Segmenting a Network Using VLANs

SCALANCE X

https://support.industry.siemens.com/cs/ww/en/view/109749844

Siemens Industry Online Support

Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice.
If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications − e.g. Catalogs − the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.
Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.
Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

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 only form one element of such a concept.
Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.
Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer’s exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Table of Contents

1 Introduction

1.1 Overview

Requirement

A stable and securely functioning network is an important fundamental requirement in a company or an automation system. If network communication fails or is limited, for example, due to overload or network errors, this can result in high costs for the company.

A minor error is often enough to paralyze an entire network. The following list shows a number of minor errors that can have a significant impact on the network:

- Accidental installation of a DHCP server.
- Use of duplicate IP addresses.
- Incorrect connection of device ports, resulting in network loops.

All these problems affect all network devices in the entire Layer 2 network segment.

Action

To increase the network's stability, larger communication networks are divided into several smaller network segments with their own broadcast domains. To save hardware costs caused by additional switches, the networks are not separated physically, but virtually.

Benefits

Segmenting a large network into several smaller network segments provides you with the following benefits:

- Different divisions get their own networks.
- Reduced network load as, for example, broadcast requests stay within a segment.
- In smaller networks, segmenting allows fast diagnostics in the event of a network disturbance and accelerated troubleshooting.

Virtual segmentation as a possible solution

To implement the above action, a larger physical network is split into several smaller virtual units using the "Virtual Local Area Network" (VLAN) function. A VLAN is a logical network segment within a physical network. To split the network into several logical units, the frames of the devices are tagged with a special VLAN ID in the Ethernet protocol.

Using this technological concept to segment your network provides you with the following advantages:

- Can be implemented in small and very large networks.
- Allows you to save costs as virtual segmentation makes additional hardware unnecessary.
- Less cabling as virtual segmentation can coexist in a reaction-free manner.
- Supports the security aspect as you can use virtual network segments for protection against interception and spying.
- Allows you to increase your network's performance. Virtual network segments reduce broadcast domains. Due to broadcast encapsulation, not all systems need to receive and process all sent broadcasts of the entire LAN.

- Special quality of service information allows you to prioritize network traffic. For example, this applies to VoIP applications and PROFINET IO.

Possible application

Virtual networks can be used in a wide range of applications. You can use VLANs for both private and corporate networks.

VLANs are used for different reasons. However, these reasons always involve increased security and/or performance requirements.

The following list illustrates how VLANs can contribute to increasing security and performance in the network:

- The logical separation of networks limits broadcasts.
- Users or devices in a VLAN can only communicate within the assigned VLAN. Communication across VLANs must be explicitly configured.
- VLANs allow you to set up a separate guest VLAN for guests in the wireless LAN.
- Using VLANs, network traffic can be forwarded with different priorities.

1.2 Application-specific implementation

Overview

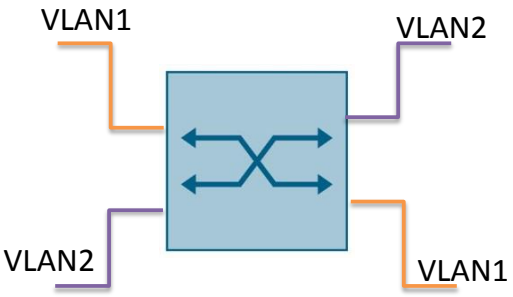
This application example shows you how "Virtual Local Area Networks" (VLANs) work. Two different sample configurations are used to explain the use of VLANs step by step. This document covers the following scenarios:

- Configuring VLANs within one switch
- Configuring VLANs between multiple switches

Scenario 1: Configuring VLANs within one switch

This scenario shows a simple VLAN configuration. The VLAN is within one switch.

Figure 1-1

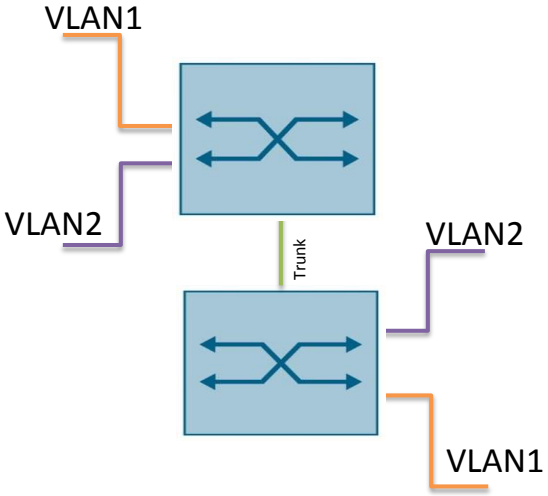


VLAN1 and VLAN2 contain network devices that are allowed to communicate with each other. VLAN2 cannot be accessed from VLAN1.

Scenario 2: Configuring VLANs between multiple switches

This scenario shows an expanded configuration of Scenario 1. The VLAN extends over two switches.

Figure 1-2



VLAN1 and VLAN2 contain network devices that are allowed to communicate with each other. VLAN2 cannot be accessed from VLAN1.
The two switches are connected through a trunk port.

1.3 Mode of operation

1.3.1 "Virtual Local Area Network"

Description

A VLAN is a logical subnet within a switch or complete physical network.

When you physically separate a network, the devices are assigned to a switch port. However, when a network is separated using VLANs, the devices are logically separated by a VLAN TAG in the Ethernet frame.

Switches with VLAN capability can assign the tagged frames to specific VLANs and therefore set up logically separated networks based on a shared infrastructure.

A physically contiguous definition of the VLANs is not mandatory. VLANs can also extend over wide-ranging networks and multiple switches.

IEEE 802.1Q specifies the principle of VLANs.

Separation at Layer 2

A VLAN has to be considered as a stand-alone LAN. At Ethernet Layer 2, data cannot be exchanged between different VLANs. Each VLAN therefore defines its own broadcast domains.

VLAN TAG

Ethernet frames in a VLAN are tagged with a VLAN TAG. This VLAN TAG adds four bytes to the Ethernet header and manages various pieces of VLAN information.

Using the VLAN configuration in the switch, you can influence the following information from the VLAN TAG:

- VLAN ID
- Frame priority

The VLAN ID defines which VLAN a data packet belongs to. All devices with the same VLAN ID are in one logical network. The VLAN ID is also often called a "tag" and adding the VLAN ID to the frame is also referred to as "tagging".

The priority is a value between 0 and 7. 7 has the highest priority. This number specifies the frame's priority. It allows you to prioritize it over other frames.

Assigning VLANs

The easiest and most frequently used tagging method is port-based tagging.

When using port-based VLAN methods, the VLAN is statically connected to a switch port. Then this port alone defines which VLAN the device connected to this port belongs to. In the switch configuration, you can define, for each port, how the incoming (ingress) and outgoing (egress) frames will be processed. On the egress side, a port can be assigned to multiple VLANS; on the ingress side, however, it can only be assigned to one VLAN.

Note Chapter 3 provides detailed information about how VLANs work.

1.3.2 Requirements/boundary conditions

Network modules

To get a VLAN running, you need a network module with VLAN capability. The network module must be capable of managing VLANs. Current managed network components usually support all VLAN functions. In most cases, you will find the VLAN configuration in the Layer 2 functions of the switch. The VLAN capability is indicated by the keyword 802.1Q in the devices' technical specifications.

Ethernet frame length

The VLAN TAG increases the permitted total frame length from 1518 to 1522 bytes. It must be checked whether the switches in the network can process this length/frame type. If this is not the case, only standard length frames may be sent to these nodes. Normally, the frame without a VLAN TAG (1518 bytes) is sent to endpoints.

Ring topology

Two ring ports are defined to create a ring topology. These ring ports must be assigned to the default VLAN (VLAN1). However, ring ports can forward frames for other VLANs.

