



Industrial Ethernet Handbook

- Design and planning
- Installation
- Commissioning

Foreword

Revisions

Version	Date	Modification
0.0	10/08	First release

Contact address



Weidmüller Interface GmbH & Co. KG
Postfach 3030
32720 Detmold
Klingenbergstrasse 16
32758 Detmold, Germany
Tel. +49 (0) 5231 14-0
Fax +49 (0) 5231 14-2083
E-mail info@weidmueller.com
Internet www.weidmueller.com

Contents

Foreword	3
Revisions	3
Contact address	3
Contents	4
1. Introduction	6
1.1 The goal of this usage guide	6
1.2 Your opinion is important to us!	6
1.3 Disclaimer	6
1.4 Weidmüller	7
1.5 Office Ethernet and industrial Ethernet	7
1.6 Explanation of symbols	9
2. Design Planning	10
2.1 Basic considerations for designing an industrial Ethernet network	10
2.2 Basic requirements and planning guidelines	15
2.3 EMC – Electromagnetic compatibility	16
2.4 Demands placed on generic communication cable facilities	18
2.5 EN 50174-2 Communication cable installation in IT	19
2.6 The MICE table	20
2.7 The capabilities of the cabling	21
2.8 Layout for generic cabling	22
2.9 Fire safety, thermal fire load and surge protection	25
2.10 Protocols (Ethernet)	26
2.11 Quality planning	27
2.12 Active components	29
2.13 Passive components for copper cabling	52

2.14	Passive components for fibre-optic cabling	58
2.15	Additional infrastructure components	62
2.16	STEADYTEC®	63
2.17	Important questions when planning your network infrastructure	64
2.18	Tender specification document	64
2.19	Planning checklist	65
2.20	Notes	66
3.	Installation	68
3.1	Installation guidelines	68
3.2	Cable routing	69
3.3	Connection methods	71
3.4	Labelling	88
3.5	Measurement and documentation processes	89
3.6	Installation checklist	90
3.7	Notes	91
4.	Initial Commissioning	93
4.1	Initial commissioning basics	93
4.2	Additional configuration and commissioning on the switch	102
4.3	Redundancy	113
4.4	Relay functions	113
4.5	Data backup	115
4.6	Network maintenance	115
4.7	Troubleshooting	116
4.8	Notes	117
	Glossary	119

1. Introduction

1.1 The goal of this usage guide

This usage guide is written for planners, installers, and commissioning contractors implementing industrial Ethernet (IE) networks. It contains tips, tricks and know-how for making your work easier.

This usage guide is not an IE compendium or reference document

1.2 Your opinion is important to us!

We have done our best to put the most helpful selection of our practical knowledge into this usage guide, without any intent of creating a complete reference. Is something missing? Please help us to improve this usage guide.

Send your expertise, opinion, tips, tricks or questions to ethernet@weidmueller.com.

1.3 Disclaimer

For the creation of this usage guide, all information was integrated to the best of our ability. However it is not possible to rule out deviations and we cannot be held liable for the complete consistency of this document. Moreover, we do not guarantee that the information provided is current, correct or complete.

1.4 Weidmüller

Weidmüller is the leading provider of solutions for electrical connectivity, transmission, conditioning and processing of power, signals and data in industrial environments. The company develops, produces and sells products in the field of electrical connectivity, functional electronics and communication electronics.

Weidmüller's product and service portfolio is dedicated to adding value to the products and thereby the business of our customers. The Weidmüller Group has a global focus with its own manufacturing plants, sales companies and representatives in over 70 countries.

1.5 Office Ethernet and industrial Ethernet

The importance of industrial Ethernet:

In comparison to Fieldbus systems, industrial Ethernet offers the following advantages:



- Integrated communication from the machine to the office
- No gateways are required when transmitting from the field level into the office
- Remote diagnosis and monitoring via an Internet connection
- Advantageous assignment of stations by means of virtual private networks (VPN)

Demands placed on Ethernet in office and industrial environments

	Office Ethernet	Industrial Ethernet
Cabling	<ul style="list-style-type: none">• Fixed building installation• Variable connection options• Pre-assembled connection cables• Star topology most widely in use	<ul style="list-style-type: none">• Individual, facility-influenced networks• Sturdy component characteristics• On-site, user assembled connections• Redundant network topologies (ring)
Transmission	<ul style="list-style-type: none">• Large volume of data• Mid-level network availability• Mostly only acyclic transmission• No real-time characteristics required for standard applications	<ul style="list-style-type: none">• Small data packets (measurement values)• Very high network availability• Mostly cyclic transmission• Extremely high real-time requirements
Environment	<ul style="list-style-type: none">• No extreme conditions	<ul style="list-style-type: none">• Extreme temperatures• Dust, dirt, splashing water, oils gases,• Electromagnetic fields• Risks of danger and damage from mechanical or chemical influences

1.6 Explanation of symbols

The following symbols are used in this usage guide to point out important text passages:

Symbol	Meaning
	This symbol indicates helpful advice and tips which can make your work easier.
	This symbol indicates the risk of malfunctions or errors. By following these notices, the risk of errors is minimized.

2. Design Planning

This chapter includes:

- Planning criteria, requirements and guidelines
- Demands placed on generic communication cable facilities
- Fire safety and surge protection
- Ethernet protocols
- Description of active Ethernet components
- Description of passive Ethernet components

2.1 Basic considerations for designing an industrial Ethernet network

2.1.1 Data and control networks

First determine if you are designing a data network or a control network.

Data network:

- Large volume of data
- Open connection to the office network
- The transmission times are relatively unimportant
- Functions normally with standard Ethernet protocols (TCP/IP)
- Availability and redundancy are focused on the server

Control network:

- Small volume of data
- Very limited connection to office network
- High real-time requirements
- Special network protocols (PROFINET, EtherNet/IP, Modbus/TCP, etc.)
- Availability and redundancy are critical for all network levels

2.1.2 External interface devices

Determine the terminal (end) devices and their access points (I/O modules, etc.)

- 1 Determine the number and placement of the I/O modules
- 2 Define the terminal devices: Exactly which devices are needed? And at what protection levels. IP20, 54, 67...?
- 3 Data volume of the terminal devices: this should be established now and then used to help determine the network devices
- 4 Define the interfaces to external networks
- 5 Define the interfaces to the Internet
- 6 Define the remote access methods (e.g., via modem)

2.1.3 Structure of the network

Determine the complete structure of the network. Components must then be matched to this structure.

Main and sub-networks

If necessary, sub-networks can be operated with reduced speed if data volumes are low enough. For example, the backbone line can run on Gigabit Ethernet while the sub-net runs at Fast Ethernet speeds.

Collision domains

Particularly for real-time applications, you must avoid collisions and the resulting time delays.

Address ranges

A defined addressing method from the office level usually already exists. This should be applied to maintain continuity. In order to avoid future difficulties, always coordinate your address range choices with the IT department.

Redundancy

Redundancy increases the availability of networks. Redundancy can refer to either the device or the cabling.

Device redundancy always requires specialized components. The requirements for this redundancy are always manufacturer-specific (proprietary) and cannot be found in any norm or standard.

Redundancy for cabling is more standardized. You can choose between the standard redundancy methods STP and RSTP, or manufacturer-specific methods such as RapidRing™.

You will need to determine:

- Which components will be redundantly networked
- The type of redundancy:
 - Standardized (STP, RSTP):
This method's advantage is that this process is supported by many managed switches. The disadvantage is that there are sometimes very long recovery times.
 - Manufacturer-specific (RapidRing™):
The advantage here is the significantly quicker recovery time.
The disadvantages are that these protocols are only supported by one or a few manufacturers and are not compatible with each other.

Determine the electromagnetic requirements (for example, according to MICE)

- Mechanical: mechanical shock, vibration, crushing, impact, bending, torsion
- Ingress: the penetration of dust and water
- Climate/Chemicals: ambient temperature, temperature fluctuations, air humidity, sun exposure, chemicals
- EMC: electromagnetic compatibility

2.1.4 Network devices

Define all infrastructure components according to their function and select those devices which you need.

- 1 Take all available electrical cabinets into consideration and define additional distributors if necessary.
- 2 Define the network access points and network compartmentalization (routers, modems, ...)
- 3 Define the coupling mechanisms: you should always plan for at least a 20% reserve of ports for future expansions.
 - Unmanaged switches
 - Managed switches
 - Uplinks
- 4 Define the WLAN access points:
 - WLAN bridges
 - WLAN access points and slaves
- 5 Integration of sub-systems:
 - COMServer
 - Gateways
- 6 Selection of devices according to customer specifications or user-group directives.
- 7 Calculate the power needs and determine the power supplies.

2.1.5 Network connection mechanisms

- 1 Determine the cable installation type:
 - Cable routing and channels
 - Additional measures to protect against mechanical damage
- 2 Determine the cable installation requirements:
 - Standards
 - Transmission speeds: the demands placed on shielding and the number of wires change as the transmission rate changes
 - Cable lengths
 - Electromechanical requirements (MICE): the requirements for cable cladding material and shielding come from the MICE
- 3 Determine the connector requirements:
 - Standards
 - Transmission speeds: the transmission speed is used to determine the required connector class (Cat. 5, 6) and thus also the connector type
 - Cable requirements: depending on the type of cable, certain connector requirements must be met (shield connection, outer diameter, and possible wire insulation and wire diameter)
 - Electromechanical requirements (MICE): this is used to determine the requirements for shielding and the protection class
 - Size
- 4 Determine additional connection components:
 - Jumper board
 - Media converter
 - Converter from solid to flexible conductors (e.g., mounting rail outlets)


2.2 Basic requirements and planning guidelines

Standard-compliant planning is the foundation which allows an Ethernet network to run smoothly and continually. This includes the determination of both the layout and the subsequent utilization.

- Be sure to follow the appropriate country-specific regulations (for safety, EMC).
- The regulations are EN 50173, pertaining to application-neutral cabling, and EN 50174, pertaining to communication cabling in general.
- Be sure to observe the minimum bending radius of the cable.
- Only make use of suitable cable installation systems.
- Copper communication cables must not be installed together with high-power cables. Observe the proper separating clearance distances, according to the EMC environmental influences (refer to EN 50174-2).
- Document the quality requirements by means of measurements and tracking, in accordance with the correct standards.

2.3 EMC – Electromagnetic compatibility

2.3.1 Equipotential bonding and earthing facilities

	<p>CAUTION! Electromagnetic interference</p> <p>An equipotential bonding mechanism which is in compliance with the latest standards is absolutely necessary for providing good EMC and, most importantly, adequate personal protection.</p>
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The requirements for equipotential bonding and earthing mechanisms are primarily described in:

- VDE 18014
Foundation earth electrode - General planning criteria
- VDE 0100 540
The construction of low-voltage facilities
- EN 50310 (VDE 0800 2 310)
Application of equipotential bonding and earthing in buildings with information technology equipment


2.3.2 EMC – general

In order to guarantee good EMC characteristics, you must select suitable materials and implement a proper, standardized layout. The following EMC-related standards are relevant for the operation of the facility:

- EN 55022 [13]
Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement
- EN 61000-6-1 [19]
Generic standards; Immunity for residential, commercial and light-industrial environments
- EN 61000-6-3 [20]
Generic standards; Emissions standards for residential, commercial and light-industrial environments




EN 55022, EN 61000-6-1 and EN 61000-6-3 pertain primarily to the operations of LANs.



	CAUTION! Electromagnetic interference
	<p>You should use fibre-optic cables in areas with high electromagnetic interference. Special POF (plastic optical fibre) or multimode cables with SC-duplex or SC-RJ plugs are available for this purpose.</p>

2.4 Demands placed on generic communication cable facilities


2.4.1 International standards

	Office buildings	Industrial
	ISO/IEC 11801	ISO/IEC 24702

2.4.2 German and European standards

	Office buildings	Industrial
 	EN 50173-1 together with EN 50173-2	EN 50173-1 together with EN 50173-3

2.4.3 Equivalent American standards

	Office buildings	Industrial
	Standards from the ANSI/TIA/EIA 568 series	

2.4.4 Structure of generic communication cable facilities

Primary area (campus distributor)

- Cabling connecting individual buildings at one location

Secondary area (building distributor)

- Vertical floor cabling

Tertiary area (floor distributor / machine distributor)

- Cabling to end user
- Cabling to or within a machine

2.5 EN 50174-2 Communication cable installation in IT

EN 50174-2 includes requirements for the planning and layout of cabling.

2.6 The MICE table

In compliance with EN 50173-1, the MICE table is used to show the environmental requirements for cabling. Environmental conditions are categorized as follows:

Mechanical	mechanical characteristics
Ingress	permeability characteristics
Climatic / Chemical	climatic and chemical characteristics
Electromagnetic	electromagnetic characteristics

Three levels of intensity are used as follows:

- 1 - Normally adequate for an office environment
- 2 - Normally adequate for a light industrial environment
- 3 - Adequate for a harsh industrial environment

	Class		
Mechanical	M ₁	M ₂	M ₃
Protection	I ₁	I ₂	I ₃
Climatic	C ₁	C ₂	C ₃
Electromagnetic	E ₁	E ₂	E ₃

M1 I1 C1 E1: office, foreman's office, office container
M3 I1 C1 E1: connections in closed electrical cabinet
M3 I3 C2 E3: connection in the field



Note that the MICE classifications are not applicable to special environments such as mining, petrochemicals, tunnels or pipelines.

