretical value is rarely reached. For EGPRS, most providers in Germany use the MCS8 coding scheme for modulation. For the MCS8 scheme the data rate per channel is fixed to 54.4 kbit/s.

The data rate naturally also depends on the network load and the capability of the mobile device.

4.2.3 The UMTS (3G) radio technology

UMTS (Universal Mobile Telecommunication System) is the European standard for the third generation of mobile communication and was developed to meet the requirements of both the users and the state of the art of modern communication. Apart from that, the intention with this new generation was to create an international uniform standard which could not be achieved with GSM.

UMTS technology

The transmission of playload with UMTS is based on the code division multiple access (CDMA) method.

The code division multiple access method is based on band spreading procedures aiming at extending (spreading) the required band width for the transmission of the information signal by means of a pseudo code. Using the same pseudo code, the receiver reconstructs the signal spread in the bandwidth.

Data rate for UMTS

UMTS is a cellular mobile communication system and is divided into three different zones. Each zone has different transmission speeds in the downlink. While a rate of 2Mbit/s can well be reached in the pico cell (building), the data rate in the micro cell (city) is 384 kbit/s, and in the macro cell (countryside) only 144 kbit/s.
With UMTS, data rates of up to 2 Mbit/s were predicted initially. The available data rates substantially deviate from these predicted values in rural areas; in these zones, due to poor network development, not even the EDGE data rates are reached.
The new standard HSDPA (High Speed Downlink Packet Access) promises to be a remedy in this case. The aim is to provide higher data rates to the nodes through better coding and more efficient load distribution.

4.3 Security mechanisms for wireless LAN

4.3.1 WEP (Wired Equivalent Privacy)

WEP is the oldest and, at the same time, the least secure encryption method to protect WLAN transmissions against unauthorized intruders according to the IEEE 802.11 standard.

With this method, users define a fixed key (password) when configuring the WLAN. The system of the WLAN component uses this key to generate a sequence of pseudo random numbers. Each character of the message to be transmitted is then encrypted with the next number from this sequence and decrypted by the receiver.

The method is relatively simple and can be compromised comparatively easily in two ways:

1. The key required for establishing the connection between sender and receiver is exchanged without encryption.
2. Statistical methods can be used to determine characteristics from the transmitted message traffic, which again allow drawing conclusions on the used key, as long as there is an adequate number of messages for the analysis.

For these reasons WEP is generally no longer considered to be adequately secure.

4.3.2 WPA (Wi-Fi Protected Access)

Since WEP was classified as unsecure and the development of the new encryption algorithm 802.11i by the IEEE task group was delayed, the 'Wi-Fi Alliance' recommended the application of WPA as a subset of the 802.11i standard as an interim solution.

WPA is the further development of WEP and is today still considered as a standard despite several weaknesses. Aside from technical changes of the actual encryption algorithm, the execution of the protocol was also adapted and additional functions were integrated:

- Passwords for the network access (authentication) can be stored on a central server ("RADIUS").
- The key for the message transmission changes dynamically, making statistical attacks more difficult.
- The MAC address (i.e. the unique hardware identification) of the sender is incorporated into the key, making it even more difficult to falsify the sender address of a message.

In the meantime, with the adoption of the 802.11i standard, this has become irrelevant and WPA2 or AES are available as the methods of first choice.

4.3.3 WPA2 und AES (Advanced Encryption Standard)

After adoption of the complete 802.11i standard, it was taken on by the “Wi-Fi Alliance” under the name “WPA2”. The essential difference between WPA2 and WPA is the encryption method: The weaknesses which were identified in the meantime in WPA no longer exist in the AES method used in WPA2.

The same as WEP, the “Advanced Encryption Standard” exercises the “adding up” of a key to the message. With this method, one block of the raw data is processed with the corresponding identical key, but several processing sequences each with varying block sizes take place.

If passwords are sufficiently long and complex, AES-encrypted messages will be relatively hard to decrypt with today’s technical capabilities.

4.3.4 EAP (Extensible Authentication Protocol)

EAP is a widely used framework for different authentication methods for network access. In other words, the actual EAP is not an authentication method but describes the mechanism according to which client and server can agree on a method.

One of the methods which can be used under EAP is “EAP-TLS” (“EAP-Transport Layer Security”), in which the network nodes have to be “certified” before they are authorized for the network communication, i.e. they must be authenticated at a central server. This method is comparable to SSL frequently used on the Internet.

4.3.5 MAC Filter

MAC addresses are codes for clearly identifying hardware elements (e.g. network cards, modules, motherboards, etc.) on a worldwide basis.

The addresses normally comprise 6 bytes (48 bits) and are “hard-wired” in the corresponding components; upon request, the components identify themselves by returning their MAC address.

In the network management, filter tables with MAC addresses can be created which allow or refuse access to specific addresses. That way a simple – even though comparatively unsecure – access protection can be implemented for the network.

It cannot be excluded that MAC addresses are manipulated (“spoofing”) so that MAC filters will only offer adequate protection for a network in connection with other measures.

4.4 Security mechanism: The firewall

A firewall is part of the security concept in the private and company sector which prevents or restricts unauthorized access to networks or devices. Firewalls are offered in form of a hardware component or are software-based.

4.4.1 Packet filter

From the historical point of view, packet filter firewalls are an expansion of network routers. Each router has two or more interfaces to connected networks and keeps tables about which networks are connected or available via which interfaces (routing tables).

It is quite easy to expand the routers in a similar way by sets of rules that specify whether or not the existing routers may be used by different IP packets. Routers make their routing decisions only on the link layer (layer 3) of the OSI protocol, requiring only the IP header of the packets to be analyzed so that the router can achieve sufficiently high transfer rates even with low-end hardware equipment. In a similar way, the filter mechanisms of a standard packet filter are kept comparably simple to be able to guarantee persistent transfer rates. This is why these packet filters only use information from the headers of the packets; they do not consider the data contents of the IP packets on higher protocol levels.

A well-equipped packet filter in a TCP/IP environment therefore makes its decisions based on the following parameters:

- IP addresses of sender and receiver
- IP protocol used
- TCP or UDP ports, provided that the IP packet transports one of these protocols
- IP and TCP flags, ICMP types
- the network interfaces through which the IP packet reaches the packet filter and maybe leaves it again

Not all packet filter implementations use all these parameters. The administrator determines a set of filter rules that remains static during operation. Each rule defines whether an IP packet is forwarded or not for a combination of the above parameters. When a certain IP packet is processed, the existing filter rules will check whether a rule applies to the packet parameters. If yes, the action defined in the rule will be executed (forward or block). If no filter rule matches the packet, a default setting will be activated (which should block the packet for security reasons).

