



SIEMENS

Configuring the Open Shortest Path First (OSPF) routing protocol

SCALANCE XM-400, SCALANCE XR-500,
SCALANCE SC

<https://support.industry.siemens.com/cs/ww/en/view/109808195>

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 under

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

Table of contents

Legal information	2
1 Introduction	4
1.1 Overview	4
1.2 Principle of operation	5
1.3 Components used.....	6
2 Engineering	7
2.1 Hardware configuration	7
2.2 Commissioning the PC	10
2.3 Commissioning the SCALANCE.....	14
2.4 Configuring the OSPF router	20
2.5 OSPF configuration	21
2.5.1 The routing table.....	29
3 Testing the OSPF scenario	31
3.1 Error scenarios	31
4 Useful information	34
4.1 IP routers	34
4.1.1 Function and tasks	34
4.2 Routing mechanisms	35
4.2.1 Static routing.....	35
4.2.2 Dynamic routing.....	35
4.3 OSPF hierarchy using Single Area or Multiarea.....	38
4.3.1 Single-area OSPF (backbone area)	39
4.3.2 Multi-area OSPF	39
4.3.3 Types of routers.....	40
4.3.4 Special area types	41
4.3.5 Virtual links	42
4.4 Metrics	43
4.4.1 Open Shortest Path First algorithm	44
4.4.2 Administrative distance.....	45
4.5 OSPF routers.....	46
4.5.1 Link State Advertisement (LSA)	47
4.5.1.1 LSA types	48
4.5.1.2 Example: Update for a link change.....	50
4.6 OSPF sequence	52
4.6.1.1 Start of neighbor adjacency and selection of the Designated Router	52
4.6.1.2 One-time database synchronization	59
4.6.1.3 End of synchronization	61
4.6.1.4 Database updates always occur with acknowledgment.	62
4.6.1.5 Routing table calculation	63
5 Appendix.....	64
5.1 Service and support.....	64
5.2 Industry Mall	65
5.3 Links and literature	65
5.4 Change documentation	65

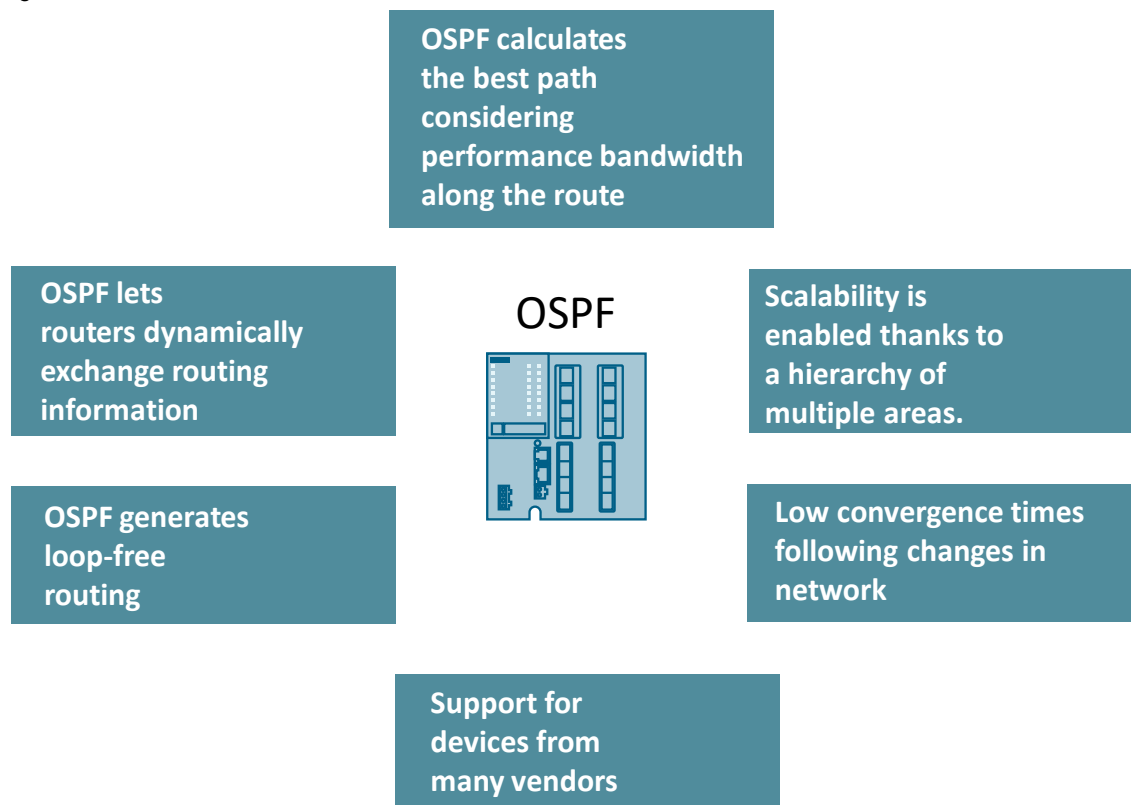
1 Introduction

The Open Shortest Path First (OSPF) routing protocol is an interior routing protocol used in autonomous systems for dynamic routing. It was developed by the Internet Engineering Task Force (IETF) for use in IP-based networks. OSPF is an open standard ([RFC 2328](#), [RFC 5340](#)), and consequently many routers from a wide number of vendors support the protocol. OSPF is a routing protocol designed for large, routed networks. This makes it possible to link entire sections of an enterprise with one another. The protocol was specially designed for networks whose older routing protocols, such as the Routing Information Protocol (RIP), were nearing the limits of their capacity.

1.1 Overview

Compared to static routing or simple routing protocols like RIP, OSPF offers numerous advantages, as well as some disadvantages. Some of the advantages are:

Figure 1-1



The disadvantages include:

- a complex protocol
- deeper expertise required to implement
- more powerful routers are necessary (routers require a certain basic level of power and intelligence to support OSPF)

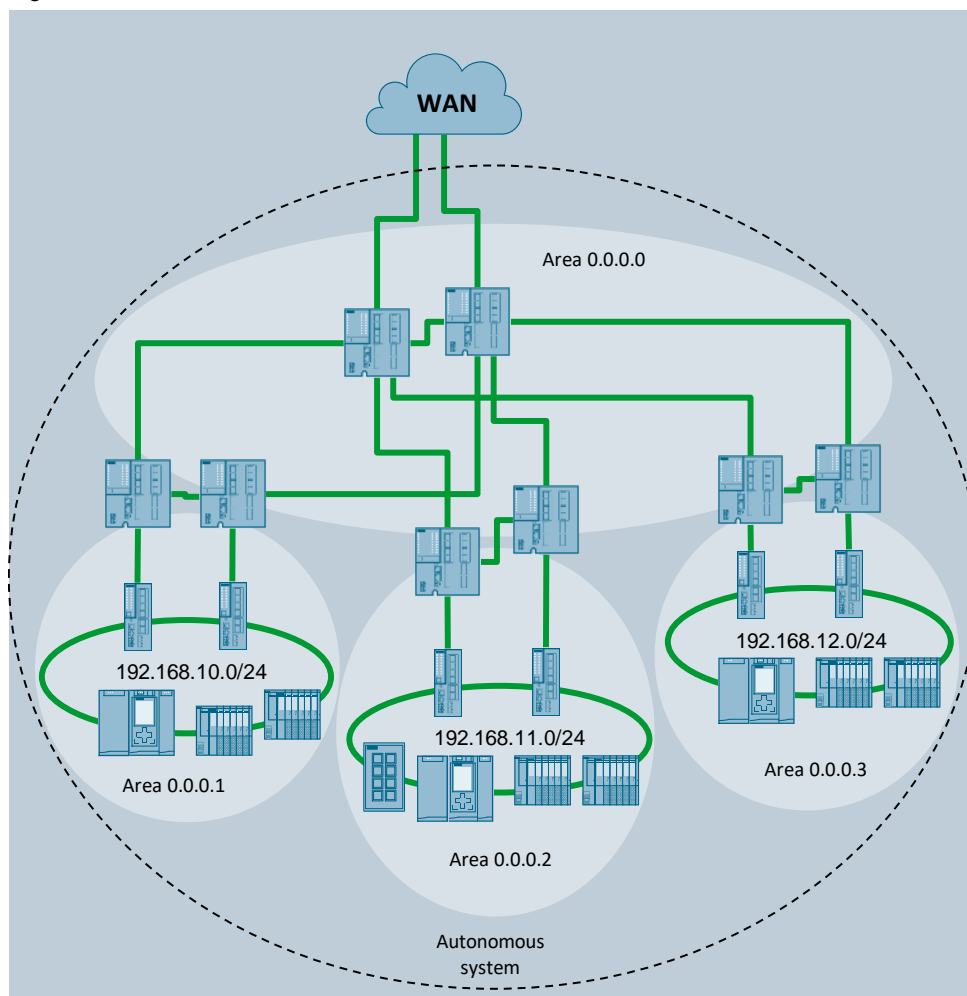
Problem

Thus far, you have been routing your data packets through the network statically (article ID: [109755344](#)), which increases the administrative overhead as the number of local subnets grows. Now you would like to use a dynamic routing protocol at your location to guarantee data exchange between various subnets.

Solution

OSPF lets routers dynamically exchange routing information. The hierarchical concept composed of multiple areas ensures scalability. OSPF-capable routers can communicate with one another in an environment composed of networks from extremely diverse vendors. For example, if you need to connect the OT network with the routers of the IT network, the OSPF protocol can be utilized to ensure the exchange of routing information.

Figure 1-2



1.2 Principle of operation

Open Shortest Path First (OSPF) finds the best path based on the link costs, which by default are calculated using the interface bandwidth and a reference value. Here, each router has a map of the network which it stores in a Link State Database (OSPF LSDB). Complete paths through a network are calculated with either the SPF (shortest path first) or Dijkstra algorithm. An area concept minimizes the router load and SPF calculations in an area. If changes occur in the network, partial information (updates) on them are sent. The hierarchical structure requires a central core area (backbone area) that the other areas can use as a transit area.

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 engineering. 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
- RIP / RIPv2

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 already integrated in the device.
- The layer 3 function (routing) can be activated by 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 SC

As of firmware V3.0, the OSPF routing protocol is available in the SCALANCE SC devices SC622-2C, SC626-2C, SC632-2C, SC636-2C, SC642-2C and SC646-2C.

The following hardware and software components were used to create this application example:

Table 1-1

Components	Quantity	Item number	Note
SCALANCE XM408-8C	4x	6GK5 408-8GR00-2AM2	
SIMATIC Field PG M6	4x	6ES7718-.....	

The components listed here can be obtained from the [Siemens Industry Mall](#).

This application example consists of the following components:

Table 1-2

Components	File name	Note
This document	109808195_OSPF_DOC_V1_0_en	

2 Engineering

2.1 Hardware configuration

The aim of the following application example is to establish communication between 4 PCs. The following redundant network contains multiple paths to each network. Diagnostics need to be checked with a ping command from PC1 to PC4.

The following Figure shows you the physical network diagram.

Figure 2-1

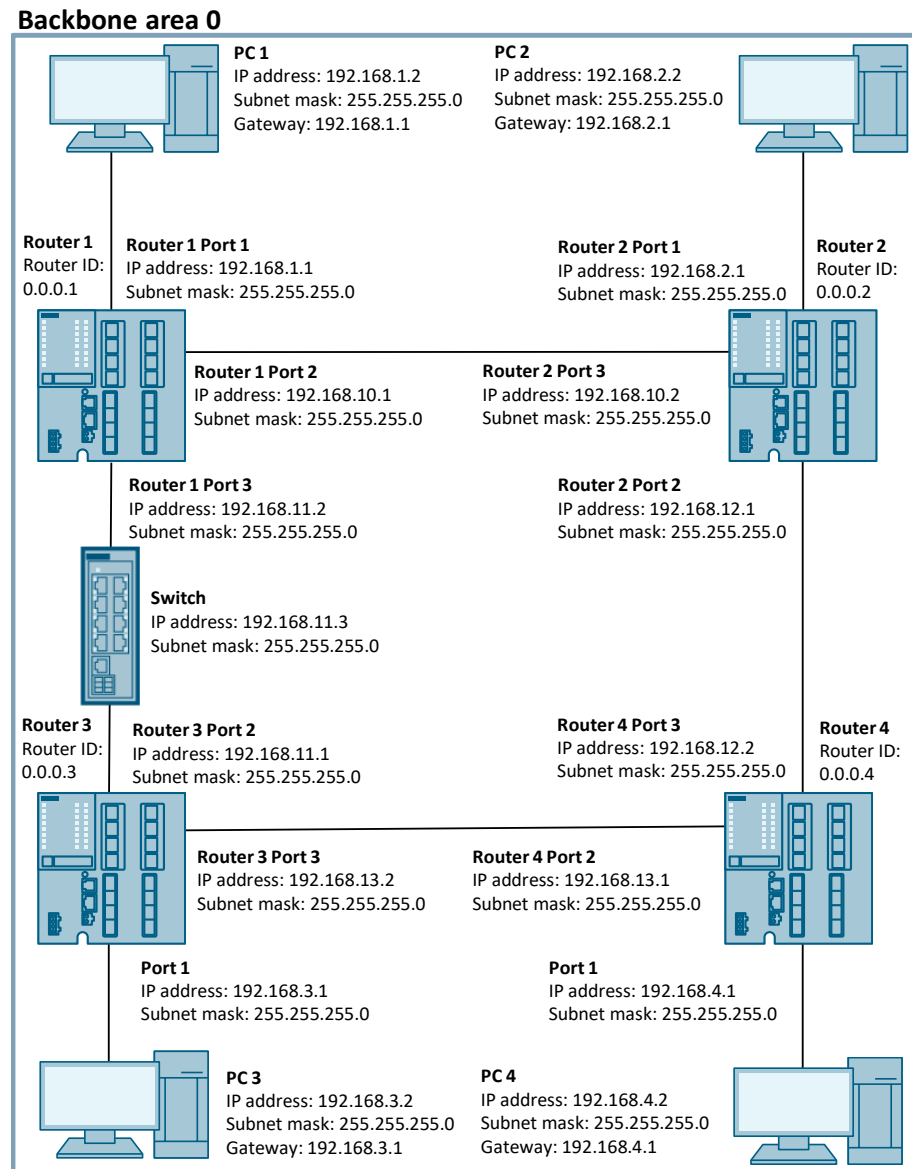
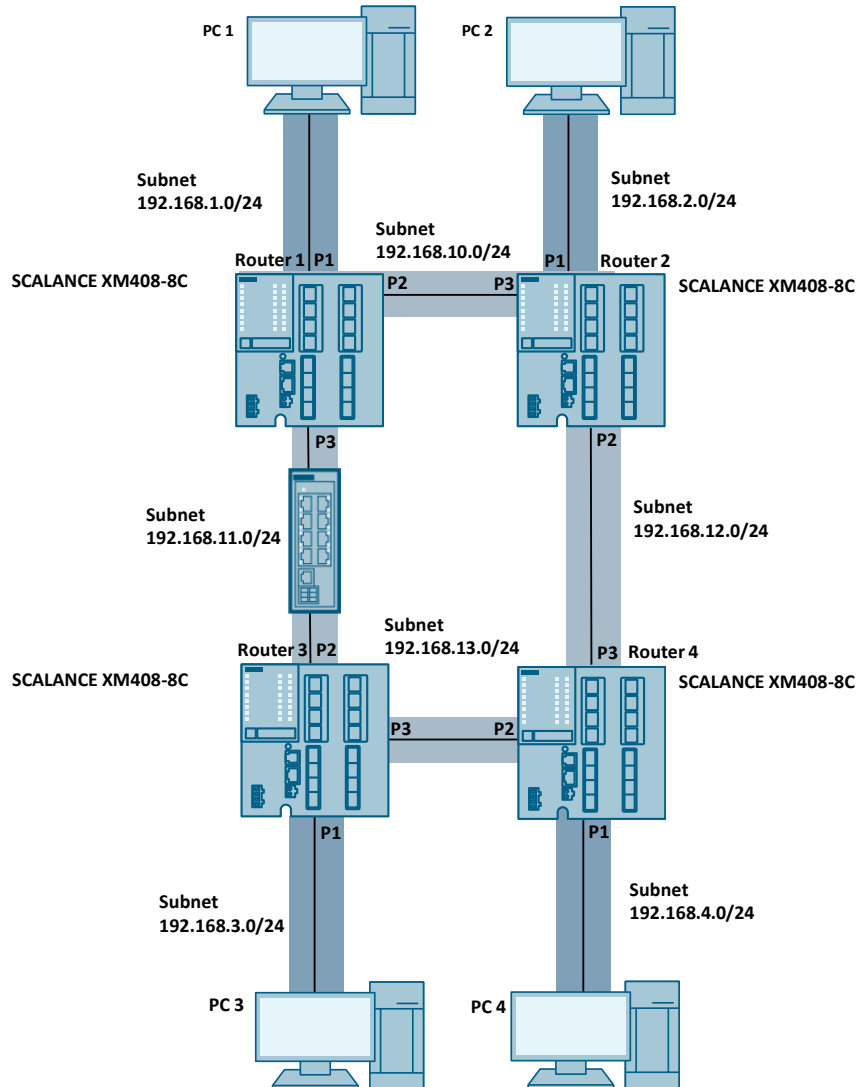


Table 2-1

Device	Interface	IP address	Subnet mask	Default gateway
Router 1	Port 1	192.168.1.1	255.255.255.0	
	Port 2	192.168.10.1	255.255.255.0	
	Port 3	192.168.11.2	255.255.255.0	
Router 2	Port 1	192.168.2.1	255.255.255.0	
	Port 2	192.168.12.1	255.255.255.0	
	Port 3	192.168.10.2	255.255.255.0	
Router 3	Port 1	192.168.3.1	255.255.255.0	
	Port 2	192.168.11.1	255.255.255.0	
	Port 3	192.168.13.2	255.255.255.0	
Router 4	Port 1	192.168.4.1	255.255.255.0	
	Port 2	192.168.13.1	255.255.255.0	
	Port 3	192.168.12.2	255.255.255.0	
Switch	Port 1/2	192.168.11.3	255.255.255.0	
PC1	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC2	NIC	192.168.2.2	255.255.255.0	192.168.2.1
PC3	NIC	192.168.3.2	255.255.255.0	192.168.3.1
PC4	NIC	192.168.4.2	255.255.255.0	192.168.4.1

The four subnets 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 and 192.168.4.0/24 connect the routers with the individual PCs. Four other subnets 192.168.10.0/24, 192.168.11.0/24, 192.168.12.0/24 and 192.168.13.0/24 connect the routers' interfaces with one another.

Figure 2-2



2.2 Commissioning the PC

Description

This application example uses 4 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 which IP addresses and which default gateways the PCs are configured with.

Table 2-2

PC	IP address	Subnet mask	Gateway
PC 1	192.168.1.2	255.255.255.0	192.168.1.1
PC 2	192.168.2.2	255.255.255.0	192.168.2.1
PC 3	192.168.3.2	255.255.255.0	192.168.3.1
PC 4	192.168.4.2	255.255.255.0	192.168.4.1

Enter default router

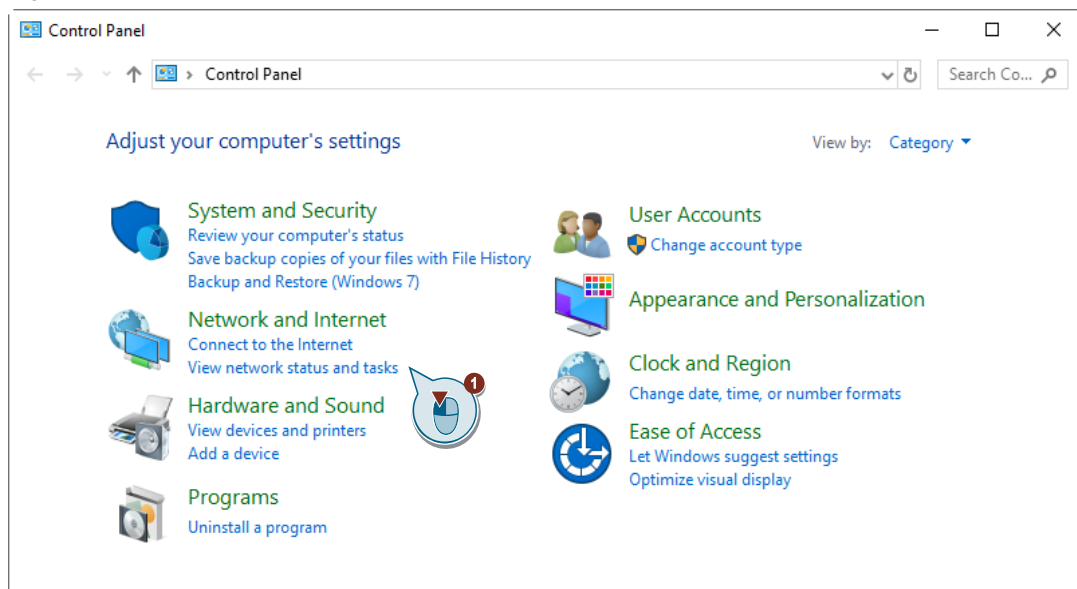
The following instructions show you how to enter a default router on the PC in Windows 10 using PC1 as an example.

