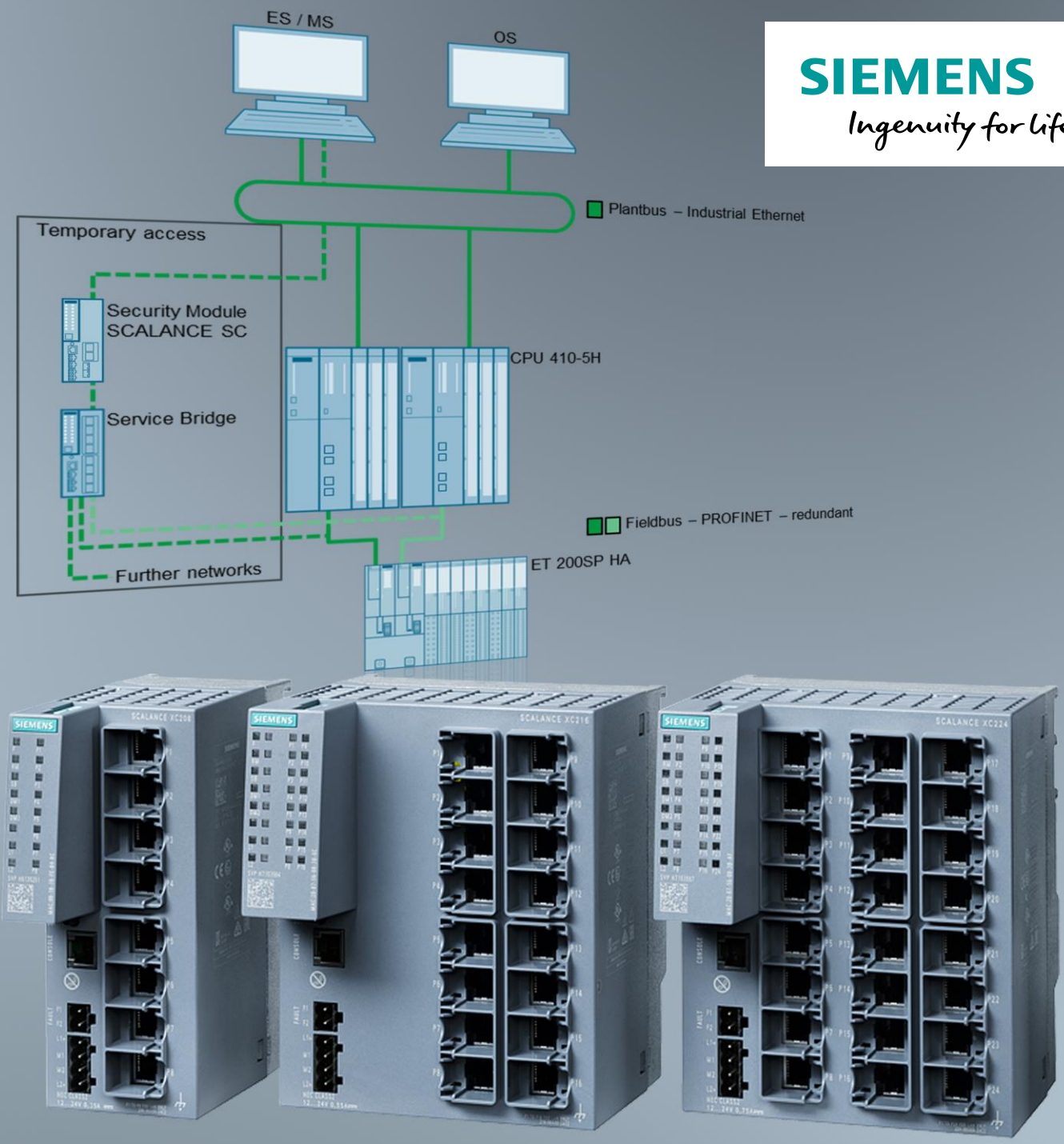


SIEMENS
Ingenuity for life

Service Bridge Setup and Configuration

SCALANCE XC-200

https://support.industry.siemens.com/cs/ww/en/view/109747975

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG (“Siemens”). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.
By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
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.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit **Fehler! Linkreferenz ungültig.**.
Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer’s exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Table of contents

1 Task and solution

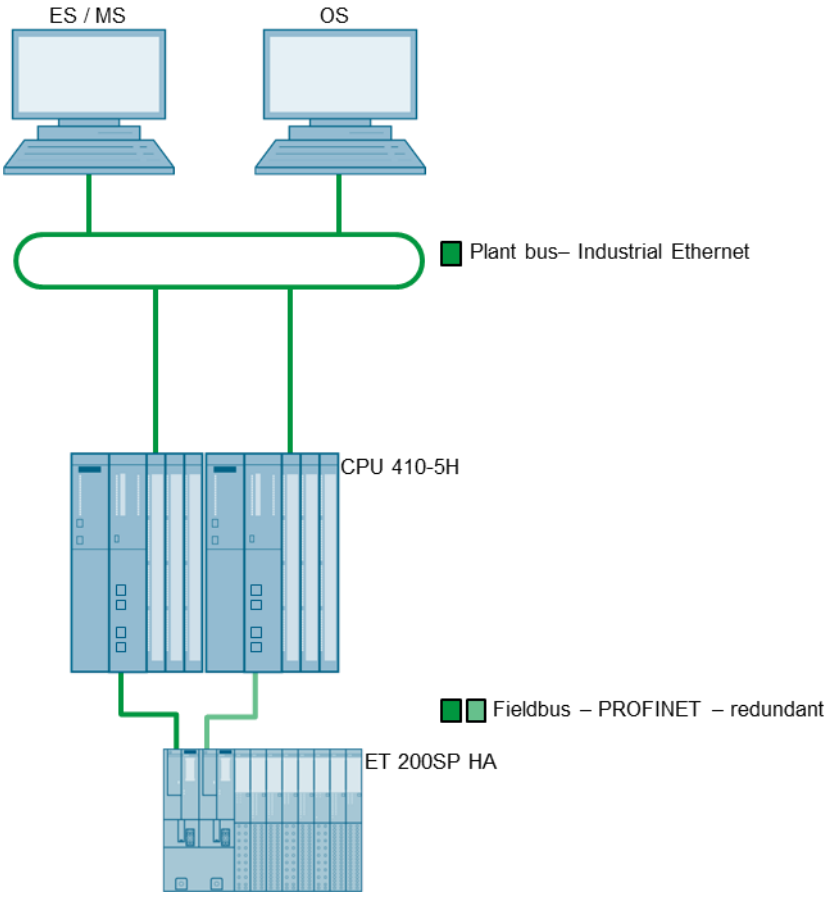
1.1 The task

The use of PROFINET as fieldbus opens up new possibilities for commissioning, maintenance and diagnostics in SIMATIC PCS 7 systems. The uniform Industrial Ethernet network standard forms the basis for vertical integration.

For security and availability reasons, plant bus and field bus are set up separately in typical systems in the process industry. This means that only limited access to the fieldbus is possible from the Engineering Station (ES) or Maintenance Station (MS), e.g. via data set routing by the CPU. Functions such as the manual node initialization of PROFINET devices (device naming) or topology scan with the topology editor are thus not available. Consequently, an access point is required to enable access from the ES to the field bus.

A simple topology of a PCS 7 plant with PROFINET is shown schematically in the following figure.

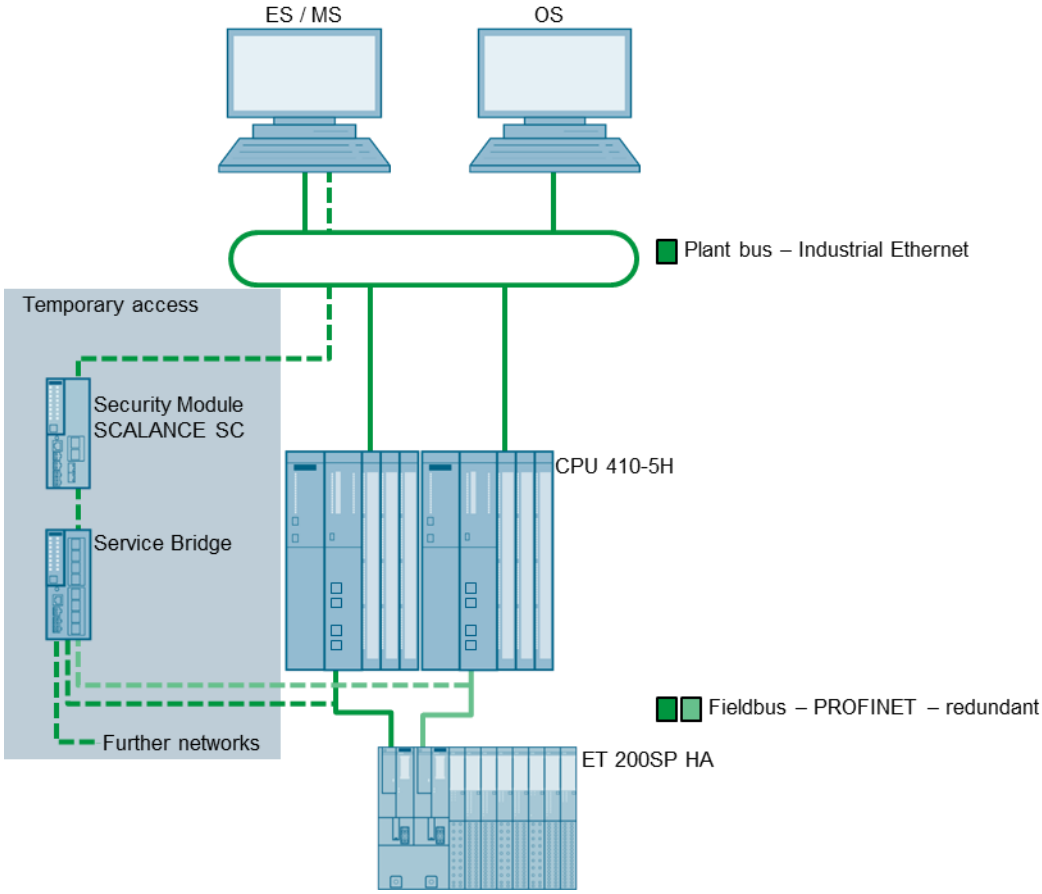
Figure 1-1



1.2 Solution

The solution to enable temporary access from the ES to the PROFINET fieldbus is the Service Bridge. This is a specially configured switch that enables dedicated temporary access from the plant bus to the fieldbus while ensuring logical separation between the fieldbuses. For security reasons, it is also recommended that a firewall, e.g. in the form of a SCALANCE SC, be provided between the plant bus and the service bridge.

Figure 1-2



The basis for the Service Bridge are the switches of the SCALANCE XC-200 series from FW V4.0.
This application example uses the SCALANCE XC216 as an example to describe the steps required to configure a SCALANCE XC-200 switch as a service bridge.
To facilitate configuration, this article also provides a prepared configuration file for download.

Benefits

- Manual addressing and naming of PROFINET devices
- Use of the scan/online functions of the STEP 7 topology editor
- Use of commissioning tools (e.g. PRONETA)
- Extended network diagnostics (e.g. SINEMA server)
- Access to the web servers of the PROFINET devices (project planning and diagnostics)
- Installation of firmware updates
- Access to up to 23 separate PROFINET subnets with XC224

1.3 Hardware and software components

The application example was created with the following components:

Hardware

Table 1-1

Hardware	Part number
SCALANCE XC216	6GK5216-0BA00-2AC2
SCALANCE SC632-2C	6GK5632-2GS00-2AC2

Software

Table 1-2

Software	Link
PRONETA	https://support.industry.siemens.com/cs/ww/en/view/67460624
Internet Explorer	

2 How the service bridge works and how to use it

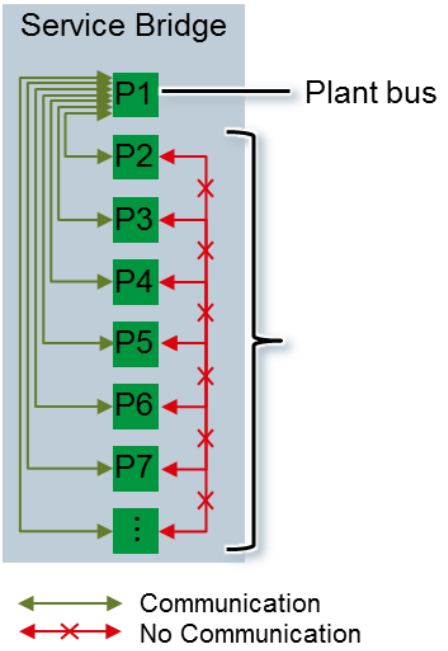
2.1 Ports

The basis for the functionality of the service bridge are the switches of the XC-200 series with a special configuration. These switches have between 8 (XC208) and 24 ports (XC224).

Regardless of the number of ports, the Service Bridge is connected to the plant bus (plant bus) via port 1. Integration into a plant bus ring is not planned.

The remaining ports are available for the PROFINET networks. In the case of the SCALANCE XC224, access to up to 23 separate PROFINET networks is possible. The separation between the networks is ensured by a VLAN configuration.

Figure 2-1



Note

Access from the plant bus to the individual PN networks should only be temporarily active and can be implemented by activating/deactivating the ports via the Web Based Management (WBM) of the service bridge, see chapter 2.1.1. If continuous access to the PROFINET fieldbus is required, we recommend using a service bridge separate from the plant bus, see chapter 6.1.

CAUTION	**When resetting the service bridge to factory settings, the configuration for network separation is lost. Therefore, disconnect all connections to the PROFINET networks before resetting.**

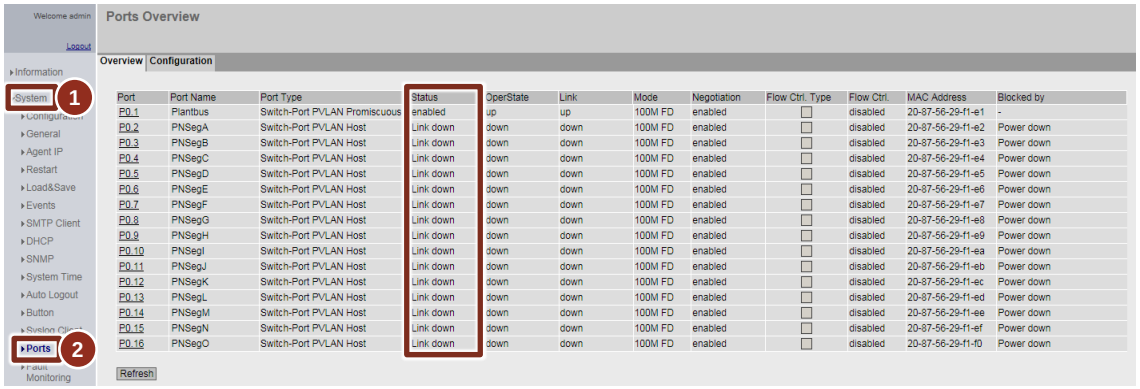
2.1.1 Enabling/disabling ports

Access from the plant bus to the individual PN networks should only be active temporarily and can be realized by activating/deactivating the ports via the Web Based Management (WBM) of the service bridge. Ports that are not required must be deactivated with the "Link down" function.

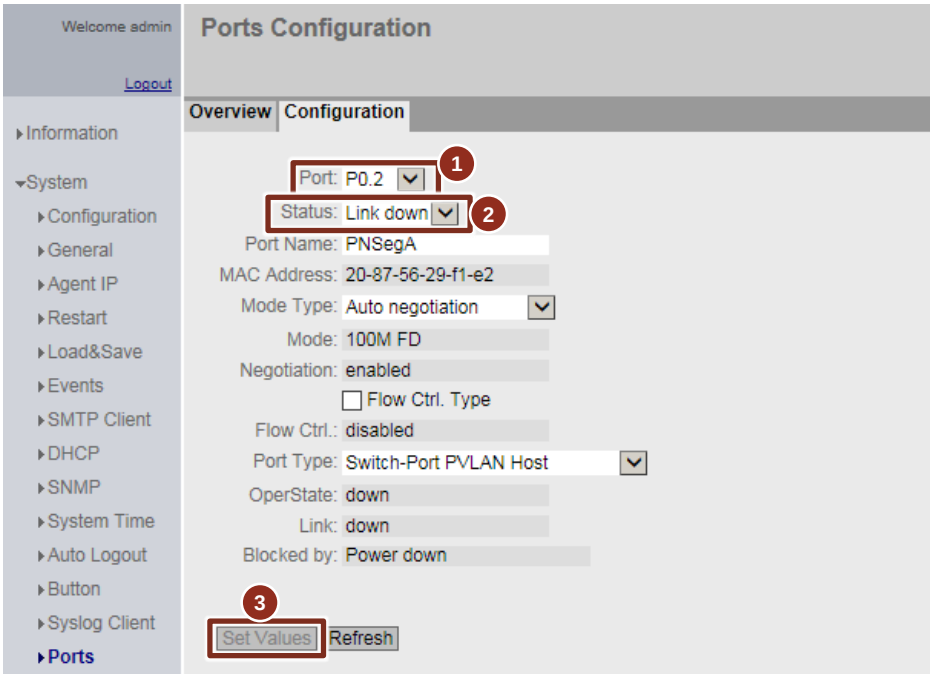
Procedure

1. Use the IP address of the service bridge to call Web Based Management in your browser.
2. Log on as Administrator.
3. Navigate to the menu "System > Ports" (1)(2). The overview now displayed shows, among other things, the current status of the ports:

Figure 2-2



4. Switch to the "Configuration" tab.
5. After selecting a port (1), you can activate or deactivate it by selecting the status (2). Use the status "enabled" for activation and the status "Link down" for deactivation.
   Click the "Set Values" button (3) to confirm the settings.



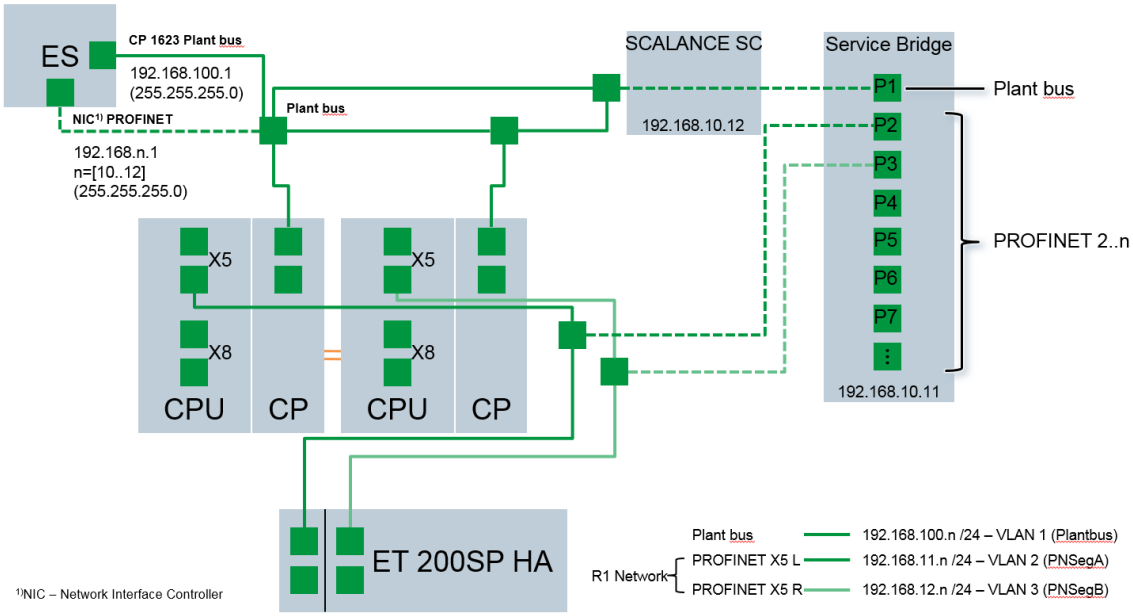
Note The "Link down" port status is used for deactivation, as it is retained even after a device restart. If the port status is "disabled", please note that this is set to "enabled" again after a device restart using the "Loop Detection" function.

2.2 Separate Network adapter and IP addresses

The service bridge enables direct Ethernet access (ISO Layer 2 - MAC level) from the plant bus to subordinate PROFINET networks.
For ISO Layer 3 access (IP) to the different subnets, an IP address multihoming on the ES is required. IP addresses Multihoming means that a device has several network addresses. For this purpose, a separate network card (NIC - Network Interface Controller) is recommended at the Engineering Station (ES). Several IP addresses are assigned to this network card according to the PN networks to be accessed.

The following example shows how it works:

Figure 2-3



The ES has a CP 1623 for communication on the plant bus. This is configured with the IP 192.168.100.1 (255.255.255.0) and is used for loading the CPU, among other things.

In addition to the CP 1623, a second network card (NIC) is available in the ES for accessing the PROFINET networks. The NIC for PROFINET has three IP addresses:

- 192.168.10.1 (255.255.255.0): for access to the Web Based Management (WBM) of the Service Bridge and access to the SCALANCE SC
- 192.168.11.1 (255.255.255.0): for access to the PN network at Port 2 of the Service Bridge
- 192.168.12.1 (255.255.255.0): for access to the PN network at Port 3 of the Service Bridge

Note To prevent communication problems caused by duplicate IP addresses, we recommend using different IP address ranges in all subordinate PROFINET networks.