A standard packet filter processes each IP packet individually. The decision about forwarding or blocking does not depend on which IP packets have been processed previously.

Many packet filters are implemented on the basis of routers. The bridging firewalls are an alternative to this. Their filter rules control the data traffic through a network bridge, i.e. on OSI layer 2. In terms of security they are almost identical to the packet filters on the routing level.

It might be considered a slight advantage that they are configured without an own IP address and are therefore not visible on IP level. From a network point of view they are useful if the connected network segments should not or cannot form autonomous subnets or if nonreactive integration is required.

4.4.2 Stateful inspection firewalls

The filter properties of a packet filter can be improved considerably if the IP packets are checked in their context. For instance, a UDP packet arriving from an external computer should only be forwarded internally if another UDP packet has been sent to that computer shortly before from within the network (e.g. in case of a DNS request of a client in the internal network to an external DNS server). To enable this, the packet filter must maintain records of all states to all current connections. Packet filters that are able to do this are therefore referred to as **stateful**. In case of TCP connections, they imitate the status monitoring of a complete TCP/IP protocol stack, and in case of UDP, they simulate virtual connections. Another important feature of a stateful inspection filter is its capability to dynamically generate and delete filter rules. In the above case, after the first UDP data packet has passed from inside to outside, a rule must be activated for a limited period of time which accepts the “response packet” and forwards it to the client. After the time window for the response has expired, this rule must be deleted again. The configuration is thus facilitated for the firewall administrator since some rule definitions do not have to be entered explicitly anymore. On the other hand, the firewall behavior is no longer fully under the administrator’s control.

Note The Stateful Inspection Firewall is implemented in all Siemens security modules.

4.4.3 Application gateways

This firewall type concentrates its monitoring functions on the application layer (OSI layer 7). There is a special proxy test program for each processed application protocol. It fully analyses the data stream of that application. This firewall type is therefore referred to as **proxy firewall**. In any case, a proxy verifies only compliance with the application protocol for which it was written. There are some further protocol-specific and configuration-dependent options:

- **Filtering protocol elements**

  Not everything defined in the application protocol may be allowed in the real application case. One example is the filtering of the PUT command in the FTP protocol if the addressed FTP server is not allowed to receive uploads.

- **Searching for malware**

  On the application layer, the data is available in a format that allows a standard virus scanner to check it for viruses, trojans, worms and other malware.

- **User authentication**

  In case the application protocol itself provides for a user authentication, this may already be requested by the proxy before the actually addressed server is addressed. An unauthorized user cannot reach the server in this case.

4.5 Security mechanism: The VPN tunnel

4.5.1 Virtual private network

Description

A VPN (virtual private network) is a private network that uses a public network (e.g. Internet) as a transit network for the transmission of data to a private target network. The private networks and the transit network do need to be compatible in this case.

VPN routers are required to establish a VPN.

Although VPN uses the addressing mechanisms of the carrier network it nevertheless uses its own network packets to separate the transport of private data packets from the others. This is why the private networks seem like common, logic (virtual) networks.

The tunneling concept

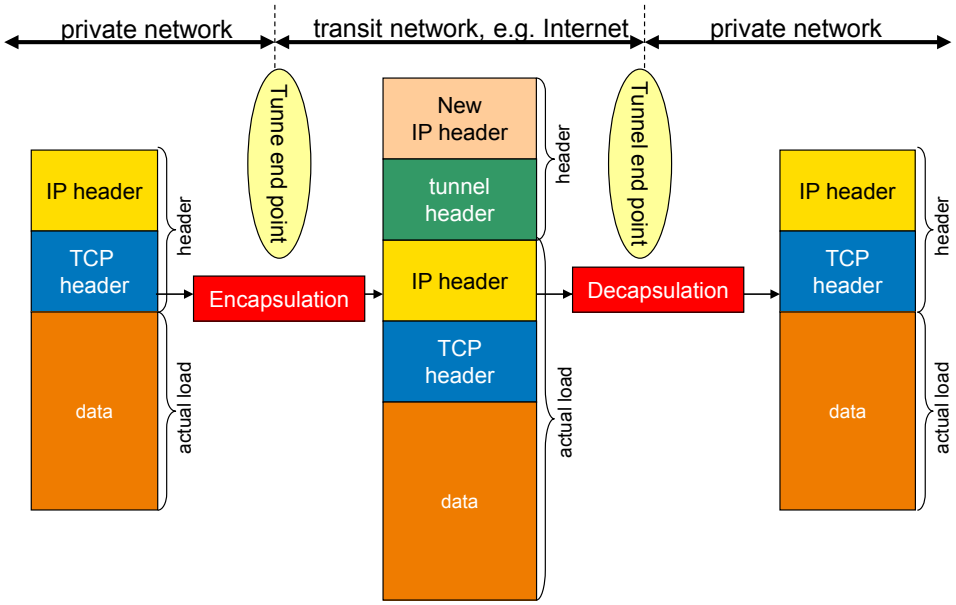
The tunneling concept is the basis of all virtual private networks. With this technology, data packets of a network protocol can be encapsulated as payload into the packets of a different network protocol (encapsulation) and transported via this network. This process creates an additional header that is placed in front of the original packet.

During forwarding, the original packet can also be encrypted, depending on the tunnel requirements.

There is a tunnel connection between sender and receiver, the tunnel end points.

The figure below shows the principle of the layer 3 tunneling:

Figure 4-8



4.5.2 IPsec security standard

Description

An important part of the data communication across network boundaries is IPsec (IP security). It is a standardized protocol suite and provides for manufacturer-independent, secure, and protected data exchange via IP networks.

IPsec is an extension of the IP protocol and thus located on layer 3 of the OSI reference model.

Targets

The main target of IPsec is protecting and securing data during a transmission via an unsecure network. All known weaknesses such as the intercepting and changing of data packets can be prevented by this security standard, through encrypted data packets, authentication and authentication of the nodes. The concrete tasks of IPsec are:

- Ensuring the authenticity of the packet (packet authentication)
- Protection against unauthorized and unnoticed changes to the data packets (data integrity)
- Confidentiality of the data packets transmitted
- Protection against replay attacks (prevents repeated receipt of the same data packet)
- Key management

IPsec architecture

The IPsec architecture is summarized in a compilation of different standards. These RFCs (request for comments) include regulations and rules on how a data packet can be converted into a protected packet and how it can be transformed back without any losses.

The most important RFCs for IPsec are:

- The IP authentication header (AH) is used for source authentication and identification and therefore ensures data integrity (RFC 2402).
- The Encapsulation Security Payload (ESP) encrypts the data and prevents unauthorized access (RFC 2406).
- The key management provides for data encryption (RFC 2407-2409, RFC 2412).
- The Security Association (SA) as an arrangement of the stations regarding the use of the same encryption techniques (RFC 2401).

