

Power Grids

# EDS500 series - Ethernet & DSL switches

## Part 2: Functions

### Manual Release 2



# Revision

<b>Document identity:</b>		<b>1KGT151021 V000 1</b>
<b>Revision:</b>	<b>Date:</b>	<b>Changes:</b>
0	08/2019	Initial version

# Contents

<b>1</b>	<b>Introduction.....</b>	<b>7</b>
1.1	About the Manual EDS500 series - Ethernet & DSL switches.....	7
1.2	References.....	7
<b>2</b>	<b>Functions.....</b>	<b>9</b>
2.1	Configuration Methods.....	9
2.1.1	Configuration via the Serial Interface.....	9
2.1.2	Configuration via the IP Network.....	9
2.1.3	Configuration via Telnet.....	10
2.1.4	Configuration via SSH.....	10
2.1.5	Configuration via the Web Interface.....	11
2.1.6	Configuration via SNMP.....	11
2.1.7	Configuration via TFTP.....	11
2.1.8	Configuration via Configuration Stick.....	12
2.2	Handling of the Command Line Interface (CLI).....	12
2.2.1	Command Input.....	12
2.2.2	Show Help for Input Format.....	12
2.2.3	Show Commands for Current Hierarchy Level.....	13
2.2.4	Shortcuts to Input Commands Quicker.....	14
2.2.5	Using the Command Stack.....	14
2.2.6	Operation Modes - View (Login) and Configuration (Enable).....	14
2.2.7	Event Messages and Status Messages at the Management Console.....	16
2.3	User Authentication.....	16
2.3.1	Login Mode Password.....	16
2.3.2	Login Mode Radius.....	17
2.3.3	Automatic Session Termination.....	17
2.4	Loading and Saving a Configuration.....	18
2.4.1	Show Configurations.....	18
2.4.2	Modifying Start Configuration.....	18
2.4.3	Power-up, Configuration Stick and Modifications during Runtime.....	19
2.4.4	Transfer, Modification and Archiving Configurations.....	20
2.4.5	Default Configuration and Reset of a Device.....	20
2.5	Handling in the Web Interface.....	21
2.6	Cold Start and Warm Start.....	24
2.6.1	Information about the last Start-up.....	24
2.6.2	Trigger Device warm Start with Command.....	24
2.6.3	Plan Device warm Start with Command.....	25
2.7	Host Name and Description.....	25
2.7.1	Host Name.....	25
2.7.2	Description, Name of Contact and Location.....	25
2.7.3	Display of the System Description.....	26
2.8	VLAN Settings.....	26
2.8.1	Assigning VLANs to Interfaces.....	27

2.8.2	VLAN Properties.....	28
2.9	Configuration of IP Addresses.....	29
2.9.1	IP Address.....	29
2.9.2	Configuration of the System IP Address.....	29
2.9.3	Configuration of VLAN IP Addresses.....	30
2.9.4	Configuration of Unnumbered Interfaces.....	30
2.9.5	Configuration of an IP Address Block for IEC 60870-5-101, IEC 60870-5-104 Conversion.....	31
2.10	Quality of Service.....	31
2.11	Rate Limiting.....	33
2.12	Alarms and Alarm Configuration.....	35
2.13	Ethernet Interfaces.....	37
2.14	Optical Interfaces.....	38
2.15	DSL Interfaces.....	39
2.15.1	Process of Establishing Connection between DSL Interfaces.....	40
2.15.2	Configuration of the Mode (Master, Slave).....	40
2.15.3	Configuration of the Data Rate.....	41
2.15.4	Termination of Link in Case of an Error.....	42
2.15.5	Configuration of Data Encapsulation.....	43
2.15.6	Signal Quality, Line Length and Data Rate.....	43
2.15.7	Link Analysis.....	45
2.16	DSL Channel Bundling.....	48
2.17	Redundancy with a Backup-Group.....	49
2.18	Layer-2-Tunnel.....	50
2.19	Spanning Tree Protocol.....	51
2.19.1	Activate, Deactivate, Spanning Tree Protocol Version.....	52
2.19.2	Commands to Display the Spanning Tree Bridge Information.....	53
2.19.3	Display the Spanning Tree Root Information.....	53
2.19.4	Display the Spanning Tree Port Roles and States.....	53
2.19.5	Display detailed Spanning Tree Information.....	53
2.19.6	Display of Specific Settings for Multiple Spanning Tree (MST).....	53
2.19.7	Configuration of Spanning Tree Bridge Parameters.....	54
2.19.8	Configuration of the Priority for Spanning Tree Port.....	54
2.19.9	Spanning Tree Port Cost.....	55
2.19.10	Spanning Tree Point-to-Point Port Property.....	55
2.19.11	Configuration of the Spanning Tree Port Edge Setting.....	56
2.19.12	Activation of the Spanning Tree Migration Check.....	56
2.19.13	Configuration of Multiple Spanning Tree Parameters.....	56
2.19.14	Assigning VLANs to Multiple Spanning Tree Instances.....	57
2.19.15	Advice on the Operation of Spanning Tree with EDS500 Devices.....	57
2.20	Serial Interfaces.....	57
2.20.1	Usage for Configuration or as Process Interface.....	58
2.20.2	Transmission Parameters of the Interface.....	58
2.20.3	Inactivity Detection for the Command Line Interface (CLI).....	59
2.20.4	Operation as RS-485 Interface.....	59
2.21	Serial Tunnel.....	60
2.21.1	Applications.....	60

2.21.2	Serial Protocols and Sampling Operation.....	62
2.21.3	Topologies and Transmission settings.....	62
2.21.4	Enhanced Parameters of the Serial Tunnel.....	63
2.21.5	Query the Status of the Serial Tunnel.....	65
2.22	IEC 60870-5-101 and IEC 60870-5-104.....	65
2.22.1	Addresses of the EDS500 Device Information Objects.....	65
2.22.2	Connection of Signals and Application as RTU.....	68
2.22.3	Concept of Interface and Polling.....	69
2.22.4	Configuration of an IEC 60870-5-101 Interface.....	70
2.22.5	Configuration of an IEC 60870-5-104 Interface.....	71
2.22.6	Configuration of the Time Monitor (Time-Out).....	71
2.22.7	Activating and Deactivating the IEC 60870-5-101 and IEC 60870-5-104 Interfaces.....	72
2.22.8	Setting Addresses and Address Parameters.....	72
2.22.9	Settings for the Protocol Conversion.....	72
2.22.10	Technological Background of the IEC 60870-5-101,104 Conversion.....	74
2.23	RADIUS.....	84
2.24	Access Control and Device Authentication with IEEE 802.1X.....	85
2.25	Access Lists.....	86
2.25.1	Concept.....	86
2.25.2	Filter for MAC Addresses.....	87
2.25.3	Filter for Ethertype.....	88
2.25.4	Filter for IP Addresses or Ranges.....	88
2.25.5	Filters for the IP Payload Protocol.....	88
2.25.6	Filter for TCP and UDP Ports.....	88
2.25.7	Access Control Lists as Incoming or Outgoing Packet Filter for Interfaces.....	88
2.25.8	Access Lists as Class Map to Qualify QoS of the Data Traffic.....	89
2.26	Syslog and Device Internal Log.....	90
2.27	SNMP Network Management.....	91
2.27.1	SNMP-Agent Settings.....	91
2.27.2	MIB Support.....	92
2.27.3	Vendor Specific Device MIB.....	92
2.27.4	Trap Server and Traps.....	100
2.28	Time Synchronization with SNTP.....	102
2.29	Monitor.....	102
2.30	State Dependencies.....	103
2.31	IP Routing.....	104
2.31.1	Routing with VLAN Interfaces.....	104
2.31.2	Routing Table and Routes.....	104
2.31.3	Configure Routing Protocol RIP.....	105
2.32	Virtual Router Redundancy Protocol (VRRP).....	106
2.33	LLDP Neighbour Recognition.....	107
2.34	Firmware Update.....	107
2.34.1	Update via Command Line Interface (CLI).....	107
2.34.2	Update via Web Interface.....	108
2.34.3	Update via a Management Program or a Script.....	108

2.35	Cryphographic Key.....	108
2.35.1	Device Specific Cryptographic Key.....	108
2.35.2	Generate and Apply Cryptographic Key.....	109
2.36	Certificate Management.....	112
2.36.1	Host Key Type.....	112
2.36.2	Combination of Key and Certificate.....	112
2.36.3	Step-by-Step Instructions.....	117
<b>3</b>	<b>Glossary.....</b>	<b>153</b>

# 1 Introduction

## 1.1 About the Manual EDS500 series - Ethernet & DSL switches

The Manual consists of several parts:

Document identity	Part name	Explanation
1KGT150966	Part 1: Devices	Description of the device portfolio
1KGT151021	Part 2: Functions	Description of the functions
1KGT151018	Part 3: Command reference	Description of the command line interface

Table 1: Parts of the Manual EDS500 series - Ethernet & DSL switches

## 1.2 References

[1]	Individual Ident	EDS500 series Hardware data sheets	Individual hardware data sheets of all devices and auxiliary equipment
[2]	Individual Ident	EDS500 series Operating instructions	Individual operating instructions of all devices and auxiliary equipment





## 2 Functions

### 2.1 Configuration Methods

The devices can be configured as follows:

- connected directly locally or
- remotely via the IP network

The devices support the following configuration methods:

- Configuration via Telnet
- Configuration via SSH
- Configuration via Web interface
- Configuration via SNMP
- Configuration via TFTP
- Configuration via Configuration Stick

#### 2.1.1 Configuration via the Serial Interface

EDS500 series devices can be configured via the serial interface console0 or (if available) console1 if these are in operation mode "configuration".

With a configuration cable (500CAB03, 1KGT038909) the device can be connected to the serial interface of a PC. For the pin assignment and pins of the configuration cable refer to EDS500 Manual - Part 1: Serial Interfaces (Con0 - Con1).

Ready-made cables to connect to a 9-pin Sub-D-plug are available at ABB.

For operation of the command console (command line interface, CLI) use a common terminal program (e.g. Tera Term, PuTTY, HyperTerminal).

The default value for the serial interface is: 57600 Baud 8N1 (8 data bits, no parity, 1 stop bit), no flow control.

With the help of the terminal program you can enter commands as alpha-numeric commands that are executed after pressing "Enter". For operating the command line interface (CLI) refer to Chapter 2.2, "Handling of the Command Line Interface (CLI)"

If a login password has been set for user authentication (Chapter 2.3, "User Authentication"), then this has to be entered when asked to do so before access to the management console is activated.

The RADIUS user authentication is not used when configuring via the serial interface.

#### ADVICE

To keep the display of special characters uniform, we recommend to set the code page of the terminal program to that of the browser (code page ISO-8859-15, Latin-9).

#### 2.1.2 Configuration via the IP Network

All further, in the following described configuration methods require an IP connection to the EDS500 device. After installation a device usually has one or more IP addresses that can be reached via the network. By default all devices have the following settings:

IP Setting	Parameter
IP Address	10.0.0.2
Subnet mask	255.0.0.0
Gateway IP address	10.0.0.1

Table 2: Default values for IP

For further configuration you should first check the network connectivity e.g. with ICMP echo request ("ping"). Use the device IP address as target address.

### 2.1.3 Configuration via Telnet

With the help of a Telnet client program the management console can be accessed.

Prerequisite is the reachability of the device via the IP network (Chapter 2.1.2, "Configuration via the IP Network"). Common programs are PuTTY, HyperTerminal or Microsoft Windows Telnet.exe.

Target address is the device IP address (refer to "Tab. 2: Default values for IP").

Default configuration:

In default configuration Telnet is disabled.

Depending on the system login mode it may be necessary to enter a user name and/or password before the Telnet access to the management console is granted (refer to "User Authentication").

The default value for loginmode is: password. The default login password is empty.

Parameter	User name	User password
Loginmode password	-	Login password
Loginmode radius	RADIUS user	RADIUS password

Table 3: Login with Telnet

After successful login Telnet offers access to the command line interface (CLI) (handling see Chapter 2.2, "Handling of the Command Line Interface (CLI)").

### 2.1.4 Configuration via SSH

The command line interface (CLI) can be accessed with the help of a SSH client program.

Prerequisite is the reachability of the device via the IP network (Chapter 2.1.2, "Configuration via the IP Network")

Common programs are Tera Term, PuTTY or OpenSSH.

Target address is the device IP address (refer to "Tab. 2: Default values for IP").

Default configuration:

In default configuration SSH is enabled.

Depending on the system login mode it may be necessary to enter a user name and/or password before the SSH access is granted to the command line interface (CLI), (refer to Chapter 2.3, "User Authentication").

The default value for loginmode is "password". The default login password is empty.

Parameter	Loginmode password	Loginmode radius
User name		RADIUS user
User password	Login password	RADIUS password

Table 4: Login with SSH

After successful login the SSH connection offers access to the command line interface (CLI) (handling see Chapter 2.2, "Handling of the Command Line Interface (CLI)").

Establishing a connection via SSH can take a few seconds as the encryption has to be negotiated.

### 2.1.5 Configuration via the Web Interface

Using one of the common web browsers like Mozilla Firefox, Opera, Apple Safari, Google Chrome or Microsoft Internet Explorer the web interface of the EDS500 device can be accessed. The major device properties and functions can be set with the web interface. Also, the full extent of the commands can be executed either by typing in the commands into a input field or assemble them by clicking on the keywords. Prerequisite is the reachability of the device via the IP network (Chapter 2.1.2, "Configuration via the IP Network"). Use the device IP address as target URL.

Default configuration:

The Web-Server is activated with the configuration HTTP with redirection to HTTPS.

The handling of the web interface is described in detail in Chapter 2.5, "Handling in the Web Interface" .

### 2.1.6 Configuration via SNMP

Some of the device parameters can be set via SNMP access, see Chapter 2.27, "SNMP Network Management" . Prerequisite is the reachability of the device via the IP network (refer to Chapter 2.1.2, "Configuration via the IP Network"), and activated write access with SNMP.

The default value for the write community string is: private.

### 2.1.7 Configuration via TFTP

The Trivial File Transfer Protocol (TFTP) is a very simple file transfer protocol. TFTP only supports reading or writing files. The EDS500 managed switches uses TFTP to transfer for example firmware, config files and certificates from and to the device.

The device configuration as a whole (refer to Chapter 2.4, "Loading and Saving a Configuration" , running-config, startup-config, stick-config) can be downloaded as a file via TFTP and uploaded again from a TFTP server to a device (startup-config, stick-config).

Prerequisite is the reachability of the device via the IP network (Chapter 2.1.2, "Configuration via the IP Network").

The TFTP transmission has to be started with the command line interface (CLI) (via serial terminal, Telnet or SSH), via the web interface or via SNMP.

### 2.1.8 Configuration via Configuration Stick

If you plug in a configuration stick at the EXT plug during booting an EDS500 series device, then that configuration is used (refer to Chapter 2.4, "Loading and Saving a Configuration").

This enables e.g. a fast exchange of a faulty device when the configuration stick is plugged into the replacement device. After power-up the configuration of the exchanged hardware is identical to the faulty device.

## 2.2 Handling of the Command Line Interface (CLI)

The command line interface (CLI) of the EDS500 devices can be accessed with a terminal program using the serial connection, with Telnet or SSH. Access is also possible with graphical support of the web interface. All functions and settings of the EDS500 devices can be configured by the command line interface (CLI).

### 2.2.1 Command Input

A command is entered as an alphanumeric command and concluded with "Enter". After complete and correct input the command is executed.

---

#### Input a command

---

```
switch>show interface
```

```
<show interface>
```

```
Interface Summary:
```

Interface	Admin	State	Link state	Speed	SQ	Alias
dsl1	up		down	8192 kbps	-	-
system0	up		up	100 Mbps	-	-
port1	up		up	100 Mbps!	-	-
port2	up		down	auto	-	-
port3	up		down	auto	-	-
port4	up		up	100 Mbps!	-	-
console0	up		up	57600 bps	-	-

```
! : auto negotiated
```

---

Errors during input lead to an error message. This shows that the command parser could not find match for the entered command.

---

#### Input error for a command:

---

```
switch>show imterface
```

```
% Unknown command: 'show imterface'
```

```
switch>
```

---

### 2.2.2 Show Help for Input Format

Some commands require the input of parameters that have to follow a certain format. If such a command is entered and the required parameter is not present or in an invalid format then a help text is displayed.

---

**Help text after incomplete input of a command**


---

```
switch>ping

<ping *>

Usage: ping [-arp] {IP address}

switch>
```

---

**ADVICE**

To get a help text about the input of a parameter you have to enter the command without parameters but with a following blank space and acknowledge it with Enter.

**ADVICE**

Help texts use curly brackets {} to symbolize a parameter. For alternatives the | character is used. Optional parameters are enclosed in square brackets [].

### 2.2.3 Show Commands for Current Hierarchy Level

The command line interface (CLI) of the EDS500 devices offers an online help to show the further input options of the current hierarchy level.

The list of input options is shown after entering the question mark (?) or pressing the tab key.

---

**Command list at the top hierarchy level**


---

```
switch>?

enable exit ping show telnet

switch>
```

---



---

**Command list at the hierarchy level <show ?>**


---

```
switch>show ?

alarm arp cdp debug dot1x iec101 iec104 interface ip mac mir-
roring monitor neighbor router stp switch system tcp udp ver-
sion vlans

switch>show
```

---



---

**Command list at the hierarchy level <show system ?>**


---

```
switch>show

system ? frame-counters snmp sntp syslog temperature

switch>show system
```

---

The example shows, how the command <show system temperature> can be found.

## 2.2.4 Shortcuts to Input Commands Quicker

EDS500 devices accept abbreviated input of commands as soon as they are unambiguous. Not all keywords have to be typed in the full extent.

---

### Concatenated input of commands

---

```
switch>sh mo
<show monitor>
Monitor is disabled.
switch>
```

---

If the input command is ambiguous this is reported.

---

### Input of ambiguously concatenated command

---

```
switch>sh m

% Ambiguous command

switch>
```

---

If there is an ambiguity it is possible to get a list of further options with the question mark (?) or pressing the tab key .

---

### Listing for concatenated command input

---

```
switch>sh m?

mac mirroring monitor

switch>sh m
```

---

## 2.2.5 Using the Command Stack

The command line interface (CLI) has a command stack for the last 5 commands.

With the help of the cursor-up and cursor-down keys the list of commands can be scrolled. It shows always only one command.

The currently shown command can be edited.

Pressing the Enter key executes the command.

The command stack is purged at Logout or Disable (refer to Chapter 2.2.6, "Operation Modes - View (Login) and Configuration (Enable)").

## 2.2.6 Operation Modes - View (Login) and Configuration (Enable)

The management console of the EDS500 managed switches has a two-level access concept: view mode and operation mode configuration.

Most of the system parameters can be shown in view mode whereas safety critical settings are excluded.

The view mode is accessed with a successful login. Depending on the connection type to the management console (CLI) (serial, Telnet, SSH...) and depending on the user authentication

scheme (refer to Chapter 2.3, "User Authentication") a login name and/or a login password have to be entered.

In operation mode configuration all system parameters can be shown and all commands for system configuration can be executed. The operating mode configuration is accessed at the management console with the command `<enable>` after login to the command line interface (CLI).

Depending on the set user authentication scheme (refer to Chapter 2.3, "User Authentication") a login name and/or a login password have to be entered for the operating mode configuration.

The command `<disable>` terminates operation mode configuration. Afterwards, the device is in view mode.

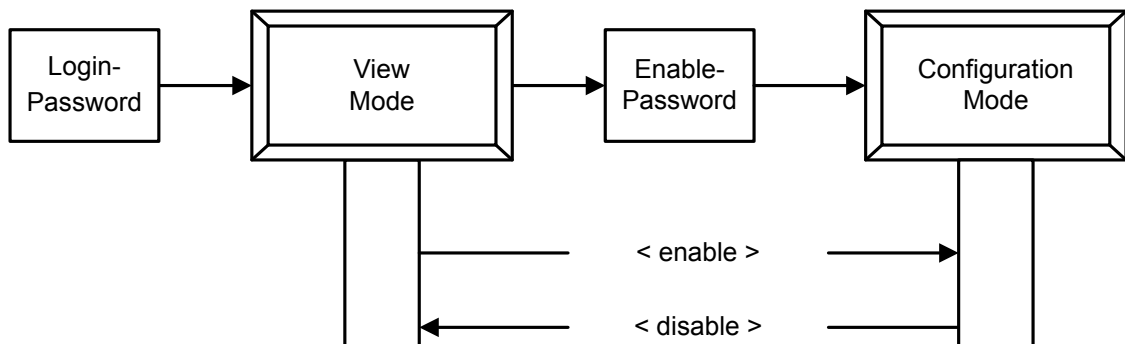


Figure 1: Access modes

The command `<exit>` terminates view mode and operating mode configuration and closes the command line interface (CLI).

The prompt at the command line interface (CLI) shows the current access mode:

---

#### Prompt for view mode

---

```
switch>
```

---

The symbol `>` indicates the login permission (view mode).

---

#### Prompt in operation mode configuration

---

```
switch#
```

---

The symbol `#` indicates the operation mode configuration.

---

#### Entering and exiting operation mode configuration

---

```
switch>enable
<enable>
switch#
switch#disable
<disable>
switch>
```

---

Depending on the connection type to the command line interface (CLI) (serial, Telnet, SSH...) the operation mode configuration and view mode are automatically terminated after a configurable period (auto-logout and auto-disable), refer to Chapter 2.3.3, "Automatic Session Termination".

## 2.2.7 Event Messages and Status Messages at the Management Console

Event and status messages and processes like changes of interfaces, user login events and changes of the system states are stored in an internal memory, refer to Chapter 2.26, "Syslog and Device Internal Log".

In addition to storing the messages in the system log, they are also sent to the first available management console that has at least login permissions. It is called terminal monitor. Alternatively, the terminal monitor can be redirected to any other management console by a command from the target management console.

### ADVICE

The default value for the function of the serial interface Console0 is: monitor.

Commands to set the terminal monitor:

```
<terminal monitor>
<terminal no monitor>
```

## 2.3 User Authentication

Access to the command line interface (CLI) (refer to Chapter 2.2, "Handling of the Command Line Interface (CLI)") and the web interface (refer to Chapter 2.5, "Handling in the Web Interface" ) is protected by a two-step authorization concept (refer to Chapter 2.2.6, "Operation Modes - View (Login) and Configuration (Enable)").

The default value for passwords is "" (empty). It is recommended to set a new password during first login. This reminder will appear as long as no password is not set.

The following sections describe how the device can be protected against unauthorized access.

### ADVICE

The web application login (local authentication) is not used for user administration. It is recommended to manage the user administration via Radius which supports various password policies. The local authentication does not support password policies.

### 2.3.1 Login Mode Password

The login mode determines in what way the user is authenticated.

The default value for loginmode is: password.

Login password and password for the operation mode configuration (enablepass) are not set.

This means that any access (via serial interface, Telnet, SSH or web interface) is allowed without password.

### ADVICE

Passwords may be up to 20 characters long and contain upper and lower-case characters, numbers and special characters.



**ADVICE**

Danger of an unreachable system due to different character encoding.

When accessing the system the code page used by the accessing program has to be ISO 8859-15 (Latin-9). Due to different character encoding of diacritical characters on login, different code pages may lead to falsely interpreted and, hence, invalid passwords. The system may become unreachable.

Commands to set the login mode and passwords

```
<set system loginmode password>
<set loginpass {...}>
<set no loginpass>
<clear loginpass>
<set enablepass {...}>
<set no enablepass>
<clear enablepass>
```

### 2.3.2 Login Mode Radius

As an alternative to the loginmode password that uses a fixed password for authentication, a login is also possible with the help of a (remote) authentication server. User name and password combinations can be verified by a RADIUS server.

To use the login mode radius on a EDS500 device, the RADIUS server that can be reached via the network has to be configured first, refer to Chapter 2.23, "RADIUS". If no RADIUS server is configured the login mode password stays active as a fall-back. After successful login with RADIUS (e.g. via Telnet or SSH) the user is in view mode. If the web interface is used with RADIUS, the user is in operation mode configuration after authentication.

Commands to set login mode radius

```
<set system loginmode radius>
```

**ADVICE**

Serial connections to the command line interface (CLI) via serial connections are not authenticated by RADIUS but always with the login and enable password (refer to Chapter 2.3.1, "Login Mode Password").

### 2.3.3 Automatic Session Termination

To avoid that authenticated connections stay open due to a forgotten logout there is an automatic function for logout and disable on EDS500 managed switches.

A timeout can be set for the access to the management console via serial connections, Telnet connections, SSH connections and the Web-interface.

A serial connection to a management console gets only terminated if a login password is set and the value for idle-logout timeout does not equal 0.

The default value for the automatic termination of the operation mode configuration after inactivity is 600 seconds.

The default value for the automatic termination of the view mode is 1200 seconds.

Commands to set the automatic logout / disable

```
<set interface {console...} idle-logout {...}>
<set interface {console...} idle-disable {...}>
<set telnet idle-disconnect {...}>
<set system web-server session-timeout {...}>
<set system ssh idle-disconnect {...}>
```

## 2.4 Loading and Saving a Configuration

All device settings are configured via commands.

A particular device state corresponds to a certain set of commands that is called a configuration. Configurations can be loaded and saved device internally but can also be stored on external servers for backup or installation of further devices with an identical configuration and can be loaded from there to the respective device.

The configuration that runs on a device is called running-config. All configuration command input is saved as running-config.

### ADVICE

Configuration commands that reset parameters to default values in the current operation are not stored as command as the default values get loaded first at reboot and then the configuration commands are executed that set the values to special settings.

The persistent configuration memory, the startup-config, allows a device to restore a configuration after a restart. The stored configuration commands are executed during start-up and create the initial running-config.

In addition to the device internal startup-config an optional external hot-pluggable storage in the shape of a configuration stick is available. It can be plugged permanently into the device or be connected if required and can be used for the following tasks:

- Quick exchange of a device in case of a failure without new configuration
- Applying a standard configuration
- Backup of a device configuration on portable hardware.

An EDS500 device detects the configuration stick automatically during operation. If the configuration stick is plugged into the device at power on then the configuration is loaded from the stick and copied to the internal configuration memory. A previously saved startup-config gets overwritten.

### 2.4.1 Show Configurations

Commands to show the configurations

```
<show config>
<show running-config>
<show startup-config>
<show stick-config >
```

### 2.4.2 Modifying Start Configuration

Commands to modify the start configuration

```
<write>
<write memory>
```

```

<copy running-config startup-config>
<copy running-config stick-config>
<clear startup-config>
<clear stick-config>
<set config-stick read-only>
<set config-stick no read-only>

```

#### ADVICE

If a configuration is copied to the internal startup-config then it is also copied to the configuration stick if that is plugged in and not write-protected.

#### ADVICE

An empty configuration is not identical with the default configuration. The default configuration represents the state at the time of shipping and eases the access to the device (Chapter 2.4.5, "Default Configuration and Reset of a Device").

### 2.4.3 Power-up, Configuration Stick and Modifications during Runtime

At start-up there is no running-config yet. The device internal start up configuration is loaded and the included commands are executed. The result is the initial running-config that is identical to the startup-config. If during operation further configuration commands are executed then the running-config is modified. If the configuration stick is plugged in during operation then the stored configuration can be accessed. There is no automatic transfer of the configuration.

The data of the configuration stick is used not before a restart of the device and then the data is copied to the startup-configuration.

"Tab. 5: Modification of configuration with and without plugged-in configuration stick" shows which configuration is modified by which action.

Action	Current device configuration (running-config)	Internal startup configuration (startup-config)	Configuration stick (stick-config)
1. Delivery State	-	A1	-
2. Power on (no configuration stick)	A1	A1	-
3. Command input <set ...>	A2	A1	-
4. Command input <copy running-config startup-config>	A2	A2	-
5. Command input <set ...>	A3	A2	-
6. Plug in configuration stick	A3	A2	B1
7. Command input <copy running-config stick-config>	A3	A2	A3
8. Command input <set ...>	A4	A2	A3
9. Device restart (with configuration stick)	A3	A3	A3

Table 5: Modification of configuration with and without plugged-in configuration stick

## 2.4.4 Transfer, Modification and Archiving Configurations

Configurations cannot only be displayed on the devices but can also be copied over the network as files.

Like that, configuration data can be archived (centrally).

It is possible to edit configurations at a workstation and then transfer them to the devices.

The web interface (refer to "Handling in the Web Interface") gives a comfortable overview. Files can be uploaded or downloaded via the web browser or via TFTP. TFTP transmissions can also be started via SNMP (refer to Chapter 2.27, "SNMP Network Management").

The command line interface (CLI) has copy commands, to load files from a TFTP or save them on a TFTP server.

During the execution of the copy command, the IP address of the TFTP server and the required file names are requested interactively.

If a configuration is copied from a TFTP server to the device the format is checked for plausibility.

Commands to transfer the configurations

```
<copy tftp {...}>
<copy running-config {...}>
<copy {...config} tftp>
```

## 2.4.5 Default Configuration and Reset of a Device

The default configuration of a device contains configuration commands that allow access to the broadest set of functions of a system. On shipping all devices have the default configuration. The default configuration is not identical with an empty configuration.

Device Settings	Value	Implicit default value	Explicit command
System IP	10.0.0.2	Yes	No
Subnet mask	255.255.255.0	Yes	No
Gateway address	10.0.0.1	10.0.0.1	No
Host name	switch	Yes	No
System VLAN	none	Yes	No
Ethernet ports	Admin state up	No	Yes
Ethernet speed	Auto Negotiation	Yes	No
Optical ports	Admin state up	No	Yes
Opt. port speed	100 Mbps, Full Duplex	Yes	No
DSL ports	Admin state up	No	Yes
Properties dsl1	Master, 192 kbps	Yes	No
Properties dsl2	Slave, auto speed	Yes	No
Serial interfaces	Operation mode con- figuration	Yes	No
Baud rate	57600 bps, 8N1	Yes	No
Telnet	Disabled	Yes	No
SSH	Enabled	Yes	No

Table 6: Parameters of the default configuration

Device Settings	Value	Implicit default value	Explicit command
Web interface	Enabled	No	Yes
SNMP	Enabled	Yes	No
Read-Community-String	public	Yes	No
Write-Community-String	private	Yes	No

Table 6: Parameters of the default configuration

To reset a device to the default values automatically, the following options are available:

- Via command `<reload -default-config>`
- At the serial interface console0 during startup and pressing the key i(gnore) once.

Instead of the start up configuration the default configuration is loaded. The device internal startup configuration remains unchanged. For security reasons the start up configuration cannot be accessed after booting with the default configuration.

If the device should use the default values permanently then the default configuration has to be saved with the command `<write>`.

#### 2.4.5.1 Method 1: Reset with Command

Command to restart a device with the default configuration.

```
<reload -default-config>
```

#### 2.4.5.2 Method 2: Reset during Startup of Device

During start-up the serial interface console0 is always in operation mode configuration (interface settings 57600 Baud, 8N1), even if it is configured as process interface or similar after start-up. During start up the key i may be pressed once to signal to ignore the start up configuration. Subsequently, this has to be acknowledged by pressing the Enter key.

##### Start-up with loading the default configuration:

```
Performing self-test:
Testing LEDs... [done]
Testing memory... [ok]
Testing stack... [ok]
Loading image... [ok]
Keystroke <i> has been detected.
Press Enter to confirm to ignore config, otherwise press any
other key: Enter

Testing I-Bus... [ok]

Ignoring config, loading default...
```

## 2.5 Handling in the Web Interface

The EDS500 devices provide a web-based interface for configuration. The web interface can be used with common web browsers like Mozilla Firefox, Opera, Apple Safari, Google Chrome or Microsoft Internet Explorer.

Default configuration:

The Web-Server is activated with the configuration HTTP with redirection to HTTPS.  
An IP connection between a PC and the device is required for configuration.

Enter the IP address of the device into the URL field of the browser to access the web interface.

If a non-standard TCP port is configured for the web server then the port must be appended to the IP address by a colon and the port number.

The default value for TCP port is: 80.

The default value for TCP secure port is: 443.

Only if a different TCP-port is to be used then it has to entered in the address explicitly.

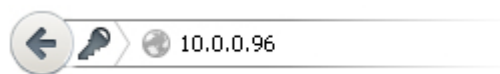


Figure 2: Input of the IP address to access the web interface

After calling the URL in the browser, a dialogue pops up for authentication. Depending on the set mode for user authentication (refer to Chapter 2.3, "User Authentication") enter the access data.

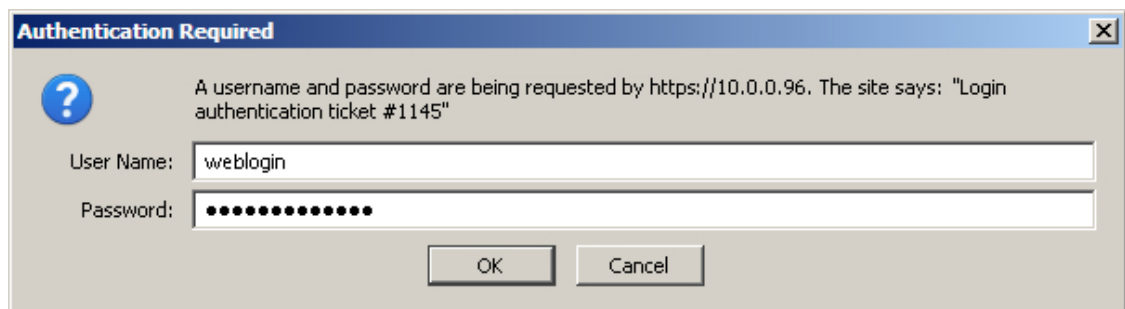


Figure 3: Dialogue for authentication when accessing the web interface

Login mode	User name	Password
password	weblogin	Login password or Enable password
radius	RADIUS user name	RADIUS user password

Table 7: Access data for Web interface

The default value for loginmode is: password. The default login password is empty.

Login with user name edslogin but without password.

The web interface allows to differentiate between view mode and configuration mode (refer to Chapter 2.2.6, "Operation Modes - View (Login) and Configuration (Enable)"). Depending on the configuration of the login password and enable password you have read-only or read-write permissions in the web interface.

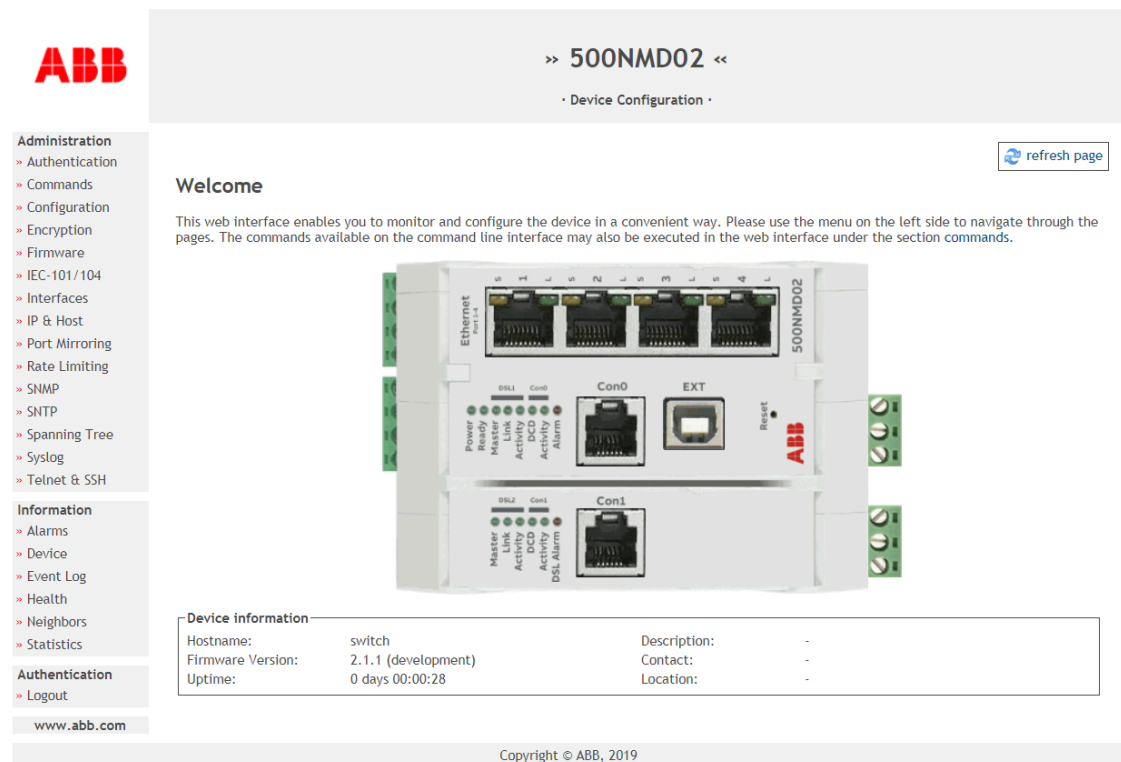


Figure 4: Web interface of a 500NMD02

Login password	Enable password	Password input for view mode	Password input for configuration mode
not configured	not configured	not possible	Empty password
not configured	Configured	Empty password	Enable password
Configured	not configured	not possible	Login password
Configured	Configured	Login password	Enable password

Table 8: Permissions for access of the Web interface

On the left side of the web interface you find the navigation menu, the display area on the right shows information and possible settings. There are hyperlinks to specific configuration pages in the navigation menu for the main function units.

All modifications initiated by the web interface effect the running configuration (running-config) of the device.

Settings that have no dedicated web page can be executed with the help of the built-in command parser of the web interface.

The function "Commands" is the interface to the command line interface (CLI) of the device (Chapter 2.2, "Handling of the Command Line Interface (CLI)"). Click on the command hyperlink to get from one command level to the next or execute a command similar to the character oriented access methods like Telnet or serial terminal when pressing the Enter key.

If required, icons are shown to inform about e.g. system alarms or that the running-config has not yet been saved.

Commands to configure the web interface

```
<set system web-server enable [http-and-https | no-https |
only-https | redirect-to-https]>
```

```
<set system web-server no enable>
<set system web-server port {1-65536}>
<set system web-server secure-port {1-65536}>
<set system web-server session-timeout {...}>
```

## 2.6 Cold Start and Warm Start

The device performs a cold start after the power supply is switched on.

A warm start is performed when the device is initialized without switching off the power supply. A warm start can be triggered by pressing the reset button, refer to EDS500 Manual - Part 1: Reset Button, as well as by command or due to a device failure.

The command for a restart can be executed via the command line interface (CLI) at the management console, the web interface or SNMP.

The restart interrupts all connections on all interfaces. First all LEDs light up (LED test, refer to EDS500 Manual - Part 1: Display Elements).

As soon as the start-up has been concluded successfully (about 30 seconds after switching on the device) the display Ready switches to green. At this time the specified device configuration has been loaded (refer to Chapter 2.4, "Loading and Saving a Configuration").

### 2.6.1 Information about the last Start-up

The general output on system information includes the device uptime since the last system start (system uptime) and the reason for the restart (last reload reason). Possible triggers are:

Last reload reason	Description
coldstart	Power up
warm start (hardware reset)	Press reset button
warm start (software reset)	Restart after command
warm start (watchdog)	Device fault

Table 9: Last reload reason

Commands to show the system information

```
<show system>
```

### 2.6.2 Trigger Device warm Start with Command

Commands for restart of device

```
<reload>
<reload -force>
<reload -default-config>
```

#### ADVICE

<reload -force> can potentially set the device into a state in which it is incapable of starting. A device with such a defect has to be returned for repair.



### 2.6.3 Plan Device warm Start with Command

When modifying the configuration of a remote device it can get into a state in which it cannot be reached any more.

To get an automatic reset of the device settings you can use a planned restart.

A planned restart resets the device to the startup configuration if the planned restart is not cancelled or a modified configuration has been saved with the command <write>.

While the timer for the planned restart is running the remaining time is reported in intervals of days, hours, 10 minutes and finally minutes.

Commands to plan a delayed start

```
<reload later {1-525600}>
<reload cancel>
```

## 2.7 Host Name and Description

Besides a host name further metadata can be set to describe a EDS500 device to grant unique identification and easy location in the network. Especially in larger networks this feature becomes important.

### 2.7.1 Host Name

The host name is the unique identification for a device in the network. The host name of an EDS500 device may be up to 20 characters long and consist of any combinations of characters, numbers and special characters.

The default value for Hostname is: switch.

A Hostname should consist only of 'A'-'Z', '0'-'9', '-' and '.' and the case is not significant.

Do not use any special characters or the underscore to comply with RFC 1123 (Requirements for Internet Hosts).

Command to set the host name

```
<set system hostname {...}>
```

#### ADVICE

The host name is used as prompt at the command line interface (CLI).

#### Display of the host name as prompt at the command line interface (CLI)

```
switch#set system hostname test
```

```
<set system hostname *>
```

```
Hostname set.
```

```
test#
```

### 2.7.2 Description, Name of Contact and Location

Setting this meta data is optional. Use the descriptions to e.g. save identification data for your organisation.

The names correspond to the objects in the group “system “ of the SNMP MIB-2.

The maximum length is 50 characters.

The default value for a description is empty.

Commands to set system descriptions

```
<set system description {...}>
<set system contact {...}>
<set system location {...}>
```

### 2.7.3 Display of the System Description

In addition to the web interface and the SNMP MIB-2 group system the system description can be displayed at the command line interface (CLI):

---

#### Display of the system description

---

```
M2-USPW#show system
```

```
<show system>
```

---

```
System Description:  Modem 2 Umspannwerk
Location:           Station Umspannwerk / Schaltschrank 4
Contact:            Max Mustermann
Temperature:        38.1875 deg. Celsius
Time:               time server not set
[...]
```

---

## 2.8 VLAN Settings

Virtual networks allow to transmit different services separated from each other over the same infrastructure. Although the physical topology of a network connects all network elements, setting VLANs can take care that the individual logical topologies are separated from each other. This separation can fulfil among others a security aspect. But also in respect to the performance aspect can the assignment of priorities lead to a preferred transmission of certain data (refer to "Quality of Service").

The EDS500 devices support VLANs according to standard IEEE 802.1Q. According to this, Ethernet frames get an additional VLAN tag that shows the membership to a specific VLAN id.

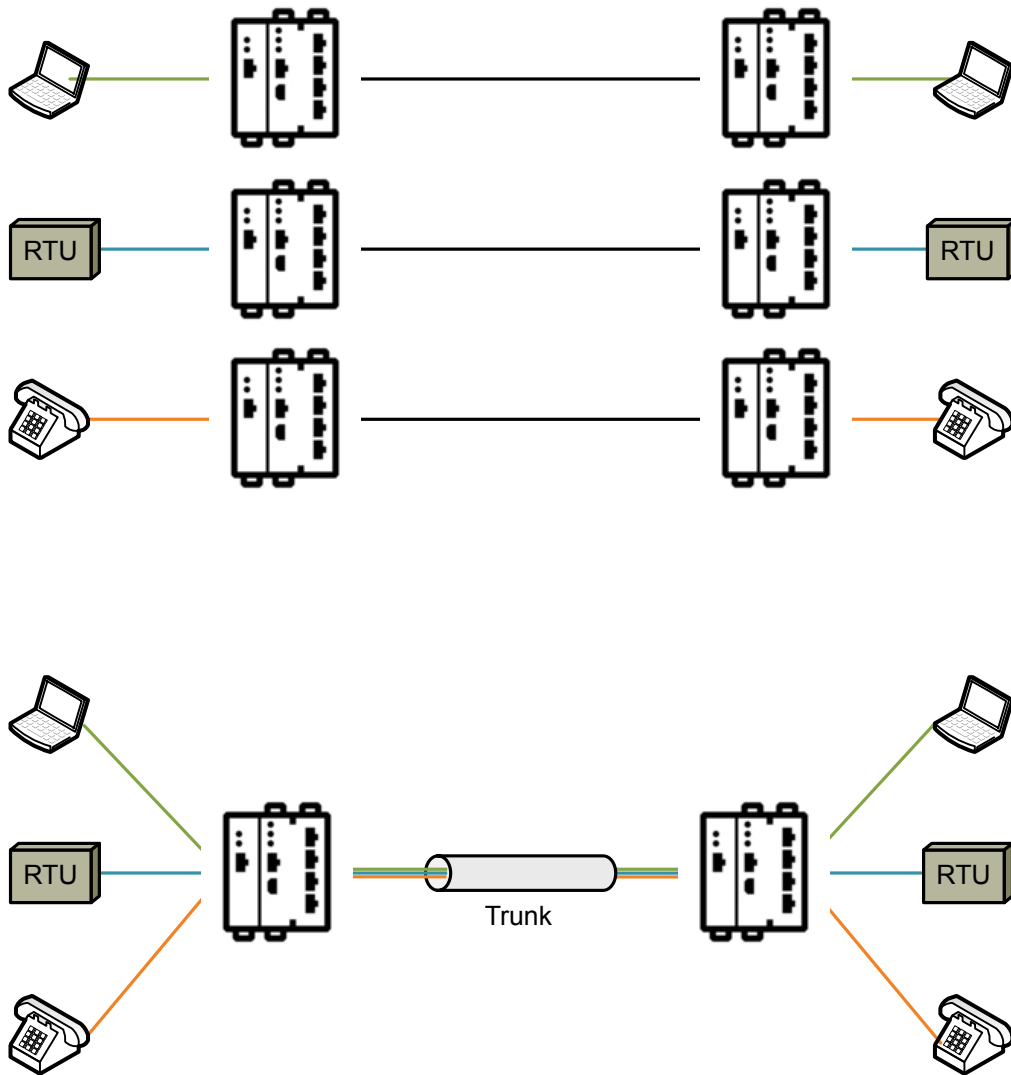


Figure 5: Using VLANs

Default configuration:

In default configuration VLANs are disabled.

