# Industrial Ethernet Training 07

# Configuring Port-based VLAN on a Weidmueller switch

**Abstract:**
Virtual Local Area Networks (VLAN) split a physical network into multiple virtual and logical networks. Communicating with two devices connected to two different VLANs is not possible, as they are (virtually) in different networks. This application note demonstrates a possible separation of networks with VLAN in Weidmueller switches.

**Hardware reference**

| No. | Component name | Article No. | Hardware / Firmware version |
|---|---|---|---|
| 1 | IE-Training Kit-01 | 2881730000 | 1.1.2 (Build 125086) |
| 2 | | | |
| 3 | | | |

**IE-Training Kit Content**

| No. | Component name | Article No. | Hardware / Firmware version |
|---|---|---|---|
| 1 | IE-SR-4TX | 2751270000 | 1.4.7 |
| 2 | IE-SW-AL08M-8TX | 2682280000 | 1.08 |
| 3 | IE-SW-AL05M-5TX | 2682250000 | 1.14 |
| 4 | IE-CS-MBGW-2TX-1COM | 2682600000 | 3.11 |

**Software reference**

| No. | Software name | Article No. | Software version |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

**File reference**

| No. | Name | Description | Version |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

**Contact**
Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
www.weidmueller.com

For any further support please contact your local sales representative:
https://www.weidmueller.com/countries

# Content

# 1 Warning and Disclaimer

**Warning**
Controls may fail in unsafe operating conditions, causing uncontrolled operation of the controlled devices. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be safety equipment provided / electrical safety design or other redundant safety features that are independent from the automation system.

**Disclaimer**
This Application Note / Quick Start Guide / Example Program does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this Application Note / Quick Start Guide / Example Program prepared by Weidmüller, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use.

**Note**
The given descriptions and examples do not represent any customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. Application notes / Quick Start Guides / Example Programs are not binding and do not claim to be complete in terms of configuration as well as any contingencies. By using this Application Note / Quick Start Guide / Example Program, you acknowledge that we cannot be held liable for any damages beyond the described liability regime. We reserve the right to make changes to this application note / quick start guide / example at any time without notice. In case of discrepancies between the proposals Application Notes / Quick Start Guides / Program Examples and other Weidmüller publications, like manuals, such contents have always more priority to the examples. We assume no liability for the information contained in this document. Our liability, for whatever legal reason, for damages caused using the examples, instructions, programs, project planning and performance data, etc. described in this Application Note / Quick Start Guide / Example is excluded.

**Security notes**
In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

# 2 Prerequisites for doing

You need to have the following hardware and documentation

- Industrial Ethernet Training Kit
- Application Note Industrial Ethernet Training 01 “Setting up default configuration of IE Training Kit” for applying default IP address configuration

# 3 Port-based VLAN

Virtual Local Area Networks (VLANs) are used for dividing a physical network into multiple different virtual and logical networks.
VLANs are used to group devices so we can broadcast our traffic only to certain devices, resulting in reduced network traffic and lower usage of resources.
Furthermore, VLANs can improve security. For example, dangerous or malicious packets sent by an attacker will not be sent to devices within different VLANs.
All in all, virtual networks are a very important feature in Weidmueller switches. Without it, we would have to build up multiple physical networks to separate our network traffic and devices, which would result in high costs and immense effort to configure each network and device.
In the following example, we are using port based VLAN. This means that we assign the ports of a switch to different VLANs. Let us presume the two 5-port lite switches from the Training Kit (both connected to the 8-port switch) are managing two different machines, which we want to split into two VLANs. Therefore, we identify the physical ports where our lite switches are connected to the 8-port switch and then assign these ports to two different VLANs.

# 4 Configuring Port-based VLAN

We will now configure our 8-port managed switch to have two different virtual networks for our two 5-port switches on the Training Kit.

1. First, we want to connect to our 8-port switch (IE-SW-AL08M-8TX). Make sure you are connected to the switch's network or directly to the switch via an Ethernet cable. Next, we can type in the IP *"192.168.1.20"* into our browser's URL field and log in with our credentials.