2.7 The capabilities of the cabling

The classification of symmetrical copper cabling is described in both IEC 11801 and EN 50173. Up to now, classes A through F have been specified. In general the following principal can be applied: the higher the class, the better the transmission characteristics.

Typical transmission line classes for industrial applications

Class D - specifies up to 100 MHz;
commonly used transmission channel with capability for 100 Mbit/s or 1000 Mbit/s.

Class E - specifies up to 250 MHz;
transmission channel with capability for 100 Mbit/s, 1000 Mbit/s, and additional performance reserves.

Class E_A - specifies up to 500 MHz;
transmission channel with capability for 100 Mbit/s, 1000 Mbit/s, and 10 Gbit/s.

The advantages of Gigabit Ethernet

- Higher data rate and higher network performance
- Fully backwards compatible with a large number of installed Ethernet and Fast Ethernet nodes



An increasing number of 10-Gigabit components are currently entering the market at comparable prices as 1-Gigabit components. These components should be used to ensure your network remains sustainable in the future. Thus as the technology develops, high-bandwidth components for processing photo and video can be integrated into your networks.

2.8 Layout for generic cabling

Generic cabling can be constructed either by:

- The planning and determination of the component requirements (cable, connection mechanisms), or
- The use of standardized components.

2.8.1 Standardized components:

Standardized components are classified into quality categories (Cat.).

The typical categories for industrial applications are as follows:

- Category 5 – parameter specified to 100 MHz
- Category 6 – parameter specified to 250 MHz
- Category 6_A – parameter specified to 500 MHz

Comprehensive implementation of components from:

- Category 5 results in Class D
- Category 6 results in Class E
- Category 6_A results in Class E_A



When combining categories, the following is valid: The components with the lowest category determine the class of the connection or network.

2.8.2 Line lengths with copper cabling

When using components which comply with the minimum requirements for standardized components, it is possible to have at least a 100 meter maximum length for the entire copper connection between the devices and distributors. The following formula can be used:

$$\begin{aligned} & 5 \text{ m} \quad \text{connection cable} \\ + & 90 \text{ m} \quad \text{installation cable} \\ + & 5 \text{ m} \quad \text{connection cable} \\ = & 100 \text{ m} \quad \text{line distance} \end{aligned}$$

- You can implement longer lines when using higher quality components. However these are not included in the specifications.
- If you are using longer patch cabling, the installation cable must be reduced in length – not linearly but disproportionately, in accordance with 50173-1 / IEC 11801 (refer to IEC 11801 "Table 11801: "Table 21 horizontal link length equations").

2.8.3 Line lengths with fibre-optic cabling

Determining the lengths of fibre-optic cables is more complex and dependent on a variety of factors. To simplify the determination: the total of all attenuations which influence the fibre-optic stretch must be less than the power budget of the active devices.

$$\begin{aligned} \text{Power budget} &\geq \Sigma \text{attenuation}_{\text{connector}} \\ &+ \Sigma \text{attenuation}_{\text{splices}} \\ &+ \Sigma \text{attenuation}_{\text{cable}} * \text{cable length} \end{aligned}$$

- Power budget: the difference between the power of the output signals from device 1 and the readable input power from device 2 (for example: 4 dB for multimode)
- Attenuation_{connector}: the attenuation of all connectors in the transmission channel (depending on the connector type, about 0.3 dB each)
- Attenuation_{splices}: the attenuation of all splices located on the transmission channel (about 0.1 – 3.0 dB each)
- Attenuation_{cable}: the attenuation of the cable, depending on the light wave length (for example: 1.5 dB/km at 1300 nm wave length for a multimode fibre)
- Cable length: Length of the cable, in km (for example: 1.2 km)

For example, the above equation can result in:

$$4 \text{ dB} \geq 2 * 0.3 \text{ dB} + 2 * 0.1 \text{ dB} + 1.5 \text{ dB/km} * 1.2 \text{ km} = 2.6 \text{ dB}$$

→ the cable length is thus appropriate

2.9 Fire safety, thermal fire load and surge protection

Fire safety

The main causes of fires in and around electrical lines include:

- Short circuits and earth (grounding) faults, such as those resulting from mechanically or thermally damaged cables or lines
- Malfunctioning electrical connections or contacts (e.g., loose connections)
- Previous damage to insulation
- Overload
- Heat accumulation

Please note:

- Large sections of cable should be installed in suspended ceilings or in raised floors.
- Cables should be used which have cladding made from halogen-free, non-corrosive, non-flammable, low-gas, low-smoke materials.

Thermal fire load / fire conductivity

The thermal fire load characterizes the flammable energy of a cable. Fire conductivity characterizes the behaviour of the cable during a fire.

- Good fire conductivity indicates that the cable's flammable material can encourage the spread of fire (similar to a fuse line).
- Poor fire conductivity is desired; this is attained by using materials with minimum flammable energy.
- Determine the fire conductivity for the cabling in each zone and document it.



CAUTION!

Be sure to follow local fire and building regulations!

Surge protection

Overvoltage surges are extremely high voltages which disrupt or destroy the insulation and function of electrical and electronic components.

Therefore you should protect your machine and facility against:

- Lightning strikes
- Transient switching operations (with direct or indirect impact)

Make sure that:

- There is sufficient clearance space between facilities having different rated voltages
- Surge protection components are of the correct protection class.

2.10 Protocols (Ethernet)

You should use industrial Ethernet protocols. This will ensure that your facility is deterministic and has real-time characteristics. The most common protocols are:

- PROFINET
<http://www.profibus.com/pn>
- EtherNet/IP
<http://www.odva.org>
- EtherCat
<http://www.ethercat.org>
- Ethernet Powerlink
<http://www.ethernet-powerlink.org>
- ModBus/TCP
<http://www.modbus.org/>

2.11 Quality planning

The basic requirements for the quality plan and documentation are described in EN 501741.

Documentation

Be sure to make adequate documentation of all installation procedures. These can then be referred to during operations and modifications.

Inventory lists contain:

- Delivery information concerning products used (cables, junction boxes, etc.) and their data sheets
- Technical information (connection diagrams, assembly tips, etc.)
- Measurement protocols for all installed lines
- Layout diagrams with connection points and distributor locations
- Details about equipotential bonding methods

Test procedures

Test can be used in order to:

- Optimize the production
- Improve the quality of production
- Increase the efficiency of production
- Reduce the costs caused by malfunctioning components

You should test for:

- Breakages and short circuits (continuity)
- Missing, defective and false components
- Incorrect assembly
- Compliance with the cabling's electrical parameters

Bandwidth reserves



Do not exploit the full bandwidth of your network. Rather, you should set aside about one third bandwidth as reserve for possible expansions and adjustments.

Labelling



You should label both sides of all connection cables in your network. Make use of commercially-available markers and labelling components which offer labelling in advance. Weidmüller offers a comprehensive line of industrial markers for a wide range of applications.



You should avoid using a marking pen to write directly on the cable or marker since this will not last long enough.

2.12 Active components

2.12.1 Basic information

Networks consist of two or more devices which are connected via a central point. The central node is usually a switch which manages the communication between the individual devices.

IP addresses provide:

- Unique addressing within a network
- Pinpoint communication between individual clients



In order to avoid conflicts and malfunctions, make sure that you do not assign the same IP address twice within a network.

An IP address consists of four decimal numbers with values ranging from 0 to 255. The numbers are separated from each other by decimal points.

An IP address consists of:

- The address of the (sub-) network and
- The address of the station (also called host or network node).

Example: 192.168.0.110

MAC address

- The MAC address is a globally unique, distinct serial number for all Ethernet components
- It is hard-coded into the network card.
- It is a 48-bit sequence which normally consists of six hexadecimal number separated by dashes (-).

The sections of the address are divided as follows:

- 3 bytes manufacture identification and
- 3 bytes device identification (a sequential number)

Example: 00-15-7E-01-00-2F

Subnet mask

The main task of the subnet mask is:

- To separate the network section of the IP address from the host section
- This is critical for communications over an IP network.

Example: 255.255.255.0

Broadcast address

The broadcast address is a special address which reaches every node within a given network.

The last address in the range for the host address section is always used for the network's broadcast address.

Example: 192.168.0.255



Never assign the broadcast address to an individual node. This would lead to the complete loss of a number of network functions!

Default gateway

The default gateway is the forwarding address which nodes use for data packets if the packet's target address is not located in the internal network and the node has no specific routing information for the target address.

- The gateway knows itself how the target network can be reached, or
- Can forward the packet to the next higher default gateway.

Example: 192.168.0.1

Dynamic Host Configuration Protocol (DHCP)

- This protocol is used to automatically configure network component IP addresses.
- A router is used for this function.

Immediately after a network node is started, it sends a DHCP request out. The DHCP server answers and assigns an IP address from a predefined address range to the node. In addition to the IP address, the server sends the subnet mask, default gateway, and when required, a DNS address and lease time.

The domain name server is responsible for translating the IP addresses into computer names.

The lease time is used to establish the time period that a network node is allowed to keep the IP address which was assigned dynamically by the DHCP server.

Subnets

Subnets are partial networks with their own subnet addresses.



If devices must communicate with each other outside of the subnet boundaries, then you must setup the router to allow this communication.

Collision domain

A collision domain is a segment of a network. The terminal devices in all Ethernet networks are located on only one physical Ethernet segment.

Virtual Local Area Network (VLAN)

- The VLAN groups individual devices of various physical structures into a common logical structure.
- It allows you to make changes to the network with relatively little overhead.
- There are no geographical restrictions.

It is important to distinguish between static and dynamic VLANs:

a) Static VLANs

- The assignment of a physical port to a VLAN
- If a node is connected to the port, it is automatically assigned to this VLAN

b) Dynamic VLAN

- Based on the MAC address of the node, a VLAN-ID is assigned to the port
- If the node is connected to another device port, the node remains in the same VLAN (in contrast to the static VLAN)

Quality of service (QoS)

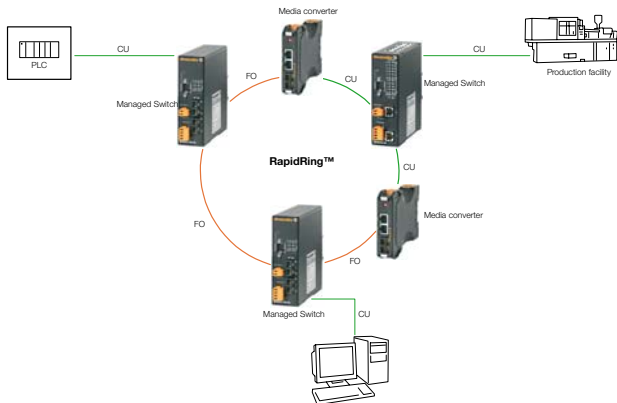
QoS is a process for influencing the data traffic and quality of service on networks.

Goal: Data from certain services are sent to receivers according to predefined quality parameters.

QoS ensures the optimization of network traffic. This is done by:

- A higher predictability for network data transmission
- The allocation of staggered bandwidth ranges for data transmission
- The allocation of transmission priorities throughout the entire network
- The improvement of the network's loss characteristics

RapidRing



RapidRing may be employed to increase the availability and reliability of industrial Ethernet systems. This method is known as redundancy.

RapidRing is a method that can be used to achieve fast network redundancy.

Devices are connected and cabled to each other in the form of an actual ring.

Since this ring structure leads to a loop in the network, one of the links is logically deactivated and used as a backup link. If a connection in the RapidRing malfunctions, the backup link is automatically activated to replace the standard connection.

If the controlling switch is equipped with an error relay, then a technician can be notified in the event of a connection outage and the connection can be restored.

Network address translation (NAT)

Network address translation describes the conversion and assignment of IP addresses between the local (private) and public networks.

a) Source NAT (SNAT)

A static process:

- The source IP address is replaced
- Used by packets
- The router stores the address conversion
- Normally only used for address translation between two local users

b) Destination NAT (DNAT)

A dynamic process:

- The target IP address is replaced
- Synonymous for incoming data packets
- These procedures are transparent to participating terminal devices; they are not aware of the address conversion.
- This address mapping is used when there are many local nodes but only a few public IP addresses

2.12.2 Security

Port security

Port security is used to protect against unauthorized access to unused ports. This security includes deactivating the port with software or sealing the port with a cap. The deactivated port must be reactivated if you want to reuse it.

Ports

Each network node has single permanent IP address which can be used for direct communication. Ports are used by different applications so that the applications can all be individually reached using the same IP address.