### 2.8.1 Assigning VLANs to Interfaces

The interfaces of the EDS500 devices can transmit Ethernet frames either without 802.1Q VLAN tag (untagged, Access-Port) or with VLAN tag (tagged, Trunk-Port). For this you can select a VLAN id from the range between (including) 1 and 4094.

Access ports are used mainly to connect terminal devices. On an access port incoming Ethernet frames get a VLAN tag, frames that leave the port in the direction of the terminal device get stripped off the VLAN tag and the data is transmitted untagged. Each access port is associated with exactly one VLAN id.

Those interfaces that connect the network infrastructure are configured as trunk ports. Ethernet frames are transmitted with 802.1Q VLAN tag (tagged). You must differentiate between secure trunk ports and trunk all ports. While trunk all ports accept and transmit any VLAN id (and are therefore not associated with specific VLAN ids), the secure trunk ports have

a filter function: only those Ethernet frames are transmitted where the VLAN tag has a VLAN id that is assigned to a secure trunk port. Each secure trunk port can be associated with up to 16 VLAN ids.

The VLAN ids do not have to be defined in e.g. a VLAN table but can be assigned directly to the interfaces. In total 16 different explicit VLAN ids can be defined system-wide (trunk all ports are not counted for this).

#### Commands to configure VLANs on interfaces

```
<set interface {channel...} access-vlan {...}>
<set interface vlan {1-4094} ip-address [{IP address} [{IP
address range end}] {subnet mask}] | {unnumbered vlan {vlan-
id}}>
<set switch {fo1 | fo2} access-vlan {1-4094}>
<set interface {channel...} trunk-vlan [{1-4094} | all]>
<show vlans>
<set interface {tunnel...} trunk-vlan {...}>
<set interface tunnel0 trunk-vlan [{1-4094} | all]>
<set stp msti {...} [no] vlan {...}>
<set stp msti {1-4094} vlan {1-4094}>
<set stp msti {1-4094} no vlan {1-4094}>
<set switch {port1 | port2 | port3 | port4} access-vlan
{1-4094}>
<set switch port1 access-vlan 10>
<set switch {port1 | port2 | port3 | port4} trunk-vlan
[{1-4094} | all]>
<set switch port3 trunk-vlan all>
<set system radius source vlan {1-4094} [dependency
{inverse-monitor | monitor}]>
<set system snmp trap-source vlan {1-4094} [dependency
{inverse-monitor | monitor}]>
<clear interface {channel...} trunk-vlan {...}>
<clear interface {dsl...} access-vlan>
<clear interface {fastethernet...} access-vlan>
<clear interface {fastethernet...} trunk-vlan {...}>
<clear interface {tunnel...} access-vlan>
<clear interface {tunnel...} trunk-vlan {...}>
<clear interface console source vlan [{1-4094}]>
<clear interface vlan {...} gateway>
<clear interface vlan {...} ip-address [...]>
<clear interface vlan {1-4094} vrrp id>
<clear switch {fo...} access-vlan>
<clear switch {fo...} trunk-vlan {...}>
<clear switch {port...} access-vlan>
<clear switch {port...} trunk-vlan {...}>
<clear system radius source vlan [{1-4094}]>
<clear system snmp trap-source vlan [{1-4094}]>
<clear system snmp source vlan [{1-4094}]>
<clear system syslog source vlan [{1-4094}]>
```

## 2.8.2 VLAN Properties

For an easier identification a description can be set per VLAN, e.g. "VoIP", "Guest" or "Management".

Different VLANs are strictly separated from each other in respect to data traffic.

A MAC table contains the assignment between learnt MAC addresses and interfaces. It is possible to assign an individual MAC table to a VLAN.

The property mac-table can be set to:

- shared
- individual

Up to 16 individual MAC tables can be defined.

The default value for the MAC table is: shared.

When using MSTP (Chapter 2.19.13, "Configuration of Multiple Spanning Tree Parameters") each MST instance has its own MAC table, that is valid for those VLANs of an MSTI that set their MAC tables to shared.

Commands to configure VLAN properties

```
<set vlan {1-4094} alias {string20}>
<set vlan {1-4094} mac-table individual>
<set vlan {1-4094} mac-table shared>
```

## 2.9 Configuration of IP Addresses

To access the EDS500 devices e.g. for network management purposes or to use the device functions like tunnelling, IEC 60870-5-101 / IEC 60870-5-104 conversion or to use the devices as IP routers it is necessary to define one or more IP addresses. The devices support the IP protocol version 4 and 6.

### 2.9.1 IP Address

The default value for the IP address is: 10.0.0.2.

If several devices are connected to a network without individually changing the IP address it cannot be predicted which device is reached under the IP address 10.0.0.2.

Property	Value
IP Address	10.0.0.2
Subnet mask	255.0.0.0
Gateway IP address	10.0.0.1

Table 10: Default values for the IP configuration

### 2.9.2 Configuration of the System IP Address

The system IP address and corresponding subnet mask can be set with a command. To reach IP addresses outside one's own subnet a gateway IP address can be set.

The system IP address and system gateway IP address describe a network without VLAN configuration (frames without VLAN tag and frames without IEEE 802.1p priority tag).

If the system IP address is not used then it should be deactivated. The same applies to the gateway IP address that remains at 10.0.0.1 without explicit configuration.

**Commands to configure system IP address and gateway**

```

<set system ip {IP address}>
<set system subnetmask {subnet mask}>
<set system gateway {IP address}>
<set system no ip>
<set system no gateway>
<show system>
<show interface ip-address>

```

**2.9.3 Configuration of VLAN IP Addresses**

When using IEEE 802.1Q VLANs these are isolated from each other and cannot reach especially the system IP address. Therefore a so-called VLAN interface with one IP address can set up VLANs under which this device is reachable in this VLAN (up to 16 VLANs).

For each VLAN interface an IP address and a subnet mask and optionally a gateway IP address can be set. When setting the IP addresses take care that the ranges of the VLAN IP addresses are not in the same subnet as the other IP addresses of the same device.

To migrate an existing system IP address to a specified VLAN use the command `<set system vlan {1-4094}>`. The system IP address and the system gateway are deactivated and the formerly set IP address and gateway for the specified VLAN interface are activated. The other way round, the configuration of an individual VLAN interface can be adopted as system IP address and gateway with the command `<set system vlan none>`.

**Commands to configure VLAN IP addresses**

```

<set system vlan {...}><set system vlan {1-4094}>
<set system vlan {1-4094}>
<set interface vlan {1-4094} ip-address [{IP address} [{IP
address range end}] {subnet mask}] | {unnumbered vlan {vlan-
id}}>
<clear interface vlan {1-4096} ip-address [{IP address}]]>
<show interface ip-address>

```

**2.9.4 Configuration of Unnumbered Interfaces**

Unnumbered interfaces are used for IP routing to avoid to equip a point-to-point connection with an individual IP subnet but to re-use the IP address of another (local) IP interface. This can drastically reduce the number of configured IP sections.

The two IP addresses of the WAN/point-to-point connection are not in the same subnet.

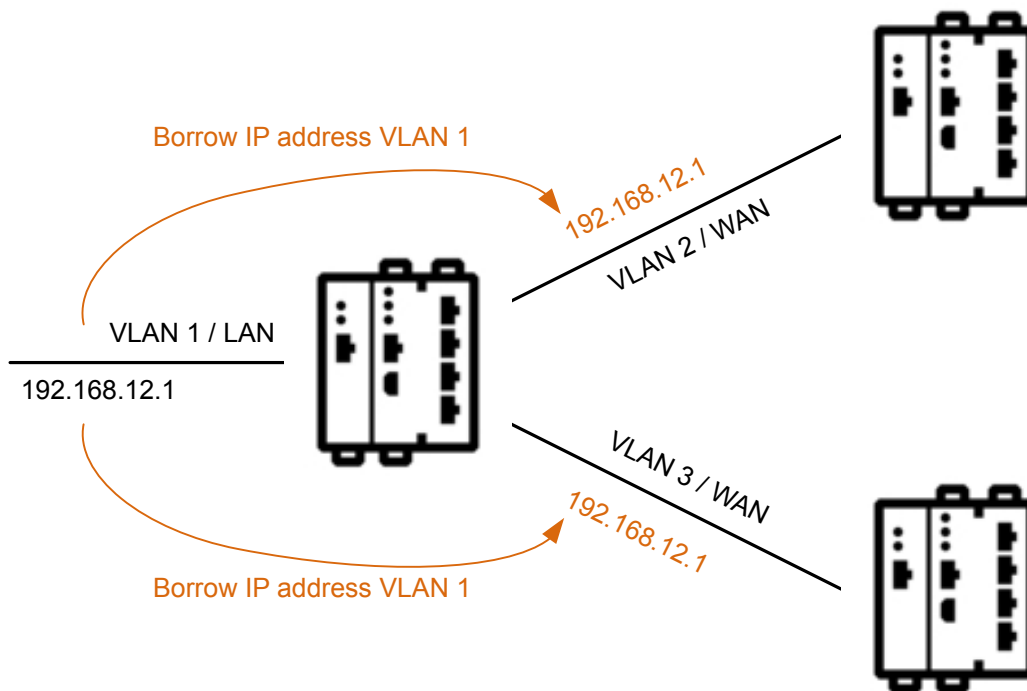


Figure 6: Unnumbered interface

Command for configuration of an unnumbered VLAN interface

```
<set interface vlan {1-4094} ip-address unnumbered vlan
{vlan id}>
```

### 2.9.5 Configuration of an IP Address Block for IEC 60870-5-101, IEC 60870-5-104 Conversion

During the operation of the IEC 60870-5-101 / IEC 60870-5-104 conversion, link addresses (IEC 60870-5-101) are translated to IP addresses (IEC 60870-5-104). For each IEC 60870-5-101 connection an individual IP address can be assigned to the IEC 60870-5-104 side. To get the required number of IP addresses the EDS500 devices have the option to reserve a whole block of IP addresses instead of only one. For this a second parameter with IP address is added that marks the included end of the block. When setting the block, take care that it is included completely in the subnet set by the subnet mask. Only the first IP address has to be considered a full-fledged one. All the following ones are especially for the IEC 60870-5-101 / IEC 60870-5-104 conversion.

Commands to configure an IP address block

```
<set system ip {start-IP-address end-IP-address}>
<set interface vlan {1-4094} ip-address [{IP address} [{IP
address range end}] {subnet mask}] | {unnumbered vlan {vlan-
id}}>
<show interface ip-address>
```

## 2.10 Quality of Service

If at a network node the transmission rate of an interface is not sufficient to transport the occurring traffic then, either, Ethernet frames have to be discarded or the incoming frames have to be slowed down with the help of flow control. Using flow control can avoid that

frames are lost but potentially huge delays may arise for all connections so that the use of flow control together with QoS is not recommended.

The default value for flow-control is: off.

With the use of QoS (Quality of Service) Ethernet frames get a priority. If an overload situation occurs at one place in the network then it is decided under consideration of the IEEE 802.1p tag priority which frames should be preferred and which are discarded. Like this, e.g., it can be guaranteed to transport critical data traffic and less important connections may be delayed.

Higher values for priority are better (lower probability of loss) than low ones.

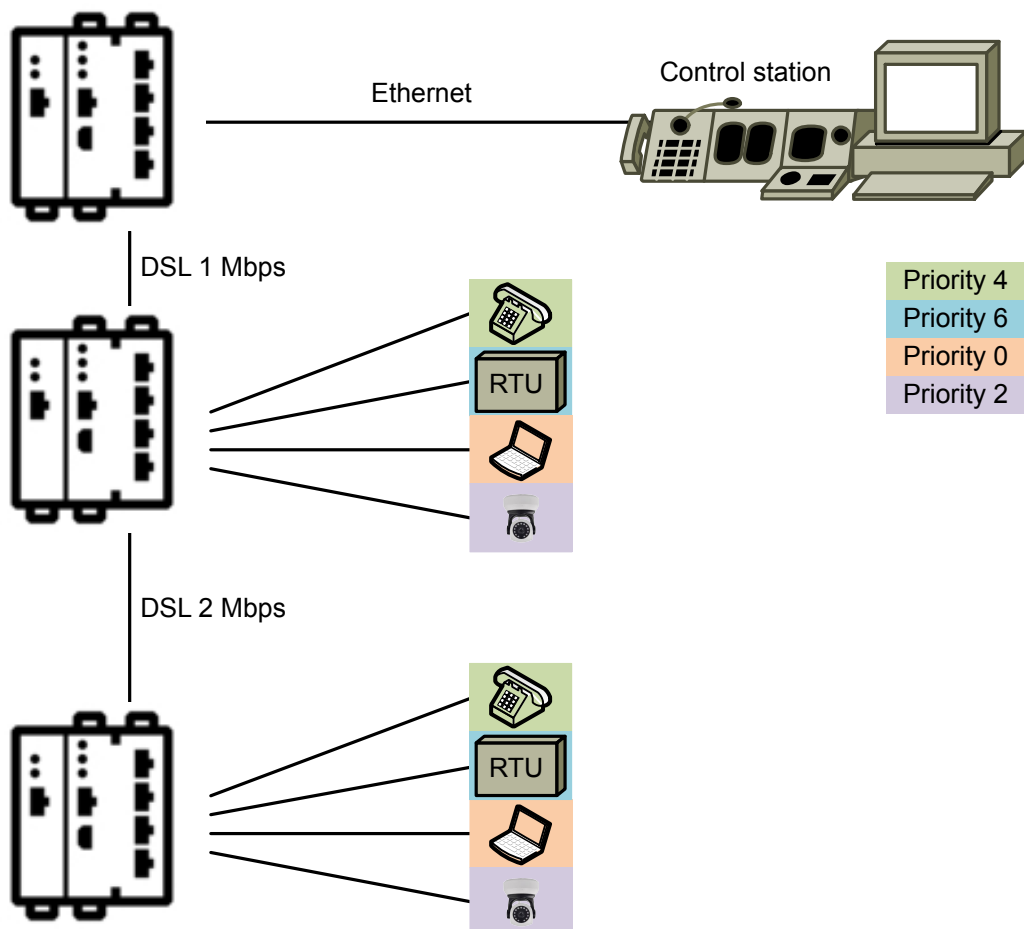


Figure 7: Priorities for data traffic in the network with QoS

To avoid that certain services get compromised, their priority is set to a higher level. In this example the telecontrol link of the RTUs has priority over all other links, especially the IP cameras.

EDS500 devices have eight priorities (CoS, Class-of-Service) according to IEEE 802.1p. These are divided into four non-blocking queues.

The default value for the processing of this queue is: weighted-fair.

This avoids the blocking of lower priorities.



CoS (Class-of-Service)	Queue	Weighted-Fair priority
7	0	8
6		
5	1	4
4		
3	2	2
2		
1	3	1
0		

Table 11: Class-of-Service and queues

If any loss of data of the critical services should be avoided at high loads on the bandwidth then the scheduling has to be set to strict i.e. the priority queuing has to be modified.

To set the connections for the network infrastructure (when using VLANs then these are the trunk ports) where the IEEE 802.1p priority is considered these ports have to trust the CoS tag (example: <set switch port1 trust cos>).

The default value for trust is: cos.

If instead incoming frames on a port should be assigned to a fixed CoS (when using VLANs these are the access ports) then, on the one hand, the port CoS has to be configured (example: <set switch port1 cos {0-7}>) and, on the other hand, the port has to be configured in such a way that possibly existing tags are not used to determine the priority but the set CoS (example: <set switch port1 trust none>).

If QoS is to be used without VLANs then the IEEE 802.1p tag has to be activated explicitly for that port (priority tagging). Otherwise the packets are forwarded without tag. (Example: <set interface port1 encapsulation eth-dot1p>).

Commands to configure QoS

```
<set switch scheduling {...}>
<set system cos {...}>
<set switch {port...} cos {...}>
<set switch {port...} trust {...}>
<set switch {port...} encapsulation {...}>
```

## 2.11 Rate Limiting

While QoS/IEEE 802.1p CoS takes care that frames can be prioritized at the place where bandwidth overload happens, it is the task of the rate limiting to limit the incoming or outgoing data rate at an interface in general. It can also be set which frame types should be limited and can be used as broadcast storm control function.

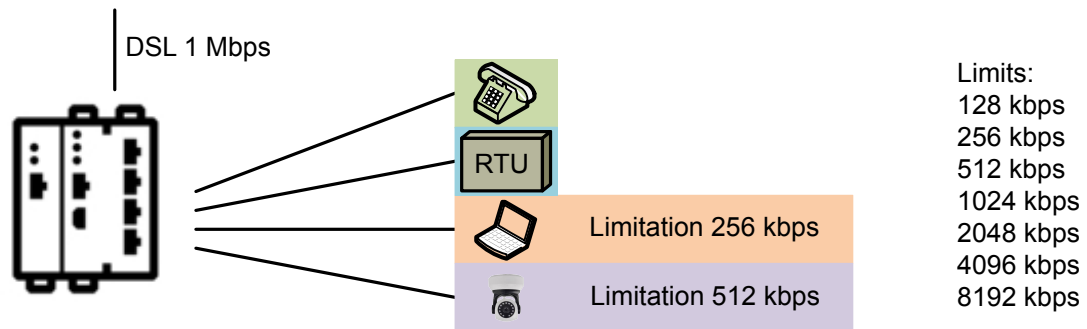


Figure 8: Rate Limiting per port

In estimating the bandwidth, already when feeding in the data stream a later overload situation can be avoided in the further network.

Default configuration:

In default configuration receive-rate-limit and transmit-rate-limit are not set.

Some typical estimations for bandwidth requirements are:

Data transmission type	Quality
Voice over IP	ISDN-grade approx. 80 kbps
	GSM-grade approx. 16 kbps
Serial tunnel	Appr. 64 kbps
IP camera (VGA, 25 pictures per s)	Still picture: H.264 approx. 440 kbps - 1,7 Mbps
	Moving picture: MPEG-4 app. 735 kbps - 2,4 Mbps
	MJPEG app. 8,8 Mbps - 12,1 Mbps
IEC 60870-5-104 (TCP/IP)	Appr. 64 kbps

Table 12: Estimation of bandwidth requirement

When limiting the rate limiting only to certain frame type then the rate limiting can be used as broadcast storm control.

Limit mode	Effect
all	The rate of all frames is limited
flooding	The rate of unicast frames with unknown target, multicast- and broadcast frames are limited.
multicast	The rate of multicast- and broadcast frames are limited.
broadcast	The rate of broadcast frames is limited.

Table 13: Rate limiting and frame types

Commands to configure the Rate limiting:

```
<set switch {port...} limit-mode {...}>
<set switch {port...} {receive-rate-limit | transmit-rate-limit} {...}>
```

## 2.12 Alarms and Alarm Configuration

EDS500 devices have an alarm concept to communicate certain error conditions with an alarm relay, LEDs for display or software signalisation. The individual alarms (referring to interfaces or the system) are summarised in the system-wide alarm state. The alarms have three levels of severity.

Alarm level	Description	Alarm- Relais state	System alarm LED (Alarm)	Subsystem Alarm LED (DSL Alarm, FO Alarm)
No alarm / information	There are no or only informative conditions	Normal	Off	No alarm: off Information: on
Warning	Pre alarm: there is a noncritical error	Normal	Flashing	On
Alarm	Alarm: there is a critical error	Alarm	On	On

Table 14: Alarm level and signalling

The alarm relais is described in EDS500 Manual - Part 1: Alarm-Relais (X2).

The LED display is described in EDS500 Manual - Part 1: Display Elements.

The alarm table can be displayed via the command line interface (CLI) and the Web interface.

The alarm table can also be evaluated with SNMP (refer to Chapter 2.27.3, "Vendor Specific Device MIB" and Chapter 2.27.4, "Trap Server and Traps").

Alarm	Stage	Enabled (as default value)	Configurable	Reason	Command
Speed mismatch	Warning	Yes	Yes	Negotiated data rate does not match set data rate.	<set switch {fo1   fo2} [no] {warn-duplex-mismatch   warn-speed-mismatch}>
Link down	Alarm	No	Yes	Shows that the link is interrupted.	<set switch fo1 alarm-ifdown>
Link up	Alarm	No	Yes	Shows that the link is established.	<set switch fo1 alarm-if-up>
Overtemperature	Alarm	Yes	Yes	The allowed system temperature has been exceeded.	<set system overtemp-warning {40-125}>
System booting	Alarm	Yes	No	The system starts anew.	
Duplex mismatch	Warning	Yes	Yes	Settings for duplex of the communication partners do not match (shared links?)	<set switch {fo1   fo2} [no] {warn-duplex-mismatch   warn-speed-mismatch}>
Link aggregation mismatch	Alarm	Yes	No	Settings for channel bundling do not match as one of the	

Table 15: Alarms

Alarm	Stage	Enabled (as default value)	Config- urable	Reason	Command
				partners has not set channel bundling.	
Signal quality warn threshold reached	Warning	Yes	Yes	Quality of signal too low.	<set interface {dsl1   dsl2} sqthreshold {{threshold}   no} [alarm   warning]> <set switch {fo1   fo2} sqthreshold {{threshold}   no} [alarm   warning]>
Signal quality alarm threshold reached	Alarm	Yes	Yes	Threshold for signal quality has been subseeded.	<set interface {dsl1   dsl2} sqthreshold {{threshold}   no} [alarm   warning]> <set switch {fo1   fo2} sqthreshold {{threshold}   no} [alarm   warning]>
SSH server not ready	Warning	Yes	Yes	SSH session cannot (yet) be established.	<set system ssh [no] warn-ifnotready>
SSH server not ready	Alarm	Yes	Yes	Alarm if no session is ready for a connection.	<set system ssh [no] alarm-ifnotready>
SFP is not inserted	Information	Yes	No	Shows that a link has been activated but no SFP is plugged in.	
Internal switch uplink down	Alarm	Yes	No	Internal hardware error condition.	
SHDSL encapsulation mismatch	Alarm	Yes	No	Incompatible SHDSL settings.	
Internal switch interconnect down	Alarm	Yes	No	Internal hardware error condition.	
Ethernet remote fault	Alarm	Yes	Yes	Ethernet alarm; for optical connections: only one connected fibre.	<set switch {fo1   fo2} [no] {alarm-if-down   alarm-ifremote-fault   alarm-if-up}>
Monitor is up	Alarm	No	Yes	Monitoring by the monitor is normal.	<set monitor [no] {alarm-ifdown   alarm-if-up}>
Monitor is down	Alarm	No	Yes	Monitoring by monitor is in the state "backup".	<set monitor [no] {alarm-ifdown   alarm-if-up}>

Table 15: Alarms

Certain alarms are set in such a way that they can occur during system start (or as a reaction to configuration commands).

A list of possible alarms can be displayed with the command `<show alarm enabled>`. As soon as an alarm condition applies to one of these alarms it is activated and adopted by the system-wide state.

The list of active alarms can be displayed with the command `<show alarm active>`. The web interface has also an overview of possible and active alarms.

Commands for alarm configuration

```
<show alarm [...]>
<set switch {fo...} [no] {alarm-...}>
<set switch {fo...} sq-threshold {...}>
<set switch {fo...} [no] {warn-...}>
<set system ssh [no] alarm-if-notready><set switch {fo...}
[no] {alarm-...}>
<set system ssh [no] warn-if-notready>
<set interface {dsl...} [no] {alarm-...}><set system ssh
[no] alarm-if-notready>
<set interface {dsl...} sq-threshold {...}>
<set system overtemp-warning {...}>
<set monitor [no] {alarm-if-down | alarm-if-up}>
```

## 2.13 Ethernet Interfaces

The Ethernet ports of the EDS500 devices are IEEE 802.3 compliant interfaces capable of Fast Ethernet, auto negotiation, auto sense and flow control designed as RJ-45 plugs (8P8C) (see EDS500 Manual - Part 1: Ethernet interfaces (Port1 - Port4)). They support 100Base-TX and 10Base-T.

The default value for speed is: auto (Nway).

Therefore, usually no special configuration of the Ethernet connection settings is necessary. Still, the following settings can be configured manually:

- Data rate (auto/10/100 Mbps)
- Duplex (auto/full/half)
- Flow control (auto/on/off)

The default value for the interfaces is: shutdown.

Using the default-config (refer to Chapter 2.4.5, "Default Configuration and Reset of a Device") grants simple connectivity and sets the interface (Admin State = up) to this value: no shutdown.

The Admin state of a link can be controlled by the following commands: `<set switch {fo1 | fo2} [no] shutdown>`.

The auto MDI-X setting which is active by default, allows to establish Ethernet connections with normal or twisted pair cables. A command can set the connection type to 'MDI' or limit it to 'MDIX'.

For a better identification of a connection in a topology each optical interface can have a description (alias).

The current link state of the Ethernet interface can be displayed in an overview. Detailed information about the data traffic that runs over an Ethernet interface is also available and can be requested alternatively via RMON (SNMP).

#### Commands to configure Ethernet interfaces

```
<set switch {port1 | port2 | port3 | port4} shutdown>
<set switch {port1 | port2 | port3 | port4} no shutdown>
<set switch {port1 | port2 | port3 | port4} speed {...}>
<set switch {port1 | port2 | port3 | port4} duplex {...}>
<set switch {port1 | port2 | port3 | port4} auto-mdix {...}>
<set switch {port1 | port2 | port3 | port4} flow-control
{...}>
<set switch {port1 | port2 | port3 | port4} alias
{string20}>
<show switch {port1 | port2 | port3 | port4}>
<show switch {port1 | port2 | port3 | port4} frame-counters
>
```

## 2.14 Optical Interfaces

The optical Ethernet ports of the EDS500 devices are IEEE 802.3 compliant Fastethernet interfaces, that are designed as SFP plug-ins according to INF-8074i (see EDS500 Manual - Part 1: Optical Interfaces (Fo1 - Fo2)).

### WARNING

Only transceivers up to laser class 1 according to EN 60825-1 are allowed to be used for the SFP interfaces.

The plug for the optical fibres is of the type Duplex LC (IEC 61754-20, TIA604-10-A).

The supported transmission rate is fixed to 100 Mbps.

The default value for duplex is: full.

The settings can be modified with <set switch fo1 duplex half> and <set switch fo2 duplex half>.

The default value for the interfaces is: shutdown.

Using the default-config (refer to Chapter 2.4.5, "Default Configuration and Reset of a Device") grants simple connectivity and sets the interface (Admin State = up) to this value: no shutdown.

For a better identification of a connection in a topology each optical interface can have a description (alias).

The current link state of an optical interface can be displayed in an overview. Detailed information about the data traffic that runs over an Ethernet interface is also available and can be requested alternatively via RMON (SNMP).

#### Commands to configure optical interfaces

```
<set switch {fo1 | fo2} shutdown>
<set switch {fo1 | fo2} no shutdown>
<set switch {fo1 | fo2} duplex {...}>
<set switch {fo1 | fo2} alias {string20}>
```

```
<show switch {fo1 | fo2}>
<show switch {fo1 | fo2} frame-counters >
```

#### ADVICE

For optical interfaces the alarm 'Ethernet remote fault' means that only one of two optical fibres has a link. If such an alarm occurs then the fault has to be searched in send direction.

#### ADVICE

A pre-alarm and an alarm exist to monitor the signal quality of an optical interface when a threshold is passed.

The default value to trigger the pre-alarm signal quality warn threshold reached is: 1 dB

The default value to trigger the alarm signal quality alarm threshold reached is: 0.5 dB

For further alarms see Chapter 2.12, "Alarms and Alarm Configuration".

Commands to configure alarm thresholds

```
<set switch {fo1 | fo2} sq-threshold {{threshold} | no}
[alarm | warning]>
```

## 2.15 DSL Interfaces

The DSL interfaces of EDS500 devices are SHDSL interfaces (Single-pair High-speed Digital Subscriber Line) according to ITU-T G.991.2.

The interfaces are not compatible to ADSL or VDSL, that is frequently used by internet providers.

EDS500 Manual - Part 1: DSL interfaces of compact devices (X3 - X4) show the specification of the interfaces and give advice on the electrical installation.

The default value for all DSL interfaces is: shutdown.

Using the default-config (refer to Chapter 2.4.5, "Default Configuration and Reset of a Device") grants simple connectivity and sets the interface (Admin State = up) to this value: no shutdown.

On shipping the interface dsl1 is set to master mode and interface dsl2 is set to slave mode. This can be modified with a command refer to Chapter 2.15.2, "Configuration of the Mode (Master, Slave)". Subsequently take care that an interface in the mode master is connected to an interface in the mode slave.

The data rate can be adapted in a wide range.

The default value for speed of the interface dsl1 is 192 kbps.

The default value for speed of the interface dsl2 is auto.

For settings and possible combinations refer to Chapter 2.15.3, "Configuration of the Data Rate". To select the best data rate in respect to the required distance refer to Chapter 2.15.6, "Signal Quality, Line Length and Data Rate".

The configuration of a controlled interruption of a line in case of interruptions of the transmission refer to Chapter 2.15.4, "Termination of Link in Case of an Error".

To connect legacy devices of the HYTEC EDS series with actual devices via DSL you have to activate the compatibility mode on both sides, refer to Chapter 2.15.5, "Configuration of Data Encapsulation".

For a better identification of a connection in a topology each DSL interface can have a description (alias).

The current link state of the DSL interface can be displayed in an overview. The link quality can also be seen there. Detailed information about the data traffic that runs over an DSL interface is also available and can be requested alternatively via RMON (SNMP). For a further analysis of the connection state refer to Chapter 2.15.7, "Link Analysis" .

Commands to configure DSL interfaces

```
<set interface {dsl1 | dsl2} shutdown>
<set interface {dsl1 | dsl2} no shutdown>
<show interface {dsl1 | dsl2}>
<show interface {dsl1 | dsl2} frame-counters>
```

### 2.15.1 Process of Establishing Connection between DSL Interfaces

DSL interfaces can be activated and deactivated with commands.

The default value for all DSL interfaces is: shutdown.

Connection process:

- 1 A suitably DSL counterpart is discovered.
- 2 The connection properties are negotiated.
  - > DSL Activity-LED flashes for up to a minute.
  - > DSL Link-LED is off.
- 3 Link established successfully.
  - > DSL Link-LED lit permanently.
  - > DSL Activity-LED flashes to indicate payload traffic.
- 4 Link not established successfully.
  - > Negotiation phase newly starts.

For details on LEDs see also EDS500 Manual - Part 1: Display Elements .

Commands to activate or deactivate the DSL interfaces

```
<set interface {dsl1 | dsl2} shutdown>
<set interface {dsl1 | dsl2} no shutdown>
```

### 2.15.2 Configuration of the Mode (Master, Slave)

The operation mode of the interfaces of a DSL line has to be configured in such a way that the interface on the one side is set to mode master and the interface on the other side is set to mode slave.

The default value for mode of the interface dsl1 is master.

The default value for mode of the interface dsl2 is slave.

Commands can modify these settings as required.

Legacy EDS500 devices additionally have the setting Jumper, where the mode of interfaces dsl1 and dsl2 is set by a hardware jumper on the main board.

The default valuemode on Legacy EDS devices is: jumper.



The identification plate shows the default value for the operation mode: master, slave or jumper.

Commands to configure mode Master or Slave on DSL interfaces

```
<set interface {dsl1 | dsl2} mode {jumper | master | slave}>
```

#### ADVICE

Devices with dedicated DSL Master LED signal the current state also optically, refer to EDS500 Manual - Part 1: Display Elements.

## 2.15.3 Configuration of the Data Rate

The data transmission rate of a DSL line can be set on both sides of a line. The following combinations are possible:

- Both sides with a fixed data rate
- One side with a fixed data rate, the other with auto-negotiation
- Both sides with auto-negotiation

### 2.15.3.1 Both Sides with a fixed Data Rate

Data rate at the local side	Data rate at the remote side
192 ... 15000 kbps in steps of 8 kbps	192 ... 15000 kbps in steps of 8 kbps

Table 16: DSL connection with fixed data rates on both sides

Data rates of up to 5696 kbps are compliant to ITU-T Standard G.991.2 or G.991.2 Annex F respectively. Rates beyond this use a proprietary technique.

### 2.15.3.2 One Side with a fixed Data Rate, the other with Auto-Negotiation

Data rate at the local side	Data rate at the remote side	SHDSL Standard
192, 256, 512, 768, 1024, 1280, 1536, 1792, 2048 or 2304 kbps	auto	ITU-T G.991.2
192, 256, 512, 768, 1024, 1280, 1536, 1792, 2048, 2304, 2560, 3072, 3584, 4096, 4608, 5120 or 5696 kbps	ext-auto	ITU-T G.991.2, ITU-T G.991.2 Annex F

Table 17: DSL connection with auto-negotiated and fixed data rate respectively

### 2.15.3.3 Both Sides with Auto-Negotiation

#### ADVICE

This method is not advised! Even though always the highest achievable rate is selected, it can be different with every negotiation.

### 2.15.3.4 Recommendations for Operation

The general recommendation for the operation of DSL lines is to set one side to a fixed data rate and the other to auto-negotiation. It is recommended to set that station to auto-

negotiation that is further away or cannot be reached as easily. Like that in case of an error the option to set the reachable side to a lower data rate to re-establish the line.

For an estimation of the achievable data rate at a given distance refer to Chapter 2.15.6, "Signal Quality, Line Length and Data Rate"

#### ADVICE

Setting a DSL data rate interrupts the connection and starts a new negotiation. Special care has to be taken if the configuration of the corresponding line is carried out by oneself.

The default value for speed of the interface dsl1 is 192 kbps.

The default value for speed of the interface dsl2 is auto.

Commands to configure the data rate of DSL interfaces

```
<set interface {dsl1 | dsl2} speed {{192-15000} | auto |
ext-auto}>
```

#### ADVICE

If compatible data rates have not been set on both sides of the DSL line, a connection establishment can happen (if possible on that line). This causes the alarm Speed mismatch (Alarm LED flashes, DSL Alarm LED permanently lit) (refer to Chapter 2.12, "Alarms and Alarm Configuration").

### 2.15.4 Termination of Link in Case of an Error

Depending on the application scenario it can be desirable to interrupt the logical interface connection as quickly as possible when there is an interrupted or intermittently errored transmission line or to keep it as long as possible during a perhaps only temporary interruption.

The error rate of DSL interfaces is monitored by the system. If it reaches a threshold that is dynamically adapted to the transmission rate then the connection is terminated and re-established. The threshold can be set with a command.

Setting	Description
fast	This setting detect a line interruption within a few milliseconds but there is the danger that the connection has to be interrupted and re-established due to very shortlived interferences. For a quick convergence of a redundancy protocol like Spanning Tree it is important that the information on link failures is recorded as quickly as possible. On the other hand it may not be desirable that a failure in the range of milliseconds causes a convergence process that potentially takes a couple of seconds.
slow	This sets an error threshold to a high value, so that the link becomes more tolerant to interferences and a short disruption does not lead to terminate the connection. However, the detection of a cable failure (line interruption) takes longer, up to a maximum of 6 seconds. Logically, the line appears to be OK during this time. This setting can be sensible in periodically errored environments if it is desirable that the connection does not fail regularly.
medium	This is the default and should represent the best compromise for most transmission lines between robustness of the connection on the one hand and detecting a cable fault on the other hand.

Table 18: Settings to terminate a DSL connection

Commands to configure the connection cut of DSL interfaces

```
<set interface {dsl1 | dsl2} badline-disconnect {fast |
medium | slow}>
```

## 2.15.5 Configuration of Data Encapsulation

The legacy EDS500 devices and 3rd party equipment may use another kind of data encapsulation for the DSL transmission than current devices. Still, two devices of different generations or vendors can be connected via a common mode. In case of legacy EDS500, this device should be configured to the interface mode slave and the counterpart correspondingly to the mode master (refer to Chapter 2.15.2, "Configuration of the Mode (Master, Slave)").

Device types, connected to each other	DSL data encapsulation on both sides
Current devices	hdlc-enhanced
Current device with EDS500 legacy	hdlc-compatible
EDS500 legacy with EDS500 legacy	hdlc-native
Current devices with third party	efm

Table 19: Data encapsulation to connect with legacy EDS500 devices

### ADVICE

The DSL interfaces of any two devices have to be connected with the same data encapsulation.

Commands to configure the data encapsulation of DSL interfaces

```
<set interface {dsl1 | dsl2} encapsulation {efm | hdlc-
compatible | hdlc-enhanced | hdlc-native}>
```

## 2.15.6 Signal Quality, Line Length and Data Rate

### 2.15.6.1 Signal Quality

The signal quality describes the quality of a connection on the receive side as relative signal-noise-ratio in dB, that is based on an absolute signal-noise-ratio of 30 dB at which a bit error probability of  $10^{-7}$  occurs.

The achievable signal quality depends on the impedance of the line (resistance, capacity and inductivity) and the interference through other signals. For this the cable type (attenuation, shield), the connections (impedance discontinuity) and naturally the length of the line play a role. On each side of the connection a value for the DSL signal quality is determined in the device; these values are not necessarily identical on both sides (refer to Chapter 2.15.7, "Link Analysis").

To have a buffer against fluctuations in quality (e.g. caused by interferences or cable faults) it is sensible to aim for a minimum value for signal quality. Depending on the application area (especially in respect to occurring interferences) values of 3 dB, 6 dB or more can be necessary. But also an operation with a signal quality of 0 dB (bit error rate of  $10^{-7}$ ) is possible.

### ADVICE

A pre-alarm and an alarm exist to monitor the signal quality of a DSL interface when a threshold is reached.

The default value to trigger the pre-alarm Signal quality warn threshold reached is 1 dB

The default value to trigger the alarm Signal quality alarm threshold reached is 0.5 dB

For further alarms see Chapter 2.12, "Alarms and Alarm Configuration".

Command to modify the alarm behaviour

```
<set interface {dsl1 | dsl2} sq-threshold {{threshold} | no}
[alarm | warning]>
```

### 2.15.6.2 Estimation of Line Length

To estimate an existing (and installed) line's length it is reasonable to investigate the ohmic resistance. For this a short circuit can be applied at the one end of a 2 wire line (connect line 1 with line 2) and measure the resistance with an Ohm meter at the other end. According to "Tab. 20: Typical line resistance per km" and the following formula the line length can be estimated.

Line length:  $l = R_L / 2R_T$

The resistance measured with the Ohm meter is called  $R_L$ , the comparison value from the table is called  $R_T$ . The values in the table describe the typical line resistance per kilometre at a given line diameter.

Diameter [mm]	Resistance $R_T$ [ohms/km] Diameter [mm]	Resistance $R_T$ [ohms/km] Alu- minium wire
0.4	137.7	210.9
0.6	61.2	93.7
0.8	34.4	52.7
1.0	22.0	33.7

Table 20: Typical line resistance per km

### 2.15.6.3 Estimation of Transmission Rate

In general no definitive predictions can be made about the achievable data rates at a certain line length as this depends on the signal quality of the DSL signal. However reference values can be given.

As a reference a family of curves is shown for a copper wire with 0.8 mm wire diameter (shielded telecommunication cable) with low noise. The horizontal axis shows the distance in km, the vertical axis shows the signal quality.

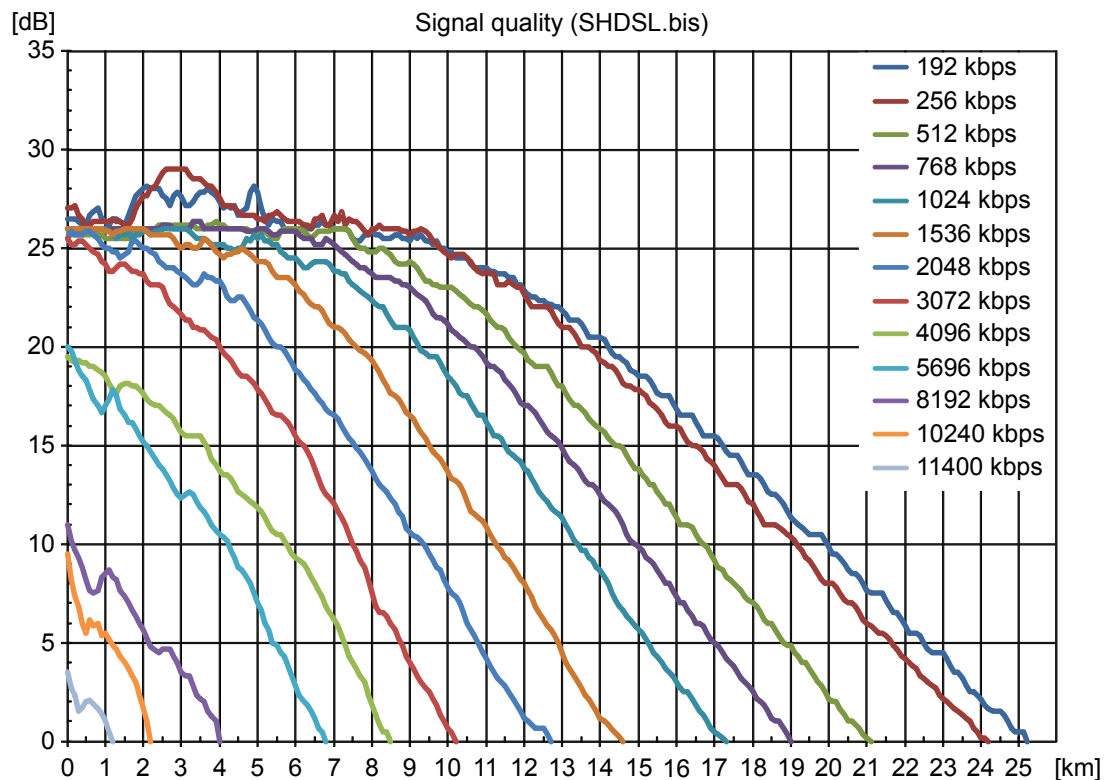


Figure 9: Achievable signal quality in relation to distance

## 2.15.7 Link Analysis

### 2.15.7.1 Information and Frame Statistics

To get an overview over the state of a DSL link, the output of the command `<show interface dsl1>` and `<show interface dsl2>` can be used. It shows information on the link quality and frame statistics.

#### Example of the display of DSL interfaces

```
switch>sh int dsl1
```

```
<show interface dsl1>
```

```
DSL interface 1 is up, line protocol is up (took 0 days
00:01:02). DSL mode is set to master, encapsulation is hdlc-
enhanced. Interface speed is 1024 kbps.
```

```
Incoming QoS tag is trusted. Priority is based on 802.1p tag,
cos is set to 0 if no tag found. Outgoing QoS tag enabled for
native vlan 0. Interface is the spanning tree port 128.2, des-
ignated and forwarding.
```

```
Frame Statistics:
```

Dir.	Good	Dropped	CRC Err.	Fragment	Align E.	Oversize	Non-Unic.
Out	990360	0	-	-	-	-	982288
In	3681	0		0	0	0	3681

```
1/10/60 s out data rate is 5/5/5 kbps, in is 0/0/0 kbps.
```

### Example of the display of DSL interfaces

Link uptime is 0 days 23:44:57 (4 transition(s) to up)

Signal quality: 26 dB

Lineloss ratio: 0 dB

Display	Description
DSL interface 1 is up	Interface dsl1 is operating.
line protocol is up	Connection to remote location.
(took 0 days 00:01:02)	Establishing the link took 1 minute and 2 seconds.
Interface speed	Shows the data rate, here 1024 kbps.
Link uptime	Shows for how long the link has been established
4 transition(s) to up	Shows that since the system powered up, this DSL line has been negotiated 4 times successfully (and has correspondingly been interrupted three times).
Signal quality	Shows the value of the signal quality, refer to Chapter 2.15.6, "Signal Quality, Line Length and Data Rate".
Lineloss ratio	Shows the attenuation of the copper line in dB. A value of 0 dB allows the conclusion that there is only short distance between the two stations of the point-to-point connection.

Table 21: Comments on the example of the display of DSL interfaces

#### Commands to show information and frame statistics of DSL interfaces

```
<show interface {backup-group1 | channel0 | console0 |
console1 | dsl1 | dsl2 | fastethernet0 | tunnel0}>
<show interface {channel0 | dsl1 | dsl2 | fastethernet0 |
tunnel0} frame-counters>
<clear interface channel0 counters>
```

### 2.15.7.2 Interferences and Cable Faults

The signal quality allows conclusions about interferences and cable faults. Even though the values have a measuring error of 1-2 dB, if both sides of a DSL line show vastly different values for signal quality then this may point to one-sided disturbances from other signals or discontinuities in impedance of the line (e.g. due to cable faults).

The following figures which effects (one-sided) interferences and cable faults may have:

- 1 In this example, transmission without interference leads to a signal quality of 11 dB on both sides.

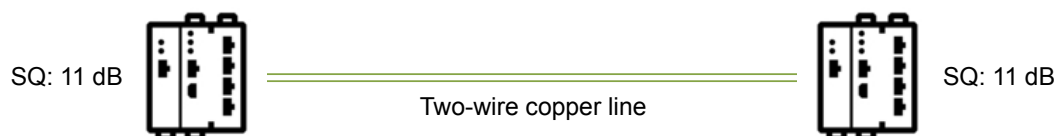


Figure 10: Transmission line without references

- 2 If another service is transmitted in the same cable but on different wires then this may potentially cause interference and reduced signal quality on both sides.