Note Optionally, the plant bus can also be structured with VLANs to logically separate communication for service bridge access from process communication.
Further information on configuring VLANs can be found in the following FAQ:
"How is a Virtual Local Area Network (VLAN) configured in PCS 7?"
https://support.industry.siemens.com/cs/ww/en/view/66807297

2.3 A firewall using the example of a SCALANCE SC

It is recommended to use a firewall between the Service Bridge and the plant bus in order to protect the plant bus against unauthorized accesses from the field. This firewall must be able to operate as a Stateful Inspection Firewall, i.e. to check packages depending on their state. It must also support bridge mode for operation in flat networks, where external and internal interfaces are located on the same IP subnet.

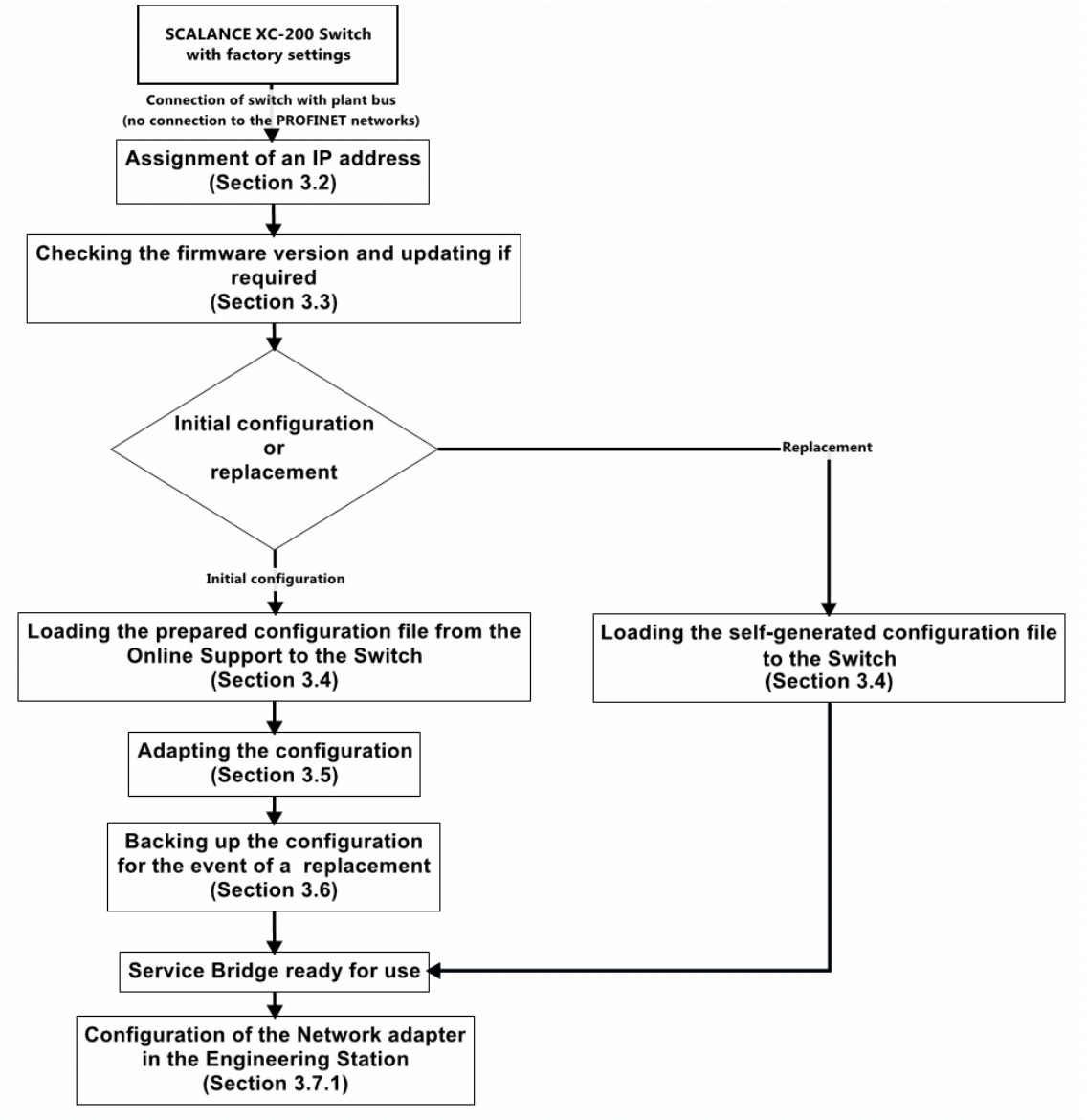
The firewall must be configured in such a way that it only allows communication that is initiated by selected sources in the plant bus (e.g. the ES). This means that the firewall allows the ES communication at any time but only allows devices from the field bus to respond to message frames by the ES. Communication that is initiated by devices from the field bus is blocked by the firewall.

This functionality can, for example, be implemented by the Security Modules of the SCALANCE SC600-series from the firmware version V2.0. Instructions for configuring the firewall using the example of a SCALANCE SC632-2C can be found in chapter 5.

3 Configuration and commissioning of the Service Bridge

The following steps are necessary in order to configure a SCALANCE XC-200 switch to a Service Bridge:

Figure 3-1



These steps can be carried out either in a separate network or directly on the plant bus using the switch. In both cases, the switch is accessed via port 1.

CAUTION	**Connect the PROFINET networks to the Service Bridge only after the configuration steps are completed. Otherwise the network separation will not be maintained.**

3.1 Preparing the switch

A prerequisite for the proper configuration of the Service Bridge is that the XC-200 Switch is initially in the as-supplied state, i.e. reset to factory settings. In addition, at least firmware version V4.0 is required for the service bridge configuration.
In section 3.3 of this manual, you can find information on how to check the firmware version and carry out any updating that may be required.

Restoring to factory settings

If the Switch is not in the as-supplied state, it can be reset to factory settings with the "SELECT/SET" button. If the "SELECT/SET" button is disabled, this can only be done during device startup.

1. Power down the device.
2. Now press the "SELECT/SET" button and reconnect the voltage supply to the device while holding down the button.
3. Keep the button pressed until the red "F" fault LED stops flashing and switches to continuous light.
4. Release the button and wait for the "F" fault LED to go out again.
5. The device restarts automatically with factory settings.

Note

You can download the pre-set configuration file at the following link:
https://support.industry.siemens.com/cs/ww/en/view/109747975

The download of firmware version V4.0 can be found under the following link:
https://support.industry.siemens.com/cs/ww/en/view/109757688

3.2 Assigning an IP address

An XC-200 switch that is reset to factory settings has no network parameters (IP address/name). To access Web Based Management (WBM) in later steps, an IP address must be assigned to the switch that is to be used as a service bridge.

There are several ways to assign an IP address to an unconfigured device:

- DHCP
- PRONETA
- SINEC PNI (Primary Network Initialization)
- STEP 7 - SIMATIC Manager
- CLI (Command Line Interface) via the serial interface

Note

For the Service Bridge, it is recommended to assign an IP address from a IP address range other than that of the plant bus.

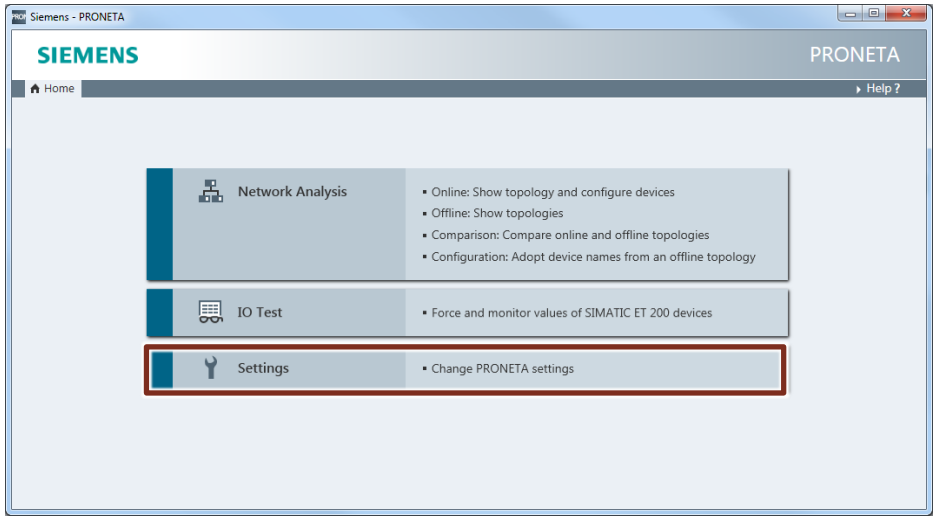
Addressing with PRONETA

The procedure for addressing with the PRONETA tool (free of charge) is described in the following section. A requirement for addressing the switch is that it must be accessible in the network.

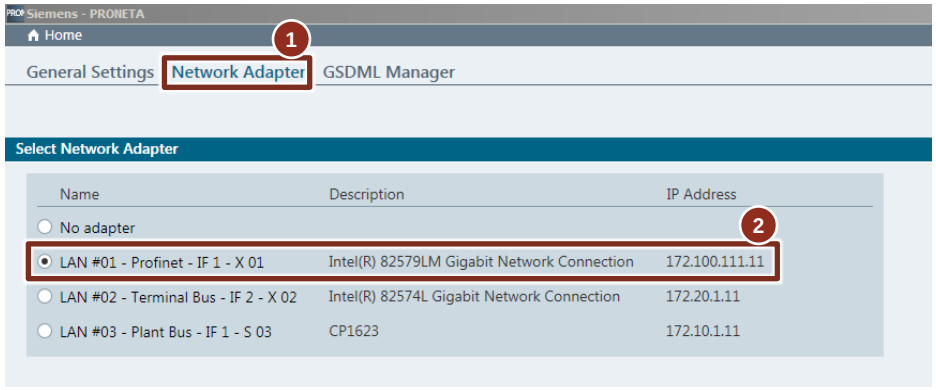
Note

Download and manual
"PRONETA Commissioning and Diagnostics Tool for PROFINET"
https://support.industry.siemens.com/cs/ww/en/view/67460624

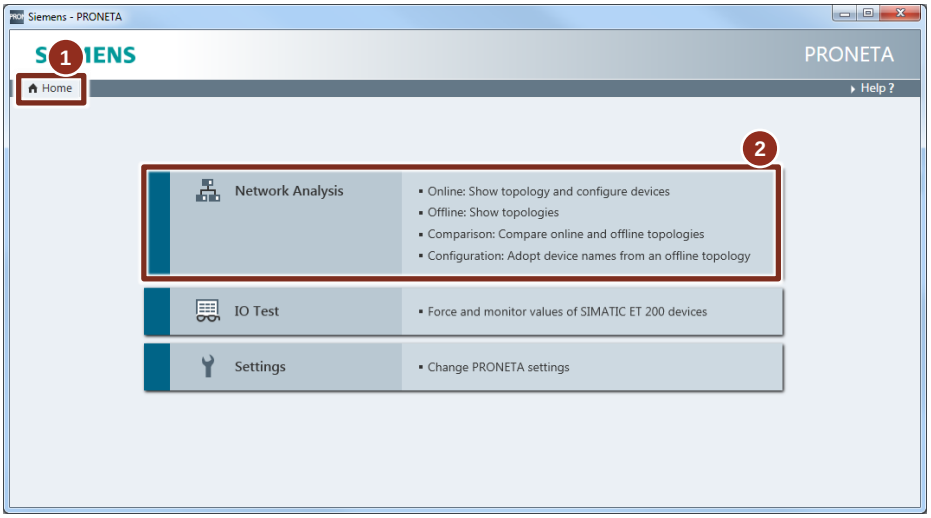
1. Open PRONETA and click on "Settings".



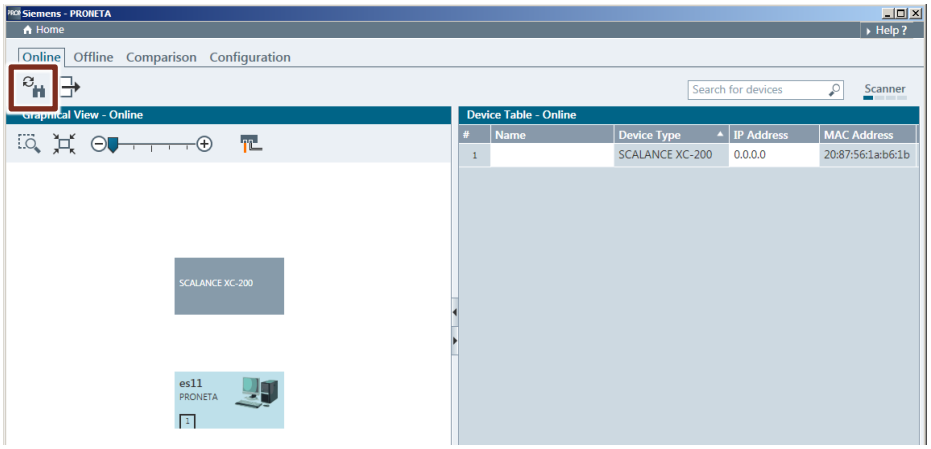
2. Click on "Network Adapter Selection" (1) and select the network adapter with which the switch can be accessed (2).



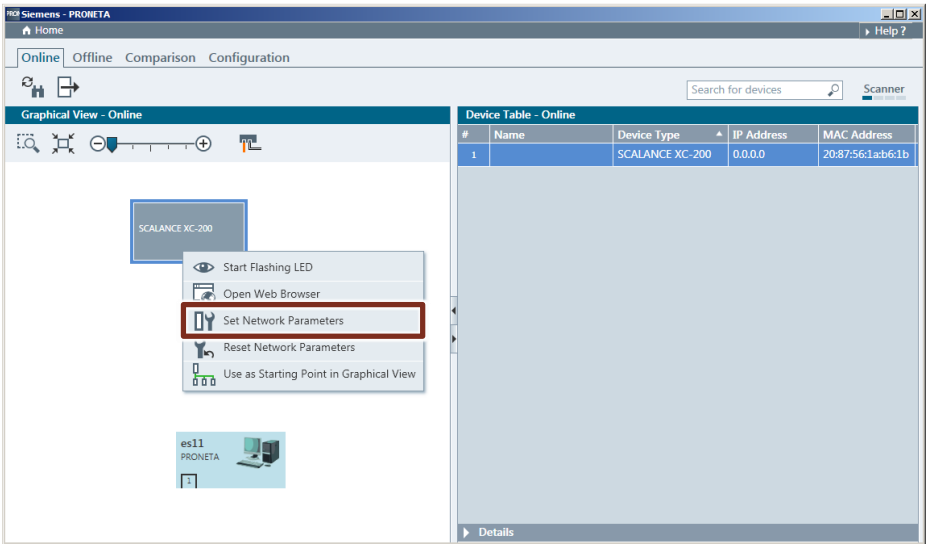
3. Click on "Home" (1) and then click on "Network Analysis" (2) to open the network analysis view.



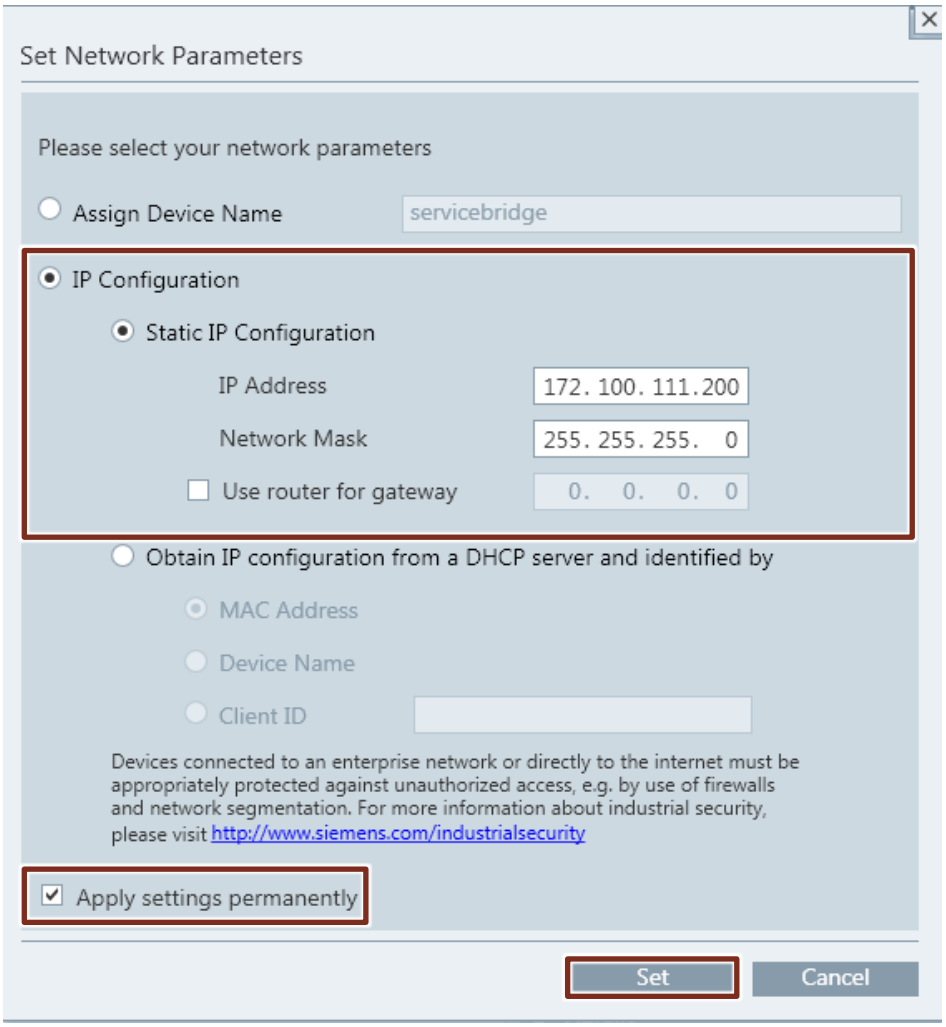
4. After opening the network analysis view, a scan is automatically performed. The SCALANCE XC-200 switch is then listed in the graphic and tabular view. If the switch is not found, you can perform another scan using the "Refresh" button.



5. Open the shortcut menu by right clicking on the switch and then click on "Set Network Parameters". Optionally, you can use the "Start Flashing LED" function in the shortcut menu to make sure that you have selected the correct switch.

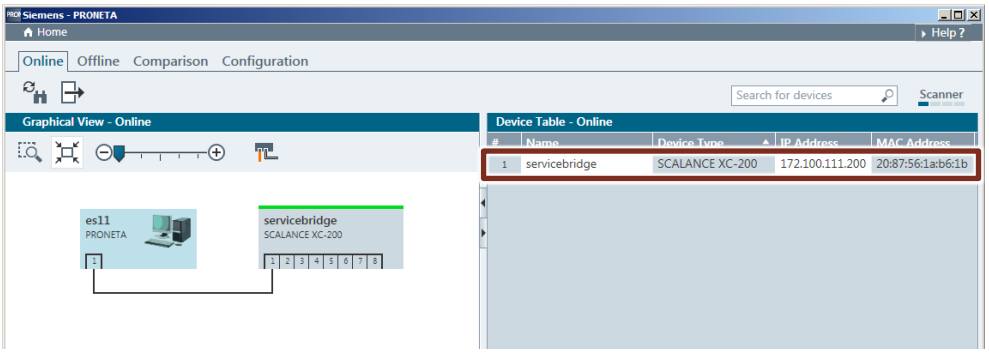


6. You can also assign the IP address and optionally a device name via the "Set Network Parameters" dialog.
   Enter the desired IP address and subnet mask. Check whether the "Apply settings permanently" check box is enabled and then click on "Set" to assign the network parameters.



After assigning the IP address, it is displayed by PRONETA in the tabular view. The Web Based Management (WBM) function of the switch can now be accessed via this IP address.

Figure 3-2



3.3 Checking the firmware version and updating it if required

Firmware version V4.0 or higher is required to load the Service Bridge configuration file.

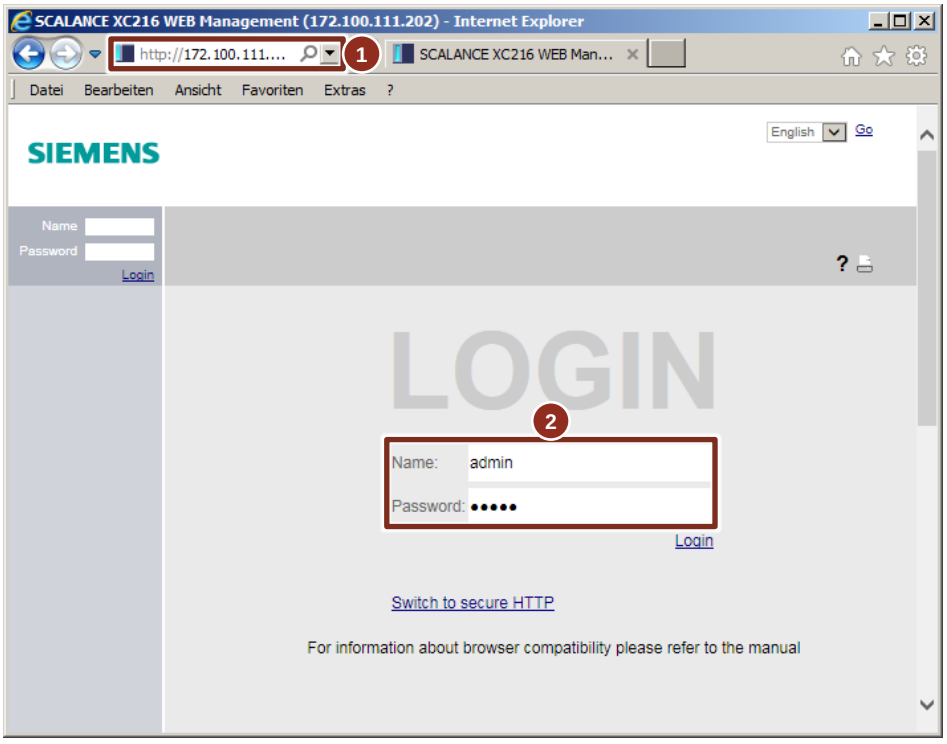
Note

Download Firmware V4.1
The firmware V4.1 can be downloaded from the following link:
https://support.industry.siemens.com/cs/de/en/view/109762982

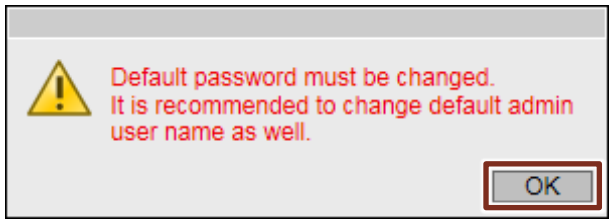
The Web Based Management (WBM) of the switch is used for checking the firmware version and updating the firmware if necessary. To access the WBM, the ES must have an IP address in the same IP address range of the Service Bridge.

