HIRSCHMANN

A BELDEN BRAND

# User Manual

## Routing Configuration
## Industrial ETHERNET (Gigabit-)Switch
## PowerMICE, MACH 104, MACH 1040, MACH 4000

UM Routing L3P
Release 8.0 05/2013

Technical Support
https://hirschmann-support.belden.eu.com

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Rel. 8.0 - 05/2013 – 29.04.2013

# Contents

# About this Manual

The “Routing Configuration User Manual” document contains the information you need to start operating the routing function. It takes you step-by-step from a small router application through to the router configuration of a complex network.
The manual enables you to configure your router by following the examples.

The “Routing Configuration” user manual requires you to be familiar with the content of the “Basic Configuration” user manual.

You can use this manual to configure simple networks without any special knowledge. The configuration of complex networks requires well-founded knowledge on the subject of routing and of the protocols IP, RIP, OSPF, IGMP and VRRP.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Basic Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Redundancy Configuration” user manual document contains the information you require to select the suitable redundancy procedure and configure it.

The “Industry Protocols” user manual describes how the device is connected by means of a communication protocol commonly used in the industry, such as  EtherNet/IP and PROFINET IO.

You will find detailed descriptions of how to operate the individual functions in the “Web-based Interface” and “Command Line Interface” reference manuals.

The Industrial HiVision Network Management Software provides you with additional options for smooth configuration and monitoring:

- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- Auto-topology discovery
- Event log
- Event handling
- Client/server structure
- Browser interface
- ActiveX control for SCADA integration
- SNMP/OPC gateway.

**Maintenance**

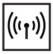
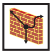
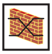
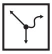
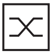
Hirschmann is continually working to improve and develop our software. You should regularly check whether there is a new version of the software that provides you with additional benefits. You will find software information and downloads on the product pages of the Hirschmann website.

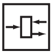
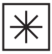
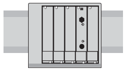
# Key

The designations used in this manual have the following meanings:

| | |
|---|---|
| ▶ | List |
| □ | Work step |
| ■ | Subheading |
| Link | Cross-reference with link |
| **Note:** | A note emphasizes an important fact or draws your attention to a dependency. |
| `Courier` | ASCII representation in user interface |
| 🟪 | Execution in the Graphical User Interface |
| 🟩 | Execution in the Command Line Interface |

Symbols used:

| | |
|---|---|
|  | WLAN access point |
|  | Router with firewall |
|  | Switch with firewall |
|  | Router |
|  | Switch |

| | |
|---|---|
|  | Bridge |
|  | Hub |
| | A random computer |
| | Configuration Computer |
| | Server |
|  | PLC -<br>Programmable logic controller |
| | I/O -<br>Robot |

# 1 Configuration

Because the configuration of a router is very dependent on the conditions in your network, you are first provided with a general list of the individual configuration steps. To optimally cover the large number of options, this list is followed by examples of networks that usually occur in the industry sector. The examples are selected so that the configurations for other applications can be easily derived from them.

The configuration of the routing function usually contains the following steps:

□ Drawing a network plan
Create a picture of your network so that you can clearly see the division into subnetworks and the related distribution of the IP addresses.
This step is very important. Good planning of the subnetworks with the corresponding network masks makes the router configuration much easier.

□ Router basic settings
Along with the global switching on of the routing function, the router basic settings also contain the assignment of IP addresses and network masks to the router interfaces.

**Note:** Adhere to the sequence of the individual configuration steps so that the configuration computer has access to all the layer 3 Switches throughout the entire configuration phase.

**Note:** When you assign an IP address from the subnetwork of the management IP address to a router interface, the Switch deletes the management IP address. You access the Switch via the IP address of the router interface.
Activate the routing globally before you assign an IP address from the subnetwork of the management IP address to a router interface.

**Note:** When you assign the VLAN ID of the management VLAN to a router interface, the Switch deactivates the management IP address. You access the Switch via the IP address of the router interface. The management VLAN is the VLAN by means of which you access the management of all the Switches.

**Note:** Depending on your configuration steps, it may be necessary to change the IP parameters of your configuration computer to enable access to the layer 3 Switches.

☐ Selecting a routing procedure
On the basis of the network plan and the communication requirements of the connected devices, you select the optimal routing procedure (static routes, RIP, OSPF) for your situation. In doing so, consider which routing procedures the routers can use along a route.

☐ Configuring a routing procedure
Configure the selected routing procedure.

