Welcome to the SIMATIC NET Documentation-DVD for SCALANCE X, CSM377 und CSM1277

09/2018, A5E00364553-CC

1 Introduction

Note on the DVD

This SIMATIC NET Documentation-DVD contains the following documents and tools:

- Information on the product
- Primary Setup Tool
- OPC Profiles
- Open Source Informationen

Note on the readme file

Read this readme file carefully before using the products or software.

The following sections describe deviations or provide additional information compared with the information in the product documentation.

It contains additional information about the product. The content of this readme file can be considered more valid than statements made in other documents.

Copyright

Disclaimer of Liability

If the relevant functions are used despite the restrictions listed below, no guarantee or liability will be accepted.

We have checked the contents of this DVD for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this DVD are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcomed.

Validity

Prior to each entry, you can see which device the entry applies to.

If information relates to one device, the corresponding device is named explicitly in the text. If no device is named, the information applies to all devices listed under "Validity“.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions constitute one element of such a concept. For more information about industrial security, please visit https://www.siemens.com/industrialsecurity.

2 Notes on SCALANCE XM-400 and SCALANCE XR-500

The deviations or information supplementing the product documentation in this section apply to the following products and firmware versions:

- SCALANCE XM-400 firmware as of version 6.2
- SCALANCE XR-500 firmware as of version 6.2

2.1 Entering IP addresses

Validity

- SCALANCE XM-400
- SCALANCE XR-500

Entry options

Numbers in IPv4 addresses can be entered in the CLI as follows:

- decimal
- hexadecimal (notation "0xa", results in 10 decimal)
- octal (notation "010", results in 8 decimal)

Examples

Notation	Meaning
192.168.1.0x14	192.168.1.20
192.168.1.024	192.168.1.20

2.2 PROFINET configuration with activated ring redundancy

Validity

- SCALANCE XM-400
- SCALANCE XR-500

PROFINET configuration with activated ring redundancy for devices with default settings

If you download a PROFINET configuration in which ring redundancy is activated to a device with default settings, you first need to deactivate spanning tree on the device using WBM or the CLI.

2.3 Deviating bit field coding in SNMP object

Validity

- SCALANCE XM-400
- SCALANCE XR-500

Deviating bit field coding in SNMP object "vacmViewTreeFamilyMask"

If you want to set the SNMP object "vacmViewTreeFamilyMask" via SNMP, note the following difference between the coding of the SNMP object conforming with the standard and the implementation in SCALANCE X.

Coding of the SNMP object "vacmViewTreeFamilyMask" conforming with the standard

Each bit of the bit mask is assigned to an element of the OID and specifies whether or not the element is masked.

Implementation of the SNMP object "vacmViewTreeFamilyMask" in SCALANCE X

Each byte of the octet string is assigned to an element of the OID. The last bit of every byte specifies whether or not the element is masked.

Example

OID	1.3.6.1
Mask	1.1.1.1
Coding conforming with the standard	F0
SCALANCE X coding	01.01.01.01

2.4 No optical power measurement

Validity

- SCALANCE XM-400
- SCALANCE XR-500

No optical power measurement

The devices listed do not support diagnostics by means of optical power measurement.

2.5 Configuration via STEP7

Validity

- SCALANCE XM-400
- SCALANCE XR-500

Discrepancy between firmware and configuration manual

Contrary to the information in the configuration manuals "SCALANCE XM-400/XR-500 Web Based Management" and "SCALANCE XM-400/XR-500 Command Line Interface", you cannot configure the functions "Loop Detection" and "Mirroring" via STEP7.

2.6 Description of the VLAN assignment via the name with the function "RADIUS VLAN Assignment Allowed"

Validity

- SCALANCE XM-400
- SCALANCE XR-500

Incorrect positioning of the description in the configuration manual CLI

The following description of the VLAN assignment via the VLAN name was assigned to the wrong CLI command in the configuration manual "SCALANCE XM-400/XR-500 Command Line Interface": `dot1x guest-vlan vlan-id` (section 11.7.3.3). The description belongs to the CLI command: `dot1x mac-auth vlan-assign` (section 11.7.3.10).

VLAN assignment via the VLAN name

When during authentication a port is assigned to a VLAN dynamically with the function "Adopt VLAN assignment from RADIUS" the assignment via the VLAN-ID or the VLAN name is possible. Configure the following values on the RADIUS server:

- Tunnel-Type = VLAN
- Tunnel-Medium-Type = IEEE-802
- Tunnel-Private-Group-Id = VLAN-ID or VLAN-Name

The IE switch distinguishes as follows:

- VLAN-ID: The RADIUS server transfers a numeric string for the parameter "Tunnel-Private-Group-Id".
- VLAN-Name: The RADIUS server transfers an alphanumeric string for the parameter "Tunnel-Private-Group-Id".