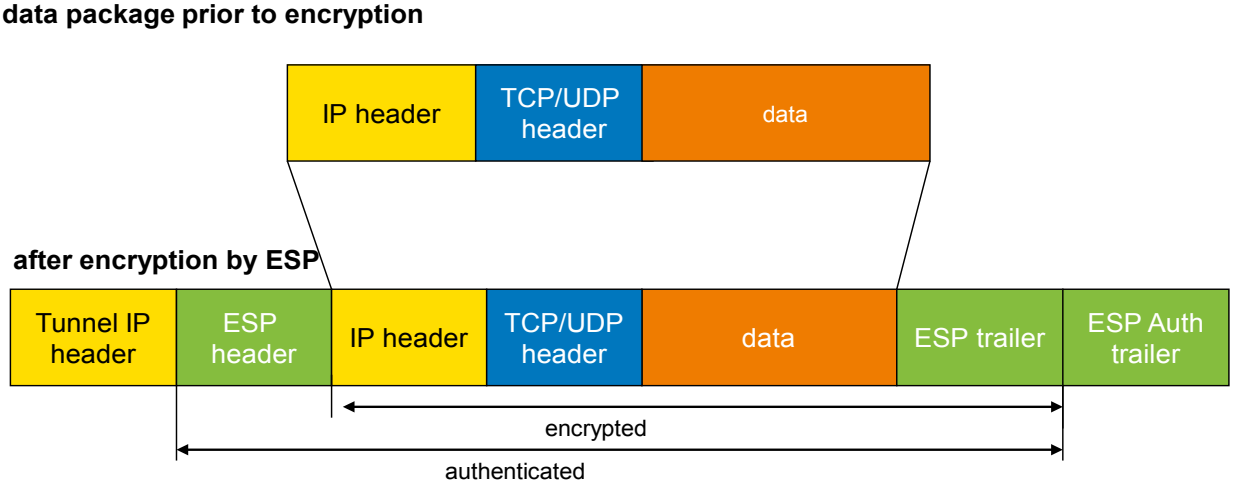
IPsec has a modular structure, this means that the most important components – the AH protocol, the ESP protocol, and the key management – can be used together as desired.

In addition two operating modes are specified for IPsec. They include regulations on which parts of the data packet must be protected.

- The transport mode is used if the cryptographic endpoints are also communication endpoints (computer-computer connections). Here, only the user load of the IP packet is protected but not the IP header.
- The tunnel mode is selected if the cryptographic endpoints are only used as security gateways and if remote subnetworks are interlinked via an insecure transit network. Special router or firewall systems can be security gateways.

In this mode, the entire IP packet is protected and inserted as user load in a new IP packet (see Figure 4-8). The original IP address cannot be viewed from outside anymore.

Figure 4-9



Significance and function of the individual segments:

Table 4-7

Segment	Function
Tunnel IP header	This IP header includes the address of the cryptographic endpoint (VPN gateway).
ESP header	The ESP is used to encrypt the original IP data packet and the ESP trailer. The ESP header provides protection against replay attacks and includes the SPI (Security Parameters Index).
ESP trailer	If the amount of user data to be transmitted is smaller than the block size, the ESP trailer adds the missing amount and stores the number of filled-in bits.
ESP authentication trailer	Includes the integrity check value for authentication and check of the integrity of the message.

Note

Restriction with IPsec

If IPsec is used for transmitting IP messages via a (layer 3) VPN tunnel of the security module, no VLAN tagging will be transmitted. The VLAN tags included in the IP messages will be lost when passing the security modules. IP broadcast or IP multicast messages cannot be transmitted through IPsec as a standard, either.

4.5.3 Key management

The reason for setting up an IPsec connection is the security requirements for data transmission. The AH and ESP IPsec protocols use cryptographic algorithms and security associations (SA), which require a key. They require all IPsec connection partners to have already exchanged the confidential identical keys and the key management to meet the following requirements:

- The keys and SA must apply to all used algorithms and cryptographic processes.
- SAs must be negotiated via a secure network.
- All requirements of the IPsec connection partners must be aligned.

Internet Key Exchange (IKE)

With the Internet Key Exchange (IKE), a key exchange process meeting the following requirements was specified:

- IKE specifies which protocols, algorithms, and keys will be used.
- It ensures key exchange, change, and renewal via a secure connection.
- Data transmission in the start and authentication phase is secure.
- All requirements of the IPsec connection partners are aligned.

IKE initiates two essential components:

- Internet Security Association and Key Management Protocol (ISAKMP; RFC 2408); ISAKMP controls the exchange processes between the two participating peers and defines the required messages for creating, negotiating and modifying security associations. ISAKMP only specifies the packet formats and the frame structure of how a key management is performed.
- Oakley protocol (RFC 2412) is a key exchange protocol and uses the key management procedures specified by ISAKMP.

The key exchange process is performed in two phases:

Phase 1 (main mode or aggressive mode)

In this phase no security services such as encryption, authentication and integrity check are available yet, since the required keys and the IPsec SA have not yet been created. Phase 1 serves for building up a secure channel for phase 2.

The communication partners negotiate an ISAKMP security association (ISAKMP SA) which defines the required security services (algorithms used, authentication methods). These secure the further messages and phase 2.

The SAs can be negotiated either in main mode or in aggressive mode.

The difference between the two variants is the number of messages to be exchanged and the encryption of the exchanged data.

Phase 2 (quick mode)

Phase 2 serves for negotiating the required IPsec SA. Similar as in phase 1, an agreement regarding the authentication methods, algorithms and encryption methods is made by mutual offering, in order to protect the IP packets with IPSec AH and IPSec ESP.

The message exchange is protected via the ISAKMP-SA negotiated in phase 1.

Through the ISAKMP security association negotiated in phase 1, the identity of the stations as well as the method for the integrity check is already given.

Preshared key and certificates

Keys are required for encrypting data. The ‘preshared key’ or the ‘digital signatures’ (certificates) method can be selected.

Preshared key

The use of a preshared key is a symmetric cryptosystem. Each station has only one secret key for decrypting and encrypting data packets. A common password is used for authentication.

Certificates

Using certificates is an asymmetrical cryptosystem, where each station has a pair of keys: one secret, private key and one public key of the peer. The private key allows for decrypting data, generating digital signatures and authenticating. The public key allows for encrypting data packets for the peer.

4.5.4 Key exchange techniques

Asymmetric techniques

The basic idea with asymmetric algorithms is to use a pair of keys. One key is for encrypting the message. This public key is accessible to everybody. The second key is for decrypting the message. This key must by all means remain secret (private key). These kinds of techniques are also referred to as public key algorithms. It is essential that the private key cannot be derived or calculated from the public key.