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".

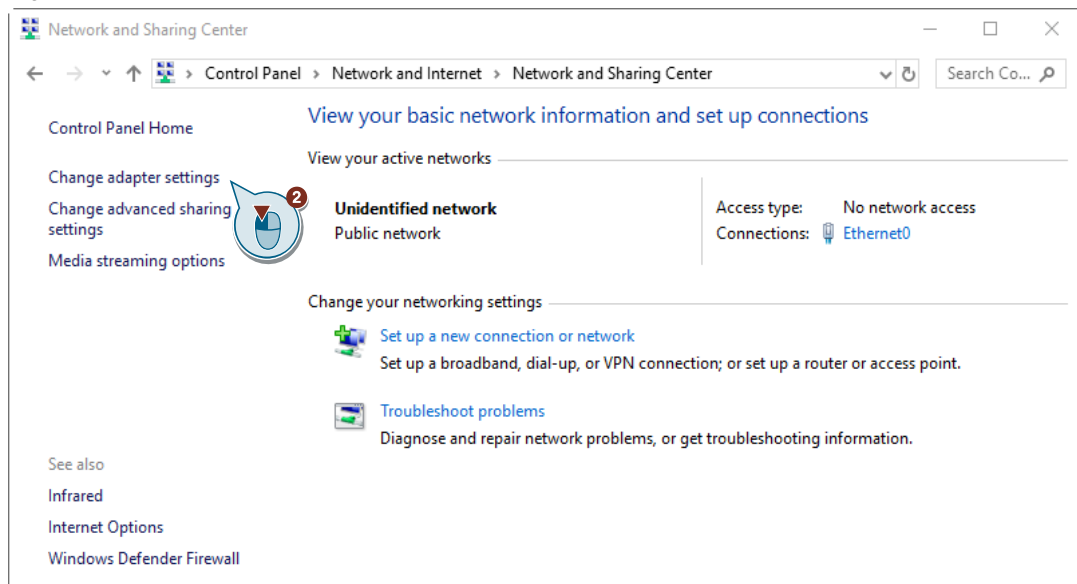
Figure 2-3



The "Network and Sharing Center" window opens.

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

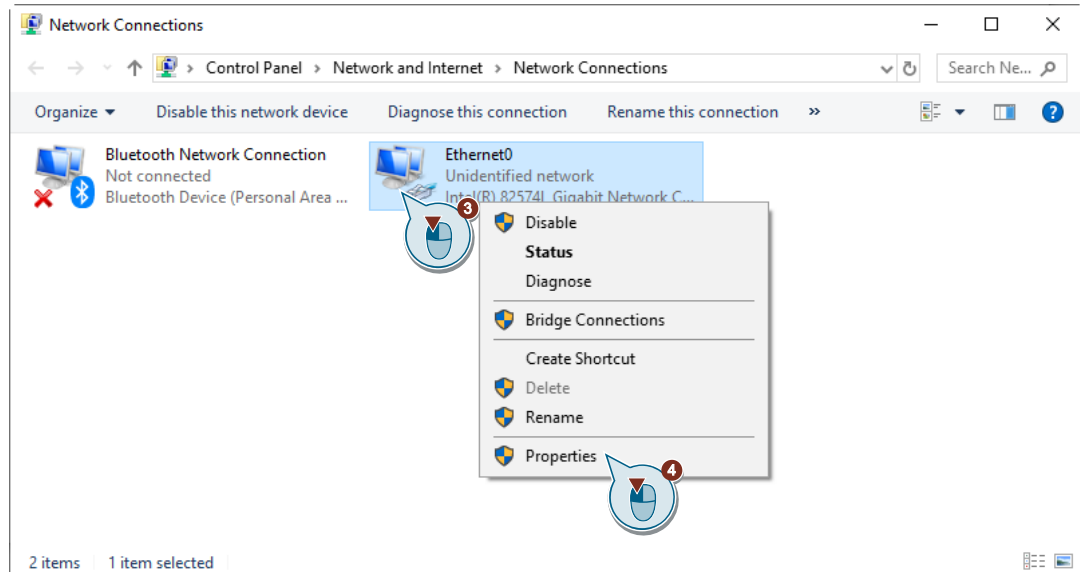
Figure 2-4



The "Network Connections" window will open.

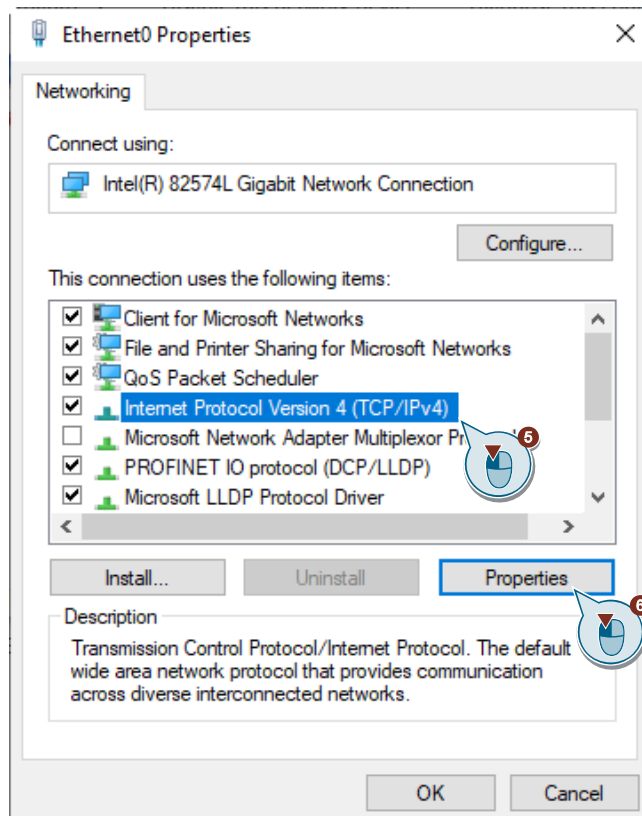
3. You will see all available network adapters / network cards. With the left mouse button, select the entry you are using from the list.

Figure 2-5



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

Figure 2-6

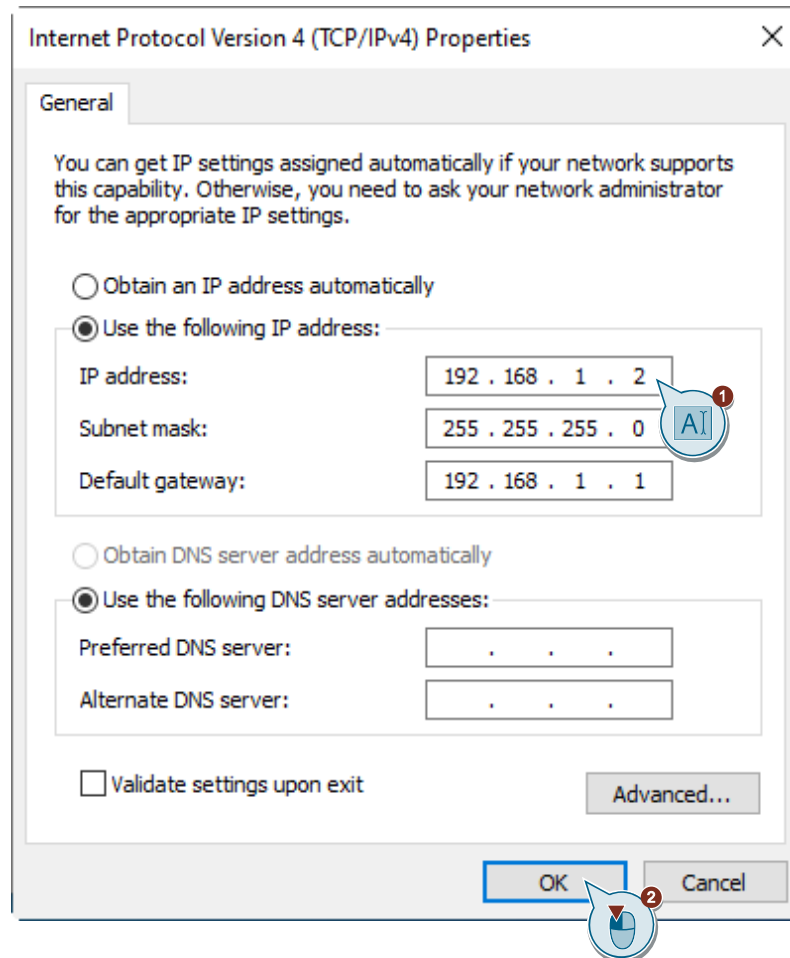


6. Then click the "Properties" button.

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".

Figure 2-7



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 default gateway in all the PCs. The PCs need these settings to communicate with remote subnets.

2.3 Commissioning the SCALANCE

Some preparation is necessary before you can configure the SCALANCE XM-400 devices with the OSPF protocol.

You must prepare the following requirements 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

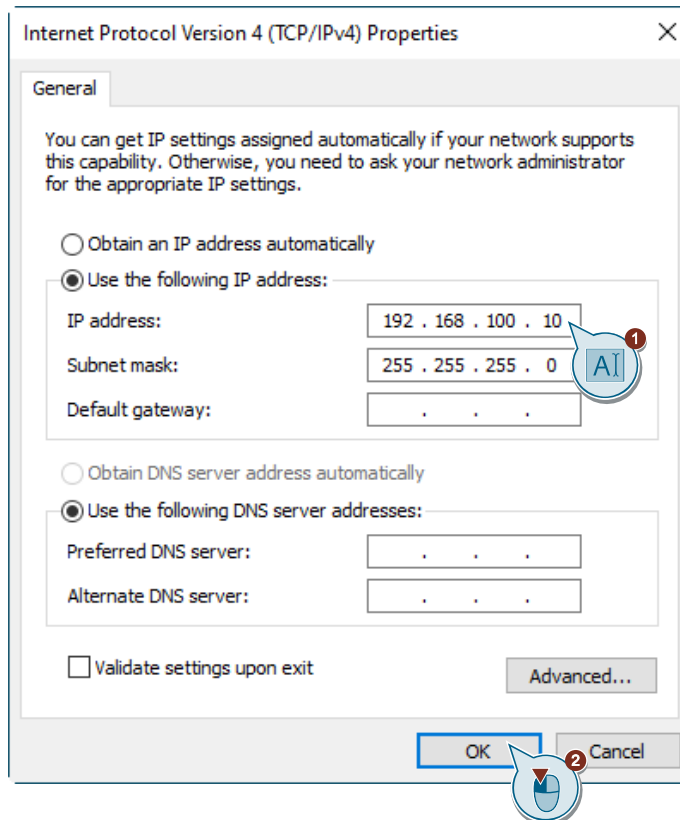
The engineering PC is used to configure the SCALANCE devices using web-based management.

Assign the engineering PC the following IP addresses in order to commission the SCALANCE devices in sequence:

Table 2-3

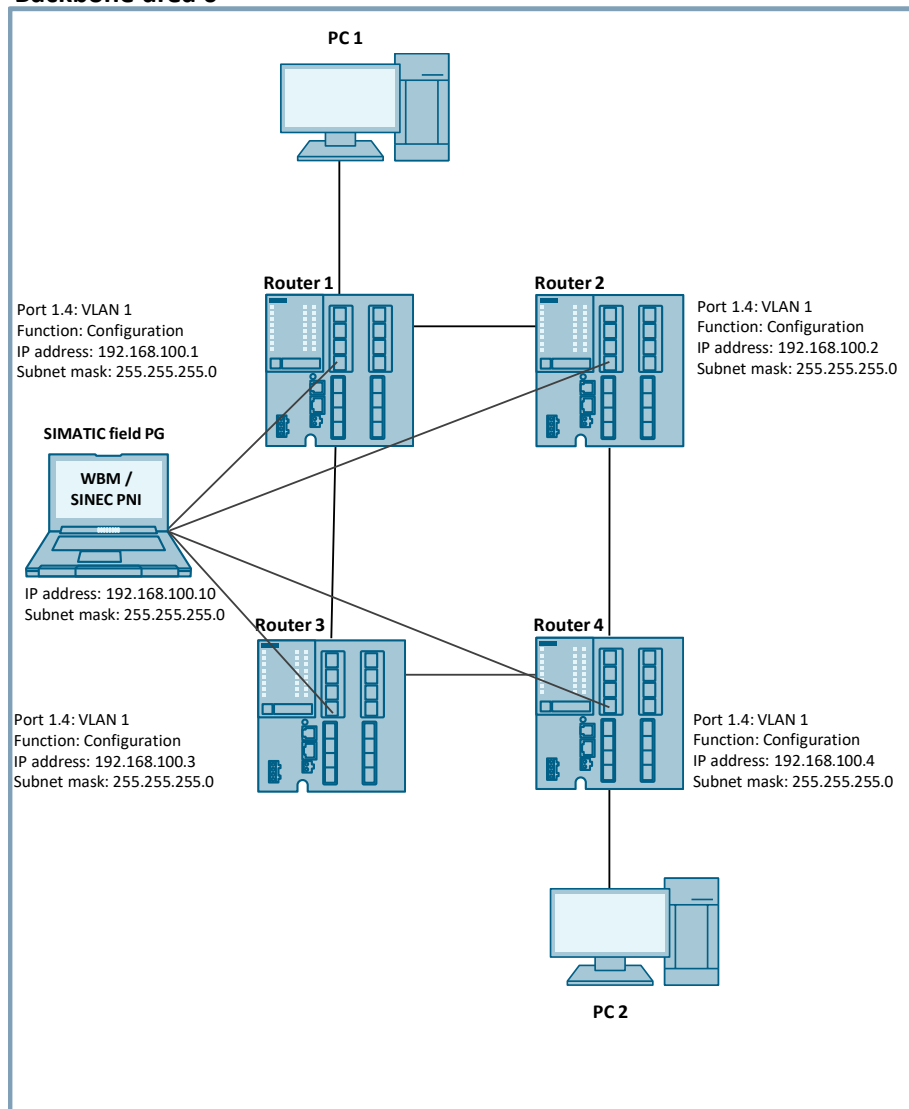
PC	IP address	Subnet mask
Field programming device	192.168.100.10	255.255.255.0

Figure 2-8



To establish a connection with the SCALANCE devices, the engineering PC is connected with port 1.4 of the respective SCALANCE. This is used for the initial configuration of the devices with the field programming device.

Figure 2-9

Backbone area 0**Reset the SCALANCE**

If you are not using brand-new SCALANCE devices, it is recommended to reset the devices to their 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](#).

Assign the IP address

The first assignment of an IP address for the SCALANCE router 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 SCALANCE routers with one of the aforementioned tools:

Table 2-4

Device	IP address	Subnet mask
SCALANCE XM408-8C router 1	192.168.100.1	255.255.255.0
SCALANCE XM408-8C router 2	192.168.100.2	255.255.255.0
SCALANCE XM408-8C router 3	192.168.100.3	255.255.255.0
SCALANCE XM408-8C router 4	192.168.100.4	255.255.255.0

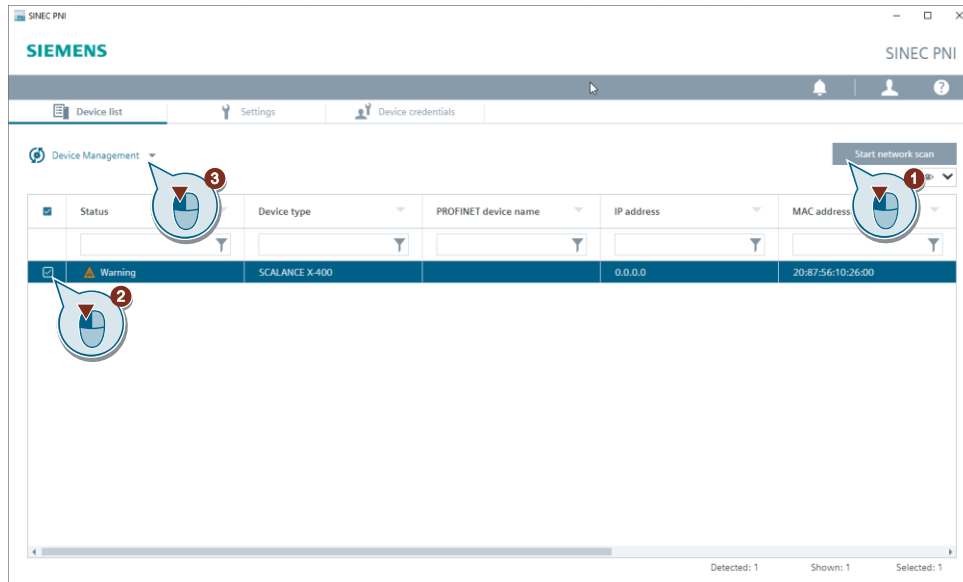
Note

OSPF supports IPv4 and IPv6.

The following figures describe configuration with SINEC PNI.

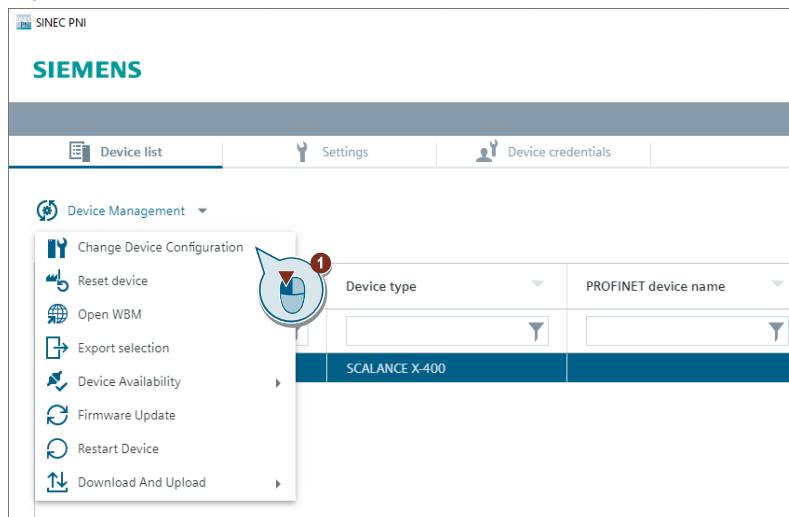
1. Click "Start network scan".
2. Select the device found.
3. Click the "Device Management" button.

Figure 2-10



4. Click "Change Device Configuration".

Figure 2-11



5. Assign an IP address and a subnet mask.

Figure 2-12

The screenshot shows the 'Device configuration' web interface. At the top, there are tabs for 'IP configuration', 'System', 'PROFINET', and 'Device cr >'. The 'IP configuration' tab is active. Below the tabs, there are input fields for 'IP address:' (192.168.100.1), 'Subnet mask:' (255.255.255.0), and a checkbox for 'Use router:' (unchecked) with a value of 0.0.0.0. A blue callout bubble with a red '1' points to the 'Use router:' checkbox. Below these fields, there is a section for 'DHCP:' with a toggle switch (turned off), 'DHCP mode:' (set to 'MAC address'), and 'Client ID:'. At the bottom, there are three buttons: 'Cancel', 'Load', and 'Load All'. A blue callout bubble with a red '2' points to the 'Load' button.

6. Click the "Load" button

Result

The IP address and subnet mask have been assigned.

7. Assign the other OSPF routers (Router 2, Router 3 and Router 4) their corresponding IP addresses and subnet masks.

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.