Opening WBM and logging on

1. Start Web Based Management by typing the IP address of the Service Bridge in your browser (1).
2. Log on as Administrator. The default login details for the administrator are as follows:
   - User: "admin"
   - Password: "admin"



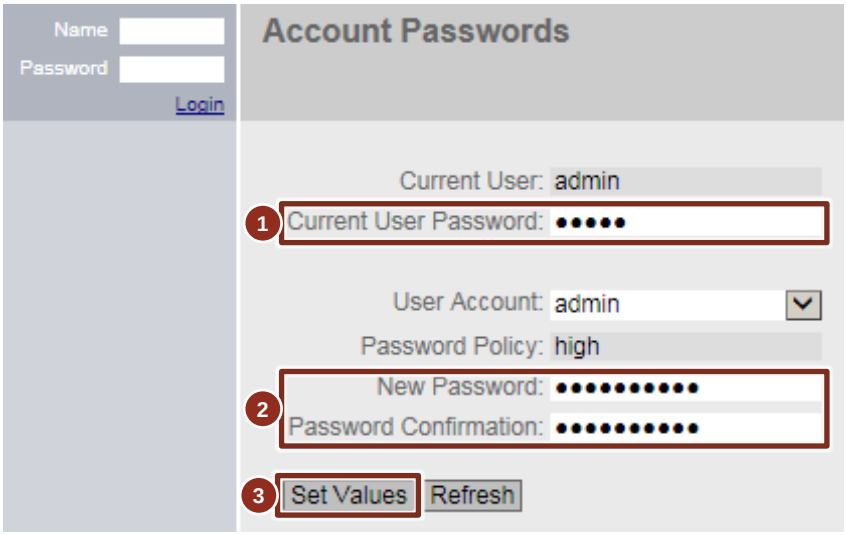
3. After the first login a message appears that the default password must be changed. Confirm the message with "OK".



Changing the password

After the first login, a prompt will ask you to change the default password of the admin user.

1. Enter the current password (1).
2. Enter a new password (2).
3. Click the "Set Values" button (3) to confirm the settings.



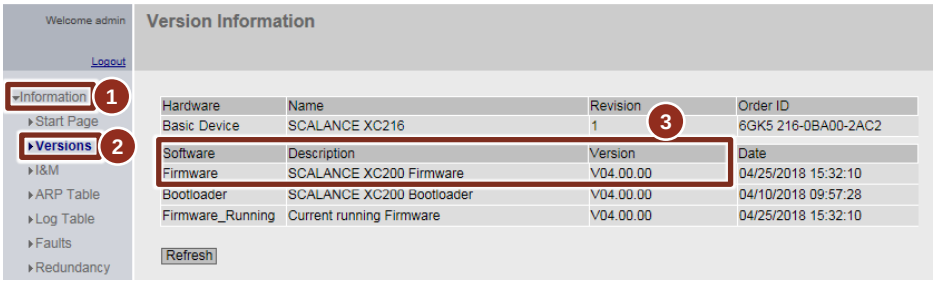
Note

The new password must conform to the following guidelines:

- Password length: a minimum of 8 characters, a maximum of 128 characters
- At least 1 upper case letter
- At least 1 special character
- At least 1 digit

Checking the firmware version

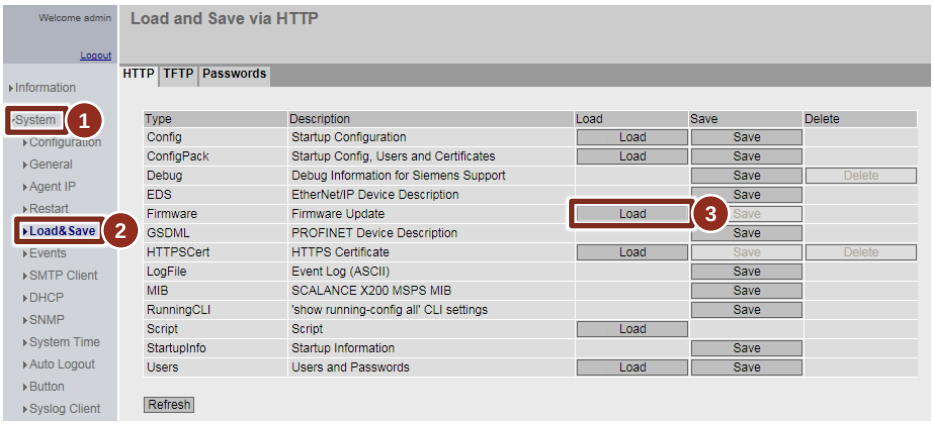
1. Navigate to the "Information > Versions" menu (1)(2).
2. Check whether the firmware version is at least V4.0 ("V04.00.00") (3).



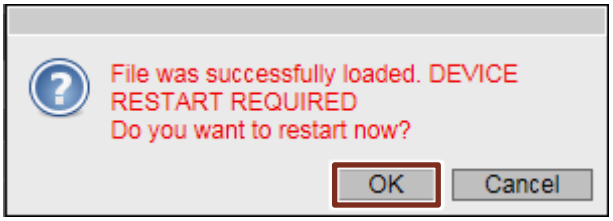
Updating the firmware version

If the firmware version of the switch is lower than V4.0, follow the steps below to update the firmware:

3. Navigate to the "System > Load&Save" menu (1)(2).
4. Click on the "Load" button (3).



5. A dialog box for uploading the firmware file opens. Select the firmware file and upload it.
6. After successfully uploading the firmware, the Service Bridge needs to be restarted.
   Confirm the restart dialog by clicking on "OK".



3.4 Loading the configuration file in the Switch

To facilitate the configuration of the Service Bridge, a pre-set configuration file is provided for download on the article page of this Application Example. By loading this configuration file, the switch acquires the settings described in Section 4 and thus the basic functionality of the Service Bridge. Subsequently, system-specific adjustments have to be made by hand – see Section 3.5.

If you have already configured the Service Bridge and replaced the switch (in the case of a parts replacement, for instance), you can restore the configuration with the self-generated configuration File. The plant-specific adaptations are already included in it.

Note You can download the pre-set configuration file at the following link: https://support.industry.siemens.com/cs/ww/en/view/109747975

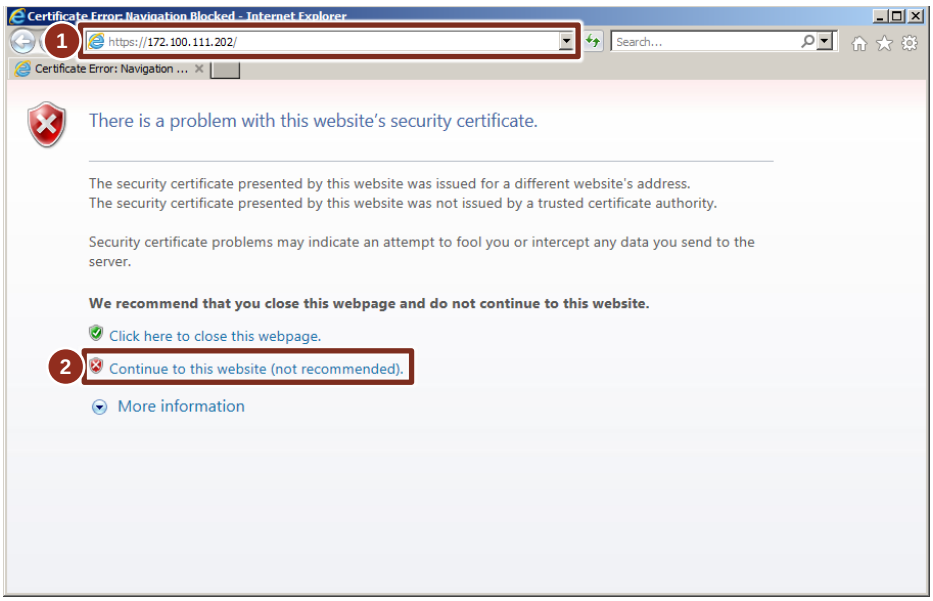
The configuration of the Service Bridge is loaded to the Switch via Web Based Management (WBM).

The WBM can only be accessed via HTTPS after loading the configuration because HTTP access is disabled. For this reason we recommend using HTTP to connect before loading the configuration file.

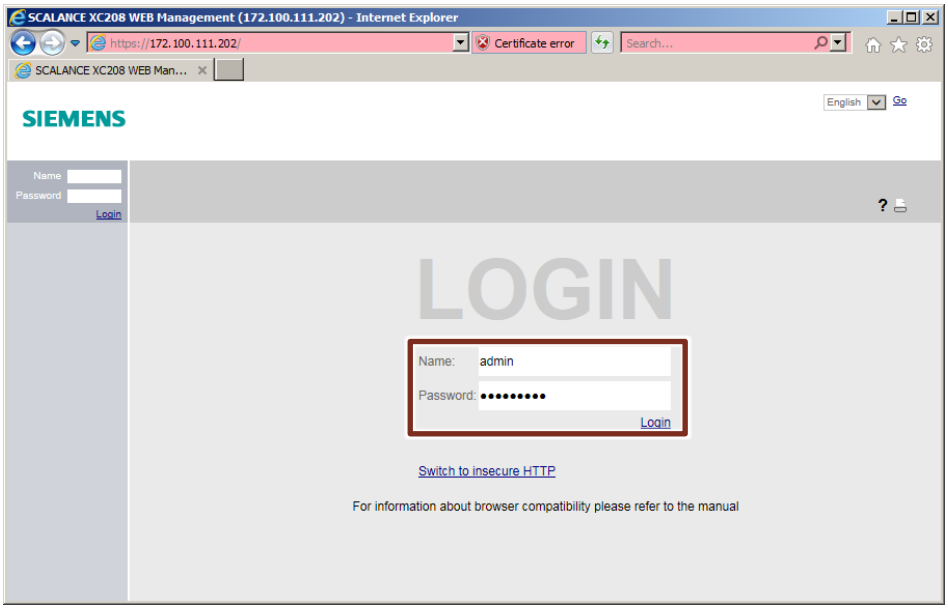
Access via HTTPS

To access the WBM via HTTPS, enter the IP address in the browser, placing "https://" before it.
For example: https://172.100.111.202/

7. Start Web Based Management via HTTPS in your browser (1).
8. Confirm the certificate warning that appears (2). The certificate warning is shown because the default HTTPS certificate is not trusted.



9. Log on as Administrator.



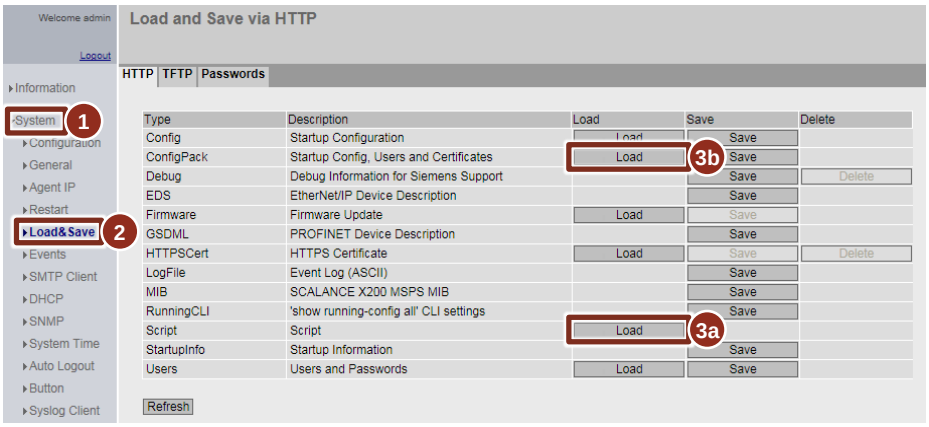
Note

An automatically generated HTTPS certificate, including a key, is provided by default on the switches. To prevent the certificate warning appearing, it is possible to install it on the engineering station.

It is recommended to create and use your own HTTPS certificates. These can be uploaded to the switch via the menu
"System > Load&Save" in the same way as the configuration script.

Loading a configuration

10. Navigate to the "System > Load&Save" menu (1)(2).
11. If you are using the pre-set configuration script file from the Online Support, click on the "Load" button (3a).
    If that you are using a self-generated configuration file (ConfigPack), click on the "Load" button (3b).



12. A dialog window opens to upload the configuration file. Select the configuration file, and upload it.
13. A message appears after successfully loading the configuration file. Confirm this by clicking on "OK"

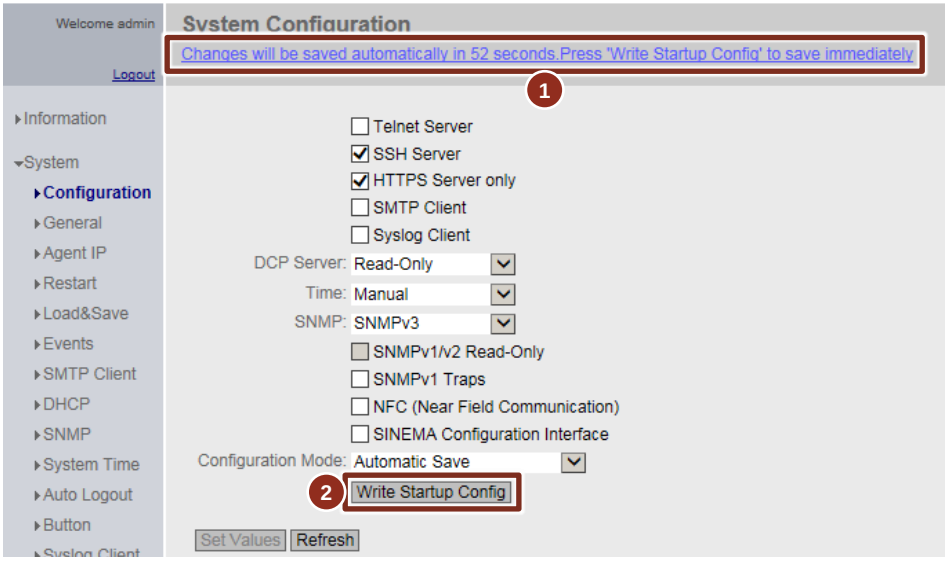
Some of the Service Bridge settings are active immediately after successfully uploading the configuration file, however you still need to restart the Service Bridge for all the settings to become effective. This must be carried out manually and can be performed via the WBM. The WBM can only be accessed via HTTPS after loading the configuration because HTTP access is disabled.

Note Configuration files (ConfigPacks) created for spare parts can only be uploaded to identical devices (same MLFB).

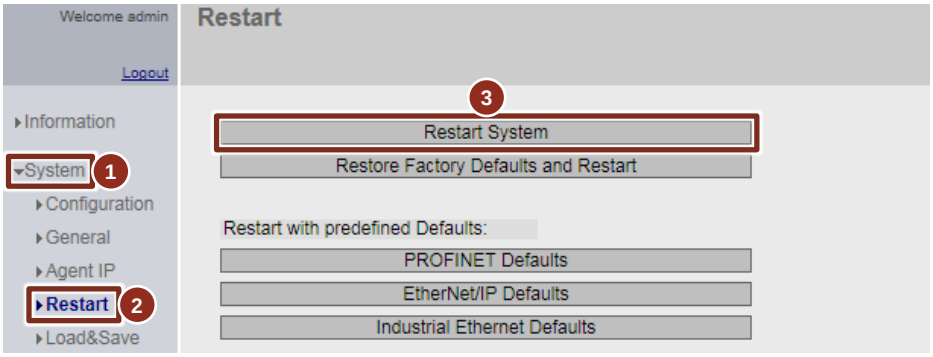
Performing a restart

Before restarting the service bridge, the "Write Startup Config" must be completed. "Write Startup Config" is performed automatically 60 seconds after configuration changes, but can alternatively be performed manually.

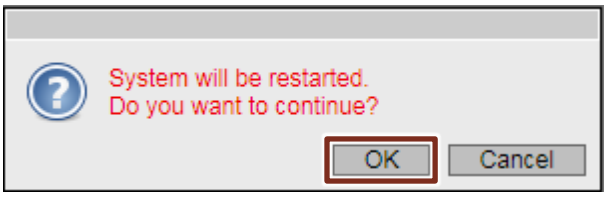
14. If the 60 seconds have not elapsed after changing the configuration, this is indicated by the following message
    "The changes are automatically saved in x seconds. To save the changes immediately, click 'Write the start configuration'.".
    ("Changes will be saved automatically in x seconds. Click "Write Startup Config", to save immediately.) (1).
    Wait until the time has expired or click on the "Write Startup Config" button (2) to save the configuration immediately.



15. Navigate to the "System > Restart" menu (1)(2).
16. Click on the "Restart System" button (3) to reboot the system.



17. Confirm the restart dialog by clicking on "OK".



3.5 Adjusting the configuration

3.5.1 Unicast filter

A Unicast filter is provided for the Service Bridge; it allows access to the plant bus only for selected stations, e.g. the engineering station. As this configuration is plant-specific due to the MAC address, the Unicast filter is not included in the pre-set configuration file. It has to be configured later.

Note

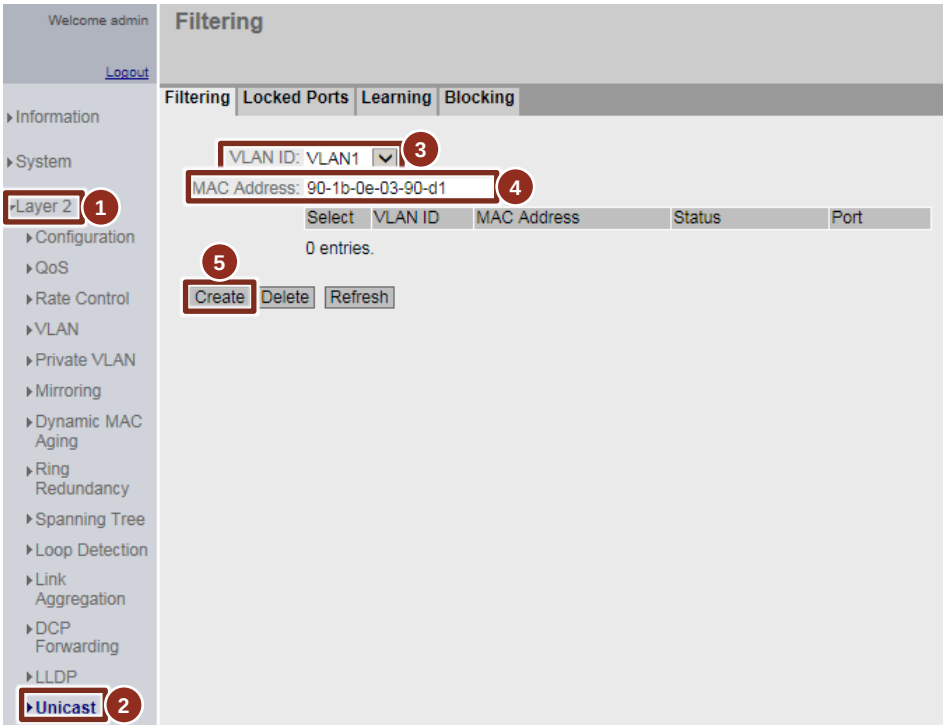
You can determine the MAC address of the network adapter, e.g. via the command prompt (CMD) using the command "ipconfig/all".

Information about all network adapters is displayed.
In the following, the MAC address of the network card is required to access the PROFINET networks.

Generating an entry in filter table

The Unicast filter works through a filter table that contains all the permitted MAC addresses. The MAC address of the ES, i.e. that of the separate network adapter for the PROFINET networks, must be entered in this table.

1. Navigate to the "Layer 2 > Unicast" menu (1)(2).
2. Select the VLAN ID "VLAN 1" (3) and enter the MAC address of the separate network adapter (4).
   Click on the "Create" button (5) to create the entry.



