

A man in a light blue shirt is shown from the side, looking at a tablet. The background is a blurred industrial setting with a clock and various equipment. Overlaid on the image are several digital graphics: a '24/7' icon with a circular arrow, a 'NEWS' icon with a person silhouette, a 'Home' icon, and a 'Industry Online Support' text. There are also binary code (0s and 1s) and network-like icons scattered throughout the digital overlay.

**SIEMENS**

*Ingenuity for life*

# Configuring the Virtual Router Redundancy Protocol (VRRP)

SCALANCE XM-400, SCALANCE XR-500, SCALANCE S

<https://support.industry.siemens.com/cs/ww/en/view/109798556>

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 <https://www.siemens.com/industrialsecurity>.

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

<b>Legal information .....</b>	<b>2</b>
<b>1 Introduction .....</b>	<b>5</b>
1.1 Overview.....	5
1.2 Principle of operation.....	6
1.3 Components used .....	8
<b>2 Hardware setup .....</b>	<b>11</b>
<b>3 Engineering VRRP .....</b>	<b>13</b>
3.1 Commissioning PC and server.....	13
3.2 Commissioning SCALANCE .....	17
3.3 Configuring the master router .....	24
3.3.1 Disable Spanning Tree Protocol .....	24
3.3.2 Create VLANs .....	25
3.3.3 Activate routing.....	27
3.3.4 Create subnets .....	28
3.3.5 Configure VRRP .....	30
Creating the virtual router instance .....	30
Configuring the router instance .....	30
Configuring the addresses .....	32
3.4 Configuring the backup router.....	34
3.4.1 Disable Spanning Tree Protocol .....	34
3.4.2 Create VLANs .....	35
3.4.3 Activate routing.....	37
3.4.4 Create subnets .....	38
3.4.5 Configure VRRP .....	40
Create the virtual router instance .....	40
Configuring the router instance .....	40
Address configuration.....	42
3.5 Checking the VRRP status.....	44
<b>4 Engineering of firewall redundancy with VRRP .....</b>	<b>45</b>
4.1 Configuring the master router .....	47
4.2 Configuring the backup router.....	48
<b>5 Testing the VRRP scenario.....</b>	<b>50</b>
5.1 Error scenarios .....	50
5.2 Diagnostics options .....	52
5.3 Error profiles.....	53
<b>6 Useful information .....</b>	<b>54</b>
6.1 Normal operation .....	54
6.2 Failure of a device or a connection .....	54
6.2.1 Router failure.....	54
6.2.2 Failure of a connection cable .....	55
6.3 Tracking process .....	56
6.3.1 Interface tracking.....	56
6.3.2 VRID tracking .....	56
6.3.3 Address monitoring .....	56
6.4 Calculating the failure time .....	57
<b>7 Appendix .....</b>	<b>59</b>
7.1 Service and support .....	59
7.2 Industry Mall .....	60
7.3 Links and literature .....	60

7.4	Change documentation .....	60
-----	----------------------------	----

# 1 Introduction

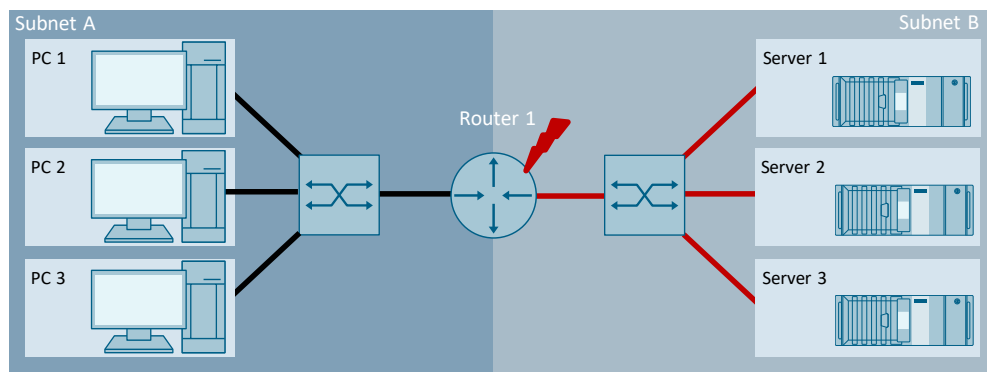
## 1.1 Overview

You have been tasked with ensuring reliability and operational security between different subnets. To accomplish this task, you need routers between the network interfaces.

### Problem

The router in the network has a technical error. All servers in subnet B are no longer reachable. Single points of failure which entail the failure of the entire system must be avoided.

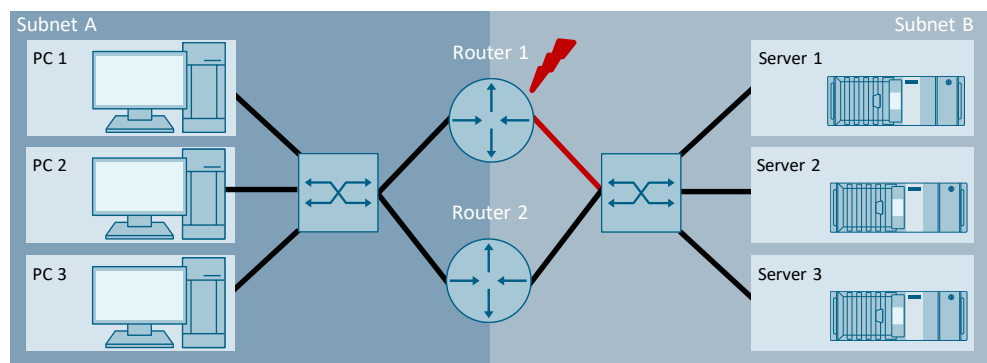
Figure 1-1



### Solution

To circumvent single points of failure, routers can be set up redundantly. The underlying principle is the Virtual Router Redundancy Protocol (VRRP). VRRP belongs to the first-hop redundancy protocols which are used in critical infrastructure, such as servers, to ensure their availability. The protocol serves to improve the availability of gateways in local networks by means of redundant routers.

Figure 1-2

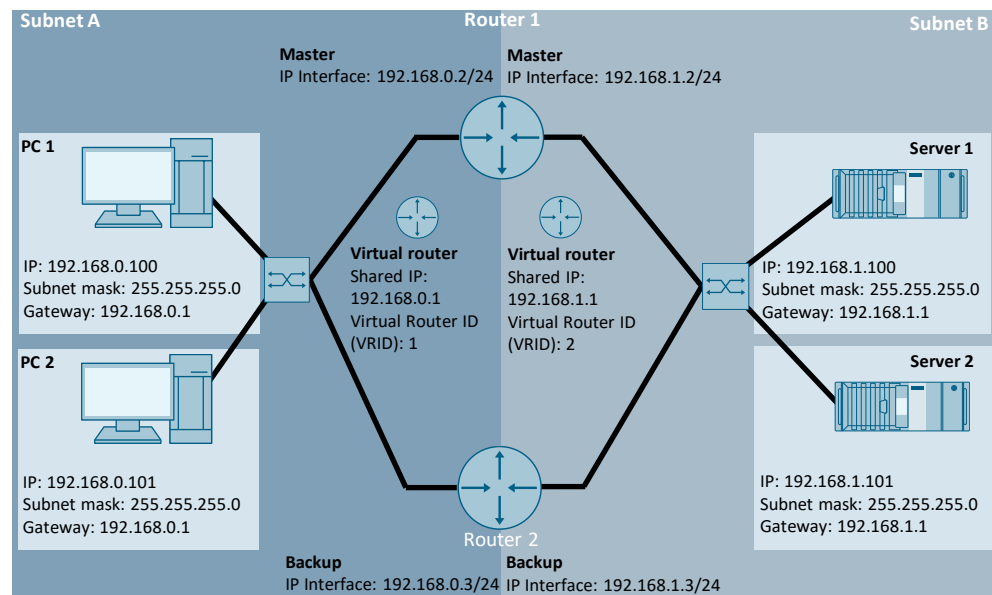




## 1.2 Principle of operation

The functional principle of the Virtual Router Redundancy Protocol (VRRP) lies in providing a virtual router as a gateway for the end nodes. Two or more routers are hidden behind this gateway. One of these routers is active and assumes the role of the master and thus the routing. All other routers function as backup routers and check whether the master is still active. If the master is not active, they take over.

Figure 1-3



### Virtual router

The virtual router is defined via a Virtual Router ID (VRID), a defined MAC address, and one or more IP address(es) that the virtual router "listens to", also known as Associated IP Addresses. The term "virtual router" is misleading. To be exact, the router is not entirely virtual, but rather individual IP interfaces. One router can be the master on one IP interface and the backup on another IP interface.

### Virtual Router ID (VRID)

To uniquely assign two or more routers to a group that together represents one virtual router, a VRID is configured in each device. This is a number from 1 to 255 and must be unique in a subnet. All routers within a group must have the same VRID configured. VRRP routers that belong to the same VRID exchange information. Each group can only have one master router.

### VRRP MAC address

Like every real router, the virtual router also needs a MAC address to which Ethernet telegrams from the end nodes can be sent. This MAC address is reserved for VRRP and is composed of a fixed part plus the VRID (in hexadecimal format): 00-00-5e-00-01-VRID.

Example:

VRID 10	00-00-5e-00-01-0a
VRID 100	00-00-5e-00-01-64

### Common IP (Associated IP Addresses)

[Figure 1-3](#) depicts two routers. Both have an IP interface in the network 192.168.0.0/24. Router 1 has the IP address 192.168.0.2, router 2 has 192.168.0.3. With the help of VRRP, an IP address is defined as the address of the virtual router. This can be one of the real IP addresses actually in use (here, 192.168.0.2 or 192.168.0.3), but it can also be a third IP address as shown in the Figure (192.168.0.1). All VRRP routers in a group must have the same Associate IP Addresses.

### Selecting the master

The decision of which router in the VRRP group will be the master is made using the configured priority, along with the parameter "Preempt lower priority Master", or "Preempt" for short.

If "Preempt" is set, then the router that has the highest configured priority will always be the master. If the priority is the same, the router that has the higher IP address on the corresponding IP interface will become the master. If a new router with a higher priority is connected to the network, a switchover will occur because the new router will become the master.

If "Preempt" is not set, the router that sends Advertisements first will be the master. If a new router with higher priority is connected to the network, there will be no switchover if "Preempt" is inactive.

Using the configuration parameter "Preempt lower priority Master" it is possible to set whether the network will define a master router deterministically ("Preempt" turned on) or whether the number of switchovers should be kept as low as possible ("Preempt" turned off).

Refer to the [Useful information](#) chapter for more information on the mechanisms and principles of VRRP.

## 1.3 Components used

### SCALANCE XM-400 and XR-500

The devices of the SCALANCE XM-400 series and the devices of the SCALANCE XR-500 series can be used as routers for automation. They meet all the requirements for IP routing.

The following routing functions are available on the devices:

- Static routing
- Dynamic routing. The following protocols are supported:
  - OSPF / OSPF v3
  - VRRP / VRRPv3
  - RIP / RIPng

#### Note

The devices of the SCALANCE XM-400 series and the devices of the SCALANCE XR-500 series are offered in two variants:

- The Layer 3 function (routing) is ready and integrated in the device.
- The Layer 3 function (routing) can be activated with a KEY-PLUG.

The Layer 3 function is required for this application example.

When choosing your device, please note whether the routing function is already included in the device or whether you need an additional KEY-PLUG with license.

### SCALANCE S

The SCALANCE S series Industrial Security Appliances protect industrial networks and automation systems by segmenting the network and establishing secure communications channels.

Only VRRPv3 is available on these devices as a routing function:

This examples uses

- 2 SCALANCE XM408-8C (item number 6GK5 408-8GR00-2AM2)
- 2 SCALANCE S615 (item number 6GK5 615-0AA00-2AA2).



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

Table 1-1

Component	Item number	IP address and subnet mask	Router	Note
SCALANCE XM408-8C	6GK5 408-8GR00-2AM2	Vlan 1: 192.168.1.2 255.255.255.0  Vlan 10: 192.168.10.2 255.255.255.0  VLAN 20: 192.168.20.2 255.255.255.0	Associated IP:  VRID 10: 192.168.10.1 255.255.255.0  VRID 20: 192.168.20.1 255.255.255.0	Master
SCALANCE XM408-8C	6GK5 408-8GR00-2AM2	Vlan 1: 192.168.1.3 255.255.255.0  Vlan 10: 192.168.10.3 255.255.255.0  VLAN 20: 192.168.20.3 255.255.255.0	Associated IP:  VRID 10: 192.168.10.1 255.255.255.0  VRID 20: 192.168.20.1 255.255.255.0	Backup
PC 1		192.168.10.20 255.255.255.0	192.168.10.1	
PC 2		192.168.20.20 255.255.255.0	192.168.20.1	
SCALANCE XC206-2SFP	6GK5206-2BS00-2AC2	192.168.10.10	192.168.10.1	
SCALANCE XC206-2SFP	6GK5206-2BS00-2AC2	192.168.20.10	192.168.20.1	
SCALANCE XC206-2SFP	6GK5206-2BS00-2AC2	192.168.20.11	192.168.20.1	
SCALANCE S615	6GK5 615-0AA00-2AA2	Vlan 1: 192.168.1.2 255.255.255.0  Vlan 10: 192.168.10.2 255.255.255.0  VLAN 20: 192.168.20.2 255.255.255.0	Associated IP:  VRID 10: 192.168.10.1 255.255.255.0  VRID 20: 192.168.20.1 255.255.255.0	This firewall master is an alternative to the XM408 router.

Component	Item number	IP address and subnet mask	Router	Note
SCALANCE S615	6GK5 615-0AA00-2AA2	Vlan 1: 192.168.1.3 255.255.255.0  Vlan 10: 192.168.10.3 255.255.255.0  VLAN 20: 192.168.20.3 255.255.255.0	Associated IP:  VRID 10: 192.168.10.1 255.255.255.0  VRID 20: 192.168.20.1 255.255.255.0	This firewall backup is an alternative to the XM408 router.

This application example consists of the following components:

Table 1-2

Component	File name	Note
This document	109798556_VRRP_V1_0.en	

## 2 Hardware setup

The aim of the following application example is to establish communication between 2 PCs. Diagnostics need to be checked with a ping command from PC 1 to PC 2.