# 2 Routing - Basics

A router is a node for exchanging data on the layer 3 of the ISO/OSI layer model.
This ISO/OSI reference model had the following goals:

- To define a standard for information exchange between open systems;
- To provide a common basis for developing additional standards for open systems;
- To provide international teams of experts with functional framework as the basis for independent development of every layer of the model;
- To include in the model developing or already existing protocols for communications between heterogeneous systems;
- To leave sufficient room and flexibility for the inclusion of future developments.

The reference model consists of 7 layers, ranging from the application layer to the physical layer.

| | | |
|---|---|---|
| 7 | Application | Access to communication services from an application program |
| 6 | Presentation | Definition of the syntax for data communication |
| 5 | Session | Set up and breakdown of connections by synchronization and organization of the dialog |
| 4 | Transport | Specification of the terminal connection, with the necessary transport quality |
| 3 | Network | Transparent data exchange between two transport entities |
| 2 | Data-Link | Access to physical media and detection of transmission errors |
| 1 | Physical | Transmission of bit strings via physical media |

*Table 1: OSI Reference Model*

What does the data exchange on the layer 3 mean in comparison with the data exchange on the layer 2?

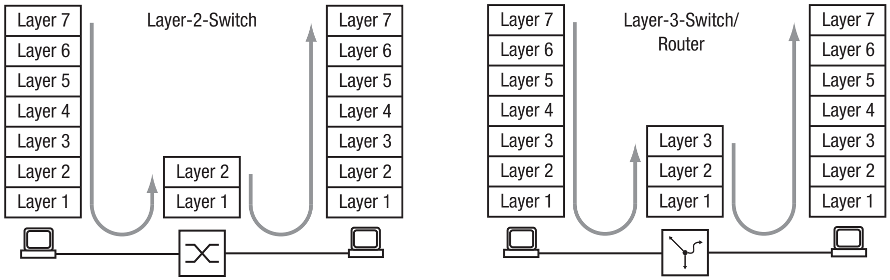


*Figure 1: Data Transport by a Switch and a Router in the OSI Reference Model's Layers*

On the layer 2, the MAC address signifies the destination of a data packet. The MAC address is an address tied to the hardware of a device. The layer 2 expects the receiver in the connected network. The data exchange to another network is the task of layer 3. Layer 2 data traffic is spread over the entire network. Every subscriber filters the data relevant for him from the data stream. Layer 2 switches are capable of steering the data traffic that is intended for a specific MAC address. It thus relieves some of the load on the network. Broadcast and multicast data packets are forwarded by the layer 2 switches at all ports.

IP is a protocol on the layer 3. IP provides the IP address for addressing data packets. The IP address is assigned by the network administrator.
By systematically assigning IP addresses, he can thus structure his network, breaking it down into subnets (see on page 19 "CIDR"). The bigger a network gets, the greater the data volume. Because the available bandwidth has physical limitations, the size of a network is also limited. Dividing large networks into subnets limits the data volume on these subnets. Routers divide the subnets from each other and only transmit the data that is intended for another subnet.

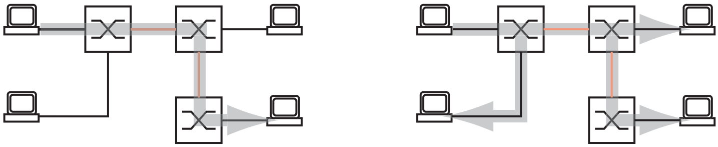


*Figure 2: MAC Data Transmission: Unicast Data Packet (left) and Broadcast Data Packet (right)*

This illustration clearly shows that broadcast data packets can generate a considerable load on larger networks. You also make your network easier to understand by forming subnets, which you connect with each other using routers and, strange as it sounds, also separate securely from each other.

A Switch uses the MAC destination address to transmit, and thus uses layer 2.
A router uses the IP destination address to transmit, and thus uses layer 3.
The subscribers associate the MAC and IP addresses using the Address Resolution Protocol (ARP).

# 2.1 ARP

The Address Resolution Protocol (ARP) determines the MAC address that belongs to an IP address. What is the benefit of this?

Let's suppose that you want to configure your Switch using the Web-based interface. You enter the IP address of your Switch in the address line of your browser. But which MAC address will your PC now use to display the information in the Switch in your browser window?

If the IP address of the Switch is in the same subnet as your PC, then your PC sends what is known as an ARP request. This is a MAC broadcast data packet that requests the owner of the IP address to send back his MAC address. The Switch replies with a unicast data packet containing his MAC address. This unicast data packet is called an ARP reply.