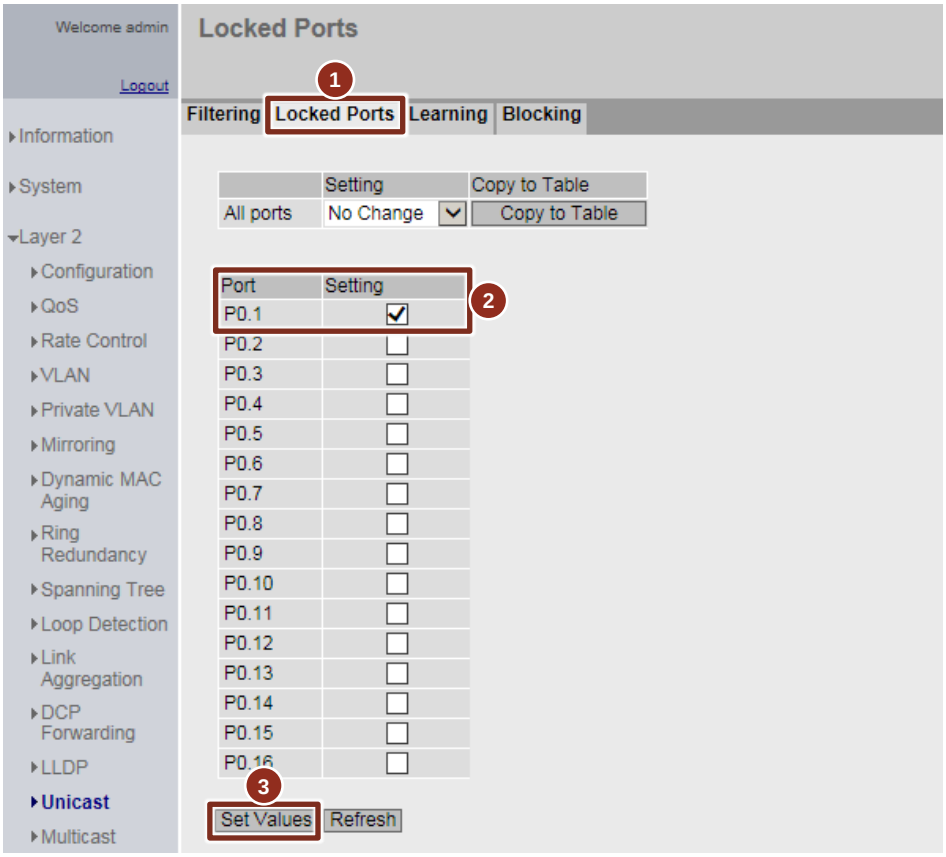
Note

When replacing the Engineering Station or the network card for access to the PROFINET networks, the entry in the filter table must be adapted accordingly.

Activating the Unicast filter

The Unicast filter for the plant bus (port 1) can be activated after entering the MAC address of the ES in the filter table. From then on, all message frames from unknown participants on Port 1 will be rejected.

1. Switch to the "Locked Ports" (1) tab.
2. Enable the check box for Port 1 (2).
   Click the "Set Values" button (3) to confirm the settings.



CAUTION	**Activate the Unicast filter only after you have entered the MAC address of the engineering station in the list of known participants. Otherwise, you may block the only access of the Service Bridge to the WBM. If this happens, it will only be possible to deactivate the filter via the serial interface using CLI, or to reset the Service Bridge to the factory settings with the "SELECT/SET" button after the system has been de-energized.**

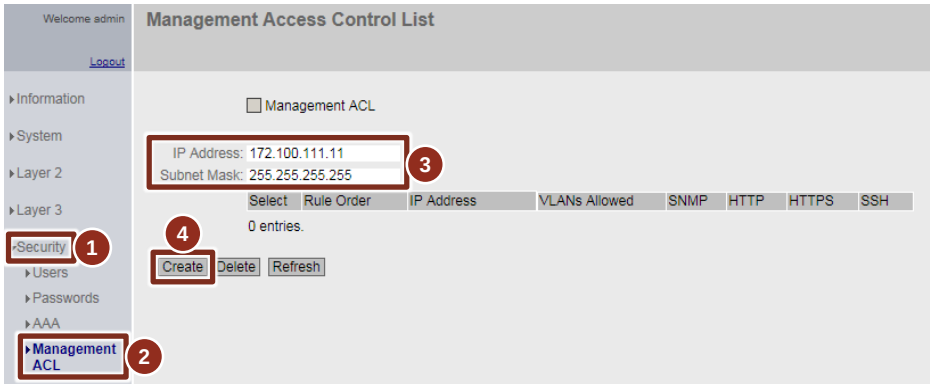
3.5.2 ACL management

Access control to the Service Bridge management is configured by means of the Management ACL (Access Control List) function. A filter is provided for the Service Bridge; it only allows access from the engineering station. As this configuration is plant-specific due to the IP address, the Management ACL configuration is not included in the pre-set configuration file. It has to be configured later.

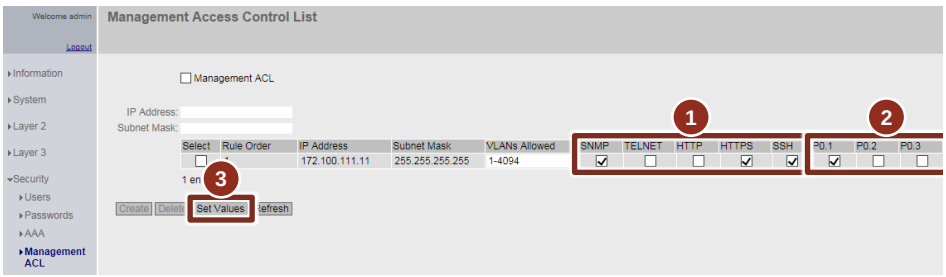
To access the service bridge, the Engineering Station must have an IP address in the same address range as the service bridge. This must be entered in the Management ACL list.

Generating an entry in the filter table

1. Navigate to the "Security > Management ACL" menu (1)(2).
2. Enter the engineering station IP address in the entry field (3).
3. Enter "255.255.255.255" as the subnet mask (3). This subnet mask restricts access to the IP address that has been entered. In other subnet masks, access is enabled for the entire address range.
4. Click on the "Create" button (4) to create the entry.



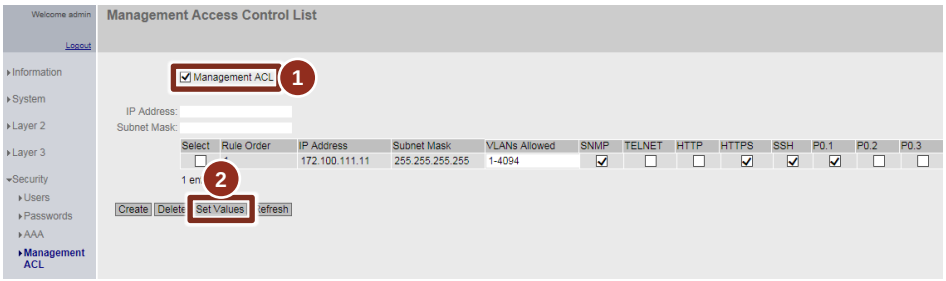
5. Only certain protocols are permitted access from this IP address (1).
   - Enable SNMP, HTTPS and SSH.
   - Disable TELNET and HTTP.
6. Access to plant bus (Port 1) is also restricted (2).
   - Enable Port 1.
   - Disable all other ports.
7. Click the "Set Values" button (3) to confirm the settings.



Activating Management ACL

The Management ACL function can be activated after the ES has been entered into the Management ACL list.

1. Activate the "Management ACL" check box (1).
2. Click the "Set Values" button (2) to confirm the settings.



CAUTION	**Activate the management ACL function only after you have entered the engineering station in the list. Otherwise, you may block the access to the WBM of the Service Bridge.** **If this happens, it will only be possible to deactivate the filter via the serial interface using CLI, or to reset the Service Bridge to the factory settings with the "SELECT/SET" button after the system has been de-energized.**

3.5.3 SNMP

The Simple Network management Protocol (SNMP) allows network components, such as the Service Bridge, to be monitored and controlled.

For security reasons, only SNMP version 3 is enabled in the configuration of the Service Bridge. The SNMPv1/v2c versions are disabled. If you require the SNMP versions v1 or v2c, for instance for the integration as a network component in the asset management of the Maintenance Station, please refer to Section 6.3 for further information.

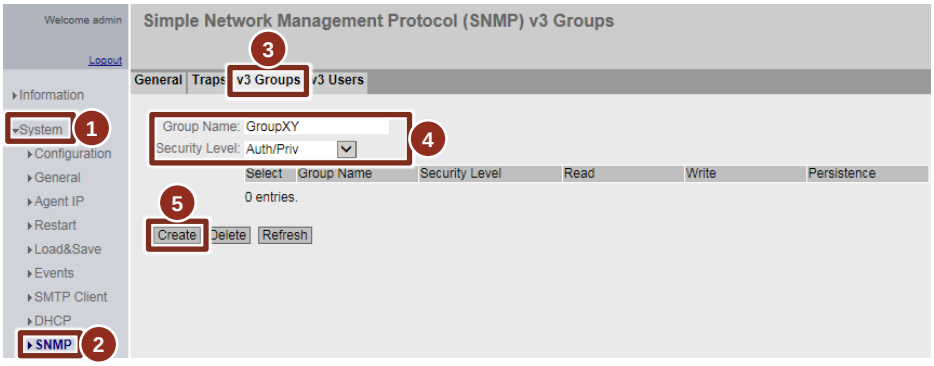
SNMP version 3 provides rights management, authentication, and encryption features based on SNMP v3 groups and users.

The pre-set configuration file does not contain any SNMP v3 groups and users. These must be created at a later stage if access is required to the Service Bridge via SNMP.

Creating an SNMP v3 group

The security level and read/write permissions are assigned according to groups. The section below shows you how to create a new SNMP v3 group with read and write permissions.

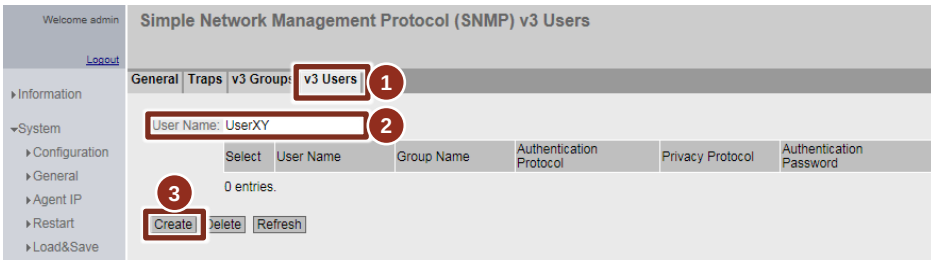
18. Navigate to the "System > SNMP" menu (1)(2).
19. Switch to the "v3 Groups" (3) tab.
20. Enter the desired group name in the "Group Name" entry field (4).
21. In the "Security Level" drop-down list, select "Auth/Priv" (4) to enable authentication and encryption.
22. Click on the "Create" button (5) to create the new group.
    After creating the group, the read and write permissions are activated automatically for it.



Creating an SNMP v3 user

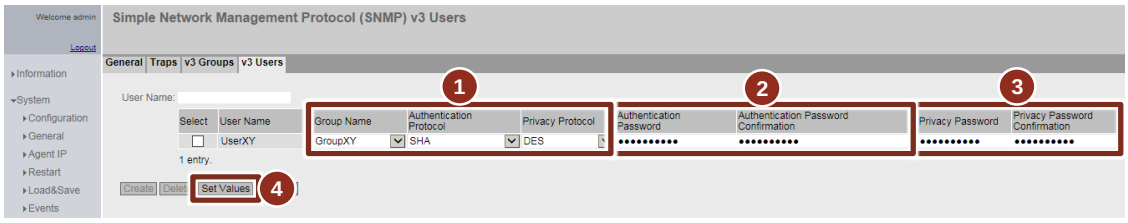
The section below shows you how to create an SNMP v3 user, assign it to a v3 group and configure it.

23. Switch to the "v3 Users" (1) tab.
24. Enter the desired user name in the "User Name" entry field (2).
25. Click on the "Create" button (3) to create the new user.



26. Select the following entries (1) in the drop down list:
    - As a "Group Name", select the group to which the new user should belong.
    - As "Authentication Protocol", select the "SHA" entry.
    - As "Privacy Protocol", select the "DES" entry.
27. Enter the desired password for the authentication in the "Authentication Password" (3) entry field and confirm it.
28. Enter the desired password for the encryption in the "Privacy Password" entry field and confirm it.
29. Click the "Set Values" button (4) to confirm the settings.

Figure 3-3



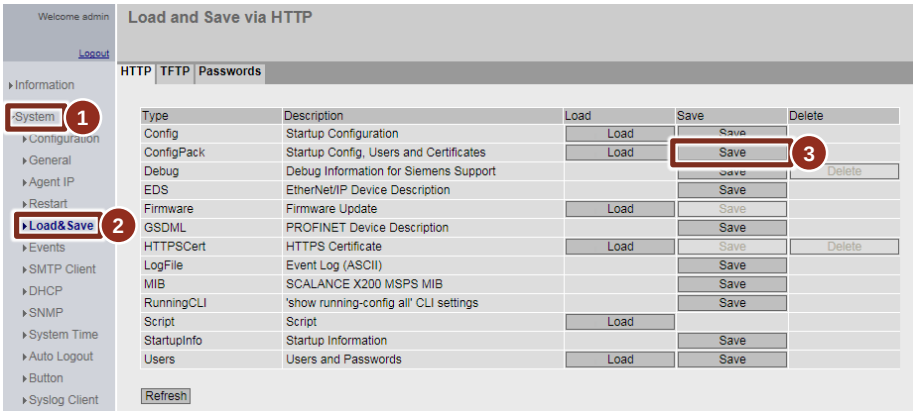
3.6 Backing up the configuration

It is recommended to back up the Service Bridge configuration after all the settings have been made. This way, when replacing the Service Bridge (e.g. in the event of a spare parts replacement), you can restore all the settings – including the plant-specific ones – by loading your own configuration file.

The download and local storage of the configuration via the WBM is described in the section below.

Procedure

1. Navigate to the "System > Load&Save" menu (1)(2).
2. Click on the "Save" button (3) to save the ConfigPack.
   A dialog for saving the configuration file opens. Select a storage path and save the file.



Note Configuration files (ConfigPacks) created for spare parts can only be uploaded to identical devices (same MLFB).

Note Alternatively or additionally, the C-PLUG can be used as a removable storage media for storing the configuration data of the service bridge. Further information about the C-PLUG can be found in the manual:
"SIMATIC NET: SCALANCE XC-200 Industrial Ethernet switches
https://support.industry.siemens.com/cs/ww/en/view/109743149

3.7 Commissioning the Service Bridge

3.7.1 Configuring the Network adapter in the engineering station

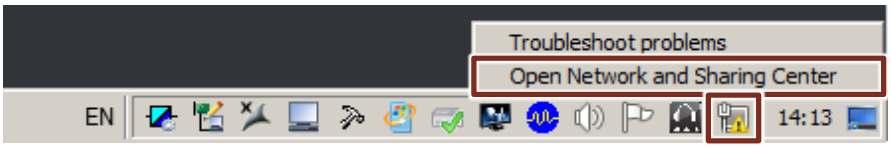
For access to the various PROFINET networks, several IP addresses are assigned to the network adapter provided in the engineering station.

The following is required:

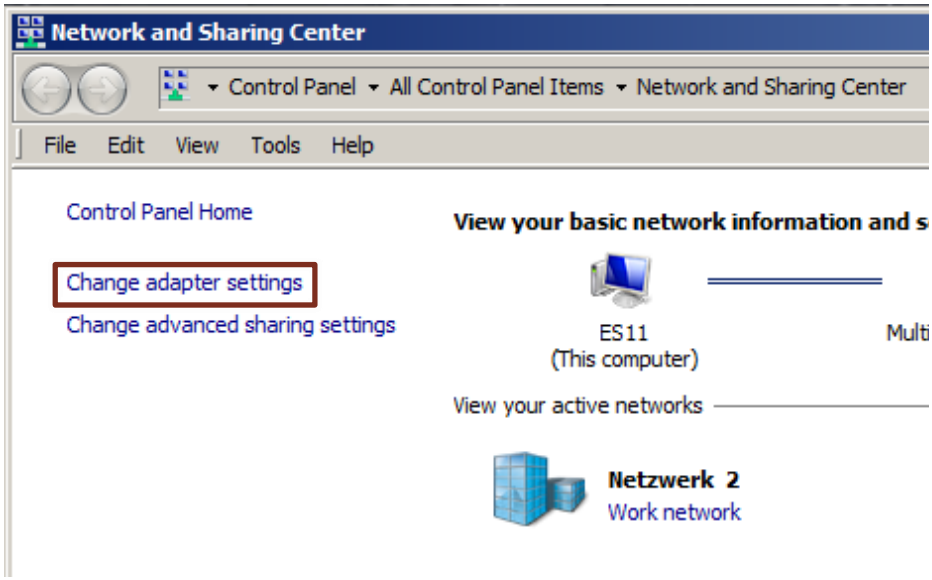
- An IP address in the address range of the Service Bridge, e.g. for access to the Web Based Management (WBM).
- An IP address for every PROFINET subnet to be accessed.

Procedure

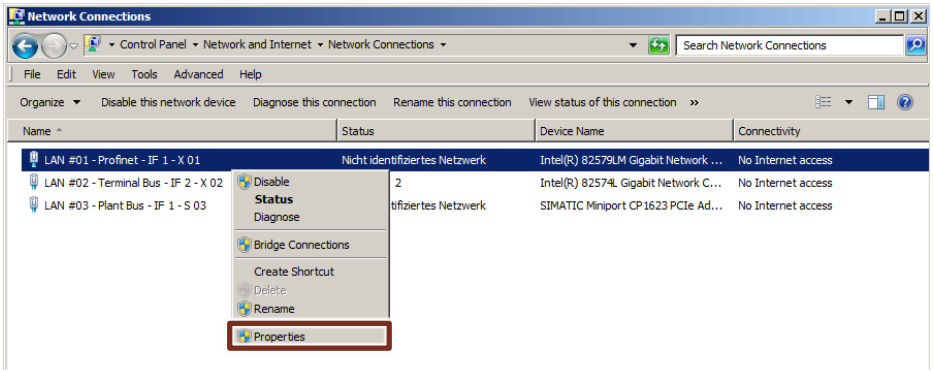
30. Open the "Network and Sharing Center" using the shortcut menu of the network icon in the task bar.



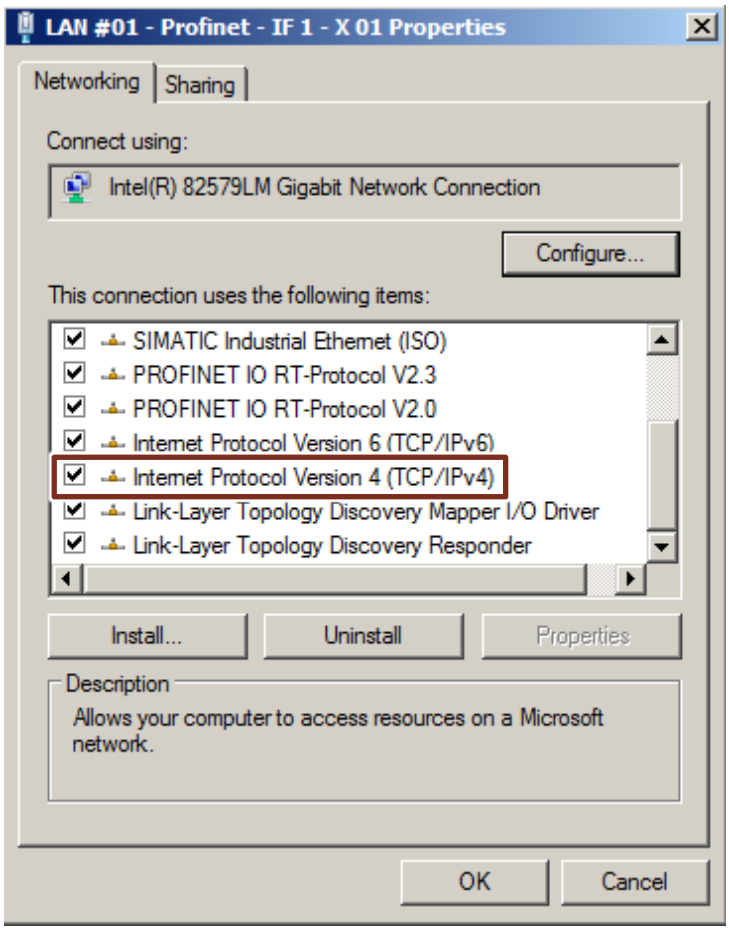
31. Click on "Change adapter settings".



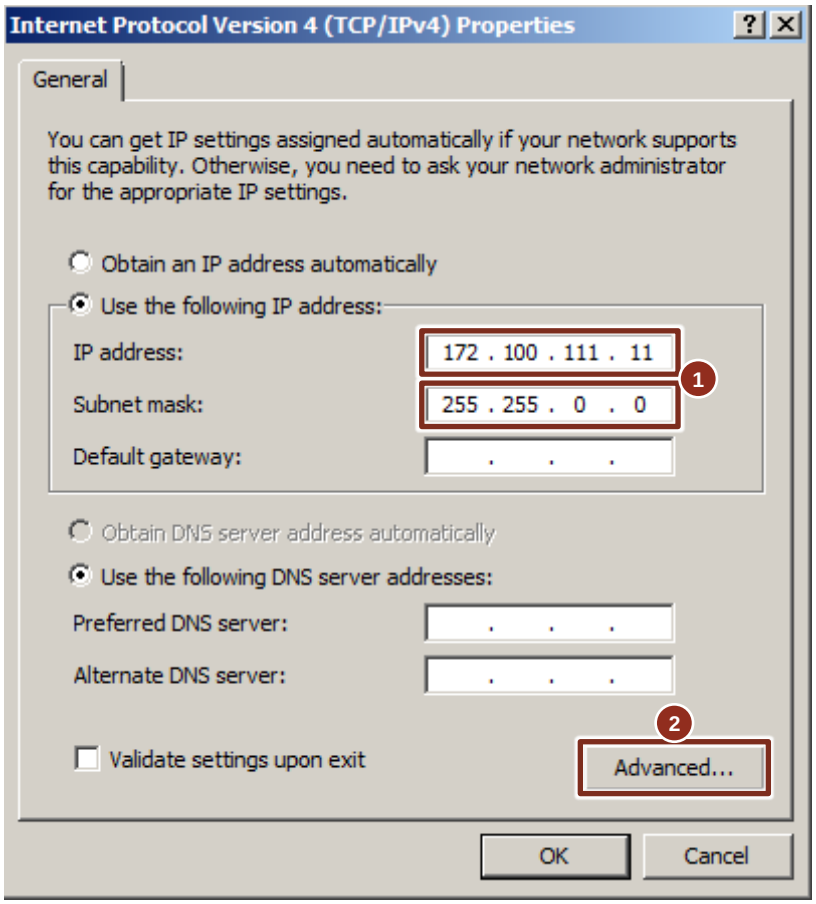
32. Open "Properties" from the shortcut menu of the intended network adapter.