1.4 Components used

This application example was created with the following hardware and software components:

Table 1-1

Component	No.	Article no.	Note
SCALANCE XC206-2	2	6GK5206-2BD00-2AC2	The SCALANCE is used for both scenarios.
CPU S7 1516-3	1	6ES7516-3AN01-0AB0	The CPU is used as a test device to demonstrate VLAN/PROFINET communication. You can also use a different IO controller.
IO device, e.g. an ET 200SP	1	6ES7155-6AU00-0BN0	The ET 200SP is used as a test device to demonstrate VLAN/PROFINET communication. You can also use a different IO device.
PC/PG			Configuration PC
Web browser			
Primary Setup Tool			Allows you to assign an IP address to the SCALANCE.

Note

In this application, you test the VLAN function by establishing PROFINET communication between the CPU and the ET 200SP and sending "ping" commands to the CPU and the ET 200SP.

If you do not have a CPU/ET 200SP to hand, you can also use a different network device. When choosing a network device, make sure that it at least responds to a ping command.

This application example consists of the following components:

Table 1-2

Component	File name	Note
This document	109749844_VLAN_DOKU_V10_en.pdf	

2 Engineering

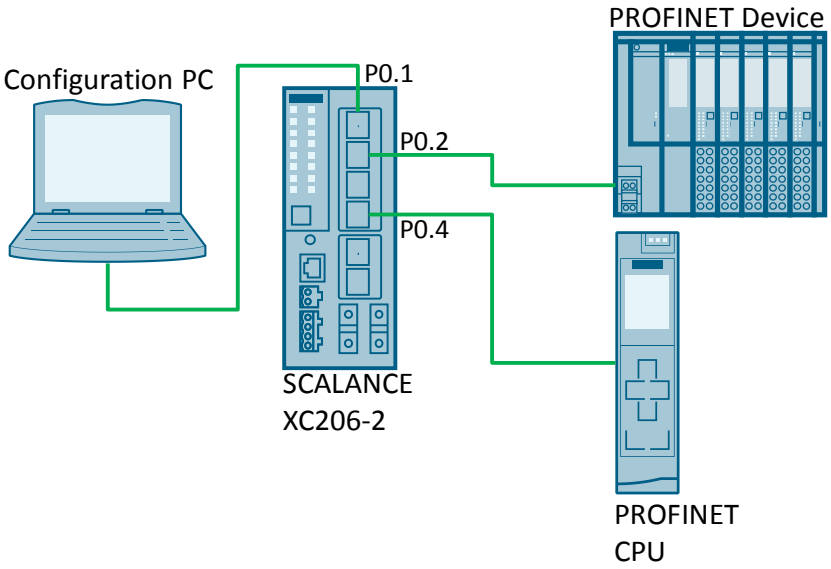
2.1 Hardware configuration

Scenario 1: Configuring VLANs within one switch

The following figure shows you how to interconnect the components for Scenario 1.

Pay attention to the port numbers on the switch. When you configure the VLAN in the next step, these port numbers will be used.

Figure 2-1

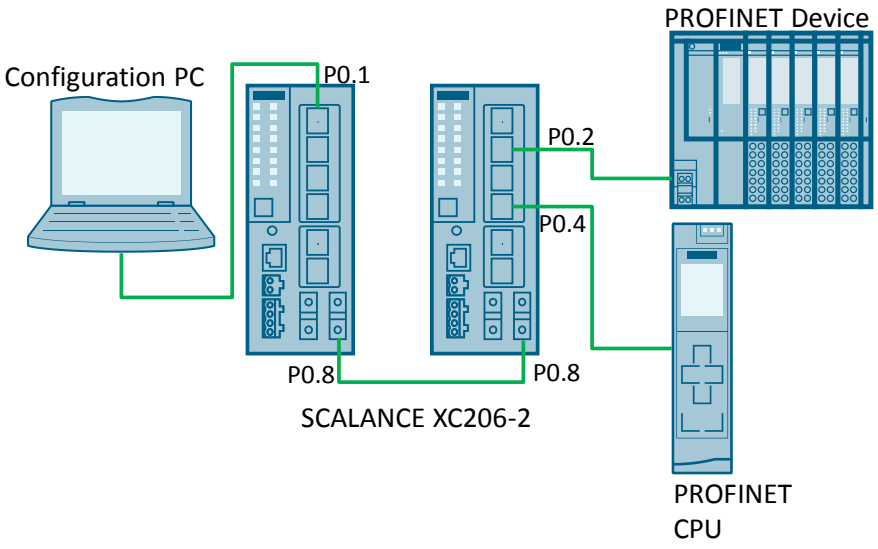


Scenario 2: Configuring VLANs between two switches

The following figure shows you how to interconnect the components for Scenario 2.

Pay attention to the port numbers on the switch. When you configure the VLAN in the next step, these port numbers will be used.

Figure 2-2



2.2 Preparing the configuration

In the last chapter, you configured the hardware for the scenario. To be able to configure the devices, you have to prepare them. This includes:

- Assigning IP addresses
- Creating the TIA project for the PROFINET components
- Starting Web Based Management in the SCALANCE

Overview of IP addresses

The following table shows you which IP addresses this application example uses. You can also use different IP addresses. In this application example, all devices are in one subnet.

Table 2-1

Component	IP address	VLAN ID
Configuration PC	192.168.0.1/24	1
SCALANCE XC206-2 (left)	192.168.0.10/24	1/2
SCALANCE XC206-2 (right)	192.168.0.11/24	1/2
CPU	192.168.0.12/24	2
ET 200SP	192.168.0.13/24	2

Note You can also use different subnets in the VLANs.

Once you have defined the VLANs in the switch, you can create subnets for the VLANS; in the switch, go to "Layer 3 > Subnets".
This application example focuses on creating and configuring VLANs. For this reason, it uses a flat network.

Assigning IP addresses

For the network devices to be accessible via Layer 3, you have to assign an IP address to all components.

- You can set the PC's IP address using the Network Center.
- Set the IP address of the CPU and the ET 200SP in the TIA project.
- In the as-supplied state or after setting to factory default, the SCALANCE has no IP address and cannot be accessed using Web Based Management. To access the SCALANCE, use, for example, the Primary Setup Tool.

Creating the TIA project

Note You only need to create the TIA project if you are using the CPU and the ET 200SP.

To configure the CPU and the ET 200SP, use TIA Portal to create a new project. Add the project to your modules and configure them as required. As IP addresses, assign the addresses listed in Table 2-1. Set up PROFINET communication.

Then download the project to your CPU.

Starting Web Based Management

To open Web Based Management of the SCALANCE, use the address "http://<IP address of SCALANCE>".

On the configuration PC, start a Web browser and enter the URL, for example, http://192.168.0.10. Default login data:

- User: admin
- Password: admin

In the as-supplied state or after setting to factory default, you will be prompted to change the admin password when logging in for the first time.

2.3 Configuring the "Trunk" port mode

When you connect two switches, the relevant ports must be set such in the VLAN configuration that the ports retain the VLAN TAG. As a result, the VLAN information is not lost when forwarding from one switch to another. This is particularly necessary if the VLAN extends over multiple switches and you want to retain the priority.