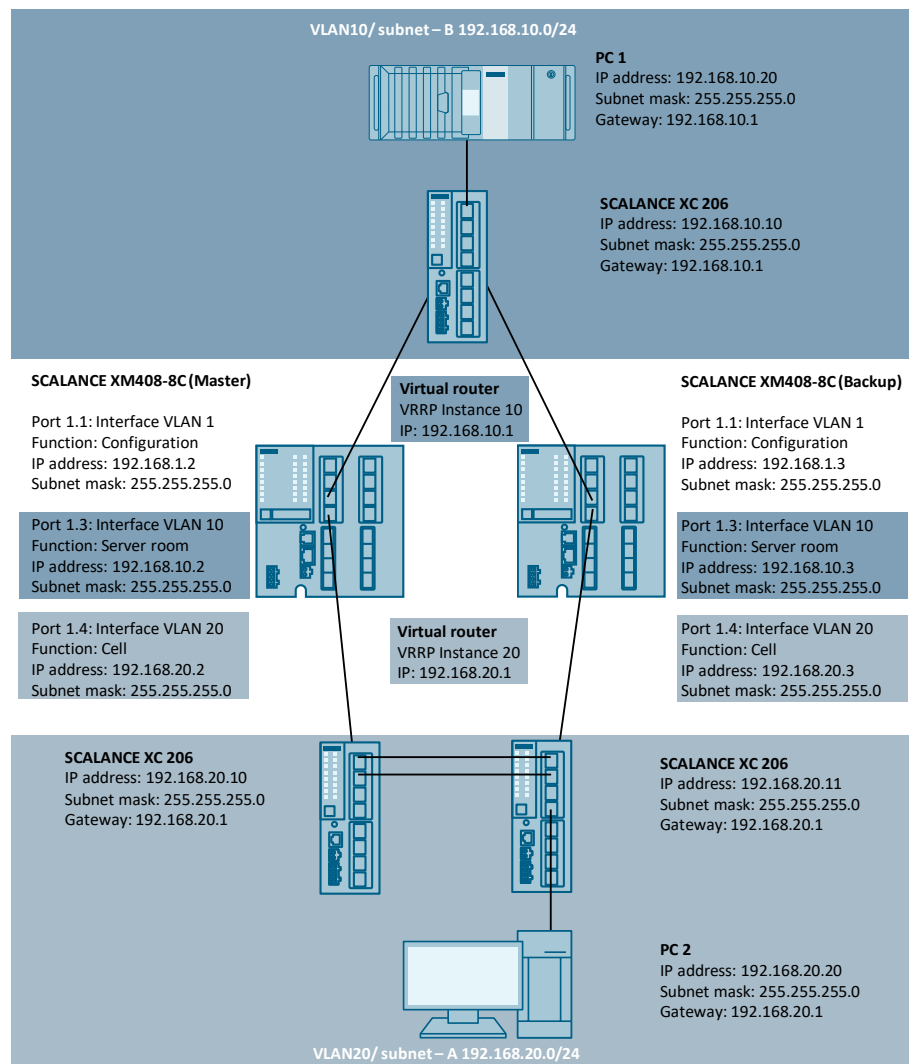
The following figures show the physical network structure.

The document explains 2 different hardware configurations:

- Hardware configuration with XM408-8C (no firewall)
- Hardware configuration with S615 (with firewall)

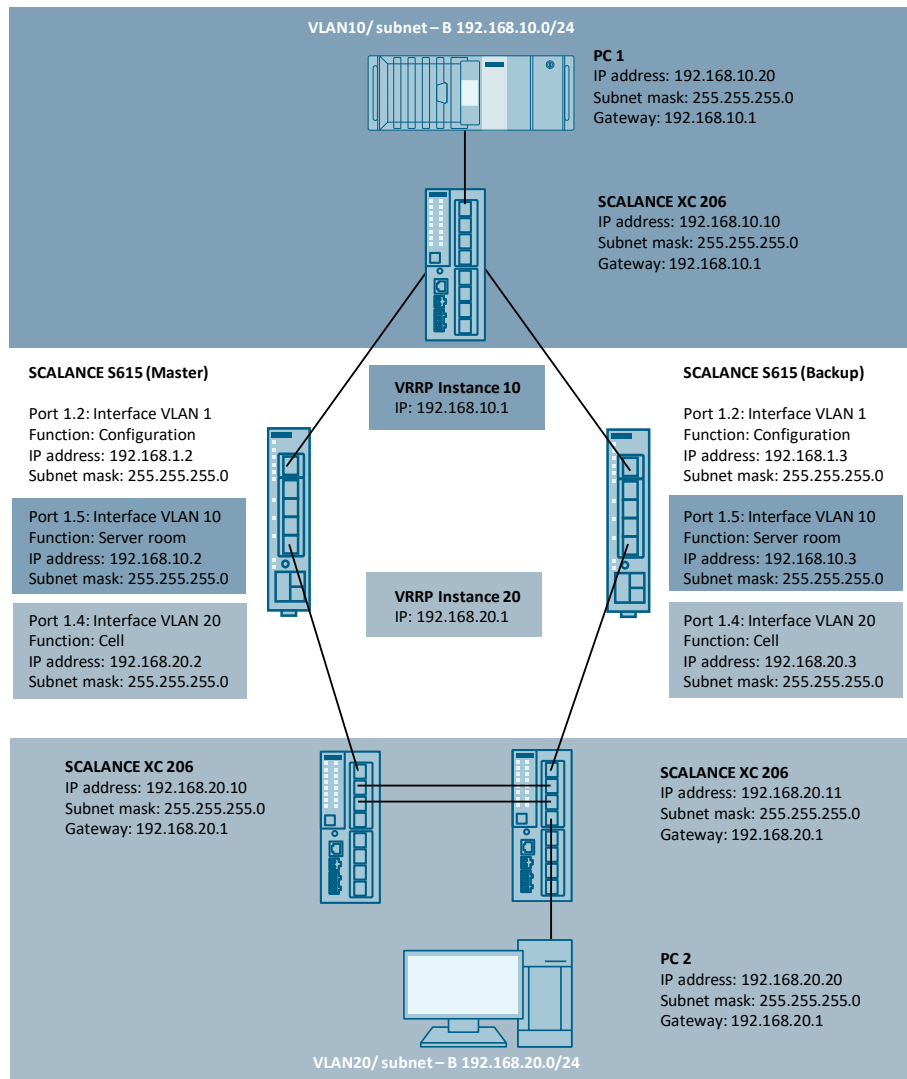
The Figure below shows the hardware setup with the SCALANCE XM408-8C.

Figure 2-1



The Figure below shoes the hardware setup with the SCALANCE S615.

Figure 2-2



## 3 Engineering VRRP

### 3.1 Commissioning PC and server

#### Description

This application example uses 2 PCs to test IP routing between the networks. You must enter a default router in all PCs. Only once it has been entered can the PC communicate with devices that are not in its own subnet.

The IP packets intended for a specific subnet are forwarded by the PC to the default router for further processing.

**Note**

In Windows, the default router is referred to as the "default gateway".

#### Overview of the addresses

The following table provides you with an overview that shows with which IP addresses and which standard gateways the PCs are configured with.

Table 3-1

PC	IP address	Subnet mask	Gateway
PC 1	192.168.10.20	255.255.255.0	192.168.10.1
PC 2	192.168.20.20	255.255.255.0	192.168.20.1

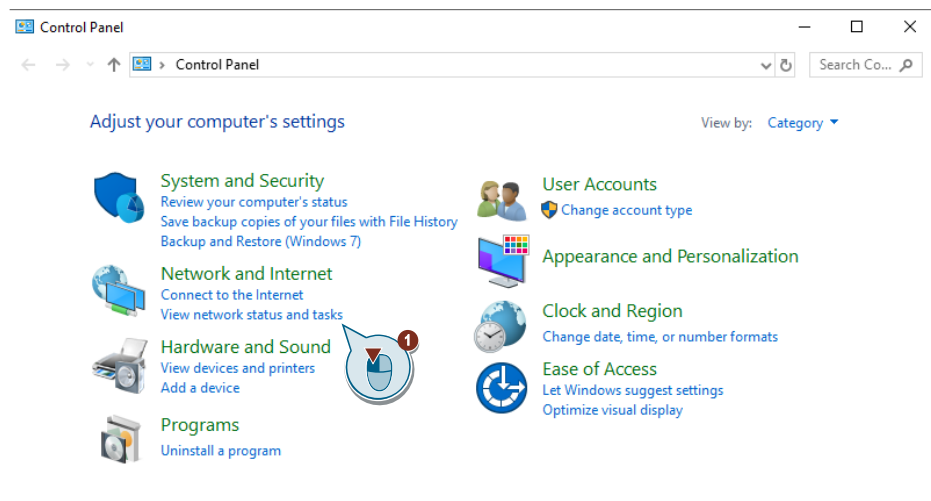
#### Entering a default router

The following instructions show you how to enter a default router on the PC in Windows 10 using PC 2 as an example.

Enter the default gateway in the Properties of your network adapter.

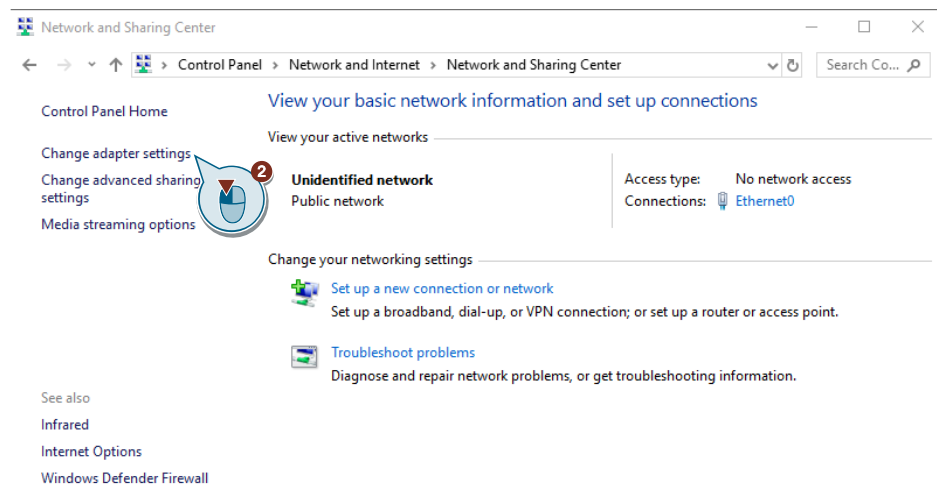
Proceed as follows to open the properties of the network adapter:

1. Navigate to "Start > Control Panel > Network and Internet" and click "View network status and tasks".



The "Network and Sharing Center" opens.

2. Click on "Change adapter settings" which appears in the left-hand sector of the window.

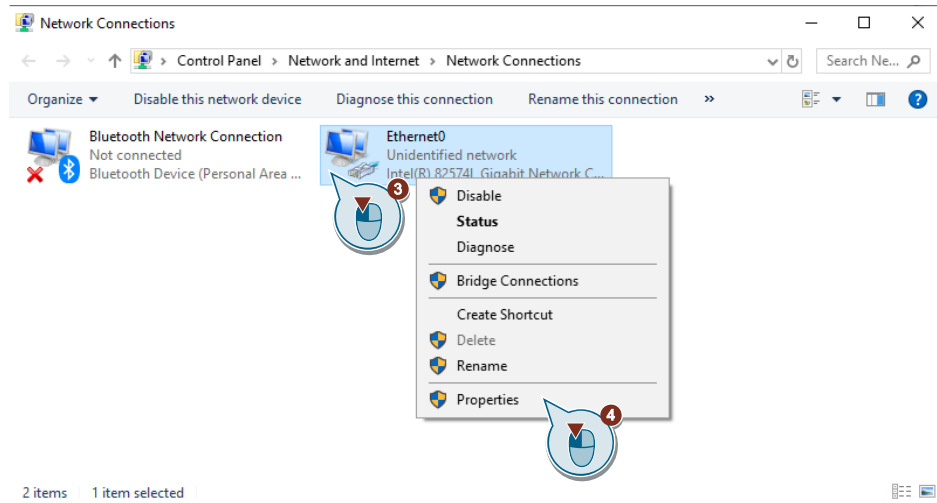


The "Network Connections" window will open.

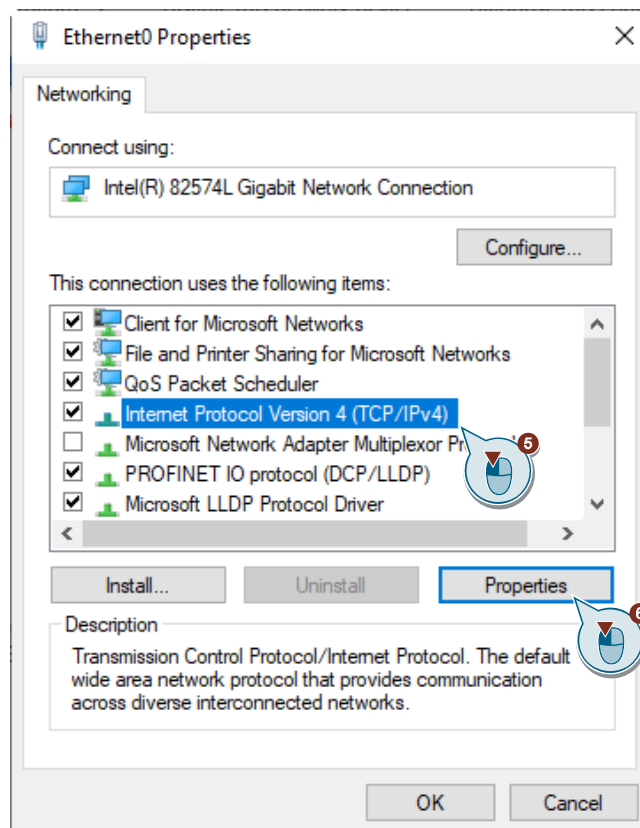


### 3 Engineering VRRP

3. You will see all available network adapters / network cards. With the left mouse button, select the entry you are using from the list.



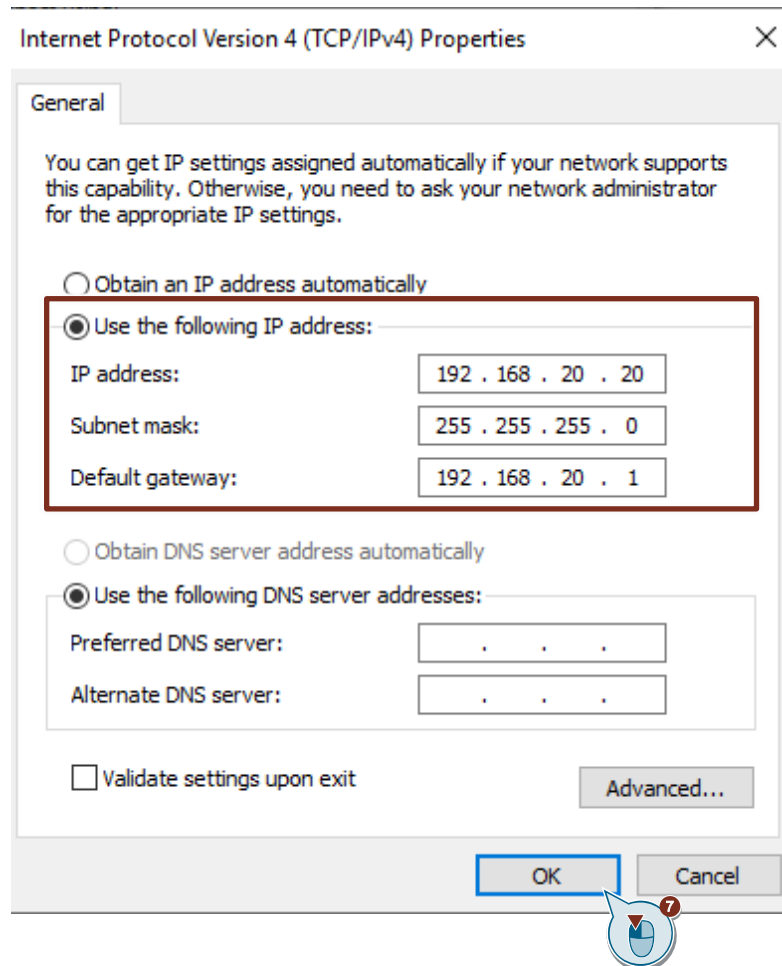
4. Right-click to open the context menu and click "Properties". The Properties window for the corresponding network adapter, network card or connection will open.
5. Left-click to select the item "Internet protocol Version 4 (TCP/IPv4)".