Symmetric techniques

With symmetric algorithms, the same key is used for encrypting and decrypting on both sides or keys are used for encrypting and decrypting that can be derived from each other. Symmetric algorithms have the advantage of being very fast and relatively easy to implement. The disadvantage is the distribution of the key material. The symmetry requires the key to be known to both the sender and the receiver. Since an algorithm is only secure if the information required for the encryption, i.e. the key, remains secret, that key has to be exchanged or negotiated on a secure channel prior to its use. If the key is revealed during this exchange, the entire encryption process is compromised.

Diffie-Hellman algorithm

The Diffie-Hellman algorithm is probably the best known method of exchanging key information. Named after the inventors Whitefield Diffie and Martin Hellman, it was first used in 1976. The aim of this technique is to generate a common key for sender and receiver for each security association. Both encryption parties agree on:

- a large prime number p
- a basis g, with 1<g<p.

The common key is generated by means of this information.

Summary

Symmetric and asymmetric techniques are often combined in practice to compensate for their disadvantages. A symmetric key is often used for the actual encryption of the data because it is very fast. Then an asymmetric procedure is used to distribute this symmetric key to all communication partners.

4.5.5 Initiating an IPsec VPN tunnel

The IPsec VPN tunnel

The designation ‘IPsec VPN tunnel’ or ‘IPsec tunnel’ includes three concrete statements:

- IPsec: To maintain the data integrity, data confidentiality and for authentication the data communication is secured via IPsec.
- VPN: logic, private connection between a sender and a receiver via an unsecure transit network.
- Tunnel: the layer 3 tunneling concept is used for data transmission. The logic connection between the communication partners can be compared with a tunnel.

At least two end devices that support IPsec and understand encapsulated data packets through layer 3 tunneling are needed for establishing an IPsec VPN tunnel.

VPN client and VPN server

A data communication secured via IPsec always starts with the negotiation of a preliminary Security Association (phase 1 of IKE), and continues in phase 2 with a final agreement on the algorithms, keys, etc.

The tunnel endpoint actively starting the negotiation of a Security Association is referred to as VPN client.

The peer waiting for the VPN client is referred to as VPN server.

4.6 Security mechanism: Address conversion with NA(P)T

Network Address Translation (NAT) / Network Address Port Translation (NAPT) are methods for converting private IP addresses into public IP addresses.

4.6.1 Address conversion with NAT

Description

NAT is a protocol for address conversion between two address spaces. The main task is the conversion of public addresses, i.e. into IP addresses used and routed on the Internet, into private IP addresses and vice versa.

Through the use of this technology the addresses of the internal network are not visible in the external network. In the external network, the internal nodes are only visible via external IP addresses defined in the address conversion list (NAT table).

The typical NAT is a 1:1 conversion, i.e. a private IP address is converted to a public one.

The target address for the internal nodes is therefore an external IP address.

NAT table

The NAT table contains the assignment of private and public IP addresses and is configured and managed in the gateway or router.

Sequence

If a device from the external network wants to send a packet to an internal device, it will use a public address as target address. This IP address will be compiled into a private IP address by the router.

The public IP address of the external device will remain unchanged as the source address in the IP header of the data packet.

The response of the internal device will be sent to the IP address which is stored as source address in the IP header. Due to the fact that its own and the source address are in different subnets, the internal device will send the packet to its router which will forward it to the external device.

4.6.2 Address conversion with NAPT

Description

NAPT is a variant of NAT and is often considered to be identical. The difference to NAT is the fact that ports can be converted also with this protocol.

The IP address is no longer converted 1:1. Instead, there is only one public IP address which is converted to a number of private IP addresses by adding port numbers.

The target address for the internal nodes is an external IP address with a port number.

NAPT table

The NAPT table contains the assignment of external ports to private IP addresses including port numbers and is configured and managed in the gateway or router.

Sequence

If a device from the external network wants to send a packet to an internal device, it will use the public address of the router with specified port as target address. Using the NAPT table, the router can assign and translate the external port number to a private IP address including port.

The public IP of the external device will remain unchanged as source address in the IP header of the data packet.

The response of the internal device will be sent to the IP address which is stored as source address in the IP header. Due to the fact that its own and the source address are in different subnets, the internal device will send the packet to its router which will forward it to the external device.

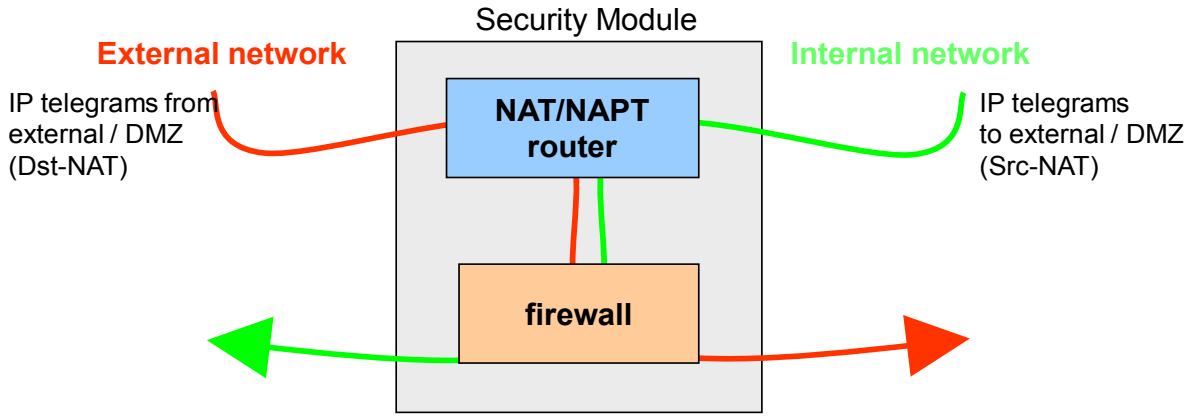
4.6.3 Correlation between NA(P)T and firewall

The use of NA(P)T and the firewall has been defined in the Siemens security modules as follows:

For the directions Src-NAT or Dst-NAT the messages must first pass the address conversion in the NAT/NAPT router and then the firewall.

The settings for the NAT/NAPT router and the firewall rules must be coordinated such that messages with converted address can pass the firewall.

Figure 4-10



If NA(P)T entries and firewall rules do not match, the security module will block the data packets which are not listed in any rule.

4.7 Basic principles of (secure) IT functions

4.7.1 File Transfer Protocol FTP

Description

The File Transfer Protocol is a specified network protocol for data transmission between an FTP server and an FTP client, or client-driven between two FTP servers.

FTP allows for exchanging data, creating and renaming directories, and also deleting them. The communication between FTP client and FTP server is an exchange of text-based commands. Each command sent by the FTP client results in a feedback by the FTP server in the form of a status code and a message in plain text.