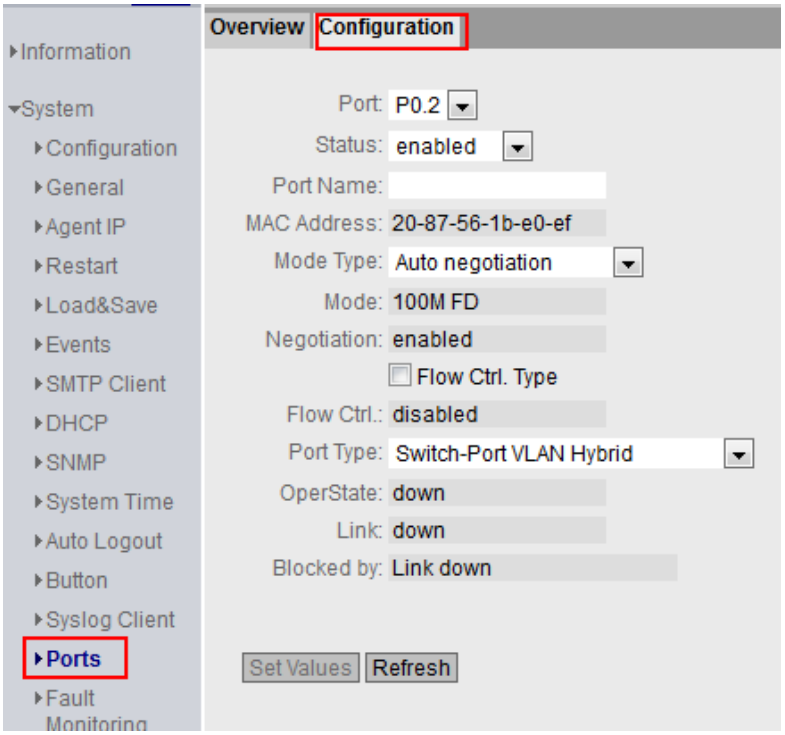
The "Trunk" port mode is available especially for this connection between switches. The "Trunk" port mode causes the frames of all VLANS configured on this device to be forwarded on this port, including the VLAN TAG.

This application example needs the trunk port for Scenario 2.

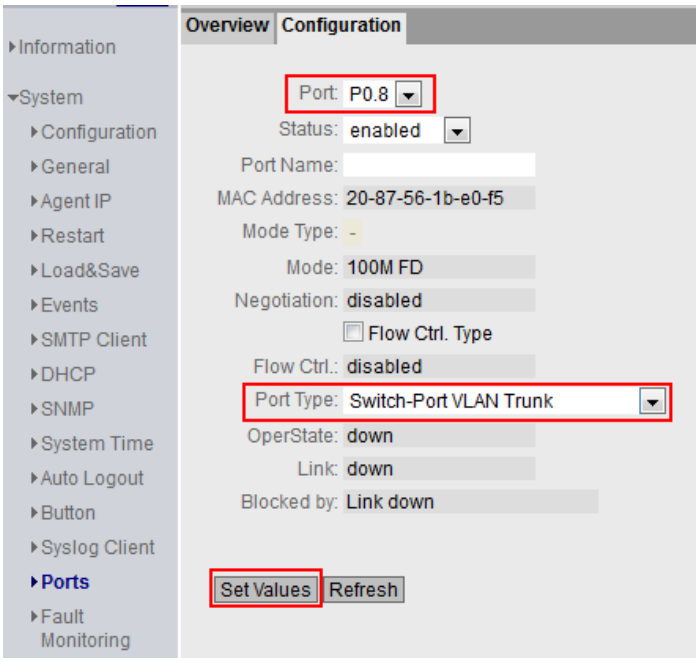
In this scenario, the switches are connected via port 0.8.

Proceed as follows to turn port P0.8 into a trunk port:

1. Navigate to the "System > Ports" menu and go to the "Configuration" tab.



2. From the "Port" drop-down list, select the value "P0.8". Use the "Port Type" drop-down list to change the type to "Switch-Port VLAN Trunk". To apply the changes, click the "Set Values" button.



Result

You have configured port P0.8 as a trunk port.

2.4 Configuring the VLANs

Configuring the VLANs consists of several steps:

- Customize VLAN mode
- Define VLANs
- Make egress settings
- Make ingress settings

2.4.1 VLAN port assignment overview

Before you configure the VLANs, it is useful to have a graphical overview that shows the assignment of the switch ports to the VLANs. The following section shows how the VLANs are assigned to the switch ports for each scenario.

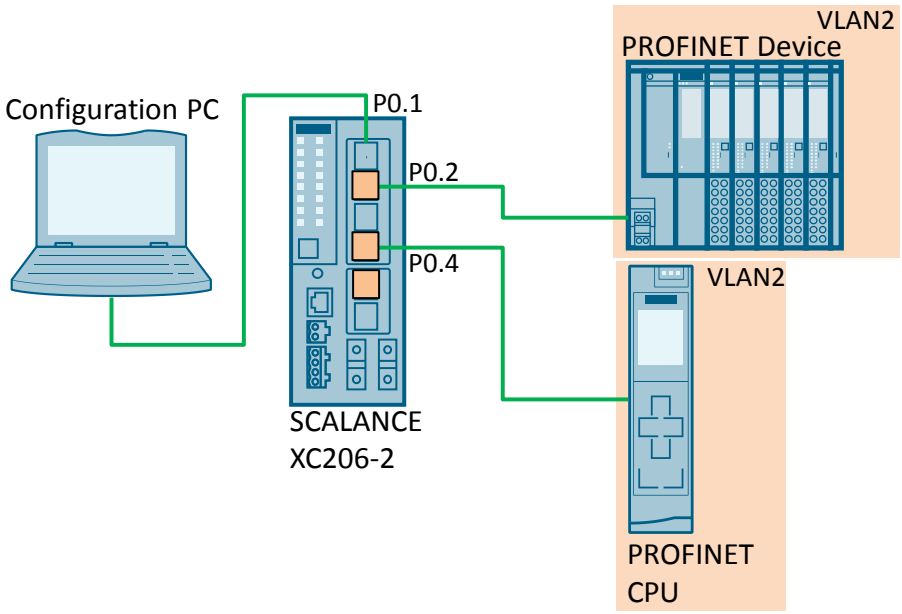
VLAN←→ port assignment for Scenario 1

The following figure provides an overview of the VLAN←→port assignment for Scenario 1.

The switch ports shown in color (port P0.2, port P0.4 and port P0.5) are assigned to VLAN2.

The other switch ports are set to their defaults and therefore belong to the default VLAN (VLAN1).

Figure 2-3



VLAN←→ port assignment for Scenario 2

The following figure provides an overview of the VLAN←→port assignment for Scenario 2.

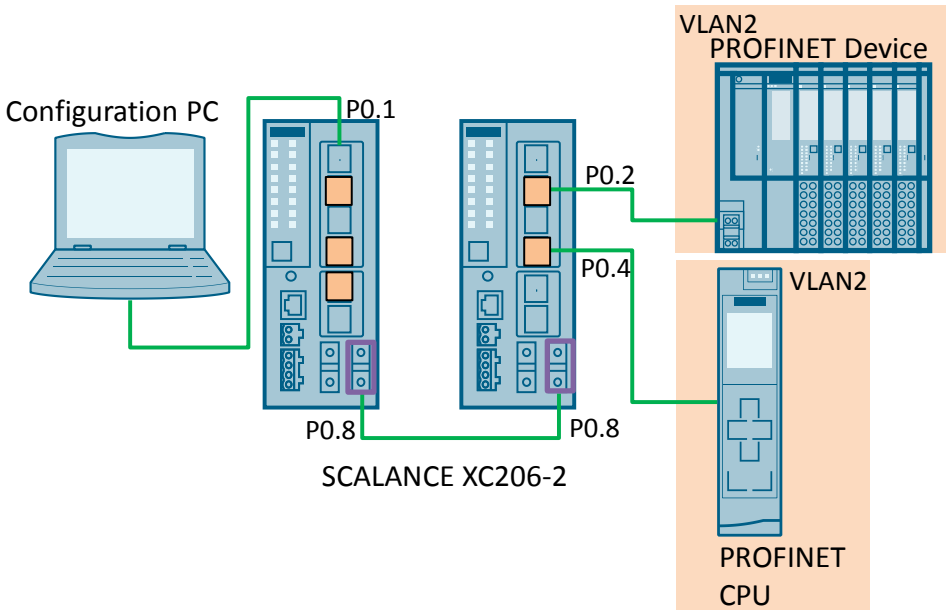
The switch ports shown in color are assigned to VLAN2. These are the following ports:

- Port P0.2, port P0.4 and port P0.5 of the left switch
- Port P0.2 and port P0.4 of the right switch

The ports bordered in color (port P0.8) are ports in "Trunk" mode.

The other switch ports are set to their defaults and therefore belong to the default VLAN (VLAN1).