6. Then click the "Properties" button.

The Properties window for Internet protocol version 4 opens. Configure the properties as follows:

- a. Set the option to "Use the following IP address".
- b. Enter the "IP address" intended for the PC.
- c. Enter the "Subnet mask" intended for the PC.
- d. Enter the "Default gateway".



7. Then click the "OK" button.
8. When you have edited the properties, click "OK" in this dialog box and in the next.

#### Result

You have entered the IP address and the corresponding standard gateway in all the PCs. The PCs need these settings to communicate with remote subnets.

## 3.2 Commissioning SCALANCE

Some preparation is necessary before the SCALANCE XM-400 devices can be configured as a VRRP group.

You must prepare the following points in advance:

- Set up an Engineering PC
- Reset SCALANCE to factory setting (if necessary)
- Assign a management IP address
- Start Web Based Management (WBM)

### Setting up an engineering PC

The engineering PC is used to configure the SCALANCE devices using web-based management.

Assign the following IP address to the engineering PC:

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . . |

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

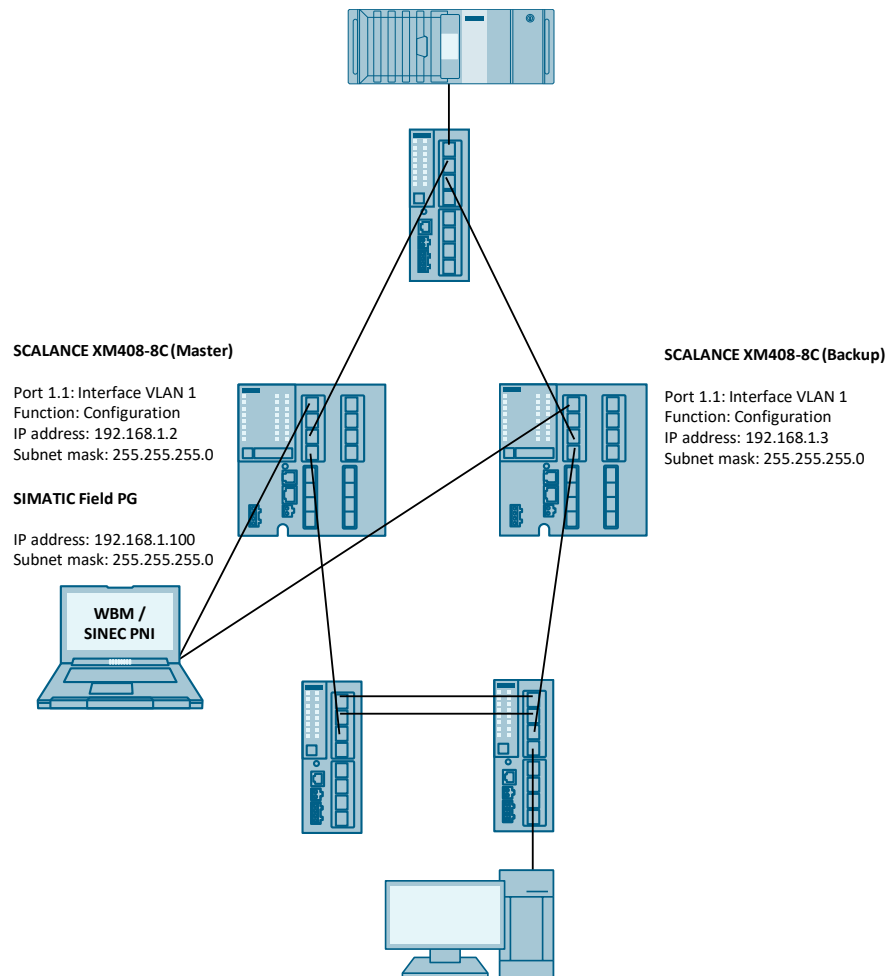
☐ Validate settings upon exit

Advanced...

OK Cancel

To establish a connection with the SCALANCE devices, the engineering PC is connected with port 1.1 of the respective SCALANCE.

Figure 3-1



### Resetting SCALANCE

If you are not using brand-new SCALANCE devices, it is recommended to reset both devices to factory settings.

That way you can be sure that no old configuration is stored in the SCALANCE.

For instructions on how to reset the SCALANCE, refer to the [Device manual](#).

### Assigning the IP address

The first assignment of an IP address for the SCALANCE cannot be done with Web Based Management, because this configuration tool requires an IP address in the first place.

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

- SINEC PNI
- PRONETA
- STEP 7
- DHCP

[SINEC PNI](#) and [PRONETA](#) are available to you for free as downloads in the Industry Online Support.

Assign the planned IP address to the two SCALANCE routers with one of the aforementioned tools:

Table 3-2

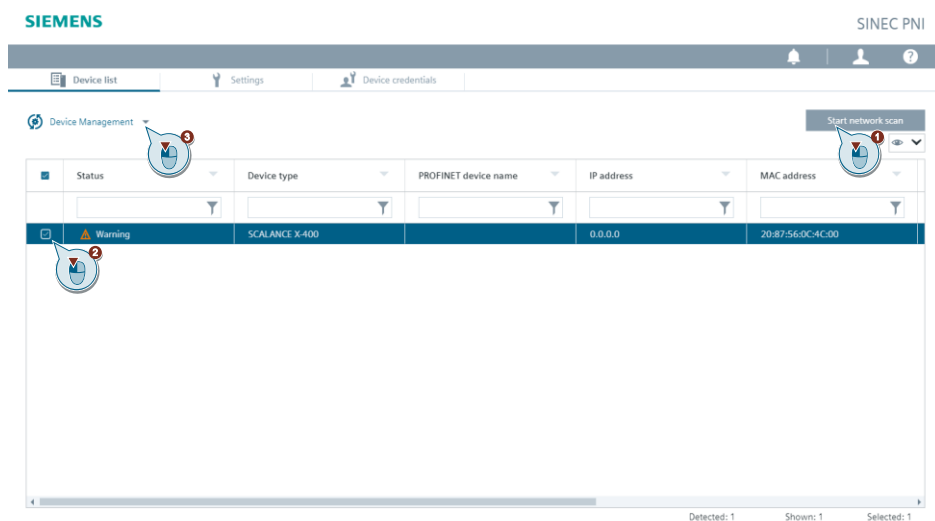
Device	Function	IP address	Subnet mask
SCALANCE XM408-8C	VRRP master	192.168.1.2	255.255.255.0
SCALANCE XM408-8C	VRRP backup	192.168.1.3	255.255.255.0

#### Note

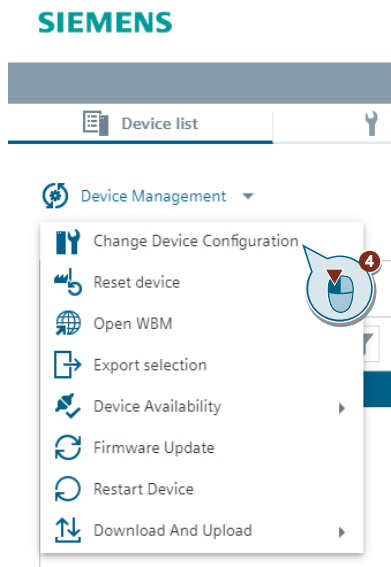
VRRPv3 supports IPv4 and IPv6. Both can be configured and operated simultaneously with VRRPv3.

The following figures describe configuration with SINEC PNI.

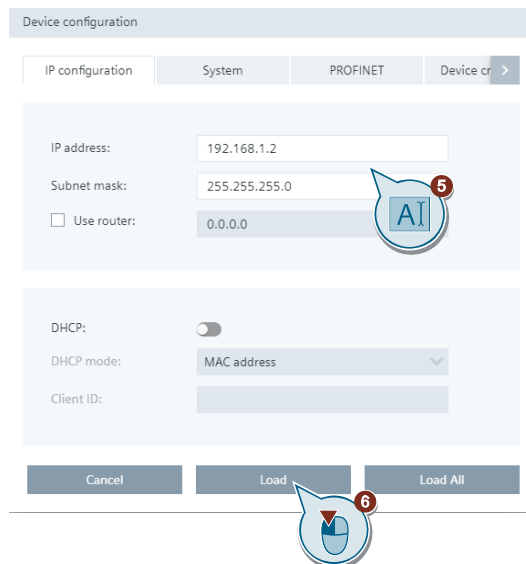
1. Click "Start network scan".
2. Select the device found.
3. Click the "Device Management" button.



- Click "Change Device Configuration".



- Assign an IP address and a subnet mask.

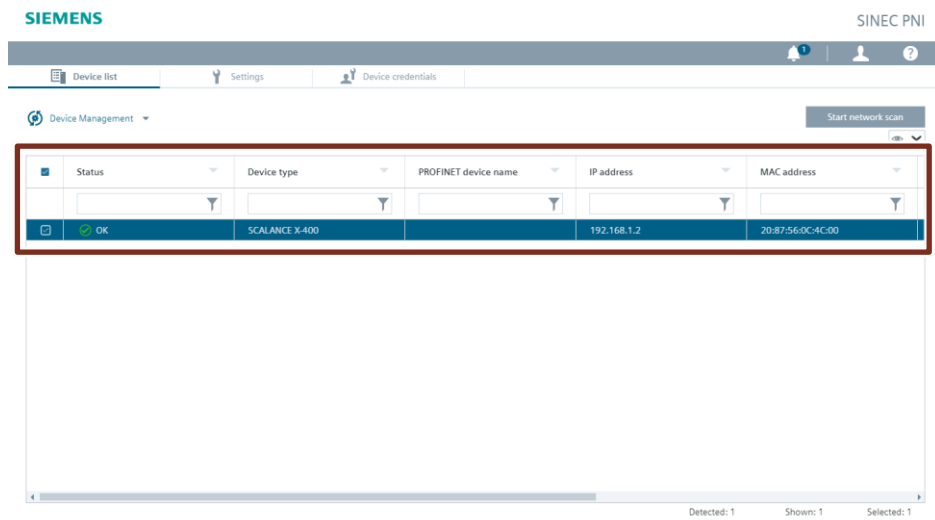


- Click "Load".



#### Result

The IP address and subnet mask have been assigned.



The screenshot shows the Siemens SINEC PNI Device Management interface. At the top, there is a navigation bar with 'SIEMENS' on the left and 'SINEC PNI' on the right. Below this is a menu bar with 'Device list', 'Settings', and 'Device credentials'. The main area is titled 'Device Management' and contains a table with the following columns: Status, Device type, PROFINET device name, IP address, and MAC address. A single device is listed in the table, highlighted with a red border. The device is a SCALANCE X-400 with an IP address of 192.168.1.2 and a MAC address of 20:87:56:0C:4C:00. The status is 'OK'. At the bottom right of the table, it says 'Detected: 1', 'Shown: 1', and 'Selected: 1'.

Status	Device type	PROFINET device name	IP address	MAC address
OK	SCALANCE X-400		192.168.1.2	20:87:56:0C:4C:00

7. Assign the VRRP routers and the switches their respective IP address, subnet mask and gateway.

#### Start Web Based Management

The SCALANCE device has an integrated HTTP server for Web Based Management.

To implement Web Based Management, the following conditions must be met:

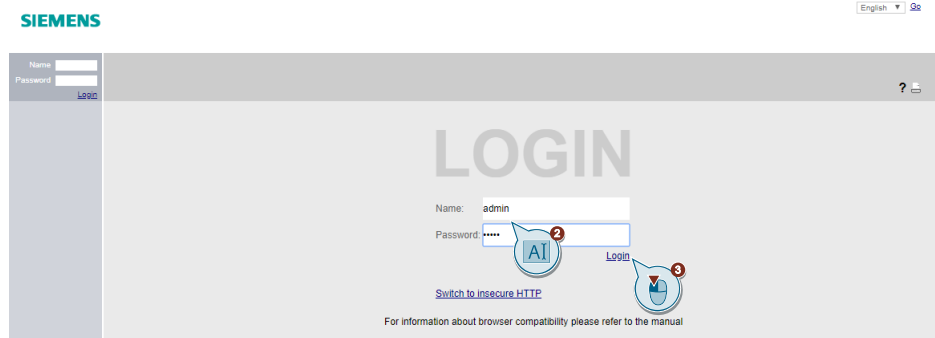
- The device has an IP address.
- There is a connection between the SCALANCE and the engineering PC. You can use the ping command to check whether the SCALANCE is accessible.

**Note**

Use the https protocol to establish a secure connection to the SCALANCE.

Proceed as follows to open Web Based Management:

1. In the address bar of the internet browser, enter the IP address of the SCALANCE, for example the address <https://192.168.1.2> for the VRRP master. If a connection to the device is established with no errors, the login page will appear.
2. When you log in for the first time or after a "Reset to factory settings and restart", enter the factory default user "admin" and password "admin".



3. Then click the "Login" button or confirm by pressing "Enter".

4. When you log in for the first time or after a "Reset to factory settings and restart" using the default user, you will be prompted to change the password.

**SIEMENS**

Welcome admin  
[Logout](#)

### Account Passwords

Current User: admin  
Current User Password: .....

User Account: admin  
Password Policy: high  
New Admin Account Name: AdminAndreas  
New Password: .....  
Password Confirmation: .....

[Set Values](#) [Refresh](#)

Enter "admin" for the current user password.

5. Select the "User account" as admin.
6. Assign a new password under "New Password". Confirm the password by entering it again ("Password Confirmation").
7. To complete the process and enable the new password, click "Set Values". If you have successfully logged in, the start page appears.

### 3.3 Configuring the master router

To configure the SCALANCE XM408 as VRRP master, the following essential parameter assignment steps must be made:

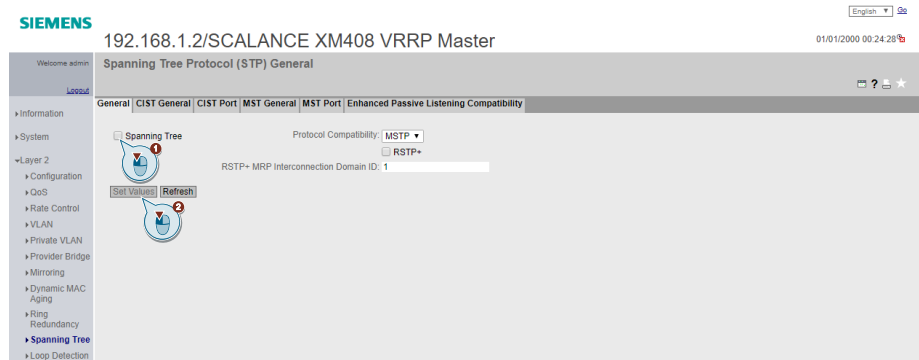
- Disable Spanning Tree Protocol
- Create VLANs
- Activate routing
- Create subnets
- Configure VRRP

The following sections will show you how to configure the SCALANCE via Web Based Management.

Connect the engineering PC to the SCALANCE and open Web Based Management.

#### 3.3.1 Disable Spanning Tree Protocol

1. Disable the "Spanning Tree" protocol. The Spanning Tree protocol is enabled by default. The Spanning Tree protocol is designed to detect loops and only permit one active path to each node. Go to "Layer 2 > Spanning Tree". Untick the checkbox.
2. Click the "Set Values" button.