If you need to communicate with an FTP server running on the node at IP address 192.168.100.125, then you can use this address followed by a colon (:) and the port number 21.

Example: 192.168.100.125:21

Using the port number allows you to communicate directly to a target application running on a network node.

The ports ranges are:

- Ports 0 to 1023 are reserved for special services such as FTP (21), SMTP (25), HTTP (80), or Pop3 (110).
- Ports 1024 to 49151 are registered ports for certain applications.
- 49152 to 65535 are private ports which can be applied for customized usage.

Trunking with higher bandwidths

Multiple physical Fast Ethernet connections between two devices can be combined into a logical unit (a virtual trunk). Thus it is also possible to crossover from Fast Ethernet (100 Mbit/s) to Gigabit Ethernet (1000 Mbit/s).

Port mirroring

In the port mirroring process, the entire network traffic for a monitored port is copied ("mirrored") to a mirror port. The copied traffic and its data content can then be analysed. This can help you, for example, to create history or log files.

Filter and forwarding tables

Goal:

- Firewall filter functions
- Blocking ports
- Enable, monitor and control data traffic

These tables are used to merge filter rules into groups defined by their different fundamental tasks. Each table contains different chains. The chains are used to define how a packet is checked. The most important chains are:

- INPUT: this chain is used on all packets which are destined to a local process
- OUTPUT: this chain is used on all packets which originate from a local process
- FORWARD: this chain is used on all packets that are being routed (forwarded)

Error relay (for security and troubleshooting)

Many switches feature a programmable relay as a triggering mechanism that can be used for notification if the switch experiences a state change. For example, an optical or acoustic signal transmitter can be connected to such a relay.

Bandwidth throttling

Bandwidth throttling is advisable when a 10 Mbit/s terminal device has no auto-negotiating function. The bandwidth can be defined so that it is the maximum possible bandwidth (i.e., as defined by the technical limitation of the terminal device).

IGMP snooping

- Controls the multicast flow
- Monitors the exchange between the router and host
- Modifies the bridge table

SecIE e.V.



<http://www.secie.org/>

Members: Nortel, Weidmüller, and others

It is often the smaller measures such as examining the data security of facility and network configurations that make a big contribution towards all-encompassing security. In order to find the right balance, you should carry out a risk analysis and define your security aims.

Together with its members, the SecIE is working to build up the required standards. In order to achieve the IT security demands (availability, integrity and confidentiality), the following possible aspects are being taken into consideration:

- Endpoint security (e.g., lockable electrical cabinets, interlocking RJ45 connectors, access to networks granted to outside devices, identity checks, compatibility checks, compliance)
- Transport security (e.g., VPN, recognition of viruses in flowing information, protection against unauthorised reading)
- Perimeter security (e.g., firewall, targeted filtering of data)
- Core security (redundancy, fault tolerance)
- Organizational security (e.g., work instructions, legal aspects, emergency planning, business contingencies)

2.12.3 Infrastructure components

The router



Industrial access routers provide a simple and secure connection between office networks, or between the Internet and production networks.

Routers purposefully separate different networks. Access to the production network behind the router is only allowed for authorized users. This allows a connected facility to be concealed behind a single IP address. Thus the installation overhead is significantly reduced.

Thanks to the integrated modem (analogue or ISDN), the router can be accessed from any point around the globe via the telephone network for configuration, administration and monitoring purposes. A VPN (virtual private network) connection can be used to connect two routers through a local Internet service provider. Only authorized applications are then allowed through.

Application areas:

- Separation of Ethernet networks
- Opening access to the Internet



Ethernet networks should be separated with a router. This simplifies the data exchange and reduces the risk of long response times.

Various options, such as VLAN or QoS, are available for isolating and prioritizing network data. A router filters data at the IP level. Only authorized users can access the secured network remotely. And only approved devices can send data out of the secured network.

The router uses a single IP address to conceal a machine with its own IP subnet and multiple network nodes. External access attempts to this IP address are automatically forwarded to a predefined IP address on the network behind the router. If required, the device can be kept isolated from the outside.

Wave-LINE SWITCH/ Industrial Ethernet switches

A switch is a network component used for connecting multiple nodes with a local network.

Tasks:

- Structuring networks
- Optimizing communication paths and times for data traffic
- Increasing the data throughput

Features:

- Very sturdy and reliable
- Assembly on top-hat rail or wall

Industrial networks with industrial Ethernet require high-performance managed switches. These switches serve as centralized intermediary units within the electrical cabinet. There are significant differences between them and unmanaged switches.

Overlapping functions and operational modes

Auto-crossing:

- Automatic detection and correction of the transmit and receive data lines.
- This allows components to be connected using both 1:1 straight-through wired cables and also cross-wired cables

Auto-negotiation:

- The data transmission rate is automatically and independently negotiated with the link partner at each port
- The link is created utilizing the highest-possible rate of data transmission at which both partners are capable of communicating

Blocking:

- Non-blocking – when the switch capacity is sufficient to deal with connection to all partners at the maximum data rate
- Blocking – when a connection cannot be established because of a capacity overload

Half-duplex:

- An operational mode where the Ethernet node is either sending or receiving data at any point in time

Full-duplex:

- An operational mode where both partners can communicate at the same time bi-directionally

Managed switches

A configuration of the managed switch is always required because of its wide array of configurable functions. A terminal program or Web interface can be used to program the switch. This simplifies the process of adjusting components and allows the operator to use almost any connected PC to configure remote, far-off devices over the network.

The implementation of a monitoring function for individual ports makes it easier to troubleshoot after a malfunction.



Application:

- Port trunking
- Port mirroring
- VLAN
- IGMP snooping
- DHCP
- RapidRing

Unmanaged switches

Unmanaged switches enable an entry into the world of industrial Ethernet. You do not need to make any configuration; rather configuration is accomplished by Plug-and-Play.



Application characteristics:

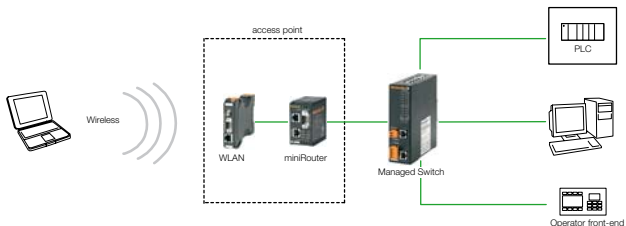
- For price-sensitive applications
- Designed as compact, Plug-and-Play modules
- Enables simple installation of industrial Ethernet networks
- Configuration or parameter assignments are not required



It is important to realize when using unmanaged switches in Ethernet/IP networks with real-time I/O traffic that the multicast broadcasts for certain address ranges are sent out unfiltered to all ports (as a broadcast). This results in an increased network load.

Wireless LAN (WLAN)

Wireless LANs are local networks not bound by physical hard-wired connections. An access point is needed to take advantage of the wireless technology. The access point serves as a gateway between the cable network and the wireless network.



Security features:

- The current encryption standards are WPA and WPA2
- A MAC address filter only allows authorized network devices access to the wireless network



The implementation of a WLAN in a corporate setting must be thoroughly planned and designed with the most stringent security measures possible.

a) Application areas

- Mobile connection for laptops
- For vehicles or machines that need to collect data in warehouses
- In the automation sector
- For recording measurements or for machine control

b) Frequencies

Two license-free frequency ranges are available for wireless network communications:

Standard	Frequencies	Channels
802.11a	5.15 GHz - 5.725 GHz	Channels: 19, all with no overlap, in Europe with TPC and DFS, according to 802.11h
802.11b/g	2.4 GHz - 2.4835 GHz	Channels: 11 in the USA / 13 in Europe / 14 in Japan. Maximum 3 channels with no overlap

For all standards, the channel bandwidth is between 10 and 30 MHz.

c) Channels

The most widespread standard is 802.11b/g. It has a frequency range of 2.4 GHz to 2.4835 GHz. The frequency ranges are distributed among the individual channels as follows:

Channel	Frequency	Application countries
1	2.412 GHz	Europe, USA, Japan
2	2.417 GHz	Europe, USA, Japan
3	2.422 GHz	Europe, USA, Japan
4	2.427 GHz	Europe, USA, Japan
5	2.432 GHz	Europe, USA, Japan
6	2.437 GHz	Europe, USA, Japan
7	2.442 GHz	Europe, USA, Japan
8	2.447 GHz	Europe, USA, Japan
9	2.452 GHz	Europe, USA, Japan
10	2.457 GHz	Europe, USA, Japan
11	2.462 GHz	Europe, USA, Japan
12	2.467 GHz	Europe, Japan
13	2.472 GHz	Europe, Japan
14	2.483 GHz	Japan

d) Range of coverage

- The permitted level of emissions for standard WLAN devices is 100 mW.
- Typical coverage ranges from 30 m to 25 km depending upon the hardware and the application.
- The coverage range is dependent on physical obstacles as well as the type and material of the surrounding buildings.
- Metallic infrastructures and stone or concrete walls cannot be easily penetrated and increase attenuation.

e) Data rates

Make sure that all network nodes share the uploading and downloading bandwidth. Furthermore, the data rates provided are only theoretical values and are based on optimal conditions. Actual data rates achieved will be considerably lower than the theoretical values.

IEEE-/Group	Description
802.11	WLAN for 1-2 Mbit/s on the 2.4-GHz band
802.11a	WLAN for 54 Mbit/s on the 5-GHz band
802.11b	Expansion of 802.11 up to 11 Mbit/s on the 2.4-GHz band
802.11g	Higher data rate (from 20 Mbit/s) on the 2.4-GHz band

f) QoS

IEEE 802.11e is an industrial standard in the IEEE 802.11 wireless LAN standard. It supports the quality-of-service concept. Data packets are assigned a priority depending on the sender. An access point recognizes the priority of the data packets and gives preferential treatment to packets of higher priority. Real-time applications can be better supported with help from IEEE 802.11e. IEEE 802.11 establishes a defined bandwidth on the network which ensures that data packets arrive at the receiver within a defined time interval.

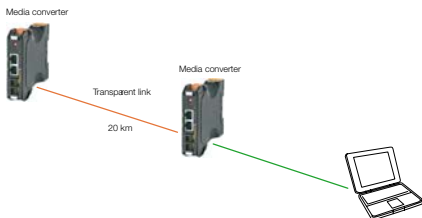
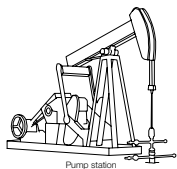
g) Interference

Different types of interference can occur with other radio transmission systems, since WLAN uses the same license-free frequency blocks as other applications (such as Bluetooth technology).

Media converter



A media converter connects copper cable with fibre-optic cable.

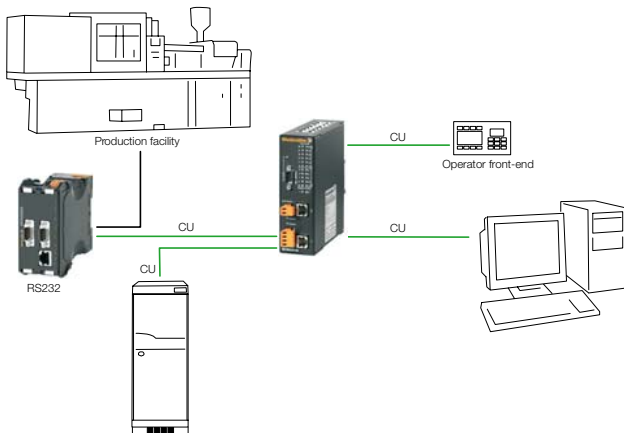


Copper conductors are adequate for the majority of applications. However fibre-optic cable is required for special applications:

- Line length is greater than 100 meters
- Electromagnetic interference
- No equipotential bonding

ComServer

A ComServer can be used to connect a device with a serial interface to the network. This allows you to easily connect an existing RS232-interface production facility into your Ethernet network. All computers integrated into the network can access the interface.



GPRS-I/O alarm module

The GPRS-I/O alarm module is designed for collecting messages which originate in decentralized industrial facilities and building installations.



Functions:

- Alarm messages via SMS, fax or e-mail
- Fully configurable messaging chain with eight target numbers per input
- Wireless, transparent data transmission to a serial interface on the machine or facility
- Additional alarm service functions via GSM, in order to also provide messages in event of malfunctions in the GPRS dedicated line
- Remote maintenance and configuration is accomplished over the analogue modem connection
- Values from a machine or system can be regularly stored to a data logger (server) on the Internet. Values can also be simultaneously retrieved from the data logger.
- Continuously online due to the GPRS connection
- Can be controlled remotely with remote switching of the outputs by means of telephone, mobile phone and SMS messages
- Minimal cost of acquisition and inexpensive operation

Industrial power supply units



The Weidmüller Power Supply Unit is an ideal partner for our complete range of Ethernet Switches and Communications Electronic devices.