Figure 2-4

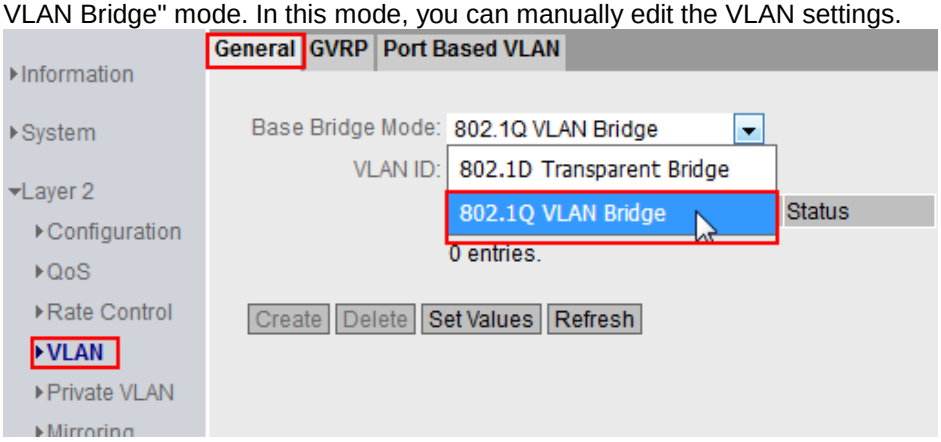


2.4.2 Customizing the VLAN mode

In this section, you set the VLAN mode.

Proceed as follows:

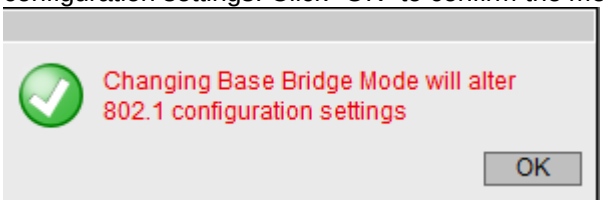
1. Use the "Layer 2 > VLAN" menu to open the VLAN configuration screen. You are automatically in the "General" tab. From the drop-down list, select "802.1Q VLAN Bridge" mode. In this mode, you can manually edit the VLAN settings.



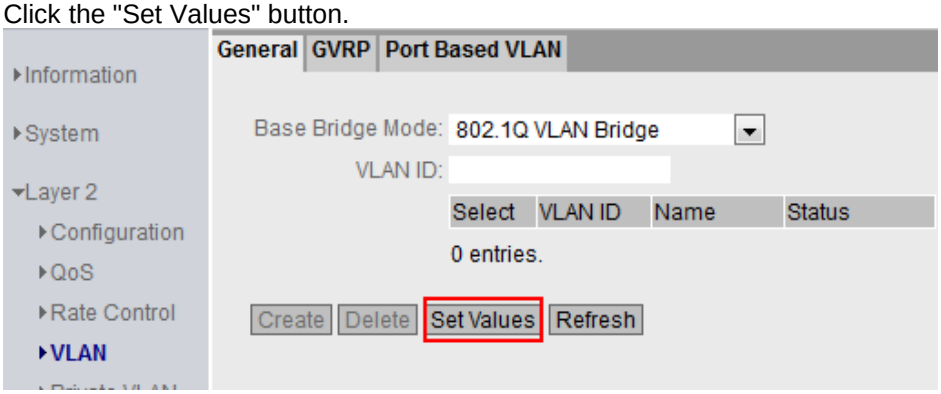
Note

The "802.1Q Transparent Bridge" setting transparently forwards all frames (with and without VLAN TAG). If a VLAN TAG exists, the switch nevertheless complies with the priority and forwards the frame accordingly.

2. A message appears that changing the mode will affect other 802.11 configuration settings. Click "OK" to confirm the message.



3. Click the "Set Values" button.



Result

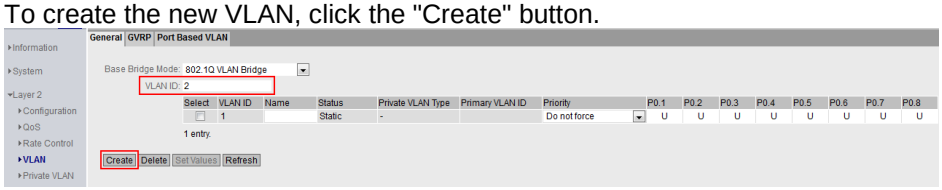
You have set the VLAN mode. The default VLAN (VLAN ID 1) is created and displayed in the list. On all ports, VLAN ID 1 is set to "U" ("Untagged") by default. To make sure that even endpoints that do not support VLANs can receive these frames, all ports on the device, by default, send frames without a VLAN TAG.

Select	VLAN ID	Name	Status	Private VLAN Type	Primary VLAN ID	Priority	P0.1	P0.2	P0.3	P0.4	P0.5	P0.6	P0.7	P0.8
☐	1		Static	-		Do not force	U	U	U	U	U	U	U	U

2.4.3 Defining VLANs

To define more VLANs, enter a new ID in the "VLAN ID" input field. For this example, use VLAN ID 2.

To create the new VLAN, click the "Create" button.



Result

You have created a new VLAN with VLAN ID 2. The new VLAN is displayed in the list. On all ports, VLAN ID 2 is set to "-" by default. This setting does not forward frames for VLAN2 via these ports.

Select	VLAN ID	Name	Status	Private VLAN Type	Primary VLAN ID	Priority	P0.1	P0.2	P0.3	P0.4	P0.5	P0.6	P0.7	P0.8
☐	1		Static	-		Do not force	U	U	U	U	U	U	U	U
☐	2		Static	-		Do not force	-	-	-	-	-	-	-	-

Note

When you configure VLANs in the switch, make sure that the port that connects you to the switch is always also assigned to the default VLAN (VLAN ID 1).

If you remove this port from the default VLAN, the switch can no longer be accessed. In this case, connect to another port assigned to the default VLAN.

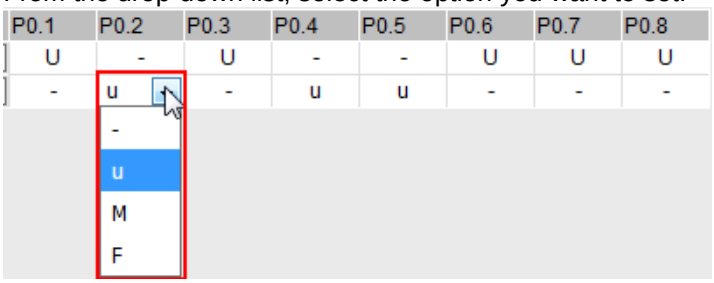
2.4.4 Making the egress settings

The next step is to define the use of the ports in the VLAN. You set which VLAN frames are allowed to be forwarded via which port and whether or not the VLAN information will be retained.

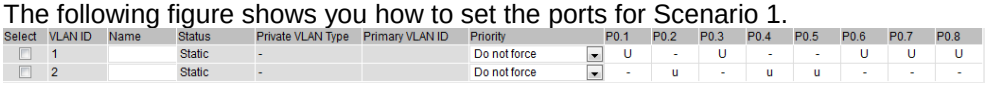
Instructions for Scenario 1

Proceed as follows to define the use of the ports in a VLAN:

1. To configure a port, click the appropriate table field in the row of the port you want to configure.
   From the drop-down list, select the option you want to set.



2. The following figure shows you how to set the ports for Scenario 1.



   Use the "u" option to assign VLAN2 to the following ports:

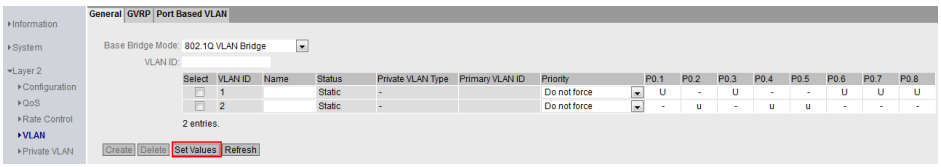
   - Port P0.2: IO device
   - Port P0.4: IO controller
   - Port P0.5: reserved for later test purposes

   As an endpoint is connected to each of these three ports, outgoing frames are to be sent without a tag ("u" option).