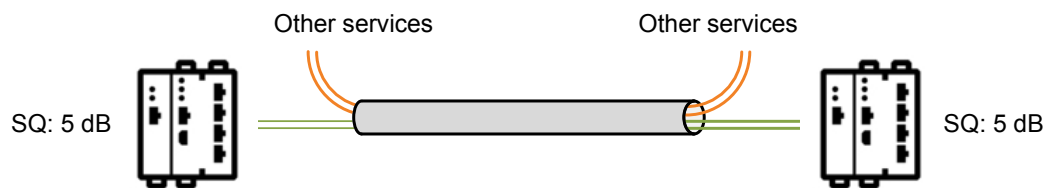


Figure 11: Interference due to different service

- 3 If the service is only transmitted on a section of the cable then the interference is only at this line segment.

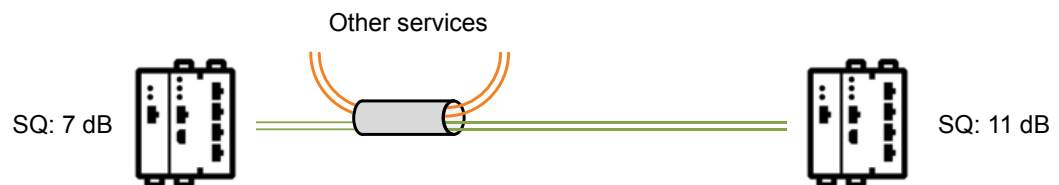


Figure 12: One-sided interference due to different service

The not yet strongly dampened transmit signal of the left side shows a lower share in interference than the already strongly dampened transmit signal of the right side. That is why the signal quality on the left receive side is worse than on the right side.

In this case the signal quality on the errored side is worse.

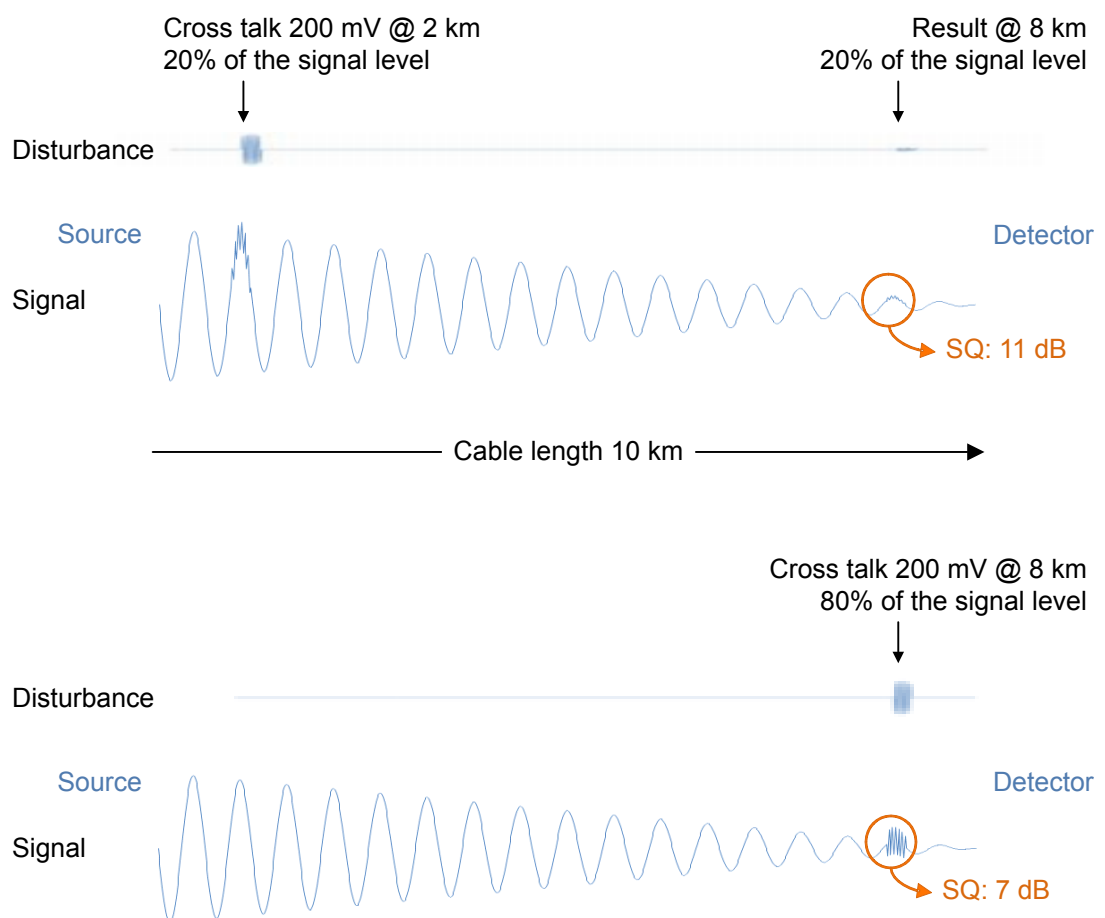


Figure 13: Background on one-sided interferences

The exact reversal of the error condition exists if one-sided cable faults are present like breaches, hair cracks, shield defects with water intrusion or isolation faults.

- 1 In this example ordinary operation shows a signal quality of 11 dB on both sides. Interferences spread evenly in the course of the line so that both sides have a symmetrical value for signal quality.

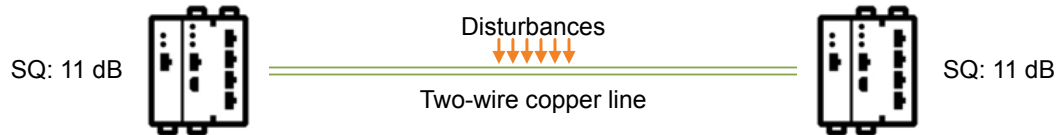


Figure 14: Regular cable with interferences

- 2 If there is a cable fault in the middle of the cable then the signal is attenuated on both sides together with the already existing interferences so that symmetrical values are measured for signal quality.

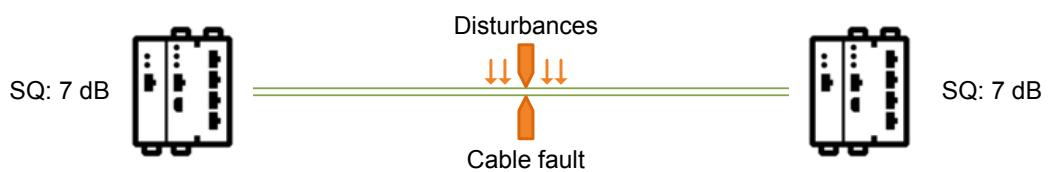


Figure 15: Attenuation due to cable fault

- 3 If there is a one-sided cable fault on the transmission line then this causes high attenuation. As a consequence the signal quality sinks on the right side (with untampered cable) while there are only minor reductions in quality on the errored left side.



Figure 16: Asymmetric values for signal quality due to one-sided cable fault

The already dampened transmit signal on the right side is attenuated further with the already existing interferences while payload signal and interference are attenuated by the same amount and the signal-to-noise ratio stays almost the same. The strong transmit signal on the left side is dampened strongly by the cable fault and collects more interferences in the course. On the right side a significantly worse signal-to-noise ration can be recorded.

## 2.16 DSL Channel Bundling

To improve the reliability against failure, the transmission bandwidth of two DSL interfaces on a device can be bundled and connected via a 4-wire connection to the counterpart. If one of the two connections fail, the transmission is switched automatically to the remaining one. If the DSL connection is restored, both channels are used automatically for data transmission.

For this purpose the interfaces dsl1 and dsl2 are bundled to the virtual interface channel0. This represents the DSL channel bundling among other also for the Spanning Tree Protocol (if activated Chapter 2.19, "Spanning Tree Protocol").

The transmission rate is the result of the individual DSL transmission rates, the employed distribution algorithm and the load on the two DSL channels. There are two distribution algorithms to choose from.



The default value activates a weighted algorithm that tries to optimize the load on both DSL channels adapted to the respective transmission rate of both DSL lines.

Alternatively, a MAC based distribution algorithm can be set that selects a DSL channel in relation of source and target MAC address.

The default value for DSL channel bundling is: shutdown.

The command `<set interface channel0 no shutdown>` activates the DSL channel bundling.

The command `<set interface channel0 shutdown>` deactivates the DSL channel bundling.

The current link state of the DSL channel bundling can be displayed in an overview. Detailed information about the data traffic that runs over an channel0 interface is also available and can be requested alternatively via RMON (SNMP).

Commands related to DSL channel building

```
<set interface channel0 [no] shutdown>
<set interface channel0 distribution-algorithm {mac-based |
weighted-left-right}>
<set interface channel0 alias {string20}>
<show interface channel0>
<show interface channel0 frame-counters>
```

#### ADVICE

As the DSL channel bundling is implemented in software, the reachable data rate is limited. DSL line with individual data rates over 2.048 kbps can be configured as channel bundling. But this does not contribute to increase the channel0 data rate. Only reliability against failure is there.

#### ADVICE

If a DSL interface that is part of a channel bundling gets connected to a counterpart that is not part of the channel bundling, the alarm Link aggregation mismatch will occur. In this state the function of Spanning Tree is not guaranteed and the network is in a potentially incoherent state. Especially when activating the DSL channel bundling you have to watch out for this.

## 2.17 Redundancy with a Backup-Group

The protocol Spanning Tree over used (refer to Chapter 2.19, "Spanning Tree Protocol") to grant the automatic switch over to an alternative route in networks with redundant connections. Depending on the existing topology and settings the switch over may take some seconds and block the network for this period in a worst case.

The backup group function of the EDS500 devices offers a sped-up switch over for two redundantly connected sites. Prerequisite is that they are connected via directly point-to-point connections. The switch-over is not protocol-based but is directly based on the link state.

The underlying principle is that of a link aggregation without the simultaneous use of the joint bandwidth of the single connections. Spanning Tree works transparently over this interface called backup-group1. The interface backup-group transmits over the fastest available connection at any time.

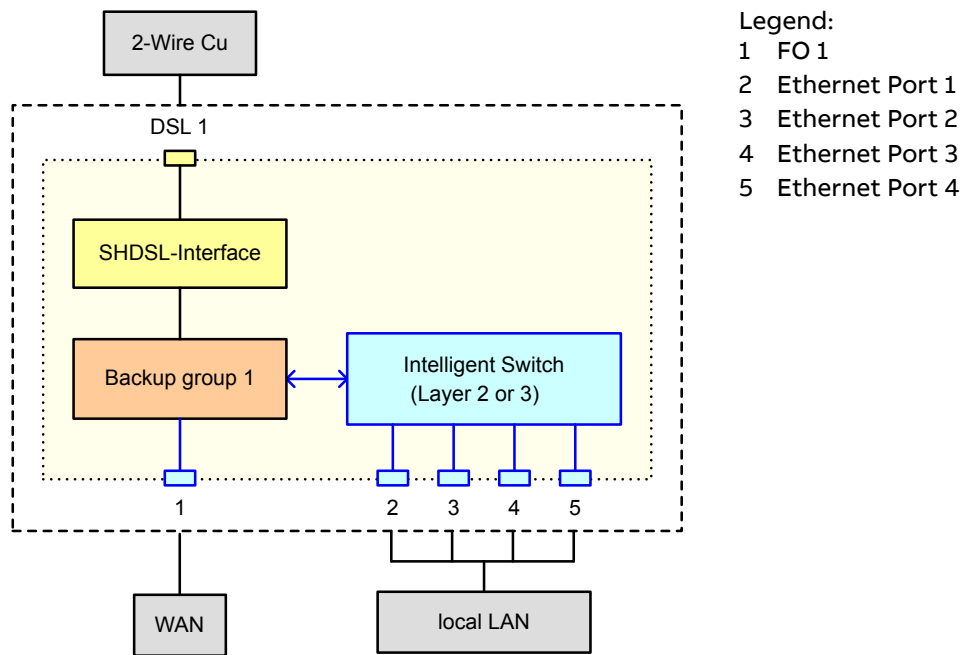


Figure 17: Example application backup-group 1:  
Grouping dsl1 and fo1

Commands to configure the backup-group

```
<set interface {backup-group...} [no] {...}>
<show interface {...}>
```

#### ADVICE

If equivalent interfaces belong to a Backup-group (e.g. fo1 and fo2) then on both sides the interfaces with the same name have to be connected (e.g. side A fo1 with side B fo1 and side A fo2 with side B fo2).

#### ADVICE

As the switch-over is triggered by the link state, Link Fault Pass-Through (LFPT) has to be activated if a media converter is used at the Ethernet ports 1-4.

## 2.18 Layer-2-Tunnel

The layer-2-tunnel protocol (L2TP) can be used to connect physically not directly connected network nodes on the layer 2 of the OSI layer model.

The data traffic is packed into L2TP packets at the terminations of the L2TP tunnel which are then transported over any arbitrary layer 3 connection (IP).

This function allows the creation of alternative routes. Also, distant isolated networks can be connected to a layer 2 broadcast domain with the L2TP function.

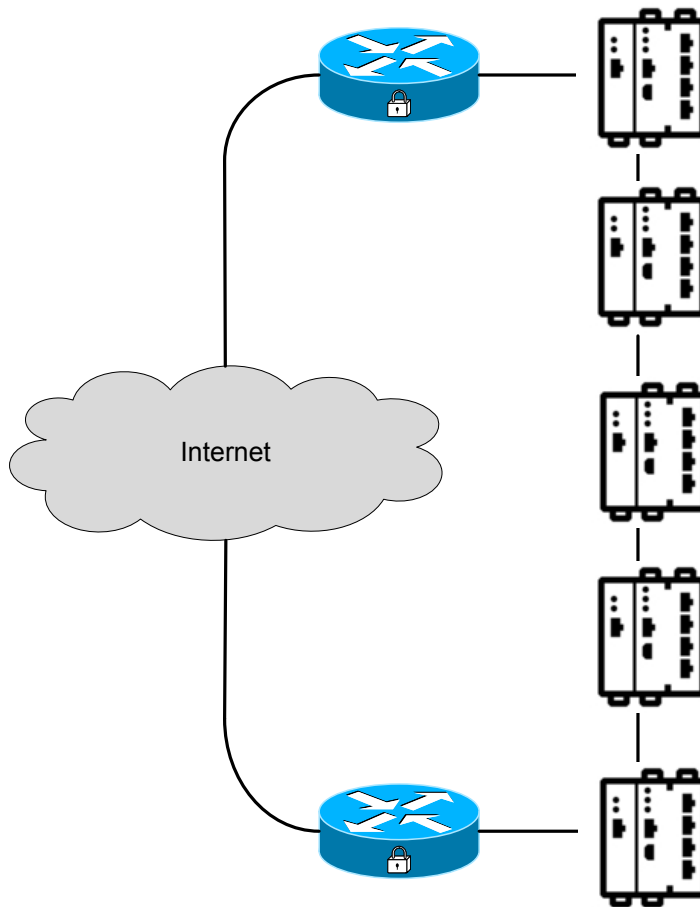


Figure 18: DSL line to layer 2 ring with L2TP

One device of a L2TP tunnel is configured as L2TP server, the other is configured as L2TP client and establishes a link to the server. Both devices need the local and the remote IP address. The local address is called source IP address, the remote address is the destination IP address. To avoid that the already encapsulated L2TP data traffic is encapsulated again, the tunnel interface should be configured as an access VLAN (untagged) or as one or more trunk VLANs (tagged) where all of them are not associated with the local or remote IP address. Then the tunnel interface has to be activated.

Default configuration:

In default configuration L2TP is disabled.

Commands related to the layer 2 tunnel function

```
<set interface {tunnel...} role {...}>
<set interface {tunnel...} source-ip {...}>
<set interface tunnel0 trunk-vlan {{1-4094} | all}>
<set interface tunnel0 destination-ip {IP address}>
<set interface tunnel0 [no] shutdown>
<show interface>
<show interface {...}>
<show interface {...} frame-counters>
```

## 2.19 Spanning Tree Protocol

EDS500 devices supports the Spanning Tree protocol (IEEE 802.1D and IEEE 802.1Q) in the versions STP, RSTP and MSTP to avoid loops in switched networks. The Spanning Tree

protocol secures in a transparent way that only one path is active for packet forwarding between two nodes of a layer-2 network segment. Redundant connections are identified and blocked if necessary.

### 2.19.1 Activate, Deactivate, Spanning Tree Protocol Version

The default value for Spanning Tree protocol on all devices is: <set stp enable>

The default value automatically grants a loop-free operation and avoids network failure. There are commands to deactivate STP on the whole device or on single ports.

Commands to activate and deactivate spanning tree

```
<set stp no enable>
<set stp enable>
<set stp no enable {backup-group1 | channel0 | dsl1 | dsl2 |
fastethernet0 | fo1 | fo2 | port1 | port2 | port3 | port4 |
tunnel0}>
<set stp no enable {backup-group1 | channel0 | dsl1 | dsl2 |
fastethernet0 | fo1 | fo2 | port1 | port2 | port3 | port4 |
tunnel0}>
```

#### ADVICE

With deactivated spanning tree protocol, loops in the network topology will lead to packet storms, undefined behaviour and consequently network failure.

#### ADVICE

A deactivated spanning tree protocol can not be reset with a global command.

Example 1: <set stp no enable port1> causes that for Port 1 STP stays deactivated even after command <set stp enable>.

Example 2: <set stp no enable> causes that for Port 1 STP stays deactivated even after command <set stp enable port1>.

The spanning tree protocol is backward compatible by design which means that a device that runs RSTP communicates with devices running STP. In analogy, a device running MSTP communicates with RSTP devices via RSTP and STP devices with STP.

The default value for STP version is: rstp.

Commands to set the spanning tree version

```
<set stp version rstp>
<set stp version stp>
<set stp version mstp>
```

Version	Specification
STP	IEEE 802.1D-1998
RSTP	IEEE 802.1D-2004
MSTP	IEEE 802.1Q-2011

Table 22: Spanning Tree Versions

### 2.19.2 Commands to Display the Spanning Tree Bridge Information

Information about the current device is summarized in the bridge information. If MSTP is used operation every MST instance (MSTI, 1-4094) has additionally its own bridge information.

Commands to display the spanning tree bridge information

```
<show stp bridge>  
<show stp msti {1-4094} bridge>
```

### 2.19.3 Display the Spanning Tree Root Information

In RSTP and STP networks the root node of the spanning tree is named Root Bridge. In MSTP networks there are several Root Bridges: for outside the region a CST Root Bridge (common spanning tree), for inside a region an IST Root Bridge (internal spanning tree, can be identical to the CST Root Bridge and is then called CIST) and additionally for each MST instance (MSTI, 1-4094) an individual Root Bridge.

Commands to display spanning tree root information

```
<show stp root>  
<show stp msti {1-4094} root>
```

### 2.19.4 Display the Spanning Tree Port Roles and States

The result of a Spanning Tree calculation are port roles and states that are summarized in a list. When using version MSTP, each additional MST instance (MSTI, 1-4094) has individual port roles and states that can deviate from those for CIST (Common and Internal Spanning Tree).

Commands to display the spanning tree port roles and states

```
<show stp port-roles>  
<show stp msti {1-4094} port-roles>
```

### 2.19.5 Display detailed Spanning Tree Information

The information about the current device, the Root Bridge and the port roles and states can be displayed together and again additionally for each MST instance (MSTI, 1-4094).

Command to display the spanning tree MST settings:

```
<show stp [details]>  
<show stp msti {1-4094} detail>
```

### 2.19.6 Display of Specific Settings for Multiple Spanning Tree (MST)

There are further parameters for operation in the version MSTP:

- MST configuration name
- MST configuration revision
- VLAN-to-MSTI-assignment
- MST configuration hash value

Devices belong to the same MST region if the following parameters are identical:

- MST configuration name
- MST configuration revision
- MST configuration hash value

The devices have to be connected to each other and have to execute MSTP.

These parameters can be displayed with a command.

Command to display the spanning tree MST settings:

```
<show stp mst>
```

## 2.19.7 Configuration of Spanning Tree Bridge Parameters

The Root Bridge is selected by its hardware address (MAC address), and a priority that can be set on each bridge. This Bridge priority can be adjusted in steps of 4096 between 0 and 61440.

The default value for priority bridge is 32768.

In general the following is valid for Spanning Tree parameters: smaller is better. A bridge priority can also be set for each MST instance (MSTI, 1-4094) that determines which Bridge becomes the MSTI Root Bridge.

Commands to configure the spanning tree bridge priority

```
<set stp priority bridge {0-61440}>
<set stp msti {1-4094} priority bridge {0-61440}>
```

Commands to configure the spanning tree timer values

```
<set stp forwarddelay {4-30}>
<set stp holdcount {1-10}>
<set stp maxage {6-40}>
<set stp maxhops {6-40}>
```

To grant the interoperability to older (IEEE 802.1D) versions it should be considered when setting forward delay and maxage that the following applies:

$2 \cdot (\text{forwarddelay} - 1) \geq \text{maxage}$ .

Timer value	Range	Default value
forwarddelay	4-30	15
holdcount	1-10	6
maxage	6-40	20
maxhops	6-40	20

Table 23: Value ranges for the Spanning Tree timers

## 2.19.8 Configuration of the Priority for Spanning Tree Port

Further settings determine the behaviour of the individual ports. Again if MSTP is used, these settings can also be applied for each individual MST instance (MSTI, 1-4094).

The port priority can be set in steps of 16 between 0 and 240.

The default value for the port priority is 128.

Set the port priority to a low value to prefer a certain transmission line. Lower port priorities get preferred.

Commands to configure the spanning tree port priorities

```
<set stp priority {backup-group1 | channel0 | ds11 | ds12 |
fastethernet0 | fo1 | fo2 | port1 | port2 | port3 | port4 |
tunnel0} {0-240}>
```

```
<set stp msti {1-4094} priority {backup-group1 | channel0
| dsl1 | dsl2 | fastethernet0 | fo1 | fo2 | port1 | port2 |
port3 | port4 | tunnel0} {0-240}>
```

### 2.19.9 Spanning Tree Port Cost

The port cost determine the selection of the preferred root path and should ideally represent the actual transmission conditions.

The default value for all ports is auto.

This means that the device sets the negotiated or set data rate automatically per port. In a few cases (example: transmission via port tunnel0 with a L2TP tunnel through a VPN network) the effective data rate cannot be determined automatically and a manual settings should be used.

Commands to configure the spanning tree port costs

```
<set stp cost {backup-group1 | channel0 | dsl1 | dsl2 |
fastethernet0 | fo1 | fo2 | port1 | port2 | port3 | port4 |
tunnel0} auto>
<set stp cost {backup-group1 | channel0 | dsl1 | dsl2 |
fastethernet0 | fo1 | fo2 | port1 | port2 | port3 | port4 |
tunnel0} {1-200000000}>
<set stp msti {...} cost {...} {...}>
```

### 2.19.10 Spanning Tree Point-to-Point Port Property

The spanning tree protocol distinguishes between ports that operate in point-to-point mode and those that operate in point-to-multipoint mode (any-to-any, shared). In point-to-point-mode STP BPDUs can only be received from exactly one other bridge. For ports in shared mode longer transition periods have to be endured as first of all several potential bridges have to reach a consent. This may lead to unnecessary long convergence periods when the topology is changed. Hence, it is desirable to set only those ports into point-to-point mode that are connected to only one other bridge.

The default value varies from interface to interface.

The following applies to the interfaces dsl1, dsl2, backup-group1, channel0 and tunnel0:

The default value for mode is point-to-point.

The following applies for Ethernet links (optical and copper ports):

The default value for mode is no point-to-point.

Commands to configure the spanning tree point-to-point port property

```
<set stp point-to-point {backup-group1 | channel0 | dsl1 |
dsl2 | fastethernet0 | fo1 | fo2 | port1 | port2 | port3 |
port4 | tunnel0}>
<set stp no point-to-point {backup-group1 | channel0 | dsl1
| dsl2 | fastethernet0 | fo1 | fo2 | port1 | port2 | port3 |
port4 | tunnel0}>
```

### 2.19.11 Configuration of the Spanning Tree Port Edge Setting

A further setting for a fast port switch when the topology is modified is setting the edge property for such ports that are only connected to terminal devices. The auto-edge property takes care that an edge port is automatically detected.

The default value for all ports is: auto-edge.

Commands to configure the spanning tree port edge settings

```
<set stp auto-edge backup-group1>
<set stp no auto-edge backup-group1>
<set stp edge {backup-group1 | channel0 | ds11 | ds12 |
fastethernet0 | fo1 | fo2 | port1 | port2 | port3 | port4 |
tunnel0}>
<set stp no edge {backup-group1 | channel0 | ds11 | ds12 |
fastethernet0 | fo1 | fo2 | port1 | port2 | port3 | port4 |
tunnel0}>
```

### 2.19.12 Activation of the Spanning Tree Migration Check

The mixed operation of STP and RSTP/MSTP can be checked as follows for a port and shows if STP is used.

Commands to activate the spanning tree migration check

```
<set stp migration-check all-interfaces>
<set stp migration-check {backup-group1 | channel0 | ds11 |
ds12 | fastethernet0 | fo1 | fo2 | port1 | port2 | port3 |
port4 | tunnel0}>
```

### 2.19.13 Configuration of Multiple Spanning Tree Parameters

There are further parameters for operation in the version MSTP:

- MST configuration name
- MST configuration revision
- VLAN-to-MSTI-assignment
- MST configuration hash value

Devices belong to the same MST region if the following parameters are identical:

- MST configuration name
- MST configuration revision
- MST configuration hash value

The devices have to be connected to each other and have to execute MSTP.

These parameters can be set with a command.

The MST configuration name is plain text with a maximum length of 32 characters. In order to have an initially unique string the default value is set to the device MAC address. The MST configuration revision can freely be chosen between 0 and 65535.

The default value for MST configuration revision is 0.

Commands to configure the spanning tree MST settings

```
<set stp mst-config-name {string32}>
<set stp mst-config-revision {0-65535}>
```



### 2.19.14 Assigning VLANs to Multiple Spanning Tree Instances

VLANs have to be explicitly assigned to MSTIs with a command. The range of valid MSTIDs is 1-4094. Per device up to 4 MSTIs can be defined (with arbitrary MSTID). Initially, all VLANs are assigned to the CIST (Common and Internal Spanning Tree).

Commands for assigning VLANs to Multiple Spanning Tree instances

```
<set stp msti {1-4094} vlan {1-4094}>
<set stp msti {1-4094} no vlan {1-4094}>
```

### 2.19.15 Advice on the Operation of Spanning Tree with EDS500 Devices

The default value for Spanning Tree is enable.

As a rule of thumb there is no further configuration required. Some general points should be considered for the planning and creation of the configuration.

It is advisable to position the Root Bridge at a defined place in the network. Usually, this is close to the uplink of a network. Depending on the topology it is reasonable to define a fall-back Root Bridge. A device is selected as root bridge by setting a better (i.e. lower) priority (example: <set stp priority bridge 24576>).

Ports, that are no edge ports and are directly connected to another STP capable device the property should be set to point-to-point mode. This is particularly advisable for optical fibre rings. (example: <set stp point-to-point fo1>).

The default value for Ethernet ports (optical fibres as well as copper) is: no point-to-point.

If, for redundant paths, particular ports should get priority then the port priority should be set accordingly. The port cost should not be adapted or if only to a small extent as these values get summed up and are distributed via STP BPDUs and should therefore represent the real conditions as much as possible. Ideally, you leave the calculation of costs to the device. Exception: the device cannot detect the speed automatically for the virtual port tunnel0, so you should set the port costs to an estimated value.

Interface speed	Default value	Recommended range
≤ 100 kbps	200 000 000	20 000 000 – 200 000 000
1 Mbps	20 000 000	2 000 000 – 200 000 000
10 Mbps	2 000 000	200,000 – 20,000,000
100 Mbps	200 000	20,000 – 2,000,000
1 Gbps	20 000	2,000 – 200,000

Table 24: Spanning Tree port cost

## 2.20 Serial Interfaces

The serial interfaces of EDS500 devices are laid out as RJ-12 plugs (6P6C) (see EDS500 Manual - Part 1: Serial Interfaces (Con0 - Con1)).

The default value for the behaviour of the interfaces is according to ITU-T V.24 / EIA RS-232.

Depending on the device switch-over to EIA RS-422/485 is possible.

The default values for the serial interfaces are:

- Baud rate 57600 Baud

- 8N1( 8 data bits, no parity, 1 stop bit)
- no flow control

### 2.20.1 Usage for Configuration or as Process Interface

The default value for the serial interfaces is: configuration.

The setting configuration allows to access the management console with its command line interface (CLI). An alternative use as process interface can be set with a command. The following modes are available.

Mode Parameter	Description
Configuration configuration	The interface allows offers access to the command line interface (CLI) to configure the device. This is the default value.
Modem modem	The interface emulates an AT dial-up modem that can establish a link to another emulated modem by using the IP address as dialled number.
Tunnel tunnel	The interface transports serial data streams to one or more remote devices. There, the data is output at the remote serial interface.
IEC101 iec101	The interface is set to telecontrol mode and can be attached to a IEC 60870-5-101 interface.
Linetest linetest	The interface generates a test pattern that is sent continuously. With the command line interface (CLI) it can be monitored whether the interface receives the test pattern correctly or whether the link is interrupted.
Loopback loopback	The interface returns all received data immediately.

Table 25: Operating modes

Commands to configure the operation mode of the serial interface

```
<set interface {console0 | console1} mode {configuration |
  iec101 | linetest | loopback | modem | tunnel}>
```

### 2.20.2 Transmission Parameters of the Interface

The parameters of the serial interface can be set by command for baud rate (300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 or 230400), data bits (5, 6, 7 or 8), parity (none, even, odd, mark or space) and stop bits (1 or 2). Also the behaviour of the control signals CTS and DCD can be set. The DCD signal can be inverted on hardware level.

DCD lead times and follow-up times can be set for switching the carrier on or off if an external modem is used. For this purpose DCD has to be set to while-tx. The DCD lead time has an additional purpose for the operation mode "tunnel", refer to "Serial Tunnel" .

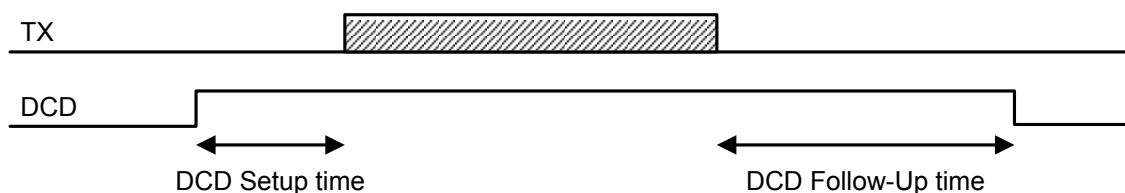


Figure 19: DCD lead time and follow-up time

The current state of a serial interface can be displayed in an overview. Detailed information about the data traffic that runs over a serial interface is available and can be requested also via RMON (SNMP).

Commands to configure the transmission parameters of the serial interface

```
<set interface {console...} baudrate {...}>
<set interface {console...} databits {...}>
<set interface {console...} parity {...}>
<set interface {console...} stopbits {...}>
<set interface {console...} cts {...}>
<set interface {console...} dcd {...}>
<set interface {console...} dcd-follow-up {...}>
<set interface {console...} dcd-setup {...}>
<set interface {console...} dcd-inversion {...}>
<set interface {channel...} alias {...}>
<show interface console0>
<show interface console1>
```

### 2.20.3 Inactivity Detection for the Command Line Interface (CLI)

The command line interface (CLI) is available in the operation mode configuration via the serial interface. In order to avoid that a login or operation mode configuration at the serial command line interface (CLI) allows potentially unauthorized access due to a forgotten logout command or disable command, it is possible to define a timeout for an automatic logout; or disable for the view mode.

The default value for the automatic termination in operation mode configuration after inactivity is 600 seconds.

The default value for the automatic termination of the view mode is 1200 seconds.

The view mode can only be terminated automatically if a login password has been set.

Setting the idle-logout-time to zero disables the automatic logout.

Commands to configure the automatic inactivity detection at the serial interface

```
<set interface {console...} idle-disable {...}>
<set interface {console...} idle-logout {...}>
```

### 2.20.4 Operation as RS-485 Interface

The transmission mode for the serial interface can be switched for console0 at devices with RS-485 support. 2-wire-operation (half duplex) and 4-wire-operation (full duplex) can be distinguished, EDS500 Manual - Part 1: Serial Interfaces (Con0 - Con1).

Also in 4-wire-operation the output lines are only used during transmission and therefore allow several transmitters on the bus (RS-485 vs. RS-422).

The line termination can be deactivated for devices that are not connected at the end of a bus line.

The default value for termination is: termination on.

Commands to configure RS-485 parameters

```
<set interface console0 physical-mode rs-232>
<set interface console0 physical-mode rs-485-half>
```

```
<set interface console0 physical-mode rs-485-full>  
<termination on>  
<set interface console0 termination off>
```

**ADVICE**

An EDS500 device with RS-485 support can usually be operated in a RS-422 network without problems.

## 2.21 Serial Tunnel

### 2.21.1 Applications

EDS500 devices can transport serial data streams via the Ethernet/IP network (asynchronous EIA-232 and EIA-485 protocols and applications). This means that modern internet technology can be used simultaneously with established legacy technology. Possible applications include RTU communication (Remote Terminal Units), AMR (Automated Meter Reading), SPS applications a.m.m.

The communication technology can be updated in a migration scenario without the need to replace the hardware or configuration of the remote terminal units if a serial tunnel is used. Furthermore, the replacement does not have to happen in one step but can be carried out step by step (e.g. to replace FSK based modem lines).

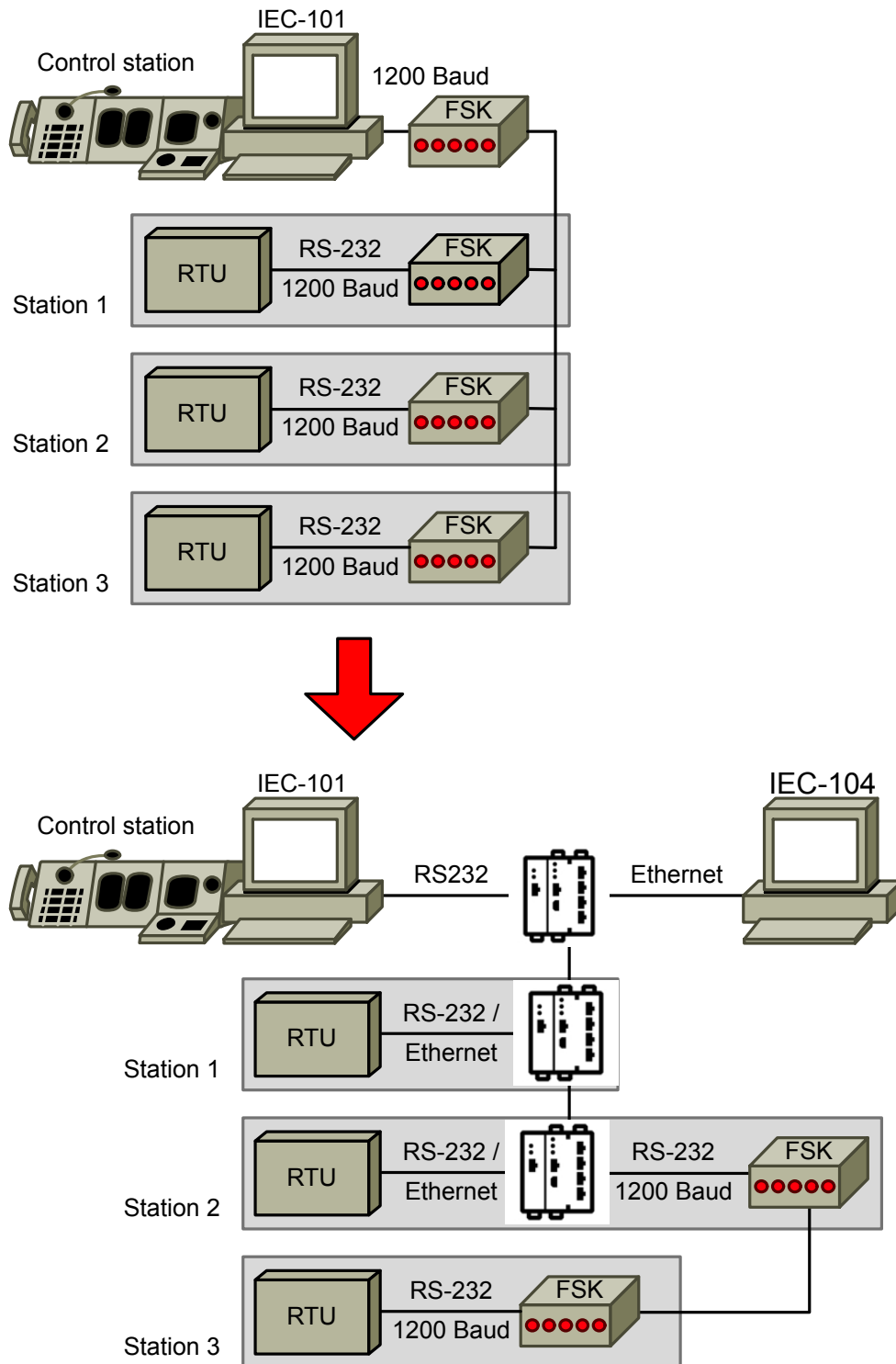


Figure 20: Step by step replacement of serial transmission devices and (temporary) preservation of the previous remote control configuration

In addition to the use for remote control protocols there are many more application options feasible for a serial tunnel e.g. the access to a remote serial management interface or the transport of more or less any (slow) digital signals ( Chapter 2.21.2, "Serial Protocols and Sampling Operation").

Commands to activate the serial tunnel

```
<set interface {console0 | console1} mode tunnel>
```

### 2.21.2 Serial Protocols and Sampling Operation

In general arbitrary serial UART format based protocols can be transported. The supported remote control protocols are (among others) IEC 60870-5-101, Modbus, RCOM, RP570/RP571 and Hibus-2. Data rates up to 115200 Baud are supported, however the tunnel ends may be configured with different baud rates. Also supported is the transmission of the break signal that keeps the transmission on zero level for longer than an UART frame.

EDS500 devices support alternatively a special sampling operation ("transparent"), that allows to transmit non-UART-compliant serial protocols and slow digital signals. For this the transmit and receiving line must not be connected with TX or RX signal of the serial interface Console0 or Console1 but with the CTS and RTS signal. For pin assignment refer to EDS500 Manual - Part 1: Serial Interfaces (Con0 - Con1).

Transmission of slow signals ( $\leq 200$  Baud) in sampling operation:

- Quantity impulses for gas / water / electricity
- Non EIA-232 compliant protocols
- Alarm relais state, door contact, ...

Commands for configuration of the sampling operation:

```
<set interface {console0 | console1} transparent {none |
rts-cts}>
<set interface {console0 | console1} transparent {fast |
slow}>
```

### 2.21.3 Topologies and Transmission settings

Data streams can be distributed in the Ethernet/IP network in various ways with a serial tunnel. Depending on the extent and type of the network (Layer-2/switched vs. Layer-3/routed) various logical topologies can be realized.

Topology	Description
Point-to-Point	A serial line is tunnelled through the network.
Point-to-Multipoint	One participant can communicate with all other participants that in return cannot communicate with each other. Typical use case for an existing partyline installation.
Any-to-Any	All participants can communicate with all other participants. The simultaneous communication overlays itself.
Mixed form	Arbitrary transmission directions can be defined (even asymmetrical). Like this a tapping mirroring can be realized.

Table 26: Topologies of the serial tunnel

Without further configuration the serial tunnel is set to a mode in which all reachable communication partners are addressed in the same broadcast domain. This transmission is not target-oriented and cannot be used in routed (Layer-3) networks. Multicast Ethernet frame transport the data.

To avoid that any recipient can receive the transmitted data, so-called IP targets can be specified. A serial tunnel can have up to 18 specific IP targets to which the incoming serial data stream is forwarded. The data traffic then happens in targeted (unicast) IP packets.

This operation mode (while using IP targets) is mandatory in routed networks. It can be used in switched networks to reduce the amount of data e.g. when the central office runs in multicast mode while the stations have been set the IP address of the central device as IP target (which means the stations cannot communicate with each other).

Tunnel groups can be defined to separate logically different data streams in the same network. Only endpoints with the same tunnel group transmit serial data streams among each other. Up to ten different tunnel groups can be set.

There is forward error correction. This can be deactivated by setting transmission mode to fast. If the forward error correction is activated then the loss of single packets in the Ethernet/IP network does not lead to interruption of the serial data stream, yet, twice the bandwidth is required.

The default value for transmission mode is fail-safe (forward error correction enabled).

A source VLAN can be defined to bind the data transmission of the serial tunnel to a certain VLAN (and therefore the IP address of the VLAN interface). This leads to a clean separation of the data traffic.

Commands for the configuration of topology and transmission of the serial tunnel

```
<set interface {console0 | console1} ip-target {IP
address}>
<clear interface {console0 | console1} ip-target {IP
address}>
<set interface {console0 | console1} tunnel-group {1-10}>
<set interface {console0 | console1} transmission {fail-safe
| fast | local-only}>
<set interface console source vlan {1-4094}>
```

## 2.21.4 Enhanced Parameters of the Serial Tunnel

The default values work for many applications without the need of an enhanced configuration via the serial interface settings (refer to Chapter 2.20.2, "Transmission Parameters of the Interface") and the basic settings of the serial tunnel (Tunnel mode, IP targets, Tunnel Group).

There are further settings for protocols that react delicately to changes in timing to minimize the effects of the transport through the Ethernet/IP network. In general the requirements are very different so that for each individual case the suitable setting has to be found.

The sampling frequency determines how often the registered serial data is sent via the Ethernet/IP network. This setting has influence on the required bandwidth for tunnelling and the delay of the serial data stream. The lower the "sampling frequency" the more bandwidth is required but the lower the delay of the data.

The default value for sampling is: 20 ms.

Depending on the applied baud rate the frequency can be set to values between 120 ms (for low baud rates) down to 1 ms (values below 10 ms should be used only in exceptional cases as the resulting network load rises out of proportion).

Caused by the sampling frequency and timing effects it can happen that serial telegrams that reach the tunnel entrance in one piece, disintegrate in respect to time into several pieces (separate bytes) at the tunnel exit. This can be critical depending on the application.

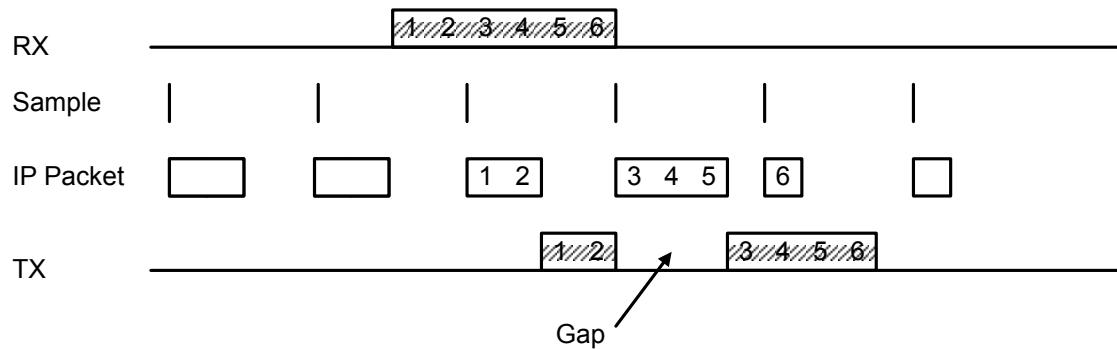


Figure 21: Interruption in the serial data stream

The data transmission as a whole has to be delayed to avoid interruptions at the tunnel exit.

Like this it is ensured that the following data is already available and can be issued without gap. A DCD lead time is set at the serial interface for this purpose (refer to Chapter 2.20.2, "Transmission Parameters of the Interface").

It does not matter if the DCD signal of the serial interface is actually used. The DCD lead time takes care that the data transmission is delayed at the tunnel exit and therefore stays coherent.

1.5 times the sampling frequency can be assumed as a guide line for DCD lead time. Possible jitter in the transmission time of Ethernet/IP packets can be buffered in this way.

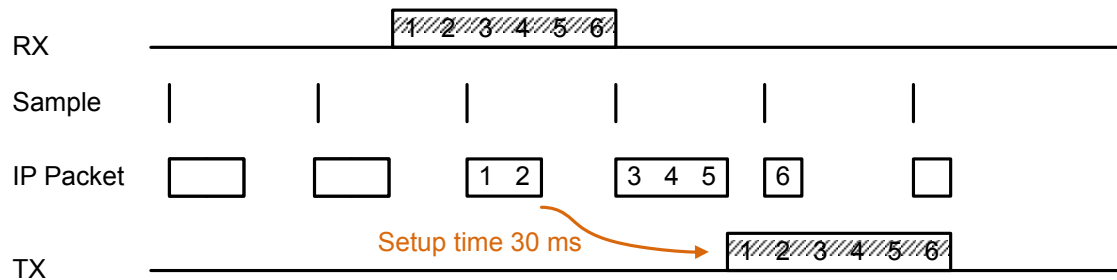


Figure 22: Avoid interruptions with lead time

Caused by jitter in the packet runtimes through the Ethernet/IP network as well as different baud rates at the tunnel entrance and exit, can cause that a serial telegram arrives at the tunnel exit while the previous telegram is still being sent or the DCD signal is still active e.g. due to a set DCD delay.

