How do you configure a Virtual Local Area Network (VLAN) in PCS 7?

SIMATIC PCS 7 V8.1

Security Notes

Siemens offers products and solutions with industrial security functions which support the secure operation of plants, solutions, machines, devices and/or networks. They are important components in a comprehensive industrial security concept. The Siemens products and solutions continue to be developed under this aspect. Siemens recommends that you keep yourself regularly informed about product updates.

For the safe operation of Siemens products and solutions it is necessary to take appropriate security measures (cell protection concept, for example) and to integrate each component in an overall industrial security concept which is state of the art. This should also cover the third-party products used. Additional information about industrial security is available at: http://www.siemens.com/industrialsecurity.

In order to keep yourself informed about product updates, we recommend subscribing to our product-specific newsletter. Additional information about this is available at http://support.industry.siemens.com.

Contents

1 Using VLANs in PCS 7 ................................................................................... 3
2 VLAN Configuration for Use in PCS 7 ........................................................... 7
1 Using VLANs in PCS 7

Below we give you an overview of the use and structure of VLAN technology in the PCS 7 environment. There is also a description of the configuration of the devices in the network.

**Note**

There are restrictions for using VLAN in PCS 7. The use of a redundancy connection via VLAN is not recommended for the sake of availability among other things. This might lead to unexpected or undesirable plant behavior.

**What is a VLAN?**

A Virtual Local Area Network (VLAN) is a logical subnetwork. This subnetwork can be assigned to a switch or be an entire physical network.
The subnetwork can extend beyond one or multiple switches. A VLAN divides physical networks into logical subnetworks. VLAN-compatible switches split up the frames (data packages) between the separate VLANs. The frames are not forwarded to another VLAN even though the subnetworks might be connected to common switches.

More information is available in this FAQ entry:
When do you use VLANs in PCS 7?

The use of VLANs in the PCS 7 environment is limited to the applications below.

- **Combined plant and terminal bus**
  This architecture consists of just one physical Ethernet network that is used for both the plant bus and the terminal bus. VLAN separates these two network levels on a logical level. By using a common medium, the networks might influence one another. The separation of communication networks recommended for PCS 7 is achieved on a logical level.

- **VMware ESXi server in virtual infrastructures**
  In virtual infrastructures various PC stations (OS clients, for example) are virtualized together on one server. This means that not all the PC stations have to be physically present.

Figure 1-3

More information is available in this FAQ entry: https://support.industry.siemens.com/cs/ww/en/view/31770396
Which devices are needed for using VLANs?

VLAN-compatible switches are needed for using VLANs in the PCS 7 environment. The following switches from the Siemens network device family support port-based VLANs with tagged frames:

- SCALANCE X-300
- SCALANCE X-400
- SCALANCE X-500

When you configure the switch you define which VLAN is assigned to which port of the switch and therefore also the nodes connected to it. The port-specific VLAN tags serve as identification.

- A VLAN tag is added to a message (Ingress) when received on the switch from a terminal node.
- A VLAN tag is removed from a message (Egress) when sent from the switch to a terminal node.

In the case of communication between two switches (Trunk) the VLAN tags are not removed when leaving the switch. When received, the VLAN tags are retained in the partner switch which ensures that the VLANs remain separated. Tagged messages are always used in the switch.

For more information please refer to this entry: https://support.industry.siemens.com/cs/ww/en/view/109476760
2 VLAN Configuration for Use in PCS 7

The following configuration instructions show how to create two static VLANs for a terminal bus and a plant bus.

Refer to the following manual for more configuration parameters:
"SIMATIC NET Industrial Ethernet Switches SCALANCE X-300 SCALANCE X-400 Configuration Manual"

Proceed as follows for the configuration.
1. Define the criteria for creating at least two or more VLANs and any VLAN priorities.
2. Assign the nodes to the separate VLANs.
3. Create a configuration list.
4. Assign the VLAN ID for each node and each switch.
5. Define to which device and at which port there is a connection.

Configure the switch as follows:
1. Define all the VLANs used on this device.
2. Define which VLAN is to be supported on which port and define the VLAN priority.
3. Define how the messages are to be processed at the input and output sides of the port (ingress and egress filters).
4. Specify whether messages at the port are to be sent with or without tag.
Before configuring the VLANs you should make sure that the Web-based Management of the switch can be reached from each port during and after parameterization of the VLAN.

Figure 2-1

Open the "Web-based Management" and in the "Agent" menu you enable the "Accessible in all VLANs" function.

For switches that do not have this option make sure that at least one port of the switch is in the "Agent VLAN" or that the "Agent VLAN" is changed according to the port configuration.