Note

This lower case "u" indicates that the egress and ingress settings for this port differ. The ingress setting contains a different VLAN ID with which incoming frames are tagged.
When the ingress setting has been made (see Chapter 2.4.5), the setting changes to an upper case "U".

3. When you have set all ports, click the "Set Values" button.



Result

With this setting, frames with VLAN ID 2 are only forwarded via ports P0.2, P0.4 and P0.5.

Instructions for Scenario 2

To set the ports for Scenario 2, follow the instructions for Scenario 1.

The following figure shows you how to set the ports for Scenario 2 for the left switch.

Select	VLAN ID	Name	Status	Private VLAN Type	Primary VLAN ID	Priority	P0.1	P0.2	P0.3	P0.4	P0.5	P0.6	P0.7	P0.8
☐	1		Static	-		Do not force	U	-	U	-	-	U	U	M
☐	2		Static	-		Do not force	-	u	-	u	u	-	-	T

If you have declared port P0.8 as a trunk port as required (see Chapter 2.2), the port is automatically registered for all VLANs ("T" option).

Use the "u" option to assign VLAN2 to the following ports:

- Port P0.2: IO device
- Port P0.4: IO controller
- Port P0.5: reserved for later test purposes

For later test purposes, an endpoint is connected to each of these three ports. Therefore, outgoing frames are to be sent without a tag ("u" option).

Result
With this setting, frames with VLAN ID 2 are only forwarded via ports P0.2, P0.4, P0.5 and P0.8.

The following figure shows you how to set the ports for Scenario 2 for the right switch.

Select	VLAN ID	Name	Status	Private VLAN Type	Primary VLAN ID	Priority	P0.1	P0.2	P0.3	P0.4	P0.5	P0.6	P0.7	P0.8
☐	1		Static	-		Do not force	U	-	U	-	U	U	U	M
☐	2		Static	-		Do not force	-	u	-	u	-	-	-	T

If you have declared port P0.8 as a trunk port as required (see Chapter 2.2), the port is automatically registered for all VLANs ("T" option).

Use the "u" option to assign VLAN2 to the following ports:

- Port P0.2: IO device
- Port P0.4: IO controller

An endpoint has already been connected to these two ports. Therefore, outgoing frames are to be sent without a tag ("u" option).

Result
With this setting, frames with VLAN ID 2 are only forwarded via ports P0.2, P0.4 and P0.8.

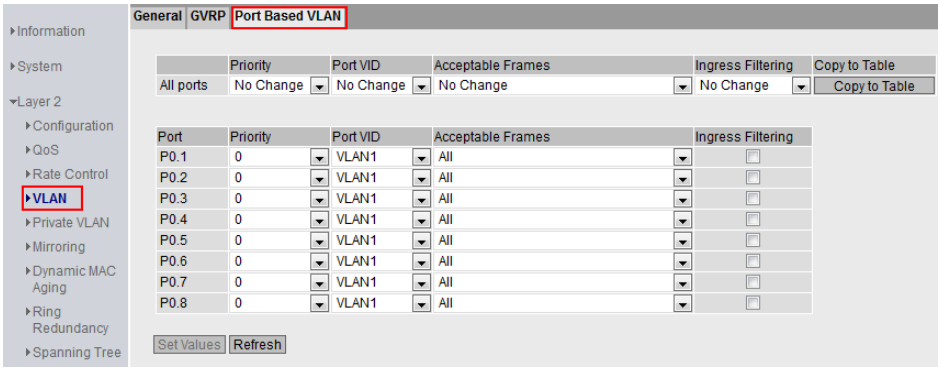
2.4.5 Making the ingress settings

In this section, you define the configuration of the port properties for receiving frames.
For each port, you define which VLAN, i.e., which VLAN ID and which priority will be assigned to a frame that arrives on this port and does not yet have a VLAN TAG. The ingress assignment must be unique. You can only assign a single VLAN to a port.

Instructions for Scenario 1

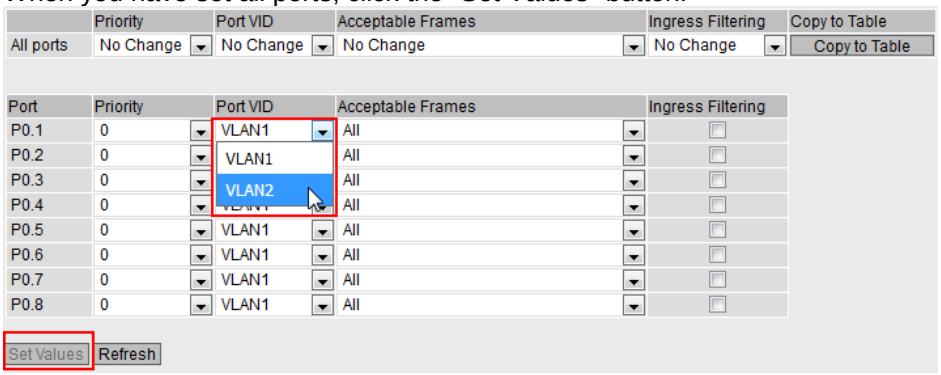
Proceed as follows:

1. Go to the "Port Based VLAN" tab.



2. To configure a port, click the appropriate table field in the row of the port you want to configure. Aside from the default VLAN, the drop-down list lists all the VLANs you have previously created. Select the desired VLAN ID. All frames that reach this port without a VLAN TAG will be tagged with the set VLAN ID.

   When you have set all ports, click the "Set Values" button.



3. The following figure shows you how to set the ports for Scenario 1.

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P0.1	0	VLAN1	All	
P0.2	0	VLAN2	All	
P0.3	0	VLAN1	All	
P0.4	0	VLAN2	All	
P0.5	0	VLAN2	All	
P0.6	0	VLAN1	All	
P0.7	0	VLAN1	All	
P0.8	0	VLAN1	All	

All frames that arrive on ports P0.2, P0.4 and P0.5 and do not have a VLAN TAG will be tagged with VLAN ID 2.

Instructions for Scenario 2

To set the ports for Scenario 2, follow the instructions for Scenario 1.

The following figure shows you how to set the ports for Scenario 2 for the left switch.

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P0.1	0	VLAN1	All	
P0.2	0	VLAN2	All	
P0.3	0	VLAN1	All	
P0.4	0	VLAN2	All	
P0.5	0	VLAN2	All	
P0.6	0	VLAN1	All	
P0.7	0	VLAN1	All	
P0.8	0	VLAN1	All	

All frames that arrive on ports P0.2, P0.4 and P0.5 and do not have a VLAN TAG will be tagged with VLAN ID 2.

The following figure shows you how to set the ports for Scenario 2 for the right switch.

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P0.1	0	VLAN1	All	
P0.2	0	VLAN2	All	
P0.3	0	VLAN1	All	
P0.4	0	VLAN2	All	
P0.5	0	VLAN1	All	
P0.6	0	VLAN1	All	
P0.7	0	VLAN1	All	
P0.8	0	VLAN1	All	

All frames that arrive on ports P0.2 and P0.4 and do not have a VLAN TAG will be tagged with VLAN ID 2.

2.5 Use

Using the application example is the same for all scenarios. To test the VLAN function, plug the configuration PC into different switch ports and run the following two test scenarios:

1. Access Web Based Management of the SCALANCE
2. "Ping" command to the test device

Test 1: Configuration PC in VLAN1

The configuration PC is connected to a switch port that is assigned to VLAN1, for example port P0.1.