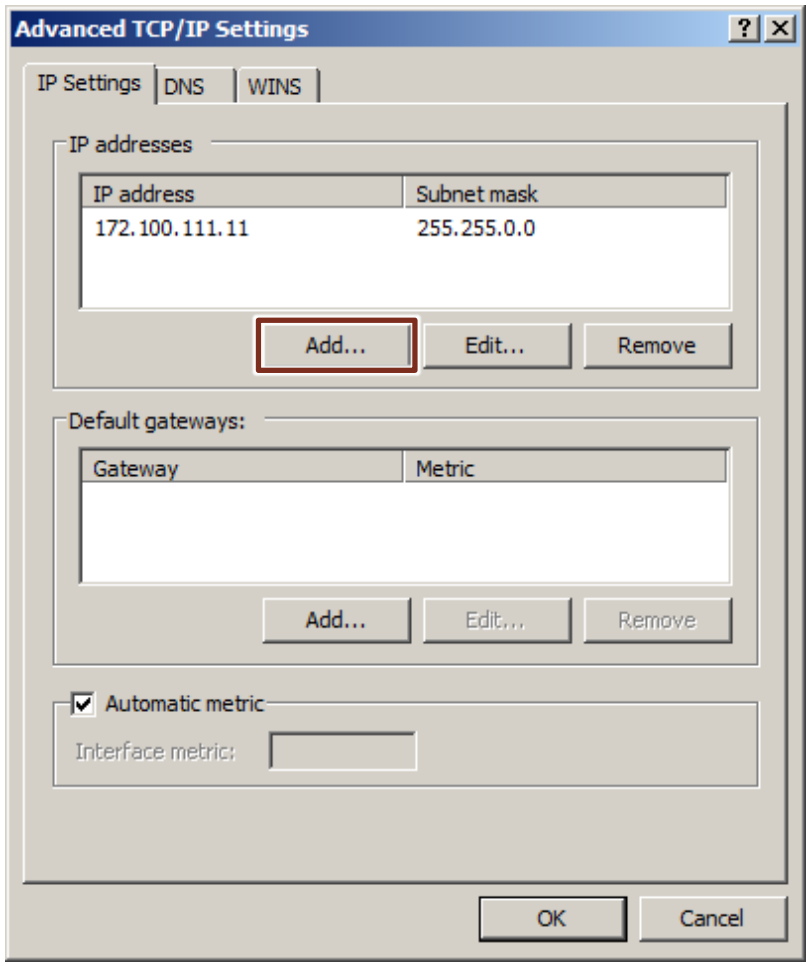
33. Double-click on "Internet Protocol Version 4 (TCP/IPv4)" to open its properties dialog.



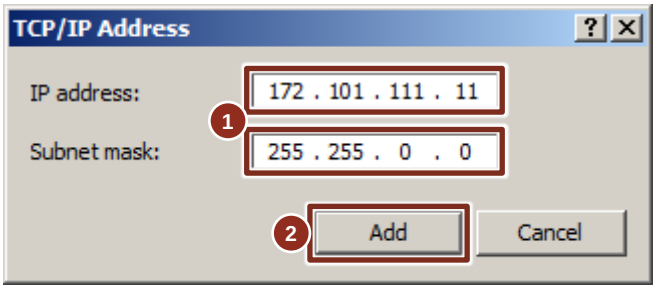
34. In the Service Bridge address range, configure an unallocated IP address with its respective subnet mask (1). This is also needed for accessing the Web Based Management (WBM) and for enabling/disabling ports. Then click on the "Advanced…" button to open the advanced settings (2).



35. Click on the "Add..." button to open the dialog box, where you can add further IP addresses.



36. Enter an unallocated IP address with the corresponding subnet mask in the address area of the PROFINET network you want to access, according to your plant planning (1).
Click on the "Add" button to assign the IP address to the network adapter (2).



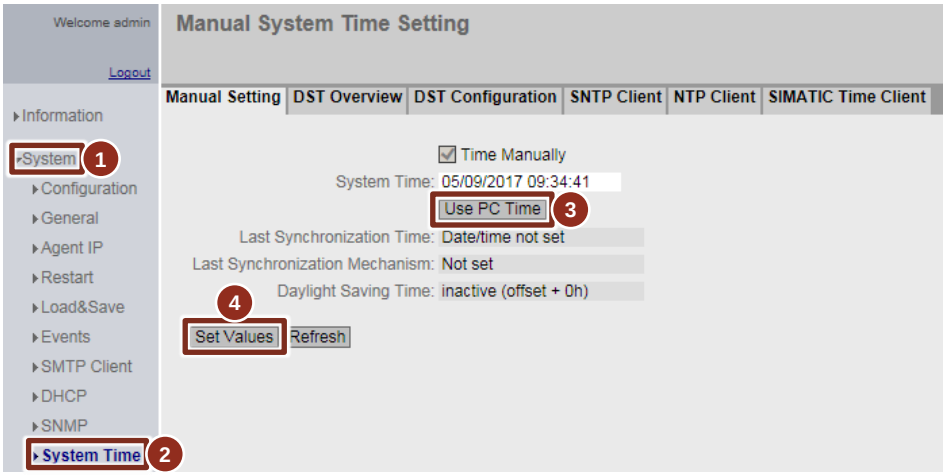
37. Repeat steps 6 and 7 until you have added all the required IP addresses.
Then confirm the open dialogs by clicking the "OK" button to apply the settings.

3.7.2 System time

In order to facilitate troubleshooting and the analysis of logs, it is recommended that the system time be set or synchronized correctly, depending on the system requirements. Setting up the synchronization / the adoption of the PC system time takes place via the "System > System time" menu.

Applying the PC system time

1. Navigate to the "System > System Time" menu (1)(2).
2. Click on "Use PC Time" (3) and confirm the settings with the "Set Values" button (4).



Note

For instructions on how to set the time synchronization, refer to the manual of the switch:
https://support.industry.siemens.com/cs/ww/en/view/109750283

4 Configuration file

The configuration of the Service Bridge is divided into the VLAN configuration, which enables the Service Bridge's basic functionality, and the settings for increasing operational reliability and IT security.

The settings for the Service Bridge, which differ from the standard configuration (factory settings) of a SCALANCE XC-200 switch, are described in the following section. These settings are already included in the pre-set configuration file and are applied automatically by loading them in the switch.

Note You can download the configuration file from the following link: https://support.industry.siemens.com/cs/ww/en/view/109747975

4.1 VLAN configuration

A VLAN configuration with the Private VLAN function is used to implement central access to the PROFINET networks and secure separation of the networks from one another.

4.1.1 Basics

VLANs (Virtual Local Area Network) allow a physical network to be divided into several logical networks that are shielded from each other. The Private VLAN (PVLAN) function makes a further subdivision possible, whereby the following units are distinguished:

Primary Private VLAN

A Primary Private VLAN refers to the subdivided VLAN. Access to all the Secondary Private VLANs is possible from the Primary PVLAN.

Secondary Private VLANs

Each Secondary PVLAN has a specific VLAN ID and is connected with the Primary PVLAN. The various Secondary PVLANs cannot communicate with each other. There are also two types of Secondary PVLANs. Isolated Secondary PVLANs are used for the PROFINET networks of the Service Bridge:

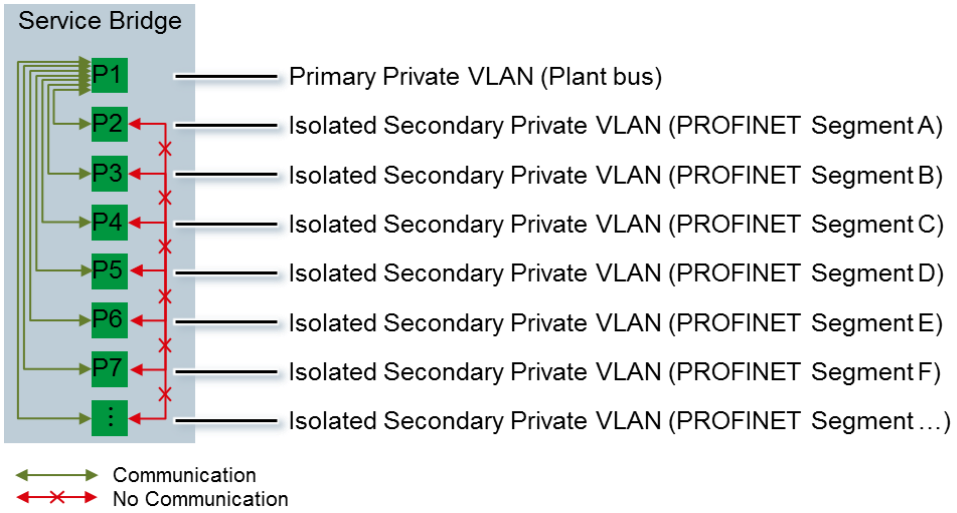
- Isolated Secondary PVLAN
  - Devices within an Isolated Secondary PVLAN cannot communicate with each other via Layer 2
- Community Secondary PVLAN (not relevant here)
  - Devices within a Community Secondary PVLAN can communicate with each other directly via Layer 2.

Application on the Service Bridge

In the Service Bridge configuration, Port 1 is configured for access from the plant bus as a Primary Private VLAN; the remaining ports are configured as Isolated Secondary Private VLANs for the PROFINET networks.

With this configuration, access to all PROFINET networks is possible from Port 1, and the PROFINET networks remain separated from each other at the same time.

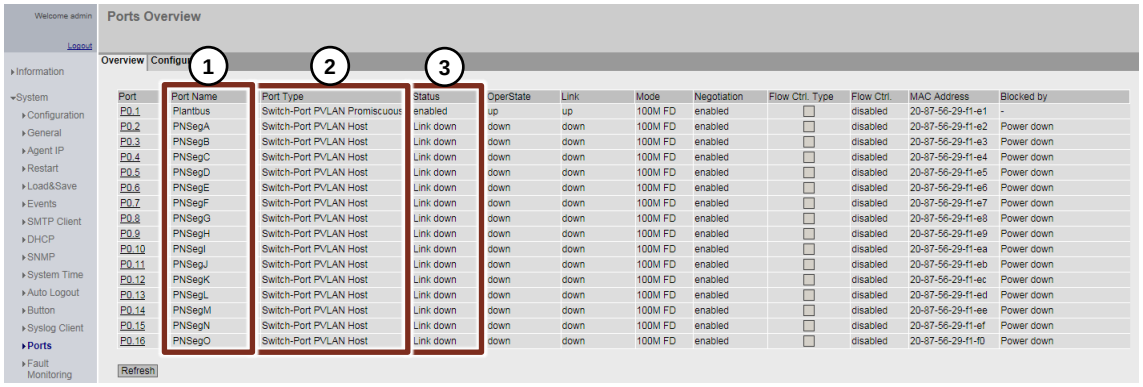
Figure 4-1



4.1.2 Ports

System > Ports

Figure 4-2



The type, status, etc. of the ports are set in the "System > Ports" menu. The following settings are provided for the Service Bridge:

(1) Port Name: The port name can be adjusted if required.

(2) Port type:

- Port type "Switch-Port PVLAN Promiscuous" is configured for Port 1 (plant bus). Promiscuous ports belong to a Primary PVLAN; devices at a promiscuous port can communicate with all the other devices of the PVLAN.
- Port type "Switch-Port PVLAN Host" is set for the remaining ports (PNSeg). Host ports belong to a Secondary PVLAN. Devices on a host port can only communicate with certain devices of the PVLAN.

(3) Status:

- Port 1 (plant bus) is enabled, i.e. activated.
- The remaining ports (PNSeg) are disabled as "Link down" and can be enabled from this menu if required.

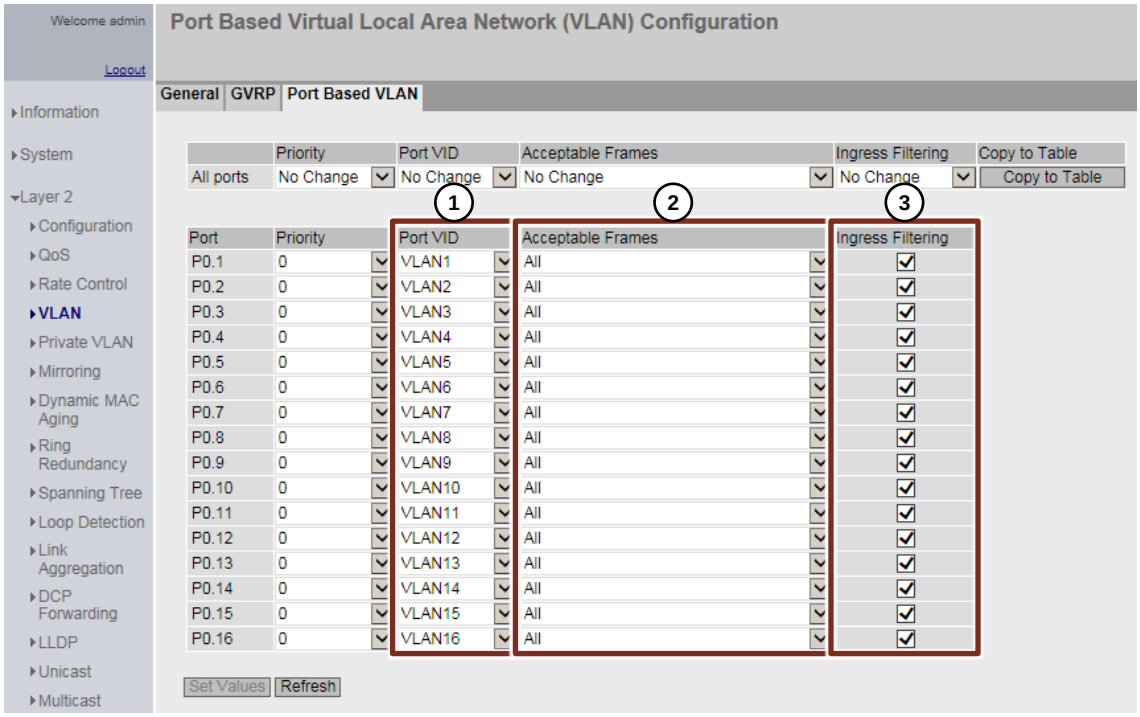
Note The "Link down" port status is used for deactivation, as it is retained even after a device restart. If the port status is "disabled", please note that this is set to "enabled" again after a device restart using the "Loop Detection" function.

Note Access from the plant bus to the individual PROFINET networks should only be active temporarily and can be done by activating/deactivating the ports via the Web Based Management (WBM) of the service bridge, see chapter 0.

4.1.3 VLAN

Layer 2 > VLAN: Port Based VLAN

Figure 4-3:



In the menu "Layer 2 > VLAN: Port Based VLAN" menu you can set how the ports react to incoming message frames. The following settings are provided for the Service Bridge:

(1) Port VID: A VLAN ID is assigned to each port. If a message frame without VLAN tag is received, it is assigned a VLAN tag with the VLAN ID stated here.

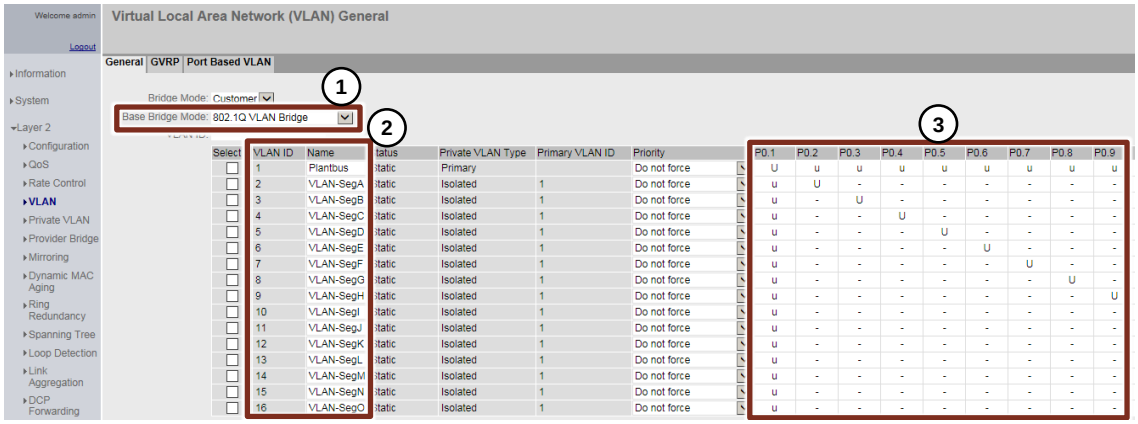
(2) Acceptable Frames: All incoming message frames (including untagged ones) are accepted.

(3) Ingress Filtering: If it is enabled it means that incoming message frames with a VLAN tag that does not correspond to the VLAN IN of the port are rejected.

With this configuration, all incoming message frames receive a VLAN ID corresponding to the port where they arrive, e.g. Port 1 – VLAN ID 1.

Layer 2 > VLAN: General

Figure 4-4



In the menu "Layer 2 > VLAN: General" menu, you can set which message frames may be output at which ports. The following settings are provided for the Service Bridge:

(1) Base Bridge Mode: 802.1Q VLAN Bridge means that VLAN information is taken into account in the Switch.

(2) A VLAN ID was assigned to each port and given a significant name.

(3) The use of the port is determined in this table:

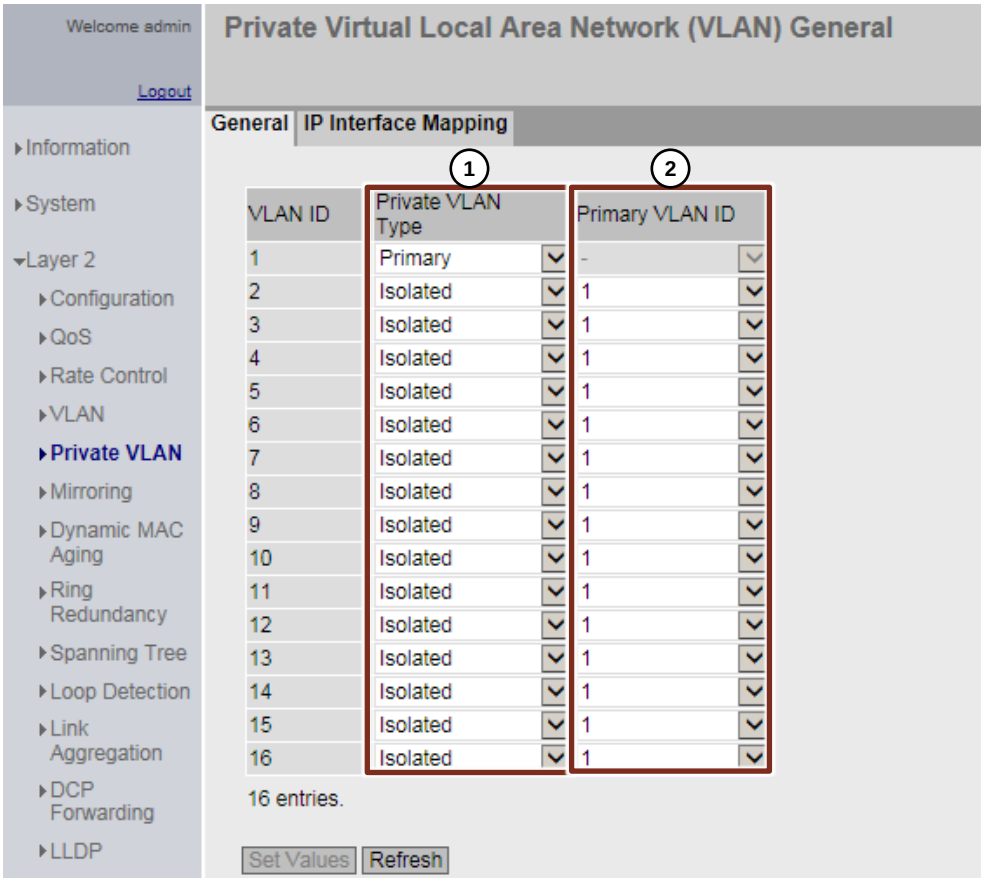
- "-": The port is not a member of the VLAN, which means that message frames from this VLAN are not output at this port.
- U (upper-case letter): The port is an untagged member of the VLAN, which means that message frames from this VLAN are output after the VLAN tag is removed.
- u (lower-case letter): The port is an untagged member of the VLAN but the VLAN is not configured as a port VID (see explanation Figure 4-3:). This means that message frames from this VLAN are output after the VLAN tag is removed.

With this configuration, message frames with the VLAN ID 1, i.e. coming from port 1, can be output on each port. Message frames coming from the ports of the PROFINET networks, i.e. with VLAN ID 2..n, may only be issued on the port itself or on port 1. The VLAN tags, which were assigned when they were received, are also removed.