This causes that the DCD lead time is not applied as the DCD signal is already active and the data is sent directly (as soon as possible).

Pauses that existed between the telegrams at the tunnel entrance can be eliminated by this at the tunnel exit. This can disturb the serial communication.

To ensure pauses at the tunnel exit, a pause detection can be set for the tunnel entrance.

The pause detection forces the DCD signal to be switched off. Like this, the set DCD lead time is kept between two serial telegrams. Pause for the detection and DCD lead time should be set to the same values.

Commands for the configuration of enhanced tunnel parameters

```
<set interface {console0 | console1} sampling {1-120}>
<set interface {console0 | console1} dcd-setup {0-255}>
<set interface {console0 | console1} pause-detection
{0-255}>
```



### 2.21.5 Query the Status of the Serial Tunnel

Command to show the serial tunnel

```
<show interface {backup-group1 | channel0 | console0 |
console1 | dsl1 | dsl2 | fastethernet0 | tunnel0}>
```

## 2.22 IEC 60870-5-101 and IEC 60870-5-104

For monitoring purposes the EDS500 devices can serve a telecontrol central office according to IEC 60870-5-104 as well as IEC 60870-5-101. The functionality is similar to SNMP Network monitoring.

The device can be assigned an ASDU address and be included as station into the telecontrol monitoring according to IEC 60870-5-104 or 60870-5-101. It is possible to monitor the device and interface state and supervise the communication network from the control center.

Default configuration:

In default configuration IEC 60870-5-104 and IEC 60870-5-101 is disabled.

Also, some signals on the serial interface can be set and read so that only with little additional external installation a telecontrol device can be realised. The IEC 60870-5-104 and 60870-5-101 station addresses and the addresses of the information objects can be chosen freely. managed switches can be assigned an ASDU address and be included as station into the telecontrol monitoring according to IEC 60870-5-104 or 60870-5-101. It is possible to monitor the device and interface state and supervise the communication network from the central office. Also, some signals on the serial interface can be set and read so that only with little additional external installation a telecontrol device can be realised. The IEC 60870-5-104 and 60870-5-101 station addresses and the addresses of the information objects can be chosen freely.

The default value for the ASDU address is 0.

In addition the devices of the EDS500 series can be used for the conversion between IEC 60870-5-101 and IEC 60870-5-104.

If a telecontrol network shall be migrated to Ethernet then it is typically desired to switch also the telecontrol protocol from IEC 60870-5-101 to IEC 60870-5-104.

The EDS500 devices feature a converter function for this purpose. The serial interfaces of the modem are connected to one or more telecontrol units. Several telecontrol units can be connected via an existing voice-frequency telegraphy circuit line. Prerequisite is the use of the protocol IEC 60870-5-101 on the telecontrol unit. Each connected telecontrol unit gets an additional IP address in the switch with which one or more IEC 60870-5-104 central offices can connect themselves. The telegram types get translated, as well as the address formats and time stamp. In order to convert, the assignment of an ASDU address (station address) to a link address (IEC 60870-5-101) as well as to a local IP address for the central office (IEC 60870-5-104) has to be configured. No information objects need to be created by configuration, instead they are forwarded transparently.

### 2.22.1 Addresses of the EDS500 Device Information Objects

The IEC 60870-5-101 and IEC 60870-5-104 station addresses (common address of the ASDU) and the addresses of the information objects can be chosen freely.

The default value for the ASDU address is 0.

For default values for the addresses of the information objects refer to "Tab. 27: Information objects".

Object / Function	State / Value range	Pre-set object address	ASDU data type
System – Warning	OFF: normal state	1	1
	ON: Warning imminent		(Single message)
System – Alarm	OFF: normal state	2	1
	ON: Alarm imminent		(Single message)
Console0 – RTS (Input)	OFF: open	3	1 / 15
	OFF: -25 ... 0 V		(Single message / counter)
	ON: 3 ... 25 V		
Console0 – CTS (output)	OFF: -2.5 ... -5 V	4	1
	ON: 2.5 ... 5 V		(Single message)
	max. 5 mA		
Console0 – DCD (output)	OFF: -2.5 ... -5 V	5	1
	ON: 2.5 ... 5 V		(Single message)
	max. 5 mA		
Link state interfaces	OFF: no link	from 128	1
	ON: link		(Single message)
Speed interfaces	Value in bps	from 160	7
	>= 2147483648: value is invalid		(Bit pattern 32 bit)
Signal quality inter- faces	16,0 dB >= value 160	from 192	11
	>= 8388608: value is invalid		(Measured value, scaled)
Port state interfaces	0x: Port blocked	from 224	5
	1x: Port learns and blocked		(Level setting message)
	2x: Port forwards		
	x0: Port is deactivated		
	x1: Port roll is Root		
	x2: Port roll is Designated		
	x3: Port roll is Alternate		
	x4: Port roll is Backup		
	x5: Port roll is Master		

Table 27: Information objects

Object / Function	State / Value range	Pre-set object address	ASDU data type
	>= 32768: value is invalid		

Table 27: Information objects

There is a basis address set as default value for each interface related information object.

Incremental object addresses result in respect to the existing interfaces of each device.

Interface	Link state	Link speed	Signal quality	Port state
dsl1	128	160	192	224
port1	129	161	193	225
port2	130	162	194	226
port3	131	163	195	227
port4	132	164	196	228
console0	133	165	197	229

Table 28: Addresses of the interface related information objects for 500NMD01

Interface	Link state	Link speed	Signal quality	Port state
dsl1	128	160	192	224
dsl2	129	161	193	225
port1	130	162	194	226
port2	131	163	195	227
port3	132	164	196	228
port4	133	165	197	229
console0	134	166	198	230
console1	135	167	199	231

Table 29: Addresses of the interface related information objects for 500NMD02

Interface	Link state	Link speed	Signal quality	Port state
dsl1	128	160	192	224
port1	129	161	193	225
port2	130	162	194	226
port3	131	163	195	227
port4	132	164	196	228
fo1	133	165	197	229
console0	134	166	198	230
console1	135	167	199	231

Table 30: Addresses of the interface related informaton objects for 500NMD11

Interface	Link state	Link speed	Signal quality	Port state
port1	128	160	192	224
port2	129	161	193	225
port3	130	162	194	226
port4	131	163	195	227

Table 31: Addresses of the interface related information objects for 500NMD20

Interface	Link state	Link speed	Signal quality	Port state
fo1	132	164	196	228
fo2	133	165	197	229
console0	134	166	198	230
console1	135	167	199	231

Table 31: Addresses of the interface related information objects for 500NMD20

**Commands to modify pre-set object addresses**

```

<set {iec101 | iec104} interface {1 | 2} object alarm
address-base {0-16777215}>
<set {iec101 | iec104} interface {1 | 2} object rts-in
address {0-16777215}>
<set {iec101 | iec104} interface {1 | 2} object cts-out
address {0-16777215}>
<set {iec101 | iec104} interface {1 | 2} object dcd-out
address {0-16777215}>
<set {iec101 | iec104} interface {1 | 2} object linkstate
address-base {0-16777215}>
<set {iec101 | iec104} interface {1 | 2} object linkspeed
address-base {0-16777215}>
<set {iec101 | iec104} interface {1 | 2} object sq address-
base {0-16777215}>
<set {iec101 | iec104} interface {1 | 2} object portstate
address {0-16777215}>

```

**2.22.2 Connection of Signals and Application as RTU**

For the assignment of the interface Console0 see Chapter 2.20, "Serial Interfaces". Input RTS and output CTS can be connected to relai contacts (refer to "Fig. 23: Connector alarm relais") to connect EDS500 with a potential free contact.

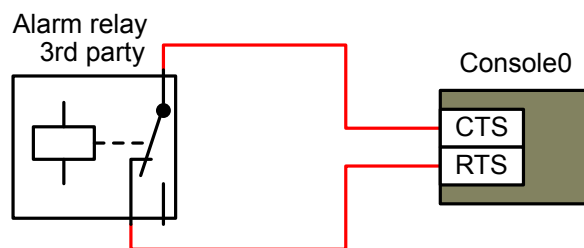


Figure 23: Connector alarm relais

The circuit shows CTS as power source. You have to take care that CTS is switched on because only then RTS will be triggered when the relay switch is up. If CTS should be kept as switchable output then the contact DCD of the interface Console0 can be used. DCD also has to be switched on.

If CTS is to be used as switched output then the contact has to be connected to a potential isolated converter (refer to "Fig. 24: Connector switch output"). This is usually an optocoupler or a triggered switch. Take care of the maximum current of 5 mA.

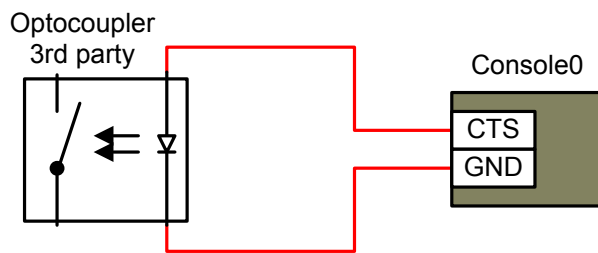


Figure 24: Connector switch output

Suitable optocouplers ideally have a nominal switch value of 3 V or 5 V and a switching current below 5 mA (e.g. Phoenix Contact PLC-BSC-5DC/1/ACT (Art.-No. 2980241) equipped with 5 V / 24 V Optocoupler (Art.-No. 2967989).

Set the output signals of the interface Console0 into a defined state for the telecontrol mode with the commands <set interface console0 dcd off> or <set interface console0 dcd on> for a deterministic state after booting of the EDS500 device.

If the DCD contact of the interface Console0 is used as feeding supply then it can be switched on by the command <set interface console0 dcd on> and switched off with command <set interface console0 dcd off>.

If the command is not applied then the state of DCD depends on the sent data at interface Console0. In normal operation data can also be sent spontaneously over the interface.

#### ADVICE

The level of the interface signals DCD and CTS is in the negative voltage area in the state off.

The information object for input RTS of interface Console0 can be operated in the following modes:

Mode	Description
switch	Switch, returns ON/OFF (ASDU data type 1) A change triggers spontaneous message.
on-counter	On-counter, returns counter (ASDU data type 15) Increment at each transition from Off to On.
transition-counter	Transition counter, returns counter (ASDU data type 15) Increment at each transition.

Table 32: RTS modes for telecontrol

Commands to set the RTS mode for telecontrol

```
<set {iecl01 | iec104} interface {1 | 2} length
transmission-cause {1-2}>
<set {iec...} interface {...} object rts-in mode {...}>
```

### 2.22.3 Concept of Interface and Polling

The IEC 60870-5-101 / IEC 60870-5-104 implementation on the EDS500 devices supports connections by several telecontrol central offices. You have to distinguish between independent central offices and central offices that depend on each other.

Every independent central office operates with its own information objects while central offices that depend on each other share information objects. The addresses (ASDU and Information objects) do not have to be the same between two independent central offices. If a configuration in an independent central office resets a counter then it will not be reset in another independent central office.

Dependent and independent central offices do not exclude each other.

In the following example the central offices 1a and 1b depend on each other, also the central offices 2a and 2b. Yet, group1 is independent from group2.

Central office 1		Central office 2		Output counters		Event
1a	1b	2a	2b	1	2	
Read		Read		10124	10124	
	Read		Read	10124	10124	
			Reset			
Read		Read		10124	0	
						+100
	Read		Read	10224	100	
	Read			10224		
	Reset					
Read				0		
	Read	Read		0	100	
			Read		100	
			Reset			
		Read			0	

Table 33: Operation with dependent and independent central offices

Independent central offices are configured with so-called interfaces. Each interface get its own set of information objects, own addresses and own time-out settings.

The interfaces are configured with the following commands where (n) stands for the interface number i.e. the central office group that shares the objects. The interface number always starts with 1.

The maximum number of groups depends on software and device.

#### 2.22.4 Configuration of an IEC 60870-5-101 Interface

The default value for the function of the IEC 60870-5-101 interfaces is: station (RTU).

Like that, IEC-101 interfaces can be configured as RTU.

A serial interface (console0 or console1) has to be set to the IEC 60870-5-101 mode to be then assigned to an IEC 60870-5-101 interface.

```
<set interface {console0 | console1} mode {configuration |
iec101 | linetest | loopback | modem | tunnel}>
```

Commands to configure an IEC 60870-5-101 interface

```
<set iec101 interface {1 | 2} attach {console0 | console1}
[balanced | unbalanced]>
```

```
<clear iec101 interface {1 | 2} attach {console0 |
console1}>
<set iec101 interface {1 | 2} link address {0-65535}>
<set iec101 interface {1 | 2} length link-address {0-2}>
<set iec101 interface {1 | 2} link retries {0-10}>
```

### 2.22.5 Configuration of an IEC 60870-5-104 Interface

If no IP address is set, any central office can connect with the device. If several interfaces are configured without IP address then the active interface with the lowest number (n) always connects.

If at least one IP address has been set then only the central office(s) with the configured IP address(es) may connect. Four IP addresses per IEC 60870-5-104 interface are configurable for central offices.

Commands to configure an IEC 60870-5-104 interface

```
<set iec104 interface {1 | 2} attach remote-ip {IP address}>
<clear iec104 interface {1 | 2} attach remote-ip {IP
address}>
```

### 2.22.6 Configuration of the Time Monitor (Time-Out)

The protocols IEC 60870-5-101 and IEC 60870-5-104 use different timeout times to control the establishment of a connection, acknowledgment and retransmission. These are typically used system-wide (central office and all remote control units) and do not have to be modified if the values are accepted that are suggested by the standard. For time parameters and default values refer to "Tab. 34: Time monitor counter".

Commands for configuring timeout for IEC 60870-5-101 / IEC 60870-5-104

```
<set {iec101 | iec104} interface {1 | 2} timeout {0-3}
{1-6000}>
```

Value for (t)	Description
0	The parameter sets the period between two connection attempts.  The default value for IEC 60870-5-101 is: 1 s The default value for IEC 60870-5-104 is: 30 s
1	Timeout for APDVs send.  The default value for IEC 60870-5-101 is: 3 s The default value for IEC 60870-5-104 is: 15 s
2	Timeout for acknowledged in case of no data messages.  The default value for IEC 60870-5-101 is: 3 s The default value for IEC 60870-5-104 is: 10 s
3	Inactivity counter for sending a test frame (TestFR, IEC 60870-5-104) or link test (IEC 60870-5-101).  The default value for IEC 60870-5-101 is: 3 s

Table 34: Time monitor counter

Value for (t)	Description
	The default value for IEC 60870-5-104 is: 20 s

Table 34: Time monitor counter

### 2.22.7 Activating and Deactivating the IEC 60870-5-101 and IEC 60870-5-104 Interfaces

In order to use IEC 60870-5-101 and IEC 60870-5-104 the corresponding interfaces have to be activated explicitly.

Also take care for IEC 60870-5-101 that the protocol is bound to a serial interface in mode iec-101.

Commands to activate / deactivate an IEC 60870-5-101 / IEC 60870-5-104 interface

```
<set {iec101 | iec104} interface {1 | 2} no shutdown>
<set {iec101 | iec104} interface {1 | 2} shutdown>
```

### 2.22.8 Setting Addresses and Address Parameters

There are degrees of freedom in respect to the protocol parameters when using IEC 60870-5-101 and IEC 60870-5-104. Typically, these are system-wide identical and have to be adapted. This includes among others the length of the protocol data fields, the acknowledging behaviour and the station and object addresses.

Commands to set the addresses and their lengths for IEC 60870-5-101 / IEC 60870-5-104

```
<set {iec101 | iec104} interface {1 | 2} station-address
{local ASDU address 0-65536}>
<set {iec101 | iec104} interface {1 | 2} length station-
address {1-2}>
<set {iec101 | iec104} interface {1 | 2} length
objectaddress {1-3}>
<set {iec101 | iec104} interface {1 | 2} object structure
{a-b-c}>
<set iec101 interface {1 | 2} length link-address {0-2}>
<set {iec101 | iec104} interface {1 | 2} length
transmission-cause {1-2}>
<set iec101 interface 1 single-character no-data-tx-rx>
<set iec101 interface 1 single-character none>
<set iec101 interface 1 single-character rx>
<set iec101 interface 1 single-character tx-rx>
```

### 2.22.9 Settings for the Protocol Conversion

To activate the protocol conversion, IEC 60870-5-101/-104 interfaces have to be bundled as pairs. Then the assignment of IEC 60870-5-101 link addresses to IEC 60870-5-104 IP addresses have to be set. Further settings include the operation of IEC 60870-5-101 interfaces as Master and details for the protocol conversion.



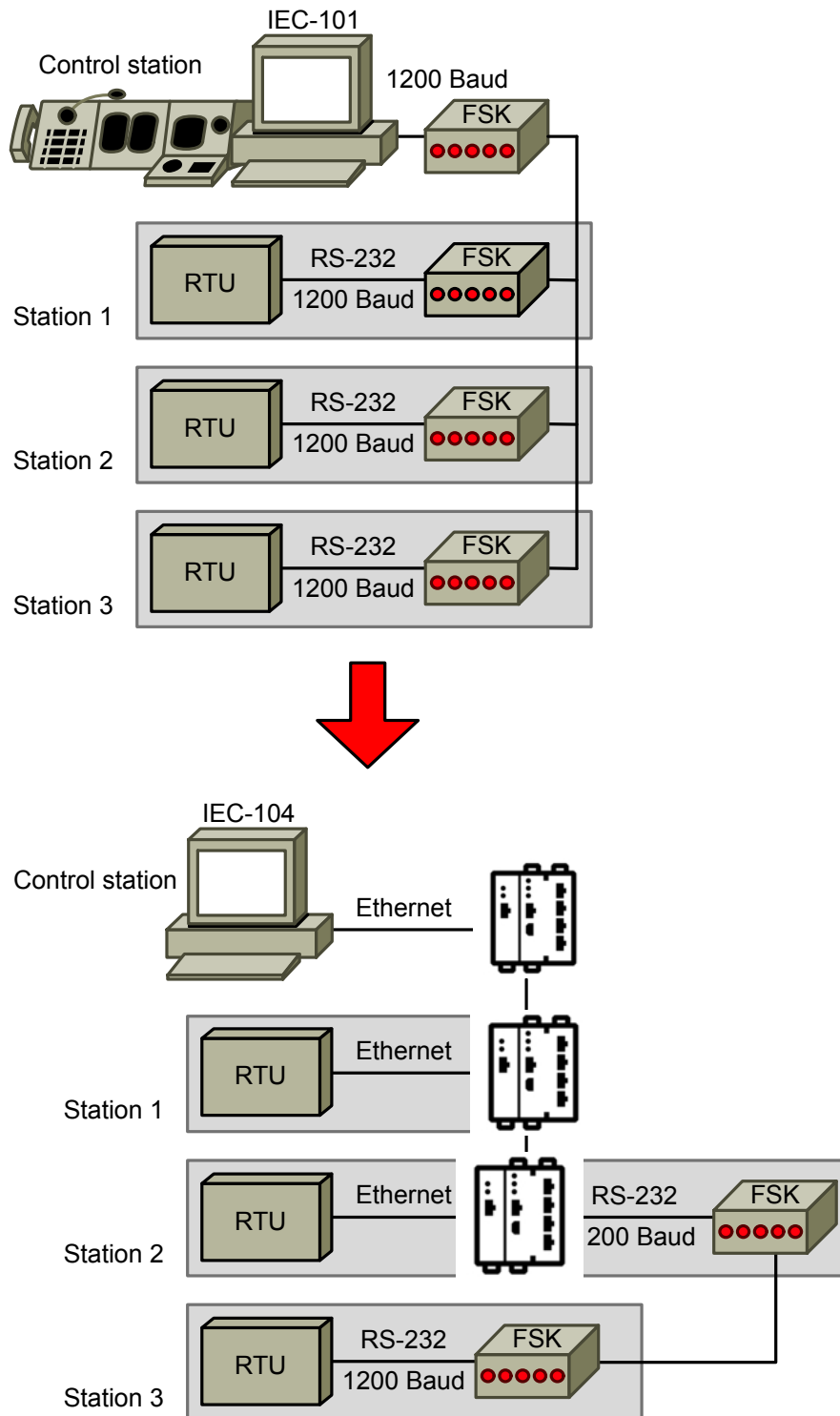


Figure 25: Step-by-step replacement of communications technology

Commands for configuring IEC 60870-5-101 / IEC 60870-5-104 protocol conversion

```

<set {iec101 | iec104} interface {1 | 2} convert to {iec101
| iec104} interface {1 | 2}>
<set system ip {start-IP-address end-IP-address}>
<set interface vlan {1-4094} ip-address {start-ip-address}
{end-ip-address} {subnet mask}>
<set {iec101 | iec104} interface {1 | 2} station-address

```

```

{local ASDU address 0-65536}>
<set iec104 interface {1 | 2} remote-station address
{station address} ip-address {IP address}>
<set iec101 interface {1 | 2} function {master | station}>
<set iec101 interface {1 | 2} poll {data1 | data2}>
<set {iec101 | iec104} interface {1 | 2} convert [no]
acknowledge>
<set {iec101 | iec104} interface {1 | 2} convert [no] asdu-
types>
<set {iec101 | iec104} interface {1 | 2} convert [no]
timestamps>

```

## 2.22.10 Technological Background of the IEC 60870-5-101,104 Conversion

The protocols IEC 60870-5-101 (abbreviated IEC-101) and IEC 60870-5-104 (abbreviated IEC-104) are both protocols to transmit telecontrol data.

IEC 60870-5-101 is based on a serial transmission (e.g. via RS-232 and voice-frequency telegraphy circuit lines)

IEC 60870-5-104 is based on a packet-oriented TCP/IP transmission.

As for the protocol design both protocols know a protocol data unit of the application layer (APDU). In the case of IEC 60870-5-101 it is transmitted in a data frame in the format FT1.2 (defined in IEC 60870-5-2), in the case of IEC 60870-5-104 via TCP with port number 2404. Both protocols divide a telegram into protocol control data (start indicator, Telegram length, control field) and application data. The protocol control information are called application layer protocol control information (APCI) for IEC 60870-5-104.

For IEC 60870-5-101 these are part of the frame format FT 1.2. The format of the application data is almost identical for both protocols and is called service data unit of the application layer (ASDU).

The protocol control information is fundamentally different for both protocols. While IEC 60870-5-104 supports polling mode (also called point-to-multipoint, multidrop or unbalanced operation) as well spontaneous operation (also called point-to-point or balanced operation) IEC 60870-5-104 only is defined for spontaneous operation.

The tasks of the protocol control information include establishing the link, transmission repetition and confirmation of data as well as flow control. This applies to both protocols although TCP already grants a safe end-to-end connection without telegram errors or loss.

Using IEC 60870-5-101, terminal devices are addressed with link addresses the size of one or two bytes. The central office inserts the link address of the target station according to the communication request and sends the telegram.

In polling mode all stations of a line get this telegram (polling mode divides terminals into groups of devices) and the addressed device answers and inserts its own link address as address.

While a send permission is granted in polling mode, this is not true for spontaneous operation. Central office and station may send without polling.

For IEC 60870-5-104 a station is addressed with IP address and TCP port number. There are no protocol specific addresses. TCP sets a point-to-point connection, polling mode does not exist.

To test the correct operation of the communications link as well as the readiness for operation of a station, there are test procedure for IEC 60870-5-101 (test function for the link layer, link test) and IEC 60870-5-104 (test APDU, TESTFR, test frame). If errors occur then the connection is terminated and re-established.

The definition of the ASDU is identical for both protocols and always has one identification field of the data unit and one or more information objects.

The identification field of the data unit defines the type of the following information objects (type id), a variable structure id (number of information objects in the ASDU), a transmission cause and the shared address of the ASDU (station address).

For IEC 60870-5-104 the transmission cause may consist of alternatively one or two bytes. If two bytes are used then the second byte has the meaning of an origin address.

IEC 60870-5-104 always uses two bytes, if the origin address is not known or not used then the byte is set to null.

The station address can be one or two bytes long for IEC 60870-5-101 whereas IEC 60870-5-104 always uses two bytes.

The type id describes the structure of the contained information objects.

Typical information objects are:

- Single point messages
- Single point commands (one bit information),
- Double point messages
- Double point commands (two bis information),
- Bit patterns,
- Measurement data,
- Counter values, a.m.m.

The information objects are defined differently with and without time stamp.

The supported type ids for IEC 60870-5-101 and IEC 60870-5-104 share a lot of ids but there are type ids exclusively for IEC 60870-5-104 and in addition there are IEC 60870-5-101 ids that are not valid any more for IEC 60870-5-104.

The differences can mainly be found in the representation of date formats and time formats.

IEC 60870-5-101 uses time stamps of the type CP24Time2a. CP24Time2a can show values of up to an hour with a resolution of milliseconds.

IEC 60870-5-104 uses time stamps of the type CP56Time2a. CP56Time2a can show values of up to 100 year with a resolution of milliseconds.

If central office and remote control devices operate strictly according to standard and use and/or support only the defined types then the transmission format and the types have to be converted.

The conversion of type ids is listed on the following pages in command direction as well as in message direction. There is the option to switch conversion on or off.

If the conversion is switched on in message direction then there are two options in respect to the extended time stamp for IEC 60870-5-104:

- Forwarding the time information from the telecontrol unit.  
The information for year, month, day, weekday and hours is set to zero and the original information of minutes and milliseconds is copied from the original time stamp CP24Time2a. As CP56Time2a time stamp decodes itself always to the range 01.01.2000 00:00:00.000 to 01.01.2000 00:59:59:999 (where the date only completes the definition).
- Replacing the time stamp of the telecontrol unit during conversion  
The system time of the switch (has to be configured via (s)NTP) is used as time stamp. As part of the IEC standards this is a substitute time and the bit RES1 (real time or substitute time) of the time stamp CP56Time2a is set accordingly. If the converting device know no valid time then the time stamp is set to invalid (bit IV).

If a conversion is pursued then it is usually preceded by an examination of the current state and the design of a conversion concept that defines the various degrees of freedom for conversion and protocols.

Type ids IEC-101 / IEC-104			Command direction / control direction Conversion to IEC-101 type id	Command direction / control direction Conversion to IEC-101 type id
			iec104 convert asdu-types (Standard)	iec104 convert no asdu-types
0	UNDEF	not used	0	0
1	M_SP_NA_1	Single message	1	1
2	M_SP_TA_1	Single message with time stamp CP24Time2a	2	2
3	M_DP_NA_1	Double message	3	3
4	M_DP_TA_1	Double message with time stamp CP24Time2a	4	4
5	M_ST_NA_1	Level setting message	5	5
6	M_ST_TA_1	Level setting message with time stamp CP24Time2a	6	6
7	M_BO_NA_1	Bit pattern 32 bit	7	7
8	M_BO_TA_1	Bit pattern 32 bit with time stamp CP24Time2a	8	8
9	M_ME_NA_1	Measured value, standardized value	9	9
10	M_ME_TA_1	Measured value, standardized value with time stamp CP24Time2a	10	10
11	M_ME_NB_1	Measured value, scaled value	11	11
12	M_ME_TB_1	Measured value, scaled value with time stamp CP24Time2a	12	12

Table 35: Type conversion in command direction

Type ids IEC-101 / IEC-104			Command direction / control direction Conversion to IEC-101 type id	Command direction / control direction Conversion to IEC-101 type id
			iec104 convert asdu- types (Stan- dard)	iec104 convert no asdu- types
13	M_ME_NC_1	Measured value, floating point with single accuracy	13	13
14	M_ME_TC_1	Measured value, floating point with single accuracy and time stamp CP24Time2a	14	14
15	M_IT_NA_1	Counted values	15	15
16	M_IT_TA_1	Counted values with time stamp CP24Time2a	16	16
17	M_EP_TA_1	Protection event with time stamp CP24Time2a	17	17
18	M_EP_TB_1	Blocked stimulations of the protection with time stamp CP24Time2a	18	18
19	M_EP_TC_1	Blocked triggers of the protection with time stamp CP24Time2a	19	19
20	M_PS_NA_1	Packed single messages with status indicator	20	20
21	M_ME_ND_1	Measured value, standardized value without quality id	21	21
22-29	TYPE_22 - 29	Reserved (standard range)	22-29	22-29
30	M_SP_TB_1	Single message with time stamp CP56Time2a	30	30
31	M_DP_TB_1	Double message with time stamp CP56Time2a	31	31
32	M_ST_TB_1	Level setting message with time stamp CP56Time2a	32	32
33	M_BO_TB_1	Bit pattern 32 bit with time stamp CP56Time2a	33	33
34	M_ME_TD_1	Measured value, standardized value with time stamp CP56Time2a	34	34
35	M_ME_TE_1	Measured value, scaled value with time stamp CP56Time2a	35	35

Table 35: Type conversion in command direction

Type ids IEC-101 / IEC-104			Command direction / control direction Conversion to IEC-101 type id	Command direction / control direction Conversion to IEC-101 type id
			iec104 convert asdu-types (Standard)	iec104 convert no asdu-types
36	M_ME_TF_1	Measured value, floating point with single accuracy and time stamp CP56Time2a	36	36
37	M_IT_TB_1	Counted values with time stamp CP56Time2a	37	37
38	M_EP_TD_1	Protection event with time stamp CP56Time2a	38	38
39	M_EP_TE_1	Blocked stimulations of the protection with time stamp CP56Time2a	39	39
40	M_EP_TF_1	Blocked triggers of the protection with time stamp CP56Time2a	40	40
41-44	TYPE_41 - 44	Reserved (standard range)	41-44	41-44
45	C_SC_NA_1	Single command	45	45
46	C_DC_NA_1	Double command	46	46
47	C_RC_NA_1	Level setting command	47	47
48	C_SE_NA_1	Target value setting command, standardized value	48	48
49	C_SE_NB_1	Target value setting command, scaled value	49	49
50	C_SE_NC_1	Target value setting command, floating point with single accuracy	50	50
51	C_BO_NA_1	Bit pattern command 32 bit	51	51
52-57	TYPE_52 - 57	Reserved (standard range)	52-57	52-57
58	C_SC_TA_1	Single command with time stamp CP56Time2a	45	58
59	C_DC_TA_1	Double command with time stamp CP56Time2a	46	59
60	C_RC_TA_1	Level setting command with time stamp CP56Time2a	47	60
61	C_SE_TA_1	Level setting command, standardized value with time stamp CP56Time2a	48	61

Table 35: Type conversion in command direction

Type ids IEC-101 / IEC-104			Command direction / control direction Conversion to IEC-101 type id	Command direction / control direction Conversion to IEC-101 type id
			iec104 convert asdu-types (Standard)	iec104 convert no asdu-types
62	C_SE_TB_1	Level setting command, scaled value with time stamp CP56Time2a	49	62
63	C_SE_TC_1	Target value setting command, floating point with single accuracy and time stamp CP56Time2a	50	63
64	C_BO_TA_1	Bit pattern command 32 bit with time stamp CP56Time2a	51	64
65-69	TYPE_65-69	Reserved (standard range)	65-69	65-69
70	M_EI_NA_1	End of initialization	70	70
71-99	TYPE_71-99	Reserved (standard range)	71-99	71-99
100	C_IC_NA_1	(general, station) polling command	100	100
101	C_CI_NA_1	Counter query command	101	101
102	C_RD_NA_1	Polling command	102	102
103	C_CS_NA_1	Time synchronization command	103	103
104	C_TS_NA_1	Check command	104	104
105	C_RP_NA_1	Process reset command	105	105
106	C_CD_NA_1	Command to assess telegram runtime	106	106
107	C_TS_TA_1	Check command with time stamp CP56Time2a	107	107
108-109	TYPE_108-109	Reserved (standard range)	108-109	108-109
110	P_ME_NA_1	Parameter for measured values, standardized value	110	110
111	P_ME_NB_1	Parameter for measured values, scaled value	111	111
112	P_ME_NC_1	Parameter for measured value, floating point with single accuracy	112	112
113	P_AC_NA_1	Parameter for activation	113	113
114-119	TYPE_114-119	Reserved (standard range)	114-119	114-119

Table 35: Type conversion in command direction

Type ids IEC-101 / IEC-104			Command direction / control direction Conversion to IEC-101 type id	Command direction / control direction Conversion to IEC-101 type id
			iec104 convert asdu-types (Standard)	iec104 convert no asdu-types
120	F_FR_NA_1	File ready	120	120
121	F_SR_NA_1	Section ready	121	121
122	F_SC_NA_1	Polling directory, selection, polling, section polling	122	122
123	F_LS_NA_1	Last section, last segment	123	123
124	F_FA_NA_1	File acknowledgement, section acknowledgement	124	124
125	F_SG_NA_1	Section	125	125
126	F_DR_TA_1	Directory	126	126
127-225	TYPE_127-255	Reserved (user-defined range)	127-255	127-255

Table 35: Type conversion in command direction

Type ids IEC-101 / IEC-104			Message direction / Monitor direction Conversion to IEC-104 type id	Message direction / Monitor direction Conversion to IEC-104 type id
			iec104 convert asdu-types (Standard)	iec101 convert no asdu-types
0	UNDEF	not used	0	0
1	M_SP_NA_1	Single message	1	1
2	M_SP_TA_1	Single message with time stamp CP24Time2a	30	2
3	M_DP_NA_1	Double message	3	3
4	M_DP_TA_1	Double message with time stamp CP24Time2a	31	4

Table 36: Type conversion in message direction



Type ids IEC-101 / IEC-104			Message direction / Monitor direction Conversion to IEC-104 type id	Message direction / Monitor direction Conversion to IEC-104 type id
			iec104 convert asdu-types (Standard)	iec101 convert no asdu-types
5	M_ST_NA_1	Level setting message	5	5
6	M_ST_TA_1	Level setting message with time stamp CP24Time2a	32	6
7	M_BO_NA_1	Bit pattern 32 bit	7	7
8	M_BO_TA_1	Bit pattern 32 bit with time stamp CP24Time2a	33	8
9	M_ME_NA_1	Measured value, standardized value	9	9
10	M_ME_TA_1	M_ME_TA_1 Measured value, standardized value with time stamp CP24Time2a	34	10
11	M_ME_NB_1	Measured value, scaled value	11	11
12	M_ME_TB_1	Measured value, scaled value with time stamp CP24Time2a	35	12
13	M_ME_NC_1	Measured value, floating point with single accuracy	13	13
14	M_ME_TC_1	Measured value, floating point with single accuracy and time stamp CP24Time2a	36	14
15	M_IT_NA_1	Counted values	15	15
16	M_IT_TA_1	Counted values with time stamp CP24Time2a	37	16
17	M_EP_TA_1	Protection event with time stamp CP24Time2a	38	17
18	M_EP_TB_1	Blocked stimulations of the protection with time stamp CP24Time2a	39	18
19	M_EP_TC_1	Blocked triggers of the protection with time stamp CP24Time2a	40	19
20	M_PS_NA_1	Packed single messages with status indicator	20	20
21	M_ME_ND_1	Measured value, standardized value without quality id	21	21

Table 36: Type conversion in message direction

Type ids IEC-101 / IEC-104			Message direction / Monitor direction Conversion to IEC-104 type id	Message direction / Monitor direction Conversion to IEC-104 type id
			iec104 convert asdu-types (Standard)	iec101 convert no asdu-types
22-29	TYPE_22-29	Reserved (standard range)	22-29	22-29
30	M_SP_TB_1	Single message with time stamp CP56Time2a	30	30
31	M_DP_TB_1	Double message with time stamp CP56Time2a	31	31
32	M_ST_TB_1	Level setting message with time stamp CP56Time2a	32	32
33	M_BO_TB_1	Bit pattern 32 bit with time stamp CP56Time2a	33	33
34	M_ME_TD_1	Measured value, standardized value with time stamp CP56Time2a	34	34
35	M_ME_TE_1	Measured value, scaled value with time stamp CP56Time2a	35	35
36	M_ME_TF_1	Measured value, floating point with single accuracy and time stamp CP56Time2a	36	36
37	M_IT_TB_1	Counted values with time stamp CP56Time2a	37	37
38	M_EP_TD_1	Protection event with time stamp CP56Time2a	38	38
39	M_EP_TE_1	Blocked stimulations of the protection with time stamp CP56Time2a	39	39
40	M_EP_TF_1	Blocked triggers of the protection with time stamp CP56Time2a	40	40
41-44	TYPE_41-44	Reserved (standard range)	41-44	41-44
45	C_SC_NA_1	Single command	58	45
46	C_DC_NA_1	Double command	59	46
47	C_RC_NA_1	Level setting command	60	47
48	C_SE_NA_1	Target value setting command, standardized value	61	48

Table 36: Type conversion in message direction

Type ids IEC-101 / IEC-104			Message direction / Monitor direction Conversion to IEC-104 type id	Message direction / Monitor direction Conversion to IEC-104 type id
			iec104 convert asdu-types (Standard)	iec101 convert no asdu-types
49	C_SE_NB_1	Target value setting command, scaled value	62	49
50	C_SE_NC_1	Target value setting command, floating point with single accuracy	63	50
51	C_BO_NA_1	Bit pattern command 32 bit	64	51
52-57	TYPE_52-57	Reserved (standard range)	52-57	52-57
58	C_SC_TA_1	Single command with time stamp CP56Time2a	58	58
59	C_DC_TA_1	Double command with time stamp CP56Time2a	59	59
60	C_RC_TA_1	Level setting command with time stamp CP56Time2a	60	60
61	C_SE_TA_1	Level setting command, standardized value with time stamp CP56Time2a	61	61
62	C_SE_TB_1	Level setting command, scaled value with time stamp CP56Time2a	62	62
63	C_SE_TC_1	Target value setting command, floating point with single accuracy and time stamp CP56Time2a	63	63
64	C_BO_TA_1	Bit pattern command 32 bit with time stamp CP56Time2a	64	64
65-69	TYPE_65-69	Reserved (standard range)	65-69	65-69
70	M_EI_NA_1	End of initialization	70	70
71-99	TYPE_71-99	Reserved (standard range)	71-99	71-99
100	C_IC_NA_1	(general, station) polling command	100	100
101	C_CI_NA_1	Counter query command	101	101
102	C_RD_NA_1	Polling command	102	102
103	C_CS_NA_1	Time synchronization command	103	103

Table 36: Type conversion in message direction

Type ids IEC-101 / IEC-104			Message direction / Monitor direction Conversion to IEC-104 type id	Message direction / Monitor direction Conversion to IEC-104 type id
			iec104 convert asdu-types (Standard)	iec101 convert no asdu-types
104	C_TS_NA_1	Check command	107	104
105	C_RP_NA_1	Process reset command	105	105
106	C_CD_NA_1	Command to assess telegram runtime	106	106
107	C_TS_TA_1	Check command with time stamp CP56Time2a	107	107
108-109	TYPE_108-109	Reserved (standard range)	108-109	108-109
110	P_ME_NA_1	Parameter for measured values, standardized value	110	110
111	P_ME_NB_1	Parameter for measured values, scaled value	111	111
112	P_ME_NC_1	Parameter for measured value, floating point with single accuracy	112	112
113	P_AC_NA_1	Parameter for activation	113	113
114-119	TYPE_114-119	Reserved (standard range)	114-119	114-119
120	F_FR_NA_1	File ready	120	120
121	F_SR_NA_1	Section ready	121	121
122	F_SC_NA_1	Polling directory, selection, polling, section polling	122	122
123	F_LS_NA_1	Last section, last segment	123	123
124	F_FA_NA_1	File acknowledgement, section acknowledgement	124	124
125	F_SG_NA_1	Section	125	125
126	F_DR_TA_1	Directory	126	126
127-255	TYPE_127-255	Reserved (user-defined range)	127-255	127-255

Table 36: Type conversion in message direction

## 2.23 RADIUS

The RADIUS protocol (Remote Authentication Dial-In User Service) serves to authenticate when dialling in to a computer network. The authentication is not carried out by the devices in the network infrastructure but by a central RADIUS server. So, an existing user database like Active Directory can be used for authentication on arbitrary devices.

The user authentication of the EDS500 devices (Chapter 2.3.2, "Login Mode Radius") can use RADIUS to verify the validity of a login with Telnet, SSH or serial connections web interface.

Furthermore with the help of RADIUS a port authentication can be carried out according to IEEE 802.1X (Chapter 2.24, "Access Control and Device Authentication with IEEE 802.1X"). This does not safeguard the login on a EDS500 device but the whole network access via a specific port.

Commands to configure the RADIUS protocol

```
<set system radius server {IP address} [{server port}]
{shared secret}>
<clear system radius server {IP address}>
```

## 2.24 Access Control and Device Authentication with IEEE 802.1X

The IEEE 802.1X standard offers the possibility to apply an access protection for physical ports in the LAN. A device ("Supplicant") connected to an EDS500 managed switches ("Authenticator") is granted network access only after a successful authentication. The Authenticator (in this case the EDS500 device) does not perform the actual authentication, but instead uses a RADIUS server for this purpose, which must be configured (Chapter 2.23, "RADIUS").

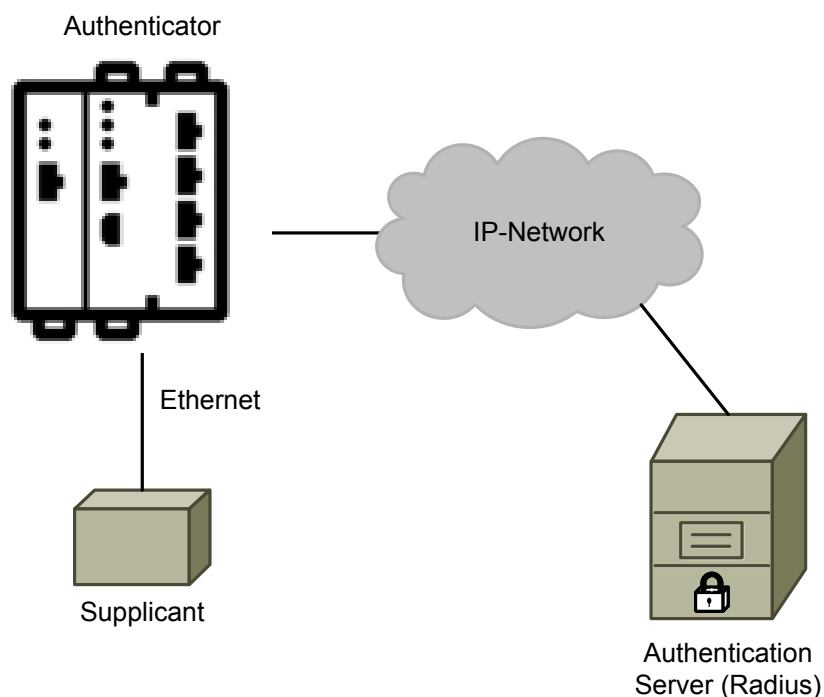


Figure 26: Access control with IEEE 802.1X

Default configuration:

By default, 802.1X is activated and every port is unlocked (`<set dot1x portcontrol {...} auth-force>`).

### Configuring access negotiation

To activate the automatic access control, it is sufficient to configure the setting `<set dot1x portcontrol {...} pae-auto>`.

The presence of a RADIUS server in the device config and the fact that this server can be reached over the network is mandatory for the function of 802.1X.

The method of access control negotiation must be synchronized between Supplicant and Authentication Server (RADIUS).

The setting `<set dot1x reauthentication port-down [no] allow>` allows to configure, whether a port may renegotiate the access following a loss of link.

#### MAC-Authentication-Bypass (MAB)

If 802.1X is to be used but a Supplicant does not support this, access control can fall back to MAC-Authentication-Bypass (MAB). This mechanism performed the authentication using the MAC address of the Supplicants.

To activate MAB configure the setting `<set dot 1x mab {...} enable>`, additional to `<set dot 1x portcontrol {...} pae-auto>`.

RADIUS Attribute	Format	Example
1 (Username)	12 hexadecimal digits, all lowercase, and no punctuation	30b216002f3a
2 (Password)	The username (encrypted)	
31(Calling-Station-Id)	6 groups of 2 hexadecimal digits, all uppercase, and separated by hyphens	30-B2-16-00-2F-3A

Table 37: Configuration of the RADIUS server for a Supplicant with MAB

Commands to related 802.1X:

```
<set dot1x [no] enable>
<set dot1x portcontrol {fastethernet0 | fo1 | fo2 | port1
| port2 | port3 | port4} {auth-force | pae-auto | unauth-
force}>
<set dot1x mab {port1 | port2 | port3 | port4} [no] enable>
<set dot1x reauthentication port-down [no] allow>
<show dot1x>
```

#### ADVICE

The setting `<set dot1x reauthentication port-down allow>` includes the danger that by plugging in an Ethernet switch or something similar between Supplicant and Authenticator potential illegal network access is possible. When using a hub the 802.1X authentication can be recorded.

## 2.25 Access Lists

### 2.25.1 Concept

EDS500 devices offer 16 access lists that help to classify Ethernet frames. If at least one rule from a list matches an Ethernet frame then the linked action is carried out (forwarding, blocking, change Class-of-Service).

Access lists can either be defined as deny lists (blacklist, allowed is anything outside the specified criteria) or as permit list (whitelist, allowed is everything from the list).

Default configuration:

Access lists are disabled.

Every access list can contain up to 16 rules.

Creating the first rule of an access list determines if this is a deny list or a permit list.

Subsequent, deviating commands are ignored.

Each rule can define several criterias that all have to match before the action of the rule is executed.

Example:

“Allow all Ethernet frames with a defined source MAC address and a defined target TCP port”.

The following criteria ( Chapter 2.25.2, "Filter for MAC Addresses" to Chapter 2.25.6, "Filter for TCP and UDP Ports" ) can be freely combined in all of the 16 rules (several commands per rule).