Now run the two test scenarios and analyze the reaction. The following table shows the results of action and reaction:

Table 2-2

Action	Reaction	Reason
Open your Web browser and enter the URL of the SCALANCE.	Web Based Management opens.	The configuration PC's frames are tagged with VLAN ID 1. By default, the "agent" of the SCALANCE is only assigned to VLAN1. The configuration PC and the "agent" are in a common VLAN.
Send a "Ping" command to the CPU: Open Command Prompt on your PC and enter the "ping <IP address of CPU>" command.	The "Ping" command fails. No reply packets from the CPU arrive.	The configuration PC's frames are tagged with VLAN ID 1. The CPU is assigned to VLAN2. Frames from VLAN1 are not forwarded via the CPU port.

Test 2: Configuration PC in VLAN2

The configuration PC is connected to a switch port that is assigned to VLAN2, for example port P0.5.

Now run the two test scenarios and analyze the reaction. The following table shows the results of action and reaction:

Table 2-3

Action	Reaction	Reason
Open your Web browser and enter the URL of the SCALANCE.	Web Based Management does not open.	The configuration PC's frames are tagged with VLAN ID 2. By default, the "agent" of the SCALANCE is only assigned to VLAN1. The configuration PC and the "agent" are in different VLANs.
Send a "Ping" command to the CPU: Open Command Prompt on your PC and enter the "ping <IP address of CPU>" command.	The "Ping" command is successful.	The configuration PC's frames are tagged with VLAN ID 2. The CPU is assigned to VLAN2. The frames of the PC are forwarded via the CPU port.

3 Valuable Information

3.1 VLAN basics

3.1.1 The IEEE 802.1Q standard

A VLAN is a logical subnet within a switch or complete physical network.

Unlike the physical separation through the assignment to a switch port, the separation using VLANs logically separates the devices by a VLAN TAG in the Ethernet frame.
Switches with VLAN capability can assign the tagged frames to specific VLANs and therefore set up logically separated networks based on a shared infrastructure. The VLAN can be extended over multiple switches.

IEEE 802.1Q specifies the principle of VLANs.

3.1.2 Tagging method

Port-based VLAN

The easiest and most frequently used tagging method is port-based tagging.

Tagging means adding the VLAN ID to the frame.

Note This document covers only the port-based VLAN assignment.

When using port-based VLAN methods, the VLAN is statically connected to a switch port. Then this port alone defines which VLAN the device connected to this port belongs to. In the switch configuration, you can define, for each port, how the incoming and outgoing frames will be processed. On the outgoing side, a port can be assigned to multiple VLANS; on the incoming side, however, it can only be assigned to a single VLAN.

Note For detailed information about processing frames, see Chapter 3.2.

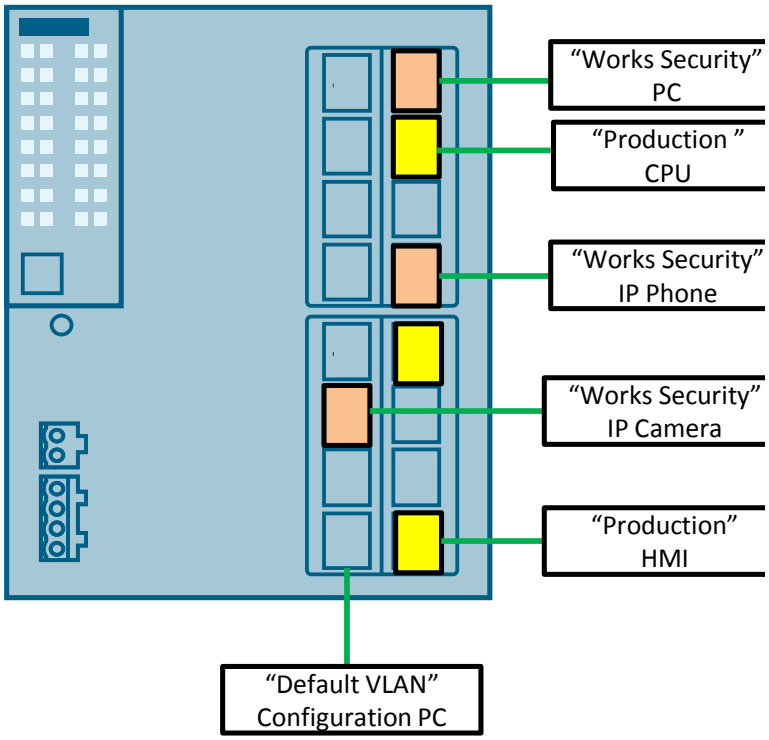
Example

The following example shows a simple configuration of a port-based VLAN.

The switch was separated into three VLANs:

- Default VLAN VLAN1 (shown in blue in the figure)
- "Production" VLAN2 (shown in yellow in the figure)
- "Works Security" VLAN3 (shown in orange in the figure)

Figure 3-1



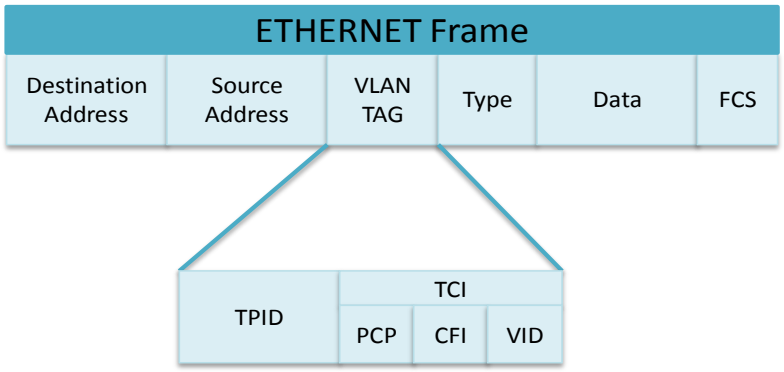
Only devices in the same VLAN can communicate with each other. Direct data exchange between the VLANs is not possible.

3.1.3 VLAN information in the Ethernet header

VLAN TAG

The Ethernet frames in a VLAN are tagged with a VLAN TAG. This VLAN TAG adds four bytes to the Ethernet header and manages various pieces of VLAN information.
The following figure shows where the VLAN TAG is placed in the Ethernet frame.

Figure 3-2



The VLAN TAG contains the following information:

- The "Tag Protocol Identifier" (TPID) specifies the specific tag. It is set to 0x8100 and cannot be modified.
- The "Tag Control Information" (TCI) contains the actual VLAN information. The TCI is divided into the following sections:
  - The "Priority Code Point" (PCP) is a value between 0 and 7. It specifies the frame priority.
  - The "Canonical Format ID" (CFI) specifies the information format.
  - The "VLAN ID" (VID) specifies the VLAN's number, which defines the membership to a VLAN. All devices with the same VLAN ID are in one logical network.

When configuring the VLAN, you can influence the following information:

- "Priority Code Point" (PCP) (see Chapter 3.3)
- "VLAN ID" (VID)

VLAN ID

Port-based VLANs virtually break up one managed switch into multiple switches. Each VLAN is tagged with a VLAN ID between 1 and 4094; VLAN ID 1 is used as the default VLAN.

Note VLAN ID 0 cannot be set. Frames with VLAN ID 0 only contain priority information and are treated as untagged frames (frames without VLAN information). VLAN ID 0 is used for PROFINET in conjunction with VLAN combination (see Chapter 3.4).

In the as-supplied state or after setting to factory default, all ports of a managed switch are assigned to the default VLAN. In this state, the managed switch works like a standard switch without VLANs. The switch's IP address is usually only accessible via ports that are permanently assigned to this default VLAN.

Note When you configure VLANs in the switch, make sure that the port that connects you to the switch is always also assigned to the default VLAN (VLAN ID 1).

If you remove this port from the default VLAN, the switch can no longer be accessed. In this case, connect to another port assigned to the default VLAN.

3.2 Processing frames

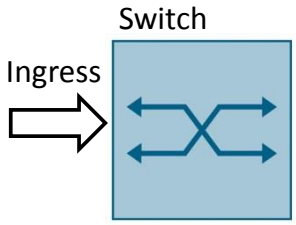
You configure the VLAN in the switch using Web Based Management or the command-line interface.