2.13 Passive components for copper cabling

2.13.1 The basics of copper cabling

Installation cable



- For fixed routing of cables over long distances
- Limited flexibility
- Preferably with Cat.7 properties

Connection and patch cables



- The cable between the connection socket and the terminal device
- A flexible cable with a small bending radius
- With Cat.5 or Cat.6 properties
- With PUR- outer cladding for extreme toughness and resistance to abrasion

Customer-specific cable assembly

Take advantage of Weidmüller's extensive range of custom cable assemblies

- This takes the strain off your assembly process
- It simplifies your order handling
- And it relieves your storage and logistic resources

You should also refer to Weidmüller's **Galaxy** configuration software (available on the Internet). With just a few mouse clicks, this program can be used to create, request and directly order customized connection cables.

The screenshot displays the Weidmüller Galaxy configuration software interface. The top navigation bar includes 'PRODUCTS' and 'INDUSTRIAL ETHERNET'. Below this, there are tabs for 'Presentation', 'Catalogue', and 'Configuration'. The main area shows a 3D model of a green cable with a grey RJ45 connector on one end and a black and orange RJ45 connector on the other. Below the model, there are configuration options for 'Plug 1', 'Type of cable', 'Colour', 'Plug 2', 'Category', and 'Length [m]'. The 'Length [m]' dropdown menu is open, showing options from 1 to 20 meters. On the right side, there are links for 'Send to shopping basket', 'Feedback', 'Export', 'Save Configuration', 'Load configuration', and 'New configuration'. The footer contains the text '1.5.0.16', 'Ent | Options | Impressum | Feedback | Manual', and 'Deutsch | English | Español | Italiano | Français'.

2.13.2 Symmetric cable types

UTP	Unshielded cable
F/UTP	Cable covered with complete foil shielding, but wire pair is unshielded
SF/UTP	Cable covered with braided shield and foil shielding, but wire pair is unshielded
S/FTP	Cable covered with braided shield, wire pair with foil shield

2.13.3 Special cable types

Use dragline cable wherever there is frequent or continuous motion in an industrial environment.

- SF/UTP cable
- Preferably 7-core stranded conductor
- Cat.5
- PUR outer cladding: halogen-free and extreme resistance to abrasion

Use an **armoured cable** (rodent-proof cable) particularly when installing in tropical or rural areas. These armoured cables protect against gnawing by animals such as termites.

Use **torsion-protected cable** which prevents twisting in the lengthwise (longitudinal) direction, particularly for robotic construction applications.

2.13.4 Definition of cable cladding materials

Cladding material	PVC	LSZH	PE	PUR
VDE designation	Y	H	2Y	11Y
Standard temperature range	-40 °... +115 °C	-25 °... +70 °C	-35 °... +80 °C	-40 °... +85 °C
UV resistance	yes	yes	yes	yes
Flame resistance	++	++	-	+
Halogen-free	no	yes	yes	yes
Oil resistance	+	no	+	++
Resistance to chemicals	+	no	+	++
Resistance to abrasion	+	-	+	++
Applications	Building	Fire safety	Food industry	Industrial dragline
Water absorption	-	+	--	-
Can be used outside	yes	yes	yes	yes
Flexibility	+	-	-	++
	++ very good	+ good	- minimal	-- very minimal

2.13.5 Definition of cable diameters (AWG)

AWG is the abbreviation for American wire gauge. This specification is used throughout the world to specify conductor size. It does not specify the actual diameter but only a range. Thus an exact conversion to the metric size is not possible. A comprehensive comparison of AWG values to metric conductor diameters can be found at

http://en.wikipedia.org/wiki/American_wire_gauge.

2.13.6 Normative characteristics for copper cabling

Remember that the transmission properties of your network are dependent on:

- The spatial dimensions of the network (cable lengths)
- The transmission characteristics of the components

EN 50173 describes the relevant characteristics:

Transmission channel

- The transmission path between the network device (switch) and the connected station (node)
- A typical transmission channel consists of the horizontal cabling and 2 connection cables (patch cables)

Installation path (permanent link)

- A transmission path for the measurement of transmission characteristics for components installed on a transmission channel

2.13.7 Copper connector

There are two standardized mating profiles in EN 50173-3.

RJ45 (also RJ-45)



- RJ is an abbreviation for "registered jack" (a standardized plug)
- This has been the dominant connection mechanism in the IT sector for many years
- It is described in IEC 60603-7
- Further developments on RJ45 for IP67-class protection are described in IEC 61076-3-106.

M12



- In the automation engineering sector, the M12 connector has been used successfully for about thirty years.
- It is a compact connection solution in IP67.
- The IEC 61076-2-101 describes the specifications of M12.

With its special D-coded mating profile, the M12 connector is specifically intended for use in industrial Ethernet networks.

Other connector types can be considered which are outside of the applicable network standards and directives. However these would not be compatible to the standard IE connections.

2.14 Passive components for fibre-optic cabling




A fibre-optic conductor refers to all glass and plastic fibres used for data transmission.

Application areas:

- Connection with high data rates over long distances
- In the primary cabling sector (from building to building)
- In the secondary sector

There are several advantages compared to copper conductors:

- No electromagnetic interference
- Protection against disturbances because of the electrical galvanic decoupling
- Not dependent on equipotential bonding
- Protected from lightning and explosion risk
- Minimal attenuation over long distances
- Higher bandwidth
- No crosstalk between fibres
- Protection against wiretapping

Cabling for distributors and electrical cabinets	Cabling for infrastructure and machines	Cabling for applications and machines
		
Patch cable, Zipcord multimode, SC-, ST-connectors, PVC outer cladding	Breakout cable, multimode, SC-, ST-connectors, PVC outer cladding	Breakout cable, multimode, SC-, ST-connectors, PUR outer cladding

Fibre optic basics

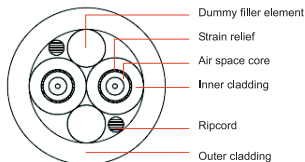
a) Fibre-optic fibres

	POF/HCS	Glass
Costs (for devices, cables, connecting mechanisms)	low	high
Range	POF: up to 50 m HCS: up to 200 m	many kilometres
Data rates	up to 100 Mbit/s	> 10 Gbit/s
Handling and assembly	relatively uncritical	complex

b) Fibre categories

Fibre	Wave-length [nm]	Attenuation [dB/km]	Bandwidth (modal) lengths [MHz*km]	Chromatic dispersion coefficient [ps/nm*km]
Multimode OM1	850	3.5	200	
	1300	1.5	500	
Multimode OM2	850	3.5	500	
	1300	1.5	500	
Multimode OM3	850	3.5	1500	
	1300	1.5	500	
Single mode OS1	1310	1.0		3.5
	1550	1.0		18

Setup for fibre-optic cables



Fibre-optic breakout cable






Zipcord cable

Cable outer cladding

Cladding material	PVC	PUR
VDE designation	Y	11Y
Standard temperature range	- 40°...+115°C	-40°...+85°C
UV resistance	yes	yes
Flame resistance	++	+
Halogen-free	no	yes
Oil resistance	+	++
Resistance to chemicals	+	++
Resistance to abrasion	+	++
Applications	Building	Industrial dragline
Water absorption	-	-
Can be used outside	yes	yes
Flexibility	+	++
	++ very good	+ good
	- minimal	-- very minimal

Fibre-optic connectors

	SC Simplex	SC duplex	SC-RJ
			
Standard	IEC 61754-4	IEC 61754-4	IEC 61754-24
Medium	MM, SM, POF	MM, SM	MM, SM, POF
IE design			PROFINET

	ST	LCD	E2000
			
Standard	IEC 61754-2	IEC 61754-20	IEC 61754-15
Medium	MM, SM, POF	MM, SM	MM, SM
IE design		EtherNet/IP	

2.15 Additional infrastructure components

Junction boxes



- These are the connection points for end-user devices on the network
- For mounting on wall

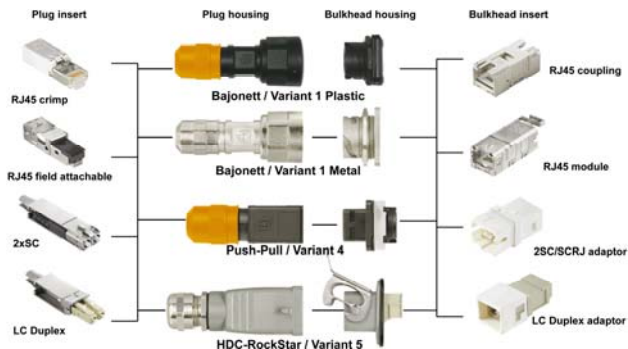
Couplings



- Intermediary piece used to connect two identical connectors together

2.16 **STEADYTEC®**

- A trend-setting connection system for data, power and signal transmission
- Initiated by three of the leading companies in connection system technology
- The basis for reliable, application-oriented and standardized solutions for both the office environment as well as the harsh industrial environment
- **STEADYTEC®** uses the principle of modular design to provide many combination possibilities



2.17 Important questions when planning your network infrastructure

- Which cabling is already available in the building or facility?
- Which cabling and connection systems are being implemented?
- How should the connection to the building network be implemented?
- Where will the machine connection points go?
- How far away is the building network?
- What connection lengths are necessary to reach all of the network nodes?
- Is redundant cable routing necessary?
- Should the machine distributor be situated in the electrical cabinet or be stand-alone?
- How is the earthing (ground) concept designed?
- Which connection system will be used?

2.18 Tender specification document

Many manufacturers of network components offer a tender specification service. The tender specification can be downloaded, often as a GAEB-formatted document (the German acronym GAEB stands for Joint Committee for Building Electronics).

2.19 Planning checklist

Requirements	Comments
Cable routing	
Have the requirements for the minimum transmission paths been observed?	
Are the minimum allowed bending radii being observed?	
Are the permitted environmental conditions met?	
Product selection	
Have all arrangements and actions required by the applicable standards been scheduled?	
Have the defined specifications been followed?	
Distributor	
Is accessibility guaranteed from both the front and rear?	
Have sufficient reserves been set aside for future expansion?	
Has enough space been allocated for the doors to completely open?	
Performance warranty	
Did you prepare documentation and measurement protocols for the cabling?	

3. Installation

This chapter contains helpful information about:

- Installation guidelines
- Cable routing
- Connection methods
- Labelling
- Measurement and documentation processes

3.1 Installation guidelines

Standards from the EN 50174 series should be strictly followed during installation. They are valid throughout the installation. Depending on the specified industrial protocols, you should also refer to this corresponding guideline.

EN 50174

The EN 50174 series of standards is targeted for the designers and installers of communication cable systems, but is also relevant for architects. It establishes requirements for designing, execution, documentation, and quality assurance. These requirements are valid for both the implementation cabling phase and the operational phase.

PROFINET installation guidelines

PROFINET describes the following installation guidelines especially for this industrial protocol:

- Specific connection lengths
- Specific connectors
- Specific cables
- PROFINET-compliant cable routing

Ethernet/IP installation guidelines

EtherNet/IP describes the following installation guidelines especially for this industrial protocol:

- Specific connectors
- Specific cables
- EtherNet/IP-compliant cable routing

3.2 Cable routing

The following tips and information can be used to make your installation easier and to guarantee that your system will operate smoothly.

Rolling up cable

Make use of stands when using cable drums. This will help you avoid exposing the cable to damaging stress or load.

In order to avoid cable twisting, you should lay out cable rings as they are situated on the floor.

Bending radius



Always observe bending radius specifications supplied by the cable manufacturer. These must be strictly followed in order to maintain the cable's transmission characteristics.



Typical bending radii are:

- Copper installation cable: 4-5 x Ø
- Flexible copper connection cable: 4-5 x Ø (non-recurrent bending), 8-10 x Ø (frequent bending)
- Copper dragline cable: approx. 7.5 x Ø



Be sure not to damage the cable when routing it near sharp edges or corners. Damage could diminish the durability or transmission characteristics of the cable.



Bundling and retaining the cable

Use cable ties which are as wide as possible. Velcro-type cables ties are even better for bundling cable or support load-bearing sections. Make sure that:

- The cable is fully pinched.
- The cable is not squeezed. This could later lead to diminished transmission characteristics or operational outages.

Cable channels and cable carriers



Be sure to consider the possible importance of separating power, data and signal lines in order to avoid disruptions in data traffic. You should use EN 50174-2 for determining the correct cable routing distances.

Cable reserves

You should always provide for two to three metres of extra cable when installing and routing cables near electrical cabinets. This is helpful since actual locations can shift from the planned locations during installation of electrical cabinets.

3.3 Connection methods

Copper connection methods

a) Cutting

Make sure that:

- You choose the correct tool with a cutting profile that fits and is optimized for the correct insert.
- You cut perpendicular to the cable.

b) Stripping

Make use of a multiple-stage stripping tool in order to simplify your work. This allows you to strip both the outer cladding and the underlying shielding from distinct cable points in just one work step.



Be sure to select the correct blade setting depending on the cable type.



- 1 Insert the end of the cable into the tool.
- 2 Press the tool closed.