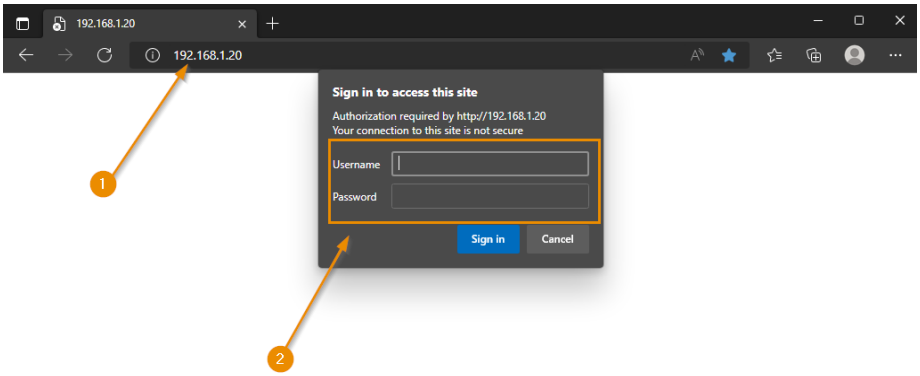


**Figure 1: Switch login**

2. After logging in, we want to navigate the menu tree path to *"VLAN"* and then select *"VLAN Setting"*. We should now be in the following menu:

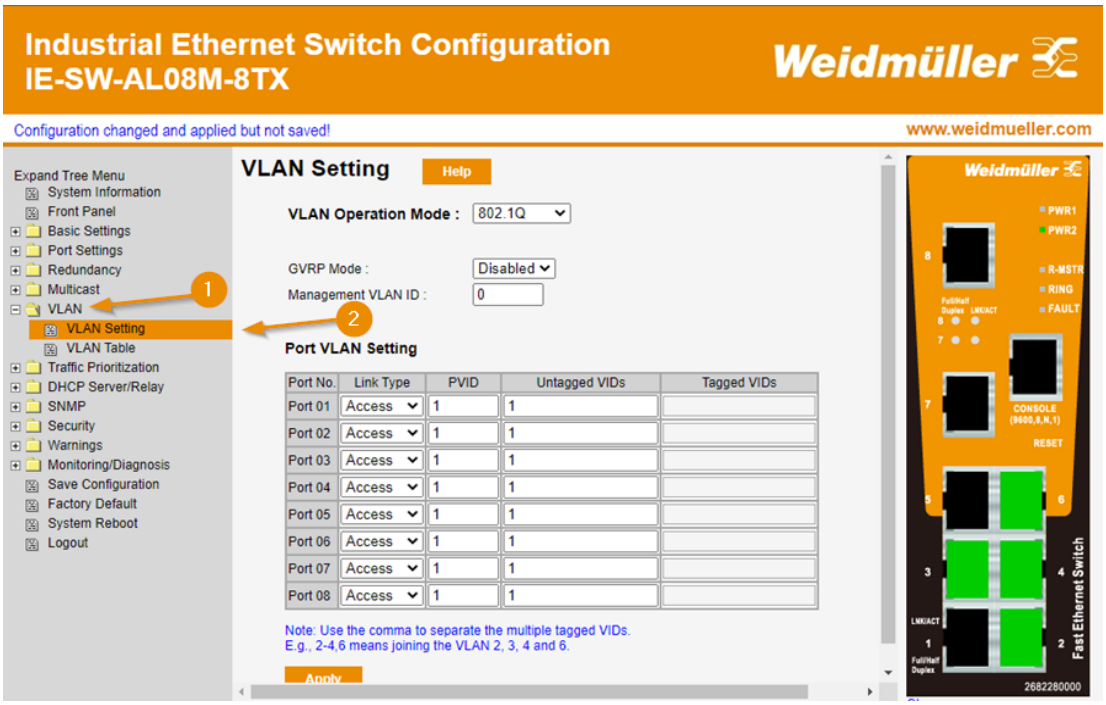


**Figure 2: Switch VLAN Settings**

3. Since we want to configure port based VLAN, we must change the switch's operation mode. Therefore, we select *"Port Based"* in the drop-down menu *"VLAN Operation Mode",* as seen below.