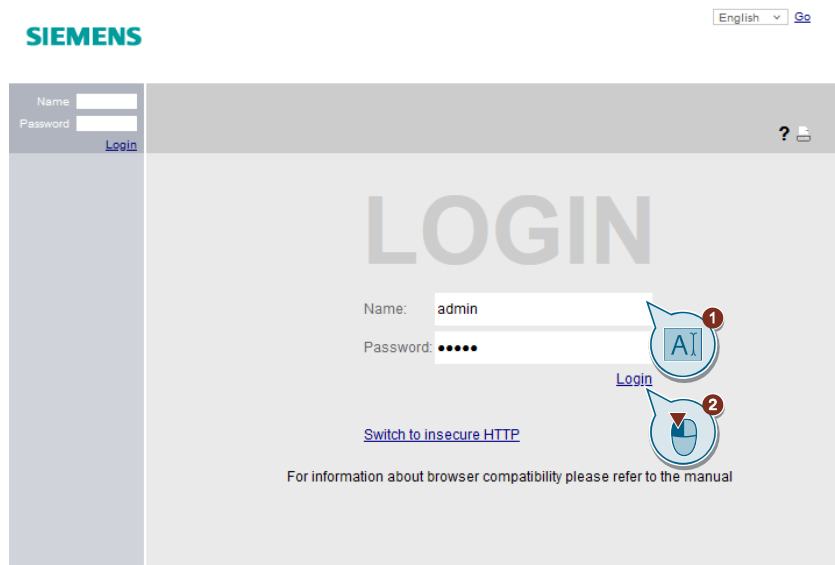
Note

Use the https protocol to establish a secure connection to SCALANCE

Proceed as follows to open Web Based Management:

1. In the address bar of your internet browser, enter the IP address of the SCALANCE, for example the address <https://192.168.100.1>. 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".

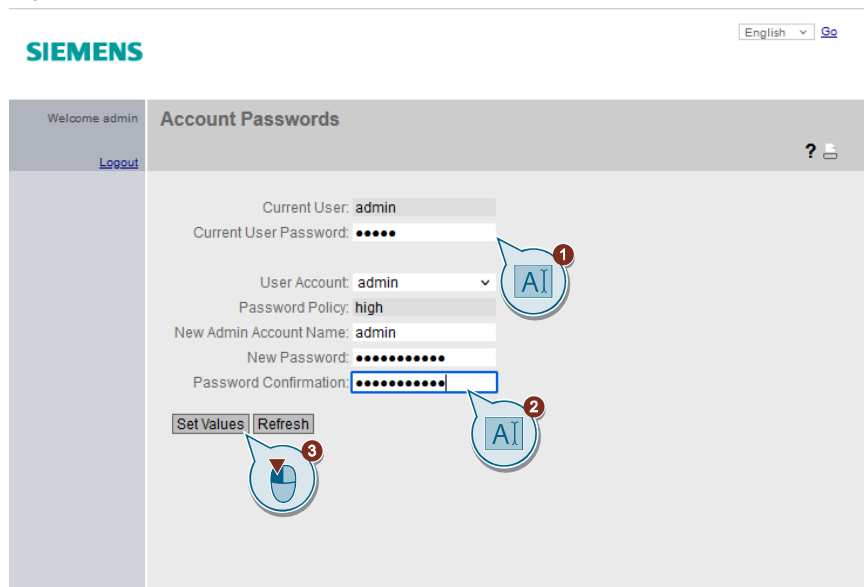
Figure 2-13



The screenshot shows the Siemens login page. At the top left is the Siemens logo. At the top right is a language dropdown set to 'English' and a 'Go' button. On the left side, there is a sidebar with 'Name' and 'Password' input fields and a 'Login' button. The main area has a large 'LOGIN' heading. Below it, there are input fields for 'Name' (containing 'admin') and 'Password' (containing dots). To the right of these fields are two callout boxes: box 1 points to the 'Name' field, and box 2 points to the 'Password' field. Below the password field is a 'Login' button. Further down is a link 'Switch to insecure HTTP' and a note: 'For information about browser compatibility please refer to the manual'.

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.

Figure 2-14



The screenshot shows the 'Account Passwords' page after login. The top left says 'Welcome admin' with a 'Logout' button. The top right has a language dropdown set to 'English' and a 'Go' button. The main area contains a form for password management. It includes fields for 'Current User' (admin), 'Current User Password' (dots), 'User Account' (dropdown menu showing 'admin'), 'Password Policy' (high), 'New Admin Account Name' (admin), 'New Password' (dots), and 'Password Confirmation' (dots). Below these fields are two buttons: 'Set Values' and 'Refresh'. There are three callout boxes: box 1 points to the 'User Account' dropdown, box 2 points to the 'New Password' field, and box 3 points to the 'Set Values' button.

Enter "admin" for the current user password.

5. Select admin as the "User account".
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.

2.4 Configuring the OSPF router

To configure the SCALANCE XM408 as an OSPF router, the following essential parameter assignment steps must be made:

- Activate routing
- Create subnets
- Configure OSPF

The following sections will show you how to configure the SCALANCE via Web Based Management. The following configuration will be shown, taking router 1 as an example. The configuration for the remaining routers 2, 3 and 4 is identical except for the IP address assignment and subnet mask.

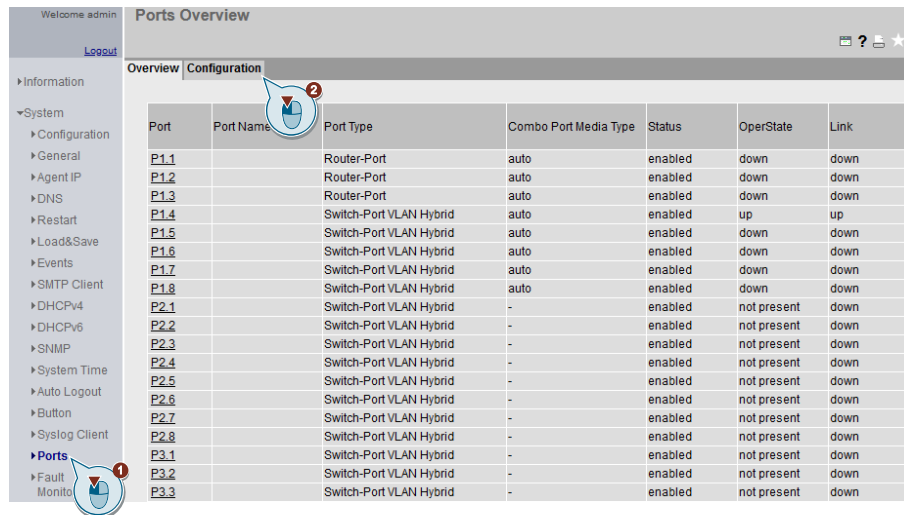
Connect the engineering PC to the SCALANCE router and open Web Based Management.

2.5 OSPF configuration

1. In a network device that operates or exchanges data on multiple OSI layers, for instance switching on layer 2 and routing on layer 3, ports on the device must be designated as switching-capable (switchport) and/or routing-capable (router port). Create three router ports that serve as connections to the adjacent routers and end devices.

Configure the router ports in the menu "System > Port". Click "Configuration".

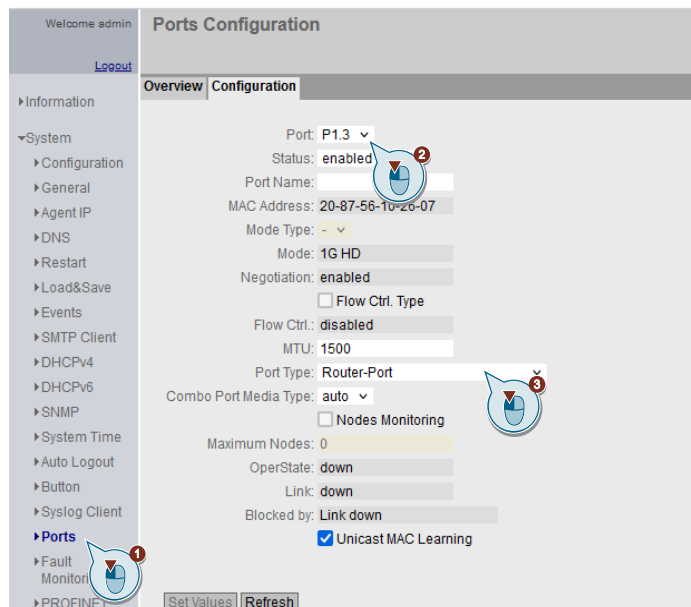
Figure 2-15



Port	Port Name	Port Type	Combo Port Media Type	Status	OperState	Link
P1.1		Router-Port	auto	enabled	down	down
P1.2		Router-Port	auto	enabled	down	down
P1.3		Router-Port	auto	enabled	down	down
P1.4		Switch-Port VLAN Hybrid	auto	enabled	up	up
P1.5		Switch-Port VLAN Hybrid	auto	enabled	down	down
P1.6		Switch-Port VLAN Hybrid	auto	enabled	down	down
P1.7		Switch-Port VLAN Hybrid	auto	enabled	down	down
P1.8		Switch-Port VLAN Hybrid	auto	enabled	down	down
P2.1		Switch-Port VLAN Hybrid	-	enabled	not present	down
P2.2		Switch-Port VLAN Hybrid	-	enabled	not present	down
P2.3		Switch-Port VLAN Hybrid	-	enabled	not present	down
P2.4		Switch-Port VLAN Hybrid	-	enabled	not present	down
P2.5		Switch-Port VLAN Hybrid	-	enabled	not present	down
P2.6		Switch-Port VLAN Hybrid	-	enabled	not present	down
P2.7		Switch-Port VLAN Hybrid	-	enabled	not present	down
P2.8		Switch-Port VLAN Hybrid	-	enabled	not present	down
P3.1		Switch-Port VLAN Hybrid	-	enabled	not present	down
P3.2		Switch-Port VLAN Hybrid	-	enabled	not present	down
P3.3		Switch-Port VLAN Hybrid	-	enabled	not present	down

2. Select "Router Port" as the "Port Type". Configure this for ports P1.1, P1.2 and P1.3.

Figure 2-16



Port: P1.3

Status: enabled

Port Name:

MAC Address: 20-87-56-10-26-07

Mode Type: -

Mode: 1G HD

Negotiation: enabled

☐ Flow Ctrl. Type

Flow Ctrl.: disabled

MTU: 1500

Port Type: Router-Port

Combo Port Media Type: auto

☐ Nodes Monitoring

Maximum Nodes: 0

OperState: down

Link: down

Blocked by: Link down

☒ Unicast MAC Learning

Set Values Refresh

3. Once the router ports are set up, it is possible to assign IP interfaces. Assign the router the planned IP addresses.

IP interfaces are selected and configured in "Configuration" tab in the "Layer 3 (IPv4) > Subnets" menu.

Figure 2-17

Connected Subnets Overview

Overview Configuration

Interface: P1_1

☐ Loopback

Interface	TIA Interface	Status	Interface Name	MAC Address	IP Address	Subnet Mask
P1_1	-	enabled	Slot1/1	20-87-56-18-d4-05	192.168.2.1	255.255.255.0
P1_2	-	enabled	Slot1/2	20-87-56-18-d4-06	192.168.12.1	255.255.255.0
P1_3	-	enabled	Slot1/3	20-87-56-18-d4-07	192.168.10.2	255.255.255.0
Out-Band	-	enabled	eth0	20-87-56-18-d4-3d	0.0.0.0	0.0.0.0
vlan1	yes	enabled	vlan1	20-87-56-18-d4-00	192.168.100.2	255.255.255.0

5 entries.

Create Delete Refresh

4. Assign the router the designated IP addresses (xxx.xxx.xxx.xxx) in the "Configuration" tab.

Table 2-5

Device	Interface	IP address	Subnet mask
Router 1	Port 1	192.168.1.1	255.255.255.0
	Port 2	192.168.10.1	255.255.255.0
	Port 3	192.168.11.2	255.255.255.0
Router 2	Port 1	192.168.2.1	255.255.255.0
	Port 2	192.168.12.1	255.255.255.0
	Port 3	192.168.10.2	255.255.255.0
Router 3	Port 1	192.168.3.1	255.255.255.0
	Port 2	192.168.11.1	255.255.255.0
	Port 3	192.168.13.2	255.255.255.0
Router 4	Port 1	192.168.4.1	255.255.255.0
	Port 2	192.168.13.1	255.255.255.0
	Port 3	192.168.12.2	255.255.255.0

Figure 2-18

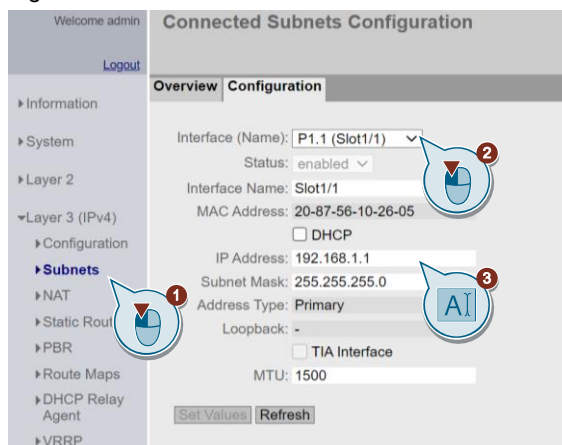


Figure 2-19

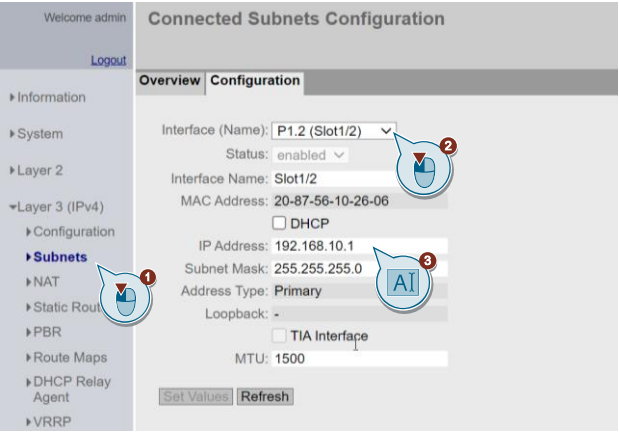
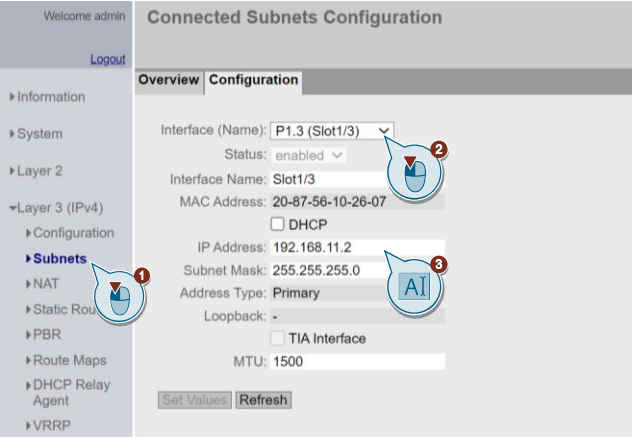
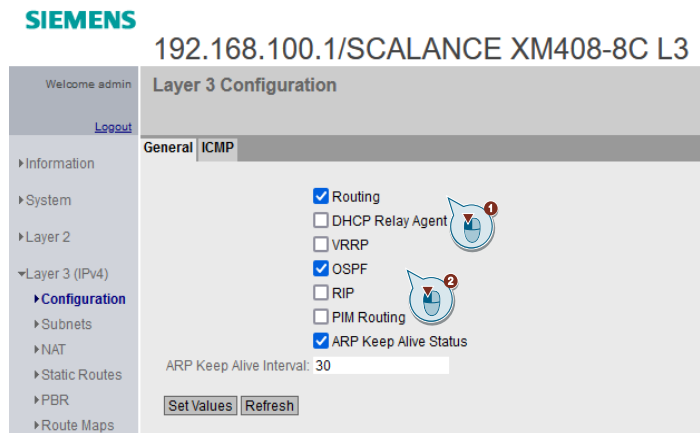


Figure 2-20



5. Enable the routing functionality to enable communication between the subnets. Enable the OSPF protocol.

Figure 2-21

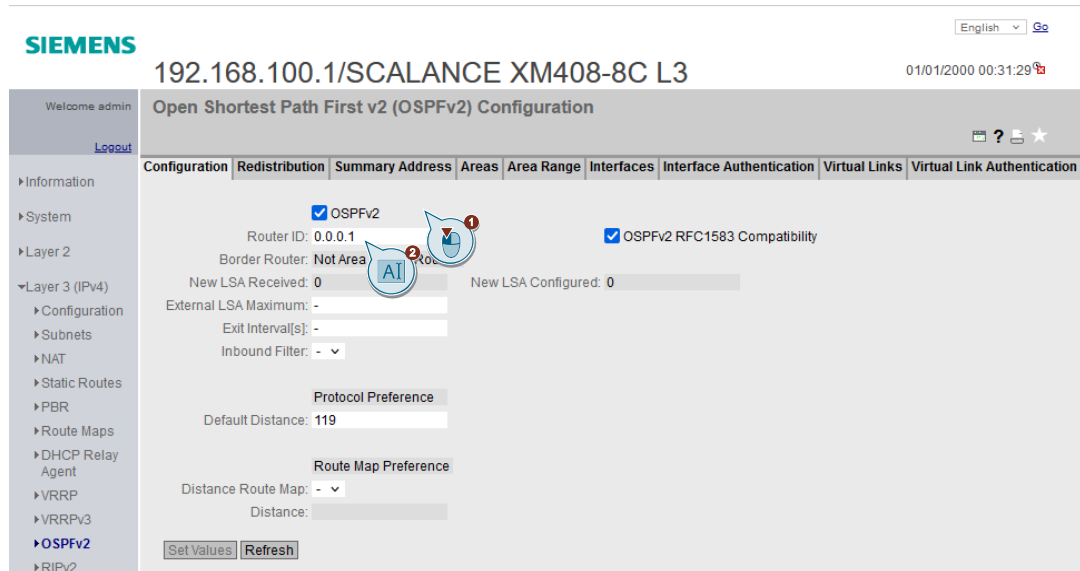


6. Select the menu "Layer 3 (IPv4) > OSPFv2 > Configuration". Tick the "OSPFv2" checkbox. Enter the ID of the router in the "Router ID" field. It has to be unique in the entire network.

Table 2-6

Router	Router ID
Router 1	0.0.0.1
Router 2	0.0.0.2
Router 3	0.0.0.3
Router 4	0.0.0.4

Figure 2-22



7. Create an OSPF interface for every IP interface of the router. An IP interface and an area must be selected to do this. Clicking "Create" creates an OSPF interface. Here, only an area is needed; all other values remain as their default settings. OSPF interfaces are set in the "Interfaces" tab in the "Layer 3 (IPv4) > OSPFv2" menu.

From the "IP Address" dropdown menu, select the IP address of the OSPF interface. From the "Area ID" dropdown menu, select the ID of the area to which the OSPF interface is connected. Area 0.0.0.0 always exists by default. Click on the "Create" button. A new entry is created in the table. If applicable, tick the "Passive Interface" checkbox. For "Trans Delay", "Retrans delay" and "Dead Interval", set appropriate values or use the default settings. Click the "Set Values" button.

Figure 2-23

Open Shortest Path First v2 (OSPFv2) Interfaces

Configuration | Redistribution | Summary Address | Areas | Area Range | Interfaces | Interface Authentication | Virtual Links | Virtual Link Authentication

☐ Default Passive Interface

IP Address: 192.168.100.1
Area ID: 0.0.0.0

Select	IP Address	Address Type	Area ID	Passive Interface	Metric	Priority	Trans. Delay	Retrans. Delay	Hello Interval	Dead Interval
<input type="checkbox"/>	192.168.1.1	Primary	0.0.0.0	<input type="checkbox"/>	1	1	1	5	10	40
<input type="checkbox"/>	192.168.10.1	Primary	0.0.0.0	<input type="checkbox"/>	1	1	1	5	10	40
<input type="checkbox"/>	192.168.11.2	Primary	0.0.0.0	<input type="checkbox"/>	1	1	1	5	10	40

3 entries.

Create Delete Set Values Refresh

Hello Interval: The time between the transmission of two OSPF Hello packets. A time of 10 seconds is set for the Hello Interval by default.

Dead Interval: The waiting time during which no OSPF Hello packet is received, which elapses until an adjoining router is declared inactive and its LSAs are discarded. By default, the Dead Interval is set to 4 times the length of the Hello Interval.