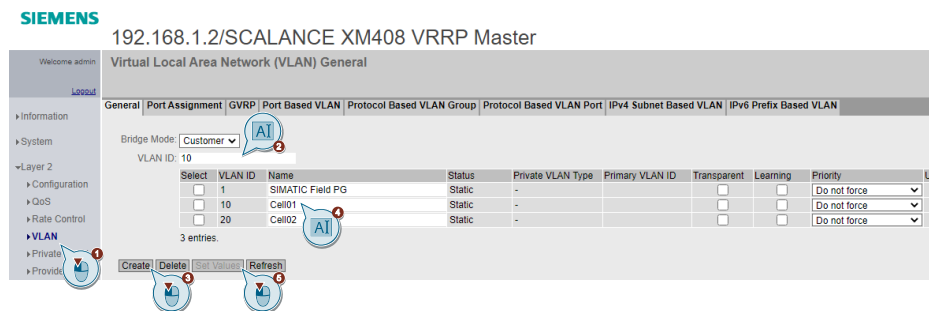
### 3.3.2 Create VLANs

**Note**

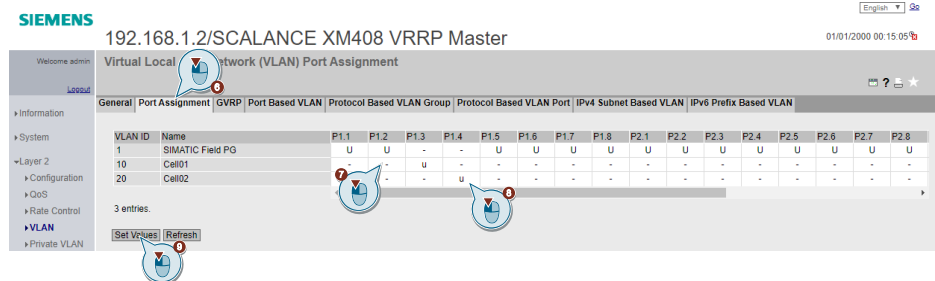
You can only use VRRPv3 in connection with VLAN interfaces. Router ports are not supported.

In the configuration discussed here, 3 different VLANs are configured: A TIA interface (VLAN 1) that serves as a configuration interface and 2 VLANs for the server (VLAN 10) and the cell (VLAN 20). The communication between the virtual networks is done via routing. Port-based VLAN is used in this setup for VLAN division. The telegrams to the cell and to the servers are sent without a tag, as there are no devices there that can interpret it.

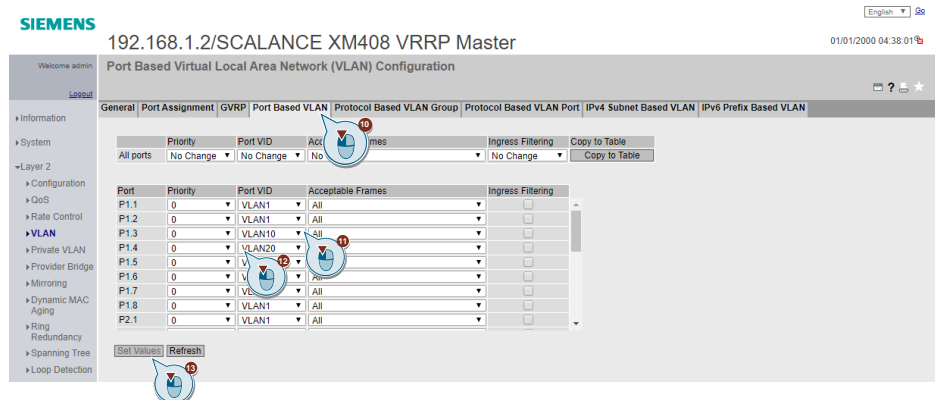
1. Open the menu "Layer 2 > VLAN".
2. Enter the VLAN ID 10 and 20.
3. "Create" the VLANs 10 and 20.
4. Assign the VLANs a name.
5. Click the "Set Values" button.



6. Open the "Port Assignment" tab.
7. Set "Port P1.3" to "U" (untagged) for VLAN 10.
8. Set "Port P1.4" to "U" (untagged) for VLAN 20. The packets will be sent without a tag. These settings apply only to outgoing telegrams.
9. Click the "Set Values" button.



10. To correctly configure the VLANs, the tagging for incoming telegrams that reach the switch without a tag must also be set. Open the "Port Based VLAN" tab.
11. Assign VLAN 10 to "Port P1.3".
12. Assign VLAN 20 to "Port P1.4".
13. Click the "Set Values" button.



## Result

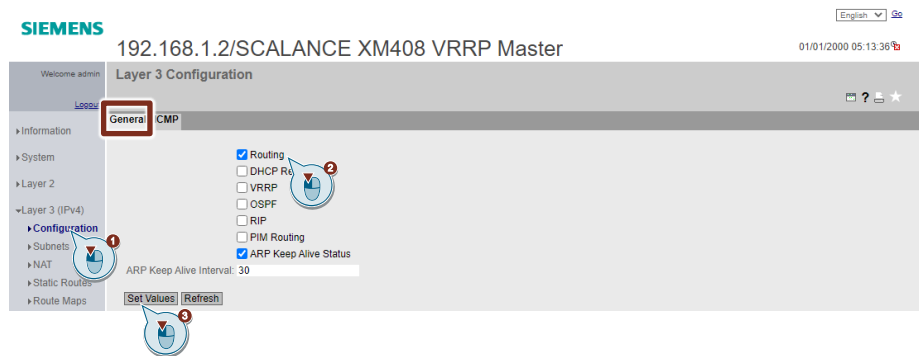
You have created the two VLANs 10 and 20 for incoming and outgoing telegrams.



### 3.3.3 Activate routing

Until now, only Layer 2 communication has functioned via the access router. However, the structure of the network makes it essential to communicate over Layer 3. Otherwise, data exchange between the network segments will not be possible.

1. Go to the menu item "Layer 3 (IPv4) > Configuration" and then to the "General" tab.
2. Enable "Routing" (when you do this, VRRPv3 will automatically be used).
3. Click the "Set Values" button.



### 3.3.4 Create subnets

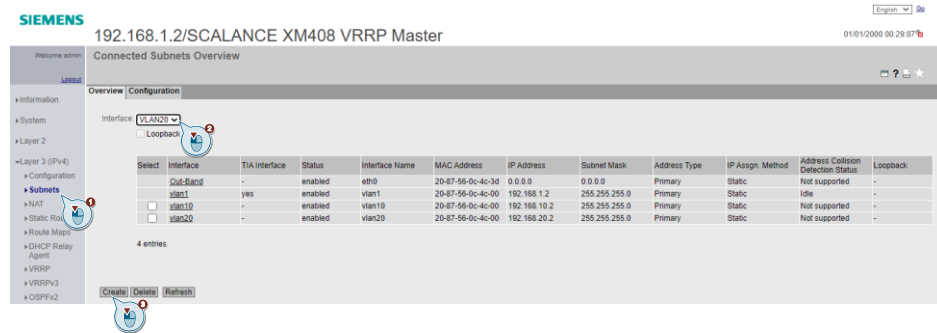
In its function as an IP router, the SCALANCE needs a separate IP address and subnet mask for each adjoining subnet. This is the only way it can send IP packets from one subnet to another subnet. Routes will be created automatically for the subnets entered.

The following table shows you which IP address the subnets are configured with.

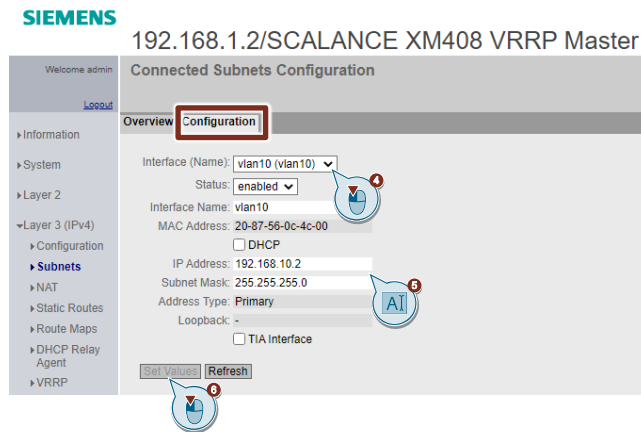
Table 3-3

Master/Backup	VLAN	IP address	Subnet mask
Master	VLAN 10	192.168.10.2	255.255.255.0
Master	VLAN 20	192.168.20.2	255.255.255.0

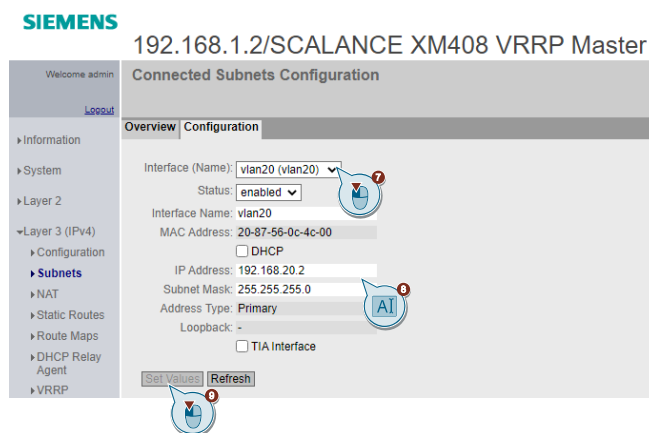
1. Open the "Overview" tab in the menu "Layer 3 (IPv4) > Subnets". There you can assign the subnets to their corresponding interfaces.
2. Select a VLAN from the dropdown menu (VLAN 20 is pictured here).
3. Click the "Create" button to generate an interface for the switch in this VLAN. The default IP address of the new interface is always 0.0.0.0.



4. Under the "Configuration" tab, select the interface whose IP address you wish to change.
5. For the "VLAN 10", enter the IP address 192.168.10.2 and the subnet mask 255.255.255.0.
6. Click the "Set Values" button.



7. Now select VLAN 20 from the dropdown menu.
8. For this VLAN, assign the IP address 192.168.20.2 and the subnet mask 255.255.255.0.
9. Click the "Set Values" button.



### 3.3.5 Configure VRRP

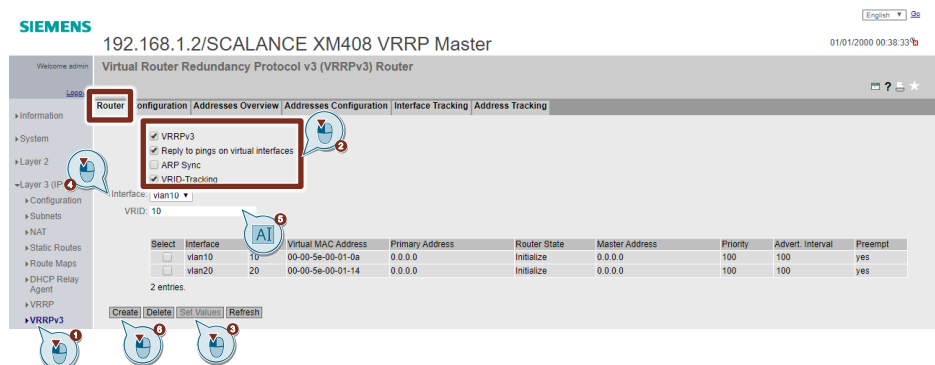
The section below describes how to configure the Virtual Router Redundancy Protocol V3 (VRRPv3). The master router will act as master in the VLANs 10 and 20.

**Note**

Running VRRP and VRRPv3 at the same time is not possible.

#### Creating the virtual router instance

1. Navigate to the "Router" tab in the menu "Layer3 (IPv4) > VRRPv3".
2. Enable routing via "VRRPv3".  
Enable "Reply to pings on virtual interfaces".  
Enable VRID tracking. For more information on VRID tracking refer to the [Useful information](#) chapter.
3. Click the "Set Values" button.
4. Now, to create a VRRP router for the VLAN 10 subnet, select the corresponding interface.
5. Enter a VRID 10.  
The VRID is any number between 1 and 255. When choosing the number, it is important to make sure that both VRRP partners have the same VRID for each VLAN and that no other VRRP devices in the same VLAN have the same VRID. For the sake of simplicity in this example, we use the VLAN ID as the VRID in each VLAN.
6. Click the "Create" button to create a virtual router instance.

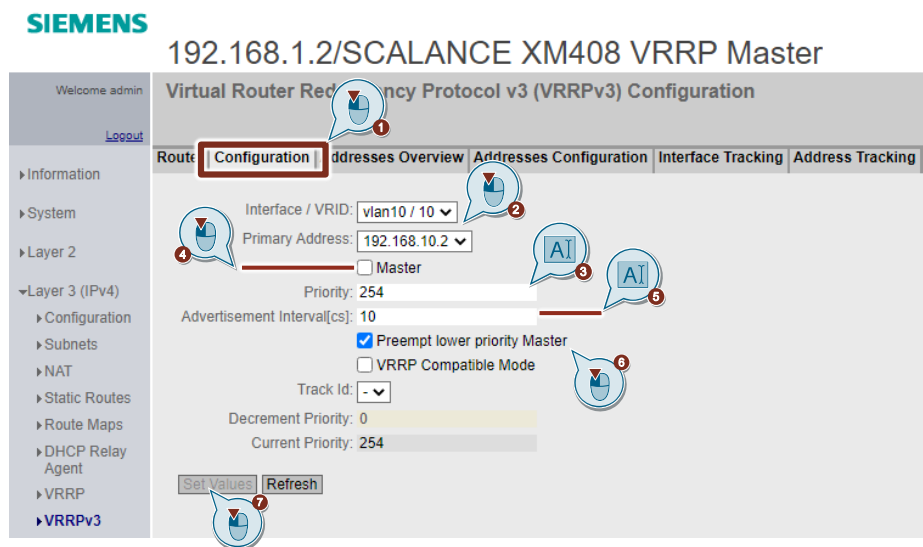


7. Follow the same procedure again to create a virtual router instance for VLAN 20 (VRID = 20).

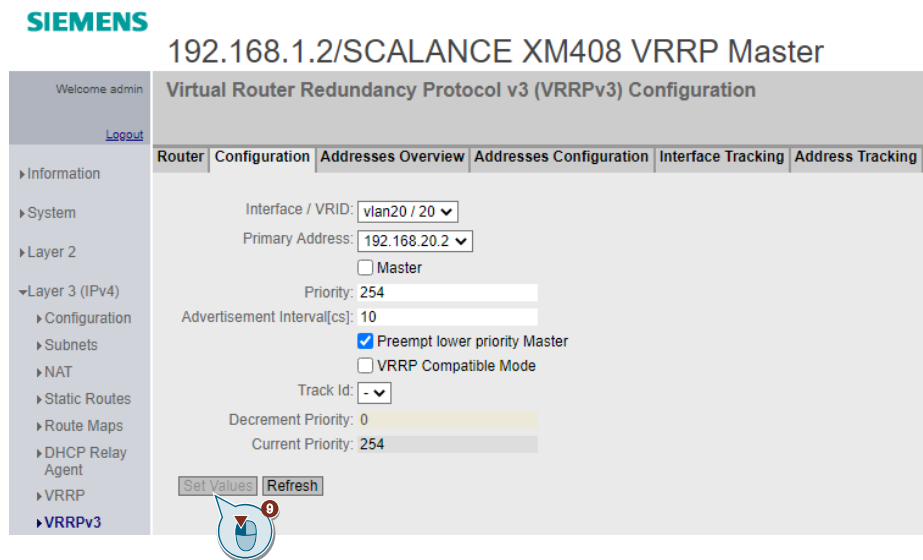
#### Configuring the router instance

1. Now switch to the "Configuration" tab to configure the virtual router.
2. Under "Interface / VRID", select vian10/ 10 and assign it the IP address (192.168.10.2) set for the subnet.
3. For the VLANs in which the router needs to function as master, enter "Priority" 254.