For this purpose, FTP creates two logic connections: A control channel via port 21 for the transmission of FTP commands and their responses as well as a data channel via port 20 for data transmission.

With passive FTP, the two channels are initiated by the FTP client, with active FTP by the FTP server.

Solution for a secure FTP

To protect data during transmission, FTP also has the option of data encryption and authentication.

The easiest way of implementing a secure FTP connection is the Secure Socket Layer protocol (also called Transport Layer Security).
SSL (Secure Socket Layer) is located in the presentation layer of the OSI layer model. At the start of a connection, the data stream is encrypted with a key directly at the lowest bit level.

The SSL handshake protocol is used for identification and authentication of the nodes. The key for the encryption is negotiated using the public key technique, the FTP server sending a certificate with its public key to the FTP client. Prior to that, the public key belonging to the certificate must be certified by a certification body and by a digital signature.

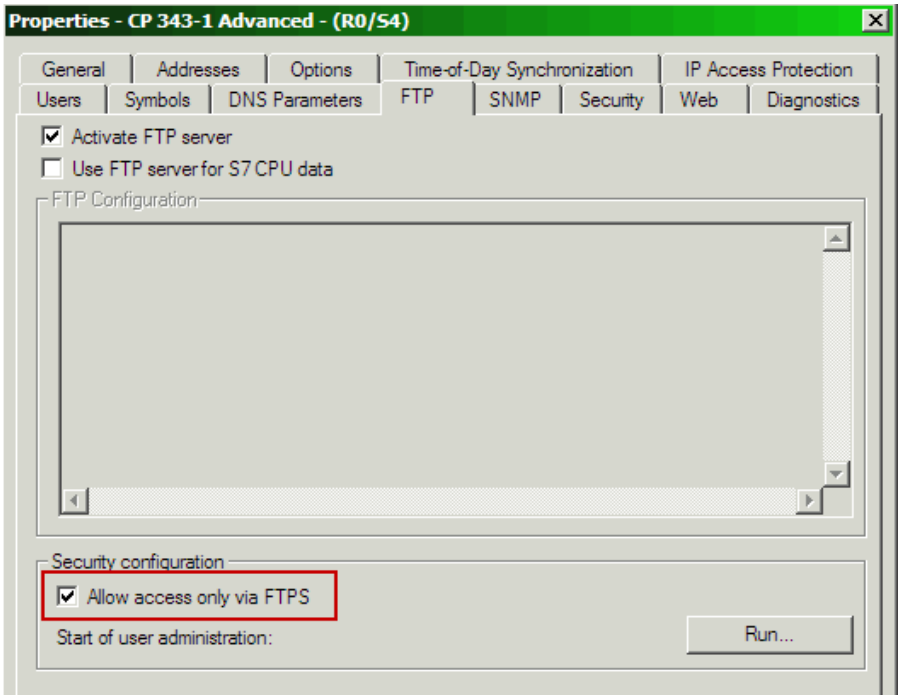
FTPES

The explicit FTP for secure data transmission is a combination of FTP and the SSL protocol and uses the same ports as in the normal FTP mode (port 20/21).

FTPES is supported by CPx43-1 Advanced V3. A certificate which is generated and delivered with the configuration of the security CP is used as the key for SSL.

Secure FTP data transfer with CPx43-1 Advanced V3 is only possible if the security function is enabled and is explicitly permitted in the configuration of the CP.

Figure 4-11



4.7.2 Network Time Protocol NTP

Description

The Network Time Protocol (NTP) is a standardized protocol for synchronizing the time on several computers / components across the network. The precision is within the millisecond range.

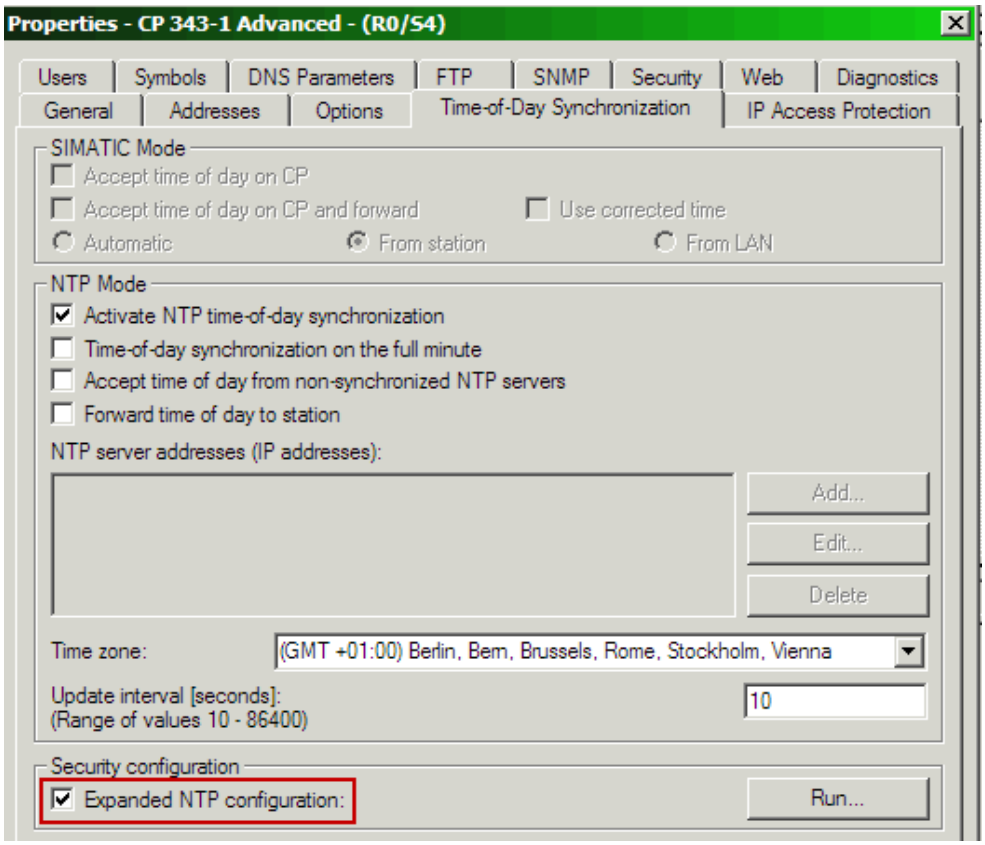
An NTP server makes the time available to the NTP clients.

NTP (secured)

NTP (secure) allows for secure and authenticated time synchronization by means of authentication methods and a joint encryption code. Both the NTP server and the NTP clients must support this function.