Retransmit delay: In the absence of an acknowledgment, time that must elapse before an LSA, a database write operation or a Link State Request packet is retransmitted. The default setting is 5 seconds.

Transmit delay: The transmit delay increases the age of the LSAs in update packets in order to adapt the transmission and forwarding times for the interface. This delay is important with very slow links for which the transmission time has a greater effect.

8. Check that all entries are present in the routing table. First, all directly connected subnets must appear; and second, the dynamically learned routes must also appear. You can find the routing table in the menu "Information > IPv4 Routing". The routes are only displayed when the associated physical interface is active.

Figure 2-24

Welcome admin [Logout](#)

Layer 3: IPv4 Routing Table

Routing Table | Policy Based Routing | OSPFv2 Interfaces | OSPFv2 Neighbors | OSPFv2 Virtual Neighbors | OSPFv2 LSDB | RIPv2 Statistics | NAT Translations

Information

Start Page

Versions

ISM

ARP / Neighbors

Log Table

Faults

Redundancy

Ethernet Statistics

Unicast

Multicast

LLDP

FMP

IPv4 Routing

PIM Interfaces | PIM Neighbors | PIM Routes | PIM RPs | PIM BSRs | MSDP Cache

Destination Network	Subnet Mask	Gateway	Interface	Metric	Routing Protocol
192.168.1.0	255.255.255.0	0.0.0.0	P1.1	0	connected
192.168.2.0	255.255.255.0	192.168.10.2	P1.2	2	OSPF
192.168.3.0	255.255.255.0	192.168.11.1	P1.3	2	OSPF
192.168.4.0	255.255.255.0	192.168.10.2	P1.2	3	OSPF
192.168.4.0	255.255.255.0	192.168.11.1	P1.3	3	OSPF
192.168.10.0	255.255.255.0	0.0.0.0	P1.2	0	connected
192.168.11.0	255.255.255.0	0.0.0.0	P1.3	0	connected
192.168.12.0	255.255.255.0	192.168.10.2	P1.2	2	OSPF
192.168.13.0	255.255.255.0	192.168.11.1	P1.3	2	OSPF

9 entries.

[Refresh](#)

9. Check that all interfaces are active. The overview of OSPF interfaces can be found in the "OSPFv2 Interfaces" tab in the "Information > IPv4 Routing" menu.

Figure 2-25

Welcome admin [Logout](#)

Open Shortest Path First v2 (OSPFv2) Interfaces

Routing Table | Policy Based Routing | OSPFv2 Interfaces | OSPFv2 Neighbors | OSPFv2 Virtual Neighbors | OSPFv2 LSDB | RIPv2 Statistics | NAT Translations

Information

Start Page

Versions

ISM

ARP / Neighbors

Log Table

Faults

Redundancy

Ethernet Statistics

Unicast

Multicast

LLDP

FMP

IPv4 Routing

PIM Interfaces | PIM Neighbors | PIM Routes | PIM RPs | PIM BSRs | MSDP Cache

IP Address	Area ID	Interface Status	Designated Router	Backup Designated Router	Events
192.168.1.1	0.0.0.0	Designated Router	192.168.1.1	0.0.0.0	2
192.168.10.1	0.0.0.0	Backup D. Router	192.168.10.2	192.168.10.1	4
192.168.11.2	0.0.0.0	Backup D. Router	192.168.11.1	192.168.11.2	4

[Refresh](#)

10. Check the state of the neighborhood relation to the other routers. The overview of OSPF neighbors can be found in the "OSPFv2 Neighbors" tab in the "Information > IPv4 Routing" menu. The state with a Designated Router or Backup Designated Router must always be "full". A router maintains the "Two-way" relationship to other routers.

Figure 2-26

Open Shortest Path First v2 (OSPFv2) Neighbors

Routing Table | Policy Based Routing | OSPFv2 Interfaces | **OSPFv2 Neighbors** | OSPFv2 Virtual Neighbors | OSPFv2 LSDB | RIPv2 Statistics | NAT Translations

PIM Interfaces | PIM Neighbors | PIM Routes | PIM RPs | PIM BSRs | MSDP Cache

IP Address	Router ID	Status	Assoc. Area Type	Priority	Hello Suppr.	Retrans Queue	Events
192.168.10.2	0.0.0.2	full	Normal	1	no	0	6
192.168.11.1	0.0.0.3	full	Normal	1	no	0	5

Refresh

11. Repeat steps 1 to 10 for Router 2, Router 3 and Router 4.

2.5.1 The routing table

Description

The routing table contains information on known networks and by which path (route) these networks can be accessed. The routing table is divided into several columns.

The most important columns in the routing table are:

- Destination network address: Identifies the subnet that is to be accessed.
- Gateway: IP address of the next router. All the IP packets intended for the destination network are forwarded to this router.

Terminal routing table

The terminals usually have two entries in the routing table:

- An entry for their own subnet. This particular entry has no gateway or has the IP Address "0.0.0.0" as gateway.
- A default route for all packets that are not addressed to the device's own subnet. In this case, the network address "0.0.0.0/0" ("all remote networks") is given as the destination network; and the IP address of the next router is given as the gateway.

Routing table of routers

The router must have an entry in its routing table for each subnet to which it is to forward the IP packets.

The routers can learn the routes and fill their table in three different ways:

- Directly connected subnets: Each IP interface is automatically entered in the table with the corresponding subnet.

Note

The route of an IP interface will only be visible in the table if the corresponding physical IP interface is active.

- Static routing: These routes are configured manually by an administrator.
- Dynamic routing: In this case, the routers automatically learn all accessible networks through one or more configured routing protocols.

Note

In this application example the routers learn the routes as follows:

- Automatically through their IP interfaces
- Dynamically

Structure of the table

The routing table has six columns. The columns can be grouped together as follows:

- Description of the destination
Column 1 ("Destination Network") identifies the network that is to be contacted
Column 2 ("Subnet mask") contains the corresponding subnet mask
- Description of the route
Column 3 ("Gateway") contains the IP address of the next router. All the IP packets intended for the destination network are forwarded to this router.
Column 4 ("Interfaces") is the device's own interface, through which the IP packet must be sent. This can be either a VLAN or a router port.
- Description of the quality
Column 5 ("Metric") determines the cost of the route.
Column 6 ("Routing Protocol") shows from which routing protocol the entry originates. The following contents are possible:
 - Connected: Connected routes
 - Static: Static routes
 - RIP, OSPF: Dynamic routing
 - Other: Other routing

If several routes exist for the same destination, these two columns determine which route is taken.

The following screenshot shows the routing table of the SCALANCE XM-400.

Figure 2-27

Destination Network	Subnet Mask	Gateway	Interface	Metric	Routing Protocol
192.168.1.0	255.255.255.0	192.168.10.1	P1.3	2	OSPF
192.168.2.0	255.255.255.0	0.0.0.0	P1.1	0	connected
192.168.3.0	255.255.255.0	192.168.10.1	P1.3	3	OSPF
192.168.3.0	255.255.255.0	192.168.12.2	P1.2	3	OSPF
192.168.4.0	255.255.255.0	192.168.12.2	P1.2	2	OSPF
192.168.10.0	255.255.255.0	0.0.0.0	P1.3	0	connected
192.168.11.0	255.255.255.0	192.168.10.1	P1.3	2	OSPF
192.168.12.0	255.255.255.0	0.0.0.0	P1.2	0	connected

From what the routing table shows, the following statements can be made:

- Rows 2, 6 and 8 were created automatically through the configured IP interfaces.
- Rows 1, 3, 4, 5 and 7 were created dynamically.

3 Testing the OSPF scenario

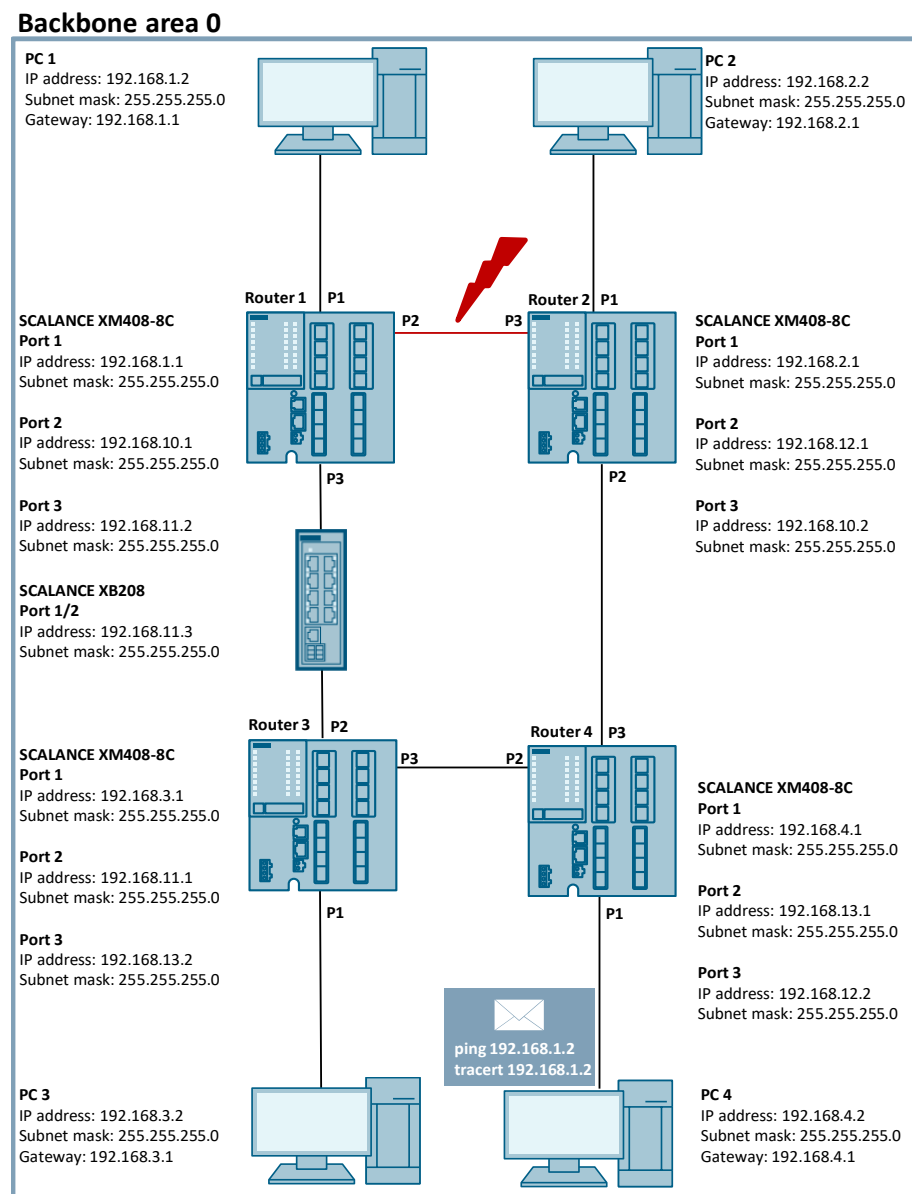
The Command Prompt (cmd) has the commands *ping* and *tracert* for testing the availability between individual PCs. Both of these commands are used to verify the availability of the network node.

3.1 Error scenarios

Connection failure

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

Figure 3-1



Switchover scenario with ping command

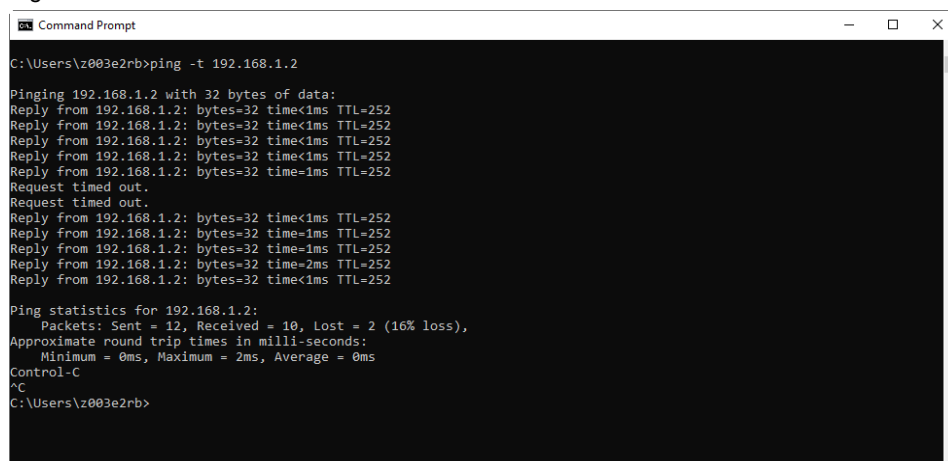
Ping sends ICMP packet echoes over the network to the specified IP address and waits for an answer in the form of an Echo reply. In the Command Prompt, the user can see how long the data transfer took and whether the availability of the node was ensured. The ping command can be used to find each of the router's interfaces. Every PC should be able to send a ping to every other PC in the topology. If this is not the case, check for errors in the configuration or the hardware setup.

The command "*ping -t IP address of the network node*" runs a continuous ping which should reveal the switchover in the event of a connection failure. This can be used to test whether all devices on the network can be reached.

Procedure:

1. Press the "[Windows]" + "R" key combination.
2. Enter "cmd" in the window that appears. Click on the "OK" button.
3. Enter the command "ping -t 192.168.1.2" to ping PC3.
4. While the continuous ping is running, unplug a network cable for the redundant path.

Figure 3-2



```
Command Prompt
C:\Users\z003e2rb>ping -t 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=252
Reply from 192.168.1.2: bytes=32 time<1ms TTL=252
Reply from 192.168.1.2: bytes=32 time<1ms TTL=252
Reply from 192.168.1.2: bytes=32 time<1ms TTL=252
Reply from 192.168.1.2: bytes=32 time<1ms TTL=252
Request timed out.
Request timed out.
Reply from 192.168.1.2: bytes=32 time<1ms TTL=252
Reply from 192.168.1.2: bytes=32 time<1ms TTL=252
Reply from 192.168.1.2: bytes=32 time<1ms TTL=252
Reply from 192.168.1.2: bytes=32 time=2ms TTL=252
Reply from 192.168.1.2: bytes=32 time<1ms TTL=252

Ping statistics for 192.168.1.2:
    Packets: Sent = 12, Received = 10, Lost = 2 (16% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
Control-C
^C
C:\Users\z003e2rb>
```

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 destination 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 on the "OK" button.
3. Enter the command "tracert 192.168.1.2" to trace the route in the network.

Figure 3-3

```
C:\Users\z003e2rb>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops

  1    2 ms    2 ms    2 ms  192.168.4.1
  2    2 ms    2 ms    2 ms  192.168.12.1
  3    2 ms    2 ms    2 ms  192.168.10.1
  4    2 ms    <1 ms   <1 ms  192.168.1.2

Trace complete.

C:\Users\z003e2rb>
```

You can see in the output from this command that the destination address now routes over Router 2 and Router 1.

4. Unplug a network cable on Router 1 (port 2).
5. Re-enter the command "tracert 192.168.1.2" to reach PC1.

Figure 3-4

```
C:\Users\z003e2rb>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops

  1    3 ms    2 ms    1 ms  192.168.4.1
  2    2 ms    2 ms    2 ms  192.168.13.2
  3    2 ms    2 ms    2 ms  192.168.11.2
  4    1 ms    <1 ms   <1 ms  192.168.1.2

Trace complete.

C:\Users\z003e2rb>
```

You can see in the output from this command that the destination address now routes over Router 3 and Router 1.

You can use ping and tracert to check the new routing information. A cable is unplugged to demonstrate that the system searches for a redundant route.

4 Useful information

4.1 IP routers

4.1.1 Function and tasks

What is a router?

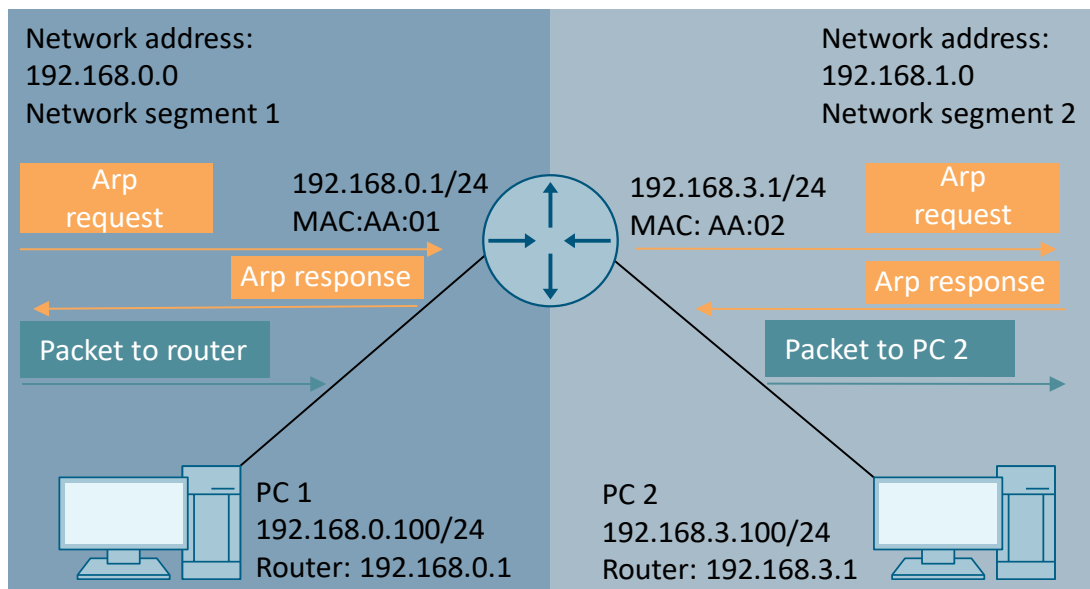
A router is a network component on layer 3 of the OSI reference model; it connects two subnets to each other. The router must have an IP address in each network that it is to connect to others. This is also referred to as an IP interface.

Note

The subnets connected to the IP router must be different. Each connected subnet must have a unique network address.

The following Figure shows a router that connects two subnets to each other. The router has its own IP interface for each adjacent subnet.

Figure 4-1



Tasks of a router

When a terminal (end device or transmitter) sends an IP data packet, the Internet Protocol checks whether the IP data packet is bound for its own subnet or not.

If the intended recipient is located in its own subnet, the data packet is handed over to the lower layers of the OSI reference model. The lower layers register the recipient's IP address from the data packet and send the data packet.

If the recipient is not in the same subnet, the sender cannot access the recipient directly. The sender needs to use the detour via the IP router and forward the IP data packet to the router.

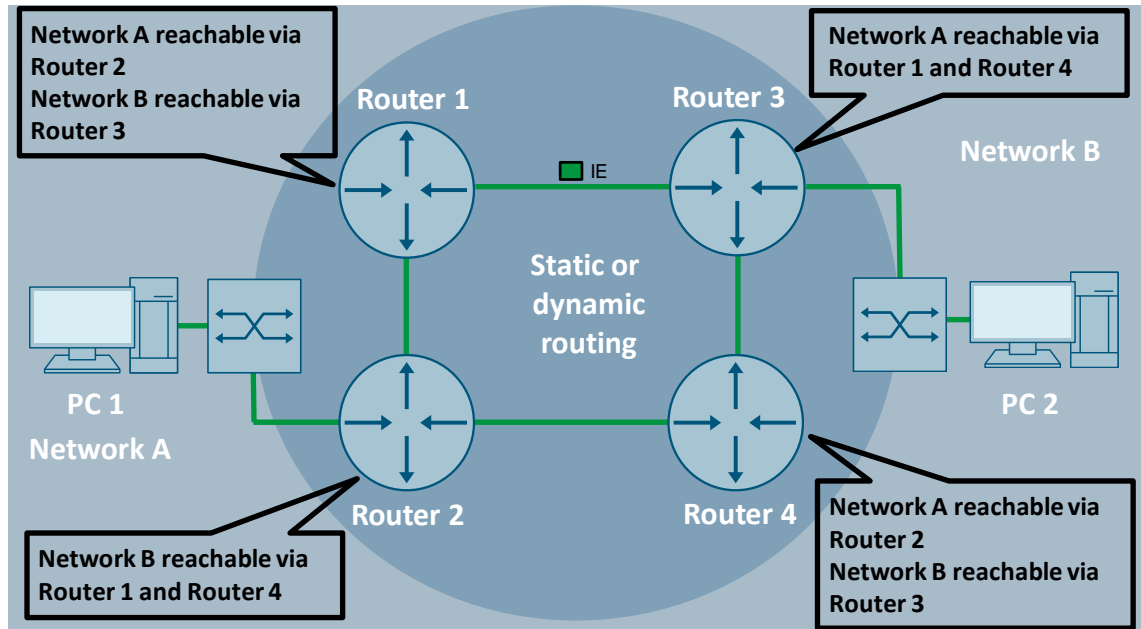
To do this, it passes the data packet to the lower two layers of the OSI reference model. The lower layers use the IP address of the default router to determine the MAC address of the router and send the data packet to the IP router.