Installation



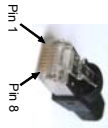
- 3 Turn the tool in the direction shown by the arrow in order to strip the cable.



- 4 Open up the tool before removing the cable.
- 5 Peel away the separated outer cladding from the cable with your hand.

Pin-out assignments for RJ45 and M12, according to TIA 568A, TIA 568B, EtherNet/IP and PROFINET

RJ45 pin and colour assignments



PIN RJ45	EIA/TIA 568 A	EIA/TIA 568 B	ETHER-NET/IP (2 pair)	PROFI-NET
1 ^{Tx+}	white/green	white/orange	wh/or	yellow
2 ^{Tx-}	green	orange	orange	orange
3 ^{Rx+}	white/orange	white/green	wh/gr	white
4	blue	blue		
5	white/blue	white/blue		
6 ^{Rx-}	orange	green	green	blue
7	white/brown	white/brown		
8	brown	brown		

M12 pin and colour assignments



ETHER-NET/IP	PROFI-NET
1 ^{Tx+} wh/or	yellow
2 ^{Tx-} wh/gr	white
3 ^{Tx-} orange	orange
4 ^{Rx-} green	blue



Connection tips

- Do not untwist the wire pair any more than necessary.
- Do not re-twist the wire pair.
- Make sure that the shielding foil is closed.

c) Connecting an RJ45 plug crimp



- 1 Strip the cable according to the connector's assembly instructions. Then peel back the remaining shielding braid over the outer cable cladding. Put on the cable sleeve.



- 2 Insert the individual cable wires into the pre-sort mechanism, according to the selected pin assignments (page 73). Then separate any remaining ends so that they are flush.



- 3 Then insert the pre-sort mechanism into the plug enclosure. If necessary, bend the strain relief mechanism back and then bend again to the front.



- Put the RJ45 plug into the crimping tool and close the tool. This one step crimps the contacts, the shielding braid, and the strain relief mechanism.



Please note: Select the crimping tool to match the connector type. Not every connector type is appropriate for every tool.

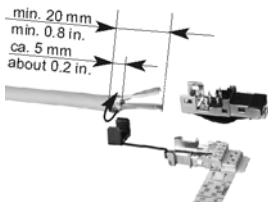


- Disconnect any remaining shielding braid.

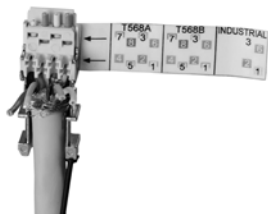


- Position the protective sleeve over the assembled connector. This sleeve ensures that the plug cannot be damaged by levering, and it protects against bending and kinks.

d) Connecting an on-site assembled RJ45 plug



- 1 Strip the cable according to the connector's assembly instructions.



- 2 Sort out the individual wires according to the coding guide located on the underside of the plug. Insert the wires into the wire guide while pushing the cable forwards as much as possible.



- 3 Close the strain relief mechanism around the cable. Then disconnect any remaining wire ends.

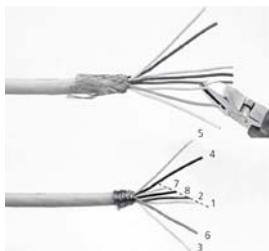


- 4 Press the upper section of the plug onto the lower section. If necessary, use an adjustable wrench for additional support.

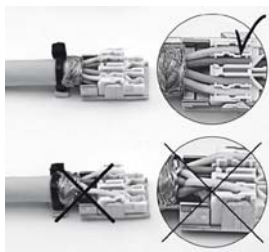
e) Connecting an on-site assembled RJ45 (female) module



- 1 Strip the cable according to the module's assembly instructions. Push back any remaining shielding braid over the cable.



- 2 Untwist the wire pair. Cut the wires off diagonally to allow for simple sorting into the lower wire guides.



- 3 Push or insert the individual wires into the wire guides of the lower section of the module, according to their colour. Any standard cable tie can be used for providing strain relief. Disconnect any remaining wire ends so that they are flush.

Installation



- 4 Press the upper section of the module onto the lower section.
If necessary, use an adjustable wrench for additional support. Retain the shielding braid with the second cable tie.

g) Testing



Each cable that you make/install should be tested for:

- The correct assignments
- Continuous shield (ground) connection
- Short-circuits
- Split pair errors

POF (polymer optic fibre) connection methods

a) Tools and assistance

Stripping tool:

Remove the outer cladding (breakout) of the fibre-optic cable with a suitable stripping tool.

Knife:

A knife blade should be used to cut the POF fibres from the connector after assembly.



Crimping tool:

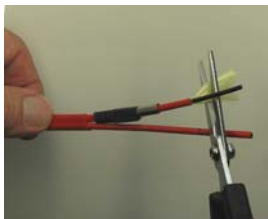
The crimping tool is used to crimp the crimp barrel onto the connector. This connects the POF cable mechanically with the connector.



Polishing disc and polishing foils:

These are used for accommodating the connector and for polishing the fibre's end surfaces.

b) Fibre preparation and assembly, using the example of a SC connector on a POF cable



- 1 Prepare the cable according to the manufacturer's specifications. Put on the cable sleeve.



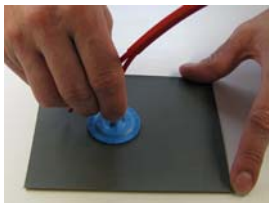
- 2 Distribute the Kevlar braid evenly over the plug body. Push on the crimp barrel up to the end stop. Crimp this on with the crimping tool. Cut off any remaining Kevlar braiding using the Kevlar shears.



- 3 Push the kink-prevention sleeve over the crimp barrel and up to the plug body.



- 4 Cut off the remaining fibres so that they are flush.
- 5 Place the sanding foil (1500 μm , grey) on the polishing base support.



- 6 Insert the connector into the polishing device and rub the plug's end surface with an 8-shaped polishing motion.

- 7 Place the sanding foil (3 μm , pink) on the polishing base support.
- 8 Insert the connector into the polishing device and polish the plug's end surface with an 8-shaped rubbing motion.
- 9 Then test the light conductivity with the assistance of a light source.

Installation

Glass fibre connection methods

a) Tools and aids



Fast-cure adhesive set:

The adhesive is used to fix the fibre in the connector. You should select a fast-curing adhesive to speed up and simplify the assembly significantly.

Stripping tool:

Remove the outer cladding (breakout) of the fibre-optic cable with a suitable stripping tool.



Stripping tool:

The stripping tool is used to remove the Zipcord outer cladding and the secondary and primary layers.



Kevlar shears:

Kevlar shears are used to remove the remaining Kevlar braiding.



Crimping tool:

The crimping tool is used to crimp the crimp barrel onto the connector. This connects the POF cable mechanically with the connector.



Stylus:

The stylus is used to score and break off any remaining glass fibre.



Polishing disc and polishing foils:

These are used for accommodating the connector and for polishing the fibre's end surfaces.

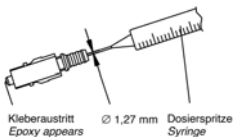
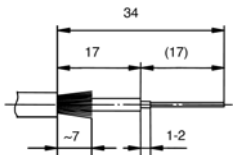


Microscope:

This is used to check that the fibre is correctly polished.

b) Fibre preparation and assembly, using the example of an SC connector on a fibre-optic glass fibre cable with fast-cure adhesive (an LC assembly is carried out in a similar manner)

Before first use, shake the bottle with the adhesive and activator.



- 1 Prepare the cable according to the manufacturer's specifications.
- 2 Use the dosage syringe to apply the activator to the split-off glass fibre, and on about 5 mm of the secondary layer.
- 3 Apply adhesive to the rear side of the connector until it comes out of the hole on the end surface of the plug pin.
- 4 Push the fibre in and out of the connector two or three times and then hold it briefly and firmly at the end stop position.
- 5 Distribute the Kevlar braid evenly over the plug body. Push on the crimp barrel up to the end stop. Crimp this on with the crimping tool. Cut off any remaining Kevlar braiding using the Kevlar shears.
- 6 Push the kink-prevention sleeve over the crimp barrel and up to the plug body.



- 7 Use the stylus to score and break off any remaining fibre.
- 8 Take polishing foil (30 μm , green) in the hand and then rub with a circular motion and with light pressure on the fibre excess until there is only a minimal length remaining.



- 9 Place the polishing foil (3 μm , pink) on the polishing support base. Then evenly coat the polishing foil with polishing fluid.
- 10 Insert the connector into the polishing device and rub the plug's end surface with an 8-shaped polishing motion. Rub until there is no more adhesive visible on the plug's end surface.



- 11 Place the polishing foil (0.3 μm , grey) on the polishing support base. Then evenly coat the polishing foil with polishing fluid.
- 12 Insert the connector into the polishing device and polish the plug's end surface with an 8-shaped rubbing motion.

Installation



- 13** Put the connector into the microscope (use an adapter if necessary) and check the end surface.



If you detect a poor quality surface (with scratches), then the connector must be re-polished. The connector must be replaced if fibre is sticking out.



good



poor

- 14** Then test the light conductivity with the assistance of a light source.

Splicing

Splicing refers to the connection of two glass fibres which are connected to each other permanently by a melting process. Splicing is performed with a specialized splicing device using a light arc. The fibres of, for example, installation cables are then connected at their ends with "pigtailed". The splicing device adjusts the light-conducting cores of the two glass fibres so that they are precisely aligned with each other. In modern splicing devices, the alignment process is fully automatic. Subsequently the fibres are melted (fused) together with a light arc. Depending on the quality of the splicing process, the attenuation on the splice point may be 0.3 dB. For good splices, the attenuation can be less than 0.02 dB. From experience, the attenuation values for high-quality devices are typically not greater than 0.1 dB.



Special equipment and experience is required to perform splicing correctly.

Pigtail

- Pre-assembled glass fibre connection containing a fibre-optic connection mounted by the manufacturer
- Used for connecting optical components
- The goal is to avoid on-site connector assembly

The advantages of pigtails:

- Minimal attenuation values and inexpensive automatic production
- Consistently good quality, defined ferrule surface since no handwork (polishing, etc.) is required

3.4 Labelling

Make sure that the cable is labelled in a clean manner and will be permanently readable. Make use of:

- Labelling sleeves and strips
- Colour-coded rings
- Adhesive labels



3.5 Measurement and documentation processes

Cable and line measurement is a requirement of the documentation for many installations. This process measures the system's line characteristics and documents the quality of the installed network.

- 1 Set the measurement device to the appropriate transmission class category.
- 2 Measure the cable's transmission characteristics (copper) or attenuation characteristics (fibre optic).
- 3 Document the lengths of the cables.
- 4 Print out these values and attach them to the documentation.

Measurement for copper

Use a mobile cable analyzer to measure the transmission parameters, such as:

- Pin assignments
- Cable length
- Near end crosstalk (NEXT)
- Far end crosstalk (FEXT)
- Return loss (RL)
- Insertion loss (IL)

Fibre optic measurement

The most important measurement to make after assembly is the spatial resolution attenuation for the installed stretch. This can be measured using a measuring device called an optical time domain reflectometer (OTDR). For this measurement, the connector attenuation must be less than 0.5 dB. Typical attenuation is less than 0.3 dB and very good attenuation values are under 0.1 dB. The measurement should take place using two wave lengths (850 nm and 1300 nm).

The final technical approval follows this step.

3.6 Installation checklist

Requirements	Comments
Have the defined specifications been followed?	
Does the cable type correspond with the design planning?	
Was the cable routed and installed according to the design plan?	
Were adequate reserves set aside for commissioning and expansions?	
Were the minimum prescribed cable clearance distances followed?	
Were the appropriate connectors used according to the design plan?	
Are the manufacturer's testing certificates available for the connectors?	
Have all cable and connections been inspected and tested?	
Have all testing results been documented?	
Do the electrical parameters for the transmission lines include sufficient reserve capacity?	
Are all connections labelled?	

4. Initial Commissioning

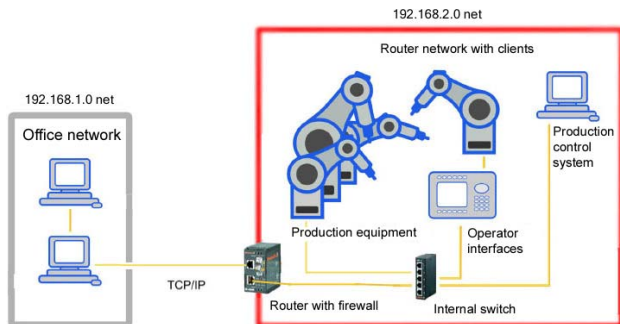
4.1 Initial commissioning basics

This chapter contains helpful information about:

- Basic and extended commissioning
- Redundancy
- Data backup
- Network maintenance
- Troubleshooting

Here we will use a complete application example to provide you with tips and solutions.