4. Leave the "Master" function unticked.  
The reason for this is that when the master is named explicitly, its IP address is also automatically entered as the Associated IP Address. This is not desired here, as the VRRP partners should respond to a third, virtual IP address.
5. Leave the "Advertisement Interval" at one second (10 cs = 1 s).
6. Check the box for "Preempt lower priority master".  
This ensures that, if a master returns, it will reassume the master role.
7. Click the "Set Values" button.



8. Now select vlan20/ 20 under Interface / VRID in the same dialog and enter the values according to the following image.

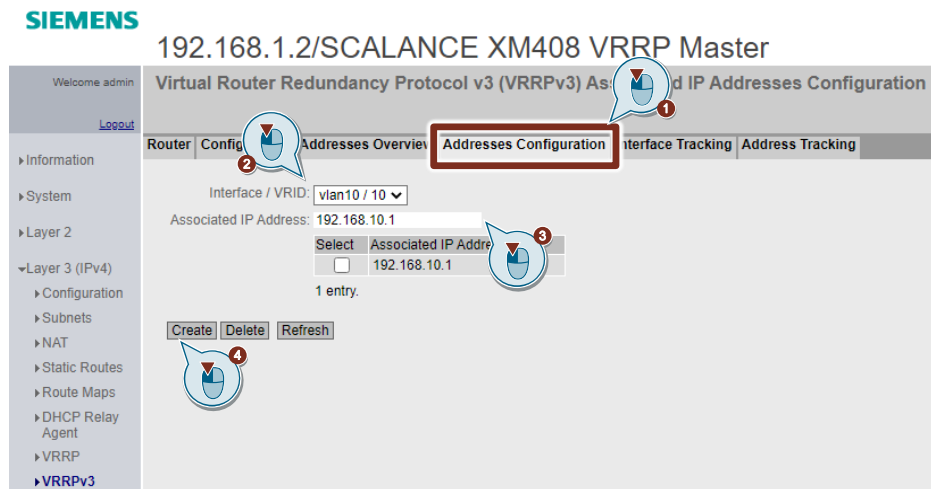


9. Click the "Set Values" button and close the dialog.

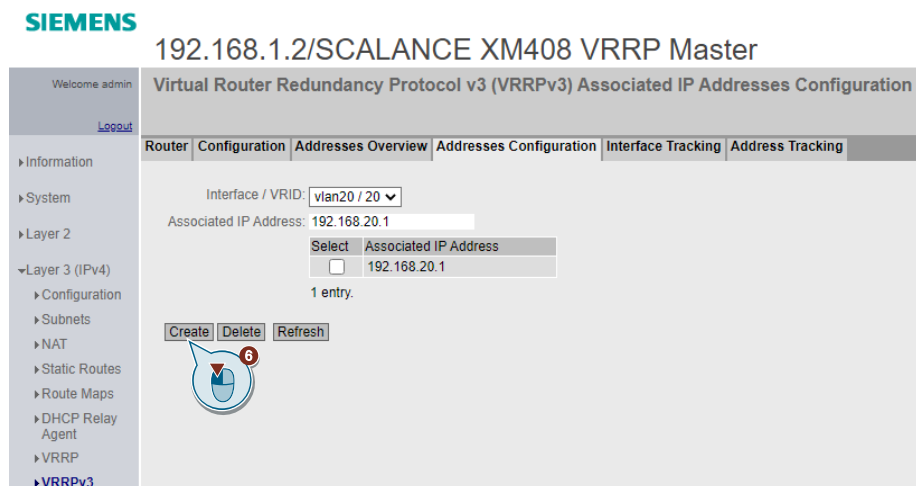
#### Configuring the addresses

For VRRP to function, the VRRP router instances must be assigned IP addresses. Here, both Layer 3 routers receive the first address in the subnet. As a consequence, one router will always be reachable at the address XX.XX.XX.1, which is the first address in the subnet.

1. Switch to the "Address Configuration" tab.
2. Under "Interface / VRID", select vlan10/ 10.
3. Enter the "Associated IP Address" 192.168.10.1.
4. Click on the "Create" button.



5. Now select vlan20/ 20 in the same dialog under "Interface / VRID" and enter the values as shown in the image below.



6. Click on the "Create" button.



## Result

The "Addresses Overview" tab lists an overview of all assigned addresses.

**SIEMENS** 192.168.1.2/SCALANCE XM408 VRRP Master

Welcome admin [Logout](#)

Virtual Router Redundancy Protocol v3 (VRRPv3) Associated IP Addresses Overview

Router | Configuration | **Addresses Overview** | Addresses Configuration | Interface Tracking | Address Tracking

Interface	VRID	Number of Addresses	Associated IP Address (1)	Associated IP Address (2)	Associated IP Address (3)	Associated IP Address (4)
vlan10	10	1	192.168.10.1	0.0.0.0	0.0.0.0	0.0.0.0
vlan20	20	1	192.168.20.1	0.0.0.0	0.0.0.0	0.0.0.0

[Refresh](#)

Information

- System
- Layer 2
- Layer 3 (IPv4)
  - Configuration
  - Subnets
  - NAT
  - Static Routes
  - Route Maps
  - DHCP Relay Agent
  - VRRP
  - VRRPv3**

## 3.4 Configuring the backup router

To configure the SCALANCE XM408 as VRRP backup, the following essential parameter assignment steps must be made:

- Disable Spanning Tree Protocol
- Create VLANs
- Activate routing
- Create subnets
- Configure VRRP

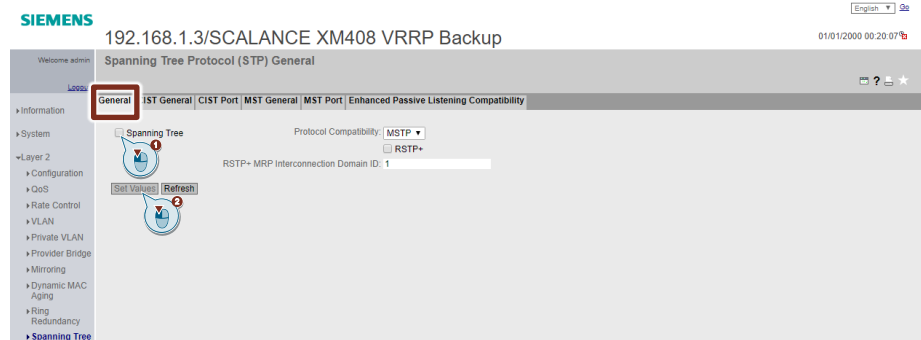
The following sections will show you how to configure the SCALANCE via Web Based Management.

Connect the engineering PC to the SCALANCE and open Web Based Management for the backup router.

The configuration for the backup router is largely the same as with the master. The general settings are identical, the Layer 2 functions are configured the same, and the VLAN division is also exactly the same.

### 3.4.1 Disable Spanning Tree Protocol

1. Disable the "Spanning Tree" protocol. The Spanning Tree protocol is enabled by default. The Spanning Tree protocol is designed such that it detects loops and only one active path to each node exists. Go to "Layer 2 > Spanning Tree" and then to the "General" tab in the menu. Untick the checkbox "Spanning Tree".
2. Click the "Set Values" button.



### 3.4.2 Create VLANs

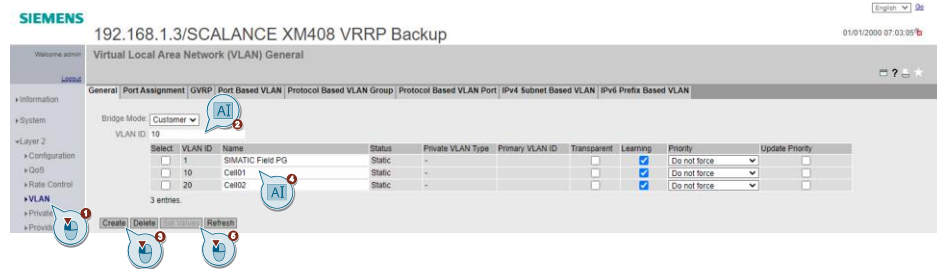
**Note**

You can only use VRRPv3 in connection with VLAN interfaces. Router ports are not supported.

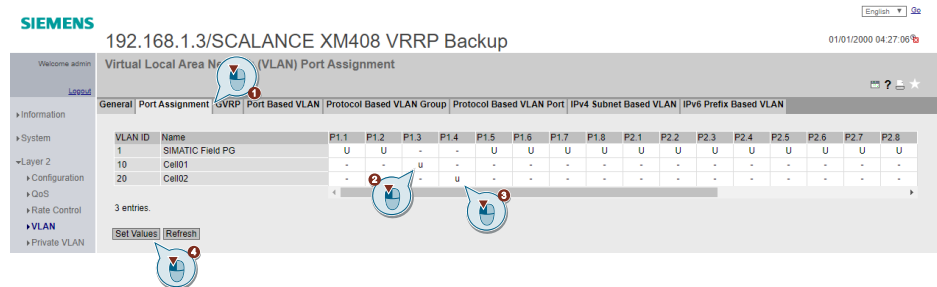
In the configuration discussed here, 3 different VLANs are configured: A TIA interface (VLAN 1) that serves as a configuration interface and 2 VLANs for the server (VLAN 10) and the cell (VLAN 20). The communication between the virtual networks is done via routing. A port-based VLAN is used in this setup for VLAN division. The telegrams to the cell and to the servers are sent without a tag, as there are no devices there that can interpret it.

**General settings**

1. Open the menu "Layer 2 > VLAN".
2. Enter the VLAN ID 10 and 20.
3. "Create" the VLANs 10 and 20.
4. Assign the VLANs a name.
5. Click the "Set Values" button.


**Port assignment**

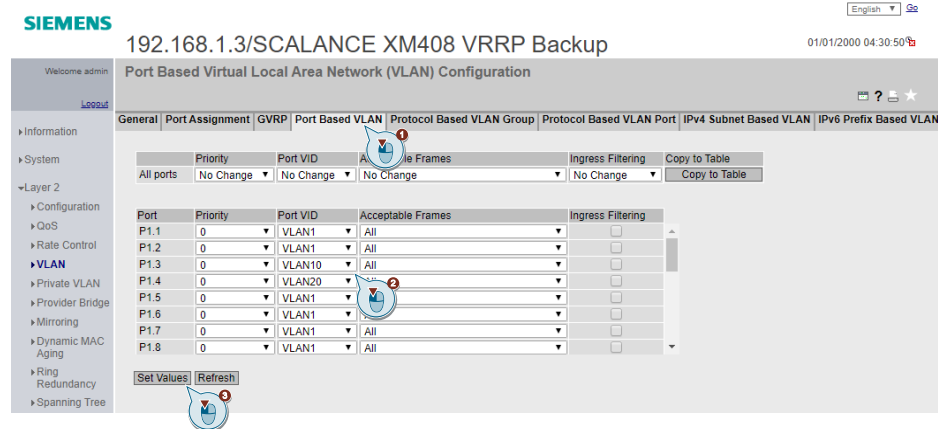
1. Open the "Port Assignment" tab.
2. Set "Port P1.3" to "U" (untagged) for VLAN 10.
3. Set "Port P1.4" to "U" (untagged) for VLAN 20. The packets will be sent without a tag. These settings apply only to outgoing telegrams.
4. Click the "Set Values" button.



## Tagging

To correctly configure the VLANs, the tagging for incoming telegrams that reach the switch without a tag must also be set.

1. Open the "Port Based VLAN" tab.
2. Assign "VLAN 10" to "Port P1.3".
3. Assign "VLAN 20" to "Port P1.4".
4. Click the "Set Values" button.



## Result

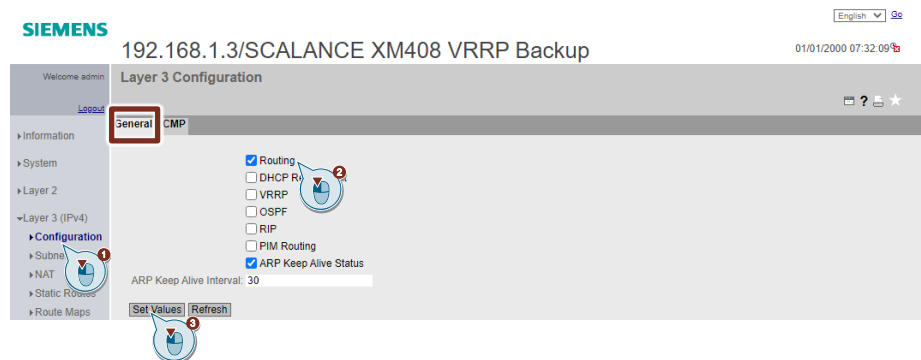
You have created the two VLANs 10 and 20 for incoming and outgoing telegrams.

### 3.4.3 Activate routing

Until now, only Layer 2 communication has functioned via the access router. However, the structure of the network makes it essential to communicate over Layer 3. Otherwise, data exchange between the network segments will not be possible.

Enable Layer 3 routing as follows:

1. Go to the menu item "Layer 3 (IPv4) > Configuration" and then to the "General" tab.
2. Tick the "Routing" checkbox. By enabling routing, VRRPv3 will be used automatically.
3. Click the "Set Values" button.



### 3.4.4 Create subnets

In its function as an IP router, the SCALANCE needs a separate IP address and subnet mask for each adjoining subnet. This is the only way it can send IP packets from one subnet to another subnet. Automatic routes will be created for the subnets entered.

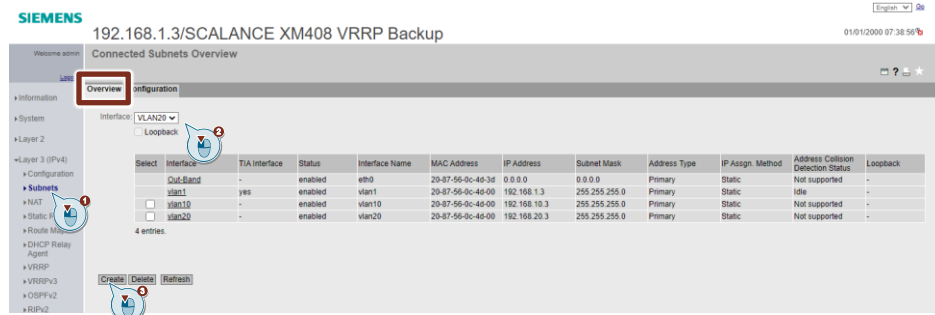
The following table shows the IP addresses with which the subnets are configured.