**WARNING**
If the parameters are set incorrectly, it is possible that the web interface and the configuration of the switch can no longer be called.
VLAN configuration

The "Current VLAN Configuration" page shows the current VLAN configuration parameters of the port.

Table 2-1

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>–</td>
<td>The port is not a member of the specified VLAN.</td>
</tr>
<tr>
<td>M</td>
<td>Member: the port is member of the VLAN; sent messages receive a VLAN tag with the VID specified in the first column.</td>
</tr>
<tr>
<td>R</td>
<td>Registered: The port is member of the VLAN; registration was through a GVRP message.</td>
</tr>
<tr>
<td>U</td>
<td>Untagged: The port is member of the VLAN; sent messages do not receive a VLAN tag.</td>
</tr>
<tr>
<td>F</td>
<td>Forbidden: The port is not member of the VLAN and it is not possible for a VLAN to be registered dynamically at this port by means of GVRP.</td>
</tr>
<tr>
<td>G</td>
<td>Guest VLAN: The port is a member of the Guest VLAN. Registration was done dynamically through the &quot;Guest VLAN&quot; authentication. See also: <a href="https://support.industry.siemens.com/cs/ww/en/view/109476760">https://support.industry.siemens.com/cs/ww/en/view/109476760</a></td>
</tr>
<tr>
<td>A</td>
<td>Authenticated: The port is a member of the VLAN. Registration was done dynamically through the &quot;MAC Authentication&quot; procedure. See also: <a href="https://support.industry.siemens.com/cs/ww/en/view/109476760">https://support.industry.siemens.com/cs/ww/en/view/109476760</a></td>
</tr>
</tbody>
</table>

In the case of a new definition all the ports are preset with the ID "–".

A switch that supports VLAN is parameterized by default on all ports with the VLAN ID "1" (default VLAN).

The VLAN-ID "500" is reserved and already configured for a future application.

All the ports on the switch send messages by default without a VLAN tag to ensure that the terminal nodes can receive the messages.
This basic setting is necessary because it is not sure whether a node can interpret tagged frames.

Figure 2-3

Click the "New Entry" button or click an available configuration to assign ports to a VLAN. The "Static VLAN Configuration" page is displayed.

Create a new VLAN for the terminal bus. Define a unique VLAN ID of your choice (from area 2 – 4096. In the example: VLAN ID = 10).

Where applicable you assign a VLAN priority (from the range 0 – 7; with the "Do not force" parameter the priority of the messages remains unchanged). Now select the ports to be used for the terminal bus.

Set "U" for the ports to which terminal nodes are connected (Static Access Port).

Set "M" for ring ports or connection ports that lead to other switches (Trunk Port).

**Note**

If a VLAN is to communicate through the ring ports, the ring ports must be located in the VLAN. In the case of multiple VLANs the ring ports must be configured accordingly in each of the VLANs concerned.

Now create a new VLAN for the plant bus. Proceed exactly as for the configuration of terminal bus VLAN.
In our example we have selected the VLAN ID = "20" for the plant bus.

Figure 2-4

On the "Current VLAN Configuration" page you select the item "Default VLAN 1". Set "–" for all the ports to be used for the terminal bus and the plant bus.

Set "U" for all the ports not used.

Set "M" for ring ports or connection ports that lead to other switches (Trunk Port).

Set "F" for the port to forbid membership of this VLAN. In this way the port cannot be dynamically registered on this VLAN via GVRP (GARP VLAN Registration Protocol).
Figure 2-5

The "Current VLAN Configuration" page shows the current VLAN configuration parameters of the ports for the terminal bus and the plant bus. The overview shows which VLANs are created and at which ports messages of the corresponding VLANs are output (Egress Configuration).
Switch configuration

In the next step we define the input behavior (Ingress behavior) of the switch for the VLANs concerned.

Figure 2-6

On the “VLAN Port Configuration” page all the ports have their associated Port IDs. The “Trunk” option automatically makes this port member of all the configured VLANs and it only sends tagged frames.

- The ports on the terminal bus have the Port VLAN ID of the terminal bus.
- The ports on the plant bus have the Port VLAN ID of the plant bus.
The "VLAN Port Parameters" page shows all the ports with their configured Port VLAN-IDs and the associated Ingress behavior.

Untagged messages sent to the switch received the relevant VLAN tag depending on the configured Ingress behavior.
The basic parameterization of the VLANs for the terminal bus and plant bus is completed. The networks are defined port for port and are separated logically. Direct communication between nodes of the plant bus and nodes of the terminal bus is not possible.