Commands for access list management:

```
<show access-list>
<show access-list {1-16}>
<access-list {1-16} clear>
<access-list {1-16} clear rule {1-16}>
<access-list {...} ethertype {...}>
<access-list {1-16} {deny-rule | permit-rule} {1-16}
ethertype {arp | ip | {0x0800-0xffff}}>
<access-list {...} ip [...] {...}>
<access-list {1-16} {deny-rule | permit-rule} {1-16} ip
[{destination | source} {IP address} [{subnet mask}]]>
<access-list {...} mac [...] {...}>
<access-list {1-16} {deny-rule | permit-rule} {1-16} mac
{destination | source} {aa-bb-cc-dd-ee-ff | aabb.ccdd.eeff |
aabbccddeeff}>
<access-list {...} protocol {...}>
<access-list {1-16} {deny-rule | permit-rule} {1-16}
protocol {tcp | udp | icmp | {0-255}}>
<access-list {...} tcp dst-port {...}>
<access-list {1-16} {deny-rule | permit-rule} {1-16} tcp
dst-port {0-65535}>
<access-list {...} tcp src-port {...}>
<access-list {1-16} {deny-rule | permit-rule} {1-16} tcp
src-port {0-65535}>
<access-list {...} udp dst-port {...}>
<access-list {1-16} {deny-rule | permit-rule} {1-16} udp
dst-port {0-65535}>
<access-list {...} udp src-port {...}>
<access-list {1-16} {deny-rule | permit-rule} {1-16} udp
src-port {0-65535}>
```

## 2.25.2 Filter for MAC Addresses

The target MAC address and the source MAC address of an Ethernet frame can be checked. To treat broadcast frames use the target MAC address ff-ff-ff-ff-ff-ff.

Commands to filter for MAC addresses:

```
<access-list {1-16} {deny-rule | permit-rule} {1-16} mac
{destination | source} {aa-bb-cc-dd-ee-ff | aabb.ccdd.eeff |
aabbccddeeff}>
```

### 2.25.3 Filter for Ethertype

To check the Ethertype field of a frame the parameter can either be set as a number (0x0800 to 0xffff), or as keyword (ip for the Internet protocol (version 4), arp for the Address Resolution Protocol).

Commands to filter for Ethertype:

```
<access-list {1-16} {deny-rule | permit-rule} {1-16}
  ethertype {arp | ip | {0x0800-0xffff}}>
```

### 2.25.4 Filter for IP Addresses or Ranges

The target and source IP addresses can be entered explicitly. It is also possible to enter subnet ranges by adding the subnet mask. The Ethernet frame implicitly has to contain an IP packet to match this criterion.

Commands to filter for IP addresses or ranges:

```
<access-list {1-16} {deny-rule | permit-rule} {1-16} ip
  [{destination | source} {IP address} [{subnet mask}]]>
```

### 2.25.5 Filters for the IP Payload Protocol

The payload protocol that is contained in the IP packet payload data can be checked by either entering the protocol ID as a number (0 to 255) or as a keyword (tcp for the Transmission Control protocol, udp for the User Datagram protocol, icmp for the Internet Control Message protocol). The Ethernet frame implicitly has to contain an IP packet to match this criterion.

Commands to filter for IP follow-up protocol:

```
<access-list {1-16} {deny-rule | permit-rule} {1-16}
  protocol {tcp | udp | icmp | {0-255}}>
```

### 2.25.6 Filter for TCP and UDP Ports

The target and source port for TCP and/or UDP packets can be checked. The Ethernet frame implicitly has to contain a TCP/IP or UDP/IP packet to match this criterion.

Commands to filter for TCP/UDP ports

```
<access-list {1-16} {deny-rule | permit-rule} {1-16} tcp
  dst-port {0-65535}>
<access-list {1-16} {deny-rule | permit-rule} {1-16} tcp
  src-port {0-65535}>
<access-list {1-16} {deny-rule | permit-rule} {1-16} udp
  dst-port {0-65535}>
<access-list {1-16} {deny-rule | permit-rule} {1-16} udp
  src-port {0-65535}>
```

### 2.25.7 Access Control Lists as Incoming or Outgoing Packet Filter for Interfaces

Each access control list can be set as packet filter at the interfaces of EDS500 devices for incoming and outgoing direction.



Depending whether it is a Deny or a Permit list the packets are blocked or forwarded that match the criteria of the Access Control List of the interface.

An incoming and outgoing list can also be configured for the system. Like this the security can be enhanced and/or a firewall can be established.

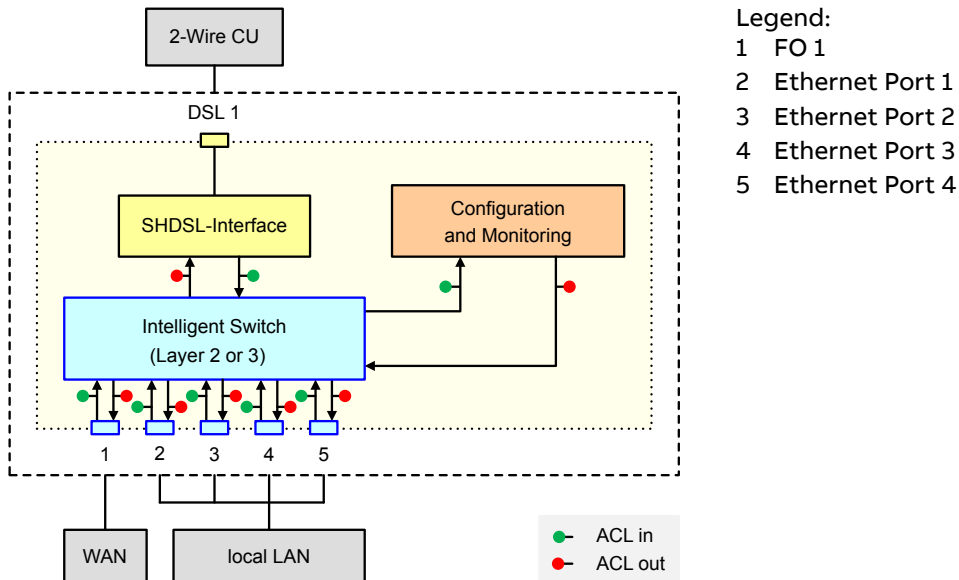


Figure 27: ACL overview for a 500NMD11

Commands for the configuration of incoming / outgoing packet filters for interfaces:

```
<set interface channel0 acl {1-16} [in | out]>
<set interface {dsl1 | dsl2} acl {1-16} [in | out]>
<set switch {fo1 | fo2} acl {1-16} [in | out]>
<set switch {port1 | port2 | port3 | port4} acl {1-16} [in | out]>
<set system acl {1..16} [in | out]>
<clear interface channel0 acl {1-16} [in | out]>
<clear interface {dsl1 | dsl2} acl {1-16} [in | out]>
<clear switch {fo1 | fo2} acl {1-16} [in | out]>
<clear switch {port1 | port2 | port3 | port4} acl {1-16} [in | out]>
<clear system acl [in | out]>
```

## 2.25.8 Access Lists as Class Map to Qualify QoS of the Data Traffic

Access lists can be used as any Class Maps for QoS classification. A Class-of-Service can be assigned to an access list at interface of a EDS500 device. If an Ethernet frame matches the criteria of this Class Map the CoS is set to the configured class. Like this e.g. the data traffic of devices that are not capable of QoS can be tagged with a certain Class-of-Service.

### ADVICE

The Class-of-Service gets rewritten (remapped) for those frames that are classified as allowed (permitted) by the list. The other (denied) frames keep the present CoS.

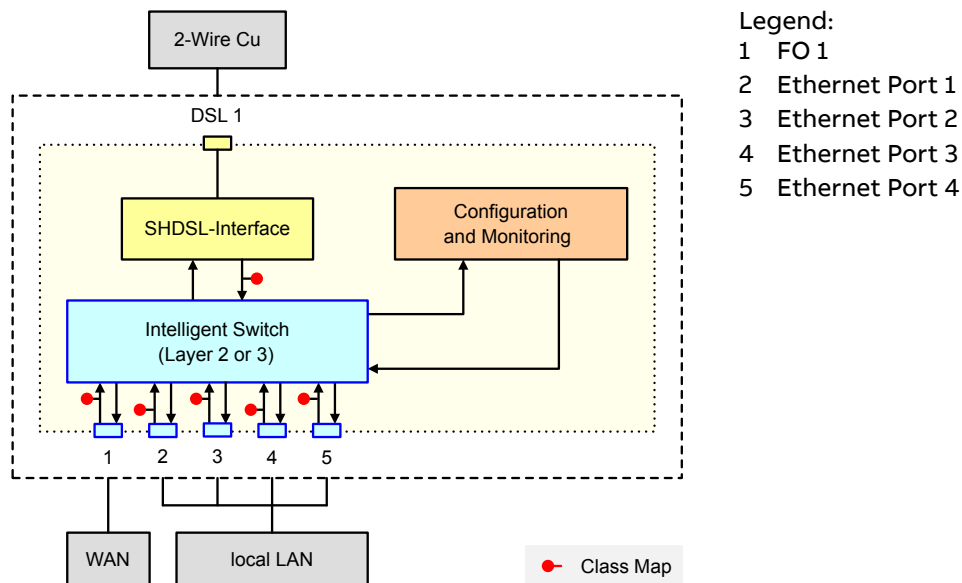


Figure 28: Class Map overview for a 500NMD11

Commands for the configuration of Class Maps for interfaces

```
<set interface channel0 class-map {0-7} acl {1-16}>
<set interface {dsl1 | dsl2} class-map {0-7} acl {1-16}>
<set switch {fo1 | fo2} class-map {0-7} acl {1-16}>
<set switch {port1 | port2 | port3 | port4} class-map {0-7}
acl {1-16}>
<clear interface channel0 class-map>
<clear interface {dsl1 | dsl2} class-map>
<clear switch {fo1 | fo2} class-map>
<clear switch {port1 | port2 | port3 | port4} class-map>
```

## 2.26 Syslog and Device Internal Log

EDS500 devices store information messages in an internal event storage. If there is synchronization with a time server (NTP server), the time stamp with date and time is used, otherwise the current system uptime is used as time stamp.

The event log can be displayed as follows:

- at the command line interface (CLI)
- at the web interface where it is also available as text file

Commands to use the internal device logs

```
<show log>
<clear log>
```

Logged events can be distributed to up to 10 Syslog servers in the network. There the messages can be processed and evaluated.

Default configuration:

Client mode - n/a

Commands to configure Syslog:

```
<set system syslog server {IP address} {{0-7} | abb-
security-events}>
<clear system syslog server {IP address}>
```

```
<show system syslog>
<debug system syslog testmessage [{IP address}]]>
```

## 2.27 SNMP Network Management

SNMP (Simple Network Management Protocol) is intended for the central monitoring and control of network devices.

The EDS500 devices support SNMP in the versions SNMPv1, SNMPv2c and SNMPv3.

Devices support queries (Get, Set, GetNext, GetBulk) and spontaneous messages (traps/notifications) to configured trap servers and registered managers. Many important system parameters can be monitored and set with SNMP.

### 2.27.1 SNMP-Agent Settings

Default configuration:

In the default configuration SNMP is disabled.

The extent of the access as well as user-defined passwords (community strings) can be defined.

Commands to activate/deactivate the SNMP agent:

```
<set system snmp {{enable [read-only | read-write]} | {no
enable}}}>
<set system snmp enable>
<set system snmp enable read-write>
<set system snmp enable read-only>
<set system snmp no enable>
<set system snmp version {any | v3-only}>
<show system snmp>
```

By default there are no user-defined community strings. In this case the fallback community strings for read and write access are active.

Community type	Community-String	Read access	Write access
Read-Community	public	Yes	No
Write-Community	private	Yes	Yes

Table 38: Fallback-Community-Strings in SNMP agent

If at least one user-defined read community string is set, then the fallback community string 'public' is invalid. If at least one user-defined write community string is set, then the fallback community string 'private' is invalid.

#### ADVICE

If in addition to the user-defined community strings the fallback strings 'public' and 'private' should also be valid they have to be set as user-defined community strings.

Up to 6 user-defined read and write community strings can be set. These can be used simultaneously. Community strings may have a length of up to 48 characters.

Commands to set SNMP community strings:

```
<set system snmp read-community {string48}>
<set system snmp write-community {string48}>
```

```
<clear system snmp read-community [{community string}]]>
<clear system snmp write-community [{community string}]]>
```

## 2.27.2 MIB Support

EDS500 devices support the following MIBs:

Name	Reference:
MIB-2	RFC 1213
SNMPv2-MIB	RFC 3418
BRIDGE-MIB	RFC 1493 / RFC 4188
IF-MIB	RFC 2863
IP-MIB	RFC 4293
TCP-MIB	RFC 4022
UDP-MIB	RFC 4113
RMON-MIB	RFC 2819
LLDP-MIB	IEEE 802.1AB
HYTEC-MIB	Manufacturer specific device MIB

Table 39: Supported MIBs

## 2.27.3 Vendor Specific Device MIB

In addition to the objects of the standard MIBs listed in Chapter 2.27.2, "MIB Support" the EDS500 devices have further, device specific objects that are defined in a dedicated vendor proprietary MIB. This is called ABB-EDS500-MIB and includes definitions of product ids, trap ids and object ids (OIDs).

Product IDs

Return value for the object sysObjectID (1.3.6.1.2.1.1.2.0) of the MIB-2 group 'system'.

Object name	OID	Device name
eds500nmd01	1.3.6.1.4.1.21939.1.5.1	500NMD01
eds500nmd02	1.3.6.1.4.1.21939.1.5.2	500NMD02
eds500nmd11	1.3.6.1.4.1.21939.1.5.11	500NMD11
eds500nmd20	1.3.6.1.4.1.21939.1.5.20	500NMD20

Table 40: Product IDs for sysObjectID

### 2.27.3.1 Trap IDs

Refer to "Tab. 57: Trap messages of EDS500 devices".

### 2.27.3.2 Object IDs

Object name	Read object	Write object
<b>OID</b>		
runConfigSizeValue	Size of the running-config	

Table 41: Objects of the group abb->abbConfig

Object name	Read object	Write object
<b>OID</b>		
1.3.6.1.4.1.21939.8.1.0		
startConfigSizeValue	Size of the startup-config	
1.3.6.1.4.1.21939.8.2.0		
startConfigLastSave	System Uptime since last saving of the startup-config	Any value executes command <copy running-config startup-config>.
1.3.6.1.4.1.21939.8.3.0		
stickConfigSizeValue	Size of the stick-config	
1.3.6.1.4.1.21939.8.4.0		
stickConfigLastSave	System Uptime since last saving of the stick-config	Any value executes command <copy running-config stick-config>.
1.3.6.1.4.1.21939.8.5.0		
runConfigLastSave	Like startConfigLastSave	Like startConfigLastSave
1.3.6.1.4.1.21939.8.6.0		
runConfigLastModified	System Uptime since last modification of running-config	
1.3.6.1.4.1.21939.8.7		
stickIsPresent	Information whether a configuration stick is plugged in:	
1.3.6.1.4.1.21939.8.8.0	–sticknotpresent (0)  –stickpresent (1)	
stickIsReadOnly	Information whether a plugged in configuration stick has been set to read-only:	readwrite (0) executes command <set config-stick no read-only>.
1.3.6.1.4.1.21939.8.9.0	–readwrite (0)  –readonly (1)	readonly (1) executes command <set config-stick read-only>.

Table 41: Objects of the group abb-&gt;abbConfig

Object name	Read object	Write object
<b>OID</b>		
reload	–no (0)	triggerreload (1) executes command <reload>.
1.3.6.1.4.1.21939.9.0.0	–triggerreload (1)  –reloading (2)	

Table 42: Objects of the group abb-&gt;abbMgmt

Object name	Read object	Write object
<b>OID</b>		
boardVersion	Coded version of the main-board	
1.3.6.1.4.1.21939.9.1.1.1.0		

Table 43: Objects of the group abb-&gt;abbMgmt-&gt;system-&gt;version

Object name	Read object	Write object
<b>OID</b>		
firmwareVersion 1.3.6.1.4.1.21939.9.1.1.2.0	Coded version of the firmwareversion, shows as 4 bytes:  –Byte 0: Version Main  –Byte 1: Version Major  –Byte 2: Version Minor  –Byte 3: Version Flags  Example: Version 1.37.3 coded as hex 01 25 03 00, decimal 19202816	
subsystemVersion 1.3.6.1.4.1.21939.9.1.1.3.0	Coded version of the sub-system if applicable	
cpIdVersion 1.3.6.1.4.1.21939.9.1.1.4.0	Coded version of the CPLD if applicable	
systemDescription 1.3.6.1.4.1.21939.9.1.1.5.0	ASCII text: firmware message incl. version	
subsystemDescription 1.3.6.1.4.1.21939.9.1.1.6.0	ASCII text: Subsystem messages, if applicable	
extensionBoard 1.3.6.1.4.1.21939.9.1.1.7.0	ASCII text: type of the expansion board if applicable	
extensionBoardVersion 1.3.6.1.4.1.21939.9.1.1.8.0	Coded version of the expansion board if applicable	
powerBoardVersion 1.3.6.1.4.1.21939.9.1.1.9	Coded version of the PSU board if applicable	

Table 43: Objects of the group abb->abbMgmt->system->version

Object name	Read object	Write object
<b>OID</b>		
sensorDetected 1.3.6.1.4.1.21939.9.1.2.1.1.0	Temperature sensor detected:  –notdetected (0)  –detected (1)	
actualTemperature 1.3.6.1.4.1.21939.9.1.2.1.2.0	Device temperature as integer	
minimalTemperature 1.3.6.1.4.1.21939.9.1.2.1.3.0	Lowest device temperature ever as integer	
minimalTemperatureTime-stamp 1.3.6.1.4.1.21939.9.1.2.1.4.0	Time of the lowest temperature as SNTP seconds or zero	
maximalTemperature	Highest device temperature ever as integer	

Table 44: Objects of the group abb->abbMgmt->system->enviroment->temperature

Object name	Read object	Write object
<b>OID</b>		
1.3.6.1.4.1.21939.9.1.2.1.5.0		
maximalTemperatureTime-stamp	Time of the highest temperature as SNTP seconds or zero	
1.3.6.1.4.1.21939.9.1.2.1.6.0		
externalSensorsCount	Number of detected external temperature sensors	
1.3.6.1.4.1.21939.9.1.2.1.7.0		
extTempTable	Table for external temperature sensors	
1.3.6.1.4.1.21939.9.1.2.1.8...		

Table 44: Objects of the group abb->abbMgmt->system->enviroment->temperature

Object name	Read object	Write object
<b>OID</b>		
remotelP	Source IP of the SNMP request (use for NAT/PAT)	
1.3.6.1.4.1.21939.9.1.3.1.0		
lastReloadReason	Device start:	
1.3.6.1.4.1.21939.9.1.3.2.0	-unknown (0) -coldstart (1) -warmstarthardware (2) -warmstartsoftware (4) -watchdog (8)	

Table 45: Objects of the group abb-&gt;abbMgmt-&gt;system-&gt;information

Object name	Read object	Write object
<b>OID</b>		
dsaKeyFingerprint	Fingerprint of the DSA system crypto key	
1.3.6.1.4.1.21939.9.1.4.1.0		
dsaSessionsReady	Number of prepared DSA sessions	
1.3.6.1.4.1.21939.9.1.4.2.0		

Table 46: Objects of the group abb-&gt;abbMgmt-&gt;system-&gt;crypto

Object name	Read object	Write object
<b>OID</b>		
tftpIP	IP address of the TFTP server.	Sets the IP address of the TFTP server. has to be set together with tftpFilename and state.
1.3.6.1.4.1.21939.9.1.8.1.0		
tftpFilename	TFTP filename	Sets the filename has to be set together with tftpIP and state.
1.3.6.1.4.1.21939.9.1.8.2.0		

Table 47: Objects of the group abb->abbMgmt->system->tftpControl

Object name	Read object	Write object
<b>OID</b>		
tftpBytesTransferred 1.3.6.1.4.1.21939.9.1.8.3.0	Number of transported bytes via TFTP	
state 1.3.6.1.4.1.21939.9.1.8.4.0	Current state of transmission: -ready (0) -transfer (1) -erase (2) -program (3)	Starts a TFTP transmission. has to be set together with tftpIP and tftpFilename. -doFirmwareUpdate (64) -copyStartConfigToTftp (65) -copyRunConfigToTftp (66) -copyStickConfigToTftp (67) -copyTftpToStartConfig (68) -copyTftpToStickConfig (69) -copyTftpToDssKey (70)
owner 1.3.6.1.4.1.21939.9.1.8.5.0	Information about the origin of the TFTP transmission: -none (0) -console (1) -telnet (2) -http (4) -snmp (8)	
progBytesTransferred 1.3.6.1.4.1.21939.9.1.8.6.0	Progress in bytes when programming the firmware	
transferResult 1.3.6.1.4.1.21939.9.1.8.7.0	ASCII text: status message of the last TFTP transmission	
Table 47: Objects of the group abb->abbMgmt->system->tftpControl		

Object name	Read object	Write object
<b>OID</b>		
dsaKeyFingerprint 1.3.6.1.4.1.21939.9.1.4.1.0	Fingerprint of the DSA system crypto key	
dsaSessionsReady 1.3.6.1.4.1.21939.9.1.4.2.0	Number of prepared DSA sessions	
Table 48: Objects of the group abb->abbMgmt->system->crypto		



Object name	Read object	Write object
<b>OID</b>		
speedsetbyuser 1.3.6.1.4.1.21939.9.2.2.1.2.x	Set data rate in bps	sets a configured data rate in bps
speedsetbysystem 1.3.6.1.4.1.21939.9.2.2.1.3.x	Selected data rate in bps	
speednegotiated 1.3.6.1.4.1.21939.9.2.2.1.4.x	Effectively negotiated data rate in bps	
speedmode 1.3.6.1.4.1.21939.9.2.2.1.5.x	Mode of the data rate: –manual (0) –auto (1) –adapt (2) –fallback (3)	Sets the mode of the data rate
duplexsetbyuser 1.3.6.1.4.1.21939.9.2.2.1.6.x	Configured duplex: –half (0) –full (1)	Sets a configured duplex
duplexsetbysystem 1.3.6.1.4.1.21939.9.2.2.1.7.x	Selected duplex: –half (0) –full (1)	
duplexnegotiated 1.3.6.1.4.1.21939.9.2.2.1.8.x	Effectively negotiated duplex: –half (0) –full (1)	
duplexmode 1.3.6.1.4.1.21939.9.2.2.1.9.x	Mode of duplex: –manual (0) –auto (1)	Sets the mode of the duplex
adaptProgress 1.3.6.1.4.1.21939.9.2.2.1.10.x	Progress of the adapt DSL speed negotiation	
connectProgress 1.3.6.1.4.1.21939.9.2.2.1.11.x	Progress of the DSL speed negotiation	
signalQuality 1.3.6.1.4.1.21939.9.2.2.1.12.x	Signal quality in dB	
resetCounter 1.3.6.1.4.1.21939.9.2.2.1.13.x	Reset counter for subsystem	
lineLossRatio 1.3.6.1.4.1.21939.9.2.2.1.14.x	Line loss in dB	

Table 49: Objects of the group abb->abbMgmt->interface->ifTable (table index - ifIndex)

Object name	Read object	Write object
<b>OID</b>		
sfpModule	ASCII text: name of the SFP module	
1.3.6.1.4.1.21939.9.2.2.1.15.x		
sfpTemperature	Temperature of the SFP module	
1.3.6.1.4.1.21939.9.2.2.1.16.x		

Table 49: Objects of the group abb->abbMgmt->interface->ifTable (table index - ifIndex)

Object name	Read object	Write object
<b>OID</b>		
systemAlarmLevel	System-wide alarm state:	
1.3.6.1.4.1.21939.9.3.1.0	-levelNone (0)	
	-levelWarning (1)	
	-levelError (2)	

Table 50: Objects of the group abb-&gt;abbMgmt-&gt;alarm

Object name	Read object	Write object
<b>OID</b>		
activeAlarmReason	ASCII text: Alarm message	
1.3.6.1.4.1.21939.9.3.2.1.3.x.y		
activeAlarmLevel	Severity of the alarm	
1.3.6.1.4.1.21939.9.3.2.1.4.x.y	-levelNone (0)	
	-levelWarning (1)	
	-levelError (2)	
activeAlarmTimestamp	System Uptime when the alarm occurred	
1.3.6.1.4.1.21939.9.3.2.1.5.x.y		

Table 51: Objects of the group abb-&gt;abbMgmt-&gt;alarm-&gt;activeAlarmsTable (table index - ifIndex.alarmId)

Object name	Read object	Write object
<b>OID</b>		
enabledAlarmReason	ASCII text: Alarm message	
1.3.6.1.4.1.21939.9.3.3.1.3.x.y		
enabledAlarmLevel	Severity of the possible alarm	
1.3.6.1.4.1.21939.9.3.3.1.4.x.y	-levelNone (0)	
	-levelWarning (1)	

Table 52: Objects of the group abb-&gt;abbMgmt-&gt;alarm-&gt;enabledAlarmstable (table index - ifIndex.alarmId)

Object name	Read object	Write object
<b>OID</b>		
	-levelError (2)	

Table 52: Objects of the group abb->abbMgmt->alarm->enabledAlarmstable (table index - ifIndex.alarmId)

Object name	Read object	Write object
<b>OID</b>		
timeRegistered 1.3.6.1.4.1.21939.9.9.1.1.2.a. b.c.d	System Uptime at the time of first login	
timeLeftToExpire 1.3.6.1.4.1.21939.9.9.1.1.3.a. b.c.d	Number of seconds before manager will be discarded	Login and refresh of the manager: Number of seconds but maximum 3600
mgrVersion 1.3.6.1.4.1.21939.9.9.1.1.4.a. b.c.d	freely assignable 32 bit version field	sets a freely assignable 32 bit version field
sendSnmpNotification 1.3.6.1.4.1.21939.9.9.1.1.7.a. b.c.d	Manager receives traps: -no (0) -send (1)	Sets the preferred Manager setting for traps
snmpNotificationPort 1.3.6.1.4.1.21939.9.9.1.1.8.a. b.c.d	UDP port for SNMP traps	Sets the UDP port for SNMP traps  Default value: 162
sendSyslogSeverity 1.3.6.1.4.1.21939.9.9.1.1.9.a. b.c.d	Bits 0-2: minimum severity for Syslog messages	Sets the minimum severity for Syslog messages (bits 0-2). Bit 3 activates the sending of Syslog.
syslogPort 1.3.6.1.4.1.21939.9.9.1.1.10.a. .b.c.d	UDP port for Syslog messages	Sets the UDP port for Syslog messages
sysUpTime 1.3.6.1.4.1.21939.9.9.1.1.11.a. .b.c.d	Convenience object: return the System Uptime (like MIB-2 sys- UpTime)	ignored

Table 53: Objects of the group abb->abbMgmt->mgr->mgrTable (table index - ip)

Object name	Read object	Write object
<b>OID</b>		
tcpReceiveIdle 1.3.6.1.4.1.21939.9.10.3.1.6.a .b.c.d.x.e.f.g.h.y	TCP inactivity in 100 ms	

Table 54: Objects of the group abb->abbMgmt->tcpExt->tcpTable (table index - tcpLocalIp.tcpLocalPort.tcpRemoteIp-tcpRemotePort).

ifIndex	Name
1	fastethernet0
2	dsl1
3	dsl2
4	system0
5	port1
6	port2
7	port3
8	port4
9	fiberoptics1
10	fiberoptics2
11	channel0
12	console0
13	console1
14	tunnel0
15	backup-group1

Table 55: ifIndex

alarmId	Name
1	speedMismatch
2	linkDown
3	linkUp
4	temperature
5	systemBoot
6	duplexMismatch
7	aggregationMismatch
8	sqThresholdWarning
9	sqThresholdError
10	sshNotReady
11	sfpNotInserted
12	internalSwitchUplinkDown
13	dslEncapsulationMismatch
14	internalSwitchInterconnectDown
15	ethernetRemoteFault
16	monitorUp
17	monitorDown

Table 56: alarmID

### 2.27.4 Trap Server and Traps

For the report of spontaneous events EDS500 devices support SNMP trap messages. Traps can be sent in the SNMPv1 format or SNMPv2c format, depending on the settings. The traps are sent to the configured trap server as well as to logged in network management systems (ABB-EDS500-MIB Group 'mgr', refer to Chapter 2.27.3, "Vendor Specific Device MIB" ). Up to 10 different trap target IP addresses can be defined.

The default value for Community-String is: public.

Command to configure SNMP Trap servers

```
<set system snmp trap-target {IP address} [{v1|v2c}]
[{community}]]>
<clear system snmp trap-target {IP address}>
<show system snmp>
```

Trap name	Description	SNMPv1	SNMPv2c
coldStart	Reports a cold start of the device, delayed by 2 minutes	Generic Trap ID: coldStart (0)	Trap OID: 1.3.6.1.6.3.1.1.5.1
warmStart	Reports a warm start of the device, delayed by 2 minutes	Generic Trap ID: warmStart (1)	Trap OID: 1.3.6.1.6.3.1.1.5.2
linkDown	Reports a loss of link. Included objects: ifIndex, ifAdminSta- tus, ifOperStatus	Generic Trap ID: linkDown (2)	Trap OID: 1.3.6.1.6.3.1.1.5.3
linkUp	Reports the establish- ing of a link. Included objects: ifIndex, ifAdminSta- tus, ifOperStatus	Generic Trap ID: linkUp (3)	Trap OID: 1.3.6.1.6.3.1.1.5.4
newRoot	Reports that this device has become 'root' in a spanning tree.	Generic Trap ID: spe- cific (6) Specific Trap ID: 1 Enterprise OID: 1.3.6.1.2.1.17	Trap OID: 1.3.6.1.2.1.17.0.1
topologyChange	Reports that for this device a change in the spanning tree topol- ogy has occurred.	Generic Trap ID: spe- cific (6) Specific Trap ID: 2 Enterprise OID: 1.3.6.1.2.1.17	Trap OID: 1.3.6.1.2.1.17.0.2
systemOvertemp- Warning	Reports an overtem- perature alarm. Included object: actu- alTemperature	Generic Trap ID: spe- cific (6) Specific Trap ID: 1 Enterprise OID: 1.3.6.1.4.1.21939	Trap OID: 1.3.6.1.4.1.21939.0.1
activeAlarmsChanged	Reports a change in the system's alarm state Included object: systemAlarmLevel	Generic Trap ID: spe- cific (6) Specific Trap ID: 2 Enterprise OID: 1.3.6.1.4.1.21939	Trap OID: 1.3.6.1.4.1.21939.0.2

Table 57: Trap messages of EDS500 devices

## 2.28 Time Synchronization with SNTP

EDS500 devices can synchronize date and time with a time server via the Simple Network Time Protocol. This time information is used in Syslog messages and the internal log (command `<show log>`).

The SNTP time can be used in timestamps by the telecontrol protocol IEC 60870-5-104.

After a synchronization the up-to-date time is displayed in the system overview (command `<show system>`). If the time zone is set to `cet-cest` then winter and summer time are toggled automatically; otherwise the displayed time is always winter time. Time is synchronized with the server every 24 hours.

The default value for time zone is: `cet`.

Time zone	Name	Comment
<code>gmt</code>	Greenwich Mean Time	UTC +0
<code>cet</code>	Central European Time	UTC +1 (Default value)
<code>cet-cest</code>	Central European Summer Time	UTC +1 / UTC +2 (automatic switch)
<code>eet</code>	Eastern European Time	UTC +2
<code>hkt</code>	Hong Kong Time	UTC +8

Table 58: Time zones

If the synchronization with the time server should fail, a new attempt is started every minute.

The default value for all further synchronizations with the time server after the first successful synchronization is: 24 hrs.

The interval between two synchronizations can be set by a command.

### Commands for SNTP

```
<set system sntp server {IP address}>
<clear system sntp server {IP address}>
<set system sntp timezone cet>
<set system sntp interval {60-86400}>
<show system sntp>
<debug system sntp sync>
```

## 2.29 Monitor

The EDS500 devices support the monitoring of an IP address or IP route in respect to reachability and existence. This can be achieved by the configuration of a so-called monitor that can also be used to control the interfaces (Chapter 2.31, "IP Routing").

The IP address is periodically checked with an ICMP echo request (ping). If three successive requests fail then the state of the monitor changes to not available. The first successful reply rates the address as available again.

The monitor can also be used for the checking of a route the existence. Dynamic Montes are usually handed by a routing protocol like RIP (refer to Chapter 2.31, "IP Routing")

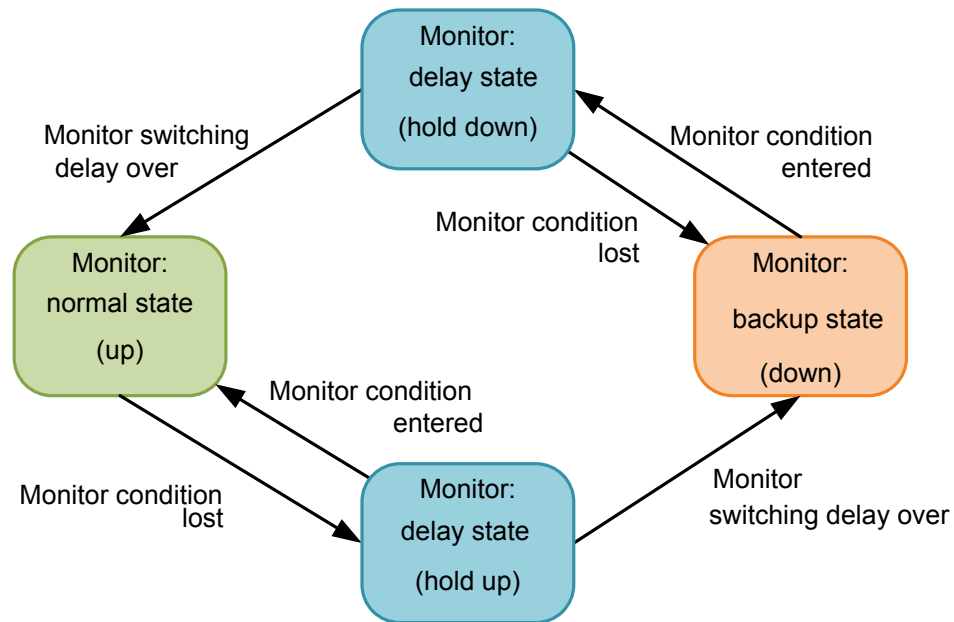


Figure 29: State transitions of the monitor

Commands for the monitor:

```

<set monitor enable>
<set monitor no enable>
<set monitor target-ip {IP address}>
<set monitor ip-route {IP address} {subnet mask} {next hop}
{metric}>
<set monitor interval {100-60000}>
<set monitor switching-delay {1-300}>
<set monitor alarm-if-down>
<set monitor no alarm-if-down>
<set monitor alarm-if-up>
<set monitor no alarm-if-up>
<show monitor>

```

## 2.30 State Dependencies

EDS500 devices offer the option to bind certain settings to certain conditions, e.g. the link state of another interface (Link Fault Pass-Through, LFPT) or to a monitor (refer to Chapter 2.29, "Monitor"). Further settings for dependencies deal with the selection of the source VLAN for system services and serial tunnelling.

Commands to configure state dependencies

```

<set switch {port1 | port2 | port3 | port4} dependency
{channel0 | ds11 | ds12 | inverse-monitor | monitor | none}>
<set interface {console0 | console1} transmission dependency
{inversemonitor | monitor | none}>
<set interface console source vlan {1-4094} [dependency
{inverse-monitor | monitor}]]>
<clear interface console source vlan [{1-4094}]]>
<set system radius source vlan {1-4094} [dependency
{inverse-monitor | monitor}]]>
<clear system radius source vlan [{1-4094}]]>
<set system snmp trap-source vlan {1-4094} [dependency

```

```
{inverse-monitor | monitor}}]>
<clear system snmp trap-source vlan [{1-4094}]]>
<set system snmp source vlan {1-4094} [dependency {inverse-
monitor | monitor}}]>
<clear system snmp source vlan [{1-4094}]]>
<set system syslog source vlan {1-4094} [dependency
{inverse-monitor | monitor}}]>
<clear system syslog source vlan [{1-4094}]]>
```

## 2.31 IP Routing

EDS500 can be operated as IP router.

EDS500 devices support static and dynamic routing.

### 2.31.1 Routing with VLAN Interfaces

VLAN IP addresses have to be configured to use routing, refer to Chapter 2.9.3, "Configuration of VLAN IP Addresses".

Routing has to be activated for all VLAN interfaces that participate in routing. Routing takes place only between those VLANs that have enabled the routing property (<set interface vlan {...} [no] routing>). There is no routing to or from VLAN interfaces that do not have this property. These can only be reached in their own VLAN.

---

#### Display of IP address overview

---

```
<show interface ip-address>
```

Interface Summary:

Interface	IP Address	IP Gateway	Admin State	Link State
vlan 10	10.0.0.11/ 8	-	up	up
vlan 20	20.0.0.10/29	-	up	down

---

Commands to configure routing with VLAN interfaces

```
<set interface vlan {1-4094} routing>
<set interface vlan {1-4094} no routing>
<set interface vlan {1-4094} ip-address [{IP address} [{IP
address range end}] {subnet mask}] | {unnumbered vlan {vlan-
id}}]>
<clear interface vlan {1-4096} ip-address [{IP address}]]>
<show interface ip-address>
```

### 2.31.2 Routing Table and Routes

The routing table of the system can be displayed to show the current state of the IP routing.

The routing table shows the following:

- entries for static routing,
- entries for dynamic routing that are added via the routing protocol,
- local default gateways, if present.

---

#### Display of routing table

---

```
<show ip route>
```



**Display of routing table**

Routing List Entries: 3 entries (static local gateways excluded)

Id	Dest. IP	Met	TTL	Next Hop	Interface	Protocol
-	0.0.0.0/ 0	-	-	10.0.0.1	sys0	Local
1	10.0.0.0/ 8	1	180	-	sys0	Local
2	20.0.0.0/ 8	1	180	-	vlan 10	Local
3	30.0.0.0/ 8	1	180	-	vlan 20	Local

Static routes can be configured with a command while stating target IP address, Subnet mask, next router IP address, Metric and are added permanently to the routing table.

Preconditions are:

- The target network is not identical with the local network
- The next-hop-address is included in the address range of the local network
- Metric, if mentioned at all has a value between 1 and max. Diameter (the typical maximum value is Diameter 16)

Commands for the routing table and routes

```
<set ip route {IP address} {subnet mask} {next hop}
[{metric}]>
<clear ip route {IP address}>
<clear ip dynamic-routes>
<set interface vlan {1-4094} rip metric-offset {0-255}>
<set router auto-summarization {advanced | normal | off}>
<show ip route>
```

### 2.31.3 Configure Routing Protocol RIP

The Routing Information Protocol (RIP) is a distance vector routing protocol that automatically synchronizes the routing tables of connected routers.

EDS500 devices support RIP in the versions 1 and 2 including split horizon and triggered updates.

Default configuration:

The default value for RIP is: no rip.

**Example for show router rip**

```
RIP routing protocol is enabled on this router.
Maximum network diameter configured is 15 hops.
Time to live (TTL) for route entries: 180 seconds
Hold down time for removed entries: 120 seconds
Update interval (advertisements) 30 seconds
Incoming RIP version(s) accepted: 2
Authentication is disabled.
```

Commands for RIP

```
<set router [no] rip>
<set router rip [no] accept-v1>
<set router rip authentication-key {password}>
<set router rip no authentication-key>
<set router rip max-diameter {0-254}>
<set router rip time-to-live {1-65535}>
<show router rip>
```

## 2.32 Virtual Router Redundancy Protocol (VRRP)

The Virtual Router Redundancy Protocol (VRRP) serves the fail safeguarding of gateways by using redundant routers.

Failures in routed Layer-2 networks can be countered with redundant connections and dynamic routing protocols.

The Spanning tree protocol offers this function in Layer-2 networks. In general only a single standard gateway can be found at the changeover from Layer-2-subnetworks to Layer-3-networks.

The gateways can be set-up redundantly when using VRRP by grouping several physical routers to one logical router.

This logical router uses a virtual MAC address and a virtual IP address that is transferred in no more than three seconds from the master router to the backup router (hot standby) in case of an error.

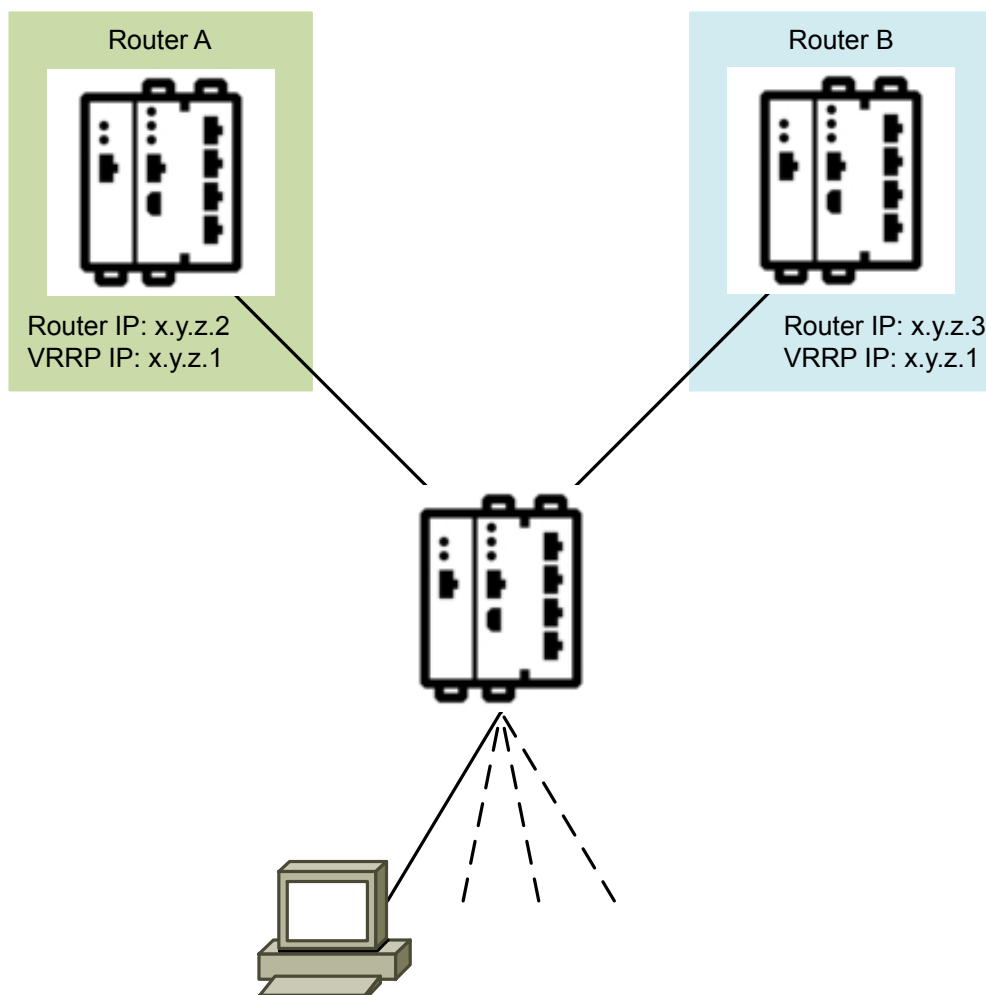


Figure 30: VRRP with EDS500 devices

EDS500 devices support VRRP if they are operated as router (refer to Chapter 2.31, "IP Routing"). For this the gateway IP address is configured as VRRP address for the IP subnetwork that shall contain a redundant gateway.

This VRRP IP address as well as the VRRP-ID (1 to 255) have to be identical on all grouped routers. Furthermore, an individual VRRP priority can be configured per router (1 to 255) where the router with the highest VRRP priority becomes master router.

Finally, VRRP has to be activated on the specified interface.

Commands to configure VRRP

```
<set interface vlan {1-4094} vrrp [no] shutdown>
<set interface vlan {1-4094} vrrp id {1-255}>
<set interface vlan {1-4094} vrrp ip {IP address}>
<set interface vlan {1-4094} vrrp priority {1-255}>
<set interface vlan {1-4094} vrrp priority master>
<clear interface vlan {1-4094} vrrp id>
<clear interface vlan {1-4094} vrrp ip>
<clear interface vlan {1-4094} vrrp priority>
<show vrrp>
```

## 2.33 LLDP Neighbour Recognition

EDS500 devices support the protocol LLDP (IEEE 802.1AB, Link Layer Discovery Protocol) for neighbour detection. If the protocol is also supported by the neighbouring devices then the information like device name, port name and management addresses are exchanged. This information can be displayed and controlled with the following commands and can be used to catalogue the topology and detect faulty configurations. The information can also be queried via the SNMP LLDP-MIB.

Commands for LLDP

```
<show neighbor>
<show neighbor summary>
<show neighbor>
<show cdp neighbor>
<set system lldp enable>
<set system lldp no enable>
```

## 2.34 Firmware Update

The firmware is updated by transferring a firmware image to the device. It can be downloaded with the help of the command line (Telnet, SSH, serial terminal) as well as with the help of the integrated web interface, scripts or a management program. It is mandatory that there is an IP connection to the device.

### ADVICE

During a firmware update the power supply must not be interrupted or a reboot must not be triggered as this could leave the device in an inoperable state.