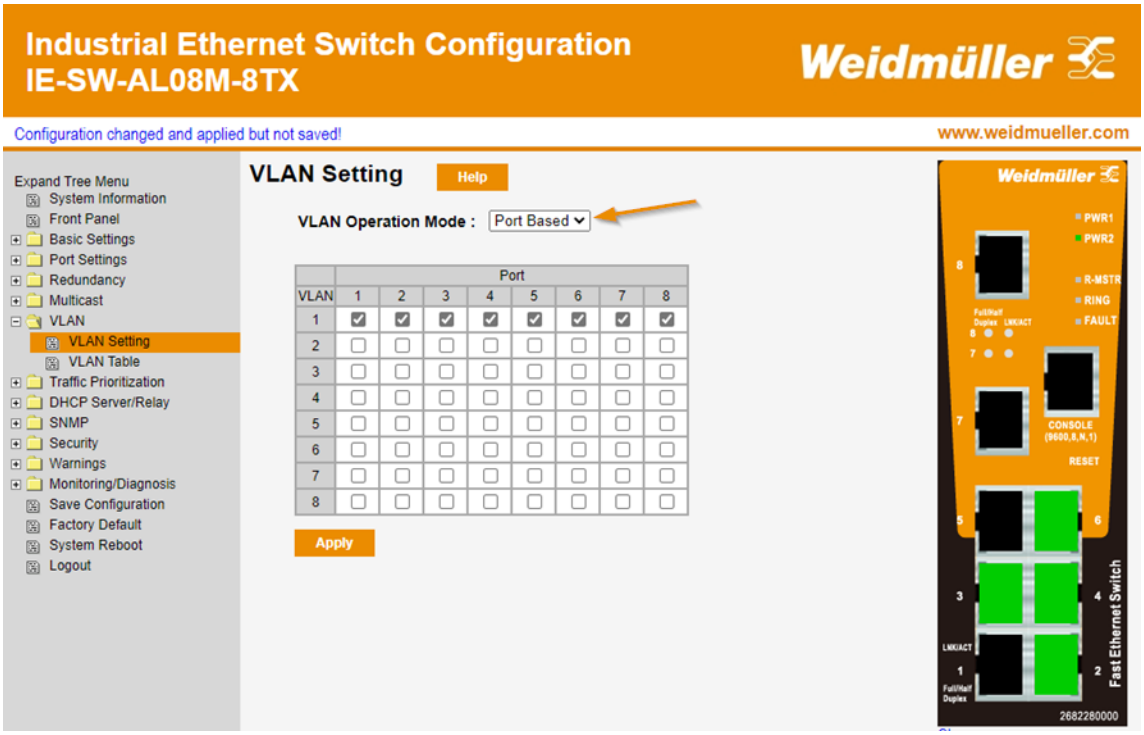


**Figure 3: VLAN Operation Mode port based**

As per default, every port is in the first VLAN in order to have every device communicate with each other properly. In the next step, we will change the check boxes to create two virtual networks.

4. As mentioned before, we want to create two different virtual networks for our lite switches. Therefore, we want to identify which ports are occupied with our lite switches by checking out the cables to the corresponding port numbers (in our example, ports 2 and 4 are connected to the lite switches).
   Now, we want to create the virtual network for each switch. The 8-port switch offers 8 different VLANs to use. For this purpose, we are going to put port number 2, which is the third switch on the right side of the Training Kit, on VLAN 2. To do this, we want to uncheck the check box in port number 2, then select VLAN 2 for port number 2 and apply the new settings.