Secure time synchronization is supported, for example, by CPx43-1 Advanced V3 and CP1628, if the security function is enabled and NTP (secured) is explicitly permitted in the configuration of the CP.

Figure 4-12



4.7.3 Hypertext Transfer Protocol (HTTP)

Description

The Hypertext Transfer Protocol (HTTP) is part of the family of Internet protocols and is a standardized procedure for transferring data within a network. HTTP is preferably used for loading websites from a web server to a web browser.

HTTPS

Data transported via HTTP are readable as plain text and can be intercepted by third parties.

Today particularly – in the age of online banking, online shopping, and social networks – it is important that the transmission of confidential and personal data is secure and protected against unauthorized access.

The Hypertext Transfer Protocol Secure (HTTPS) is the easiest way of securely transmitting data.
HTTPS has the same structure as the HTTP protocol, but in addition uses the Secure Socket Layer Protocol for encryption.

4.7.4 Simple Network Management Protocol (SNMP)

Description

SNMP – **S**imple **N**etwork **M**anagement **P**rotocol – is a UDP-based protocol that was specified particularly for the administration of data networks and in the meantime has established itself also as a de facto standard for TCP/IP devices. The individual nodes in the network – network components or terminals – feature a SNMP agent that provides information in a structured form. This structure is referred to as MIB (Management Information Base). In the network node, the agent is usually implemented as a firmware functionality.

Management Information Base – MIB

An 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. Due to the cross-vendor standardization of MIBs and access mechanisms, even a heterogeneous network with components from different manufacturers can be monitored and controlled. If component-specific, non-standardized data is necessary for network monitoring, this data can be described by the manufacturers in “private MIBs”.

Sequence

A network management solution based on SNMP operates according to the client/server model. The management station (SNMP client) can poll information from the agents to be controlled that act as servers. The MIB information is called from the management station at cyclic intervals 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, the nodes can be monitored and instructions for controlling the devices can be given. This includes, for example, the activation or deactivation of a port on a network component. The communication between agent and network management station is performed in the background and is only an insignificant load for the network.

Secure SNMP (SNMPv3)

There are several versions of SNMP: SNMPv1, SNMPv2, and SNMPv3. The original version SNMPv1 and SNMPv2 are sometimes still used. However, it is recommendable not to use SNMPv1 and SNMPv2 since security mechanisms have not been implemented in these versions, or only in a restricted way.

From version 3, SNMP additionally offers user administration with authentication and optional encryption of data packets. Security with SNMP was substantially improved by these aspects.

Secure transmission of network analysis information can be configured, for example, with CP x43-1 Advanced V3, CP1628, and SCALANCE S V3.

5 SIMATIC NET products

5.1 SCALANCE product range

The SCALANCE product range includes various industrial Ethernet switches – active network components for use directly at the SIMATIC, as standalone devices, or plug-in communication processors with integrated switch for PC and SIMATIC.

The postfix after the “family name” stands for the application field. An "**X**" stands for "**switching**", the "**W**" for "**wireless**" and the "**S**" for "**Security**".

5.1.1 Industrial Switching – SCALANCE X

Figure 5-1

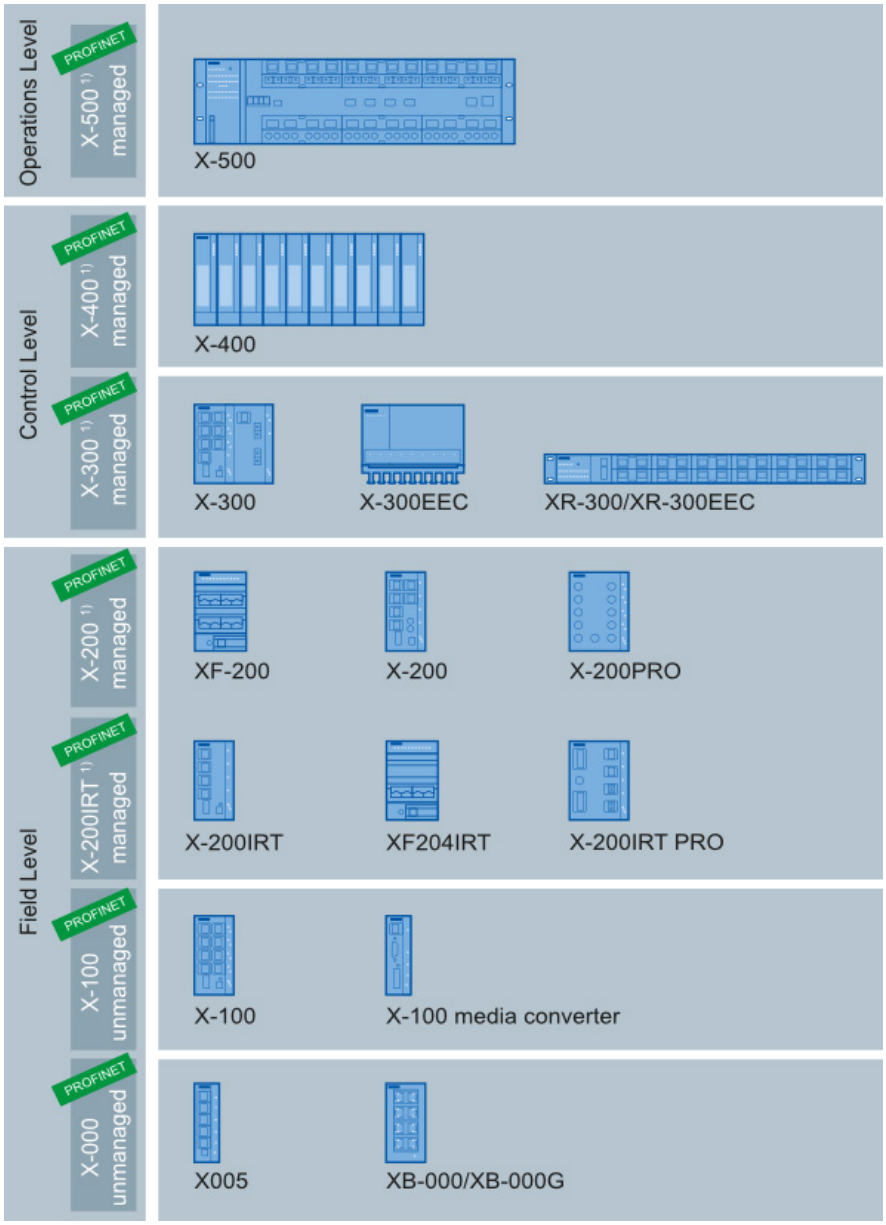
The **SCALANCE X** product range offers switches for industrial use. They are available in different performance categories, with an expanded performance spectrum for each stage. These devices offer the advantage that they were developed to match the specific requirements of automation environments, which is reflected, for example, in the extended temperature ranges in which the switches can be used. The housing, through its robustness, has also been adapted to the application environment. The devices are mounted either directly to the wall or on a top-hat rail, as required.