### 2.34.1 Update via Command Line Interface (CLI)

- 1 Enter <enable> and if required the password.
- 2 Enter <copy tftp flash> and when asked, the IP address of the TFTP servers and the name of the image file.
- 3 Reboot of the device with the command <reload>.

---

**Example for updating firmware**


---

```

switch>enable
<enable>
Enter Password: switch#copy tftp flash
<copy tftp flash>
Copy firmware from TFTP-Server to flash.
Enter TFTP Server IP: 10.0.0.100
Enter Filename: sr-0.26.4.bin
!!!!!!!!!!!!!!!!!!!!!!
Transmission complete [ 320512 bytes ok]
Erasing flash... complete
Programming image.
!!!!!!!!!!!!!!!!!!!!!!
Firmware upgrade complete. Reboot to load the new firmware.
<reload>
Reload initiated, please wait...
Performing self-test: [...]

```

---

After a reboot the system has loaded the new software.

### 2.34.2 Update via Web Interface

The page for firmware update can be reached with the link "Firmware" in the navigation bar. JavaScript has to be activated in the browser to use the update function. The web interface offers two ways to update the firmware:

Upload directly in the browser

- Select the firmware image on the local computer.
- Click on the "Upgrade" to start the process.

Upload with the help of a TFTP server

- 1 Enter:
  - the IP address of the TFTP server.
  - the name of the firmware image.
  - Click on the "Upgrade" to start the process.
- 2 Either click on "Reload" to start the updated firmware immediately.
- 3 Or carry out the new start of the device at a later time.

### 2.34.3 Update via a Management Program or a Script

The interfaces and protocols of an EDS500 device (SNMP / HTTP / TFTP / Telnet / SSH) can be used for a firmware update with a management or automatic processing with scripts. Follow the respective commands of the employed program to update the firmware.

## 2.35 Cryptographic Key

### 2.35.1 Device Specific Cryptographic Key

EDS500 devices need an individual key to encode/decode cryptographically encoded protocols tap-proof. On shipping a unique key is already present. It can be replaced at any time.

**ADVICE**

Devices that have been shipped with a software version without SSH support (SWOPS < 1.33.0), have no individual cryptographic key but use a standard value as key. An individual key has to be applied for security reasons when cryptographic protocols are used. Such devices can be detected during boot or login or by the output of the command <show system ssh> at the message

Warning: SSH server is using the default host key.

**ADVICE**

In order to establish encrypted connections so-called crypto sessions get pre-calculated to reduce the time for establishing a connection. If there are no crypto sessions in the device then encrypted connections can only be established after at least one crypto session has been calculated. This status can be monitored with an alarm with the commands <set system ssh alarm-if-notready> and <set system ssh warn-if-notready>.

### 2.35.2 Generate and Apply Cryptographic Key

The program PuTTYgen can be used to create a cryptographic key. PuTTYgen is part of the Open Source Terminal Emulator Suite PuTTY and can be obtained from the project homepage <http://www.chiark.greenend.org.uk/~sgtatham/putty/>. The file can be executed directly without installation.

A graphical user interface is shown when starting PuTTYgen to generate the key.

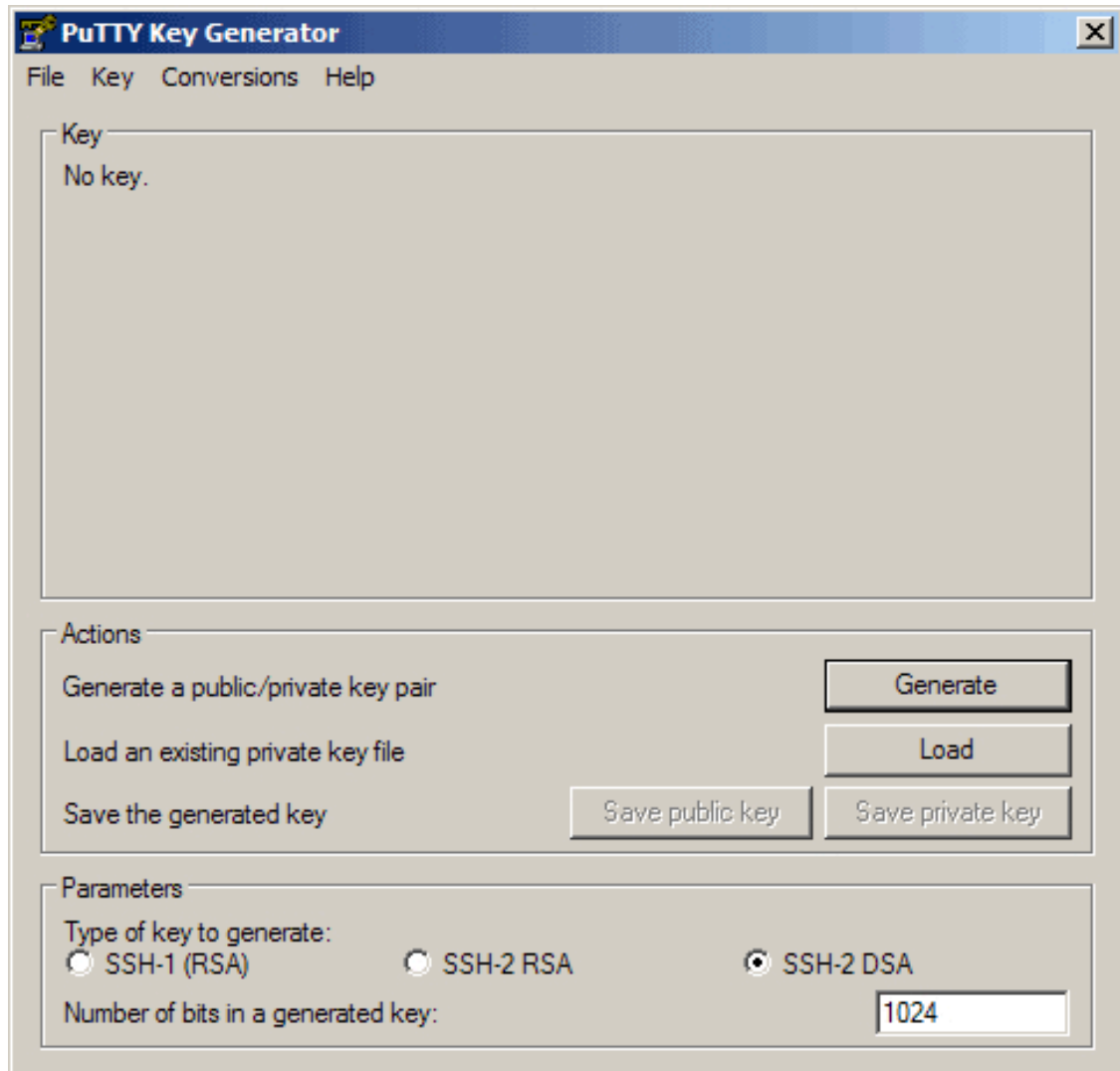


Figure 31: PuTTY Key Generator - key selection

The parameter of the key type has to be set SSH2-DSA (refer to "Fig. 31: PuTTY Key Generator - key selection"). The required key size is 1024.

Clicking on button "Generate" and moving the mouse over the plane "key" generates the key. A process bar gives visual feedback. After some time the key is calculated and can be saved (refer to "Fig. 32: PuTTY Key Generator - generated key"). Do not set a password, leave empty the field "key passphrase", ignore later subsequent related warnings. The comment field "Key comment" also has to be empty.

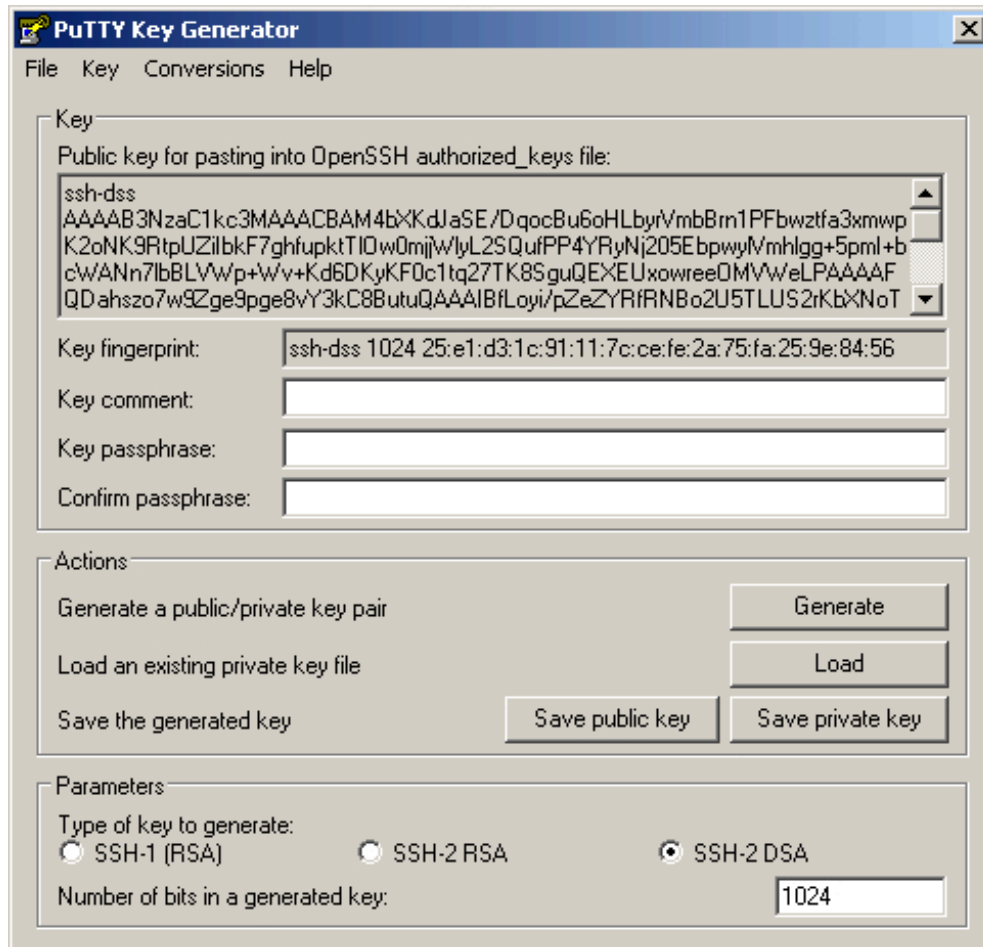


Figure 32: PuTTY Key Generator - generated key

Next, the key has to be exported in the OpenSSH format. Do this with the function "Conversions". The action "Export OpenSSH key" saves the key file ("Fig. 33: PuTTY Key Generator - key export").

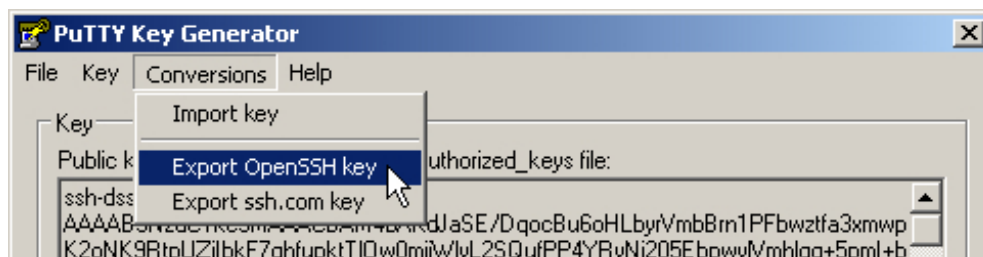


Figure 33: PuTTY Key Generator - key export

The generated file has to be transmitted to the device for application. You can do this either with the web interface and the menu item "System" (refer to Chapter 2.5, "Handling in the Web Interface") by transferring the file directly in the web browser or by using a TFTP server or with the command line interface (CLI) and the use of a TFTP server.

Commands to apply the key

```
<copy tftp cryptokey>
```

## 2.36 Certificate Management

For secure webserver (HTTPS) functionality the EDS500 managed switches requires a compatible combination of EC key (Eliptic Curve key) and certificate.

In delivery state each EDS500 managed switches has stored its EC key (device key) and its certificate (device certificate - self-signed) generated from the EC key. This combination is valid and can be used for the HTTPS functionality.

The usage of the devices' EC key and the devices' certificate (self-signed) is the easiest way for a HTTPS connection. However, the certificate of each individual device must be downloaded and integrated into the browser. That can be very complex when managing a large number of browsers and workstations.

The EC key and certificate can also be generated externally and loaded onto the device. This enables the use of customer generated keys (external key) and/or certificates (external certificates).

Every combination of device and external keys and certificates have their advantages.

- Device EC key and device certificate (default state)
- Device EC key and external certificate (CSR)
- External EC key and device certificate
- External EC key and external certificate (CSR or external generated)

The latter combination allows two possibilities. The following chapter describes the combinations and list.

Generally it should be noted that the activation of certificates takes place directly after the upload via the web interface. A restart of the device is not necessary.

### 2.36.1 Host Key Type

The EDS500 managed switches supports only EC (Elliptic curve) keys.

This key is standarized by the name:

- Secp256r1 (SEC 2)
- prime256v1 (X9.62/SECG)
- NIST P-256 (NIST)

The key length has to be 256 bit.

### 2.36.2 Combination of Key and Certificate

From a technical point of view, the device allows five different ways of using or generating keys and certificates. Depending on requirements of cyber security and the operating comfort, the following options are available.



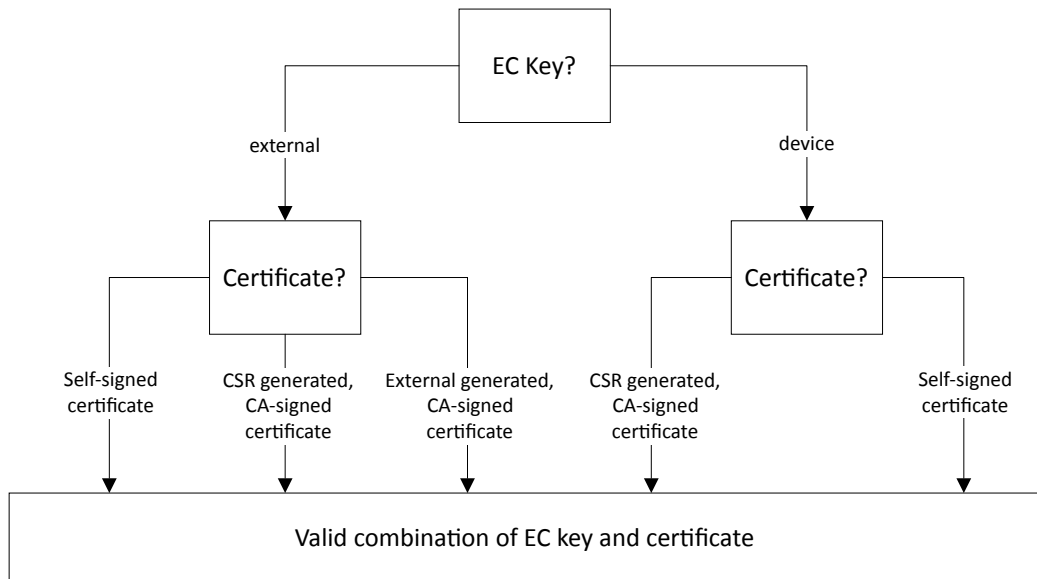


Figure 34: Key and certificate combination

**EC key**

The first decision is if the preinstalled key on the device or an external key shall be used. This decision usually depends on the guidelines of the companies. The key pre-installed in the device complies with ABB's minimum cyber security requirements. According to this, the key is unique and the private part is not read out. However, some companies need to use their own keys and this is supported by the EDS500 managed switches. How to upload keys to the device is described in the next chapter.

At this point it should be mentioned that the key, especially the private part, must never be transmitted over an insecure connection. This should also be avoided over supposedly secure connections.

**ADVICE**

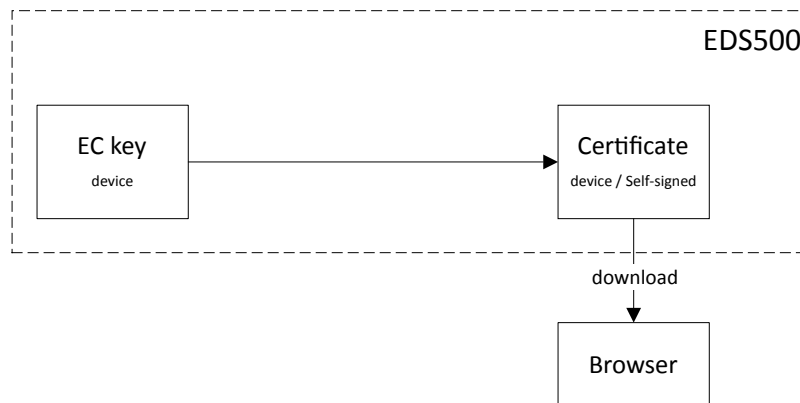
Private keys must be protected against access by third parties under all circumstances.

The device EC key is not deleted when using an external EC key. It remains in the device, but is inactive.

**Certificate**

Certificates can be generated in the device based on the current EC Key. As soon as the device has a valid EC key (external or device), it automatically generates a valid certificate (self-signed). This certificate can be downloaded and added to the used browser.

## a) Use default key and self-signed certificate of device



## b) Use external EC key and self-signed function of device.

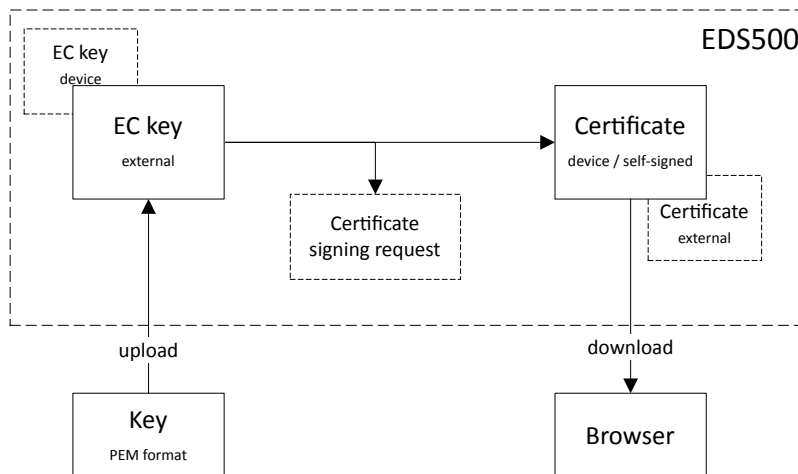


Figure 35: Device key (a) or external key (b) with self-signed certificates

The certificates generated in this way are device-specific. This means that this certificate is only valid for this device and not for other EDS500 managed switches. If several EDS500 managed switches are used, all certificates must be downloaded from the devices and integrated into the browser.

The trust in self-signed certificates is legitimated by the fact that they are signed directly by the device. However, for several reasons it may be necessary to use CA-signed certificates (e.g. security guideline, handling ...).

External certificates can be created in two ways: Via a certificate signing request (CSR) or via an external program (via external program only, if private key exists externally). In the case of the CSR method, a .csr file is downloaded from the device. This file is signed with a CA and results in a device-specific .crt file. This .crt file is the actual certificate and has to be uploaded to the device. It replaces the device certificate. In the case of the usage of an external program a .crt file can directly be generated from the EC key and a CA.

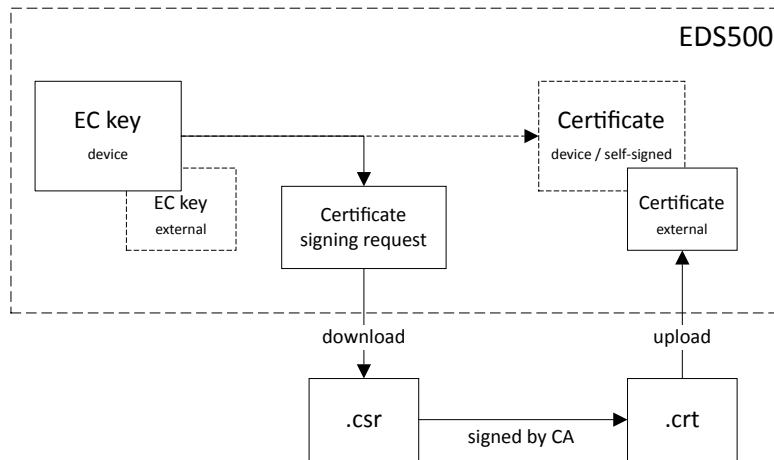
External certificates have the advantage that they not only trust themselves, they additionally trust all higher-level certificates (e.g. CA certificates). That gives you the possibility to establish a HTTPS connection to all EDS500 managed switches in a network with just one high-level certificate. The circumstance of integrating each individual certificate from all devices into the browser is eliminated.

CA certificates can be created by yourself as well as purchased from an authentication authority.

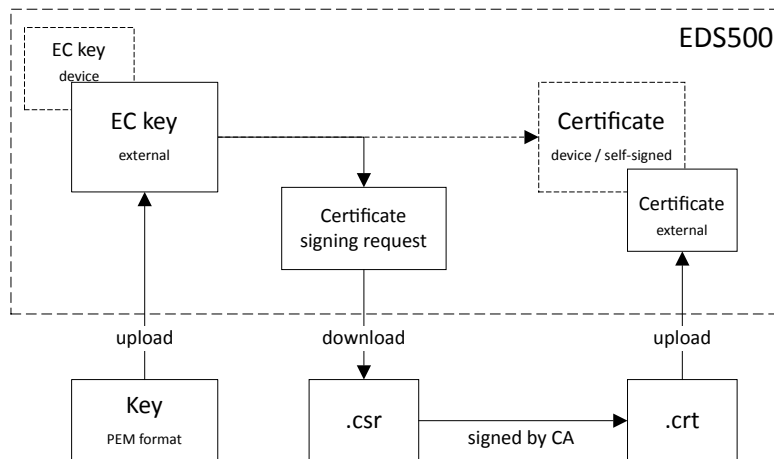
Combinations and their characteristics

- Device EC key and self-signed certificate
  - Default working
  - Out of the box
  - Each certificate must be integrated in the browser
- External EC key and self-signed certificate
  - Use of custom keys
  - Each certificate must be integrated in the browser
  - EC key upload is a security risk
- Device EC key and CA-signed certificate (CSR)
  - Browser needs only one high-level certificate
  - Automation possible
- External EC key and CA-signed certificate (CSR)
  - Browser needs only one high-level certificate
  - Time-consuming setup of the device
  - EC key upload is a security risk
- External EC key and CA-signed certificate (external generated)
  - Browser needs only one high-level certificate
  - EC key upload is a security risk
  - Compatibility of EC key and certificate is not guaranteed by the device.

## c) Device EC key, CSR and external CA-signed certificate.



## d) External EC key, CSR and external CA-signed certificate.



## e) External EC key and CA-signed certificate without CSR

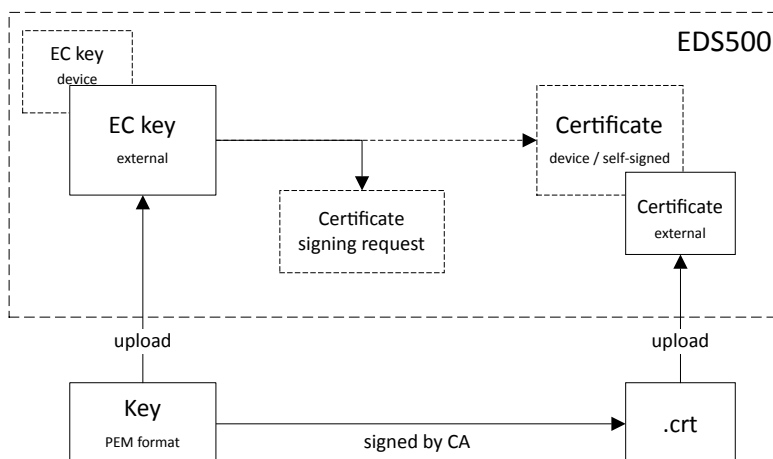


Figure 36: Device key (c), external key - CSR (d) or external key - non CSR with CA-signed certificates (e)

## 2.36.3 Step-by-Step Instructions

### OpenSSL

For certification OpenSSL can be used. In this manual a step-by-step instruction for the XCA tool is given. This tool is based on OpenSSL. It has a graphical user interface and works on Microsoft Windows workstations. An alternative is OpenSSL, which is controlled via command line interface. However, this is not covered in more detail in this manual.

### EDS500 web server

In the Web server menu, the link "Encryption" is the entry point for the certificate up- and download and the EC key upload. This link can be found under the menu item Administration. Due to the sensible information in the Crypto file up- and download the following notice has to be considered.

#### 2.36.3.1 XCA Tool

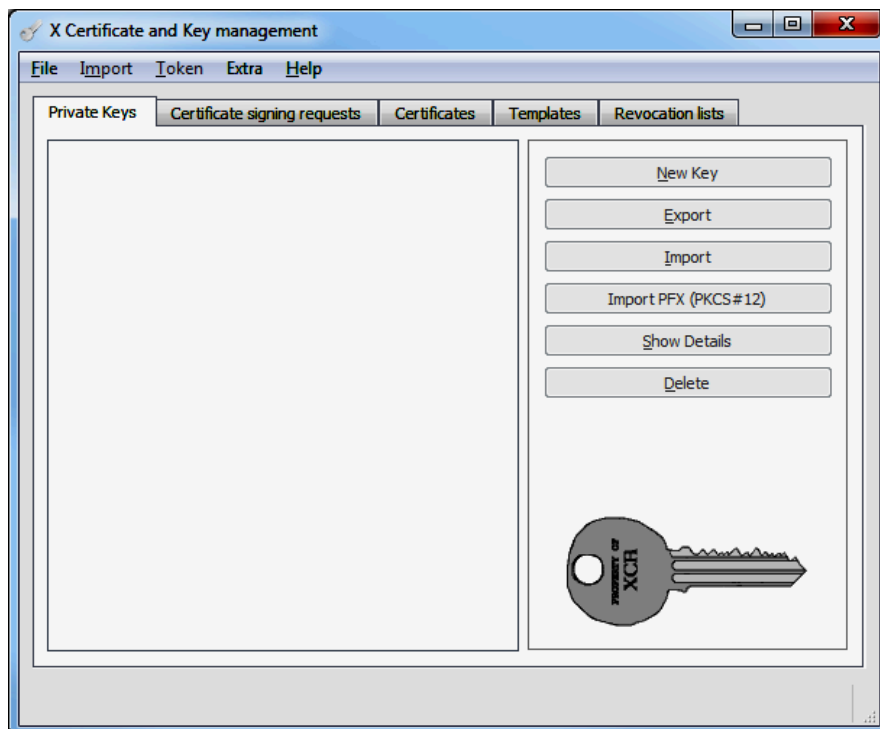
The XCA tool is a third party open source software (Copyright (C) Christian Hohnstaedt).

It is intended for creating and managing X.509 certificates, certificate requests, RSA, DSA and EC private keys, Smartcards and CRLs. The software can be downloaded under <https://hohnstaedt.de/xca/index.php/download>.

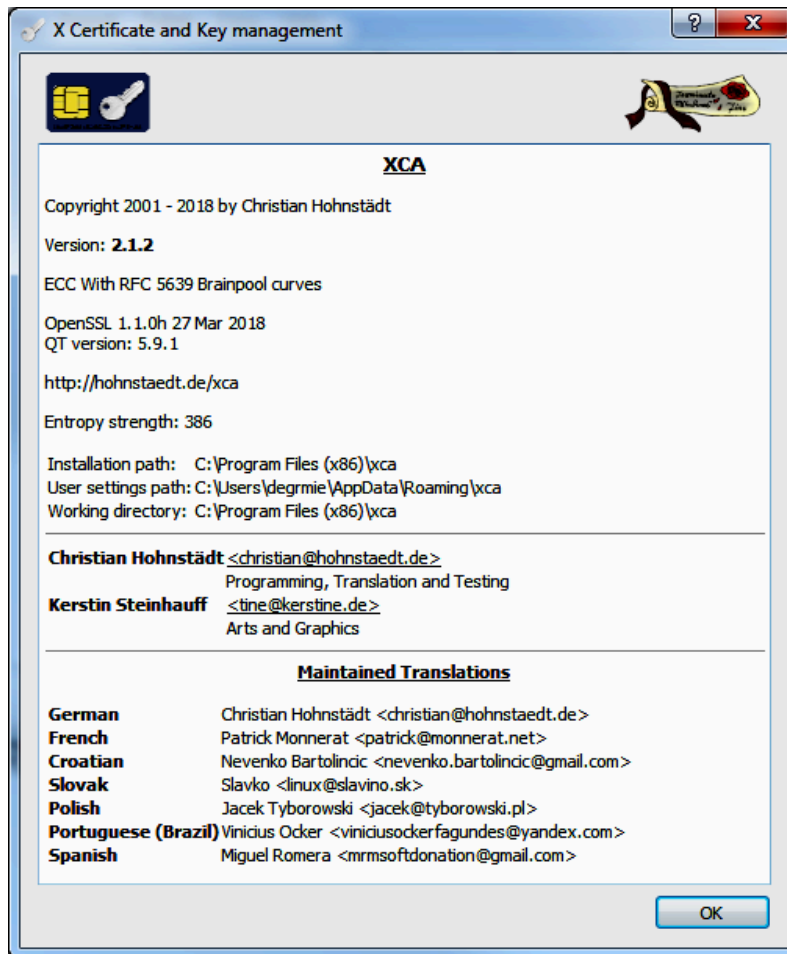
- 1 After download and installation use xca.exe shortcut to start XCA Tool.



- 2 The main window (certificate manager) opens.



3 In this example version 1.3.2 is used.

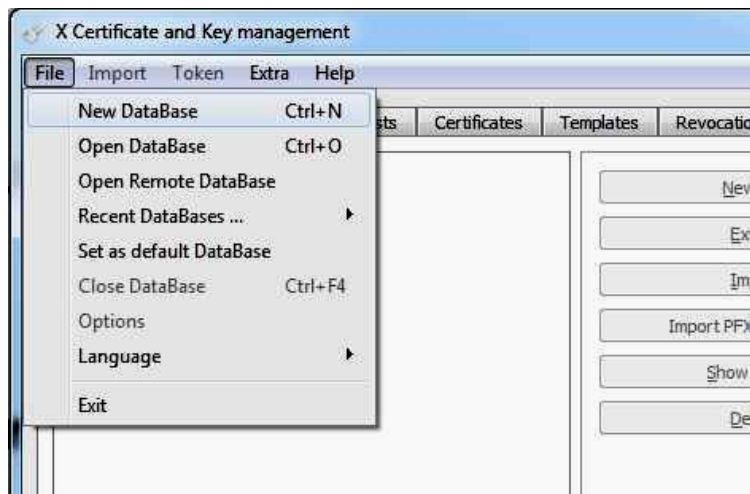


### 2.36.3.2 Generate CA Certificates

CA certificates can be purchased from an authentication authority as well as created by yourself. This chapter describes how to create a CA certificate yourself. CA certificates are mandatory for the use of non-self-signed certificates.

**Create new database**

- 1 First a data base has to be created.

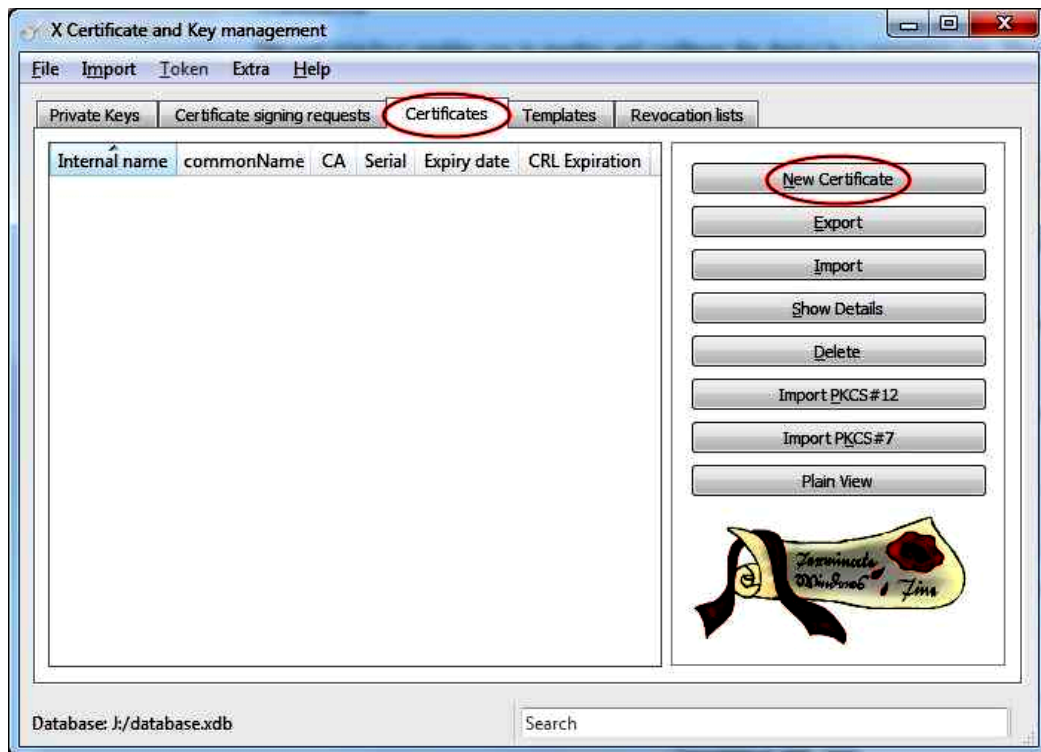


- 2 This data base is protected by password.

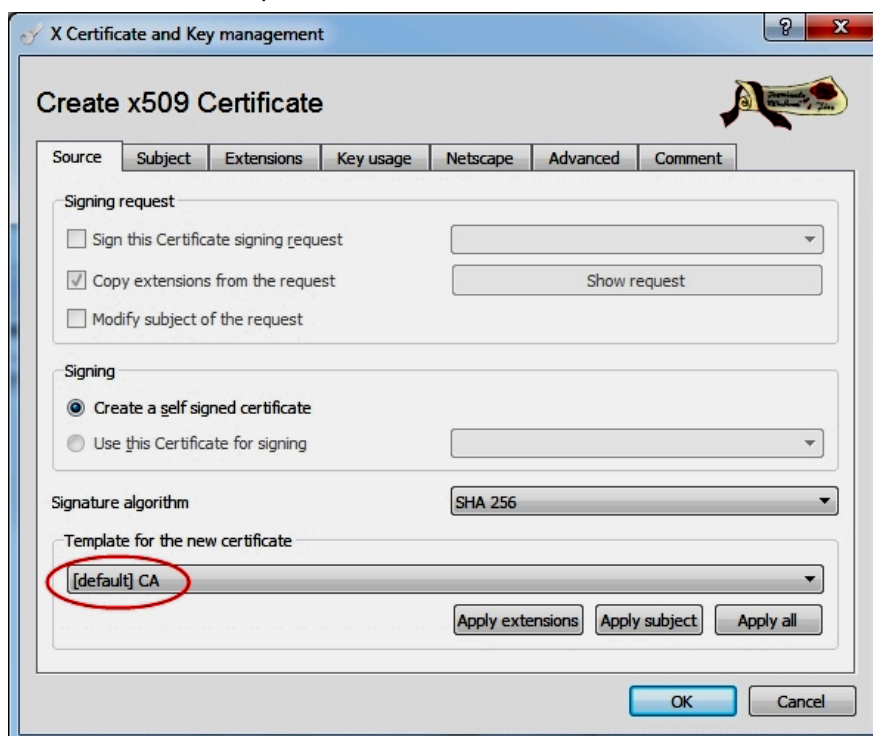


### Create new certificate

- 1 Go to Certificates and choose New Certificate



- 2 Set the Source like in picture. Select [default] CA.



- 3 To generate a CA certificate the tab Extensions has to be selected. Change Type to Certification Authority. In this tab validity period for this certificate can be defined.

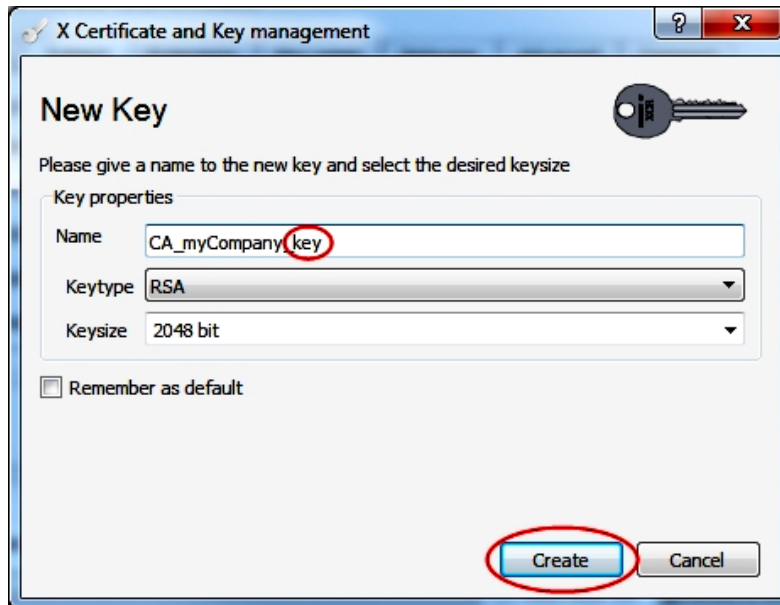


The screenshot shows the 'Create x509 Certificate' dialog box with the 'Extensions' tab selected. The 'X509v3 Basic Constraints' section has 'Type' set to 'Certification Authority' (circled in red). The 'Validity' section shows 'Not before' as '2019-05-03 12:17 GMT' and 'Not after' as '2020-05-03 12:17 GMT'. The 'Time range' section has an empty field (circled in red) and the 'Apply' button (circled in red). The 'Key identifier' section has 'Subject Key Identifier' and 'Authority Key Identifier' checkboxes. The 'X509v3 Subject Alternative Name', 'X509v3 Issuer Alternative Name', 'X509v3 CRL Distribution Points', and 'Authority Information Access' (set to 'OCSP') fields are also visible.

- 4 In tab Subject a Key for this certificate has to be generated.

The screenshot shows the 'Create x509 Certificate' dialog box with the 'Subject' tab selected. The 'Internal Name' field is set to 'CA\_myCompany\_cert' (circled in red). The 'Distinguished name' section has fields for 'countryName', 'stateOrProvinceName', 'localityName', 'organizationName', 'organizationalUnitName', and 'commonName' (set to 'CA\_myCompany\_cert', circled in red). The 'Private key' section has a dropdown menu and the 'Generate a new key' button (circled in red). The 'Add' and 'Delete' buttons are also visible.

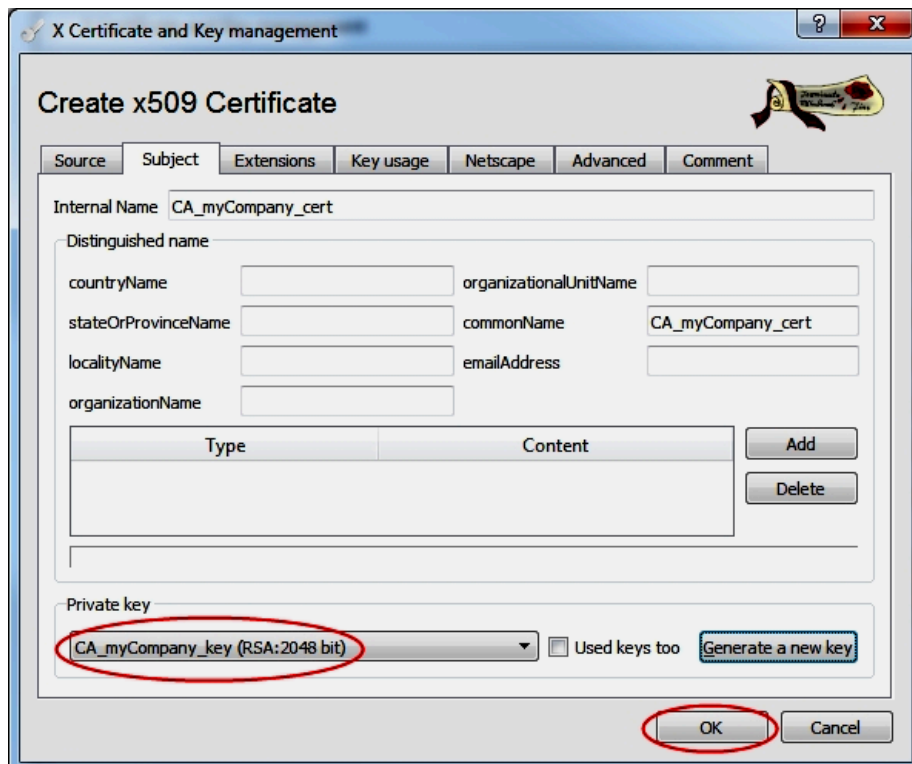
- 5 In this example we generate an RSA 2048 bit key.



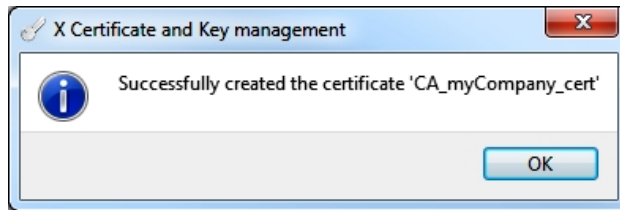
- 6 After creating the key you should get the following confirmation.



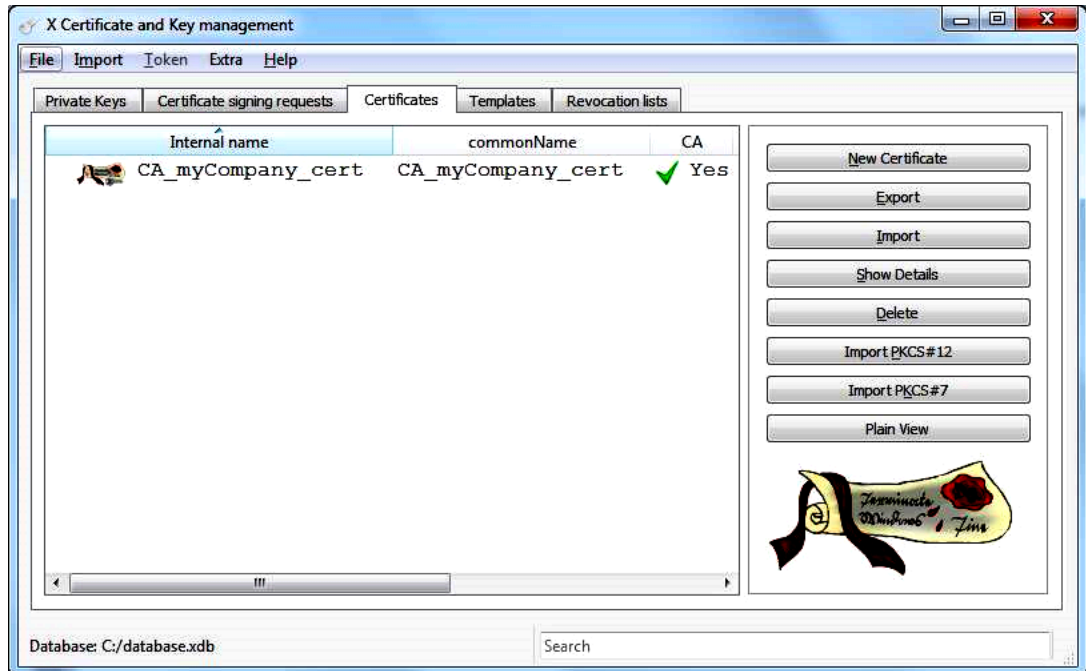
- 7 Switch back to the tab Subject and select the created key.



- 8 After clicking on OK you should get the following confirmation.



- 9 You should now see the certificate in tab Certificates. Important: The currently generated certificate have to be a CA certificate.

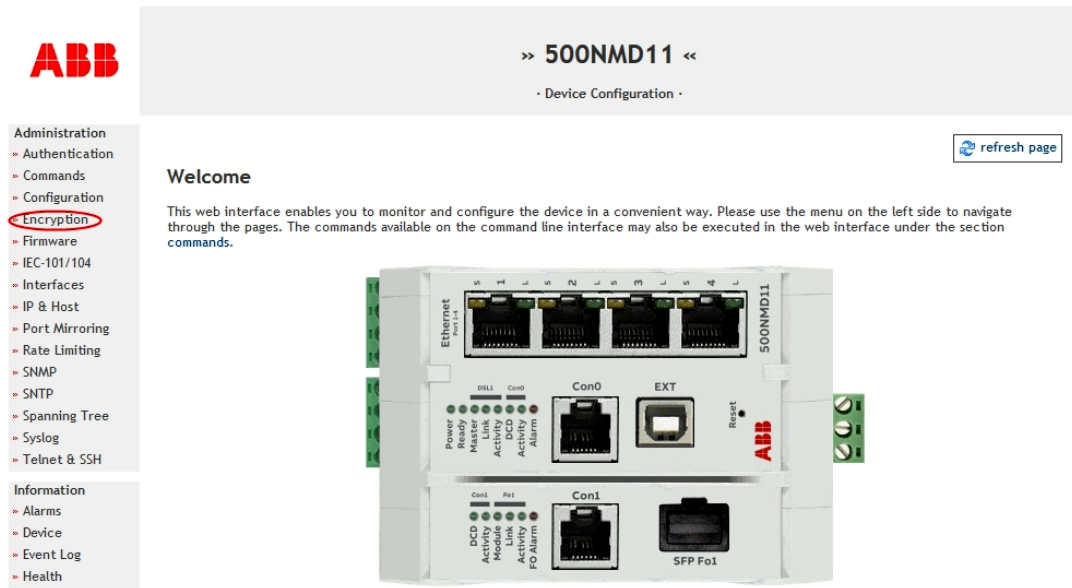


### 2.36.3.3 Generate External Certificates (CRT)

For using of external certificates the EDS500 managed switches provides CSR (Certificates Signing Request) function. This chapter describes how to use the CSR function.