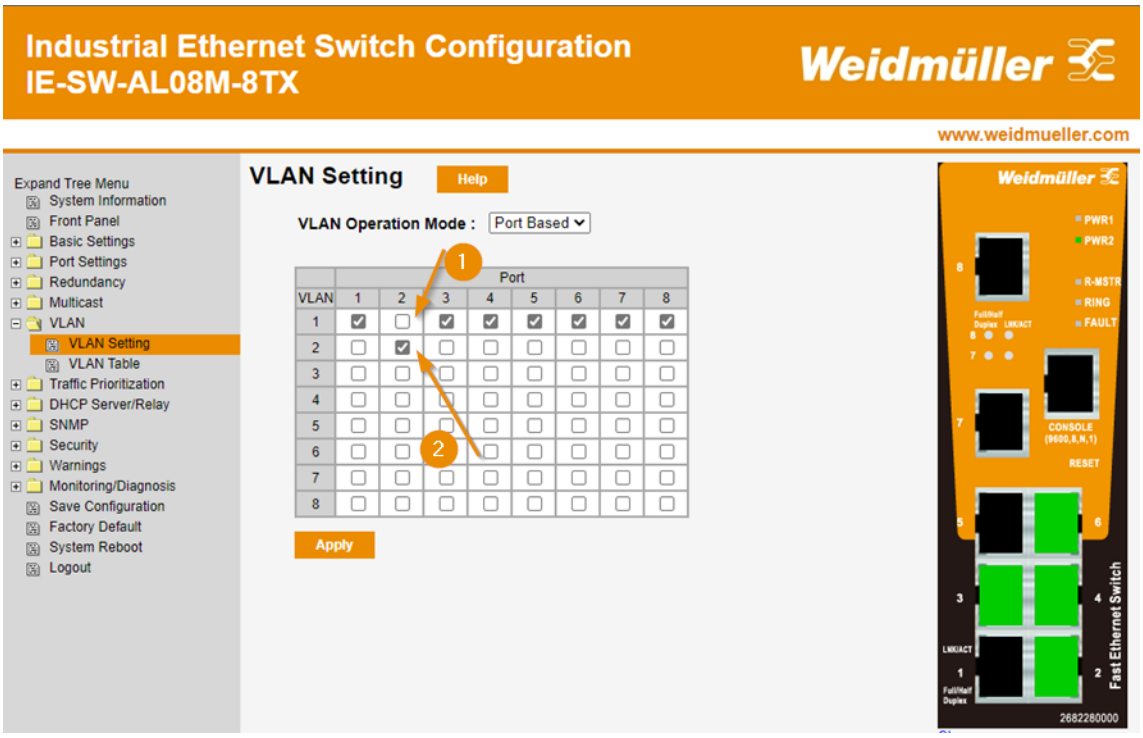


**Figure 4: Assigning switch in VLAN 2**

5. We are now neither able to ping nor to connect to the third switch. We can test this by trying to connect to the switch's web interface via its IP *"192.168.1.40"* or using command prompt to ping the mentioned IP (provided that our computer is in a network with the Training Kit devices).