Table 3-4

Master/Backup	VLAN	IP address	Subnet mask
Backup	VLAN 10	192.168.10.3	255.255.255.0
Backup	VLAN 20	192.168.20.3	255.255.255.0

#### Create interface

1. In "Layer 3 (IPv4) > Subnets", navigate to the "Overview" tab. Subnets are assigned to the interfaces in this dialog.
2. Select a VLAN (VLAN20) from the dropdown menu.
3. Click the "Create" button to generate an interface for the switch in this VLAN. The default IP address of the new interface is always 0.0.0.0.

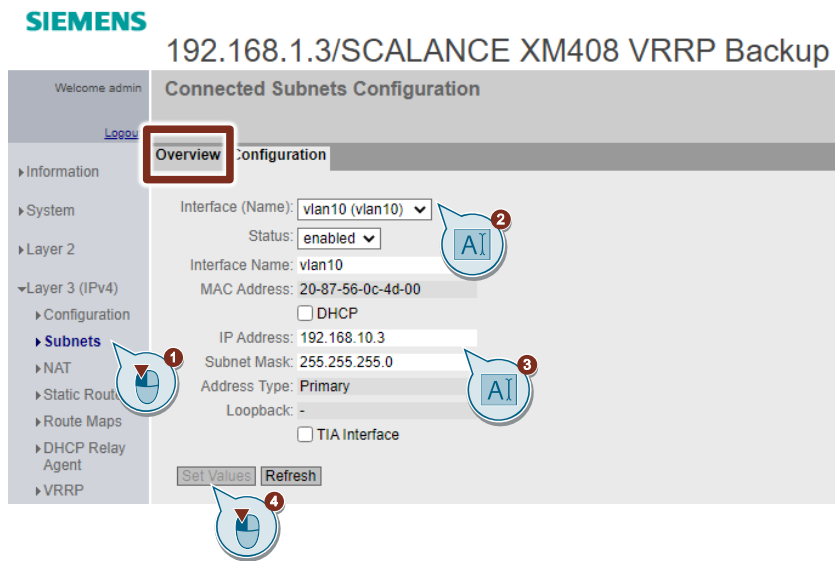


4. Also create an interface for VLAN10 in the same way.

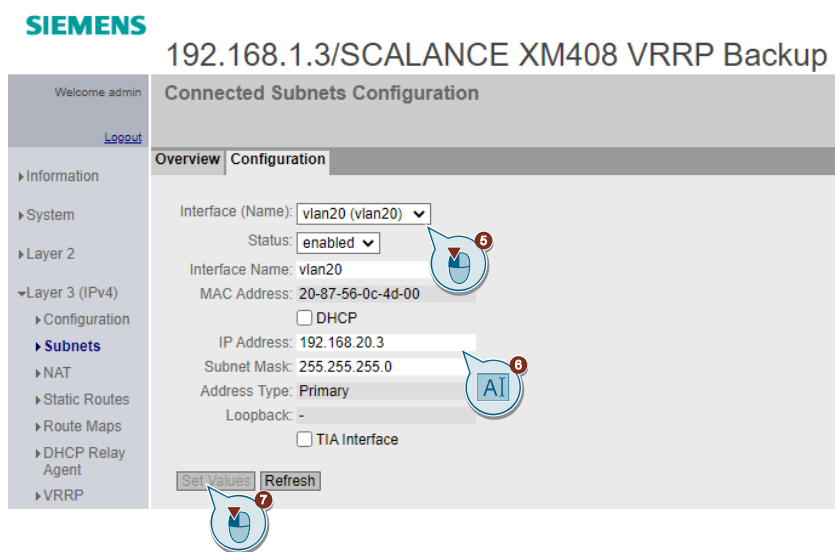
#### Interface configuration

1. Switch to the "Configuration" tab to modify the address and the subnet mask of an interface.
2. Select vlan10 (vlan10) from the "Interface (Name)" dropdown menu.
3. For the "VLAN 10", enter the IP address 192.168.10.3 and the subnet mask 255.255.255.0.

- Click the "Set Values" button.



- Select vlan20 (vlan20) from the "Interface (Name)" dropdown menu.
- For the "VLAN 20", enter the IP address 192.168.20.3 and the subnet mask 255.255.255.0.
- Click the "Set Values" button.



### 3.4.5 Configure VRRP

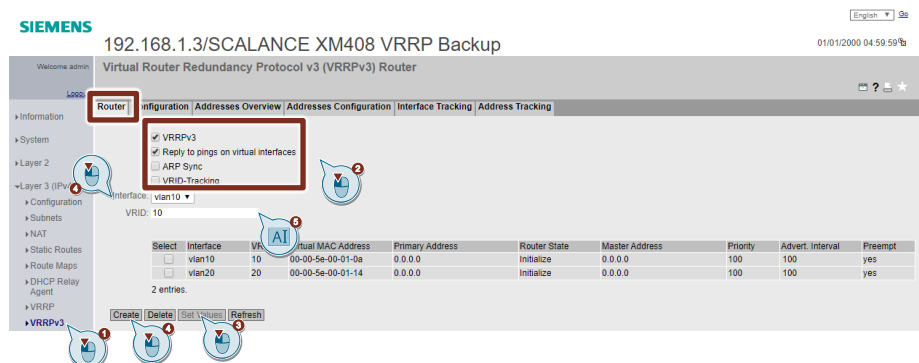
The section below describes how to configure the Virtual Router Redundancy Protocol V3 (VRRPv3). The backup router should act as a backup in VLANs 10 and 20.

**Note**

Running VRRP and VRRPv3 at the same time is not possible.

#### Create the virtual router instance

1. Navigate to the "Router" tab in the menu "Layer3 (IPv4) > VRRPv3".
2. Enable routing via "VRRPv3".  
Enable "Reply to pings on virtual interfaces".  
Enable VRID tracking. For more information on VRID tracking, refer to the [Useful information](#) chapter.
3. Click the "Set Values" button.
4. Now, to create a VRRP router for the VLAN 10 subnet, select the corresponding interface.
5. Enter a VRID 10.  
The VRID is any number between 1 and 255. When choosing the number, it is important to make sure that both VRRP partners have the same VRID for each VLAN and that no other VRRP devices in the same VLAN have the same VRID. For the sake of simplicity in this example, we use the VLAN ID as the VRID in each VLAN.
6. Click the "Create" button to create a virtual router instance.



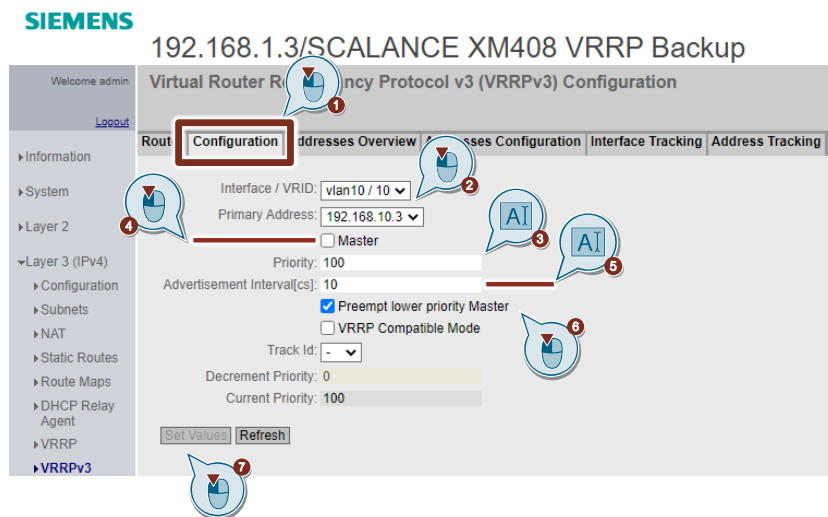
7. Follow the same procedure again to create a virtual router instance for VLAN 20 (VRID = 20).

#### Configuring the router instance

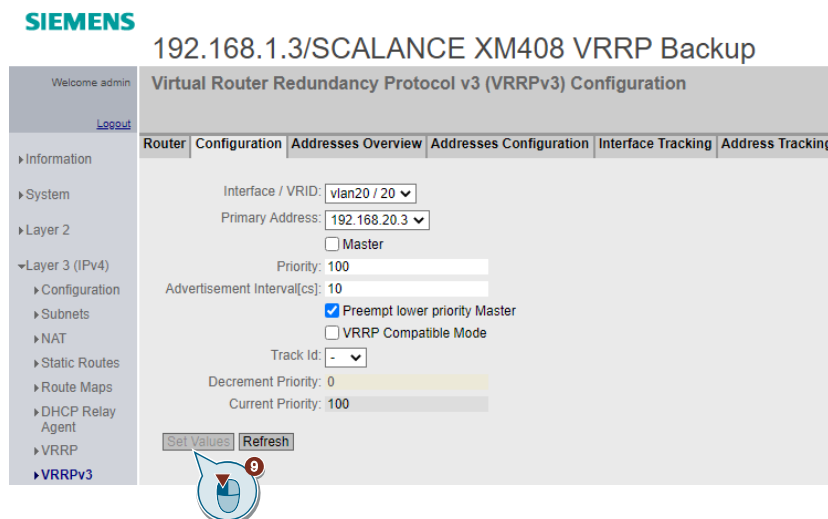
1. Now switch to the "Configuration" tab to configure the virtual router.
2. Under "Interface / VRID", select vlan10/ 10 and assign it the IP address (192.168.10.3) set for the subnet.
3. For the VLANs in which the router needs to function as master, enter "Priority" 254.



4. Leave the "Master" function unticked.  
The reason for this is that when the master is named explicitly, its IP address is also automatically entered as the Associated IP Address. This is not desired here, as the VRRP partners should respond to a third, virtual IP address.
5. Leave the "Advertisement Interval" at one second (10 cs = 1 s).
6. Check the box for "Preempt lower priority master".  
This ensures that, if a master returns, it will reassume the master role.
7. Click the "Set Values" button.



8. Now select vlan20/ 20 in the same dialog under "Interface / VRID" and enter the values as shown in the image below.

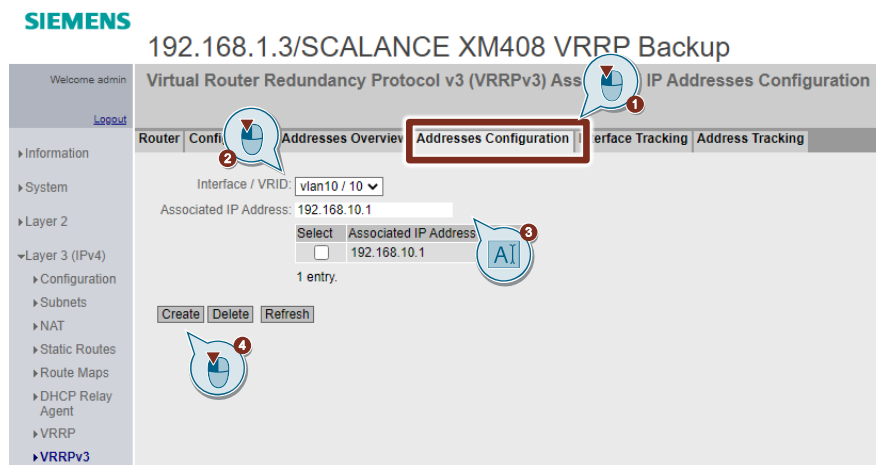


9. Click the "Set Values" button and close the dialog.

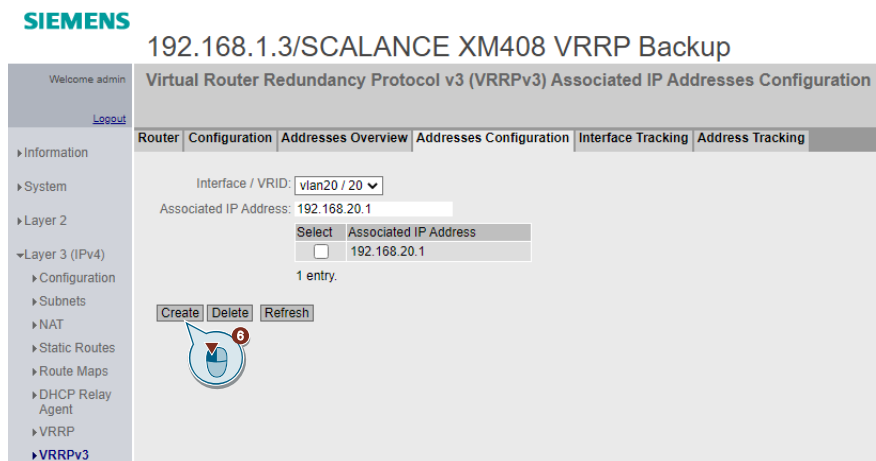
#### Address configuration

For VRRP to function, the VRRP router instances must be assigned IP addresses. Here, both Layer 3 routers receive the first address in the subnet. As a consequence, one router will always be reachable at the address XX.XX.XX.1, which is the first address in the subnet.

1. Switch to the "Address Configuration" tab.
2. Under "Interface / VRID", select vlan10/ 10.
3. Enter the "Associated IP Address" 192.168.10.1.
4. Click on the "Create" button.



5. Now select vlan20/ 20 in the same dialog under "Interface / VRID" and enter the values as shown in the image below.



6. Click on the "Create" button.

## Result

The assigned addresses will be listed in the "Addresses Overview" tab.

**SIEMENS** 192.168.1.3/SCALANCE XM408 VRRP Backup

Welcome admin [Logout](#)

Virtual Router Redundancy Protocol v3 (VRRPv3) Associated IP Addresses Overview

Router | Configuration | **Addresses Overview** | Addresses Configuration | Interface Tracking | Address Tracking

Interface	VRID	Number of Addresses	Associated IP Address (1)	Associated IP Address (2)	Associated IP Address (3)	Associated IP Address (4)
vlan10	10	1	192.168.10.1	0.0.0.0	0.0.0.0	0.0.0.0
vlan20	20	1	192.168.20.1	0.0.0.0	0.0.0.0	0.0.0.0

[Refresh](#)

Information

- System
- Layer 2
  - Configuration
  - Subnets
  - NAT
  - Static Routes
  - Route Maps
  - DHCP Relay Agent
  - VRRP
    - VRRPv3**
- Layer 3 (IPv4)

## 3.5 Checking the VRRP status

Each VRRP router as the following three states:

- Initializing
- Master
- Backup

The initial state is Initializing, while Master and Backup are chosen by comparing priorities.

In the previous chapters [Configuring the master router](#) and [Configuring the backup router](#), you defined the statuses of master and backup. A switchover is accomplished via VRID tracking.