#### Download CSR file

- 1 First of all, go to web server of the EDS500 managed switches and chose Encryption in the left Administration menu.



- 2 Scroll to the bottom of the page and download the Crypto certificate signing request web download.

**Certificate Signing Request**  
 The device may generate a PKCS #10 certificate signing request in order to apply for a certification by a Certification Authority (CA).  
 The resulting certificate may be re-uploaded to the device, for example to replace a self-signed device certificate.

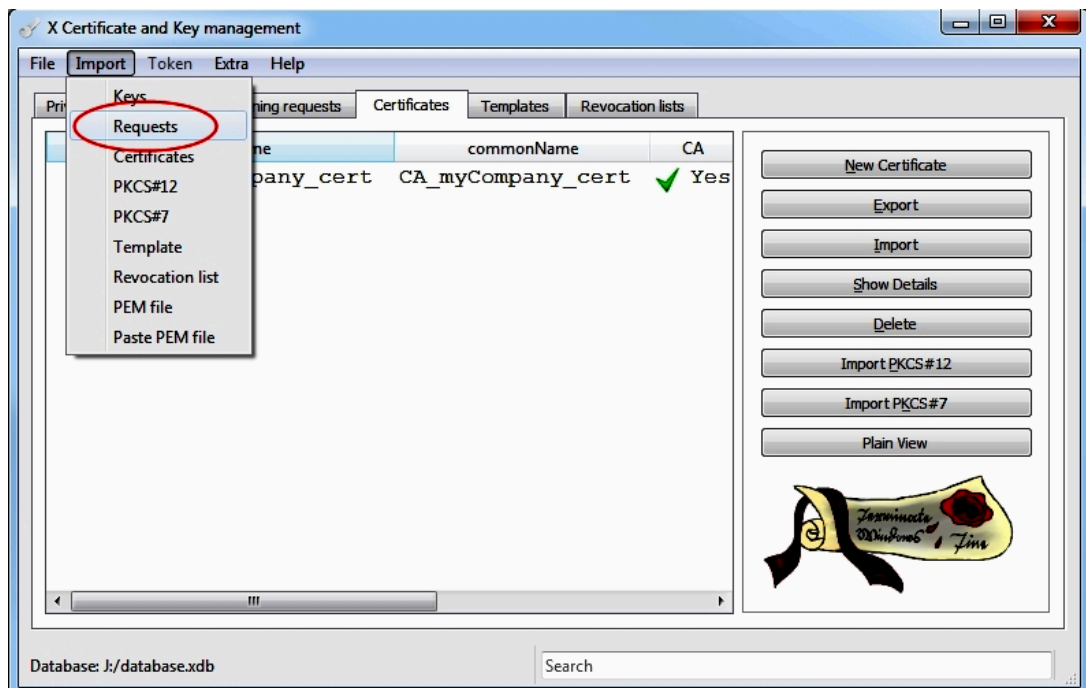
**Crypto certificate signing request TFTP download**  
 TFTP server IP:   
 CSR filename:

**Crypto certificate signing request web download**

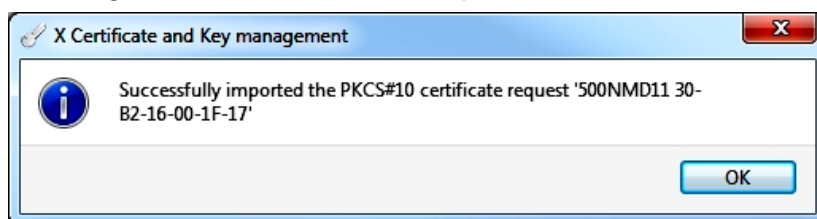
### Create CA-signed certificate

Start the XCA tool with the listed CA certificate (how this can be done is described in the previous chapter).

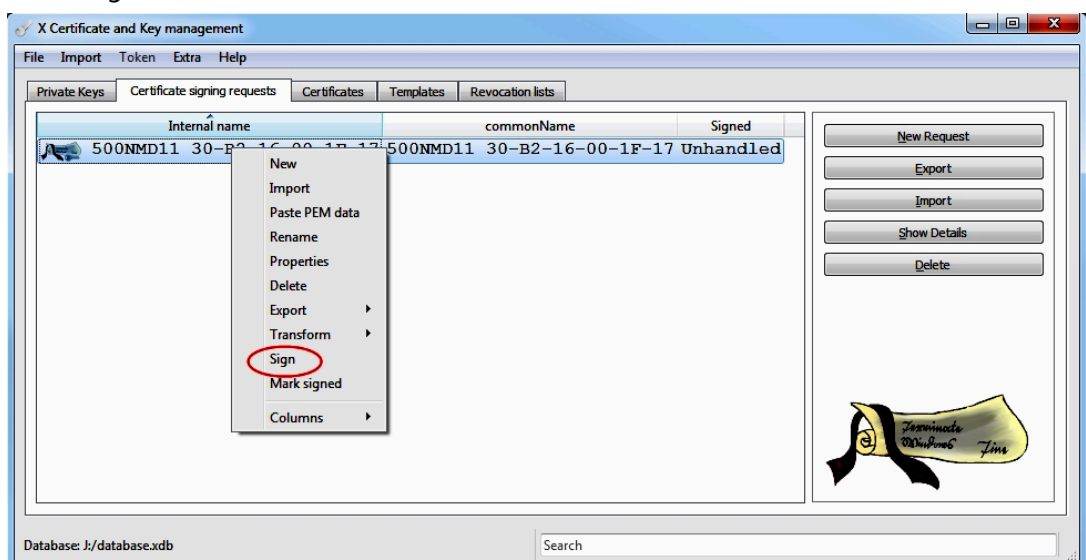
- 1 Import the CSR file: Select Import in the menu and click on Request.



- 2 A message confirms the successful import.



- 3 Select the tab Certificate signing request. Right mouse click on the imported CSR and select Sign.



- 4 A new window will open. Go to tab Source and make sure that Use this Certificate for signing is selected. Choose the CA certificate from the drop down list.

X Certificate and Key management

### Create x509 Certificate

Source | Extensions | Key usage | Netscape | Advanced | Comment

**Signing request**

- ☒ Sign this Certificate signing request
- ☒ Copy extensions from the request
- ☐ Modify subject of the request

500NMD11 30-B2-16-00-1F-17

Show request

**Signing**

- ☐ Create a self signed certificate
- ☒ Use this Certificate for signing

CA\_myCompany\_cert

**Signature algorithm**

SHA 256

**Template for the new certificate**

[default] Empty template

Apply extensions | Apply subject | Apply all

OK | Cancel

- 5 Go to tab Extensions. Select End Entity under Basic Constraints and enter Not before and Time range in the Group Validity. Chose Time range according your company security policies. Then confirm with OK.

**Create x509 Certificate**

Source Extensions **Key usage** Netscape Advanced Comment

X509v3 Basic Constraints

Type: **End Entity**

Path length:  ☐ Critical

Key identifier

☐ Subject Key Identifier

☐ Authority Key Identifier

Validity

Not before: 2019-05-03 13:49 GMT

Not after: 2020-05-03 13:49 GMT

Time range

Years **Apply**

☐ Midnight ☐ Local time ☐ No well-defined expiration

X509v3 Subject Alternative Name:  **Edit**

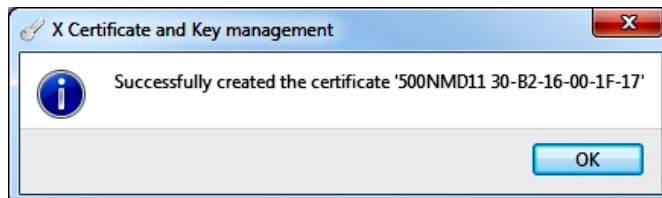
X509v3 Issuer Alternative Name:  **Edit**

X509v3 CRL Distribution Points:  **Edit**

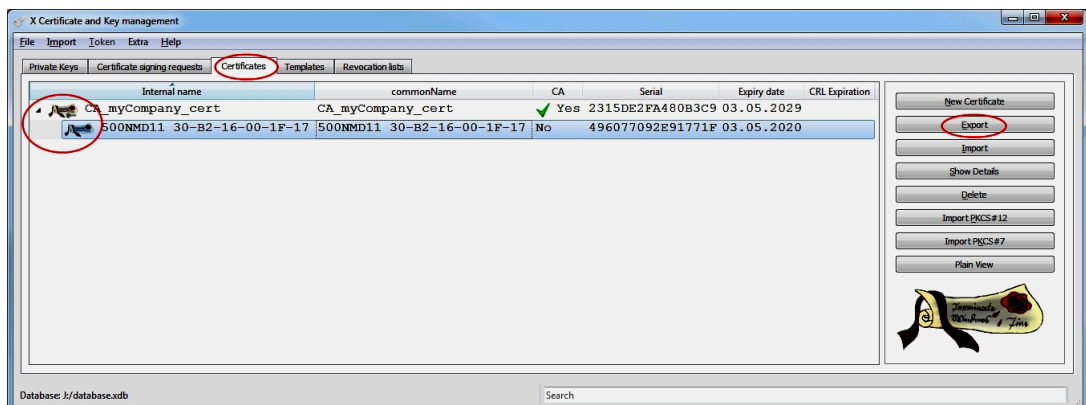
Authority Information Access: OCSP  **Edit**

**OK** Cancel

- 6 A message confirms the successful creation of the certificate.



- 7 The now created certificate will be listed as a branch of the CA certificate in the certificates overview. Select the certificate and click on Export of the right side.



- 8 Choose PEM (\*.crt) as Export Format and click on OK. An external certificate has been created and is ready for upload to the EDS500 managed switches.

## Upload CRT file

- 1 Go to web server of the EDS500 managed switches and chose Encryption in the left Administration menu. Click on Browse... under Crypto certificate web upload, select your created certificate and click on upload.

**Crypto certificate TFTP upload**  
 TFTP server IP:   
 Certificate filename:

**Crypto certificate web upload**  
 Select local certificate file:  
 No file selected.


---

**Certificate Signing Request**  
 The device may generate a PKCS #10 certificate signing request in order to apply for a certification by a Certification Authority (CA). The resulting certificate may be re-uploaded to the device, for example to replace a self-signed device certificate.

**Crypto certificate signing request TFTP download**  
 TFTP server IP:   
 CSR filename:

**Crypto certificate signing request web download**

- 2 A successful upload of a valid certificate will be confirmed by the following website.



**» 500NMD11 «**  
 · Device Configuration ·

Administration  
 » Authentication  
 » Commands  
 » Configuration  
 » Encryption  
 » Firmware  
 » IEC-101/104  
 » Interfaces  
 » IP & Host  
 » Port Mirroring  
 » Rate Limiting  
 » SNMP  
 » SNMP  
 » Spanning Tree  
 » Syslog  
 » Telnet & SSH  
 Information  
 » Alarms  
 » Device  
 » Event Log  
 » Health  
 » Neighbors  
 » Statistics  
 Authentication  
 » Logout  
 www.abb.com

**Crypto certificate transfer**  

Transfer result  
 The crypto certificate has been transferred successfully.

**System crypto keys**  
 Cryptographic keys must be uploaded in PEM format. Supported key types are DSA (1024 bit) and EC (256 bit, secp256r1).  
 DSA key SSH fingerprint (MD5): 9d:c8:62:08:75:1a:8b:c1:ab:2e:28:d0:a1:44:fd:53  
 EC key SSH fingerprint (MD5): 10:9a:8c:e5:b9:1e:65:c0:11:5e:b0:3c:d5:8f:bd:f4  

**Crypto key TFTP upload**  
 TFTP server IP:   
 Key filename:

**Crypto key web upload**  
 Select local key file:  
 No file selected.

**System crypto certificate**  
 Certificates must be provided in PEM format. The certificate must match the system EC key.  
 The system certificate status is signed by another CA.
 

X.509 certificate:  
 Version: 3 (0x2)  
 Serial Number: 49:60:77:09:2E:91:77:1F  
 Issuer: CN=CA myCompany cert  
 Validity: From 03.05.19 13:49:00 GMT to 03.05.20 13:49:00 GMT  
 Subject: CN=500NMD11 30-B2-16-00-1F-17, O=ABB, C=DE  
 Subject Public Key Info:  
 Public Key Algorithm: id-ecPublicKey  
 Curve: secp256r1 (NIST P-256)  
 Public Key: (256 bit)  
 04:22:B1:A4:82:70:0D:F2:6E:8C:33:86:AF:50:42:D2:  
 28:23:1B:27:E1:7B:2E:9F:5E:00:62:6F:57:3C:EA:33:  
 EE:E2:54:DC:27:9D:FB:DC:76:BD:48:0F:88:D6:86:CC:  
 C8:78:4D:88:AA:24:6C:14:CC:47:56:19:F8:EB:9F:6C:  
 18  
 Subject Alternative Names:  
 IP Address: 192.168.10.112  
 X.509 Signature: sha256WithRSAEncryption



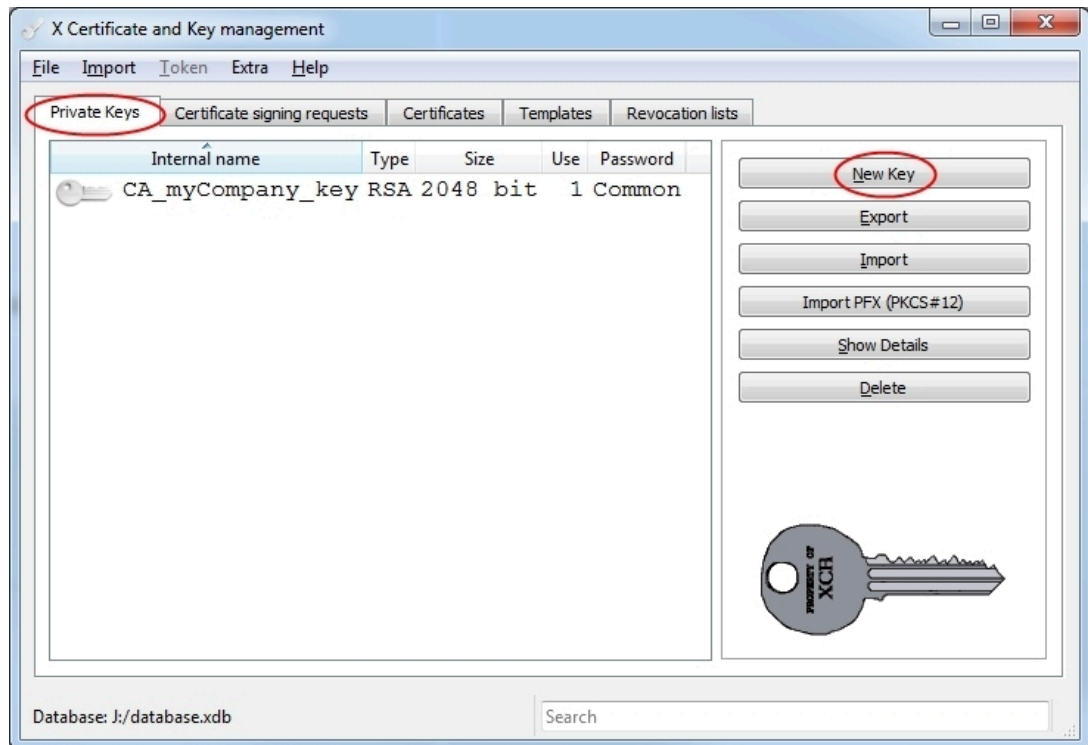
### 2.36.3.4 Generate and Upload EC Keys

This chapter describes how to create a valid EC key and upload them to the EDS500 managed switches. Based on the external key you have the possibility to create a self-signed certificate or a CSR file based by the EDS500 managed switches.

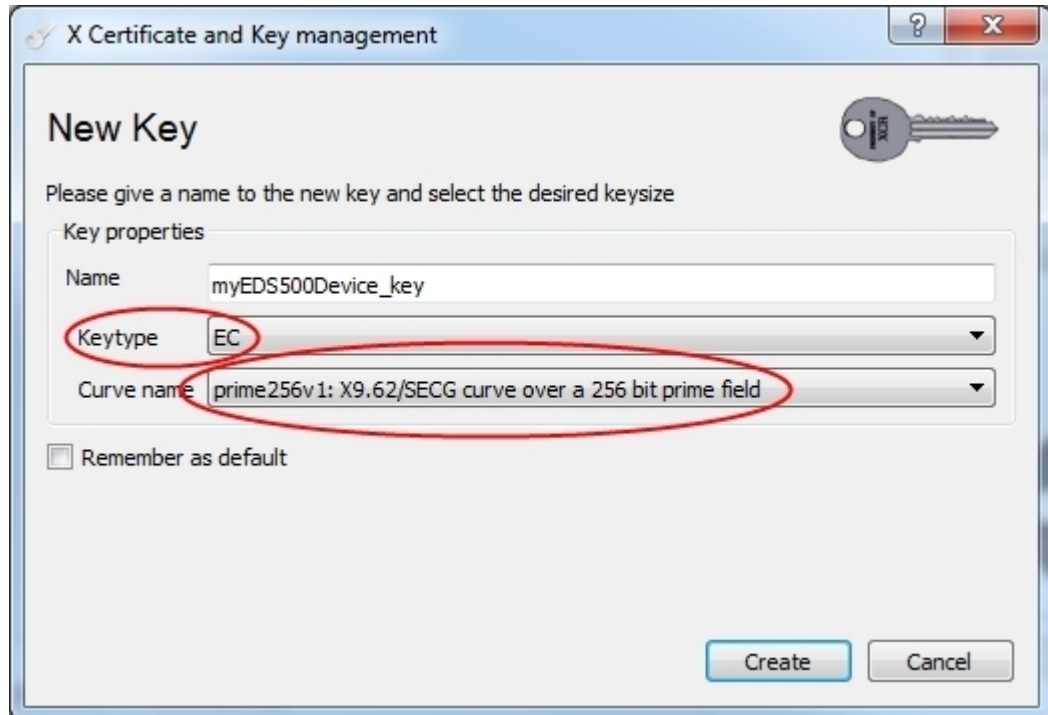
In addition, a certificate can also be created without the EDS500 managed switches by using the XCA Tool. This option is described at the end of this chapter.

#### Create the EC Key

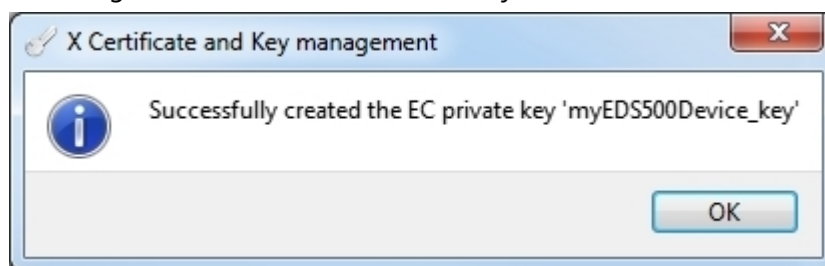
- 1 Start the XCA Tool and select New Key in the tab Private Keys.



- 2 A dialog box opens. Select EC as Keytype and prime256v1: X9.62/SECG curve over a 256 bit prime field as Curve name. Click on Create.



- 3 A message confirms the successful EC Key creation.



An external EC Key has been created and is ready for upload to the EDS500 managed switches.

### Upload EC Key

- 1 Go to web server of the EDS500 managed switches and chose Encryption in the left Administration menu. Click on Browse... under Crypto key web upload, select your created key and click on upload.

2 A successful upload of a valid EC key will be confirmed by the following website.

### 2.36.3.5 Device Certificate with External EC Key

This chapter describes how to upload an external key and download the self-signed certificate from the EDS500 managed switches web server and integrate it into the browser

The Generation of the self-signed certificate will be done by the EDS500 managed switches automatically after upload of the EC key.

#### Upload EC Key

see "Upload EC Key", page 130

#### Browser integration of self-signed certificates

For Firefox integration see

"Integration of self-signed and CA-signed certificates into Mozilla Firefox".

For Internet Explorer/Edge or Chrome see

"Integration of self-signed and CA-signed certificates into MS Internet Explorer/Edge and Google Chrome".

### 2.36.3.6 External Certificate (CRT) with External EC Key

This chapter describes how to upload an external key and generate a CSR (Certificates Signing Request) file based on the external key. The way via the CRT file ensures that the external created EC key and the external created CA-signed certificate are compatible to each other.

#### Upload EC key

see "Upload EC Key", page 130

#### Generate external certificate with CRT

see "Generate External Certificates (CRT)", page 123

#### Browser integration of CA-signed certificates

For Firefox integration see

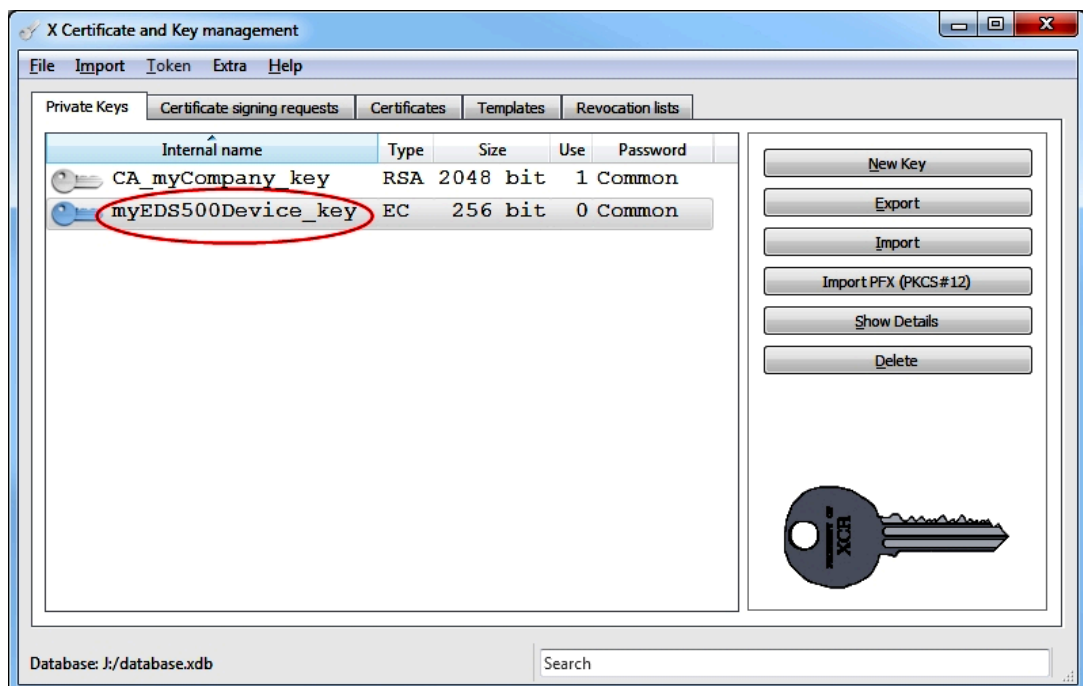
"Integration of self-signed and CA-signed certificates into Mozilla Firefox".

For Internet Explorer/Edge or Chrome see

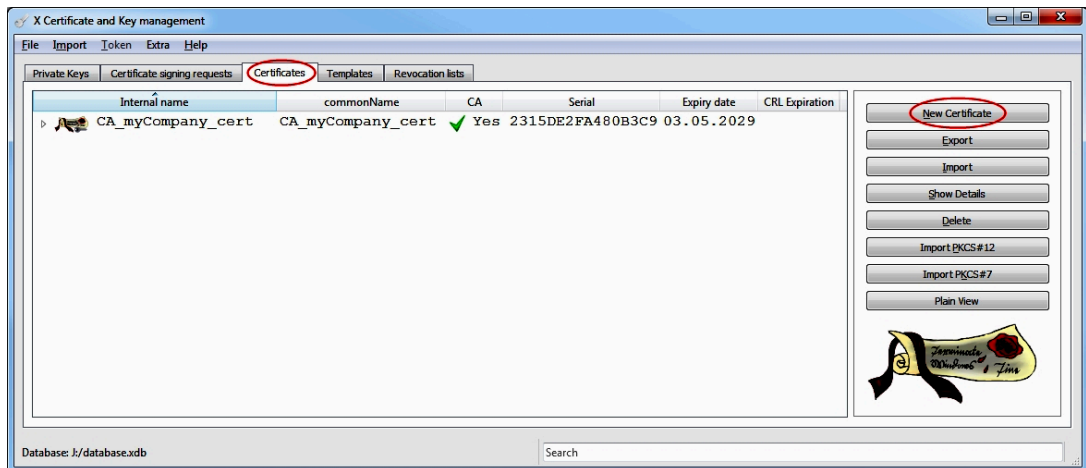
"Integration of self-signed and CA-signed certificates into MS Internet Explorer/Edge and Google Chrome".

### 2.36.3.7 External Certificate (External Generated) with External EC Key

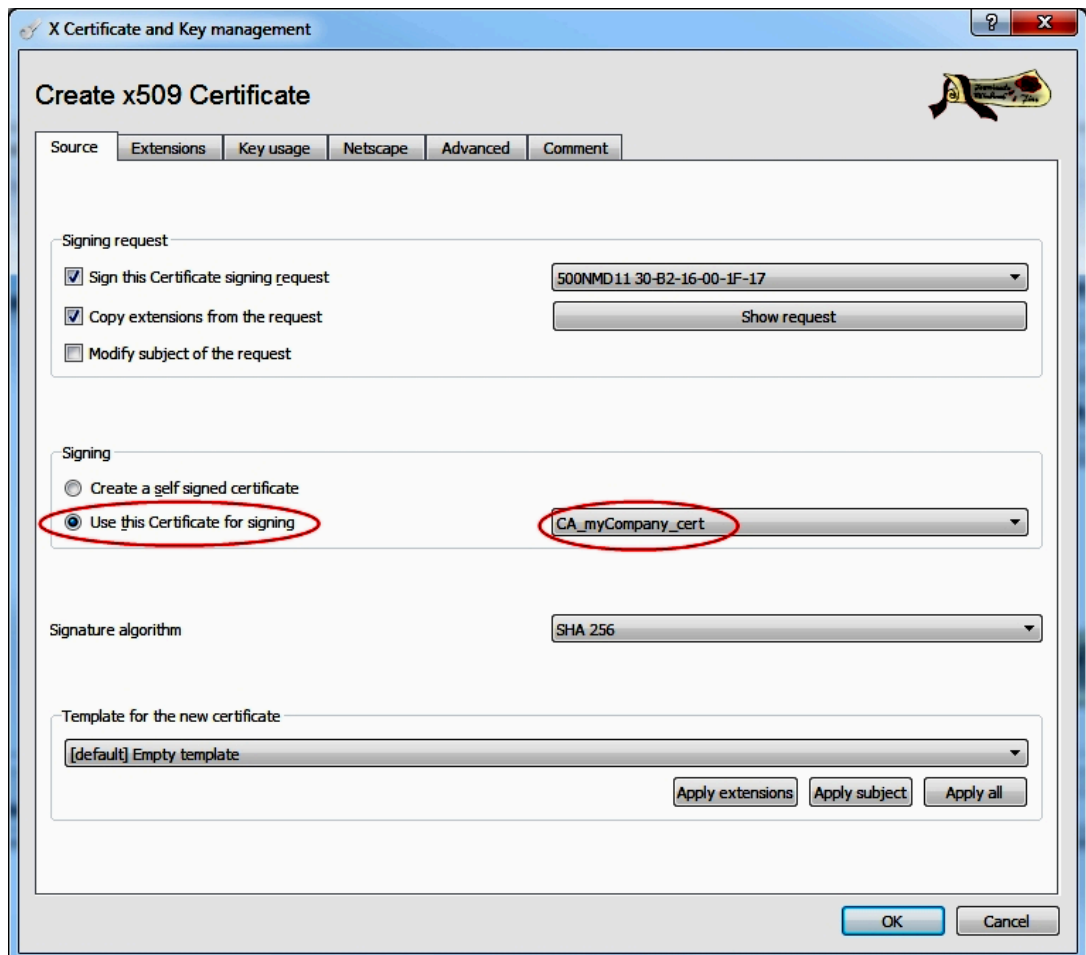
- 1 Start the XCA Tool and mark the EC Key you want to use in the tab Private Keys.



- 2 Go to tab Certificates and click on New Certificate.



- 3 A message confirms the successful import.



- 4 Go to tab Subject. Type the internal Name, the commonName and choose the EC Key in the drop down list.
- 5 Then confirm with OK.

**Create x509 Certificate**

Source Subject Extensions Key usage Netscape Advanced Comment

Internal Name: myEDS500Device\_cert

Distinguished name

countryName: organizationalUnitName:

stateOrProvinceName: commonName: myEDS500Device\_cert

localityName: emailAddress:

organizationName:

Type	Content
------	---------

Private key: myEDS500Device\_key (EC:256 bit) ☐ Used keys too

Go to tab Subject. Type the internal Name, the internal Name, the commonName and choose the EC Key in the drop down list.

Then confirm with OK.

An external certificate has been created and is ready for upload to the EDS500 managed switches.

### Upload CRT file

- 1 Go to web server of the EDS500 managed switches and chose Encryption in the left Administration menu. Click on Browse... under Crypto certificate web upload, select your created certificate and click on upload.

**Crypto certificate TFTP upload**

TFTP server IP:

Certificate filename:

**Crypto certificate web upload**

Select local certificate file:

No file selected.

---

**Certificate Signing Request**

The device may generate a PKCS #10 certificate signing request in order to apply for a certification by a Certification Authority (CA). The resulting certificate may be re-uploaded to the device, for example to replace a self-signed device certificate.

**Crypto certificate signing request TFTP download**

TFTP server IP:

CSR filename:

**Crypto certificate signing request web download**

- 2 A successful upload of a valid certificate will be confirmed by the following website.

**ABB**

» 500NMD11 «

· Device Configuration ·

**Administration**

- » Authentication
- » Commands
- » Configuration
- » Encryption
- » Firmware
- » IEC-101/104
- » Interfaces
- » IP & Host
- » Port Mirroring
- » Rate Limiting
- » SNMP
- » SNTP
- » Spanning Tree
- » Syslog
- » Telnet & SSH

**Information**

- » Alarms
- » Device
- » Event Log
- » Health
- » Neighbors
- » Statistics

**Authentication**

- » Logout

www.abb.com

**Crypto certificate transfer**

**Transfer result**

The crypto certificate has been transferred successfully.

**System crypto keys**

Cryptographic keys must be uploaded in PEM format. Supported key types are DSA (1024 bit) and EC (256 bit, secp256r1).

DSA key SSH fingerprint (MD5): 9d:c8:62:08:75:1a:8b:c1:ab:2e:28:d0:a1:44:fd:53

EC key SSH fingerprint (MD5): 10:9a:8c:e5:b9:1e:65:c0:11:5e:b0:3c:d5:8f:bd:f4

**Crypto key TFTP upload**

TFTP server IP:

Key filename:

**Crypto key web upload**

Select local key file:

No file selected.

**System crypto certificate**

Certificates must be provided in PEM format. The certificate must match the system EC key.

The system certificate status is signed by another CA.

X.509 certificate:

Version: 3 (0x2)

Serial Number: 49:60:77:09:2E:91:77:1F

Issuer: CN=CA myCompany cert

Validity: From 03.05.19 13:49:00 GMT to 03.05.20 13:49:00 GMT

Subject: CN=500NMD11 30-B2-16-00-1F-17, O=ABB, C=DE

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Curve: secp256r1 (NIST P-256)

Public Key: (256 bit)

04:22:B1:A4:82:70:0D:F2:6E:8C:33:86:AF:50:42:D2:  
28:23:1B:27:E1:7B:2E:9F:5E:00:62:6F:57:3C:EA:33:  
EE:E2:54:DC:27:9D:FB:DC:76:BD:48:0F:88:D6:86:CC:  
C8:78:4D:88:AA:24:6C:14:CC:47:56:19:F8:EB:9F:6C:  
18

Subject Alternative Names:

IP Address: 192.168.10.112

X.509 Signature: sha256WithRSAEncryption

### 2.36.3.8 Integration of Certificates Into Browser

Regardless of which combination of key and certificate is used, the certificates must be integrated into the used browser. The procedure depends on the browser and the type of certificates.

The following combinations are described:

- "Integration of self-signed and CA-signed certificates into Mozilla Firefox"
- "Integration of CA certificates into Mozilla Firefox"
- "Integration of self-signed and CA-signed certificates into MS Internet Explorer/Edge and Google Chrome"
- "Integration of CA certificates into MS Internet Explorer/Edge and Google Chrome"

The usage of the device EC key and the device certificate (self-signed) is the easiest way for a HTTPS connection. However, the certificate of each individual device must be downloaded and integrated into the browser. That can be very complex when managing a large number of devices.

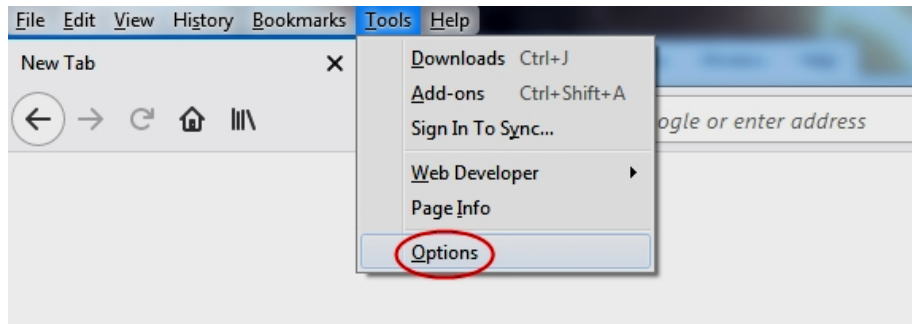
#### Integration of self-signed and CA-signed certificates into Mozilla Firefox

This section describes how to import a self-signed and CA-signed certificate into Firefox.

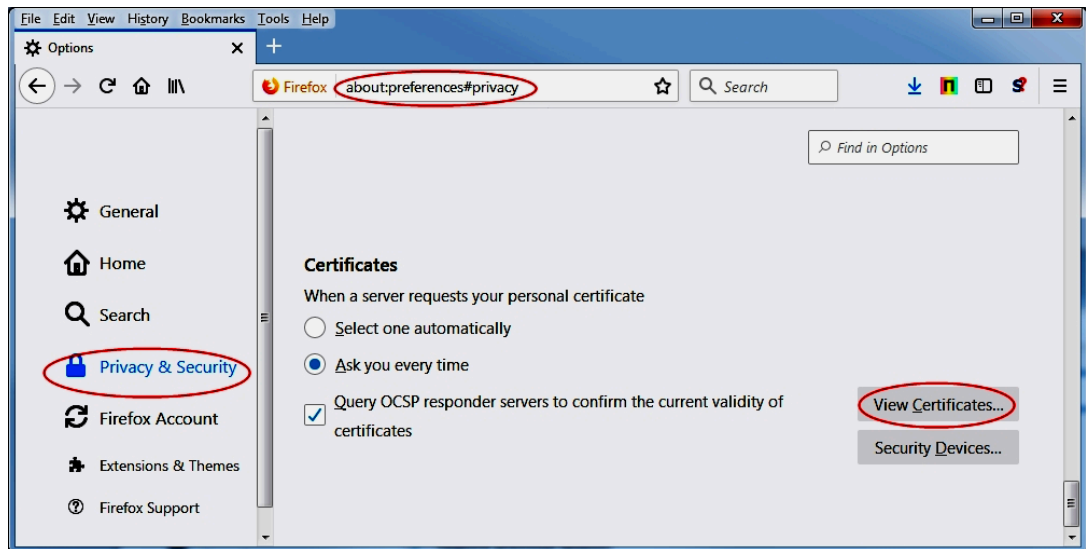
Import self-signed and CA-signed certificates

1. Open Firefox, press ALT for opening extra menu and select Options.

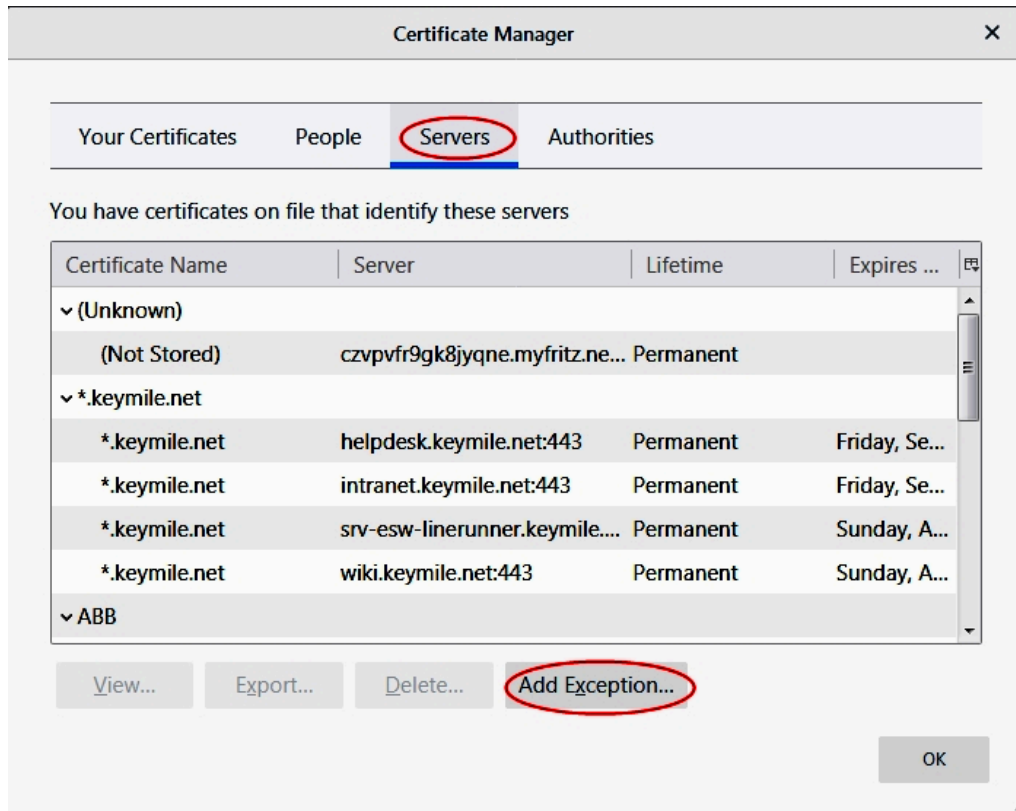




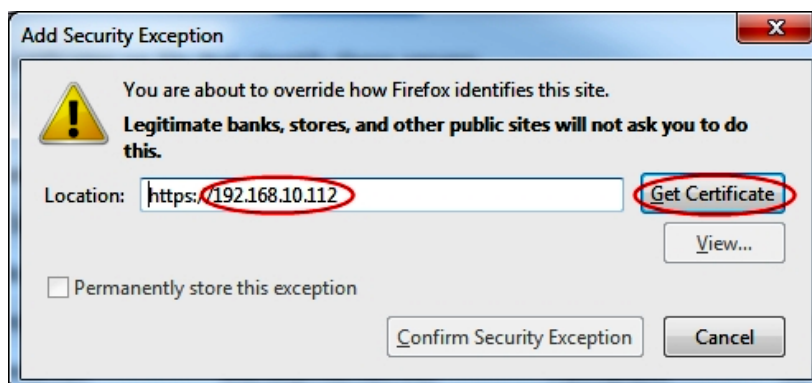
2. Select Privacy & Security from the menu and click on View Certificates...



3. Go to tab Servers and click on Add Exception...



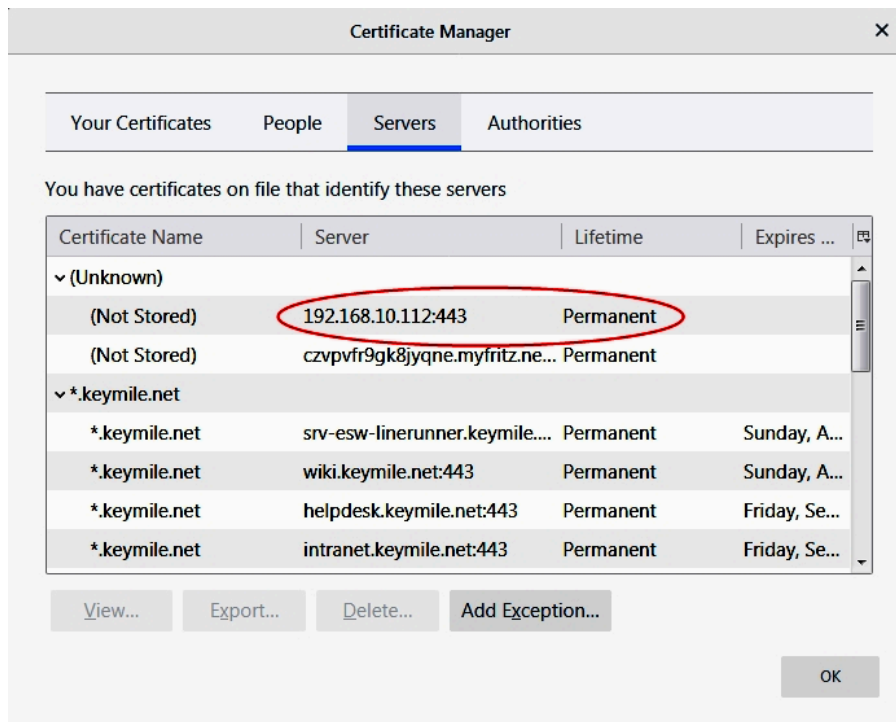
4. Write https:// and the IP address of the device under Location and click on Get Certificate



5. Select Permanently store this exception and click on Confirm Security Exception



6. The exception should then be listed in the certificate manager.

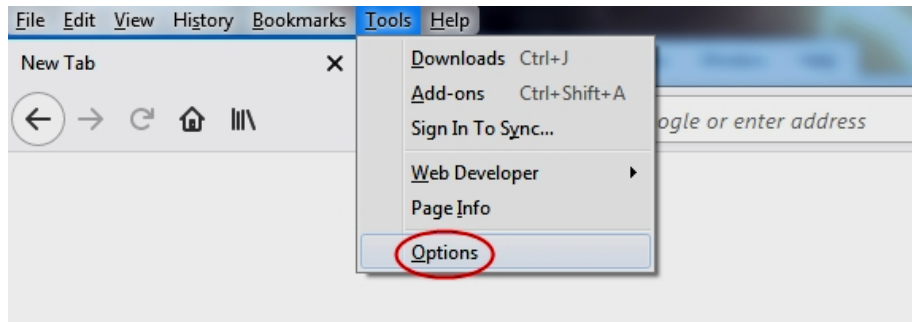


### Integration of CA certificates into Mozilla Firefox

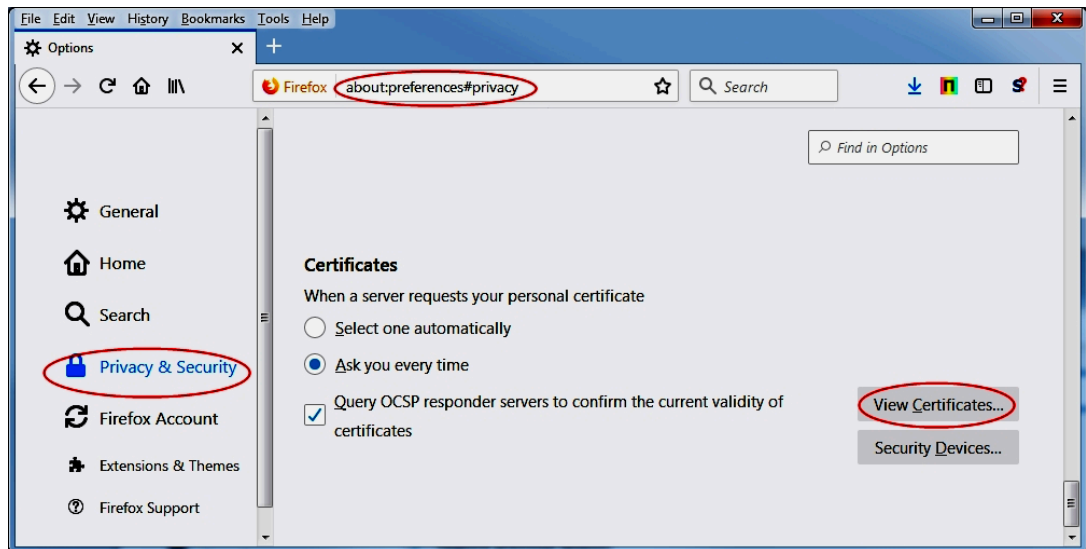
This section describes how to import a CA certificate into Firefox.