2.7 Security update regarding TLS

Validity

- SCALANCE XM-400
- SCALANCE XR-500

Consider TLS version for firmware updates

As of firmware version 6.1 TLS 1.0 is deactivated by default and TLS as of version 1.1 can be used. If you install a firmware version 6.1 on a device with a firmware version < 6.1, TLS 1.0 remains active and can be deactivated by issuing the following CLI command:

```
cli(config)# ip http secure minimum tls-version {v10 | v11 | v12}
```

If you restore the factory default settings on a device with a firmware version 6.1, TLS 1.0 is deactivated.

2.8 No static multicast addresses

Validity

- SCALANCE XM-400
- SCALANCE XR-500

Discrepancy between firmware and configuration manual

Contrary to the information in the configuration manuals "SCALANCE XM-400/XR-500 Web Based Management" and "SCALANCE XM-400/XR-500 Command Line Interface", you cannot insert static entries in the filter table. The WBM page "Internet Group Management Protocol (IGMP) Snooping Static" described in the documentation is not available in Web Based Management. The command "`ip igmp snooping static-group`" described in the documentation is not available in the Command Line Interface.

2.9 Configuration of the timeout for the standby connection

Validity

- SCALANCE XM-400
- SCALANCE XR-500

Discrepancy between firmware and configuration manual

Contrary to the information in the configuration manuals "SCALANCE XM-400/XR-500 Web Based Management" and "SCALANCE XM-400/XR-500 Command Line Interface", you can configure a timeout for the activation of a standby connection.

The input box "Wait for Standby Partner [ms]" is shown in the WBM menu "Layer 2 > Ring Redundancy" if the "Wait for Standby Partner" check box is cleared.

In the Command Line Interface for the command "`standby wait-for-partner`", there is an additional parameter for the duration of the timeout in milliseconds.

3 Notes on SCALANCE XB-200, SCALANCE XC-200, SCALANCE XF-200BA, SCALANCE XP-200 and SCALANCE XR-300WG

The deviations or information supplementing the product documentation in this section apply to the following products and firmware versions:

- SCALANCE XB-200 firmware as of version 4.0
- SCALANCE XC-200 firmware as of version 4.0
- SCALANCE XF-200BA firmware as of version 4.0
- SCALANCE XP-200 firmware as of version 4.0
- SCALANCE XR-300WG firmware as of version 4.0

3.1 Reset using the Primary Setup Tool

Validity

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XF-200BA
- SCALANCE XP-200
- SCALANCE XR-300WG

Reset device using the Primary Setup Tool

If you execute the command „Module > Reset“ in the Primary Setup Tool the device is not reset to the factory settings and there is no restart. The following parameters are reset:

- IP Address
- IP Assgn. Method
- System Name
- System Contact
- System Location
- PNIO Name of Station
- Ring Ports
- Ring Redundancy Mode

You can change the LLDP settings after a device restart.

3.2 RADIUS authentication and dynamic IP address assignment via DHCP

Validity

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XF-200BA
- SCALANCE XP-200
- SCALANCE XR-300WG

Problem definition

If you have activated RADIUS authentication „802.1X“ on a SCALANCE X there may be delays in the assignment of IP addresses to connected DHCP clients.

Constraints

- A DHCP client changes to an idle mode after 4 unanswered DHCP Discover frames.
- On standard PCs (e.g. Windows/Linux PC) DHCP clients remain in idle mode for approx. 3 - 7 minutes, on SCALANCE devices for 195 seconds.
- After a DHCP client has left the idle mode, it sends DHCP Discover frames again.

RADIUS authentication and DHCP

The DHCP client can only communicate with the DHCP server after the RADIUS authentication has been completed successfully on the device. If the authentication process is not completed successfully, before the DHCP client changes to the idle mode, you have the following options for obtaining a valid IP address for the DHCP client:

- Wait until the DHCP client exits the idle mode and automatically sends DHCP Discover frames again.
- Restart the DHCP client manually.

Reasons for delay of the authentication process

- The first configured RADIUS server is unreachable.
- There is a fallback to MAC authentication (only for SCALANCE XP-200).

3.3 Restoring the factory settings for certain SCALANCE XB-200 firmware updates – backing up the configuration file

Validity

- SCALANCE XB-200

Note on SCALANCE XB-200 firmware updates

If you install a firmware version ≥ 2.0.2 on a SCALANCE XB-200 with a firmware version < 2.0.2, the factory default settings will be restored. Back up the configuration file before performing the firmware update.

3.4 Security update regarding TLS

Validity

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XP-200

Consider TLS version for firmware updates

As of firmware version 3.0 TLS 1.0 is deactivated by default and TLS as of version 1.1 can be used. If you install a firmware version 3.0 on a device with a firmware version < 3.0, TLS 1.0 remains active and can be deactivated by issuing the following CLI command:

```
cli(config)# ip http secure minimum tls-version {v10 | v11 | v12}
```

If you restore the factory default settings on a device with a firmware version 3.0, TLS 1.0 is deactivated.