4.1.4 Private VLAN

Layer 2 > Private VLAN

Figure 4-5



All the Private VLAN types are configured in the "Layer 2 > Private VLAN" menu. For an explanation of the Private VLAN types, see Section 4.1.1. The following settings are provided for the Service Bridge:

(1) Private VLAN Type:

- For the VLAN ID 1 (Port 1 – Plant bus): Primary PVLAN
- For the remaining VLAN IDs (Port 2..n – PNSeg): Isolated Secondary PVLAN

(2) Primary VLAN ID: 1, because all Secondary PVLANs are assigned to the Primary PVLAN (Plant bus).

With this configuration, communication is possible between VLAN ID 1 (Port 1) and all PROFINET networks (VLAN ID 2 .n - Port 2..n). At the same time, the PROFINET networks are located in various Isolated Secondary PVLANs and thus remain logically separated from each other.

4.2 Operational reliability and IT Security

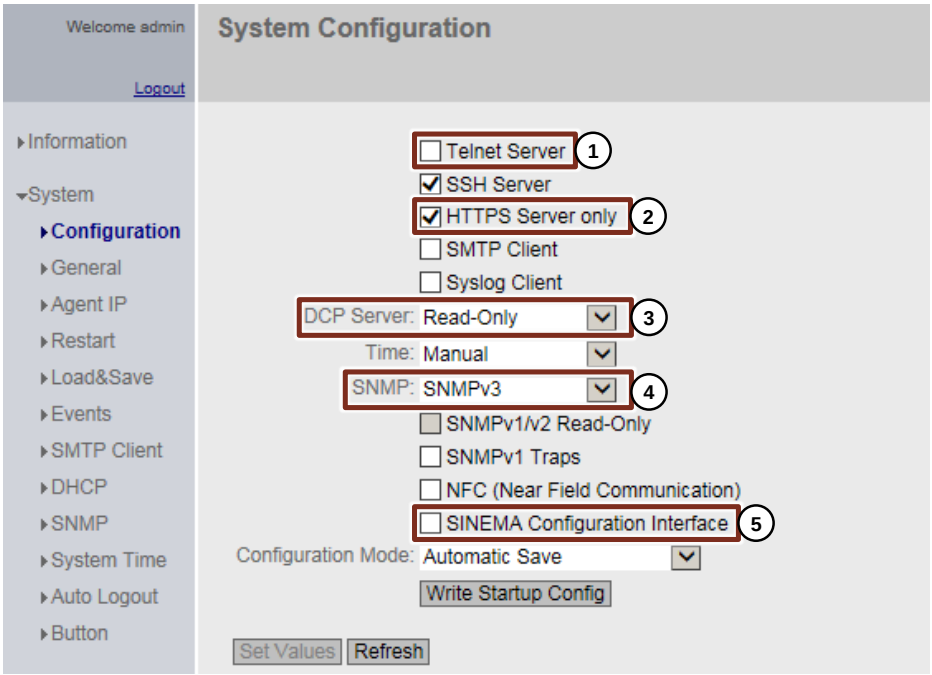
The settings for increasing operational safety are based on the "Defense in Depth" philosophy.
This means that individual, consecutive but independent protection measures are used so that an attacker has to invest time and effort again for each protection measure.

4.2.1 System configuration

Access possibilities to the device are configured in the Configuration overview in the "System > Configuration" menu. For security reasons, unencrypted protocols and some services have been disabled. The following settings are provided for the Service Bridge:

System > Configuration

Figure 4-6



(1) The "Telnet Server" service for unencrypted access to the CLI (Command Line Interface) via the Ethernet ports is disabled.

(2) The "HTTPS Server only" function is enabled, i.e. access to the WBM is only supported via HTTPS. Access via HTTP is disabled.

(3) Access to the "DCP Server" (Discovery and Configuration Protocol) is set to "Read-Only", i.e. the device parameters are write-protected. They can be read via DCP but not modified.

(4) The function "SNMP" (Simple Network Management Protocol) is set to "SNMPv3", which means that access to the device parameters is only possible with SNMP Version 3. SNMPv1/v2c are disabled.

(5) The "SINEMA Configuration Interface" function is disabled, i.e. no loading procedures are possible via PCS 7 or STEP 7 Basic / Professional.

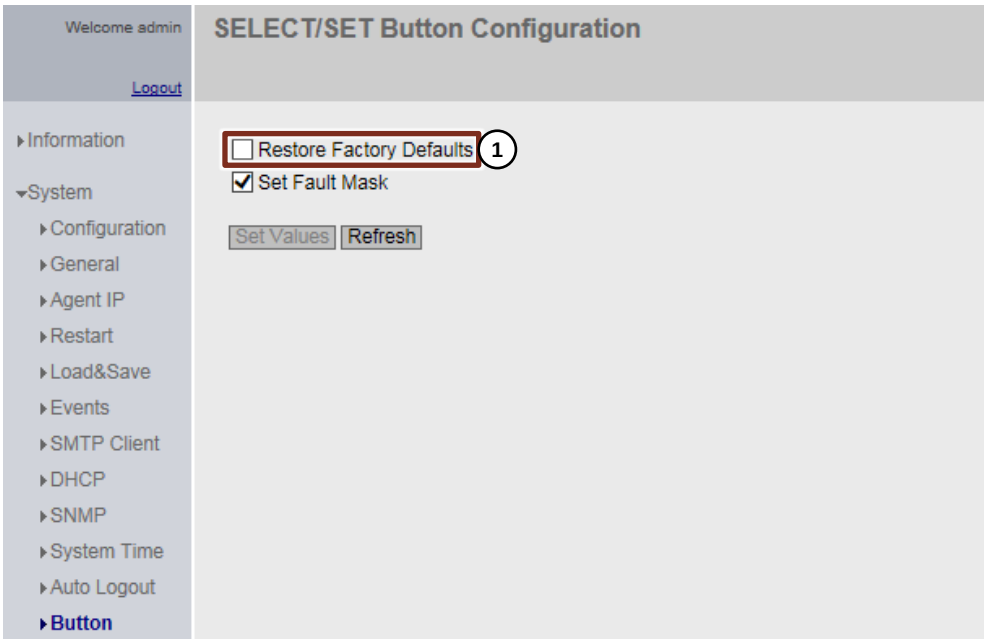
Note PRONETA and SINEC PNI use DCP for resets and assigning network parameters. These functions are not available due to the configuration of the DCP server to Read-Only.

4.2.2 "SELECT/SET" button

The "SELECT/SET" button function is configured in the "System > Button" menu. The settings of the "SELECT / SET" button are adjusted to prevent incorrect operation or incorrect configuration by unauthorized persons. The following settings are provided for the Service Bridge:

System > Button

Figure 4-7



(1) The "Restore Factory Defaults" functionality is disabled, i.e. it is not possible to reset to factory settings by means of the button during operation.

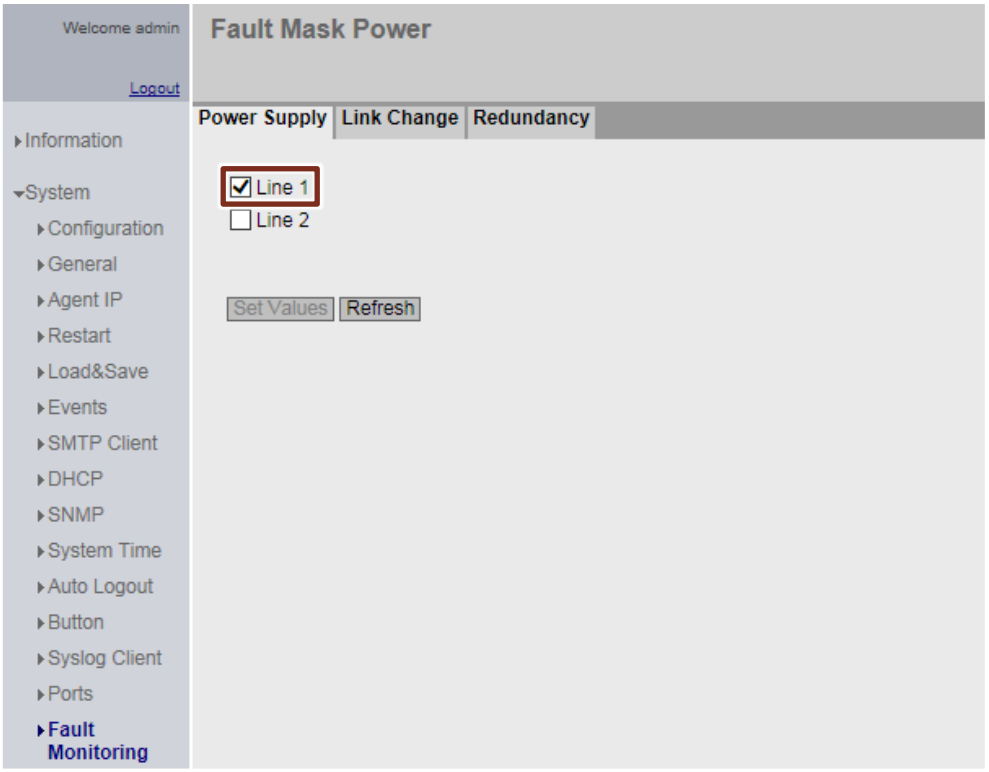
CAUTION	**When the switch is powered up, the "Restore Factory Defaults" functionality is always active, regardless of the configuration. This means that in case of emergency, it is still possible to reset to factory settings with the button during the power up after the system has been de-energized.**

4.2.3 Fault Monitoring

The monitoring functions are configured in the "System > Fault Monitoring" menu. The following settings are provided for the Service Bridge:

System > Fault Monitoring: Power supply

Figure 4-8



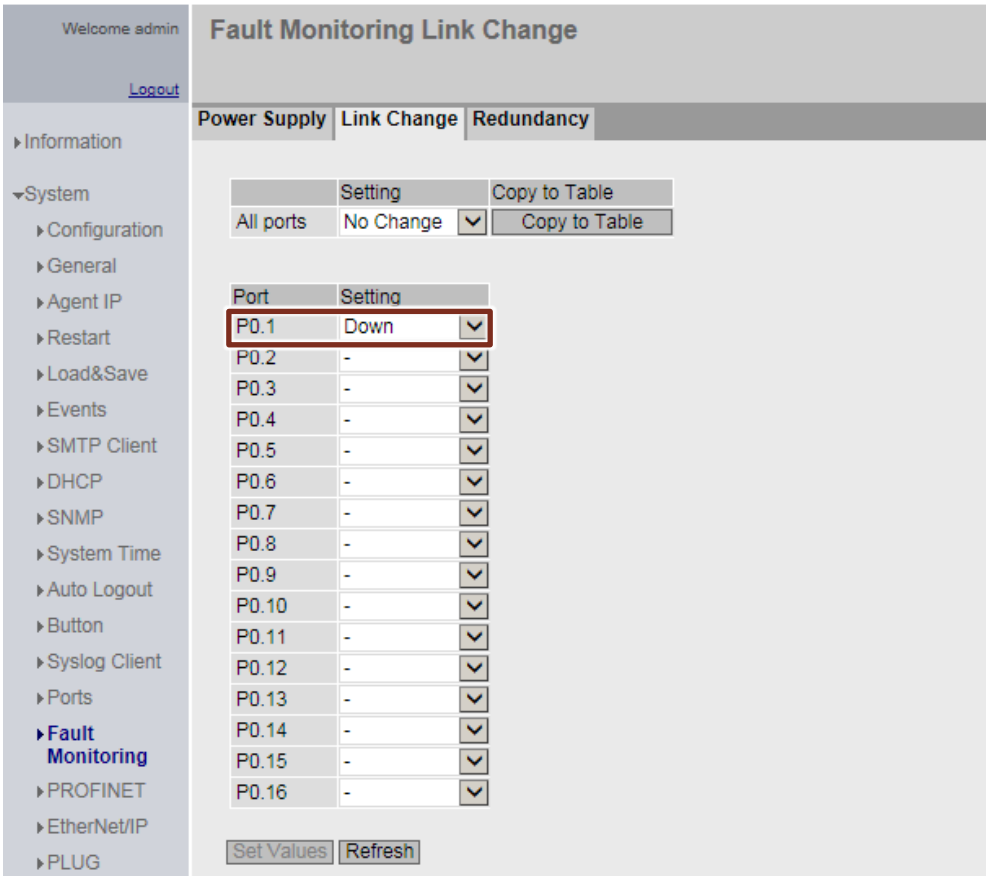
The monitoring of the power supply is configured in the "Power Supply" tab.

The power supply monitoring for connection 1 ("Line 1") is activated by default for the Service Bridge. The power supply monitoring for connection 2 ("Line 2") can be optionally activated if both power supplies are used.

An error of a power supply with simultaneous monitoring of both leads to the triggering of the signaling contact and to the flashing of the error LED on the device.

System > Fault Monitoring: Link Change

Figure 4-9



Link status change monitoring is configured in the "Link Change" tab.

Monitoring of Port 1 is configured as "Down" for the Service Bridge, which means that an error will be triggered if a link (connection) is no longer present at this port.

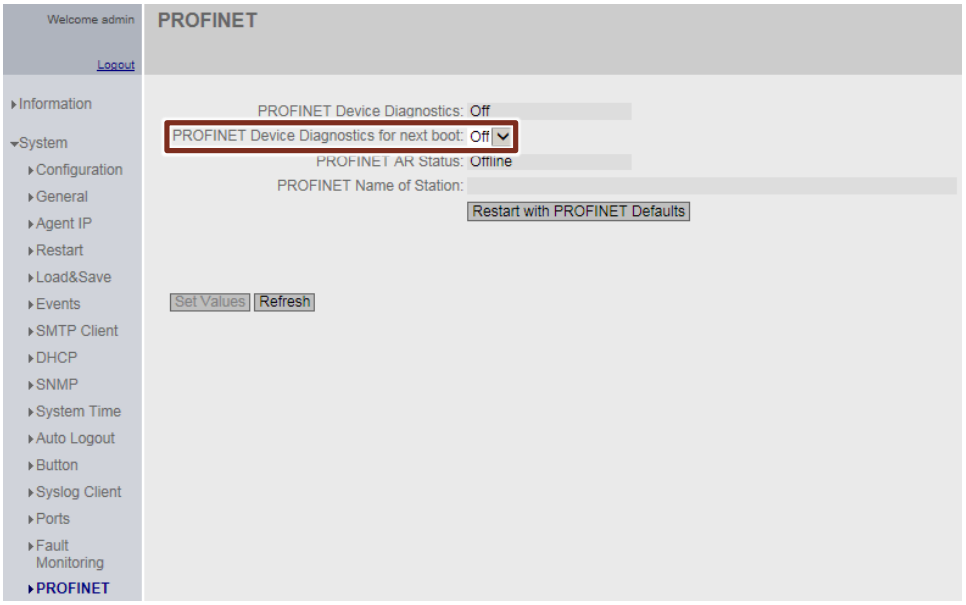
A fault leads to the triggering of the signaling contact and causes the fault LED on the device to light up.

4.2.4 PROFINET

The PROFINET properties of the Service Bridge are configured in the "System > PROFINET" menu. Since the Service Bridge is only intended for access from the plant bus to the PROFINET networks, it is configured as an IE switch. Configuration/use as an IO device is not intended.

System > PROFINET

Figure 4-10:



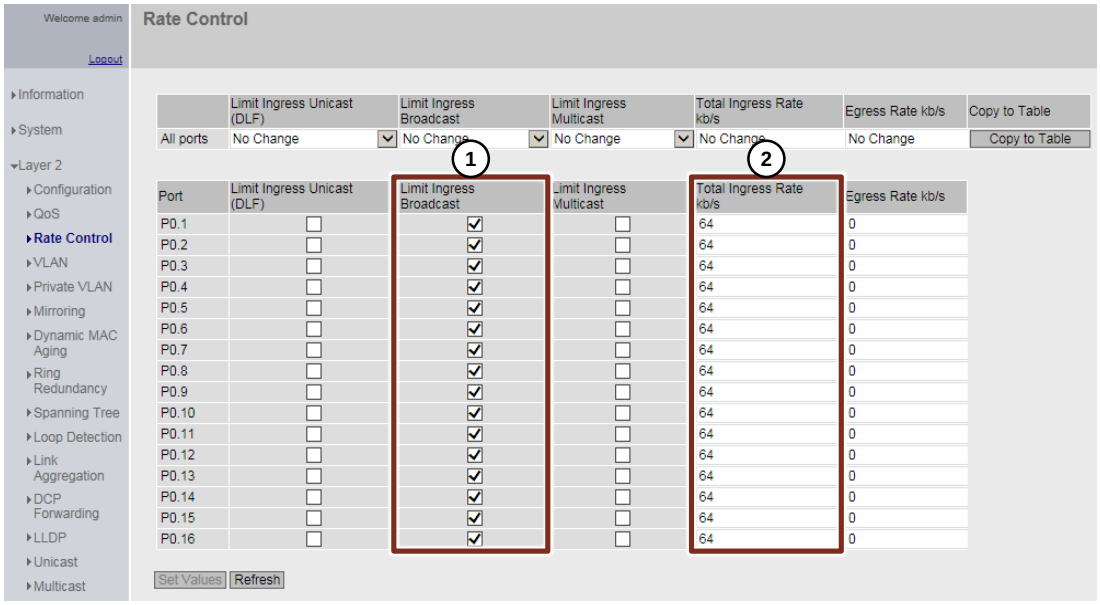
The function "PROFINET Device Diagnostics for next boot" is disabled for the Service Bridge; this means that PROFINET device diagnostics and consequently the PROFINET interface are inactive.

4.2.5 Rate control

The rate limits of the individual ports are configured in the "Layer 2 > Rate Control" menu. The purpose is to limit the spread of broadcasting storms in the event of a fault. The following settings are provided for the Service Bridge:

Layer 2 > Rate Control

Figure 4-11



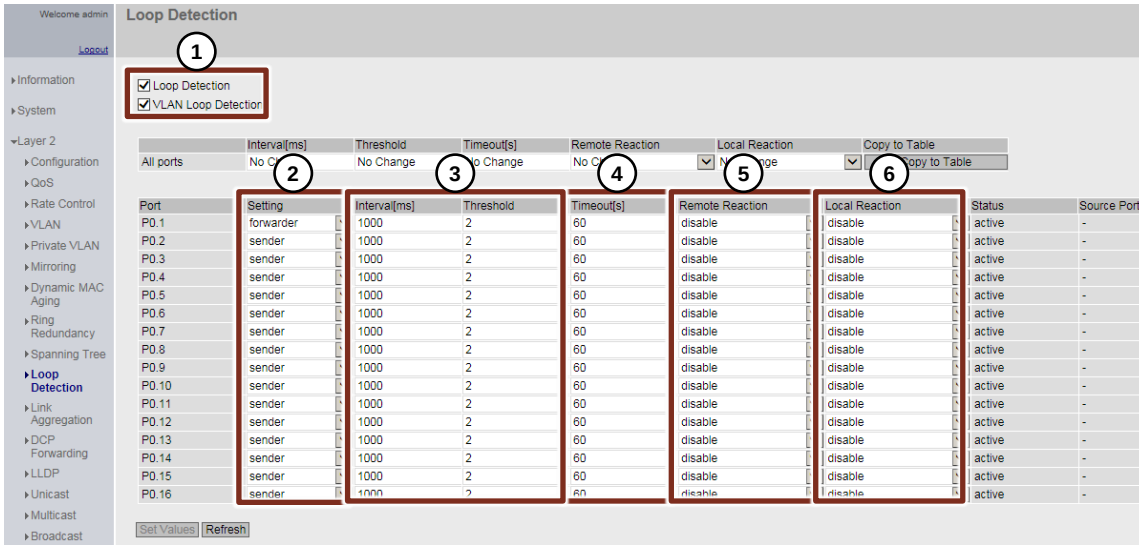
(1) The function "Limit Ingress Broadcast" is activated for all ports. This means that the data rate for incoming Broadcast message frames is restricted to the "Total Ingress Rate" (2).

4.2.6 Loop detection

The loop detection values are configured in the "Layer 2 > Loop Detection" menu. Loop detection is a function which serves to detect loops in the network and to limit their effects. The following settings are provided for the Service Bridge:

Layer 2 > Loop Detection

Figure 4-12



(1) The "Loop Detection" and "VLAN Loop Detection" functions are activated.

(2) Except for Port 1, all the ports are configured as "transmitters", i.e. they emit "Loop Detection Message frames". Port 1 remains with the default setting "Forwarder".

(3) The "Threshold" is configured to 2. This means that if two message frames are emitted by the Service Bridge itself and return to it within 1000 ms, it is assumed that a loop is present. Reaction (5) or (6) takes place.

(4) The "timeout" time is set to 60 s, which means that a check is performed every 60 seconds to see whether the loop is still present. If a loop is no longer present, the port is reactivated.

(5) "disable" is configured for all ports as a "Remote Reaction", i.e. as a response to the detection of a remote loop. This means that if a remote loop is detected on a port, the port is blocked.