4.1.1 Setting up the network

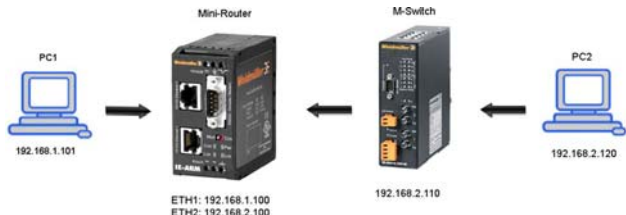


The illustration depicts a typical manufacturing site where the office network is separated from the network running in the manufacturing hall.

A router connects the two networks. Employees from the office network are not allowed access to any manufacturing equipment. Access to the machines is determined by the router and only allowed to certain authorized personnel.

Initial Commissioning

In our example, we have set up a simplified application where a switch, a router and two PCs are connected to each other. The application looks like this:



Here PC1 represents the office network and PC2 represents the manufacturing site. Both computers should be configured first. Then the managed switch is configured and finally the mini-router is configured.

4.1.2 Configuring PC1 and PC2

1 Switch on your Windows computer.



You should turn off your firewall before performing the following steps. This will ensure you have full access to your PCs.

By deactivating the firewall, the PC is no longer protected against viruses or other attacks. Only deactivate the firewall when your PC is sufficiently protected by other measures.

- 2 Click on "Start" → "Control panel", and then open "Network connections".
- 3 Select the active LAN connection. Click on the LAN icon with the right mouse button and then select "Properties" from the menu.

- 4 Under "This connection uses the following", select the Internet protocol (TCP/IP) and then click on "Properties".
- 5 Activate the option "Use the following IP address".
- 6 Enter the IP address for PC1 in the space provided: 192.168.1.101.
- 7 Press the TAB key. The correct subnet address will be automatically selected (normally 255.255.255.0).
- 8 Then enter the IP address of the gateway. Normally this is the address of the corresponding router interface where the PC is connected. For PC1 this is 192.168.1.100.

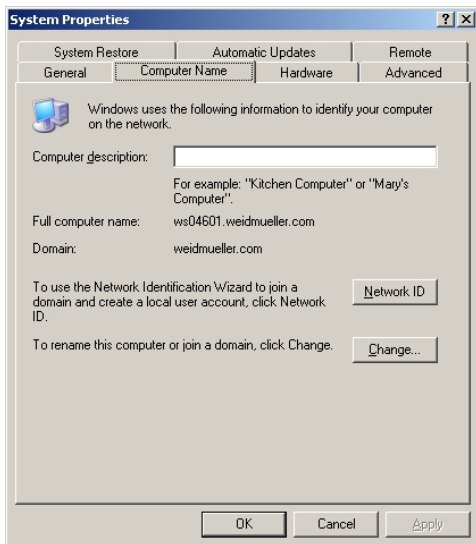
Obtain an IP address automatically

Use the following IP address:

IP address:	192 . 168 . 1 . 101
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 100

- 9 Now click on OK.
- 10 Click on the "Computer name" tag and then click on "Change" with the left mouse button. Specify or change the name of the workgroup here. The workgroup name must be identical for all network devices.

Initial Commissioning



11 Now click on OK.

12 Repeat steps 1 through 9 for PC2. For PC2, use IP address 192.168.2.120 and gateway address 192.168.2.100.

4.1.3 Configuring the managed switch

- 1 Use a patch cable to connect the configured computer with the switch.



The standard IP address for the switch is as follows:
192.168.1.110.

- 2 Open up your web browser and enter the switch IP address in the address bar. This will initiate a connection to the switch. A login window will then open.
- 3 Enter the username and password and confirm by clicking on "Submit" (factory default Username: admin, Password: detmold). The connection to the switch is now established.
- 4 In order to connect the switch to the second network, you must first change the IP address. To do this, open the menu options "System configuration" → "Configure IP address". Then enter the IP address 192.168.2.110.

- 5 Click on "Apply" to confirm. The switch has now been configured.

4.1.4 Configuring the mini-router

- 1 Connect PC1 with the first Ethernet interface on the mini-router.

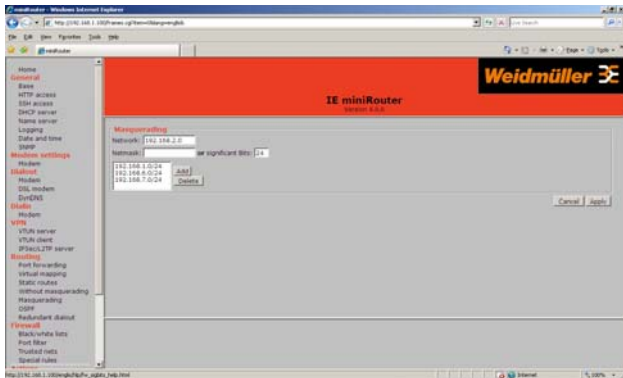


Normally the mini-router has the following standard IP address: 192.168.1.100.

- 2 Open up your web browser and enter the mini-router IP address in the address bar. This will initiate a connection to the router. A login window will then open.
- 3 Enter the username and password and confirm by clicking on "Submit" (factory default username: admin, password: detmold).
- 4 Verify that Net 1 and Net 2 are entered under the menu option "Routing" → "Masquerading".

When this is not the case:

- a For the network, enter the IP address 192.168.2.0. For bits, enter "24". Then confirm these changes.
- b Next, click on "Actions" and then "Save all".
- c Finally, you must restart the router. Click on "Restart". Wait until the router reboots and reconnects.



This completes the configuration of all components. You can now connect them to each other. Use a patch cable to connect PC1 to the first Ethernet interface on the router. Use a second patch cable to connect the managed switch to the second Ethernet interface on the router. After this, you need only connect PC2 with the switch.

Conduct a ping test to see if the configuration was successful. From PC1, try to reach both interfaces on the router and the network devices behind the interfaces: in our case this is the switch and PC2.



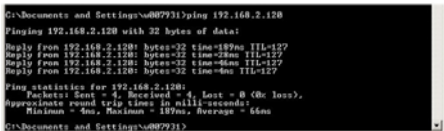
After each configuration, you should test if the device has been configured correctly. The Ping program is good for this task. Ping comes standard with both Linux and Windows.

Initial Commissioning

Ping is used to test the connectivity of a target node. It makes use of ICMP (Internet Control Message Protocol) to send queries and then wait for responses.

In Windows, you can run Ping by doing the following:

- 1 Click on "Start" and then "Run".
- 2 Enter "cmd" in the window and then click on "OK".
- 3 Now enter "ping 192.168.xxx.xxx" in the command window (where xxx is the assigned IP of the computer).
- 4 Confirm with the ENTER key.

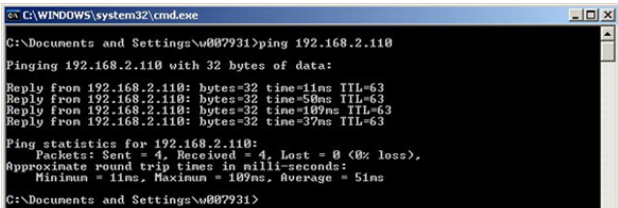


```
C:\Documents and Settings\w007931>ping 192.168.2.120
Pinging 192.168.2.120 with 32 bytes of data:
Reply from 192.168.2.120: bytes=32 time=189ms TTL=127
Reply from 192.168.2.120: bytes=32 time=28ms TTL=127
Reply from 192.168.2.120: bytes=32 time=46ms TTL=127
Reply from 192.168.2.120: bytes=32 time=4ms TTL=127

Ping statistics for 192.168.2.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 189ms, Average = 66ms

C:\Documents and Settings\w007931>
```

In the illustration above, the Ping command is executed from the second PC. The Ping was answered properly.



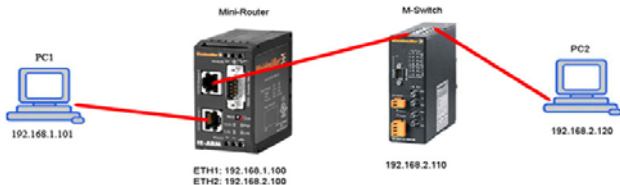
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\w007931>ping 192.168.2.110
Pinging 192.168.2.110 with 32 bytes of data:
Reply from 192.168.2.110: bytes=32 time=11ms TTL=63
Reply from 192.168.2.110: bytes=32 time=50ms TTL=63
Reply from 192.168.2.110: bytes=32 time=109ms TTL=63
Reply from 192.168.2.110: bytes=32 time=37ms TTL=63

Ping statistics for 192.168.2.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 109ms, Average = 51ms