Import CA certificates

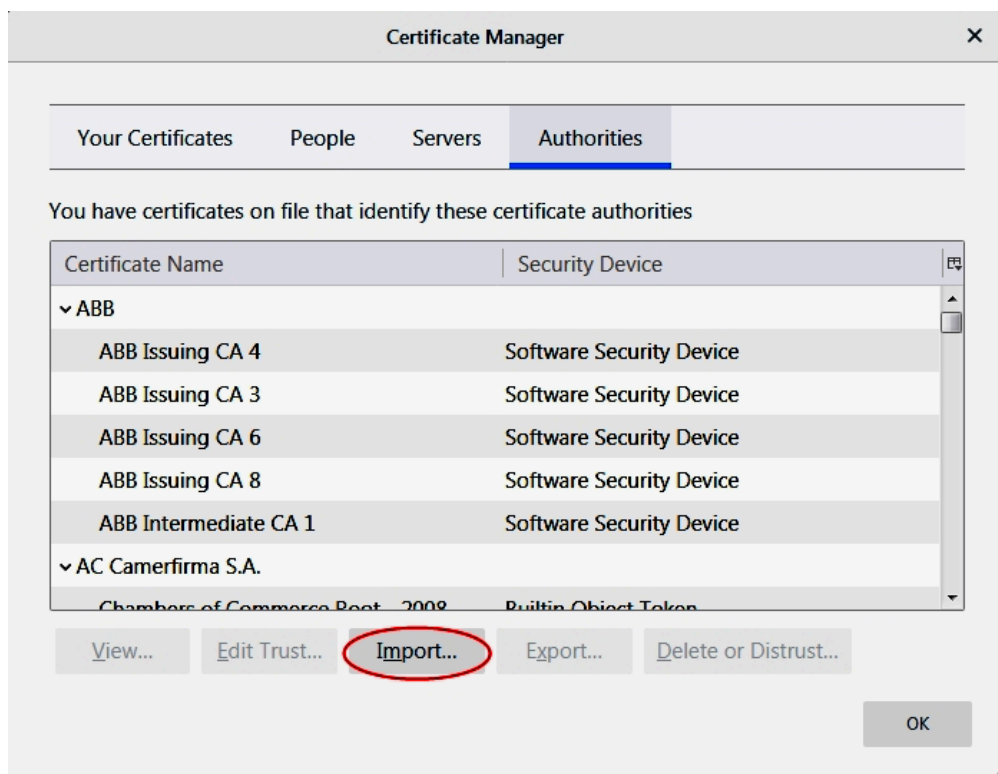
1. Open Firefox, press ALT for opening extra menu and select Options.



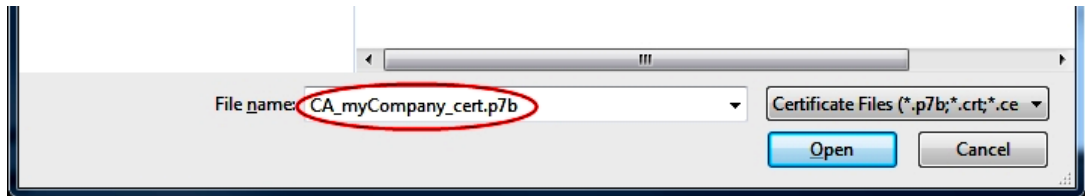
2. Select Privacy & Security from the menu and click on View Certificates...



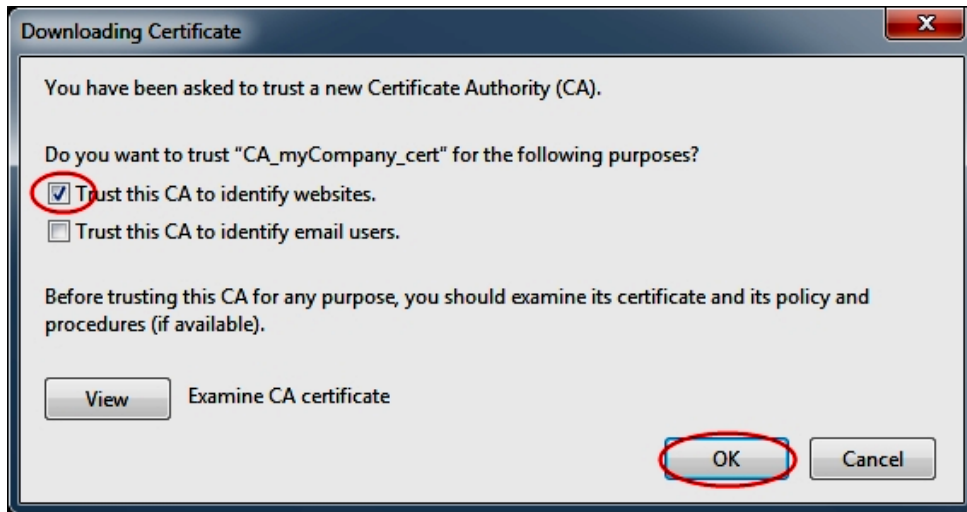
3. Go to tab Authorities and click on Import...



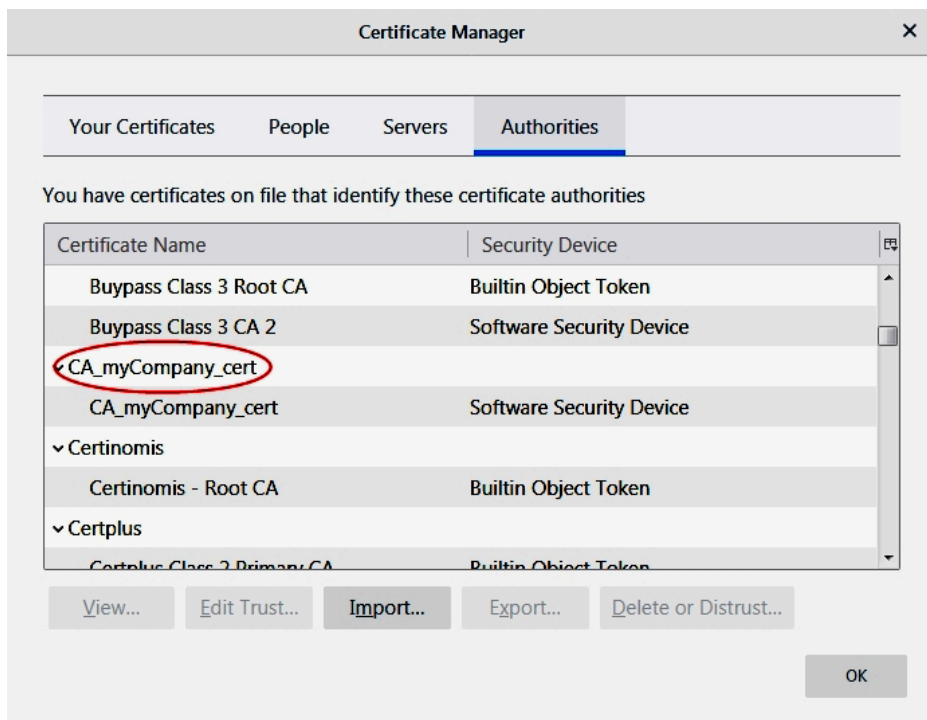
4. Select the CA certificate with .p7b extension and confirm with Open



5. A dialog window opens. Select there Trust this CA to identify websites and confirm with OK.



6. The imported certificate should be listed in the certificate manager.

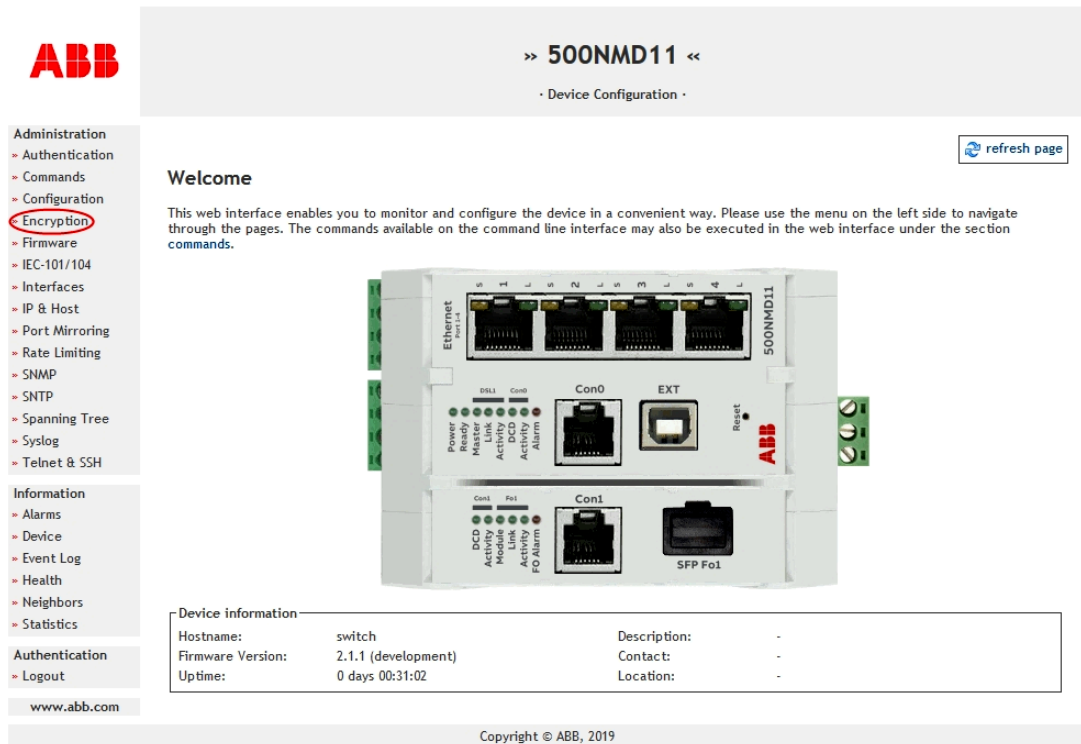


## Integration of self-signed and CA-signed certificates into MS Internet Explorer/Edge and Google Chrome

This section describes how to import a self-signed and CA-signed certificate into MS Internet Explorer/Edge and Google Chrome.

Import self-signed and CA-signed certificates

1. Open the web interface of the EDS500 managed switches and select Encryption in the Administration menu.



The screenshot shows the ABB 500NMD11 web interface. The left sidebar contains a menu with 'Administration' expanded, and 'Encryption' highlighted with a red circle. The main content area displays a 'Welcome' message and a photograph of the 500NMD11 device. Below the photo is a 'Device information' table.

Device information			
Hostname:	switch	Description:	-
Firmware Version:	2.1.1 (development)	Contact:	-
Uptime:	0 days 00:31:02	Location:	-

At the bottom of the page, the copyright notice 'Copyright © ABB, 2019' is visible.

2. Scroll to the bottom of the page and download the Crypto certificate.

**System crypto certificate**

Certificates must be provided in PEM format. The certificate must match the system EC key.

The system certificate status is *self-signed*.

```

X.509 certificate:
Version: 3 (0x2)
Serial Number: 68:0E:DA:52
Issuer: CN=500NMD11 30-B2-16-00-1F-17, O=ABB, C=DE
Validity: From 10.02.19 00:00:01 GMT to 31.12.9999 23:59:59 GMT
Subject: CN=500NMD11 30-B2-16-00-1F-17, O=ABB, C=DE
Subject Public Key Info:
  Public Key Algorithm: id-ecPublicKey
  Curve: secp256r1 (NIST P-256)
  Public Key: (256 bit)
    04:22:B1:A4:82:70:0D:F2:6E:8C:33:86:AF:50:42:D2:
    28:23:1B:27:E1:7B:2E:9F:5E:00:62:6F:57:3C:EA:33:
    EE:E2:54:DC:27:9D:FB:DC:76:BD:48:0F:88:D6:86:CC:
    C8:78:4D:88:AA:24:6C:14:CC:47:56:19:F8:EB:9F:6C:
    18
  Subject Alternative Names:
    IP Address: 192.168.10.112
X.509 Signature: ecdsa-with-SHA256
  
```

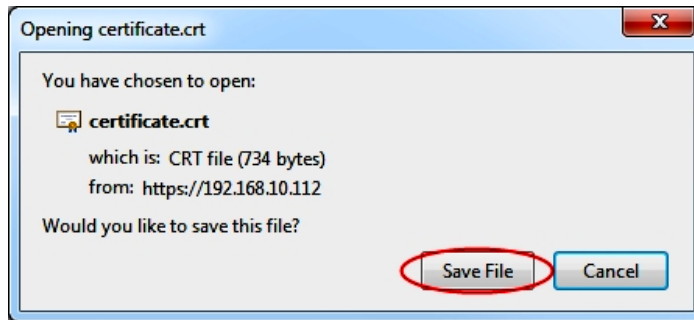
**Crypto certificate TFTP download**

TFTP server IP:

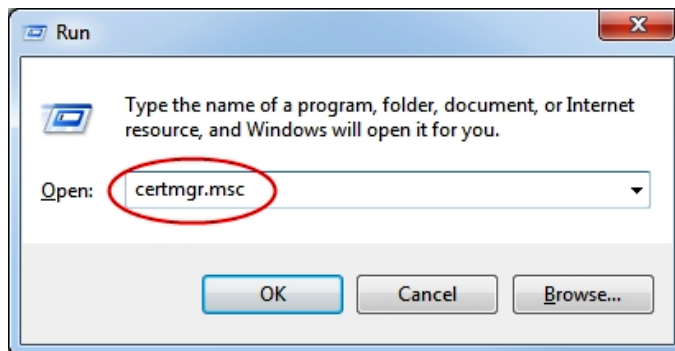
Certificate filename:

**Crypto certificate web download**

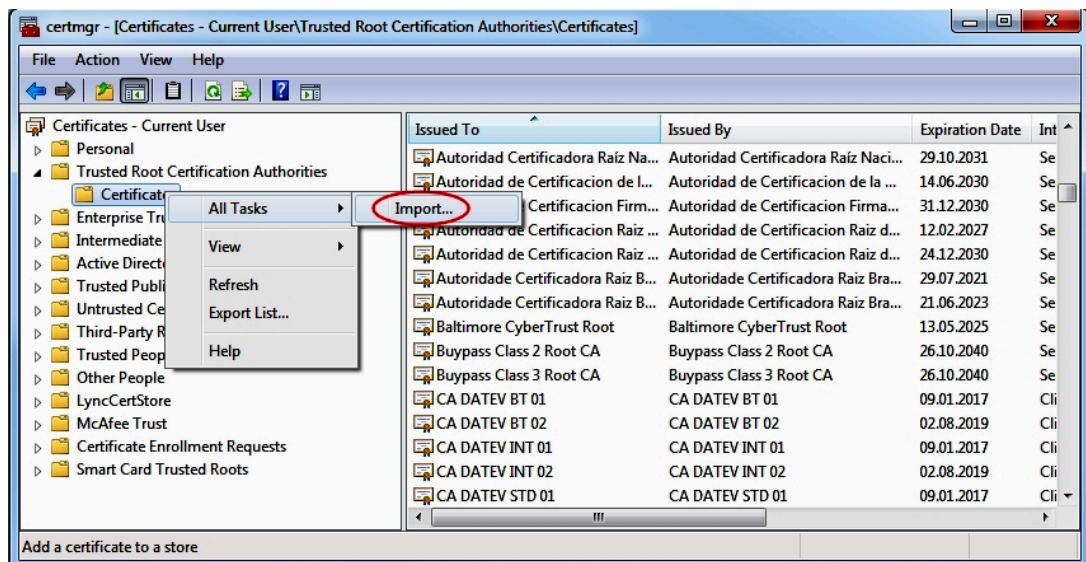
3. A message will appear. Click on Save File to store the certificate on the workstation.



4. Open the Microsoft Windows certificate manager by pressing Win+R and write certmgr.msc in the Open field and click on OK.



5. After the certificate manager is open, click on the small triangle in front of Trust Root Certification Authorities. A sub-folder Certificate will open. Right-click on the Certificate sub-folder opens the context menu. Chose All Task and Import... from the context menu.

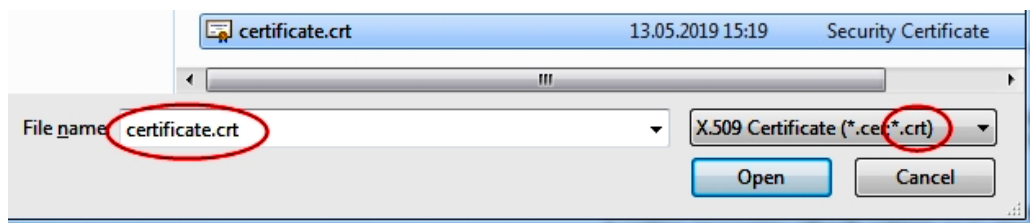


6. The Certificate Import Wizard opens. Click on Next >.



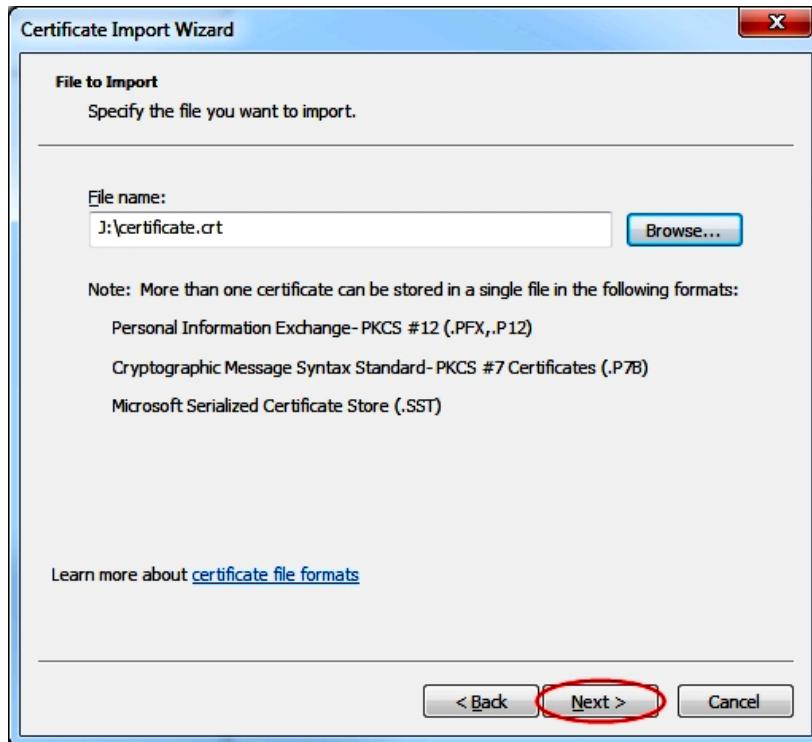


7. Chose X.509 Certificate (\*.cer; \*.crt), select the certificate to be used and click on Open.

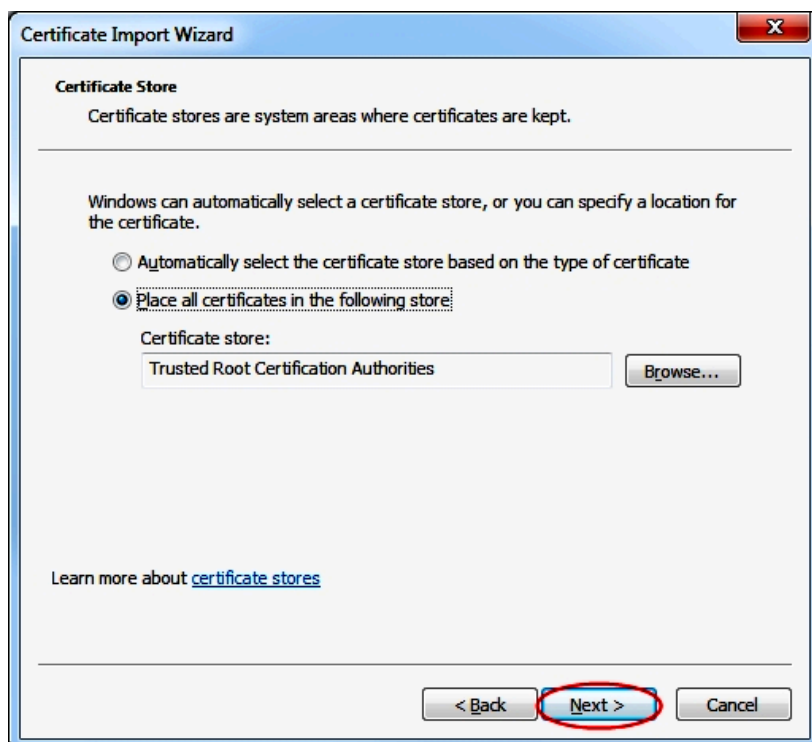


8. Confirm with a click on Next >.

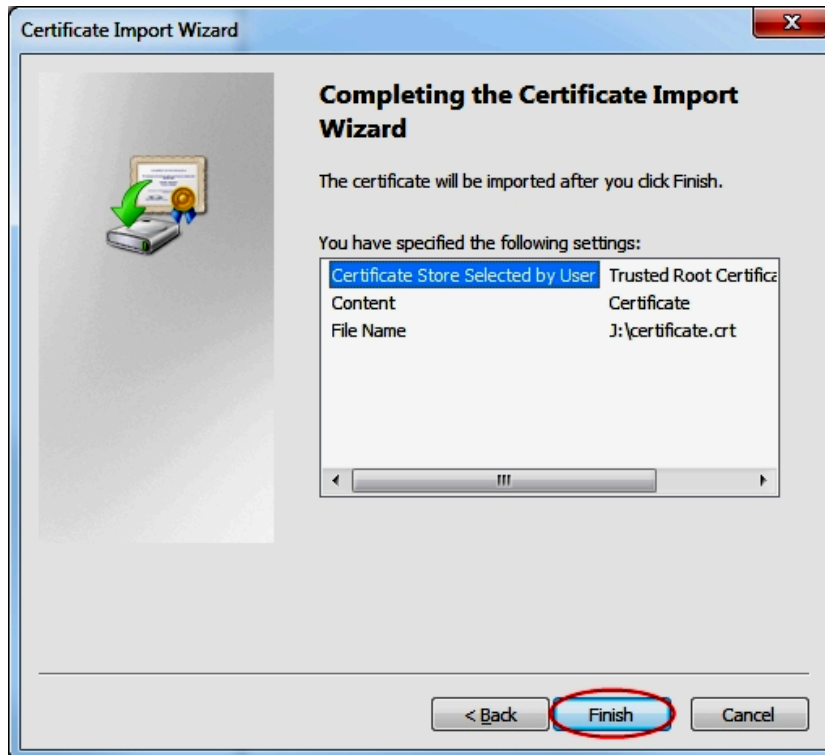




9. Make sure that the certificates are stored in Trusted Root Certification Authorities and click on Next >.



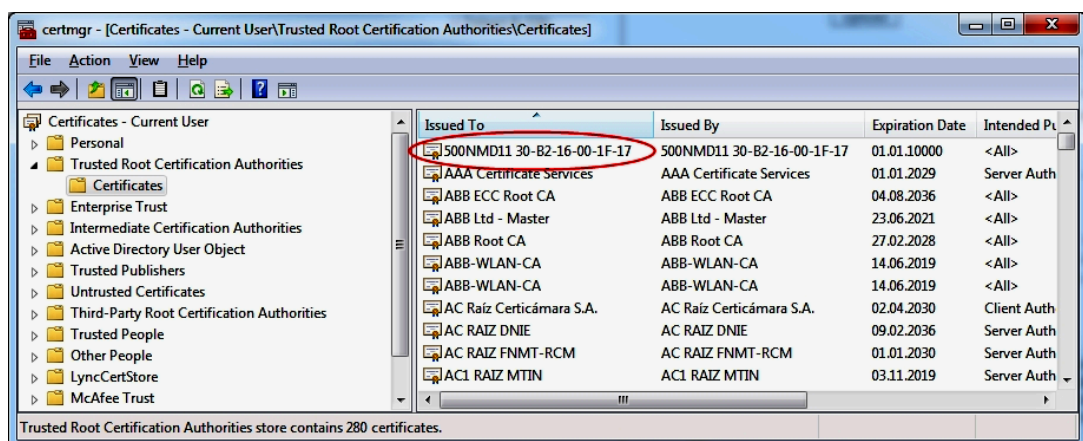
10. Complete the import by clicking on Finish.



11. The import was successful if the following message appears. Click on OK to close the wizard.



12. The new certificate should now be listed in the certificate manager.

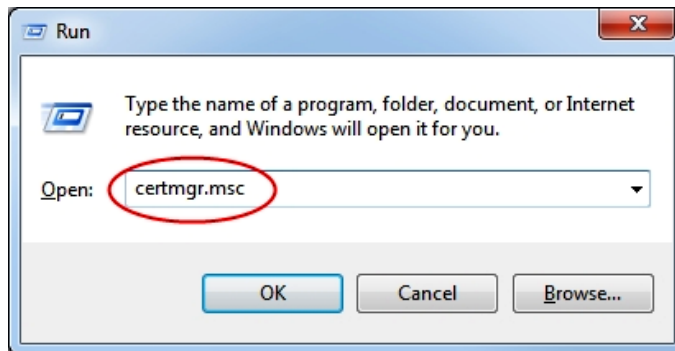


### Integration of CA certificates into MS Internet Explorer/Edge and Google Chrome

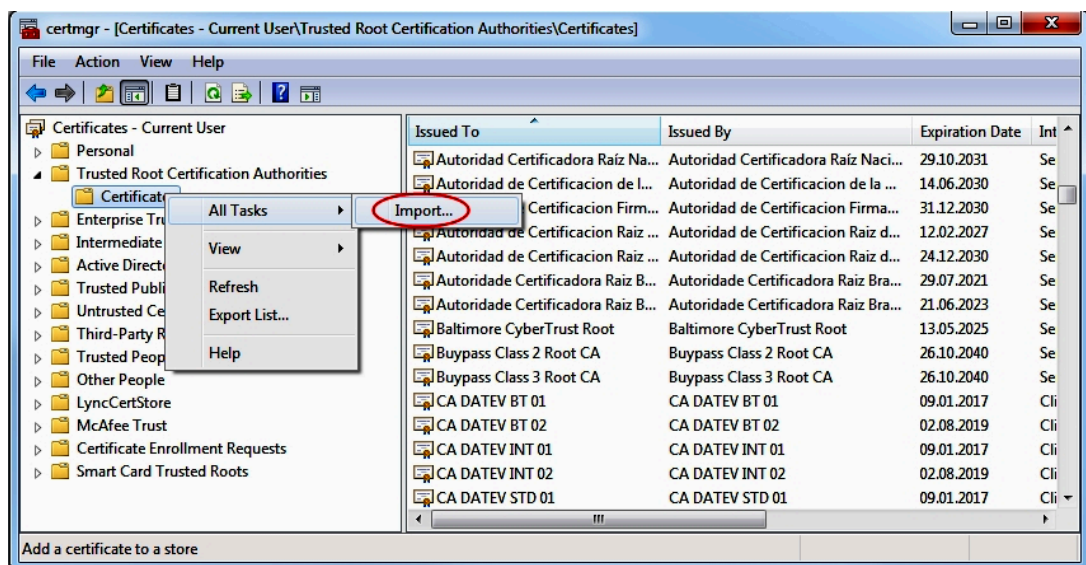
This section describes how to import a CA certificate into MS Internet Explorer/Edge and Google Chrome.

### Import CA certificates

1. Open the Microsoft Windows certificate manager by pressing Win+R and write certmgr.msc in the Open field and click on OK.



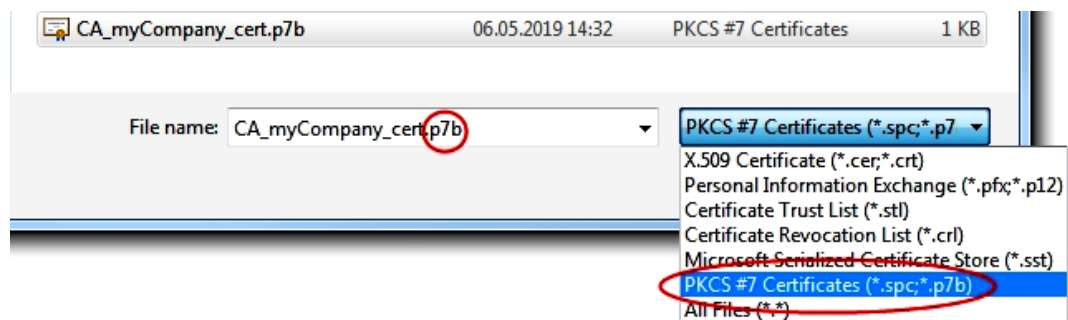
2. After the certificate manager is open, click on the small triangle in front of Trusted Root Certification Authorities. A sub-folder Certificate will open. Right-click on the Certificate sub-folder opens the context menu. Chose All Task and Import... from the context menu.



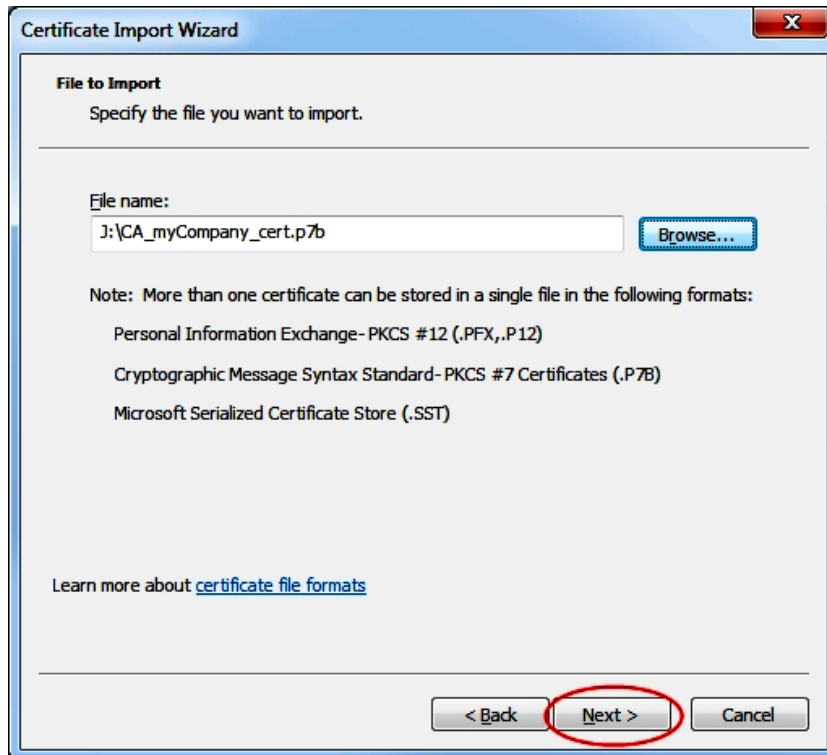
3. The Certificate Import Wizard opens. Click on Next >.



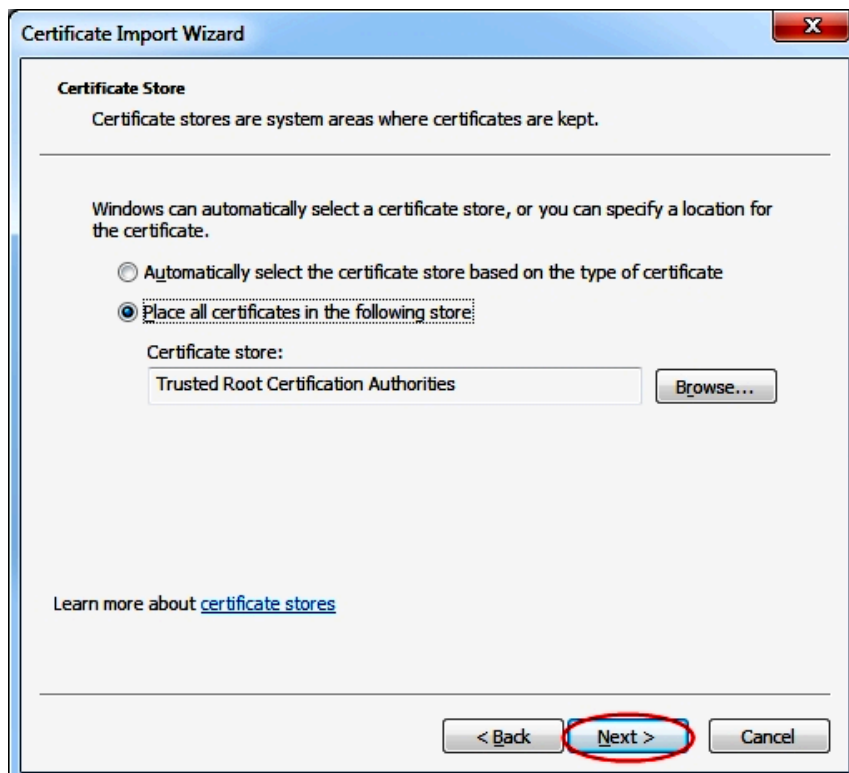
4. Chose PKCS #7 Certificates (\*.spc; \*.p7b), select the CA certificate to be used and click on Open.



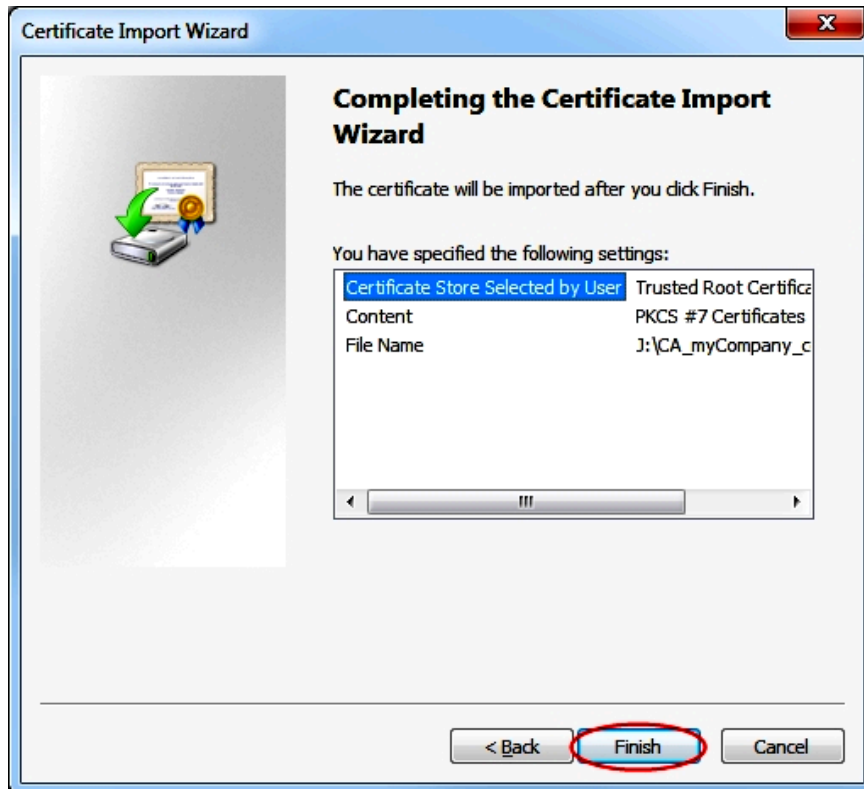
5. Confirm with a click on Next >.



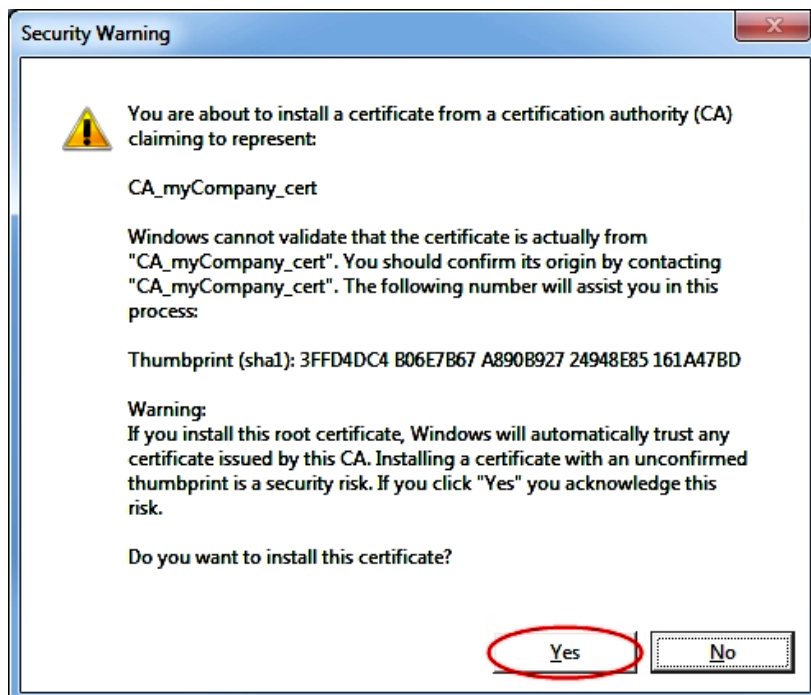
6. Make sure that the certificates are stored in Trusted Root Certification Authorities and click on Next >.



7. Complete the import by clicking on Finish.



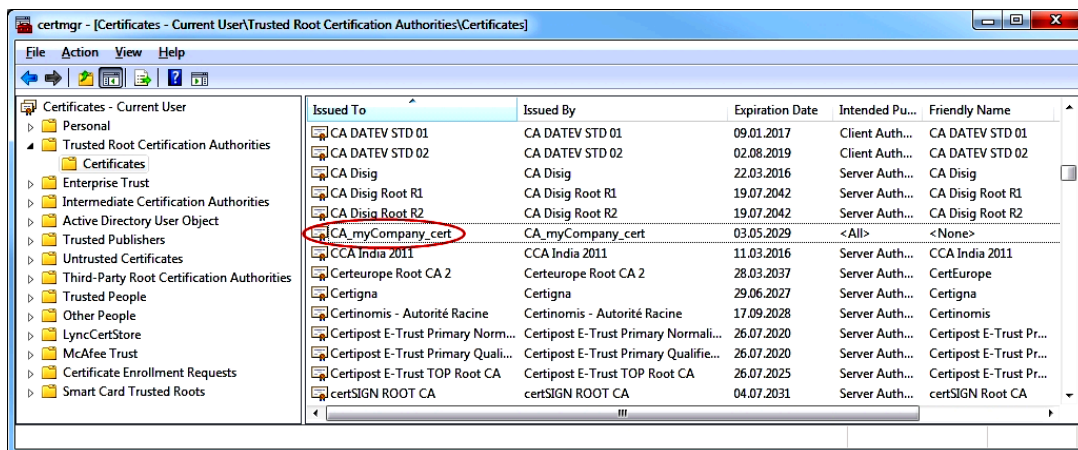
8. A Security Warning will open. Click on Yes to confirm.



9. The import was successful if the following message appears. Click on OK to close the wizard.



10. The new certificate should now be listed in the certificate manager.







### 3 Glossary

<b>AD</b>	<b>A</b> ctive <b>D</b> irectory
<b>APN</b>	<b>A</b> ccess <b>P</b> oint <b>N</b> ame of GPRS Service Provider Network
<b>ARP</b>	<b>A</b> ddress <b>R</b> esolution <b>P</b> rotocol
<b>ASDU</b>	<b>A</b> pplication <b>S</b> ervice <b>D</b> ata <b>U</b> nit
<b>CA</b>	<b>C</b> ertificate <b>A</b> uthority
<b>CLI</b>	<b>C</b> ommand <b>L</b> ine <b>I</b> nterface
<b>CRC</b>	<b>C</b> yclic <b>R</b> edundancy <b>C</b> heck
<b>CTS</b>	<b>C</b> lear <b>t</b> o <b>S</b> end
<b>dB</b>	Decibel
<b>DCD</b>	<b>D</b> ata <b>C</b> arrier <b>D</b> etect
<b>DSL</b>	<b>D</b> igital <b>S</b> ubscriber <b>L</b> ine
<b>EC</b>	<b>E</b> lliptic <b>C</b> urve
<b>GSM</b>	<b>G</b> lobal <b>S</b> tandard for <b>M</b> obile <b>C</b> ommunications
<b>HTTP</b>	<b>H</b> ypertext <b>T</b> ransfer <b>P</b> rotocol
<b>IEC</b>	<b>I</b> nternational <b>E</b> lectrotechnical <b>C</b> ommission
<b>IEEE</b>	<b>I</b> nstitute of <b>E</b> lectrical and <b>E</b> lectronics <b>E</b> ngineers
<b>ITU-T</b>	<b>I</b> nternational <b>T</b> elecommunication <b>U</b> ion - <b>S</b> ection <b>T</b> elecommuni- cation <b>S</b> tandardization
<b>kbps</b>	kbits per second
<b>L2TP</b>	<b>L</b> ayer <b>2</b> <b>T</b> unneling <b>P</b> rotocol
<b>LAN</b>	<b>L</b> ocal <b>A</b> rea <b>N</b> etwork
<b>LED</b>	<b>L</b> ight <b>E</b> mitting <b>D</b> iode
<b>LLDP</b>	<b>L</b> ink <b>L</b> ayer <b>D</b> iscovery <b>P</b> rotocol according to IEEE-802.1AB
<b>MAX</b>	<b>M</b> aximum
<b>Mbps</b>	<b>M</b> Bit per second
<b>MIB</b>	<b>M</b> anagement <b>I</b> nformation <b>B</b> ase
<b>MO</b>	<b>M</b> obile <b>O</b> riginated
<b>ms</b>	<b>M</b> illisecond
<b>MSTP</b>	<b>M</b> ultiple <b>S</b> panning <b>T</b> ree <b>P</b> rotocol
<b>NIST</b>	<b>N</b> ational <b>I</b> nstitute of <b>S</b> tandards and <b>T</b> echnology
<b>NTP</b>	<b>N</b> etwork <b>T</b> ime <b>P</b> rotocol
<b>OID</b>	<b>O</b> bject <b>I</b> dentifier ( <b>SNMP</b> )

<b>OSI</b>	Open Systems Interconnection Model
<b>PC</b>	<b>P</b> ersonal <b>C</b> omputer
<b>PIN</b>	<b>P</b> ersonal Identity <b>N</b> umber
<b>PKCS</b>	<b>P</b> ublic- <b>K</b> ey <b>C</b> ryptography <b>S</b> tandards
<b>PLC</b>	Programmable Logic Control
<b>PSU</b>	Power Supply Unit
<b>RADIUS</b>	Remote Authentication Dial-In User Service
<b>RFC</b>	Request for Comments
<b>RIP</b>	Routing Information Protocol
<b>RSTP</b>	Rapid Spanning Tree Protocol
<b>RTS</b>	Request to Send
<b>RTU</b>	Remote Terminal Unit
<b>Rx</b>	Receive Direction
<b>SFP</b>	Small Form-factor Pluggable
<b>SHDSL</b>	Single-Pair High-Speed Digital Subscriber Line
<b>SNMP</b>	Simple Network Management Protocol
<b>SNTP</b>	Simple Network Time Protocol (according to RFC 4330)
<b>SPS</b>	Programmable Logic Control ( <b>S</b> peicher <b>p</b> rogrammierbare <b>S</b> teuerung)
<b>SSH</b>	Secure Shell
<b>STP</b>	<b>S</b> panning <b>T</b> ree <b>P</b> rotocol
<b>TCP/IP</b>	<b>T</b> ransmission <b>C</b> ontrol <b>P</b> rotocol / <b>I</b> nternet <b>P</b> rotocol
<b>TFTP</b>	Trivial File Transfer Protocol
<b>Tx</b>	Transmit Direction
<b>UART</b>	<b>U</b> niversal <b>A</b> synchronous <b>R</b> eceiver- <b>t</b> ransmitter
<b>UDP</b>	User Datagram Protocol
<b>VLAN</b>	Virtual Local Area Network
<b>VPN</b>	Virtual Private Network
<b>VRRP</b>	Virtual Router Redundancy Protocol



**Note:**

The specifications, data, design or other information contained in this document (the "Brochure") - together: the "Information" - shall only be for information purposes and shall in no respect be binding. The Brochure does not claim to be exhaustive. Technical data in the Information are only approximate figures. We reserve the right at any time to make technical changes or modify the contents of this document without prior notice. The user shall be solely responsible for the use of any application example or information described within this document. The described examples and solutions are examples only and do not represent any comprehensive or complete solution. The user shall determine at its sole discretion, or as the case may be, customize, program or add value to the ABB products including software by creating solutions for the end customer and to assess whether and to what extent the products are suitable and need to be adjusted or customized.

This product is designed to be connected to and to communicate information and data via a network interface. It is the users sole responsibility to provide and continuously ensure a secure connection between the product and users or end customers network or any other network (as the case may be). The user shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB AG is not liable for any damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

ABB AG shall be under no warranty whatsoever whether express or implied and assumes no responsibility for the information contained in this document or for any errors that may appear in this document. ABB AG's liability under or in connection with this Brochure or the files included within the Brochure, irrespective of the legal ground towards any person or entity, to which the Brochure has been made available, in view of any damages including costs or losses shall be excluded. In particular ABB AG shall in no event be liable for any indirect, consequential or special damages, such as – but not limited to – loss of profit, loss of production, loss of revenue, loss of data, loss of use, loss of earnings, cost of capital or cost connected with an interruption of business or operation, third party claims. The exclusion of liability shall not apply in the case of intention or gross negligence. The present declaration shall be governed by and construed in accordance with the laws of Switzerland under exclusion of its conflict of laws rules and of the Vienna Convention on the International Sale of Goods (CISG).

ABB AG reserves all rights in particular copyrights and other intellectual property rights. Any reproduction, disclosure to third parties or utilization of its contents - in whole or in part - is not permitted without the prior written consent of ABB AG.

© Copyright ABB 2019

All rights reserved