The IP router has an IP interface with one IP address for each of the two networks. It uses its routing table to check whether it is possible to forward the data packet to the other subnet. If this is possible, the router sends the data to the other network.

4.2 Routing mechanisms

Communication between different IP subnets requires routes in order to determine the possible path from network A to network B. Each router employs a routing table to decide how IP data packets are processed and routed.

Figure 4-2



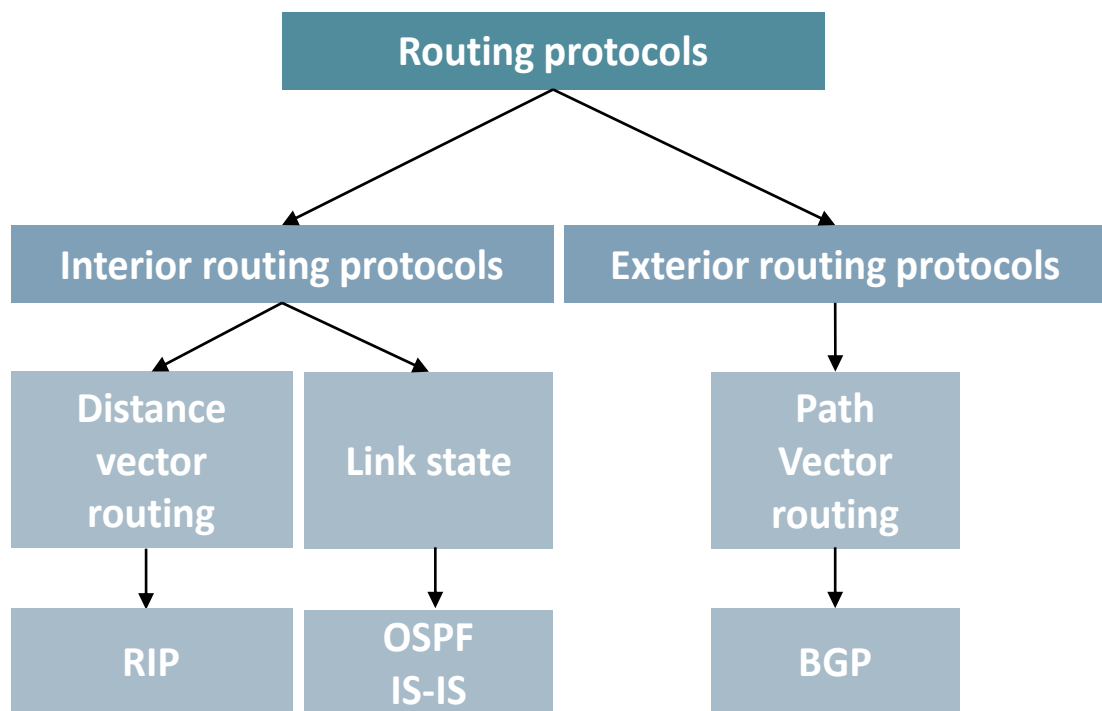
4.2.1 Static routing

In small network environments with only a few routers, it is possible manually oversee routes between different networks using static entries in the routing table. The advantage is predictable behavior when establishing connections with external networks. The disadvantage is a relatively high investment in time and energy to maintain the system. Implementing static routing can make sense when there are multiple paths to a given destination. Make sure to prevent layer 3 loops and the sending of packets through an incorrect gateway.

4.2.2 Dynamic routing

If networks grow or often change, it can become impossible (or inefficient) to manually implement changes in time. For this reason, routing protocols were developed to facilitate the automatic exchange of routing information between routers. Another reason in favor of dynamic routing is the implementation of redundancy through multiple routes between origin and destination. Dynamic routing protocols are subdivided into distance vector protocols and link state protocols. The preference for one or the other protocol can depend on factors such as network size, convergence time, etc.

Figure 4-3



Interior / exterior routing protocols

Interior routing protocols were developed to gather path information in routers that are all under the same administrative control or within the same routing domain. Exterior routing protocols are used between networks managed by different administrative entities or organizations. It may be added that routers which are "yours" and which speak the same routing protocol will probably use an interior routing protocol. If your organization exchanges routing information with another entity or routing domain that is managed by somebody else (e.g. a service provider), then exterior routing protocols can be used at the connection point in order to exchange routing information.

Distance vector protocols

The Routing Information Protocol (RIP) is an example of an early distance vector protocol. The Routing Information Protocol determines the optimal path to the destination based on the hop count between the origin and destination network. The route with the fewest hops is preferred.

Link state protocols

Open Shortest Path First (OSPF) is the most widespread link state protocol. Unlike with distance vector protocols, every router knows the entire network topology. When processing data packets, the router will use the shortest path through the network as a basis when handling data packets. To make this possible, every router shares with neighboring routers; they begin to share LSA messages (Link State Advertisements) containing information about the network topology. Open Shortest Path First finds the optimal communication path using Link Costs, which by default are calculated using the interface bandwidth and the reference value calculated from it. The route from the source to the destination is determined with the Shortest Path First algorithm (Dijkstra's algorithm). OSPF is based on an area concept. The hierarchical structure is based on a central area (backbone), used for data exchange by the areas connected to it.

Characteristics of dynamic routing protocols

Table 4-1

Protocol	Description	Characteristics	Administrative distance
RIP v1/v2 RFC 1508 RFC 2453	Routing Information Protocol	<ul style="list-style-type: none">• Small networks• Maximum of 15 hops possible• Slow convergence	120
OSPF RFC 1131 (1st version) RFC 2328 (2nd version IPv4) RFC 5340 (3rd version IPv6)	Open Shortest Path First	<ul style="list-style-type: none">• Small to large network are possible• Area-based concept• Scalable with fast convergence• Model based on a central area	110

Advantages of dynamic routing protocols

Figure 4-4

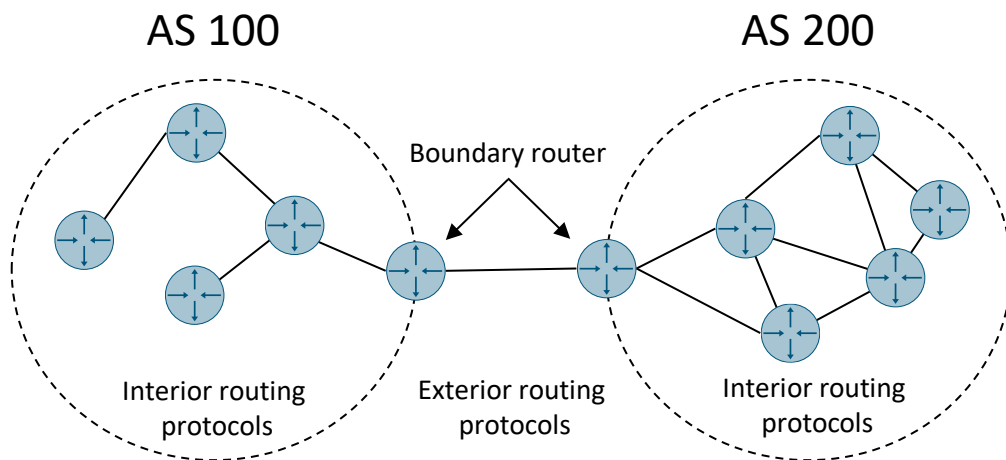
Makes sense when	Advantages
<ul style="list-style-type: none">• the network comprises a great number of paths• the topology changes dynamically• network expansions often occur through the addition of new IP subnets• automatic path optimization is needed• redundant and backup links are available• load distribution with end-to-end link monitoring is required	<ul style="list-style-type: none">• automatic, dynamic path selection and optimization• dynamic propagation of extensions/additions/changes in network segments• automatic network convergence if an active link fails. Traffic is re-routed over redundant paths and connectivity is retained• Routing information is exchanged with external networks through gateway routers

4.3 OSPF hierarchy using Single Area or Multiarea

Autonomous System (AS)

A group of networks subject to a common administrative domain or control is known as an autonomous system (AS). The routers within an autonomous system often use a common routing algorithm (e.g. Open Shortest Path First). Autonomous systems have unique global numbering (Autonomous System Number, ASN). The Internet Assigned Numbers Authority (IANA) is responsible for managing the Autonomous System Number. To ensure communication between two autonomous systems, routers must assume the role of boundary router. The division into autonomous systems allows for better scalability.

Figure 4-5



OSPF areas

To make OSPF more efficient and scalable, OSPF supports hierarchical routing and the use of areas. An autonomous system can be subdivided into multiple OSPF areas. An area comprises one or more subnets. Like an IP address, an area is represented as a 32-bit value in four octets in the form XXX.XXX.XXX.XXX. Here, X stands for a decimal value between 1 and 255.

Example:

Area 1 → 0.0.0.1

Area 2 → 0.0.0.2

Area 500 → 0.0.1.244 (500 in binary is 111110100)

The division into areas makes it easier for the routers to store data, and it speeds up route calculation. An OSPF router only needs to save link state information for all IP interfaces in its area. All routers within an area thus have the same routing information. The routers share the structure of the topology with each other. Only selected routers on area boundaries need to compile information from multiple areas. The areas should not be too large (for example, no more than 50 routers).

OSPF can be implemented in one of two area types:

4.3.1 Single-area OSPF (backbone area)

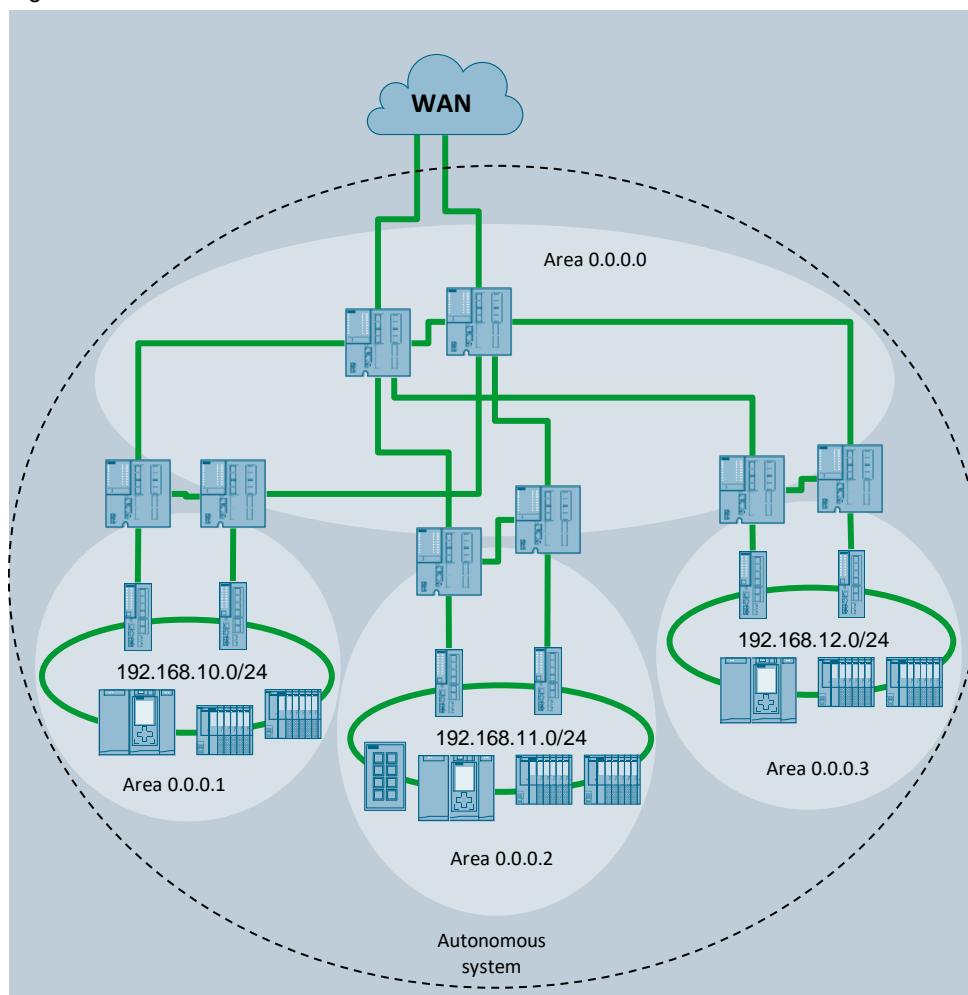
All routers are located in one area, known as Area 0 (0.0.0.0, backbone area). An OSPF network cannot work properly without Area 0. OSPF allows for a hierarchical design thanks to the backbone area. This application example uses the configuration for a single area.

4.3.2 Multi-area OSPF

OSPF is implemented hierarchically when multiple areas are used. For large networks, a single network must be subdivided into different areas in order to reduce the information such as that concerning topology. All areas must connect to the backbone area (Area 0). Routers that connect areas are known as Area Border Routers (ABRs). If it is not possible to connect an ordinary area with the backbone, then virtual links may be used to communicate with the backbone area.

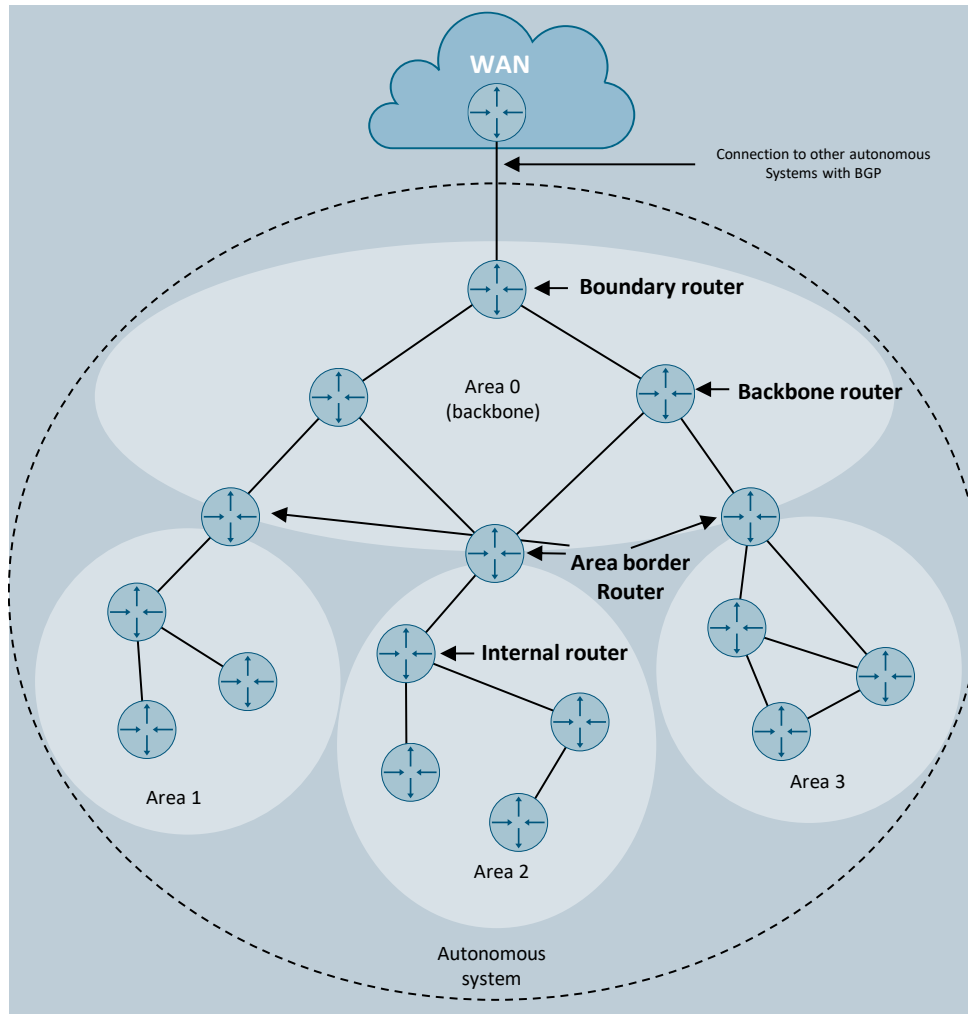
The automation network shown in the Figure has been continually expanded and now consists of many subnets. For the sake of administrative simplicity, the routes need to be entered in the routers automatically. The paths should be redundant, so that fast convergence can occur in the event that a network segment fails.

Figure 4-6



4.3.3 Types of routers

Figure 4-7



In an OSPF routing hierarchy, a distinction is made between four different types of routers.

Area Border Router

If an OSPF router has IP interfaces in different areas, it is known as an Area Border Router. An ABR must store link state information about all IP interfaces in all adjoining areas. The information is prepared (e.g. by summarizing multiple routes into a Summary Route) and then transmitted to the other areas. An ABR is typically connected to two or more areas, one of which is the backbone area. These routers service the other areas in the role of access point(s) to the backbone area.

Autonomous System Boundary Router (ASBR)

Routers located on the boundary of an autonomous system, that is, of at least one other autonomous system, are known as boundary routers (Autonomous System Boundary Routers). They are responsible for exchanging routing information with other autonomous systems. An ASBR can prepare the routing information from an adjoining non-OSPF network and feed it into the OSPF process (e.g. as a default route).

Backbone Router

The routers in the backbone route data traffic between the areas.

Internal Router (IR)

These are OSPF routers with IP interfaces within the same area. All routers belonging to the same area have an identical database (Link State Database, LSDB) on their area.

4.3.4 Special area types

When exchanging routing information between routers, an administrator can control which destination networks his/her routers can provide to others, and/or which ones they can receive from (learn of).

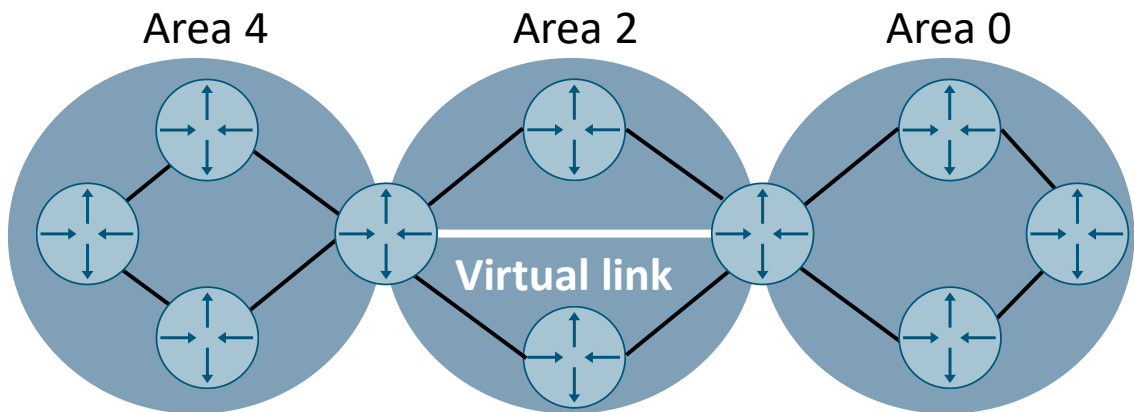
OSPF recognizes 5 types of area. The area type determines the type of routing information (LSAs) used there.

- **Standard Area:** This area accepts (intra-area) link updates, (inter-area) route summaries, and external routes. This area can contain LSA types 1, 2, 3, 4 and 5.
- **Backbone Area (transit area):** The backbone area (Area 0) connects all other areas in order to exchange routing information.
- **Stub Area:** This area does not receive any information about routes outside of the autonomous system, e.g. from non-OSPF sources. This area can contain the following LSA types: 1, 2 and 3.
- **Totally Stubby Area:** This area accepts no external autonomous system (AS) routes or summary routes from other internal areas of its AS.
- **Not-So-Stubby Area (NSSA):** Only LSA type 7 is used in this area. NSSA is used when routes are required between networks with RIP and OSPF, for example. ABRs translate type-7 LSAs of an NSSA into type-5 LSAs during routing. NSSAs do not receive or transmit type-5 LSAs.