The individual mode levels are indicated by the number affixed to the “family name”. This number always has three digits. The hundreds digit indicates the

performance class. It can be between 0 (lowest performance class) and 5 (highest performance class). The tens digit and ones digit reflect the number of electrical ports. The designation SCALANCE X224 therefore describes a switch of performance class 2 with 24 electrical ports.

The following table shows the position of SCALANCE X products in the automation environment:

Figure 5-2



Switches of performance classes 3 to 5 only are suitable for safety-relevant functions. The difference between the 300 and 400 / 500 switches is that the 400 / 500 series has a modular design whereas the 300 products have a compact design.

5.1.2 Industrial Wireless LAN – SCALANCE W

Figure 5-3

The Industrial Wireless LAN (IWLAN) components are a mobile solution for new applications up to the field level. The products offer a unique combination of reliability, robustness, and safety.

The industrial use of wireless technology requires particularly reliable connections. A modulation that is disturbance-tolerant has been taken into account in standard 802.11 b/g, a, and n. The data rate is reduced in defined steps to maintain the wireless connection even over greater distances or with reflections on metallic objects. This is all part of the IEEE 802.11 standard with data rates of up to 600 Mbit/s and frequencies of 2.4 GHz and 5 GHz.

In addition, Industrial Wireless LAN from SIMATIC NET offers an expansion of the standard which provides selected nodes a defined data rate. This enables deterministic data traffic on the basis of the shared medium wireless LAN. IWLAN supports the selected monitoring of the connection of a node to the access point in order to initiate immediate counter-measures in the event of the connection being cancelled or the radio cell being left.

Everyday use in a rough industrial environment requires **robust** products, especially if they are not installed inside control cabinets. Depending on the area of application, the IWLAN components of SIMATIC NET are ideally adapted to the environmental conditions:

- **Protection type IP65** applies to outdoor applications, with operating temperatures of -40°C to +60°C
- **Protection type IP30** applies to indoor applications, with operating temperatures of -20°C to +60°C.

All components meet the high SIMATIC requirements with regard to shock and vibrations. The connector design is **shake- and vibration-proof**.

Protection against unauthorized access and data encryption are requirements which are not only important for transmitting confidential data. Industrial Wireless LAN exactly follows the specifications defined by IEEE and WiFi in the 802.11 standard to enable a high level of interoperability. The new mechanisms from **WPA2 and an AES-based encryption** have eliminated the known security gaps of wireless LAN and WEP.

In the event of a fault, downtimes of network segments and connected industrial Ethernet nodes are eliminated through the use of a configuration plug (C-PLUG). The C-PLUG enables SIMATIC NET components to be exchanged quickly and easily without reconfiguration of the spare part.

5.1.3 Industrial Security – SCALANCE S

Figure 5-4

The hardware and software of the SCALANCE S product range form a security system that is sophisticated down to the smallest detail. It is tailored to the high demands of industrial communication.

The protection function of SCALANCE S is **to control** the entire **data traffic** from and to the cell. The security modules are simply placed upstream of the devices to be protected.

Security modules are capable of protecting **several devices simultaneously**. This implies lower costs and significantly less configuration effort for the user.

The SCALANCE S modules were equipped with a number of functions for integrating the component into the cell protection concept.

- Protection of devices with or without independent security functions through the integrated firewall:
  - Check of the data packets based on the source and target address (stateful inspection firewall)
  - Supporting Ethernet “Non-IP” messages
  - Band width limitation
  - Global and local firewall rules
  - User-specific firewall rules
- Highest-level security with SCALANCE S612 V3 and S623: VPN and IPsec support enables secure data transmission via a quasi-dedicated line. The SCALANCE S612 V3 and S623 can be both server and client and can manage up to 128 VPN tunnels.
- Protection of several devices at the same time: Integrating the SCALANCE S as a connecting link between two networks will automatically protect the devices downstream.
  - Router mode to operate the SCALANCE S module in a routed infrastructure. The internal and external network is each a separate subnet.
  - Bridge mode to operate the SCALANCE S module in a flat network. The internal and the external network are located in a subnet.
- Flexible Internet access with SCALANCE S612 V3 and S623:
  - The two modules support both the configuration of a stationary IP address for the DSL access and the PPPoE.
  - They are dynamic DNS clients and can transmit their current IP address to a DNS server.
- Nonreactive integration of the SCALANCE S modules into an existing infrastructure with flat networks.
- Additional third port for SCALANCE S623 for connecting another network.

The SCALANCE S modules also support the following network functions:

- Address conversion with NAT/ NAPT
- DHCP server for IP address assignment in the internal network and DMZ (S623 only)
- Logging and evaluation of the log files via an external server
- SNMP for analyzing and evaluating network information

The configuration data is automatically saved on a C-PLUG. If a device needs to be replaced, it will only be required to take over the C-PLUG into the replacement device. Without reconfiguration, the replacement component will then start up with the same device configuration.

5.2 S7 communication processors

Compared to the basic components, the S7 communication processors (version 3 or higher) provide integrated security functions for protecting automation cells / networks against unauthorized access (Security Integrated).

5.2.1 CPx43-1 Advanced V3

Figure 5-5

The CPx43-1 Advanced V3 communication processors are components with “Security Integrated”. Apart from their communication functions, they also have integrated, specific security functions such as firewall and VPN functionalities.

The CPx43-1 Advanced V3 acts as its predecessor modules and was additionally expanded by the following security functions:

- Protection of devices with or without independent security functions through the integrated firewall:
  - Check of the data packets based on the source and target address (stateful inspection firewall)
  - Supporting Ethernet “Non-IP” messages
  - Band width limitation
  - Global and local firewall rules
- Highest-level security: VPN and IPsec support enables secure data transmission via a quasi-dedicated line. The CP supports the VPN server and the VPN client role. Altogether, the module can manage up to 32 VPN tunnels.

- Secured IT functions: Encryption and authentication guarantee secure data transfer (FTPS), web access (HTTPS), and time synchronization (NTP (secure)).
- Protection of several devices at the same time: Integrating the CP as a connecting link between two networks will automatically protect the devices downstream.
- Router functionality: The CP can be used for passing on IP messages from a local network (PROFINET interface) to a superior network (gigabit interface) and vice versa. The CP controls the access permission in accordance with the configuration.
- Protection of the controllers themselves.