### Status in the VRRP master router

Figure 3-2

Select	Interface	VRID	Virtual MAC Address	Primary Address	Router State	Master Address	Priority	Advert. Interval	Preempt
<input type="checkbox"/>	vlan10	10	00-00-5e-00-01-0a	192.168.10.2	Master	192.168.10.2	254	10	yes
<input type="checkbox"/>	vlan20	20	00-00-5e-00-01-14	192.168.20.2	Master	192.168.20.2	254	10	yes

### Status in the VRRP backup router

Figure 3-3

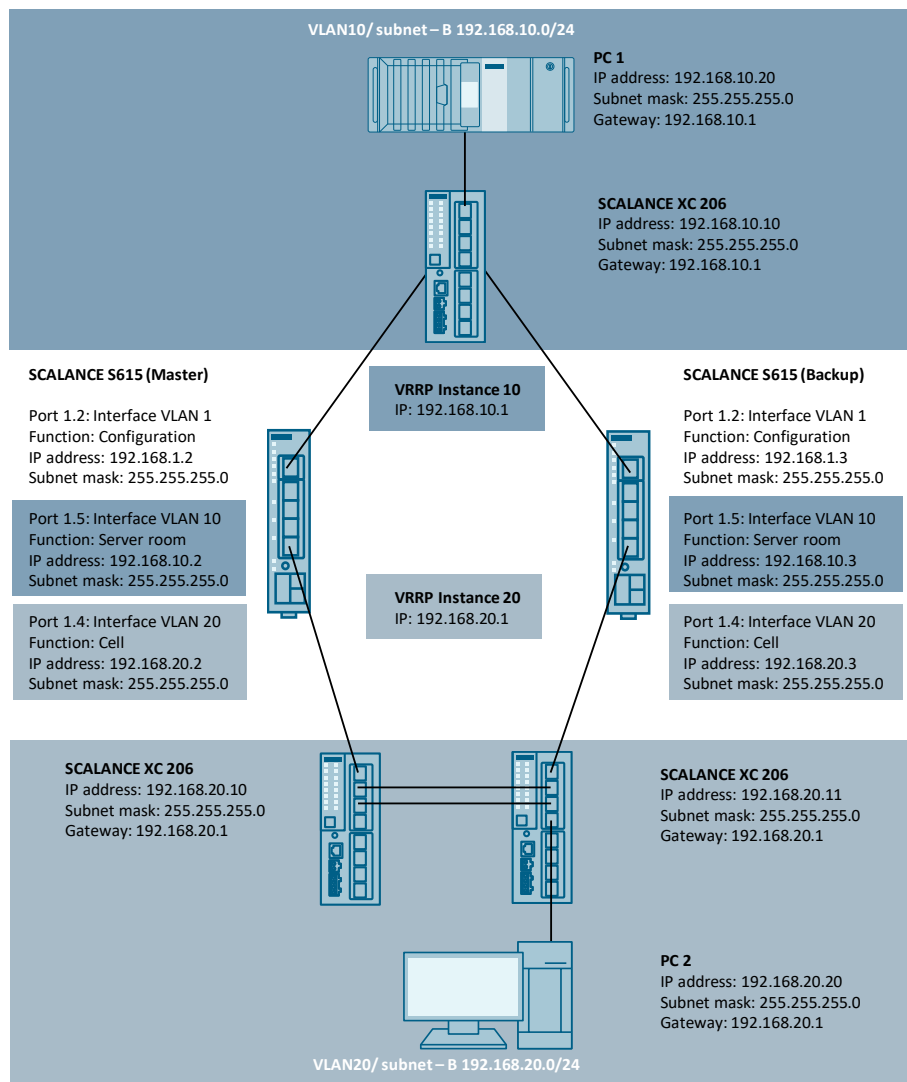
Select	Interface	VRID	Virtual MAC Address	Primary Address	Router State	Master Address	Priority	Advert. Interval	Preempt
<input type="checkbox"/>	vlan10	10	00-00-5e-00-01-0a	192.168.10.3	Backup	192.168.10.2	100	10	yes
<input type="checkbox"/>	vlan20	20	00-00-5e-00-01-14	192.168.20.3	Backup	192.168.20.2	100	10	yes

## 4 Engineering of firewall redundancy with VRRP

The following configuration example uses the SCALANCE S615 firewall routers instead of the SCALANCE XM408-8C routers. The configuration is identical to the SCALANCE XM408-8C. The following example illustrates which additional firewall settings on the master and backup need to be programmed.

### Hardware setup

Figure 4-1



### Overview of VRRP firewall configuration

To configure the VRRP firewall rules, you must perform two steps in the SCALANCE S615.

1. Create an IP protocol in the firewall configuration with IP protocol number and the protocol names. VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address. The IANA has assigned the IP protocol number 112 for VRRP.
2. Create 2 IP rules for VRRP communication. VRRP uses the IP address 224.0.0.18 as a multicast address.

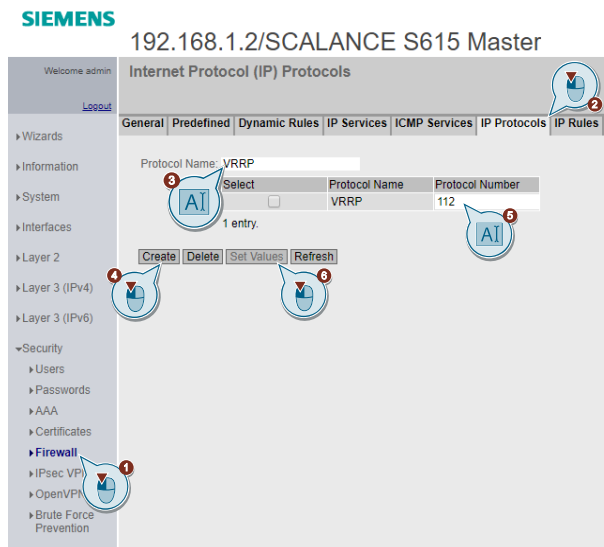
Table 4-1

Action	from	to	Source (range)	Target (range)	Service
Accept	Vlan 10	Device	192.168.10.1 or .2	224.0.0.18/32	VRRP
Accept	Vlan 20	Device	192.168.20.1 or .2	224.0.0.18/32	VRRP

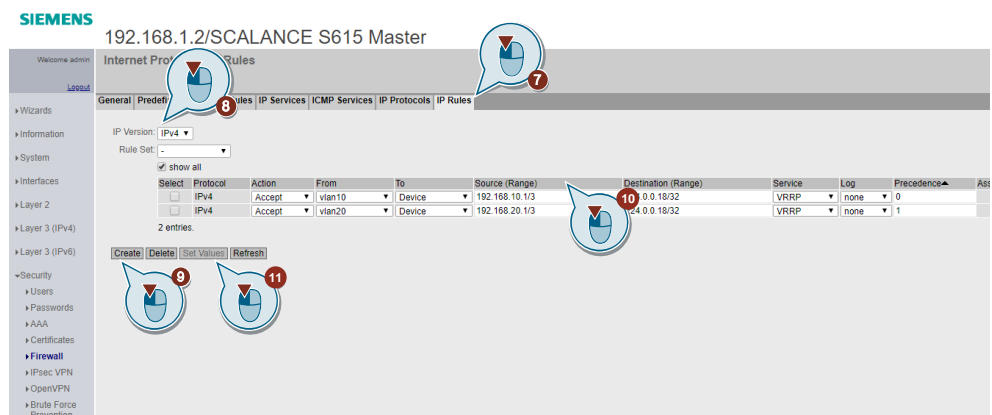
The detailed configuration in the VRRP master and VRRP backup will be covered in the following chapters.

## 4.1 Configuring the master router

1. In the Web Based Management for the SCALANCE S615 master router, navigate to the menu "Security > Firewall".
2. Click the "IP Protocols" tab.
3. Call the "Protocol Name" VRRP.
4. Click on the "Create" button.
5. Assign the value 112 as the "Protocol Number".
6. Click the "Set Values" button.



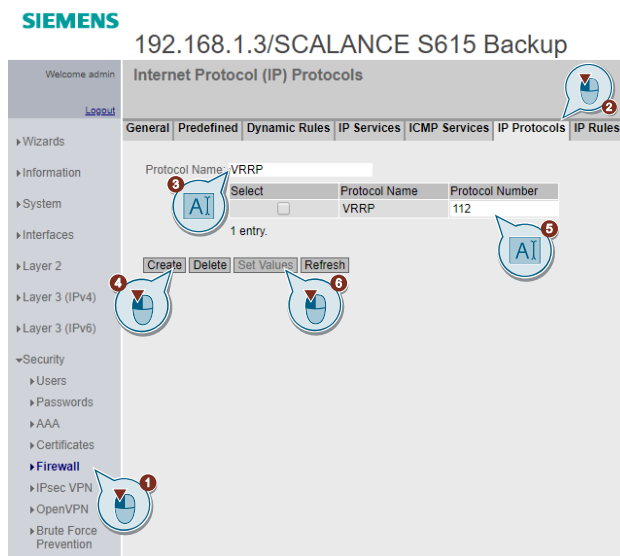
7. Switch to the "IP Rules" tab.
8. Select "IPv4" from the "IP Version" dropdown menu.
9. Click on the "Create" button.  
You will now see a new IP rule line.
10. Fill out the fields to match the first rule from [Table 4-1](#).
11. Save the rule by clicking the "Set Values" button.



12. Repeat steps 8 to 11 with the second rule from [Table 4-1](#).
13. Create another IP rule that allows a ping between the PCs.

### 4.2 Configuring the backup router

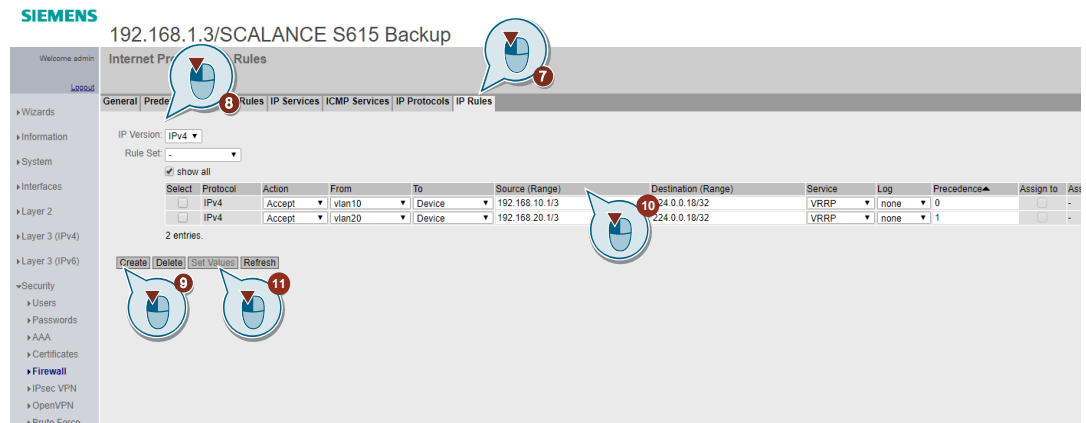
1. In the Web Based Management for the SCALANCE S615 backup router, navigate to the menu "Security > Firewall".
2. Click the "IP Protocols" tab.
3. Call the "Protocol Name" VRRP.
4. Click on the "Create" button.
5. Assign the value 112 as the "Protocol Number".
6. Click the "Set Values" button.



7. Switch to the "IP Rules" tab.
8. Select "IPv4" from the "IP Version" dropdown menu.
9. Click on the "Create" button.  
You will now see a new IP rule line.
10. Fill out the fields to match the first rule from [Table 4-1](#).
11. Save the rule by clicking the "Set Values" button.



## 4 Engineering of firewall redundancy with VRRP



12. Repeat steps 8 to 11 with the second rule from [Table 4-1](#).
13. Create another IP rule that allows a ping between the PCs.

## 5 Testing the VRRP scenario

The Command Prompt (cmd) has the commands *ping* and *tracert* for testing the availability between PC1 and PC2. Both of these commands are used to verify the availability of the network node. If errors occur between sender and receiver, the cause may be firewalls, errors along the route, or that the address was not used.

### 5.1 Error scenarios

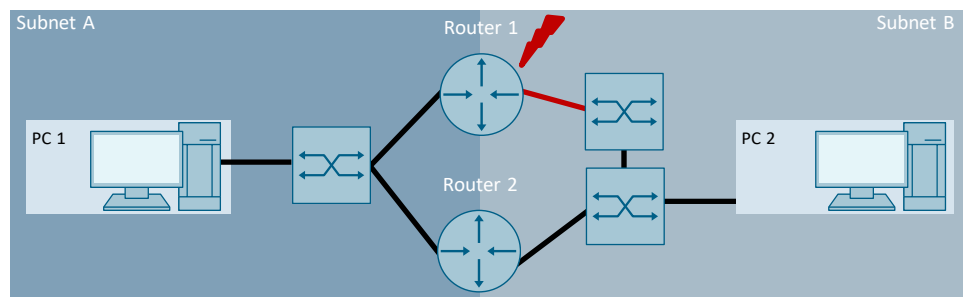
#### Router failure

A router failure is simulated by disconnecting the router from its power supply.

#### Connection failure

The following diagnostic shows how the commands *ping* and *tracert* behave when a network cable on the master router is pulled out.

Figure 5-1



#### Switchover scenario with ping command

*Ping* sends ICMP packet echoes over the network to the specified IP address and waits for an answer in the form of an Echo reply. In the Command Prompt, the user can see how long the data transfer took and whether the availability of the node was ensured.

The command "*ping -t IP address of the network node*" runs a continuous ping which should show the switchover from backup to master.

#### Procedure:

1. Press the "[Windows]" + "R" key combination.
2. Enter "cmd" in the window that appears. Click "OK".
3. Enter the command "*ping -t 192.168.10.20*" to ping PC2.
4. During the continuous ping, pull a network cable on the master router.

```

C:\Users\z003e2rb>ping -t 192.168.10.20

Pinging 192.168.10.20 with 32 bytes of data:
Reply from 192.168.10.20: bytes=32 time=7ms TTL=254
Reply from 192.168.10.20: bytes=32 time<1ms TTL=254
Reply from 192.168.10.20: bytes=32 time=1ms TTL=254
Reply from 192.168.10.20: bytes=32 time<1ms TTL=254
Request timed out.
Reply from 192.168.10.20: bytes=32 time<1ms TTL=254
Reply from 192.168.10.20: bytes=32 time=1ms TTL=254
Reply from 192.168.10.20: bytes=32 time<1ms TTL=254

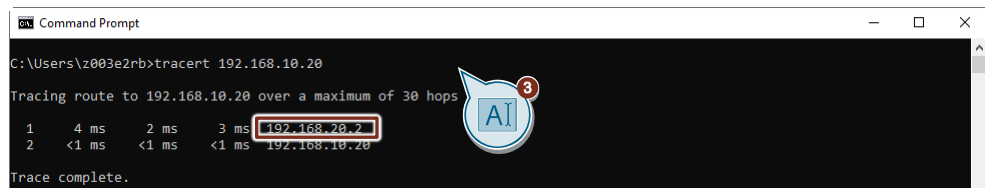
Ping statistics for 192.168.10.20:
    Packets: Sent = 8, Received = 7, Lost = 1 (12% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms
  
```

### Switchover scenario with tracert

Using the command "*tracert IP address of the network node*" it is possible to trace the route of a packet in the network. To do this, the command sends multiple ICMP echo request commands to the target address. The output shows the IP address of each intermediate node and the respective times.

#### Procedure:

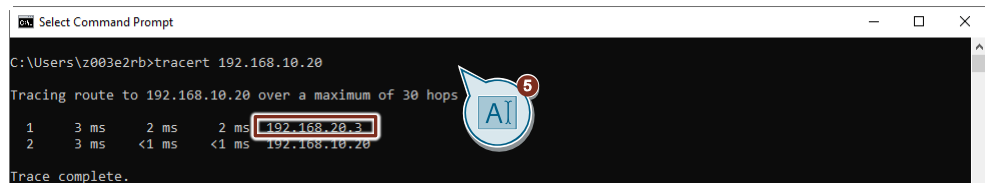
1. Press the "[Windows]" + "R" key combination.
2. Enter "cmd" in the window that appears. Click "OK".
3. Enter the command "*tracert 192.168.10.20*" to trace the route in the network.



```
Command Prompt
C:\Users\z003e2rb>tracert 192.168.10.20
Tracing route to 192.168.10.20 over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  192.168.10.1
  1  4 ms  2 ms  3 ms  192.168.20.2
  2  <1 ms <1 ms <1 ms  192.168.10.20
Trace complete.
```

In the output from this command, you can see that the target address traces over the master router (IP address: 192.168.20.2).