3.5 Additional rate limitation for unicast frames

Validity

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XF-200BA
- SCALANCE XP-200
- SCALANCE XR-300WG

Extension of the rate limitation

The following description applies additionally to the description of the rate limitation on the WBM page "Layer 2 > Rate Control" and the description of the CLI command `storm-control`.

Parameter in WBM: "Limit Ingress Unicast"
Parameter in CLI: `unicast`

Enable or disable the data rate for limiting incoming unicast frames.

3.6 Ring redundancy (client): The devices do not send VLAN tags in ring redundancy frames

Validity

- SCALANCE XC-200G
- SCALANCE XR-300WG (restricted)

Sending VLAN tags

If you configure SCALANCE XC-200G devices as MRP or HRP client, the devices do not send VLAN tags in the ring redundancy frames.

With SCALANCE XR-300WG devices, this behavior depends on the ring ports. If both ring ports are in the same group, the devices do not send any VLAN tags in the ring redundancy frames. If the two ring ports are in different groups, the devices send VLAN tags in ring redundancy frames.

Port groups with SCALANCE XR-300WG:

Group 1: P1 to P4 and P13 to P16

Group 2: P5 to P8 and P17 to P20

Group 3: P9 to P12 and P21 to P24

Group 4: P25 to P28

Ring redundancy not limited by this

This behavior has no effect on the operation of MRP and HRP rings.

3.7 Additionally supported plug-in transceivers

Validity

- SCALANCE XC-200
- SCALANCE XR-300WG

Supported plug-in transceivers

The following plug-in transceivers are supported by the above-mentioned devices. You cannot configure the plug-in transceivers with firmware version 4.0 in STEP 7 Basic and STEP 7 Professional.

Plug-in transceivers	Article number
SFP991-1 (C)	6GK5 991-1AD00-8FA0
SFP991-1LD (C)	6GK5 991-1AF00-8FA0
SFP992-1+	6GK5 992-1AG00-8AA0
SFP992-1LD (C)	6GK5 992-1AM00-8FA0

3.8 No DHCP DUID Configuration

Validity

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XF-200BA
- SCALANCE XP-200
- SCALANCE XR-300WG

Discrepancy between firmware and configuration manual

Contrary to the information in the configuration manual "SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Web Based Management" you cannot configure the following functions on the WBM page "System > DHCP > DHCP Client":

- DHCP Mode: via Iaid and Duid
- DUID-Type
- Link-layer Address Plus Time
- Vendor Enterprise Number
- Link-layer address
- Table: IAID Value

3.9 Availability of SCALANCE XR-300WG in STEP 7

Validity

- SCALANCE XR-300WG

Availability in STEP 7

As of the following versions the SCALANCE XR-300WG devices are available in STEP 7:

- STEP 7: As of V5.6
- STEP 7 Basic or Professional: As of V15

3.10 Configuration of trunk ports in private VLANs

Validity

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XF-200BA
- SCALANCE XP-200
- SCALANCE XR-300WG

Trunk ports in private VLANs

When you configure a port as trunk port, the port automatically becomes a member of all VLANs, including private VLANs. No data traffic is possible via a trunk port that is a member of a private VLAN.

For this reason, configure for a trunk port all private VLANs as forbidden (F).

In the WBM, navigate to the page "Layer 2 > VLAN > General" and select the entry "F" in the list of the ports for the trunk ports.

Change to the corresponding VLAN configuration mode in the CLI and define all port configurations of this VLAN including the forbidden ports with the command `ports`.

3.11 Limitation of the availability of the "Provider Bridge" function

Validity

- SCALANCE XF-200BA

Deviation from the information in the configuration manuals

Contrary to the information specified in the "SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Web Based Management" and "SCALANCE XB-200/XC-200/XF-200BA/XP-200/XR-300WG Command Line Interface" configuration manuals, the "Provider Bridge" function is not available for the SCALANCE XF-200BA devices.

4 Notes on SCALANCE X-200IRT

4.1 Note regarding the firmware downgrade of SCALANCE X-200IRT modules

Validity

- SCALANCE X-200IRT

The firmware version V3.1.4 may only be used to downgrade the following modules:

Device	Article number
SCALANCE X204IRT	6GK5 204-0BA00-2BA3
SCALANCE X202-2IRT	6GK5 202-2BB00-2BA3
SCALANCE X202-2P IRT	6GK5 202-2BH00-2BA3
SCALANCE X201-3P IRT	6GK5 201-3BH00-2BA3
SCALANCE X200-4P IRT	6GK5 200-4AH00-2BA3

The firmware version V2.0.25 may only be used to downgrade the following products:

Device	Article number
SCALANCE X204IRT	6GK5 204-0BA00-2BA3
SCALANCE X202-2IRT	6GK5 202-2BB00-2BA3

Document Identification number: C7900-G8974-C347-21