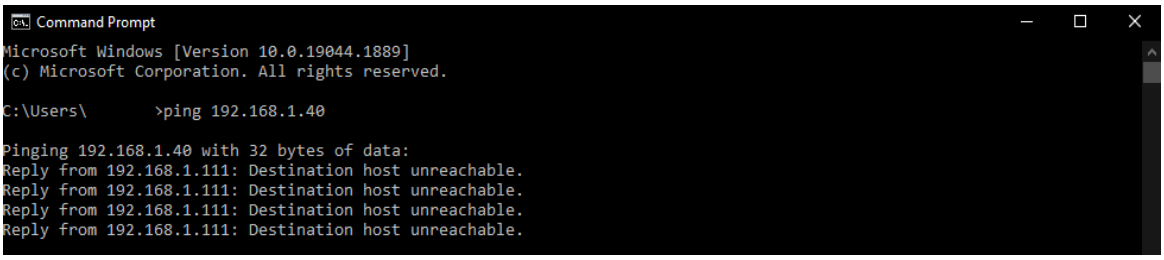


**Figure 5: Command prompt ping**

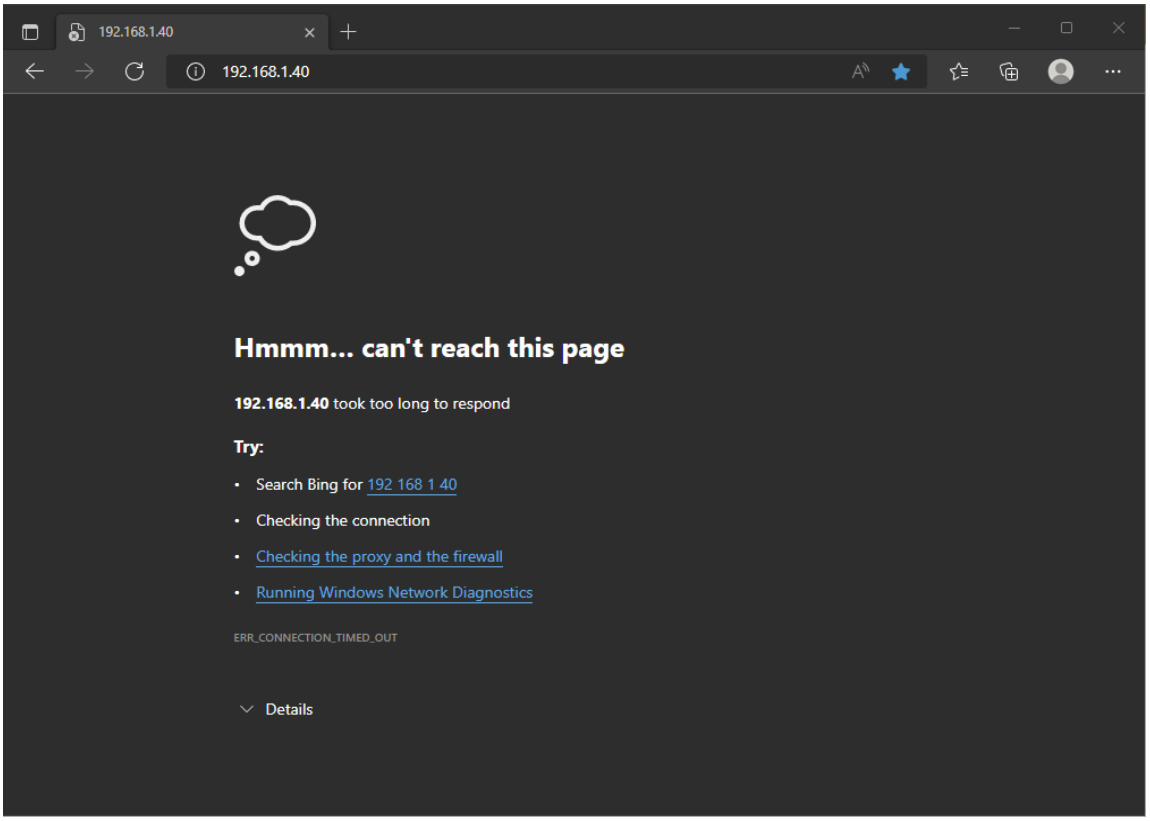


**Figure 6: Connecting to the switch**

6. As we can see, we are unable to establish a connection to the switch as it is virtually in a foreign network which is unreachable to our devices.
   To reach this device again, we must either establish a LAN connection via ethernet cable directly to any of the 5-port switches or we can connect our computer and the managed 8-port switch to any two of the LAN ports of the router.
   Assigning our router to both VLANs means that our router is capable to operate in the two virtual networks. Thus, that we can access our switch again with every device that is in the network, like our computer.
   To do so, we must identify the port used to connect our router to the switch (in our case, it is port number 3). Now, we select VLAN 2 for port number 3 as well and "*Apply*". Our router is now allowed to operate within both virtual networks. It is now possible to communicate with the two lite switches via the router.