For each port, you can assign the VLAN (ingress processing) and define which frames from certain VLANs this port is allowed to forward (egress processing).

3.2.1 Ingress setting

The ingress setting affects frames that are received on a switch port.

Figure 3-3:



Description

For each port, the ingress setting defines which VLAN, i.e., which VLAN ID and which priority will be assigned to a frame that arrives on this port and does not yet have a VLAN TAG. This assignment must be unique. This means that a frame can only be assigned to one VLAN. If a frame that has already been tagged arrives on the port, the VLAN TAG is retained and the unmodified frame is forwarded to the appropriate port(s).

Ingress filter

If you do not set up the ingress filter, all frames that already have a VLAN tag and arrive on the port remain unmodified and are forwarded through the port and processed.

If you enable the ingress filter, the VLAN ID of received frames defines the forwarding process. If the port belongs to the same VLAN both on the receiving (ingress) and on the sending side (egress), the tagged frame will be forwarded. If the port receives frames with a VLAN ID and this VLAN ID is unknown to the port, the frame will be discarded.

Example

The following screenshot from a VLAN configuration of the SCALANCE XC206-2 shows an example of the ingress setting.

Figure 3-4

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P0.1	0	VLAN2	All	☐
P0.2	0	VLAN1	All	☐
P0.3	0	VLAN3	All	☐
P0.4	0	VLAN1	All	☐
P0.5	0	VLAN1	All	☐
P0.6	0	VLAN1	All	☐
P0.7	0	VLAN1	All	☐
P0.8	0	VLAN1	All	☐

This ingress setting defines the following:

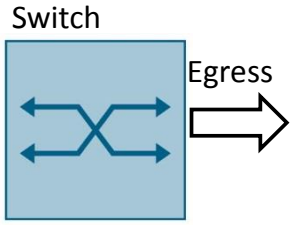
- Frames that arrive on port 0.1 and do not have a VLAN TAG will be tagged with the VLAN ID for "VLAN2".
- Frames that arrive on port 0.3 and do not have a VLAN TAG will be tagged with the VLAN ID for "VLAN3".
- Frames that arrive on the other ports will be tagged with the VLAN ID for "VLAN1" (default VLAN).
- The ingress filter is disabled and all frames that already have a VLAN TAG remain unmodified and are forwarded through the port.

Note This ingress setting does not assign priorities (Priority = 0). Chapter 3.3 shows you how to assign additional priorities.

3.2.2 Egress processing

The egress setting affects frames that may be forwarded by a switch port.

Figure 3-5:



Description

After ingress processing, the incoming frame is tagged to a certain VLAN and therefore uniquely assigned to a VLAN. On which port the frame is forwarded depends on the switch's egress setting. For each port, the egress setting specifies which VLAN will be forwarded on which port. If you want to access multiple VLANs via one port, you can assign multiple VLANs to the port in the egress setting. Only frames tagged with a VLAN ID of this VLAN are forwarded by the port; all other frames are ignored.

Forwarding option

The egress setting also defines how the frame will be forwarded. You have two different options:

3. Without VLAN TAG: The switch removes the VLAN TAG from the frame. Use this setting when an endpoint is plugged into the port.
4. With VLAN TAG: The switch forwards the frame with the VLAN TAG. Use this setting when the port is connected to another switch.

Egress setting between switches

When you connect two switches, you should normally set the relevant ports in egress processing such that the ports retain the VLAN TAG. As a result, the VLAN information is not lost when forwarding from one switch to another. This is particularly necessary if the VLAN extends over multiple switches.

The "Trunk" port mode is available especially for this connection between switches. The "Trunk" port mode causes all VLANS configured on this device to be forwarded on this port with a VLAN TAG.

Note

Of course, it would also be possible to set the forwarding option of the relevant ports to "With VLAN TAG" for each configured VLAN. If you have configured a very large number of VLANs, this takes a lot of time.

The "Trunk" port mode allows you to assign all configured VLANs to this port with a single setting, making sure that the VLAN TAG is retained.
Newly created VLANs are also automatically assigned to the trunk port and the VLAN TAG is retained.

Egress setting for endpoints

Many endpoints don't know what to do with the VLAN TAG in the Ethernet header and the VLAN information provided by the VLAN TAG. Some endpoints discard frames with a VLAN TAG.

For this reason, ports to which an endpoint is connected are configured with the "Without VLAN TAG" forwarding option. Then the frames reach the endpoint without a VLAN TAG. These ports forward only one VLAN.

Abbreviations used in the egress setting

In the egress setting, you assign each port the VLANs whose frames may be sent via this port and define the forwarding type.

The following options are available:

- Forwarding without VLAN TAG
- Forwarding with VLAN TAG
- The port is a trunk port.

For these options, the egress setting uses the following letter codes. The following table shows the abbreviations:

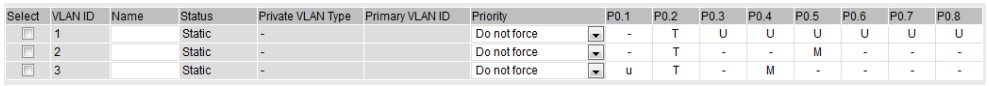
Table 3-1

Option	Meaning	Description
U	Untagged	The port is assigned to the VLAN. The frames' VLAN TAG is removed before forwarding. The port's egress and ingress settings match.
u	Untagged	The port has already been assigned to another VLAN with the "U" abbreviation. The frames' VLAN TAG is removed before forwarding. The egress and ingress settings differ. The ingress setting contains a different VLAN ID with which incoming frames are tagged.
M	Member	The port is assigned to the VLAN. The frames' VLAN TAG is not removed. The VLAN information is not lost.
-		The port is not a member of the VLAN.
F	Forbidden	The port is not a member of the VLAN and it is not possible to dynamically register a VLAN on this port. **Note:** To show you a complete table, the "F" abbreviation was included in the list. The dynamic VLAN is not part of this application example.
R	Registered	The port is assigned to the VLAN. The VLAN is dynamically registered to the port. **Note:** To show you a complete table, the "R" abbreviation was included in the list. The dynamic VLAN is not part of this application example.
T	Trunk	The port was configured as a trunk port. If you have set the "Trunk" port mode, this abbreviation is entered automatically. You cannot select the option.

Example

The following screenshot from a VLAN configuration of the SCALANCE XC206-2 shows an example of the egress setting:

Figure 3-6



Select	VLAN ID	Name	Status	Private VLAN Type	Primary VLAN ID	Priority	P0.1	P0.2	P0.3	P0.4	P0.5	P0.6	P0.7	P0.8
	1		Static	-		Do not force	-	T	U	U	U	U	U	U
	2		Static	-		Do not force	-	T	-	-	M	-	-	-
	3		Static	-		Do not force	u	T	-	M	-	-	-	-

The following VLAN settings were made in this egress setting:

- Three VLANs exist in the switch:
  - VLAN1 (default VLAN)
  - VLAN2
  - VLAN3
- Port 0.1 is only assigned to VLAN3. The frames from VLAN3 are forwarded to the endpoint without a VLAN TAG.
  Port 0.1 is not a member of VLAN1 and VLAN2. Frames assigned to these VLANs are not forwarded via this port.
- Port 0.2 was configured as a trunk port. This setting automatically forwards all frames of the configured VLANs with a VLAN TAG ("T" abbreviation).
- Port 0.3 to port 0.8 belong to the default VLAN. The frames from VLAN1 are forwarded to the endpoint without a VLAN TAG.
- Port 0.4 is additionally a member of VLAN3. The frames from VLAN3 are forwarded via the port with a VLAN TAG.
- Port 0.5 is additionally a member of VLAN2. The frames from VLAN2 are forwarded via the port with a VLAN TAG.

With these settings, the following can be said about the VLAN assignment:

- Port 0.2 and port 0.5 belong to VLAN2. Only frames for VLAN2 are forwarded.
- Port 0.1, port 0.2 and port 0.4 belong to VLAN3. Only frames for VLAN3 are forwarded.
- Port 0.2 to port 0.8 belong to VLAN1. Only frames for VLAN1 are forwarded.