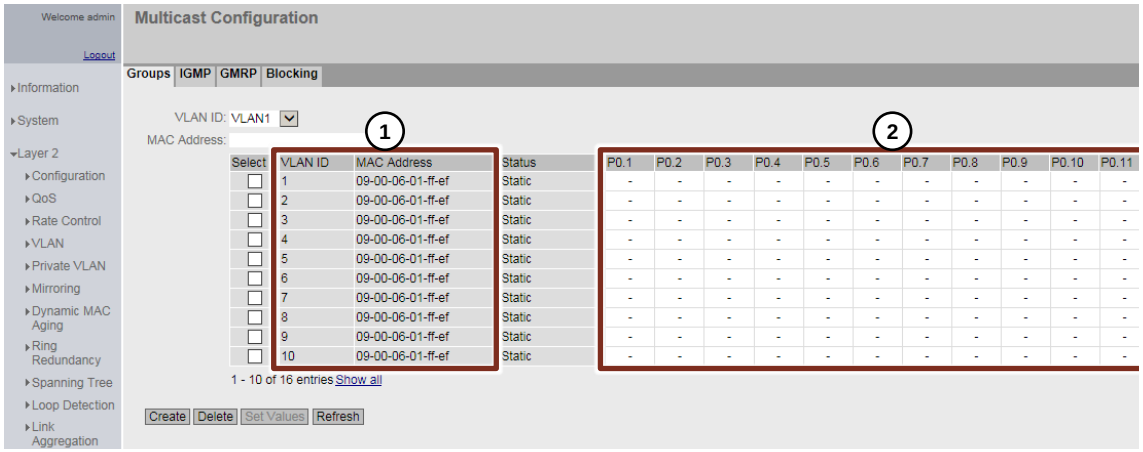
(6) "Disable" is configured for all ports as a "Local Reaction", i.e. as a response to the detection of a local loop. This means that if a local loop is detected on a port, the port is blocked.

4.2.7 Multicast filter

The Multicast filter is configured in the "Layer 2 > Multicast" menu. The Service Bridge is provided with a Multicast filter which prevents the forwarding of time message frames according to the SIMATIC method.

Layer 2 > Multicast

Figure 4-13



(1) For all VLAN IDs the Multicast MAC address "09-00-06-01-FF-EF" is entered in the Multicast Filter table.

(2) The setting "-" is configured for all ports via all VLANs so that no multicast message frames are forwarded with this multicast MAC address.

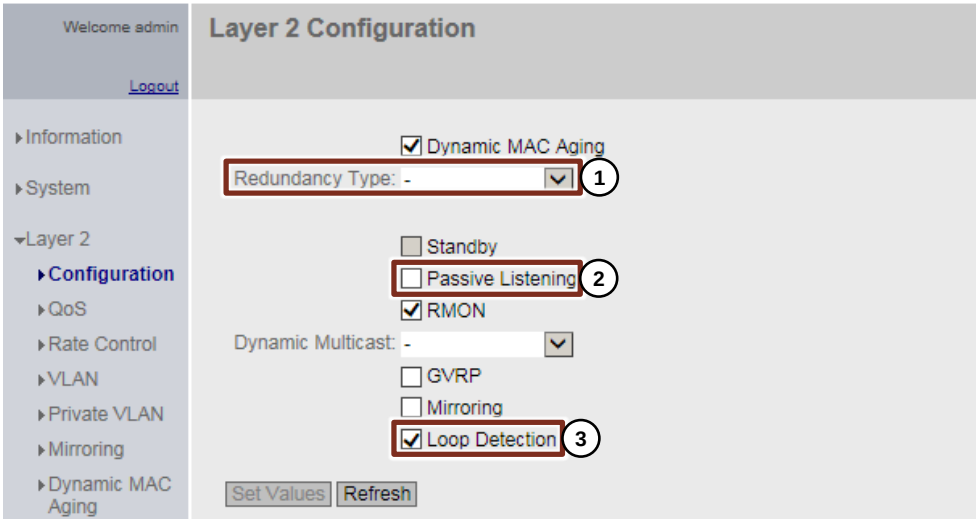
4.3 Other settings

4.3.1 Layer 2 configuration

Higher-level functions can be configured in the basic configuration of layer 2 ("Layer 2 > Configuration"). The following settings are provided for the Service Bridge:

Layer 2 > Configuration

Figure 4-14



(1) The redundancy function is disabled with the setting "Redundancy Type": "-", since the Service Bridge is only provided with a stub connection to the plant bus.

(2) The "Passive Listening" function is disabled, as Spanning Tree BPDUs (Bridge Protocol Data Unit) should not be forwarded.

(3) The "Loop Detection" function is enabled.

5 Firewall configuration using the example of a SCALANCE SC632-2C

The purpose of the firewall is to protect the plant bus against unauthorized access from the field. In the section below, the SCALANCE SC632-2C is configured in such a way that it only allows communication if is initiated by selected sources in the plant bus (e.g. the ES). This means that all the message frames stemming from the field bus are rejected with the exception of response message frames.

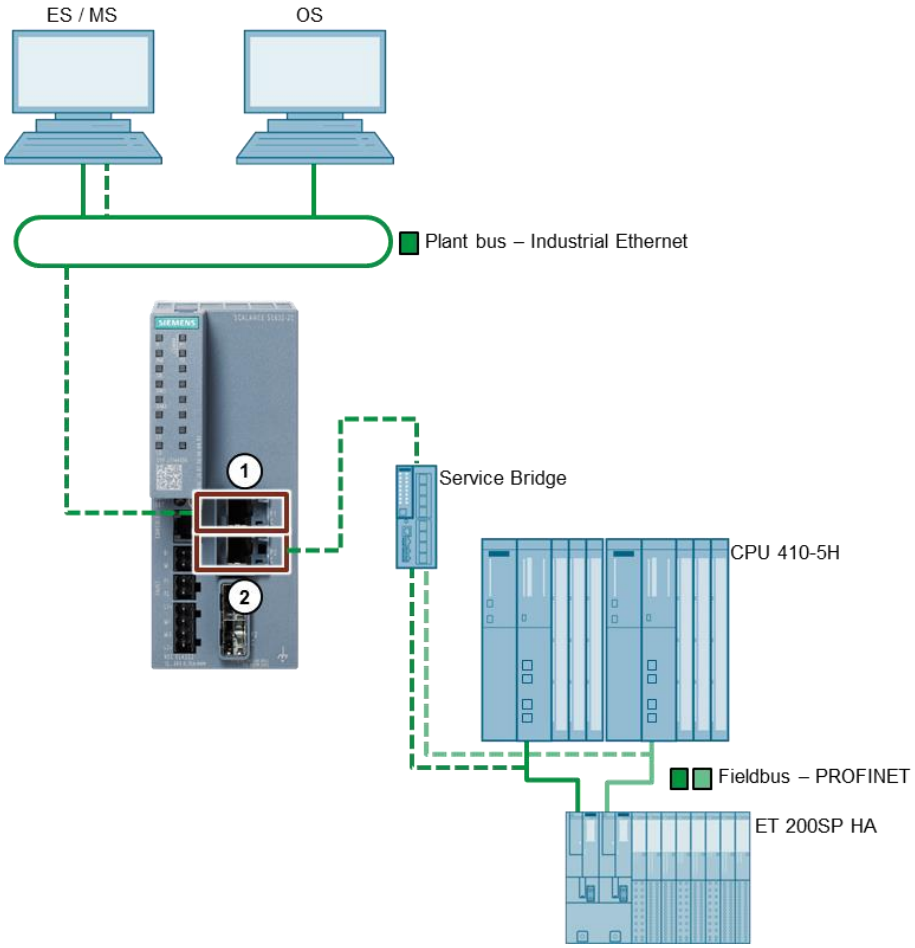
5.1 Connecting the SCALANCE SC632-2C

SCALANCE SC632-2C has two interfaces, each of is handled differently dependent of the configuration: In this application example, the upper interface P1 is configured for the internal protected network and the lower interface P2 is configured for the external network:

- Interface P1
  - Internal network, i.e. a network protected by SCALANCE SC.
- Interface P2
  - External network, i.e. unprotected network sector

To protect the system against unauthorized access from the plant bus, the plant bus is defined as a protected network (internal network), i.e., connected to Interface P1 (1), whereas the field bus is considered an unprotected network (External Network), i.e., connected to Interface P2 (2).

Figure 5-1



Note If the interfaces are interchanged, SCALANCE SC loses its protection function.

5.2 SCALANCE SC632-2C configuration

The SCALANCE SC632-2C is configured using Web Based Management (WBM).

Note The configuration of the firewall with the Security Configuration Tool (SCT) is not supported by the SCLANCE SC family.

Requirement

To configure SCALANCE SC632-2C, it must be first reset to factory settings. You can reset the SCALANCE SC632-2C to factory settings by pressing and holding the reset button for about 5 seconds during device start-up until the Fault "F" LED is constantly lit.

Furthermore, at least firmware version V2.0.1 is required.

Note The firmware can be downloaded from the following entry:

https://support.industry.siemens.com/cs/de/en/view/109769665

5.2.1 Setting up access to the Web Based Management of the SCALANCE SC632-2C

To configure the SCALANCE SC632-2C, the first step is to establish the connection to Web Based Management.

1. Assign the previously defined IP address "192.168.10.12" and subnet mask "255.255.255.0" as described in chapter 3.2
2. Access the WBM and carry out the steps described in chapter 3.3 (changing the password, checking and updating the firmware version if necessary).

5.2.2 Firewall rule configuration

The firewall rules are configured within the WBM in the "Security" tab.

In the following section packet filter rules are defined based on MAC addresses (layer 2) and IP address (layer 3).

Based on the MAC addresses (layer 2), a filter rule is created that only allows message frames that have the MAC address of selected devices (e.g. the ES) as a source or destination address. This means multicast, broadcast and message frames between other subscribers are rejected.

Based on the IP addresses (layer 3), a filter rule is created that only allows communication from selected sources in the plant bus (e.g. the ES). This means that all the message frames stemming from the field bus are rejected with the exception of response message frames.

Note

IP rules apply for Layer 3 packets, MAC rules apply for Layer 2 packets.

The processing in the firewall is controlled as follows:

- The rules in the Layer 2 firewall are checked first. If there is an IPV4 rule there, the rules are then checked in the Layer 3 firewall.
- There must be an "Allow" rule in the Layer 3 firewall, otherwise the message frame will be rejected, although this is allowed in the Layer 2 firewall.
- By default, IPV4 is active on the "Predefined MAC" tab, which allows any IP traffic through the Layer 2 firewall.

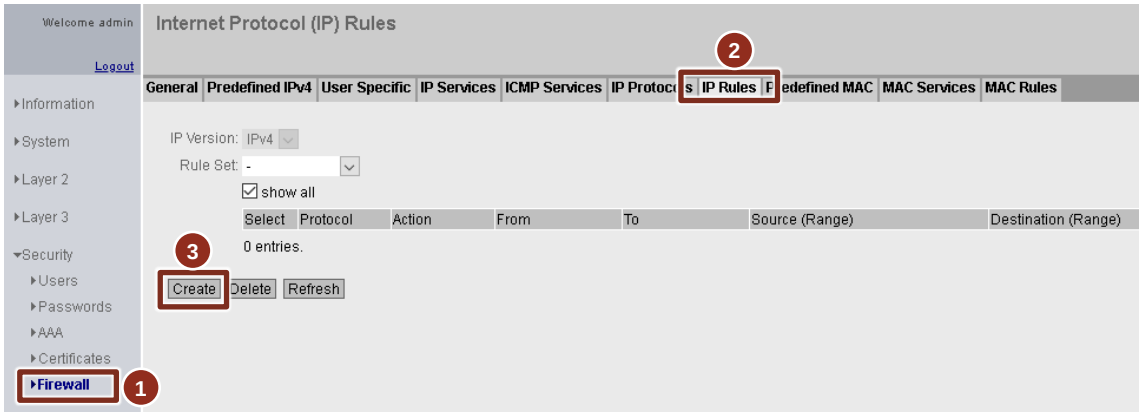
Definition of IP rules

The following are the IP rules that only allow communication from selected sources on the plant bus (e.g. the ES).

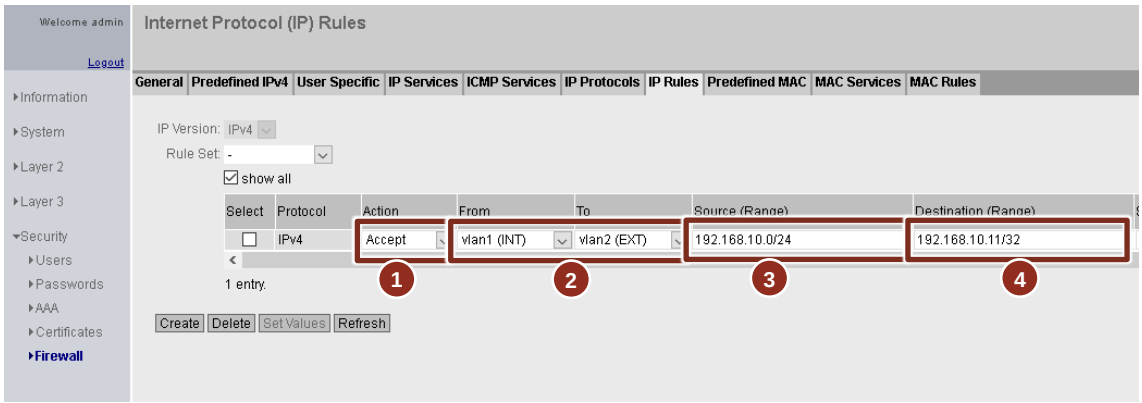
Since the ES's separate network card for accessing the Service Bridge's Web Based Management (WBM) and the various PROFINET networks has several IP addresses, several rules must be created. One rule per IP address or IP address range used.

The IP addresses and filters in the following configuration refer to the structure presented in chapter 2.2 (Figure 2-3).

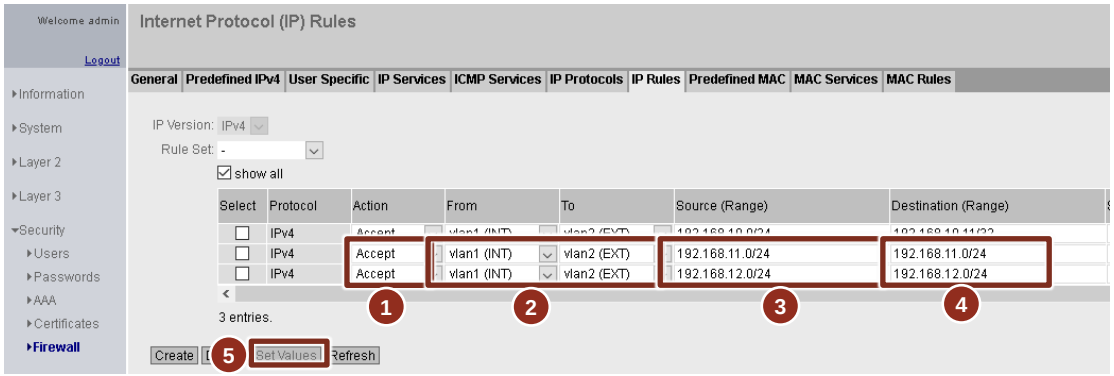
1. Go to the "Firewall" tab of the SCALANCE SC632-2C to start the configuration (1).
2. Switch to the IP Rules tab (2) and click the Create button (3) to create a new IP rule.



3. Configure the rule as follows:
   This rule allows access to the WBM of the service bridge.
   (1) Action "Accept"
   Message frames corresponding to the rule are permitted.
   (2) "From": "vlan1 (INT)" ("Internal")
   "To": "vlan2(EXT)" ("External")
   Access from the plant bus in the direction of the fieldbus.
   (3) "Source IP address" ("Source (Range)"): IP address of the separate network card in the ES for accessing the WBM of the service bridge or IP address range if multiple stations should have access.
   [IP address]/[number of bits to be included]
   e.g.
   192.168.10.0 (255.255.255.0) = 192.168.10.0/24 for one IP address range
   192.168.10.10 (255.255.255.0) = 192.168.10.10/32 for a special IP address
   (4) "Destination IP address" ("Destination (Range)"): IP address of the Service Bridge 192.168.10.11 (255.255.255.0) = 192.168.10.11/32



4. Repeat steps 2 and 3 and define another rule for each PROFINET network and IP address of the ES:
   (1) Action "Accept"
   Message frames corresponding to the rule are permitted.
   (2) From Internal
   To: External
   Access from the plant bus in the direction of the fieldbus.
   (3) "Source IP address" ("Source (Range)"): IP address range of the PROFINET network.
   (4) "Destination IP address" ("Destination (Range)"): IP address range of the PROFINET network



5. Click the "Set Values" button (5) to confirm the settings.

Note

Depending on the applications used (e.g. PRONETA), additional IP rules may be required for automatically assigned IP addresses.

By default, PRONETA temporarily uses the highest free IP address in the subnet during the network scan. In the IP address range 192.168.11.0/24, this is 192.168.11.254 if not used.

So that PRONETA can access all data during network scanning, another IP rule is necessary that allows access for this IP address or, as in this example, the complete IP address range of the PROFINET network can be released. The temporary IP address of PRONETA may change with the addition of new participants in the network.

Definition of MAC rules

In the following, the MAC rules are created which only allow communication that has the MAC address of the ES as source or destination address. This means all other frames from different participants are rejected.

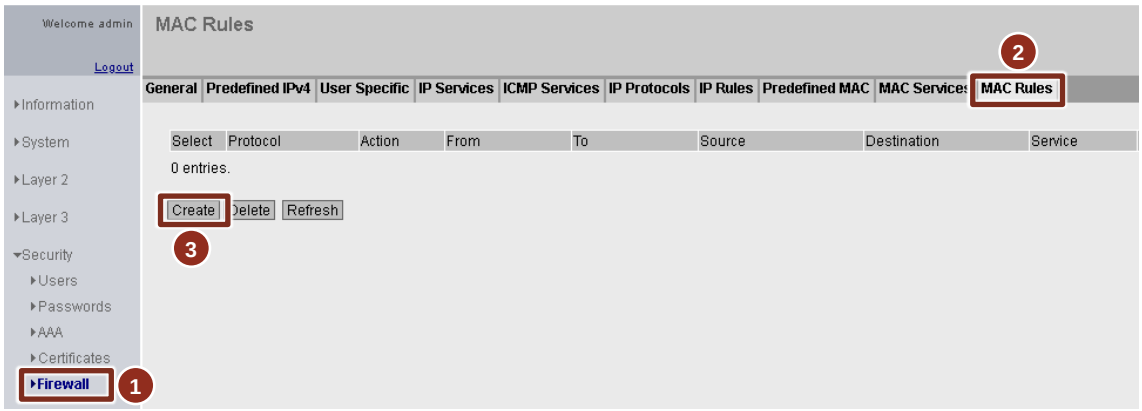
Note

You can determine the MAC address of the network adapter, e.g. via the command prompt (CMD) using the command "ipconfig/all".

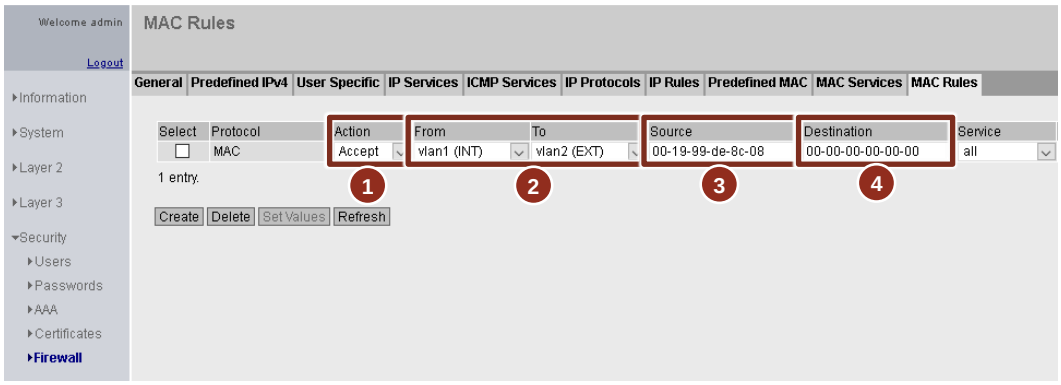
Information about all network adapters is displayed.
In the following, the MAC address of the network card is required to access the PROFINET networks.

1. Go to the "Firewall" tab of the SCALANCE SC632-2C to open the properties (1).

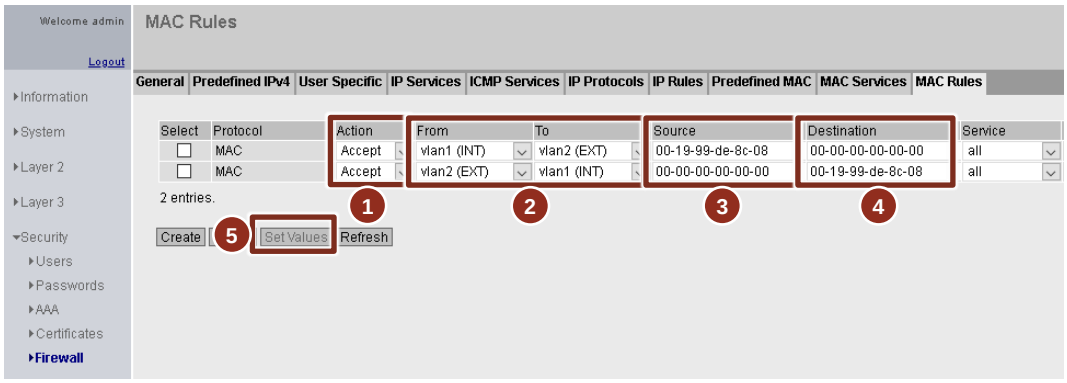
2. Switch to the tab "MAC rules" (2) and click on the button "Create" (3) to create a new MAC rule.