4. Pull a network cable on the master router.
5. Enter the command "*tracert 192.168.10.20*" again to ping PC2.



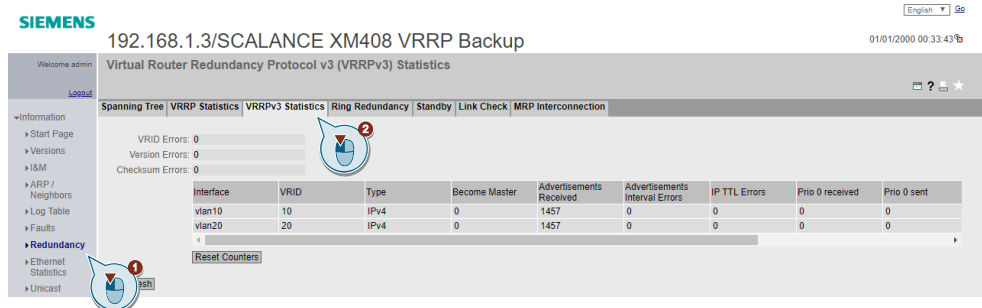
```
Select Command Prompt
C:\Users\z003e2rb>tracert 192.168.10.20
Tracing route to 192.168.10.20 over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  192.168.10.1
  1  3 ms  2 ms  2 ms  192.168.20.3
  2  3 ms  <1 ms <1 ms  192.168.10.20
Trace complete.
```

You can see in the output from this command that the target address now traces over the backup router (IP address: 192.168.20.3).

## 5.2 Diagnostics options

You can diagnose errors in the WBM under "Information > Redundancy > VRRPv3 Statistics".

Figure 5-2



The following errors will be displayed:

- VRID error**  
 Displays how many VRRPv3 packets were received which contain an unsupported VRID.
- Version error**  
 Displays how many VRRPv3 packets were received which contain an invalid version number.
- Checksum error**  
 Displays how many VRRPv3 packets were received which contain an invalid checksum.
- Advertisement interval error**  
 Displays how many faulty VRRPv3 packets were received whose interval does not match the locally set value.
- IP TTL error**  
 Displays how many faulty VRRPv3 packets were received whose TTL (Time to live) value in the IP header is not correct.
- Invalid type**  
 Displays how many faulty VRRPv3 packets were received whose value in the "Type" field of the IP header is invalid.
- Address list error**  
 Displays how many faulty VRRPv3 packets were received whose address list does not match the local configuration list.
- Telegram length error**  
 Displays how many faulty VRRPv3 packets were received whose length is not correct.

## 5.3 Error profiles

### Error in the configuration of the advertisement interval

Most of the time, these errors occur when the master router and backup router do not have the same configuration. An example of this is when the advertisement intervals are set to different values. If the routers receive different advertisement intervals, then the packets will be discarded until the problem is resolved.

### Errors with the VRRP priority

If the master and backup routers initialize in the wrong order, then check the VRRP priorities.

### Both routers are in the master role

If both routers display that they are the master, then this is a serious problem and probably indicates an error in the communication path between the routers. You can check the communication path between the routers by exchanging a *ping* command via the router's WBM.

### Ping between PC and server fails

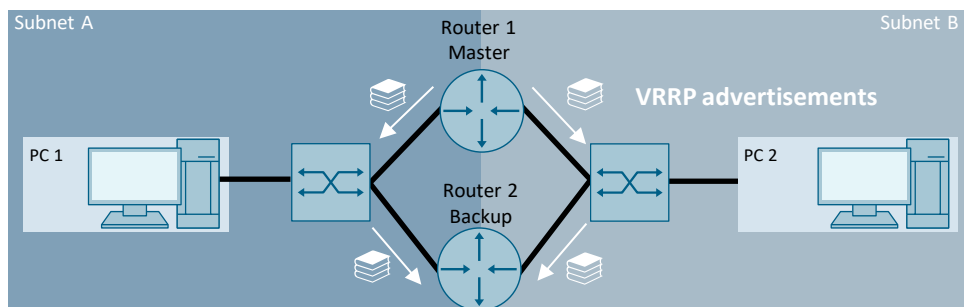
The *ping* to the server fails. Check the wiring of the VLAN configuration and the IP address configuration. Also make sure that the PC is using the right gateway address.

## 6 Useful information

### 6.1 Normal operation

The master router is responsible for the routing and cyclically sends VRRP advertisements to all its IP interfaces for which VRRP is enabled. In concrete terms, this means that sends an advertisement cyclically in both subnets. The backup router is not active here and listens to the VRRP advertisements of the master. As long as these are received, the backup remains in its role. The master router also responds to ARP requests.

Figure 6-1



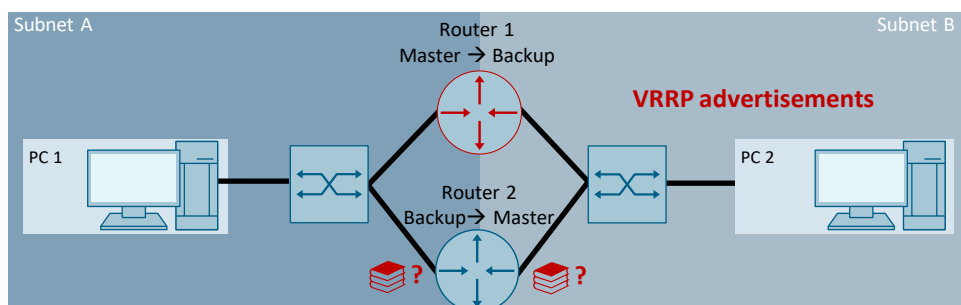
### 6.2 Failure of a device or a connection

A distinction should be drawn between a device failing and a connection failing.

#### 6.2.1 Router failure

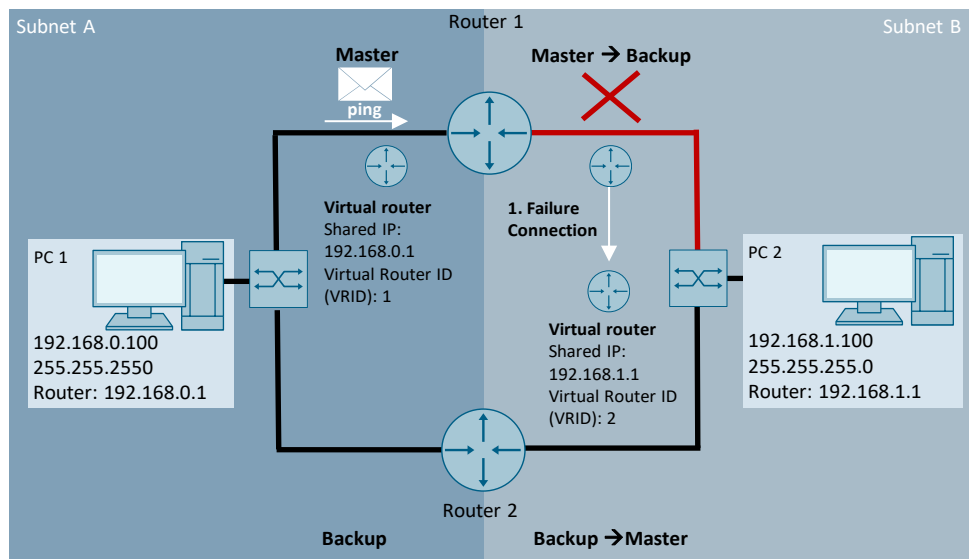
If the VRRP advertisements do not come, the backup devices interpret this as a failure of the master router or of the connection. The backup device now actively takes over the routing in this subnet until the VRRP advertisements can be received from the master router again.

Figure 6-2



## 6.2.2 Failure of a connection cable

Figure 6-3



If only one interface of the active master fails in the example shown above, then the backup router assumes the role of master only for this interface. If nothing else is done, IP telegrams from PC1 would no longer be routed to PC2.

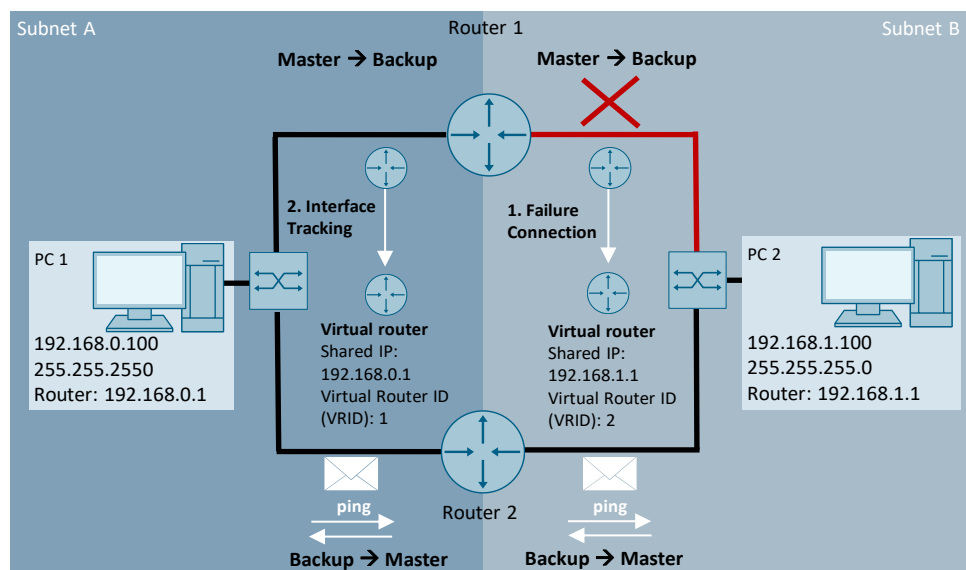
## 6.3 Tracking process

Using the tracking process, you can monitor the interfaces and thus modify the VRRP priority. The tracking methods available to you are interface tracking, VRID tracking and address monitoring.

### 6.3.1 Interface tracking

With interface tracking, the VRRP priorities of the router can be modified so that the switchover happens synchronously. In this case, a failure of an interface will cause the VRRP priority of the remaining VRRP instances to be decremented by a fixed value, thus triggering a switchover.

Figure 6-4



### 6.3.2 VRID tracking

If VRID tracking is enabled, all interfaces of a VRID will be monitored. When the link of an interface changes from "up" to "down", the priority of all VRRP interfaces with the same VRID will be reduced to the value "0". When the link of an interface changes from "down" back to "up", the original priority of the VRRP interface is restored.

### 6.3.3 Address monitoring

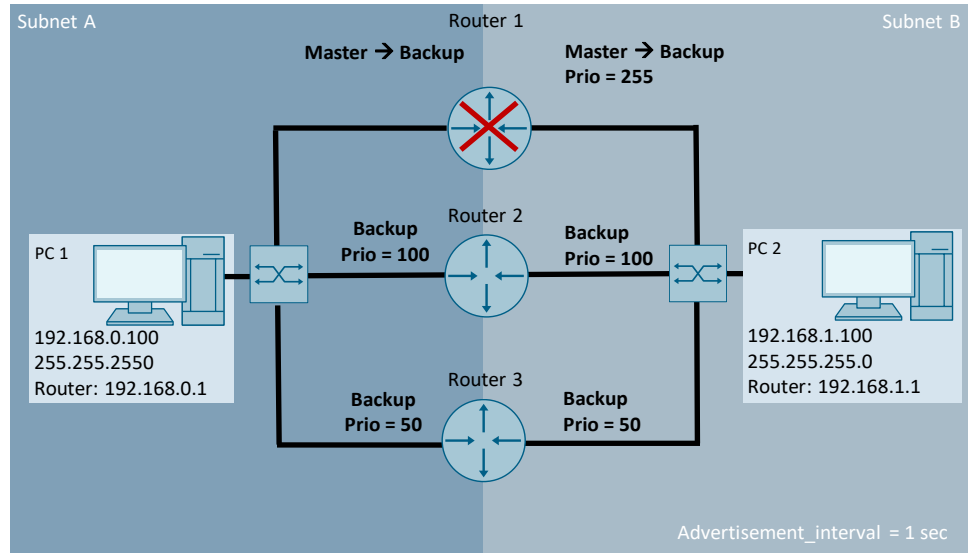
Within the specified time period, the router sends a *ping* request to each of the configured IP addresses. If it does not receive an answer within a specific time period, the VRRP priority of the corresponding interface will be reduced.



## 6.4 Calculating the failure time

In our example, the master router fails. What we need to calculate is the time until the backup router registers the failure of the master router.

Figure 6-5



The Master Down Interval corresponds to 3 times the advertisement interval plus the skew time.

$$\text{Master Down Interval} = 3 * \text{Advertisement Interval} + \text{Skew Time}$$

where the skew time is equal to 256 minus the priority of the backup router divided by 256.

$$\text{Skew Time} = \frac{(256 - \text{Priority})}{256}$$

If the master router fails, then the backup routers have received no advertisement from it within the time period  $3 \times \text{AdvIn}$ . Each backup router now calculates its Master Down Interval as follows:

Router 2

$$\text{Skew Time} = \frac{256 - 100}{256} = \frac{156}{256s}$$

$$\text{Master Down Interval} = (3 * 1) + \frac{156}{256} = 3 + \frac{156}{256} = 3.6093 \text{ s}$$

Router 3

$$\text{Skew Time} = \frac{256 - 50}{256} = \frac{206}{256s}$$

$$\text{Master Down Interval} = (3 * 1) + \frac{206}{256} = 3 + \frac{206}{256} = 3.8046 \text{ s}$$

In our example, router 2 registers the failure of the master router before the others thanks to its higher priority and resulting shorter skew time. It changes to the master state and sends advertisements. The backup routers recognize that it has now taken over the role of the master router.

## 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](https://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:

[siemens.com/SupportRequest](https://siemens.com/SupportRequest)

#### SITRAIN – Digital Industry Academy

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:

[siemens.com/sitrain](https://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](https://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](https://support.industry.siemens.com/cs/ww/en/sc/2067)

## 7.2 Industry Mall



The Siemens Industry Mall is the platform on which the entire Siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:

[mall.industry.siemens.com](https://mall.industry.siemens.com)

## 7.3 Links and literature

Table 7-1

No.	Topic
\1\	Siemens Industry Online Support <a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a>
\2\	Link to this entry page of this application example <a href="https://support.industry.siemens.com/cs/ww/en/view/109798556">https://support.industry.siemens.com/cs/ww/en/view/109798556</a>
\3\	SINEC PNI <a href="https://support.industry.siemens.com/cs/ww/en/view/109776941">https://support.industry.siemens.com/cs/ww/en/view/109776941</a>
\4\	PRONETA <a href="https://support.industry.siemens.com/cs/ww/en/view/67460624">https://support.industry.siemens.com/cs/ww/en/view/67460624</a>
\5\	SCALANCE XM-400/XR-500 manual <a href="https://support.industry.siemens.com/cs/at/en/view/109780065">https://support.industry.siemens.com/cs/at/en/view/109780065</a>

## 7.4 Change documentation

Table 7-2

Version	Date	Modifications
V1.0	09/2021	First version