C:\Documents and Settings\w007931>
```

In the illustration above, the Ping command is executed from the switch. The Ping was answered properly.

4.1.5 Interaction between networks



You should start with the cabling after all components have been configured.

- 1 Use a patch cable to connect PC1 with the first Ethernet interface on the router.
- 2 Then connect the managed switch to the second Ethernet interface.
- 3 After this, you need only connect PC2 with the switch.

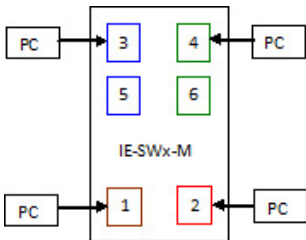
4.2 Additional configuration and commissioning on the switch

4.2.1 Configuring the VLAN

VLAN basics are detailed in Chapter 2.12, "Active components". The following example illustrates how to configure three simple VLANs and one management VLAN. The managed switch is exclusively configured (parameterized) using the management VLAN (management port). The example is limited to only one managed switch.

Port 1 is located on the first VLAN and communicates with all ports. Ports 3 and 5 are located on the second VLAN, while ports 4 and 6 are on the third VLAN. A special management VLAN is set up as the fourth VLAN and it is assigned only port 2. Port 2 allows you exclusive access to the web interface on the switch. Thus you can administrate the switch only via port 2.

The following diagram illustrates how the ports are partitioned:



At least two PCs are required for set up and testing in this example. Thus in this example all instructions and descriptions will be limited to these two computers.

All values (for example, IP addresses or ports) are only given as examples. They must be modified to fit your configuration.

Setting up the computer

Set up the following IP addresses in the "Network Connections" control panel on both computers:

PC1: 192.168.1.202

PC2: 192.168.1.204

Setting up the switch

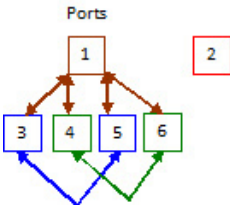
In order to set up the switch, you must first establish a serial connection between PC1 and the switch. Proceed as described below:

- 1 Use HyperTerminal to connect to the COM interface on the switch at a baud rate of 9600.
- 2 After you are connected, press [ENTER] and login with the username "admin" and the password "detmold" (as long as the password has not yet been changed from the default).
- 3 Then select "System Configuration" → "Configure IP Address".
- 4 Under "IP Address", enter the IP address "192.168.1.110" if this is not already entered.
- 5 Save these settings by clicking on "Apply".
- 6 Confirm the next dialogue window by clicking on "Yes".
- 7 Go two pages back by clicking on "<< Back".
- 8 Click on "Logout" to log off the switch. Disconnect the HyperTerminal connection.

After you have successfully completed these steps, the computer and the switch are both ready for the VLAN setup. Now use a patch cable to connect PC1 with port 2 on the switch.

Layout of the VLAN

You may structure your VLAN using the layout shown in the diagram below:



The illustration above shows which ports can communicate with each other. Here port 1 needs to be able to communicate with ports 3, 4, 5, and 6. The grouped ports 3 and 5, and ports 4 and 6 should be able to communicate within their group and with port 1. Port 2 is used only to manage the switch and should not communicate with any other ports.

The layout of the VLAN can be structured as follows:

In VLAN 1, communication is defined from port 1 to the ports 3, 4, 5, and 6. But since communication has not yet been defined to port 1, we need to set up VLAN 2. VLAN 2 establishes communication between ports 3/5 and port 1. At the same time, ports 3 and 5 are defined as VLAN 2. In order to set up VLAN 3, the same settings are required for ports 4 and 6. VLAN 4 is established for the management port (MPort) and port 2 is assigned to VLAN 4.

The table below provides the details:

VID	Switch Port	MPort
1	1 (MF), 3 (MF), 4 (MF), 5 (MF), 6 (MF)	
2	3 (MF), 5 (MF), 1 (MF)	
3	4 (MF), 6 (MF), 1 (MF)	
4	2 (MF)	Yes

The abbreviation MF in this table stands for "member with filter". This means that the device connected to the port cannot process a VLAN. In such a case, the VLAN information is lost.

Only computers are connected to the ports in this example. Thus only the MF setting is used.

The assignment of the ports to their respective VLANs is required for the next step. These assignments can be accomplished simply by using the figures from the table shown above. This would then proceed as follows:

Port	Default Tag
1	1
2	4
3	2
4	3
5	2
6	3
M	4

Initial Commissioning

The assignment of ports to the VLAN tags is explained below. Based on the figure shown on page 104 and the table above on page 105, we see that port 1 represents the first VLAN, that ports 3 and 5 represent the second VLAN, and that ports 4 and 6 represent the third VLAN. Port 2 is located in VLAN 4. The management port (M from the lower table found on page 105) is controlled via VLAN 4 and is thus defined by tag 4.

Configuring the VLANs

- 1 Start up the web browser and enter the switch IP address (in our case, 192.168.1.110).
- 2 Click on "System Configuration".
- 3 Then click on "Configure VLAN".

Configure VLAN Group and VID		Members and Tag Filter								Status	
Group	VID	-- = Non Member, M= Member without Filter, MF = Member with Filter									
1 <input type="button" value="Apply"/>	<input type="text" value="1"/>	<input type="checkbox"/> MF	<input type="checkbox"/> --	<input type="checkbox"/> MF	<input type="checkbox"/> MF	<input type="checkbox"/> MF	<input type="checkbox"/> MF	<input type="checkbox"/> MF	<input type="checkbox"/> --	<input type="checkbox"/> --	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
2 <input type="button" value="Apply"/>	<input type="text" value="2"/>	<input type="checkbox"/> MF	<input type="checkbox"/> --	<input type="checkbox"/> MF	<input type="checkbox"/> --	<input type="checkbox"/> MF	<input type="checkbox"/> --	<input type="checkbox"/> MF	<input type="checkbox"/> --	<input type="checkbox"/> --	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
3 <input type="button" value="Apply"/>	<input type="text" value="3"/>	<input type="checkbox"/> MF	<input type="checkbox"/> --	<input type="checkbox"/> --	<input type="checkbox"/> MF	<input type="checkbox"/> --	<input type="checkbox"/> MF	<input type="checkbox"/> --	<input type="checkbox"/> --	<input type="checkbox"/> --	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
4 <input type="button" value="Apply"/>	<input type="text" value="4"/>	<input type="checkbox"/> --	<input type="checkbox"/> MF	<input type="checkbox"/> --	<input type="checkbox"/> --	<input type="checkbox"/> --	<input type="checkbox"/> --	<input type="checkbox"/> --	<input type="checkbox"/> --	<input type="checkbox"/> --	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

- 4 Now enter a value for each row (taken from the table on page 105). Confirm your entries by clicking on "Apply".
- 5 Then click on "Continue to VLAN settings page 2". This will take you to the following window:

Configure 802.1Q VLAN Tag	
Port	Default Tag
1	<input type="text" value="1"/>
2	<input type="text" value="4"/>
3	<input type="text" value="2"/>
4	<input type="text" value="3"/>
5	<input type="text" value="2"/>
6	<input type="text" value="3"/>
7	<input type="text" value="15"/>
8	<input type="text" value="15"/>
M	<input type="text" value="4"/>

Apply

- Here you should transfer the values from the table found on bottom of page 105 into this "Configure 802.1Q VLAN Tag" table. Click on "Apply" when you are finished.
- Now click on "Save Settings" and wait until the process is completed.

VLAN Status:	
VLAN Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Note: Ensure the settings are correct before enabling or some ports may become inaccessible.

Apply

- After this, activate the VLAN by clicking on "Enable" under VLAN status. Then click on "Apply". If everything has been set correctly, the settings will be saved and the page will be updated.
- Click on "Save Settings".

Testing the individual VLANs

Run through the following test case in order to test each VLAN for its proper configuration:

- 1** Connect PC1 or PC2 to port 2. Then bring up the switch start page (192.168.1.110) in your web browser. If this page is displayed, then VLAN 4 has been configured properly.
- 2** Now try to bring up the switch start page from one of the other ports. If you cannot bring up the page, then VLAN 4 has been properly configured.
- 3** Connect PC1 to port 3 and PC2 to port 5. Conduct a ping test. If you receive an answer from both computers, then VLAN 2 has been properly configured.
- 4** Connect PC1 to port 4 and PC2 to port 6. Conduct a ping test. If you receive an answer from both computers, then VLAN 3 has been properly configured.
- 5** Connect PC1 to port 3 or port 5. Connect PC2 to port 4 or port 6. Conduct a ping test. If you receive no answer, then VLAN 2 and 3 have been properly configured.
- 6** Now connect PC1 to port 1 and PC2 to port 3 or port 5 and then to port 4 or port 6. Conduct a ping test. If you receive an answer, then VLAN 1 has been properly configured.

For the tests described above, you should ping from PC1 to PC2 or from PC2 to PC1.

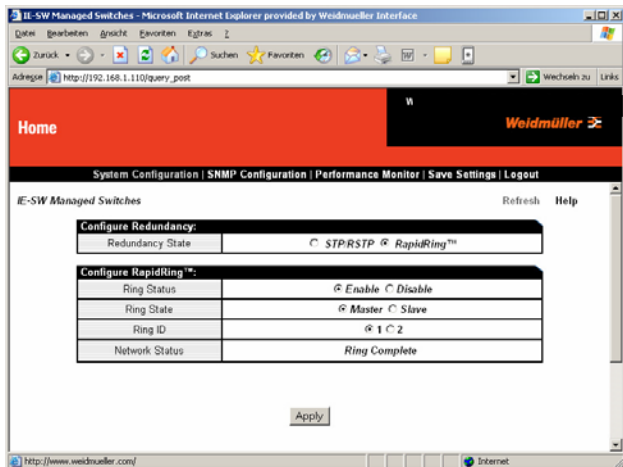
4.2.2 RapidRing

RapidRing basics are detailed in Chapter 2.12 "Active components". This RapidRing example consists of three steps.

	IP addresses provide for	RapidRing Port
Master	192.168.1.110	1,2
Slave 1	192.168.1.111	1,2
Slave 2	192.168.1.112	1,2

Step 1: Configuring the master

- 1 Start up the web browser and enter the switch IP address (in our case, 192.168.1.110).
- 2 Open up the menu "System Configuration" → "Configure Redundancy".
- 3 Select the option "RapidRing".
- 4 Select "Enable" for the Ring Status.
- 5 Select "Master" for the Ring State.
- 6 Now confirm your entries by clicking on "Save Settings" found in the upper menu bar.



Step 2: Configuring the slave:

- 1 Open up the menu "System Configuration" → "Configure Redundancy".
- 2 Select the option "RapidRing".
- 3 Select "Enable" for the Ring Status.
- 4 Select "Slave" for the Ring State.
- 5 Now confirm your entries by clicking on "Save Settings" found in the upper menu bar.

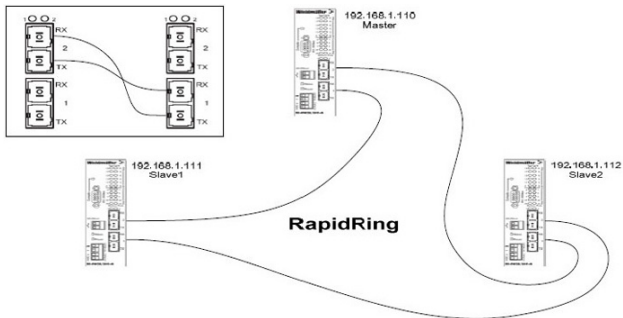


All Slaves should have the same Rapid Ring settings

Step 3: Cabling



Before starting with the cabling, switch off the configured switch in order to prevent a transmission loop from occurring.



- 1 Connect the device ports as shown in the illustration above.
 - Port 2 (Switch 1) in Port 1 (Switch 2) etc.
 - RX → TX and TX → RX



Experience shows that the danger of connection errors grows if there are more than three devices connected in a RapidRing. Therefore you should double check that all cables are properly connected.

- 2 Turn on the switch.



If the connections and settings were done properly, you will see "Ring Complete" displayed in the network status.

Your RapidRing network is now completely configured.

4.2.3 Port trunking

You can use the "Port Trunking" function to bring together multiple ports in a single group.

- 1 Open up the menu "System Configuration" → "Configure Trunking".
- 2 Select "Disable" for the Ring Status.
- 3 Now confirm your entries by clicking on "Save Settings" found in the upper menu bar.



When a link fails in the trunk group, the remaining links take over the data transmission for the failed link and maintain proper communication between both switches.

The screenshot shows the Weidmüller web interface for configuring port trunking. The top navigation bar includes "Home" and the Weidmüller logo. Below the navigation bar, there are links for "System Configuration", "SNMP Configuration", "Performance Monitor", "Save Settings", and "Logout". The main content area is titled "IE-SW Managed Switches" and contains a "Configure Trunking" section. This section has two rows, "Group 1" and "Group 2", each with a "Port:" field containing checkboxes for ports 1 through 8, and a radio button for "Enable" and "Disable". An "Apply" button is located below the groups. At the bottom, there is a menu of other configuration options: "Configure IP Address", "Configure Trunking", "Configure Port Mirroring", "Configure VLAN", "Configure Filtering and Forwarding Table", "Configure Quality of Service", "Fault Relay", "Configure Redundancy", "Configure Rate Control", "Configure Port Security", and "Configure IGMP Snooping".

4.3 Redundancy

There are many ways to implement redundancy on a router. This means that when a critical connection fails (for example when a router crashes), traffic can be re-routed to another link without any significant effort or reconfiguration.

Special settings / configuration services:

- Firewall settings can be set and are variable
for example: firewall port forwarding or firewall routing
- OSPF: Open Shortest Path First

OSPF allows you to define a process plan which establishes which router is responsible for which network. If the main link goes down on a network, the affected router automatically finds an alternative network route by means of OSPF.



This temporary connection is no longer used after the down link is restored.

4.4 Relay functions

Some switches offer a relay connection. This permits:

- The monitoring of certain process as they take place on the switch
- A signal to be sent in the event of an outage or the presence of a link at one or more ports

4.4.1 Using relay monitoring

You can activate or deactivate port monitoring on the switch. And you can configure this monitoring function:

- The option "Make on fault" closes the relay contact after a recognized error occurs.
- The option "Breaks on fault" opens (breaks) the relay contact after a recognized error occurs.

When booting up, the switch automatically determines the data rate and the duplex mode for each port. The process can take a few seconds. The "Relay activation after power" option can be set in order to prevent the switch from signalling an error during this process. This function allows the switch to first stabilize and then activate port monitoring.

4.4.2 The "Relay reset method" function

- If you select the "automatic" option for the "Relay reset method" function, the relay will be deactivated as soon as the error has been rectified.
- The "manual" setting will result in a menu option being created which will then require the error message to be manually reset.

4.4.3 Monitor ports / selecting the type of monitoring

This section describes how to select the monitor ports and the monitor types.

- "No Link" monitoring activates the relay when the connection to the port is lost.
- "Link Present" monitoring activates the relay when a connection to the port is found that is not yet configured. This allows the network to be monitored for unauthorized external access attempts.

4.5 Data backup

After you have made all changes to the configuration, select "Save all" from the menu in order to save (backup) your settings. If you do not make this backup, all your changes will be lost after a reboot.

4.6 Network maintenance

An industrial Ethernet network requires relatively little maintenance.

- A network management tool can be used to evaluate the degree of packet loss within the network.
- If packet loss concentrates itself within certain transmission sections, then you will need to inspect the quality and performance of that particular cable.
- Please note that these cables will not necessarily show signs of wear. Packet loss can also be triggered by any previously unknown disturbance.

4.7 Troubleshooting

Problem / question	Remedy / answer
The computer is completely unreachable and the settings cannot be changed.	Check to make sure that the firewall has been turned off. If it is not, turn the firewall off so that it will not block your request traffic.
The browser no longer refreshes after you click on the "Apply" button.	A false setting or configuration was made. The VLAN must be deactivated using HyperTerminal. Then check the settings in the web interface and reactivate the VLAN. Another source of error is improper connections: for example, that PC1 is not connected to port 2 of the switch.
The configuration menu can no longer be accessed with the web browser.	Make sure that the switch is connected to the correct port. If the error continues, you should deactivate the VLAN using the serial connection. Then check the settings in the configuration menu.
Can I assign multiple VLANs to a single port?	This is not possible. A port can only belong to one VLAN.
Is it always required to assign VLAN tags?	Yes. The VLAN tags are attached to the IP packets and are used to "represent" the VLAN.