3. Configure the rule as follows:
   This rule allows message frames starting from the Engineering Station.
   (1) Action "Accept"
   Message frames corresponding to the rule are permitted.
   (2) "From": "vlan1 (INT)" ("Internal")
   To: "External" ("vlan2 (EXT)")
   Message frames from the plant bus in the direction of the fieldbus.
   (3) "Source MAC address" ("Source"): MAC address of the network card in the ES via which access takes place.
   (4) "Destination MAC address" ("Destination"): No entry
   This means that the rule applies regardless of the destination MAC address.



4. Repeat steps 2 and 3 and define another rule.
   This rule allows message frames from the fieldbus with the Engineering Station as target.
   (1) Action "Accept"
   Message frames corresponding to the rule are permitted.
   (2) "From": "vlan1 (EXT)" ("External")
   "To": "vlan1 (INT)" ("Internal")
   Message frames from the fieldbus in the direction of the plant bus.
   (3) "Source MAC address" ("Source"): No entry
   This means that the rule applies regardless of the source MAC address.
   (4) "Destination MAC address" ("Destination"): MAC address of the network card in the ES via which access takes place.
   (5) Click the "Set Values" button (5) to confirm the settings.



5. To block any further traffic through the firewall, two more rules must be added.
   (1) Action " Drop "
   Message frames corresponding to the rule are blocked.

(2) "From": "vlan1 (INT)" ("Internal")
"To": "vlan2 (INT)" ("External")
Access from the plant bus in the direction of the fieldbus.

(3) "Source MAC address" ("Source"): No entry
This means that the rule applies regardless of the source MAC address.

(4) "Destination MAC address" ("Destination"): No entry
This means that the rule applies regardless of the destination MAC address.

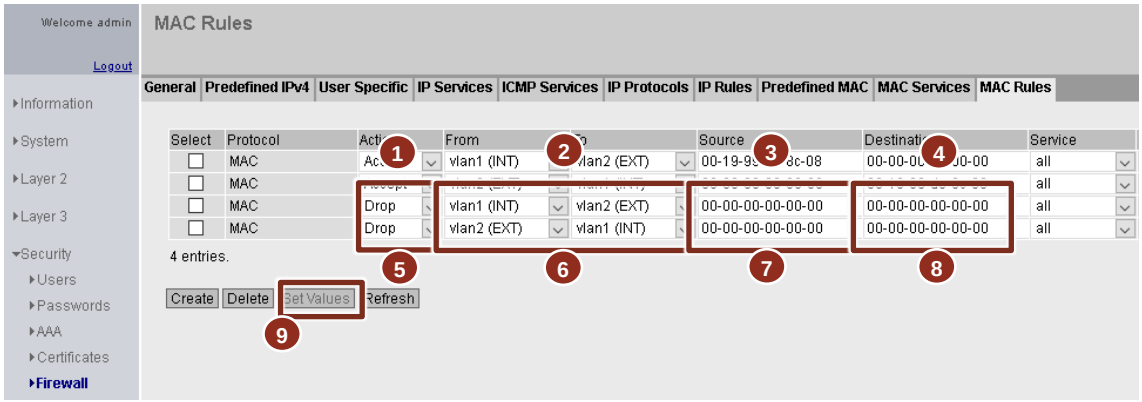
(5) Action " Drop "
Message frames corresponding to the rule are blocked.

(6) "From": "vlan2 (INT)" ("External")
"To": "vlan1 (INT)" ("Internal")
Access from the fieldbus in the direction of the plant bus.

(7) "Source MAC address" ("Source"): No entry
This means that the rule applies regardless of the source MAC address.

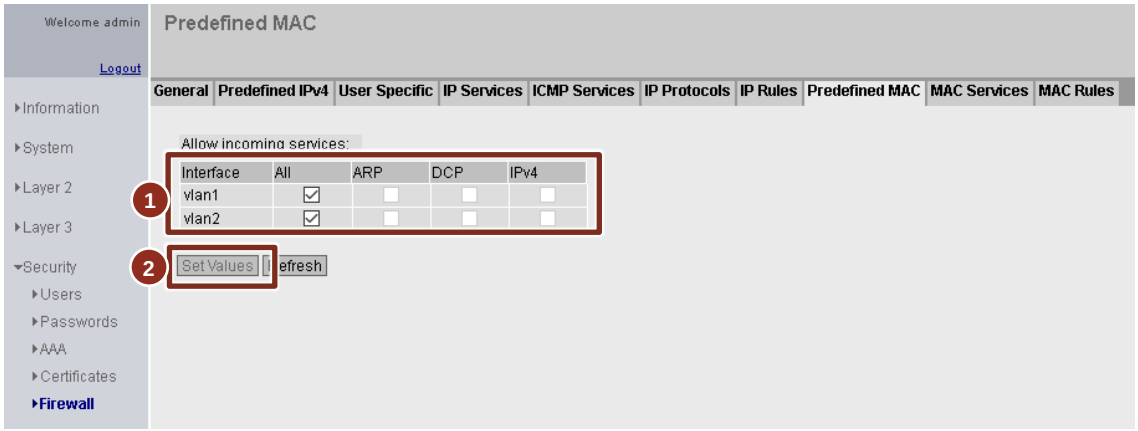
(8) "Destination MAC address" ("Destination"): No entry
This means that the rule applies regardless of the destination MAC address

(9) Click the "Set Values" button to confirm the settings.



Change to the "Predefined MAC" tab.

1. Activate all services at the interfaces "vlan1" and "vlan2" (1) and confirm the setting with "Set Values" (2)

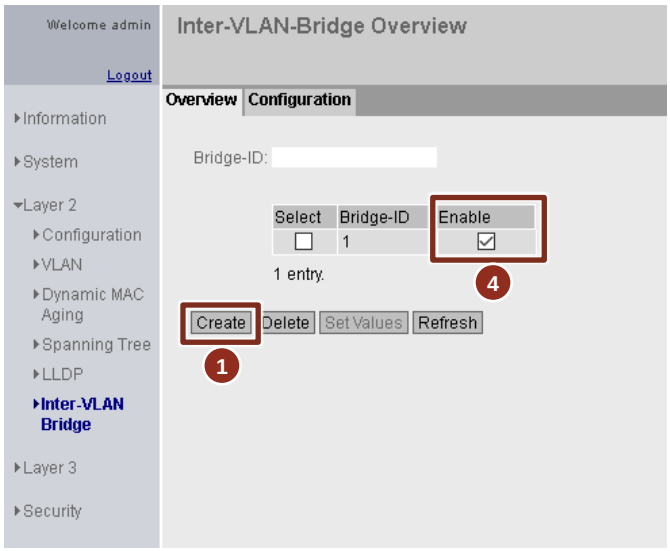


5.2.3 Bridge Mode

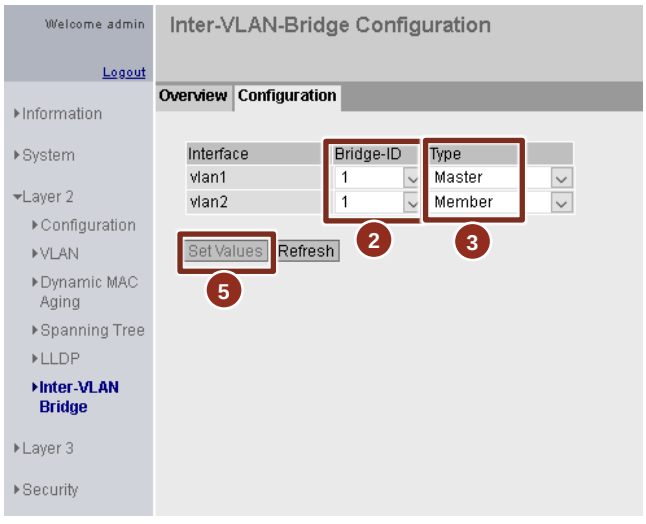
Bridge mode is required for Layer 2 firewall.

The bridge module is configured in the "Layer 2 > Inter-VLAN Bridge" menu. The following settings are provided for the SCLANCE SC632-2C:

1. First, a bridge ID must be entered in the "Overview" tab and created with "Create" (1).



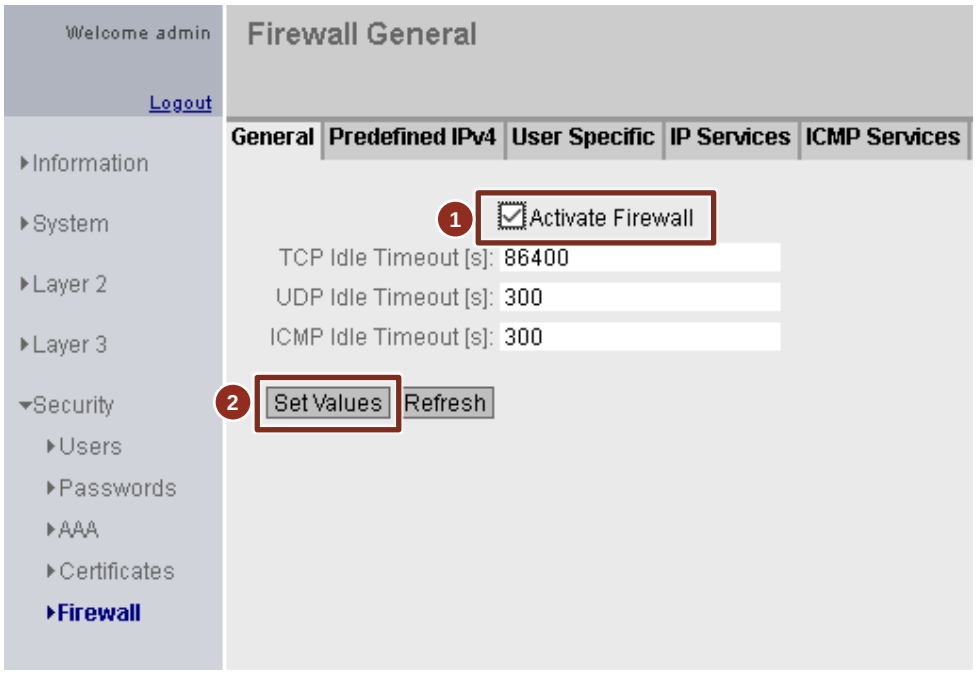
2. In the "Configuration" tab, vlan1 and vlan2 are then assigned to the same bridge ID (2).
3. In addition, vlan1 is configured as master (IP address configuration of this VLAN is used for the bridge) and vlan2 as member (IP address configuration of this VLAN is discarded and not used) (3).
4. Finally, the Inter-VLAN bridge configuration is activated via "Enable" (4) and confirmed via "Set Values" (5).



With this configuration, message frames with VLAN ID 1, i.e. coming from port 1 to port 2 with VLAN ID 2 and vice versa, can be output.

5.2.4 Activating the firewall

In the last step the firewall is activated in the register "General" (1) and confirmed via "Set Values" (2).



Result

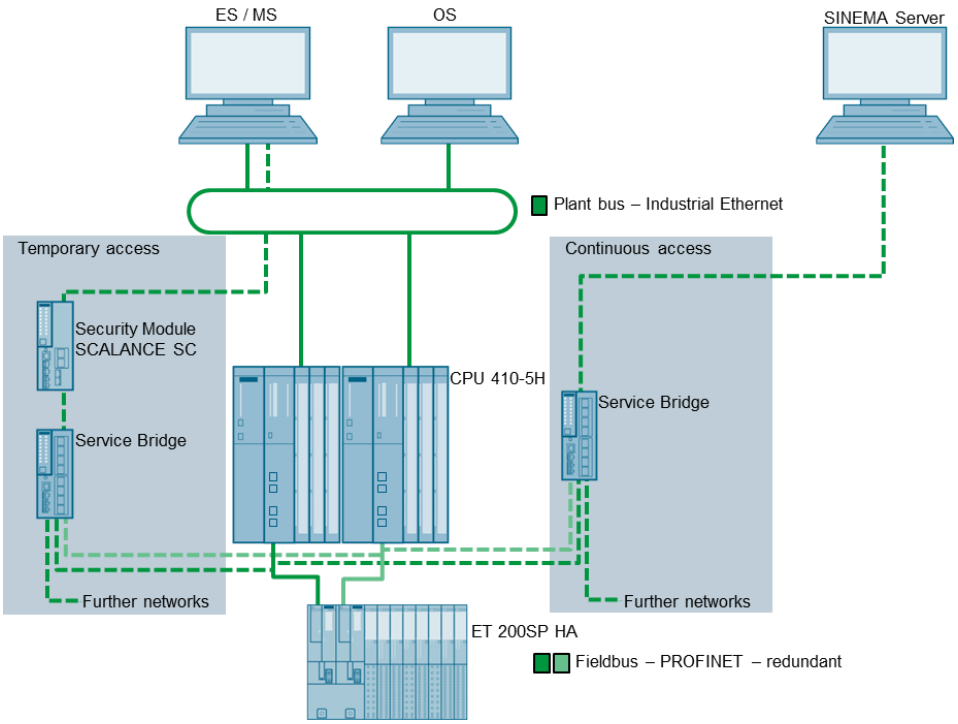
The configuration of the SCALANCE SC is now complete and it is in production operation.

6 Additional information

6.1 Continuous access, e.g. for SINEMA server

If continuous access to the PN networks is needed (e.g. when using the SINEMA server) it is recommended not to use the Service Bridge on the plant bus. In the following plant configuration, apart from the Service Bridge for temporary access from the plant bus, a second, separate, Service Bridge is also provided for the SINEMA server.

Figure 6-1



If the SINEMA server is to be additionally connected to the plant bus, this connection must be implemented via a network adapter other than the connection to the Service Bridge. Please note that no routing is allow een the network adapters and that the Windows Firewall is active on the SINEMA server. With these measures, there is no need for an additional firewall between SINEMA Server and the Service Bridge.

6.2 Networks with a Y switch (XF204-2BA DNA)

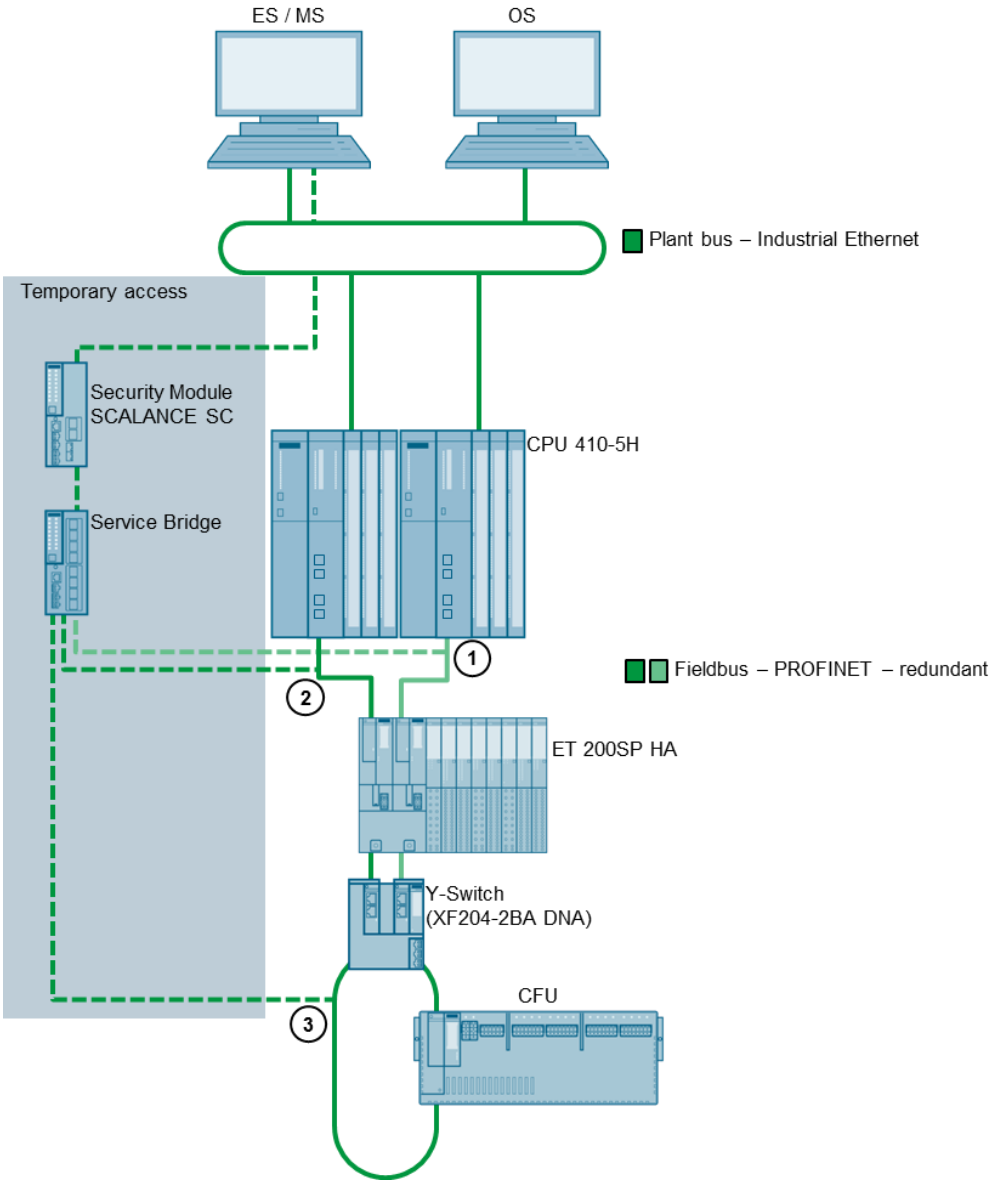
When the Service Bridge is used in a R1 network with a Y switch, the following devices are available depending on the access point (see Figure 6-2):

(1) Access in the R1 network subnet 1
Devices in this subnet and behind the Y switch are accessible.

(2) Access in the R1 network subnet 2
Devices in this subnet and behind the Y switch are accessible.

(3) Access behind the Y switch
Devices behind the Y switch and in both subnets of the R1 network are accessible.

Figure 6-2



In order to be able to reach all the devices in the network, connection is possible either via access points (1) and (2) or, alternatively, via access point (3). The connection variant can be selected depending on the local conditions.

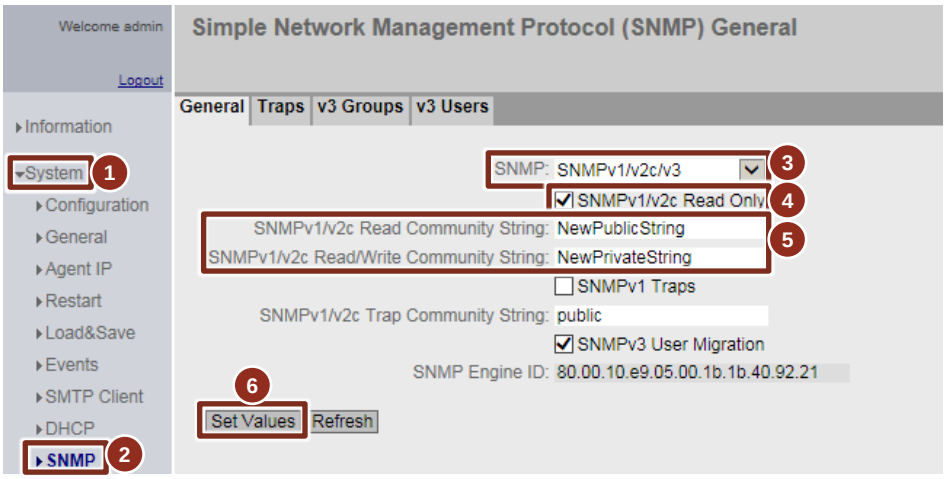
6.3 SNMP configuration for using the Maintenance Station

SNMP version v1 or v2c is required for integration of network components in the asset management of the Maintenance Station. For security reasons, only SNMP version 3 is enabled in the configuration of the Service Bridge.

The following section explains the procedure, which must be followed to enable and configure SNMPv1/v2c in the Service Bridge.

Procedure

1. Navigate to the "System > SNMP" menu (1)(2).
2. In the SNMP drop-down list, select the entry "SNMPv1/v2c/v3" (3) and select the "SNMPv1/v2c Read Only" (4) check box.
   When the check box is selected, only read access to the SNMP tags via SNMPv1/v2c is possible.
3. In the "SNMPv1/v2c Read Community String" (5) entry field, enter a character string for the community string, which is to be used for read access via SNMP.
4. In the "SNMPv1/v2c Read/Write Community String" (5) entry field, enter a character string for the community string, which is to be used for read and write access via SNMP.
5. Click the "Set Values" button (6) to confirm the settings.



Note

Since the SNMP community strings provide access protection, do not use the default values "public" or "private".

The recommended minimum length for community strings is 6 characters.

7 Appendix

7.1 Service and Support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:
support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:
www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:
www.siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:
support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:
support.industry.siemens.com/cs/ww/en/sc/2067

7.2 References

Table 7-1

	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Download page of this entry https://support.industry.siemens.com/cs/ww/en/view/109747975
\3\	Security guidelines by PROFIBUS & PROFINET International (PI): https://www.profibus.com/download/profinet-security-guideline
\4\	PROFINET in Process Automation with SIMATIC PCS 7 https://support.industry.siemens.com/cs/ww/en/view/72887082

7.3 Change documentation

Table 7-2

Version	Date	Change
V1.0	08/2017	First version
V1.1	10/2017	Expansion by chapter 3.5.3 and chapter 6.3
V1.2	05/2018	Update for Firmware V4.0
V1.3	08/2018	Firewall configuration using the example of a SCALANCE SC632-2C (Chapter 5)
V1.4	04/2019	Revised version, SCALANCE SC and Firmware V4.1
V1.5	06/2020	Adaption SCALANCE SC632-2C configuration FW V2.0.1