4.3.5 Virtual links

All areas in an autonomous OSPF system must be physically connected with the backbone area. In some cases where a physical connection is not possible, a virtual link may be used. The area with which a virtual link is configured, also known as a Transit Area, must have complete routing information. The Transit Area cannot be a Stub Area.

Figure 4-8



4.4 Metrics

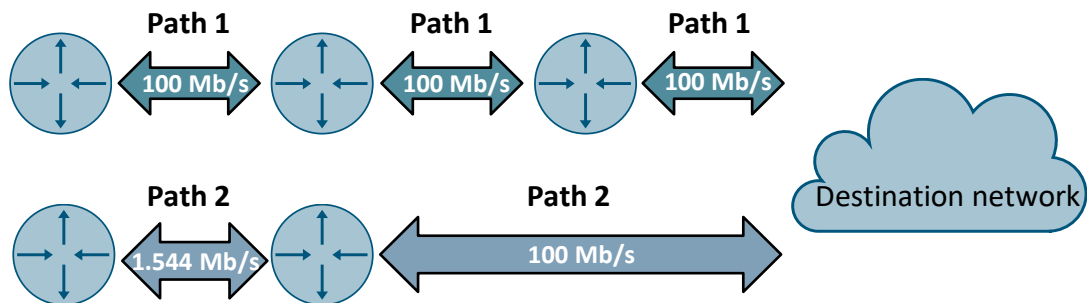
The metric is a value used by routing protocols to calculate the best route to a destination subnet.

How the respective metric is calculated depends on the routing protocol. Here, the routing protocols use different factors when calculating the metric. The lower a route's metric, the better the route is.

Table 4-2

Protocol	Metrics
Directly connected	-
Static route	-
OSPF	Link bandwidth: The best path is calculated using the interface bandwidth and a reference value.
RIP	Hop count: How many routers there are on the path to the destination.

Figure 4-9



Path 1: OSPF protocol metric calculation

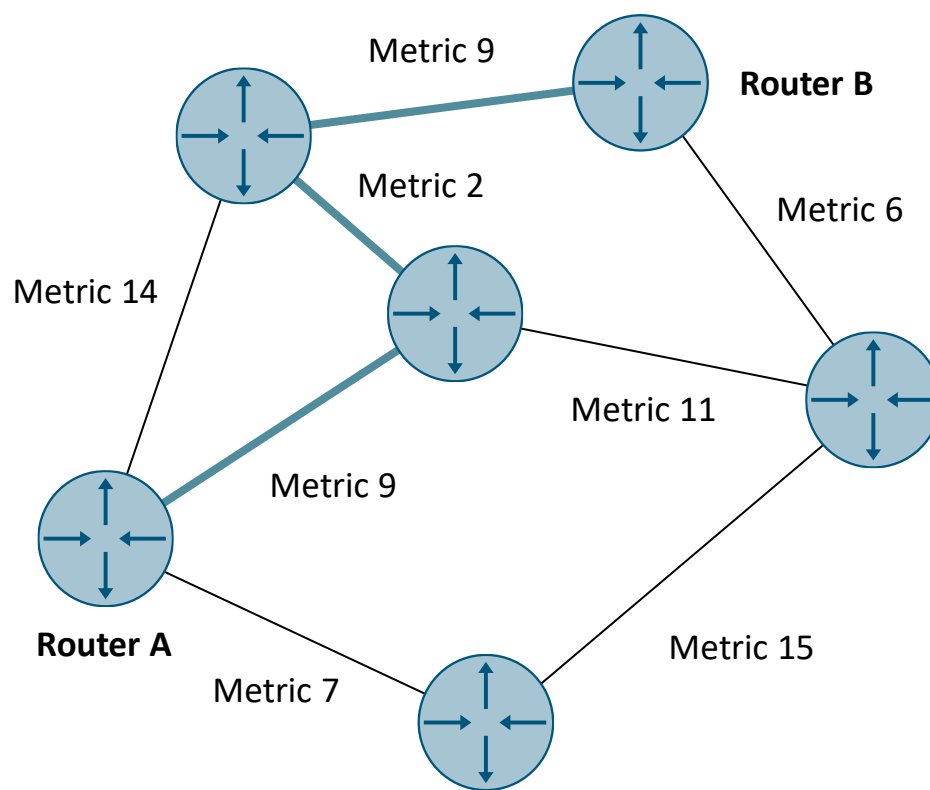
If the bandwidth is used as a metric, one can see from [Figure 4-9](#) that Path 1 would be preferred. The path has a bandwidth of 100 Mbps, compared to Path 2 that has a slower connection. A slow connection in the path increases the value of the metric. The lower the value of the metric, the higher the priority for this route or path.

Path 2: RIP protocol metric calculation

However, if we use the hop count, then Path 2 has priority. Path 1 consists of two hops or routers that must hand off packets before they get to destination network A, while Path 2 only has one hop before the packets reach destination network A. The path selection thus depends on the lowest hop count.

4.4.1 Open Shortest Path First algorithm

Figure 4-10



Calculation of routing tables in OSPF is based on link state information. This means that an OSPF router knows all active IP interfaces of all other OSPF routers in a network (IP address and subnet mask); it can calculate the paths itself using this information. Dijkstra's "Shortest Path First" algorithm is used to calculate the path.

Every router running the Dijkstra algorithm tries to find the shortest path between two network components, for example between Router A and Router B. To do this, it calculates the total cost (cumulative metric) over every possible path to the destination node. The algorithm then selects the path with the lowest cumulative cost.

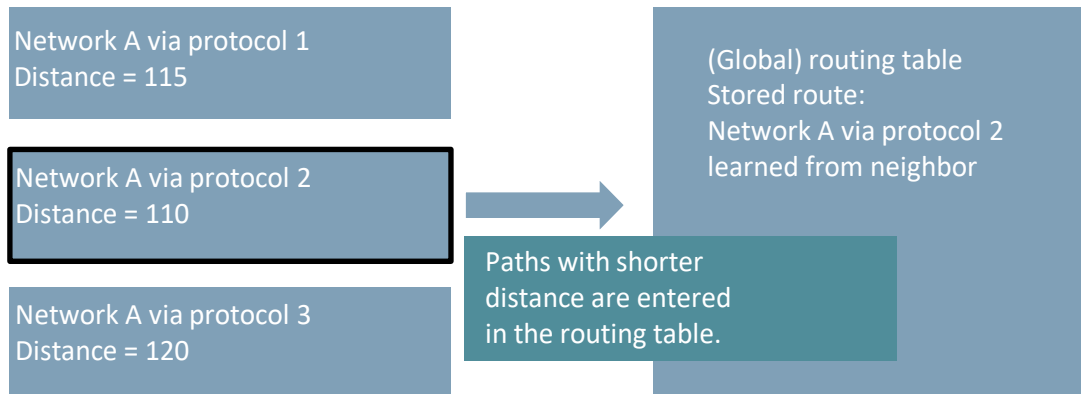
Since OSPF takes into account the interface bandwidth, faster paths have priority over slower ones.

In our example, the path with the lowest cost between Router A and Router B is $9+2+9 = 20$.

4.4.2 Administrative distance

The administrative distance is used when multiple routing protocols are running on the same router, and each has its own optimal path to the same destination network. Routers prefer protocols with the lowest administrative distance.

Figure 4-11



The following Table shows the administrative distance assigned to each.

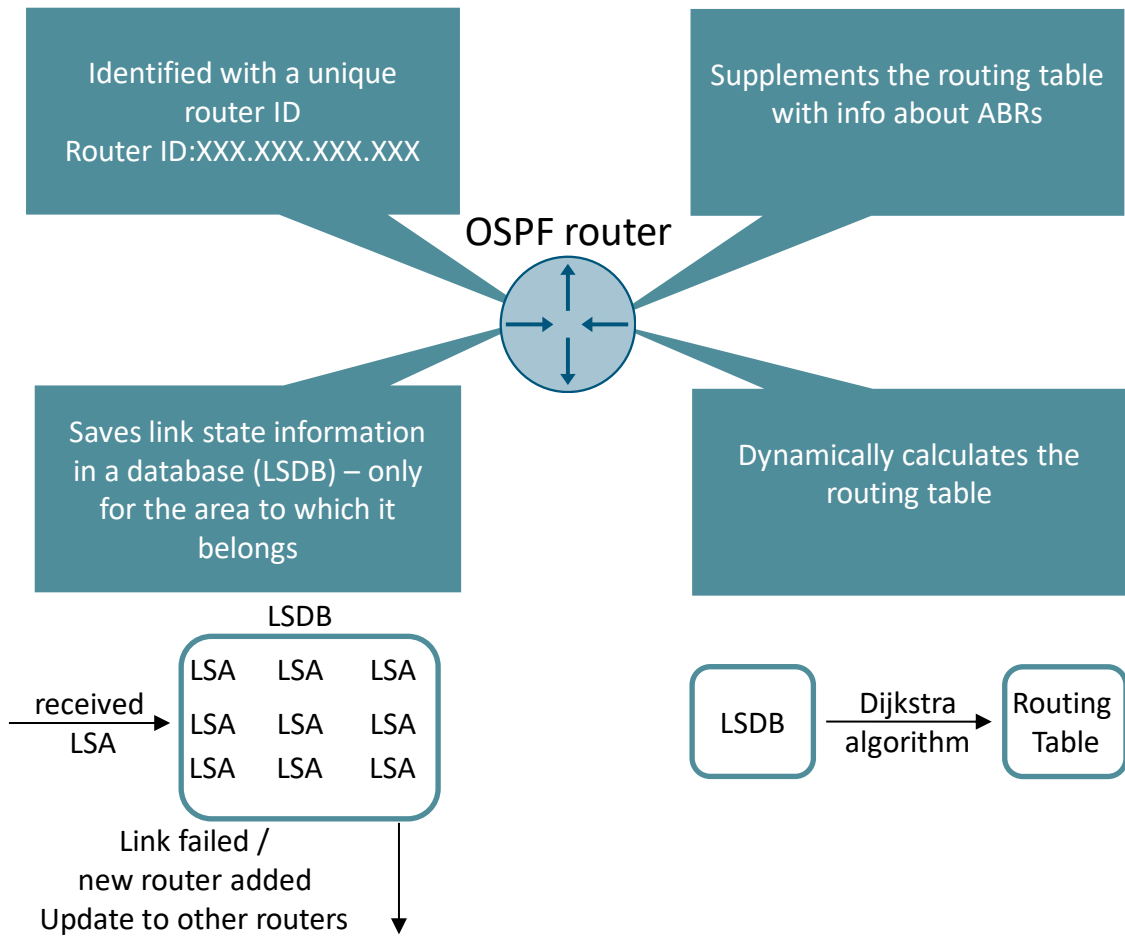
Table 4-3

Protocol	Administrative distance
Directly connected	0
Static route	1
OSPF	110
RIP	120

By default, static routes have a distance of one (1), so they are preferred over routes that were learned through dynamic routing protocols.

4.5 OSPF routers

Figure 4-12



Router identifier

Every OSPF router in an autonomous system must have a unique identifier (router ID). It is a 32-bit value written in the format XXX.XXX.XXX.XXX (like an IP address), where X is a decimal value between 1 and 255.

The administrator can configure this identifier. The router identifier can only be assigned once within an autonomous system. If the OSPF router ID is not explicitly configured by the administrator, the router will select one of the existing IP addresses of an active interface – generally the highest one available.

Link State Database (LSDB) and Link State Advertisements (LSA)

Link State Advertisements (LSAs) are exchanged between routers within an area. The LSAs contain information about the IP interfaces of the routers. All LSAs are stored in the Link State Database (LSDB). One important job of the OSPF protocol is to synchronize these LSDBs between the routers in an area by sharing the LSAs through direct neighbors (adjacency).

Routing table calculation

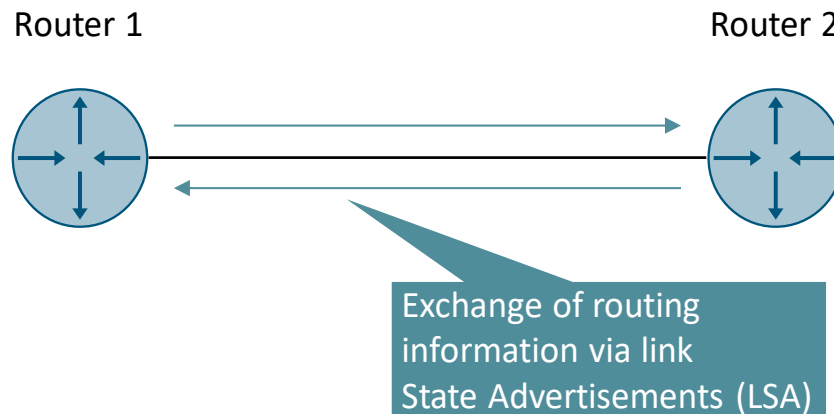
Using the data in the LSDB, every router calculates its routing table according to the Dijkstra algorithm. Every router calculates its own shortest path between itself and each subnet.

Supplementing of routing information

The calculated routing table is supplemented with information from other areas. It does not have to be calculated anew, as the information has already been prepared by the routers in the other areas.

4.5.1 Link State Advertisement (LSA)

Figure 4-13



Information exchange with LSAs

Routing information is exchanged with the help of Link State Advertisements (LSAs) between OSPF routers. The LSAs are copied to the LSDB when they are received. Every LSA is identified with the LSA source and a sequence number. The following pieces of information can be found in an LSA; they are stored in the LSDB.

LS Age

LS Age refers to the age of an LSA in seconds since its creation. Every router in the domain increases this value in its LSDB once per second. When the value of MaxAge (3600s) is reached, this information is marked in the router as invalid and is discarded. The "Link State Down" information is broadcasted throughout the routing domain by flooding the others with an LSA and setting the LS Age to MaxAge.

Link State ID

Identifies the part of the routing domain described in the LSA. Examples: ID of the originating router, IP address of the Designated Router, IP address of the destination network, and so forth.

Advertising Router

This field contains the Router ID of the router which prepares the information for the network. Only this router can create new versions – updates – of the LSA or cause it to be deleted.

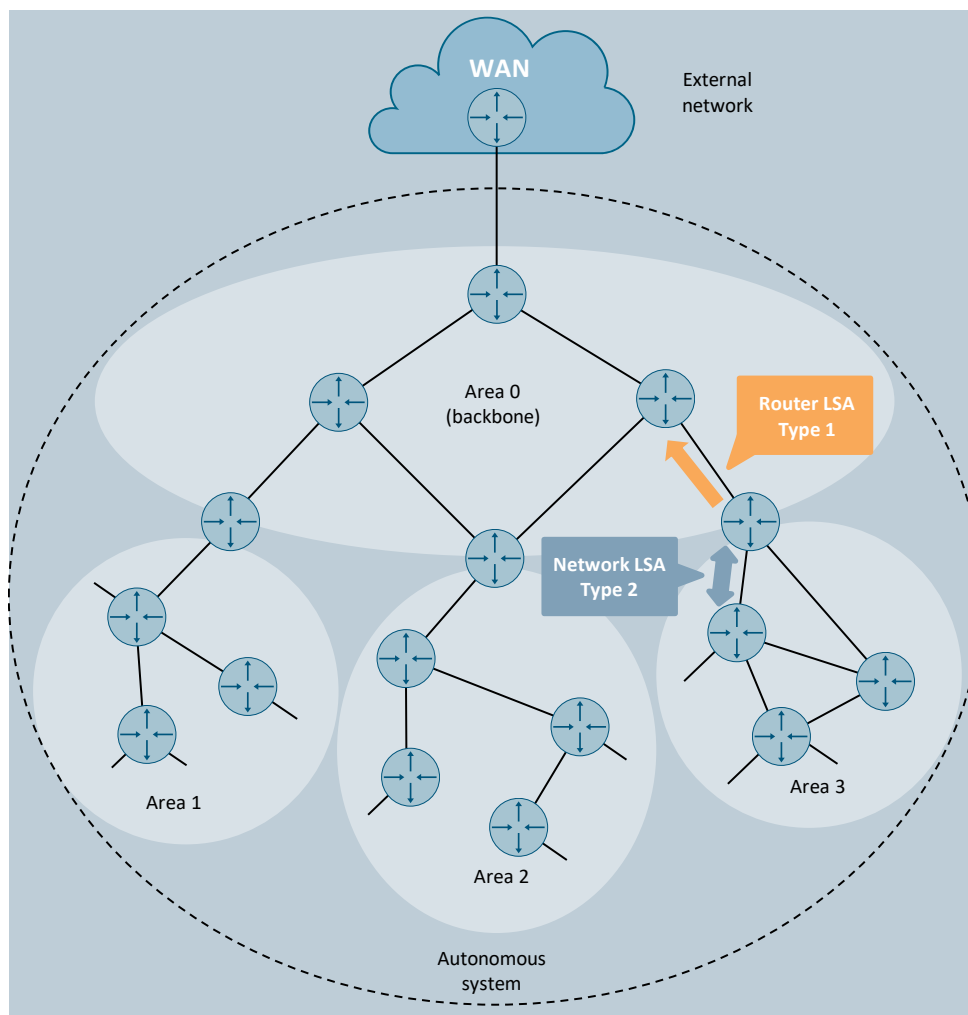
Sequence Number

While the information in Link State ID, LS Type and Advertising Router uniquely identify an LSA, the Sequence Number represents how up-to-date the information in the LSA is (the version). If an LSA with a higher Sequence Number is received, the receiving routers update their LSDB.

4.5.1.1 LSA types

Depending on the information being transported, there are different LSA types. The most important types are described in more detail in the pages below. For the sake of simplicity, the Figures each show only a subset of the LSA types.

Figure 4-14

**Type 1: Router LSA**

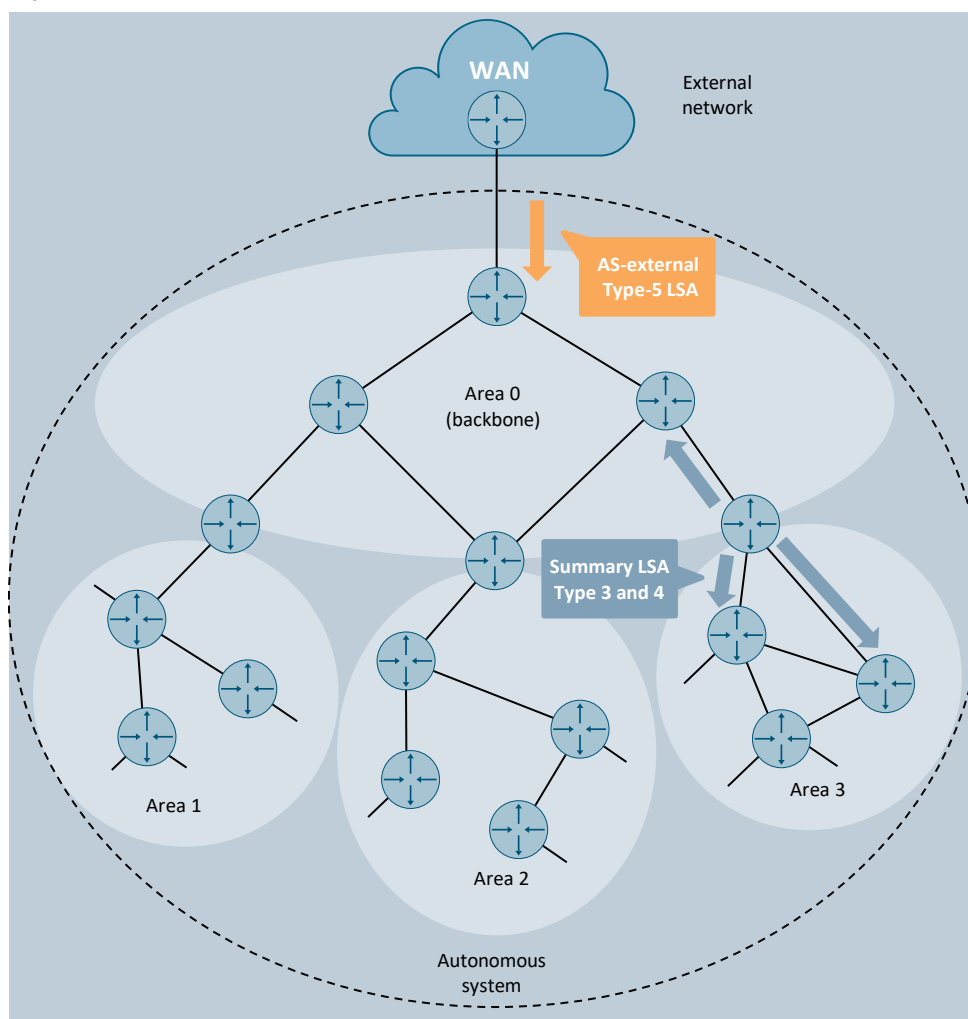
A router LSA contains information about the respective router. This information includes the Router ID and data about the states of its IP interfaces for an area. An LSA is generated for every area belonging to a router.