Glossary

Many new terms have originated which are associated with industrial Ethernet. Below is a brief summary of the most important.

4B/5B

A block coding scheme for FDDI and ATM. With 4B/5B coding, all data is divided into 4-bit units (nibbles) and encoded according to a table into 5-bit units (symbols).

10BaseFL

10 Mbit/s Ethernet over glass fibre cabling.

10BaseT

An Ethernet standard which permits 10 Mbit/s transmissions.

100BaseFX

100 Mbit/s Fast Ethernet over glass fibre cabling.

100BaseSX

100 Mbit/s Fast Ethernet - operationally identical to 100BaseFX, however it uses an 850-nm glass fibre technology.

100BaseTX

100 Mbit/s Fast Ethernet system over twisted-pair cables.

AUI (Attachment Unit Interface)

The interface between the transceiver and the network card.

Auto-negotiation

Auto-negotiation describes a process which enables network cards to detect and configure independently the correct transmission speeds and the correct duplex mode for their connected network ports.

Bandwidth

Bandwidth indicates how much information can flow through a given location during a defined period of time. Typical units of bandwidth measurement are Mbit/s or Gbit/s.

Baud

Baud is the unit for measuring the modulation rate. Modulation refers to a signal of a defined duration.

Bit

Bit is a word created from the words binary and digit. It constitutes the smallest digital unit and contains the value of either a zero or a one.

Bit rate

Bit rate is also referred to as transmission speed, transmission rate or data rate. It describes the numbers of bits per unit of time (usually one second) that are transmitted.

Blowfish

In our modern digital age, there is growing emphasis placed on the transmission of sensitive data. For this reason Weidmüller uses Blowfish. This is a symmetrical encryption algorithm used at the software level in order to guarantee secure router-to-router connections.

Bridge

Bridges are used to connect subnets according to the OSI definition. The protocol is implemented at layer 2 or the OSI reference model.

Broadcast

A broadcast transmission is a message broadcast simultaneously from one point to all nodes.

Bus

Busses are the connection systems for electronic and electrical components. The bus always refers to a physical medium terminated at both ends. In a bus topology, individual components are connected to the physical bus.

Category 5

This indicates compliance with the characteristics specified in IEC 11801. With Category 5 (Cat. 5) components, you can build networks which are then suitable for all twisted-pair-cable-based Ethernet transmission standards up to 100 Mbit/s.

Category 5e

Cat. 5e is an identical version for TIA/EIA 568 (compared to Cat. 5 and IEC 11801) and is used in 1000-Base-T networks.

Collision

A collision refers to the event when two or more stations simultaneously send data on the same channel. Since the data overlap each other, they can no longer be used.

Collision Domain

A collision domain is a segment of a CSMA/CD network. According to IEEE 802.3, all terminal devices that are located on a physical Ethernet segment (including those devices which are connected to each other via a repeater) are part of the same collision domain.

CRC (Cyclic Redundancy Check)

CRC is a process for detecting errors. It reliably detects individual errors but is less accurate at detecting multiple errors.

Cross-over Cable

A cross-over cable is a special patch cable where the receive and transmit wires are crossed over (switched) on one end. Cross-over cables are typically used for connecting two end devices.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

An access method where the sender first checks to see if a shared network is available before sending traffic to the network (not needed for IE and full-duplex mode).

DHCP (Dynamic Host Configuration Protocol)

A specially configured server can assign dynamic IP addresses and other network parameters to network computers by means of the DHCP protocol.

DTE (Data Terminal Equipment)

A data terminal device is any device on a network where a communication path either begins or ends. That is, a station (computer or host) on the network which is capable of either sending or receiving data.

Ethernet

Ethernet is a networking technology for local area networks (LANs). It is standardized in the IEEE 802.3 standard.

Fast Ethernet

Fast Ethernet is currently a very widespread Ethernet version with 100 Mbit/s transmission rates over twisted-pair cable, according to Category 5 or better. The maximum permitted range is 100 meters.

Fibre Optic Cable

This is a type of cable with a glass fibre or plastic core which is used to transmit signals in the form of light pulses.

Flow control

Flow control is a function for adjusting transmission rates based on the capability of the receiver to receive data. Flow control controls the transmission between the sender and receiver. The sender sends only that amount of data which the receiver is capable of receiving.

Forwarding

Forwarding is a process where the data from one port is forwarded to another port on the switch.

Frame

A frame is a data transmission unit located on level 2 of the OSI model (the security level). The frame contains the header and trailer information that is required for the bit transmission level. All frame formats encompass the frame's starting delimiter, the destination and source address, the data itself, and an error-detection mechanism (frame check sequence).

Full-duplex Operation

Full-duplex or duplex operations refer to communication where both partners can simultaneously send and receive.

Gigabit-Ethernet / 10 GbE (10 Gigabit Ethernet)

Gigabit Ethernet is an Ethernet version that transmits data at a rate of 1000 Mbit/s.

10 GbE works with 10 Gbit/s. Weidmüller offers a connector system with **STEADYTEC**[®] technology especially for such 10 GbE applications.

GPRS (General Packet Radio Service)

GPRS is an extension of the mobile GSM standard for packet-oriented data transmission.

Half-duplex mode

The half-duplex process enables alternating, bidirectional usage of a transmission line (two-way alternating). The interfaces cannot send and receive at the same time.

Hub

A hub is a data communication device which allows three or more other devices to be connected to it in a star topology. Incoming data is forwarded to all other nodes as broadcasts. Hubs are no longer used in Fast Ethernet networks.

IEEE 802.3

1. The IEEE workgroup (Institute of Electrical and Electronics Engineers) concerned with the CSMA/CD transmission process.
2. Also sometimes used as a synonym phrase for LAN or Ethernet.

IGMP snooping

IGMP snooping is a switch-based function. The switch listens in to IGMP traffic at its ports. This prevents multicast traffic from flooding all the ports. The network load is reduced as a result.

Internet

The Internet is the world's largest network. The Internet was developed in the sixties for military purposes and then opened up in the nineties for commercial use. Data transmission on the Internet is based on TCP/IP protocols.

Jabber

The Jabber messaging protocol is a process on Ethernet networks that prevents one station from monopolizing the transmission lines for too long.

LAN (Local Area Network)

A LAN is a network within a local space (for example, in a building).

Link Integrity Test

This test is used to test if an Ethernet connection is properly connected and if the signal is being correctly transmitted. The test is a useful tool but does not by itself prove that the link is fully functional.

Link Layer

The link layer is the security layer in the OSI reference model.

Link Pulse

A link pulse is a detection pulse which is sent from 10Base-T stations to 100Base-T stations for auto-negotiation purposes.

M12, D-coded

The M12 D-coded connector is a version of a four-pole plug used for industrial Ethernet, in compliance with ISO IEC 61076-2-101. The connector can implement Cat.5 data transmission and guarantees IP67-level protection.

MAC Address

A MAC address is a six-byte hardware address which uniquely identifies any network device.

MDI

MDI is an abbreviation for Medium Dependent Interface and relates to Ethernet connections. This indicates the network card connection for the network cable, that is, the network socket.

MDI-X

MDI-X indicates a crossed Ethernet connection. The send and receive interfaces are swapped.

Auto MDI/MDI-X (auto-crossing) enables the send and receive lines on a port to be automatically detected and configured.

Thus, both the connected Ethernet cable (whether crossed or uncrossed) and the remote station's configuration (MDI/MDI-X) are automatically detected. The local port is then configured appropriately.

Media converter

A media converter converts electrical signals into optical signals and vice versa. This allows both copper and fibre-optic cables to be used together in the same network.

Multicast

Multicast indicates a type of transmission which originates from one point and is transmitted at the same time to multiple nodes.

NIC (Network Interface Card)

A NIC (network interface card) is a printed circuit board or other hardware component which connects a terminal device directly to the network.

OLE (Object Linking and Embedding)

Object Linking and Embedding (OLE) in an interface, developed by Microsoft, which is used for linking and integrating the data between different applications. This allows an application to integrate external text, graphics or tables that come from another OLE-compliant application.

OSI (Open Systems Interconnection)

OSI describes the set of standards, as agreed upon internationally, that are used for connecting open systems.

Packet

A data packet is a defined arrangement of characters that are handled as a single unit.

Patch Cable

The patch cable is used in the wiring room for establishing flexible connections between the sub-distribution box and the horizontal cabling level. Patch cables can be either fibre-optic cable or copper cable. They are very flexible and require a very compact bending radius.

PAUSE

In full-duplex mode, this individual frame is transmitted to the available stations in order to inform them that they should reduce transmissions.

PHY (Physical Layer)

1. The physical transmission layer.
2. This can also refer to a transceiver in a Fast or Gigabit Ethernet network.

Point-to-Point Technology

A connection method which uses a direct connection between two terminal devices. Point-to-point connections are found in networks, in directional radio-link transmissions, and at the connection level.

Port

A port is a hardware connection. Normally this is an input/output channel on a computer or another hardware device such as a modem, router or switch.

Port mirroring

Data traffic on a switch can be mirrored from one port to another using this process (useful for troubleshooting or throughput measurements).

Promiscuous Mode

Promiscuous mode refers to a receive mode of operation on a network device. When a network interface on a device is switched to this mode, it reads all incoming data traffic and passes the traffic on for the operating system to process.

Propagation Delay

Propagation delay refers to the time required by a signal to travel from one point on a transmission line to another point.

Protocol

A data transmission protocol establishes the rules and arrangements for exchanging information. A protocol is an agreement which defines the processes for establishing, monitoring, and closing connections.

Quality of Service (QoS)

Quality of service refers to all network services which influence WLAN or LAN data traffic so that a defined level of quality is ensured for the receiver.

RapidRing™

RapidRing is the simplest and quickest method for achieving network redundancy.

Remote Management

A switch can be remotely managed from any network node equipped with telnet or a web browser. The switch must have its own IP address.

Repeaters

A repeater is an active component responsible for repeating (regenerating) on an Ethernet LAN. It amplifies and refreshes signals.

Repeating Hub

This is a repeater with more than two ports (also simply called a hub).

RJ45 / RJ-45

An RJ45 connector is an eight-pole miniature plug used for connecting STP and UTP cables. It is specified by IEC 60603-7 and is noted for its simplicity and small size. RJ45 is used predominantly in inter-floor building cabling and office cabling.

RSTP (Rapid Spanning Tree Protocol)

The Rapid Spanning Tree protocol (RSTP, IEEE 802.3w) is, in addition to RapidRing™, another method for establishing network redundancy

SC Duplex

SC duplex is a mating plug profile for fibre-optic cables. It features simple plugging and unplugging. Its small size enables high-density assembly. It is specified in IEC 61754-4 and used for both single mode and multimode cables.

SC-RJ

The SC-RJ plug is a smaller version of the SC plug. The mating profile is specified in IEC 61754-24. It is used for single mode, multimode and POF cables.

Segment

A network segment is a section of the network bordered by bridges, routers or switches. In a LAN, for example, there are LAN segments and collision domains.

Slot Time

This is an important Ethernet parameter. The slot time corresponds to double the value of the signal dispersion speed (between the two network nodes that are farthest away from each other) and the minimal packet length of 64 bytes. An Ethernet network's performance declines as the slot time increases.

SNMP (Simple Network Management Protocol)

SNMP enables a process for centrally managing a network with many components. The primary goals of SNMP are to minimize the management complexity, to create an expandable protocol, and to maintain the independence of network components.

Spanning Tree Protocol

Refer to RSTP.

ST Plug

This plug was specified by AT&T (in IEC 61754-2). It is suitable for both single mode and multimode fibre-optic cables. The ST plug is used in LANs throughout the world.

Star Topology

Transmitting nodes are shaped like a star in this topology with all connections to a central node. Networks based on star topology must route all data over the central node of the star.

Star-quad Cable

A star-quad cable is a symmetric copper cable with four parallel-stranded cores.

Station

The station is a hardware component on a network: for example a connected terminal device, server, router, telephone, or fax.

Straight-through

In contrast to cross-over cables, straight-through patch cables do not have their send and receive wires crossed over. Instead they are wired and connected one-to-one.

Switch

Switches are network components which perform a switching function. This can be an intermediary switching function for both WLANs and LANs.

Topology

Topology refers to the structure of a network, and can be:

- linear topology
- ring topology
- star topology
- tree topology

Transceiver

A transceiver is a word derived from the combination of transmitter (sender) and receiver. It refers to a device for fibre-optic networks that can both send and receive.

Trunking

Trunking for Ethernet networks refers to the parallel switching of multiple Ethernet links between the same devices. Transmission over parallel links can be used to scale the bandwidth.

Twisted pair cable

Twisted pair cable refers to symmetric copper cable consisting of two wires that are twisted around each other.

VLAN (Virtual Local Area Network)

Virtual networks or virtual LANs are a technical implementation of logical network segments within a physical network. Virtual routing is used to implement such networks.

Web Server

A web server is a server program which serves information to clients using the HTTP protocol. The information is typically in the form of web pages, images, etc.

Acknowledgments

The creation of this usage guide would not have been possible without the help of many people. For their actions, advice and support, we wish to particularly thank André Gerlach from the Network Industry Educational Initiative (BdNI), Manfred Patzke, Stephanie Willert and the Weidmüller Heyfra team, and Jan Klüter. We also thank the many unnamed helpers who have remained in the background on this project.

Simon Seereiner

Bernhard Kusch

Klaus Leuchs

www.weidmueller.com

Weidmüller Interface GmbH & Co. KG

Postfach 3030

32720 Detmold

Klingenbergstraße 16

32758 Detmold

Phone +49 (0) 5231 14-0

Fax +49 (0) 5231 14-2083

E-Mail info@weidmuller.com

Internet www.weidmueller.com

Order number:

1066190000/10/2008/SMMD