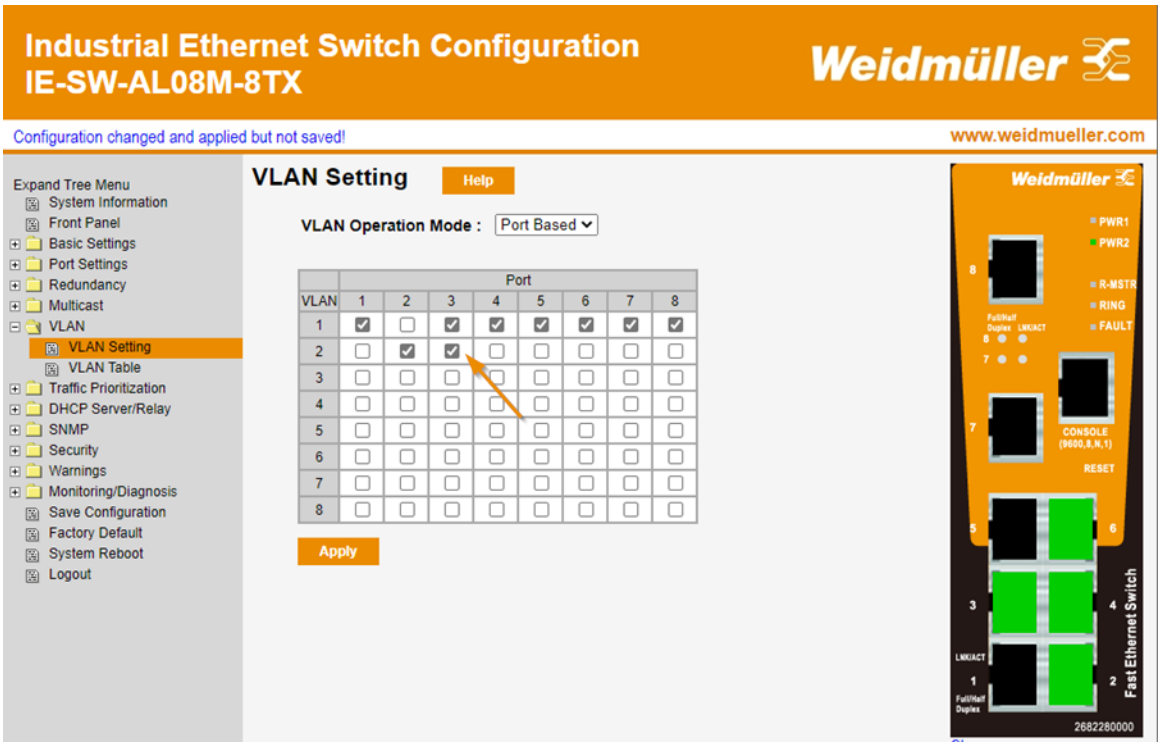


**Figure 7: Assigning router to VLAN 1 and VLAN 2**

7. With this configuration, we are able to reach our lite switches again with our computer, that is connected to the router. But, as all our other devices, such as the Modbus gateway or the first 5-port lite switch, are not connected to the router, it is not possible for them to connect to the 5-port switch in VLAN 2, as it is within a different network.
   In fact, we can connect to our 5-port switch from VLAN 1 and try to ping our second switch in VLAN 2 to see that it is not possible to establish a connection. Use the *"192.168.1.30"* IP to establish a connection to our switch in VLAN 1. Then, navigate in the menu tree to *"Monitoring/Diagnosis"* and select *"Ping"*. Lastly, type in the IP we want to ping, which is *"192.168.1.40"* and press the button *"Send Ping"*.

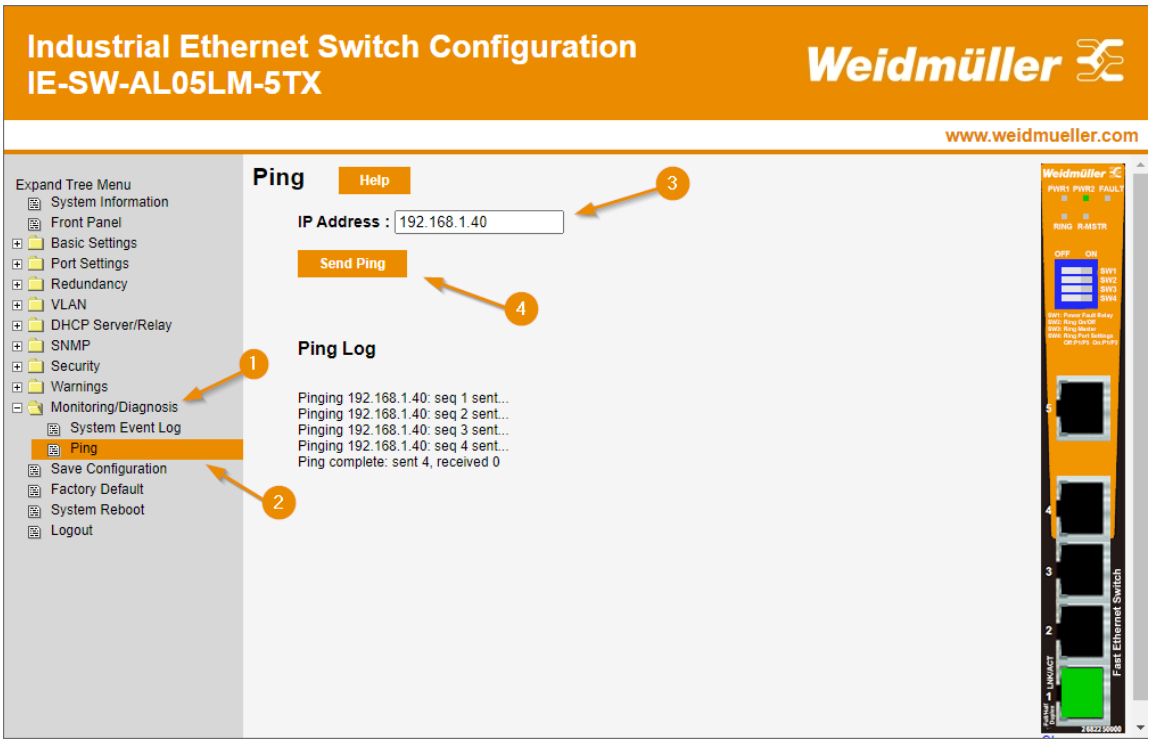


**Figure 8: Pinging the switch**

# 5 Results

We are now able to create multiple different virtual networks with our switch to reduce security risks and improve overall device management. We also know how to test if we have split the networks correctly by using the ping command, either in the command prompt or by pinging directly via our device’s web interface.