Type 2: Network LSA

In every layer 2 network with more than one OSPF router, a network LSA is generated and sent by a router. It describes the routers present in this network segment. The router that sends this LSA is known as the Designated Router (DR).

LSA types 1 and 2 are transmitted in a process known as flooding between the routers in an area. The Shortest Path Tree (SPT) for an area is calculated using these LSAs.

Figure 4-15



Type 3 or 4: Summary LSA

Describes routes between areas. Area Border Routers (ABRs) compile the routing information from their areas and generate summary LSAs (type 3). These LSAs are distributed to the other areas. In this way, the reachable networks in an area are shared with another area. Without the need for route summaries configured by an administrator, a summary LSA is generated for every subnet in an area and then distributed among the other areas. The route to the ASBR (LSA type 4) is also sent in a similar manner.

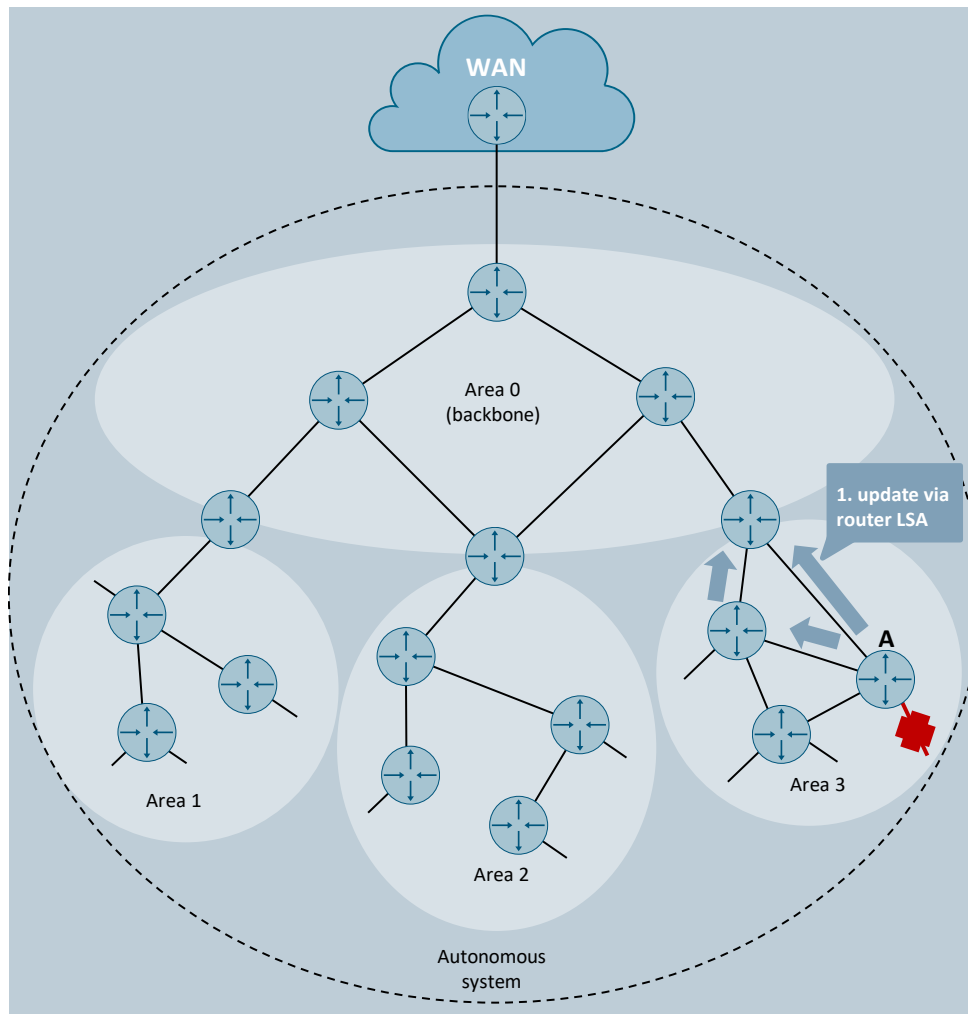
Type-3 summary LSAs describe paths to networks, while type-4 summary LSAs describe paths to ASBRs.

Type 5: AS-external LSA

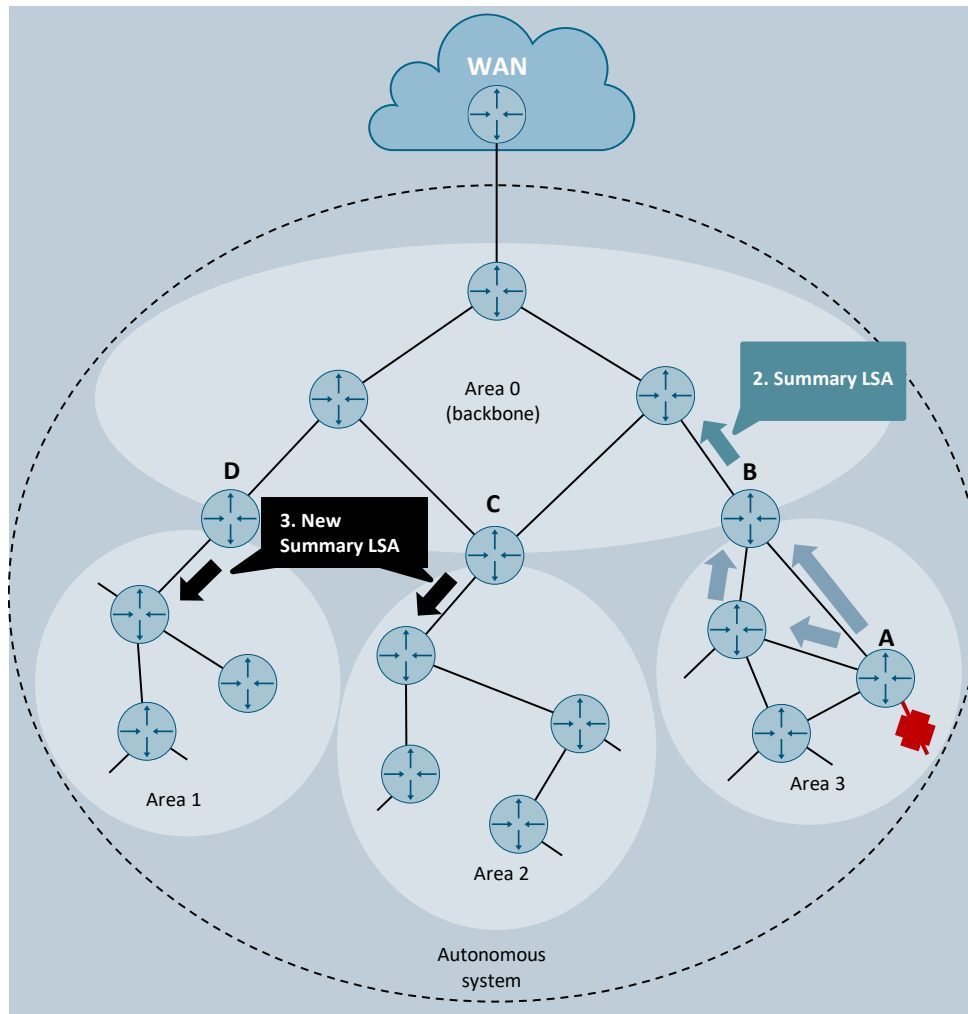
Generated and distributed by ASBRs. These describe paths to destinations outside of the autonomous system (AS). An AS-external LSA can describe a default route for the AS.

4.5.1.2 Example: Update for a link change

Figure 4-16



An IP interface of OSPF Router A in area 3 becomes inactive due to a cable break. Router A informs all routers with which it has "Full" neighbor state about the change by means of a router LSA.



Summary LSA for area 0

Router B is an Area Border Router to area 0. Their task is to propagate the changes to the other areas with a summary LSA.

Summary LSA for area 0.0.0.2 and area 0.0.0.3

The routers of the adjacent area 0 propagate the summary LSA from Router B. Routers C and D are themselves ABRs and prepare the new information in a summary LSA for area 0.0.0.2.

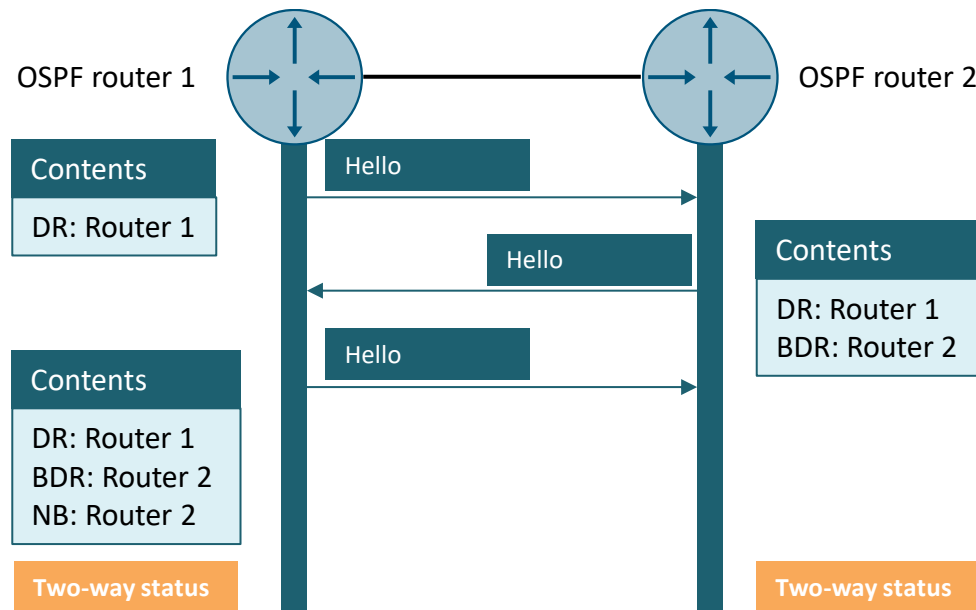
4.6 OSPF sequence

4.6.1.1 Start of neighbor adjacency and selection of the Designated Router

Structure of the neighborhood relationship

In OSPF, information is always passed from router to router. Therefore, neighborhood relationships are essential. Communication unfolds in multiple steps. The structure of the neighborhood relationship comes first.

Figure 4-17



OSPF Router 1: Send OSPF Hello packet

An OSPF Router 1 sends cyclic OSPF Hello packets on its OSPF interfaces. These packets are sent to IP address 224.0.0.5 as IP multicasts. These OSPF Hello packets contain all configuration parameters for the router for this interface. The first router on the network sets itself as the Designated Router and enters this decision in the OSPF Hello packet.

OSPF Router 2: Receive an OSPF Hello packet

OSPF Router 2 receives this Hello packet and declares itself the Backup Designated Router. Because it has already seen a Hello packet from the first router, it enters this in the neighborhood list.

OSPF Router 2: Send OSPF Hello packet

Using its information, OSPF Router 2 itself generates an OSPF Hello packet and sends it to its interface.

The "Two-Way" neighborhood state

If a router receives an OSPF Hello packet from another router, the first router will recognize the second as a neighbor. If the router in question is itself in the list of known neighbors in the packet, then the state of the neighborhood relation is "Two-Way". The routers are full-status neighbors and further information exchange can take place.

Discovering neighbors with the HELLO protocol

Once a router starts up, it sends a so-called "Hello" message via Broadcast, then receives the Hello messages of the other available routers in the area. A new router thus discovers which neighbors it has and what the connection state to them is.

The Hello protocol is responsible for:

- sending Keepalives at specified intervals (thus confirming that the neighbor router is still working and its routes are still valid)
- discovering a newly added neighbor router
- negotiating parameters such as Hello and Dead timer intervals
- selecting a Designated Router (DR) and a Backup DR

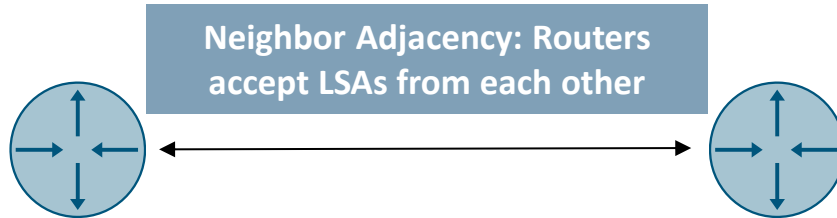
In order for routers to build their routing tables, all routers must declare the networks. OSPF uses Hello packets for this step in building the routing table. This allows the routers to assemble their neighborhood relations. Neighborhood messages are sent periodically.

The Hello protocol exchanges various pieces of information. These include the subnet mask and the Dead timer interval, an area ID, authentication (if enabled), a stub area, and an MTU (Maximum Transmission Unit).

OSPF Hello parameter verification

The following parameters must match in order for Neighbor Adjacency to be fulfilled with the Hello protocol.

Figure 4-18



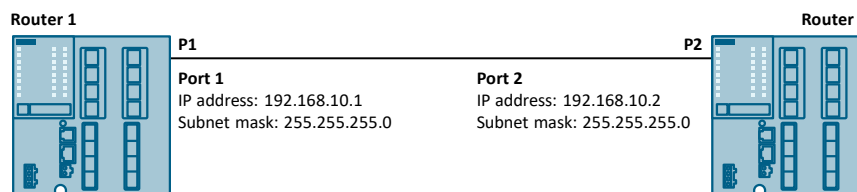
Before OSPF routers can exchange state information via interfaces, they must establish a neighborhood relationship, known as a Neighbor Adjacency. This requires proper configuration of important parameters – such as the Area Identifier, authentication type (if configured), IP address and subnet mask of the link – on all neighboring routers.

If the parameters match, the routers will synchronize their Link State Database and form an adjacency. From this point onward, they will accept routing information (Link State Updates) from each other.

This procedure prevents incorrectly configured OSPF routers from adding their information to the network. The following conditions must be fulfilled:

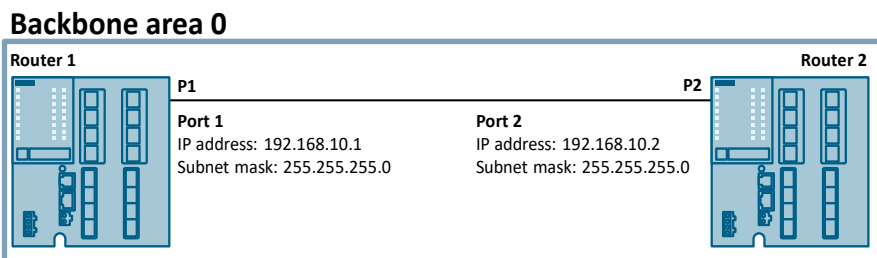
1. OSPF neighbors must be in the same IPv4 subnet.

Figure 4-19



2. OSPF neighbors must be located in the same area or have the same area type.

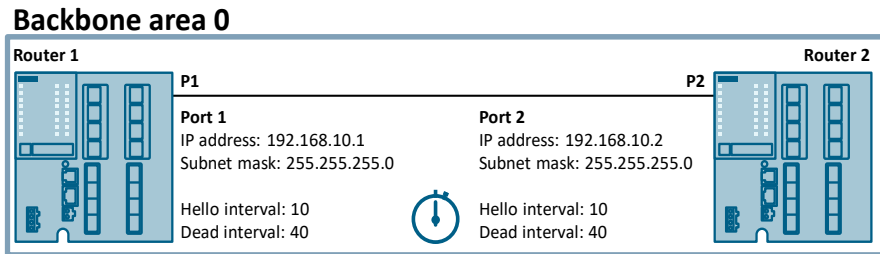
Figure 4-20



With OSPF, the devices must be in the same area and agree on the same type. This will be addressed below.

- The timers for the Hello interval and Dead interval must match. With a Hello Interval, a router sends Hello messages via its interface. The Dead timer determines a time after which no more Hello packets come from a router and the neighboring router is considered to have failed. In the default settings of the SCALANCE, the Dead timer is 4 times the Hello timer.

Figure 4-21



OSPF timers can be set incorrectly or specified incorrectly by the area. The Hello packet sets the time interval within which it is possible for both recipients to receive Hello messages. The Dead Interval defines the point after which a connection is interrupted.

- The same authentication parameters must be configured on both routers.
OSPF supports authentication via interfaces. This is intended to prevent unwanted tampering with the routing information. As a result, only neighboring devices that know each other can establish a neighborhood relation.

OSPF supports 2 authentication mechanisms:

Authentication mechanisms: Either a 64-bit password or a signature of the packets together with a shared secret that every router knows (e.g. using the MD5 algorithm).

- Each device requires a unique Router ID (RID).

Figure 4-22

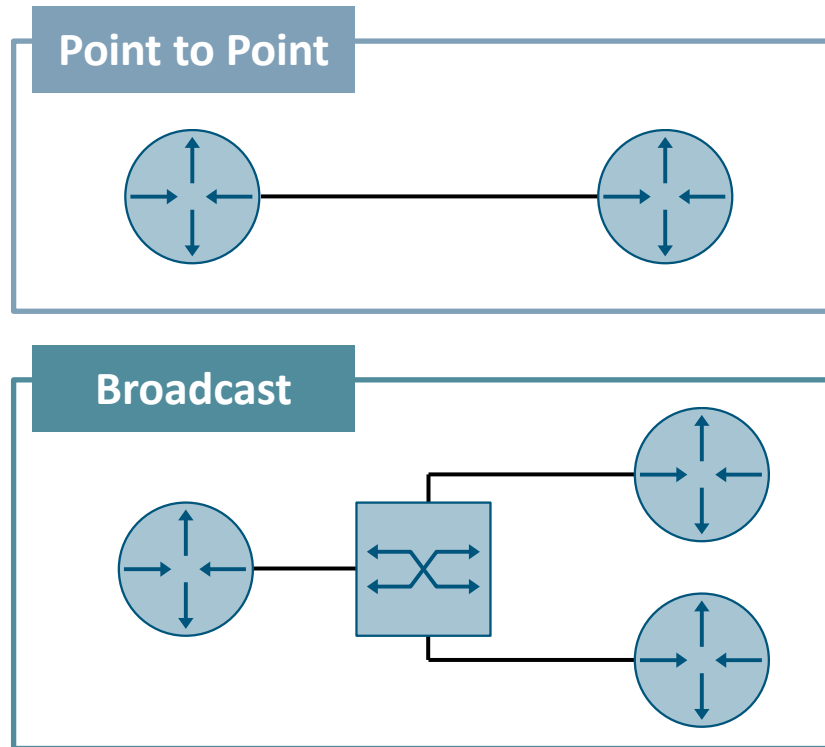


In the OSPF protocol, a way must be found to uniquely identify Router A and Router B. Every OSPF router must therefore have a unique Router ID. It is a 32-bit value, written like an IP address in the format XXX.XXX.XXX.XXX. Here, X stands for a decimal value between 1 and 255. The Router ID can be chosen freely, but it must be unique.

DR and BDR

When establishing a neighborhood relation, it matters whether it is a point-to-point connection or if a switch (broadcast) is in the middle to connect multiple routers with each other.

Figure 4-23



Neighbor Adjacency in layer 2 broadcast networks with multiple access

In a layer 2 network in which multiple OSPF routers are connected, the OSPF routers would have to create a Neighbor Adjacency for every directly accessible OSPF router. If a link state were updated, every router would have to inform every other router about the change. These updates would be redundant and would create an unnecessary load in the network.