3.3 Prioritization in the VLAN

Description

Aside from the VLAN assignment for incoming frames, you can specify one of eight priorities for each VLAN. With this prioritization, certain frames are preferred over others. In particular, this is only relevant when a switch is fully utilized and can no longer forward all frames. If a switch is overloaded, data must be buffered or, in the worst case, discarded. If one frame has a higher priority than the others, it is ensured that the prioritized frame is the first to be forwarded.

The priority level is stored as a number in the VLAN TAG's "Priority Code Point".

IEEE 802.1Q-2005 specifies the different priority levels.

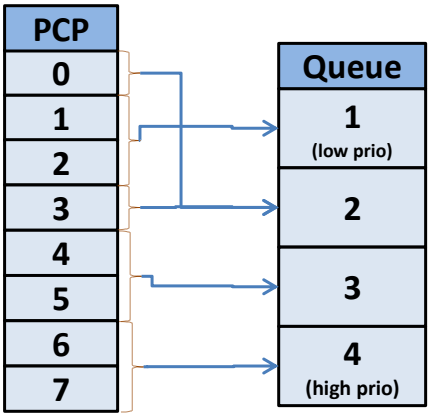
Queues in the switch

Prioritization is implemented through queues in the switch. Depending on the performance class, switches have different numbers of queues. The number of queues ranges from two to eight.

The decision as to which frame will be buffered in which queue can be made using the number in the VLAN TAG' s "Priority Code Point". Internally, each switch has a table where each priority level is assigned to a queue.

The following example shows the prioritization mechanism in the switch. The switch has four queues. The total of eight priority levels is assigned to the queues as follows:

Figure 3-7



The following rules apply to prioritizing frames:

- Frames with a low priority level are buffered in a low-priority queue.
- Frames with a higher priority level are buffered in a higher-priority queue. Frames in one of these queues are forwarded before others.

Note Frames are only prioritized if the switch is overloaded or multiple frames arrive at once.

3.4 PROFINET in conjunction with VLAN

If you want to implement PROFINET communication in a VLAN, you need to observe certain conditions and settings.

Prioritization in the VLAN TAG

PROFINET frames have real-time capability. To enable real time, the transmission of PROFINET frames is prioritized according to the IEEE 802.1Q standard. The VLAN TAG in the Ethernet header is used for this prioritization.

This real-time data is assigned VLAN priority 6 and VLAN ID 0. With this tagging, the frames are forwarded by a switch with a minimal delay.

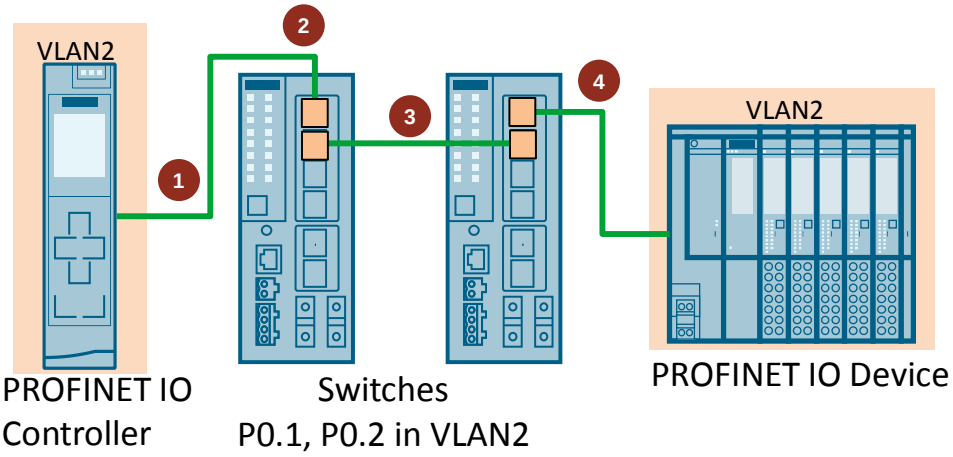
Note VLAN ID 0 indicates that the frame only contains priority information.

Example

The following figure uses an example to illustrate PROFINET communication in a VLAN.

In this network, you can see a VLAN2 that is created by two switches. Port P0.1 and port P0.2 of the two switches are assigned to VLAN2.

Figure 3-8



The following table explains how the PROFINET frame is handled in a VLAN:

Table 3-2

No.	Description	VLAN TAG
1.	The IO controller sends a PROFINET real-time frame to the network. The destination address is the IO device.	VLAN ID 0 VLAN priority 6
2.	The switch receives the frame on port 1 and detects that the frame is a PROFINET frame with VLAN ID 0. Using the configured ingress assignment, the switch sets the VLAN ID to VLAN ID 2 and keeps the default priority.	VLAN ID 2 VLAN priority 6
3.	The switches are connected to each other via port 2. Port mode is "Trunk". The frames are forwarded with the VLAN information.	VLAN ID 2 VLAN priority 6
4.	The egress configuration of the switch's port 1 is set to the "M" forwarding option (with VLAN TAG). The switch sends the frame with a VLAN TAG to the IO device. **Note**: This setting is particularly necessary when the IO device itself has an internal switch that can be used to connect other IO devices in series. If only a single IO device is connected to the switch, you can also set the "U" forwarding option in the egress configuration of port 1.	VLAN ID 2 VLAN priority 6

Note This example uses VLAN ID 2 for PROFINET real-time communication. You can use any VLAN ID for your own VLAN for PROFINET real-time communication.

Requirement for the infrastructure

To be able to use PROFINET real-time communication in a VLAN, be sure to note the following:

- The switches in the PROFINET network must be capable of evaluating the VLAN TAG and complying with the prioritization.
- The switches in the VLAN must accept and forward the PROFINET real-time frames with the 0x8892 EtherType.
- PROFINET real-time frames with VLAN ID 0 must be accepted by the switch and tagged to a separate VLAN x with PROFINET prioritization by the configuration in the switch. As an alternative, you can use the "802.1Q transparent Mode" VLAN mode in the switch. In this VLAN mode, VLAN ID 0 is still available. You cannot configure VLANs in "802.1Q transparent Mode".

4 Appendix

4.1 Service and Support

Industry Online Support

Do you have any questions or do you need support?

With Industry Online Support, our complete service and support know-how and services are available to you 24/7.

Industry Online Support is the place to go to for information about our products, solutions and services.

Product Information, Manuals, Downloads, FAQs and Application Examples – all the information can be accessed with just a few clicks:
https://support.industry.siemens.com

Technical Support

Siemens Industry's Technical Support offers you fast and competent support for any technical queries you may have, including numerous tailor-made offerings ranging from basic support to custom support contracts.

You can use the web form below to send queries to Technical Support:
www.siemens.com/industry/supportrequest.

Service offer

Our service offer includes the following services:

- Product Training
- Plant Data Services
- Spare Part Services
- Repair Services
- Field & Maintenance Services
- Retrofit & Modernization Services
- Service Programs & Agreements

For detailed information about our service offer, please refer to the Service Catalog:
https://support.industry.siemens.com/cs/sc

Industry Online Support app

The "Siemens Industry Online Support" app provides you with optimum support while on the go. The app is available for Apple iOS, Android and Windows Phone:
https://support.industry.siemens.com/cs/ww/en/sc/2067

4.2 Links and literature

Table 4-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the entry page of the application example https://support.industry.siemens.com/cs/ww/en/view/109749844
\3\	FAQ: PROFINET in a VLAN https://support.industry.siemens.com/cs/ww/en/view/24947500
\4\	Configuration Manual: SCALANCE XB-200/XC-200/ XP-200/XR-300WG Web Based Management https://support.industry.siemens.com/cs/ww/en/view/109748984

4.3 Change documentation

Table 4-2

Version	Date	Modifications
V1.0	09/2017	First version