The communication modules also support the following network functions:

- Address conversion with NAT/ NAPT
- IP Access Control Lists.
- Logging and evaluation of the log files via an external server
- SNMP for analyzing and evaluating network information
- Web diagnosis

5.2.2 CP1628

Figure 5-6

The integrated security mechanisms of the CP 1628 allow for the protection of computer systems including the associated data communication within an automation network or the secure remote access via Internet. The CP1628 grants access to individual devices or entire automation cells that are protected by security modules and enables secure connections via unsecure network structures.

The CP1628 offers the following security functions:

- Protection of devices with or without independent security functions through the integrated firewall:
  - Check of the data packets based on the source and target address (stateful inspection firewall)
  - Supporting Ethernet “Non-IP” messages
  - Band width limitation
  - Global and local firewall rules
- Highest-level security: VPN and IPsec support enables secure data transmission via a quasi-dedicated line. The CP supports the VPN server and the VPN client role. Altogether, the module can manage up to 64 VPN tunnels.
- Secured time synchronization (NTP (secure)).
- Protection of PC systems: Allows for secure communication without special settings of the operating system.

The communication module also supports the following network functions:

- Logging and evaluation of the log files via an external server
- SNMP for analyzing and evaluating network information

5.3 SCALANCE M875

Figure 5-7

The SCALANCE M875 is a UMTS router and can, owing to its integrated security functions, establish secured, wireless data connections to remote systems.

The SCALANCE M875 can be operated from any place where a mobile communication network is available that provides packet-oriented data services. Under UMTS, these are the HSPA Data Service or UMTS Data Service. Under GSM, these are the EGPRS or GPRS data services.

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

- Protection of devices with or without independent security functions through the integrated firewall. Example:
  - Check of the data packets based on the source and target address (stateful inspection firewall)
  - Anti-spoofing (faking an IP address/identity)
  - Port forwarding
- Highest-level security: VPN and IPsec support enables secure data transmission via a quasi-dedicated line. The SCALANCE M875 supports the VPN server and the VPN client role. Altogether, the module can manage 10 VPN tunnels.
- Radio modem for flexible data communication via UMTS, HSPA, EGPRS, or GPRS.
- Bidirectional data connection.
- Cyclic processing of protocol data for maintaining or monitoring the connection (NAT-T Keep Alive, Dead Peer Detection, Rx-Tx-Delay Trigger).
- Support of DNS and dynamic DNS names.

The module also supports the following network functions:

- Address conversion with NAT/ NAPT
- Web-based configuration user interface.
- Logging and evaluation of the log files
- Sending text messages from the local network
- Web diagnosis
- SNMP for analyzing and evaluating network information

5.4 SOFTNET Security Client

Figure 5-8

The SOFTNET Security Client is a PC software for secured remote accesses from PC / PG to automation devices.

The SOFTNET Security Client is used to automatically configure a PC /PG so that it can establish a secure IPsec tunnel communication in the VPN (Virtual Private Network) to one or several VPN servers.

That way PG /PC applications such as NCM Diagnosis or STEP 7 are able to access devices or networks in an internal, protected network via a secure tunnel connection.

6 List of Abbreviations

Table 6-1

Abbreviation	Description
AES	Advanced Encryption Standard
AH	Authentication Header
ARP	Address Resolution Protocol
C-PLUG	Configuration PLUG
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GHz	Gigahertz
GPRS	General Packet Radio Services
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IRT	Industrial Real Time
ISAKMP	Internet Security Association and Key Management Protocol
IWLAN	Industrial Wireless Local Area Network
LAN	Local Area Network
MAC	Medium Access Control
Mbit/s	Megabits per second
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NTP	Network Time Protocol
OSI	Open Systems Interconnection
RADIUS	Remote Authentication Dial-In User Service
RSA algorithm	Rivest Shamir Adleman algorithm
SCT	Security Configuration Tool
SSC	SOFTNET Security Client
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WEP	Wireless Encryption Standard
Wi-Fi	Wireless Fidelity
WPA	Wireless Fidelity Protected Access

7 References

7.1 Bibliographic References

This list is by no means complete and only presents a selection of related references.

Table 7-1

	Topic	Title
/1/	STEP7 SIMATIC S7-300/400	Automatisieren mit STEP7 in AWL und SCL (Automating with STEP7 in STL and SCL) Author: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-397-5
/2/	STEP7 SIMATIC S7-300/400	Automating with STEP 7 in LAD and FBD Author: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-296-1
/3/	STEP7 SIMATIC S7-300	Automating with SIMATIC S7-300 inside TIA Portal Author: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-357-9
/4/	STEP7 SIMATIC S7-400	Automating with SIMATIC S7-400 inside TIA Portal Author: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-372-2
/5/	STEP7 SIMATIC S7-1200	Automating with SIMATIC S7-1200 Author: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-355-5
/6/	SIMATIC NET Security	SIMATIC NET Industrial Ethernet Security Basics and Application Configuration Manual http://support.automation.siemens.com/WW/view/en/56577508
/7/	Getting Started	Configuring SIMATIC NET Industrial Ethernet Security Getting Started http://support.automation.siemens.com/WW/view/en/60166939
/8/	SCALANCE S V3	SIMATIC NET Industrial Ethernet Security SCALANCE S V3.0 Commissioning and Installation Manual http://support.automation.siemens.com/WW/view/en/56576669
/9/	SCALANCE M875	UMTS Router SCALANCE M875 Operating Instructions http://support.automation.siemens.com/WW/view/en/58122394
/10/	CP343-1 Advanced	System Manual Part B CP343-1 Advanced http://support.automation.siemens.com/WW/view/en/62046619
/11/	CP443-1 Advanced	System Manual Part B CP443-1 Advanced http://support.automation.siemens.com/WW/view/en/59187252

7.2 Internet Links

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

Table 7-2

	Topic	Title
\1\	Link to this document	http://support.automation.siemens.com/WW/view/en/27043887
\2\	Siemens Industry Online Support	http://support.automation.siemens.com
\3\	Security with SIMATIC NET	http://support.automation.siemens.com/WW/view/en/27043887
\4\	Setting up a Demilitarized Zone (DMZ) using the SCALANCE S623	http://support.automation.siemens.com/WW/view/en/22376747
	Protection of an Automation Cell using the Security Module SCALANCE S602 via Firewall (Bridge/Routing)	
\5\	Industrial Security with SCALANCE S Modules via IPsec VPN Tunnels (Configuration 4)	http://support.automation.siemens.com/WW/view/en/22056713
\6\	Secured Remote Access to SIMATIC Stations via Internet and UMTS	http://support.automation.siemens.com/WW/view/en/24960449
\7\	Industrial Ethernet Security	http://support.automation.siemens.com/WW/view/en/18701555/130000

8 History

Table 8-1

Version	Date	Modifications
V1.0	10/2007	First version
V2.0	01/2013	Integration of the new security modules Update and extension of the existing chapters