The following formula demonstrates how the number of neighborhood relations increases as the number of routers grows.

$$\text{OSPF Adjacencies Formula} = [n*(n-1)]/2$$

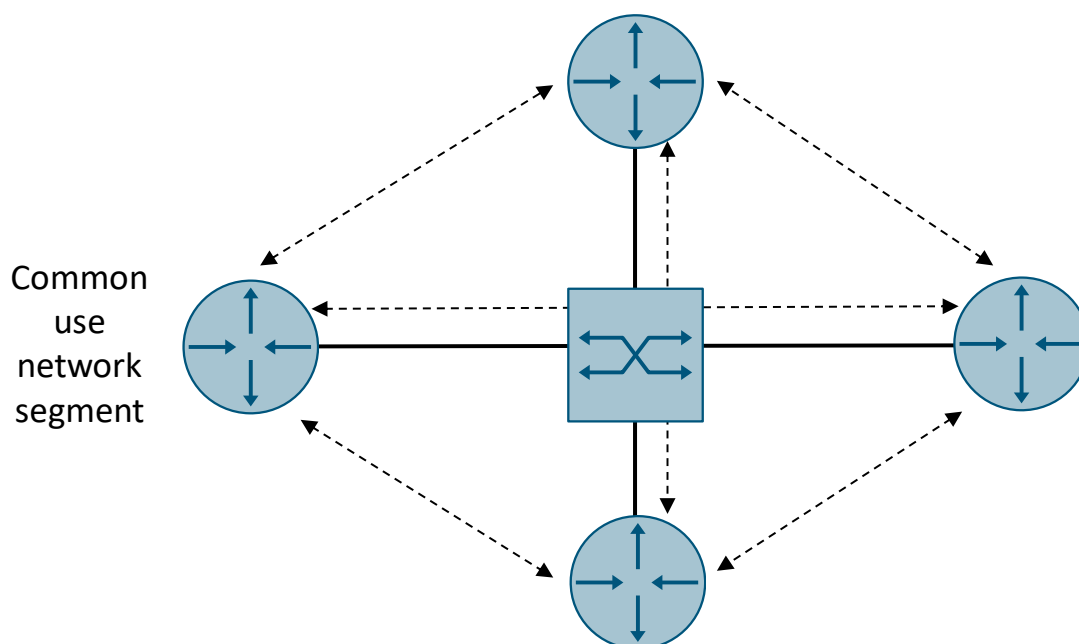
With 4 routers,

$$[4*(4-1)]/2 = 6 \text{ relations would have to be exchanged.}$$

With just 10 routers,

$$[10*(10-1)]/2 = 45 \text{ relations would have to be exchanged}$$

Figure 4-24



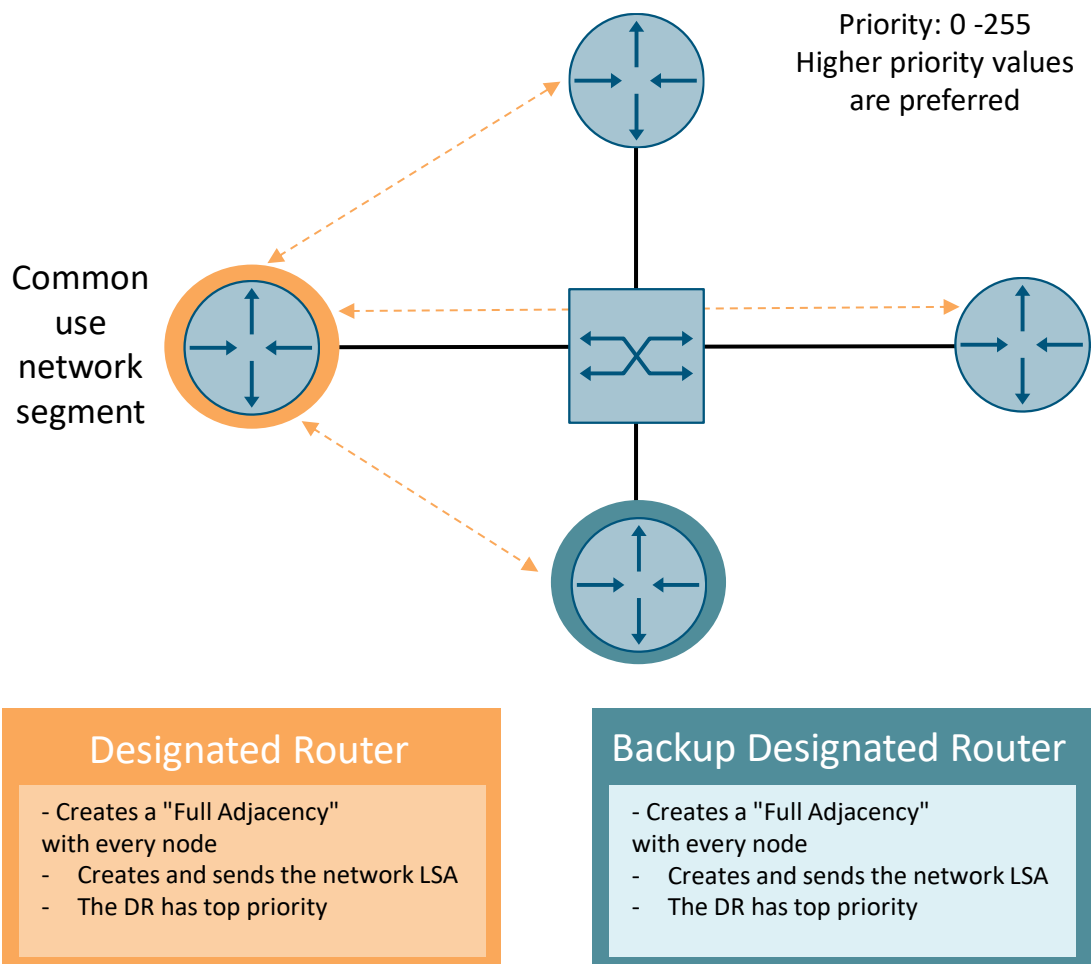
The solution: Designated Routers (DRs) and Backup Designated Routers (BDRs)

When setting up a Neighbor Adjacency, a Designated Router and a Backup Designated Router must be selected. The DR determines the Neighbor Adjacency with all routers in a layer 2 network segment; it ensures that the information from the individual routers is shared with all other routers in this network segment.

The BDR takes over this responsibility if the DR fails. For the switchover to happen quickly, the BDR must also determine the Neighbor Adjacencies. When the DR and BDR determine the Neighbor Adjacency, the advantage is that the rest of the routers do not need to carry out this process.

If the link state of a router changes, only the DR and BDR need to be informed. The Designated Router informs all other routers in the network in the form of a network LSA.

Figure 4-25

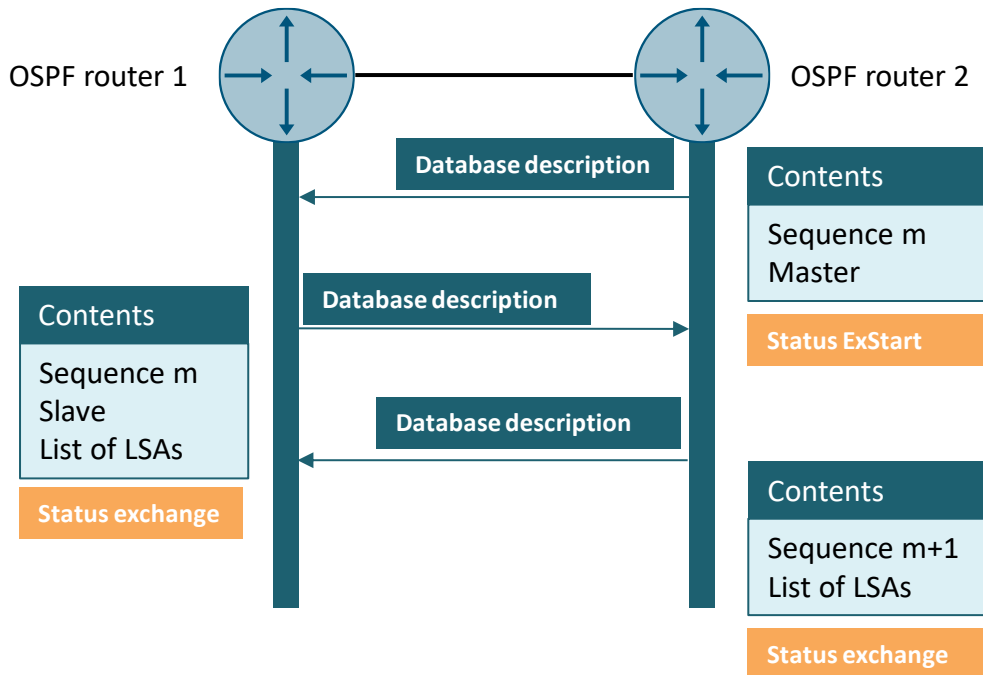


4.6.1.2 One-time database synchronization

Database exchange

Once the neighborhood relation attains "Two-Way" status, further actions can commence. If one of the two routers is a DR or BDR, then the database is synchronized between the two. One can say the "Adjacency" has been "formed".

Figure 4-26

**Exchange of Database Description Packets**

First, the routers synchronize their LSDBs. The routers detect that they should synchronize databases if and only if one of the two routers is a DR or BDR. They set their neighborhood state to "EXStart" and send a Database Description Packet, in which each declares itself the master of the exchange. The OSPF router with the highest Router ID then becomes the actual master.

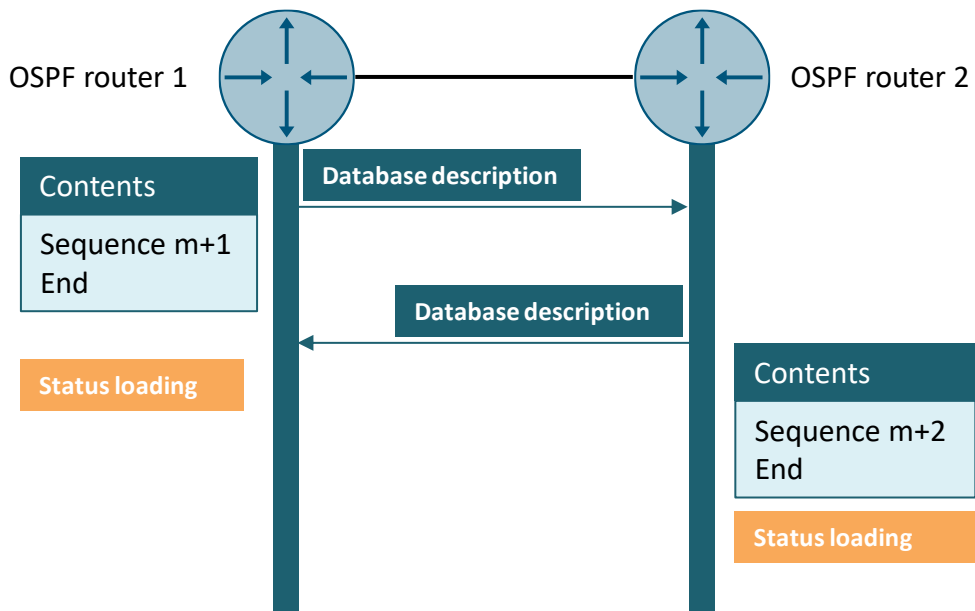
Sending LSA headers

The slave accepts the sequence number and sends a part of the table of contents of its LSDB as part of the confirmation. For the master, receipt is equivalent to confirmation. It counts up the sequence number and similarly starts filling the packet with a table of contents of its LSDB.

End of database exchange

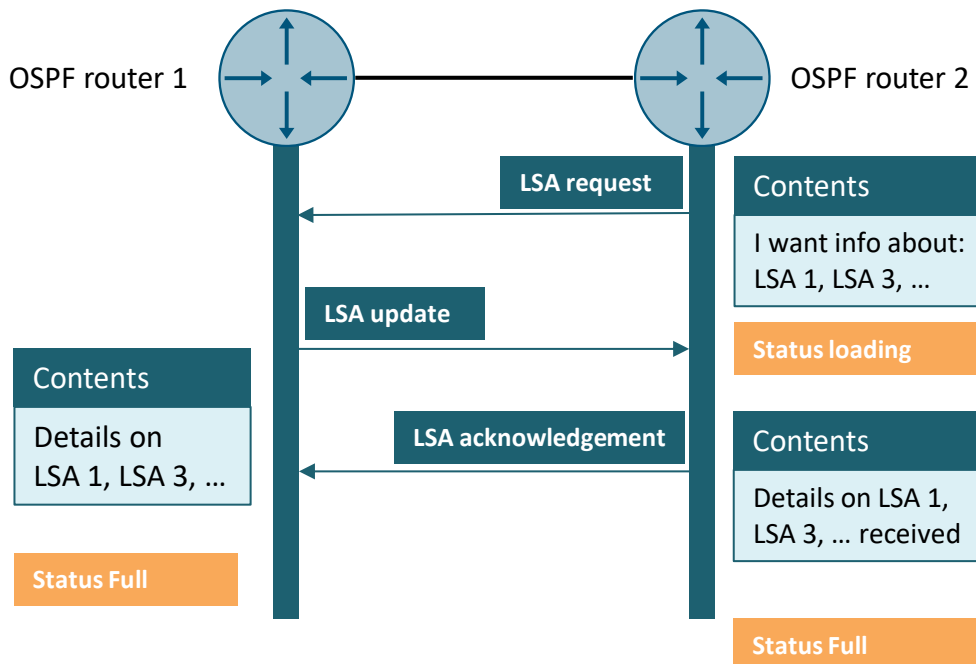
Once all tables of contents have been sent, both routers independently transmit an empty packet and place an end marker (deleted More bit). If both packets are empty, the database exchange is complete. The neighborhood state changes to the state "Loading".

Figure 4-27



4.6.1.3 End of synchronization

Figure 4-28

**LSA request**

By exchanging the Database Description Packets, both routers know which LSAs are in the other router. If one of the routers does not recognize certain entries, it must query them from a neighbor. This is done by sending an LSA request. This request contains the LSAs from which the router wishes to query more information. If the requests do not fit in a packet, multiple packets are sent.

LSA update

The router being contacted works through the LSA requests in order. It looks for the matching information in its own database, from which it compiles one or more LSA update packets.

LSA acknowledgement

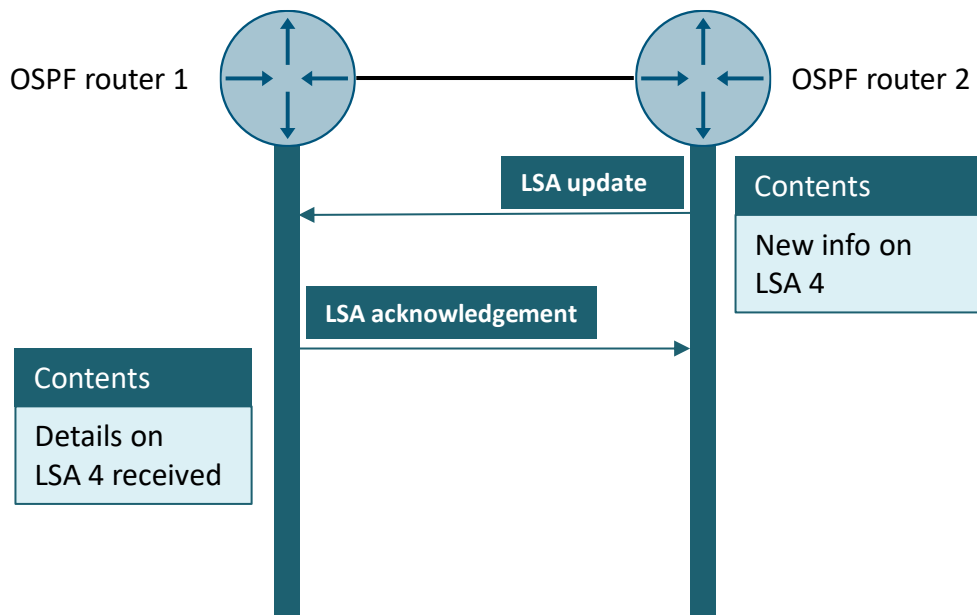
Each individual LSA must be confirmed by the receiving side. For this to happen, an LSA acknowledgement is populated with a list of LSAs requiring confirmation, then sent back.

Neighborhood state "Full"

The neighborhood state "Full" has now been reached, as the complete LSDB has now been initially synchronized.

4.6.1.4 Database updates always occur with acknowledgment.

Figure 4-29

**Online LSA update**

During operation, it may be necessary to refresh LSAs. This is the case, for example, when IP interfaces become inactive because new interfaces receive IPs. If a router generates a new LSA itself or is transmitted one by another router, it will check whether it must send it onward to its neighbors. This process uses the same packet formats as with the initial database exchange.

LSA update

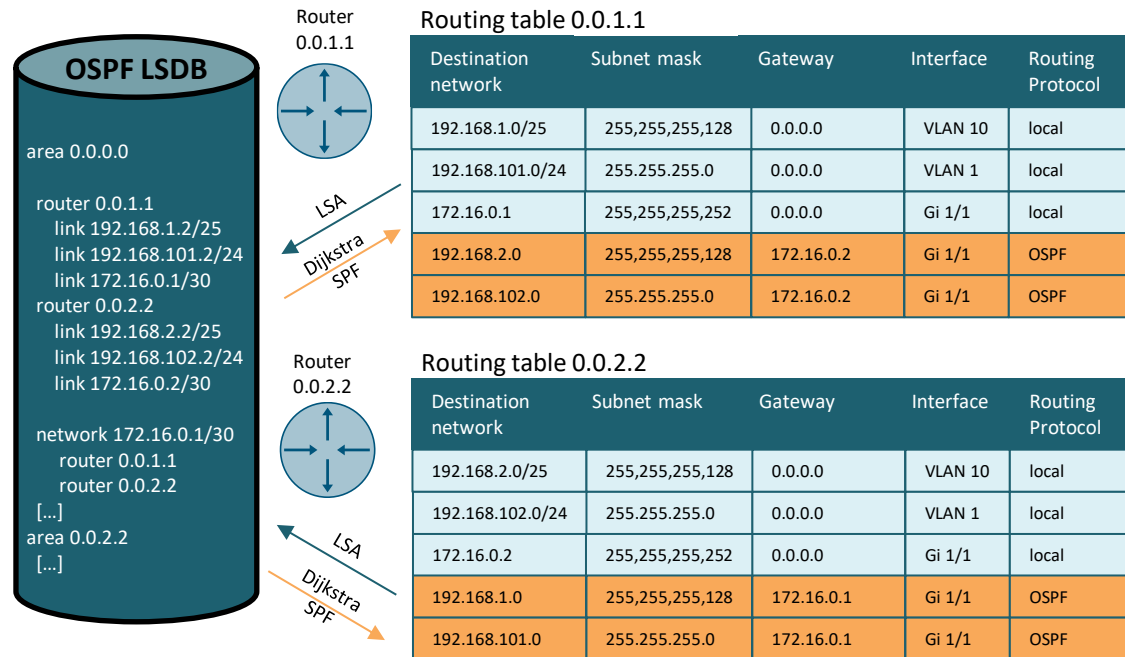
If the router is in the "Full" state with a neighbor, it sends the neighbor an LSA update packet, thereby sharing the new information with the neighbor.

LSA acknowledgement

The neighbor confirms receipt of the information with an LSA acknowledgement packet.

4.6.1.5 Routing table calculation

Figure 4-30



Every router saves the information from received Link State Advertisements (LSAs) in the Link State Database (LSDB). Since these are synchronized within an area, all routers in an area have access to the same LSDB. If a router is a member of multiple areas in the role of ABR, it will save the link states of the different areas in its LSDB.

In the event of changes, every router uses the Dijkstra SPF algorithm to calculate its local routing table. This ensures that a loop-free routing path with the lowest cost is found.

5 Appendix

5.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

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

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

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

support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts.

Please send queries to Technical Support via Web form:

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

Service offer

Our range of services includes the following:

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

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support App

You will receive optimum support wherever you are with the "Siemens Industry Online Support" APP. The app is available for iOS and Android:

support.industry.siemens.com/cs/ww/en/sc/2067

5.2 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

5.3 Links and literature

Table 5-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to this entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/109808195
\3\	SINEC PNI https://support.industry.siemens.com/cs/ww/en/view/109804190
\4\	PRONETA https://support.industry.siemens.com/cs/ww/en/view/67460624
\5\	SCALANCE XM-400/XR-500 manual https://support.industry.siemens.com/cs/at/en/view/109780065

5.4 Change documentation

Table 5-2

Version	Date	Modifications
V1.0	06/2023	First version