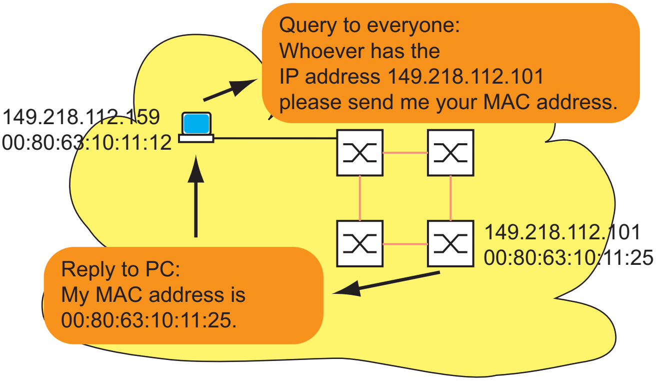


*Figure 3: ARP request and reply*

If the IP address of the Switch is in a different subnet, then the PC asks for the MAC address of the gateway entered in the PC. The gateway/router replies with its MAC address.
Now the PC packs the IP data packet with the IP address of the switch, the final destination, into a MAC frame with the MAC destination address of the gateway/router and sends the data.
The router receives the data and releases the IP data packet from the MAC frame, so that it can then forward it in accordance with its transmission rules.

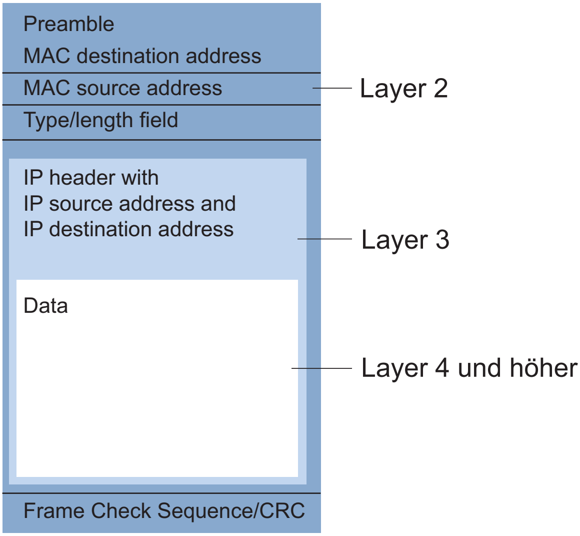


*Figure 4: Structure of a data packet from the ISO/OSI layer model perspective*

All terminal devices still working with IPs of the first generation, for example, are not yet familiar with the term 'subnet'. They also send an ARP request when they are looking for the MAC address for an IP address in a different subnet. They neither have a network mask with which they could recognize that the subnet is a different one, nor do they have a gateway entry. In the example below, the left PC is looking for the MAC address of the right PC, which is in a different subnet. In this example, it would normally not get a reply.

Because the router knows the route to the right PC, the proxy ARP function replies to this router interface on behalf of the right PC with its own MAC address. Thus the left PC can address its data to the MAC address of the router, which then forwards the data to the right PC.

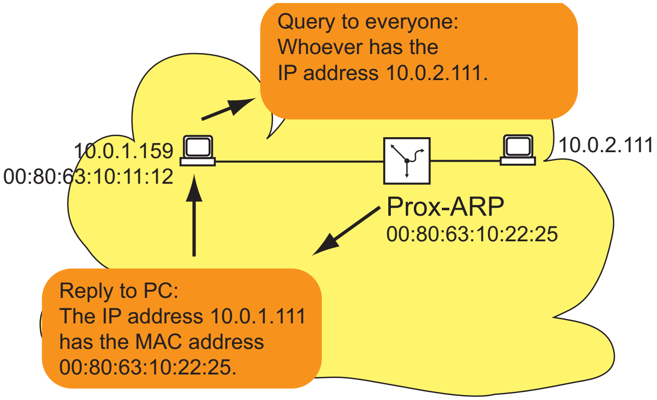


*Figure 5: ARP proxy funktion*

The proxy ARP function is available on the router interfaces on which you switch on the proxy ARP.

## 2.2 CIDR

The original class allocation of the IP addresses only planned for three address classes to be used by the users (see “Basics of IP Parameters” in the basic configuration of the user manual).

Since 1992, five classes of IP address have been defined in the RFC 1340.

| Class | Network part | Host part | Address range |
|---|---|---|---|
| A | 1 byte | 3 bytes | 1.0.0.0 to 126.255.255.255 |
| B | 2 bytes | 2 bytes | 128.0.0.0 to 191.255.255.255 |
| C | 3 bytes | 1 byte | 192.0.0.0 to 223.255.255.255 |
| D | | | 224.0.0.0 to 239.255.255.255 |
| E | | | 240.0.0.0 to 255.255.255.255 |

*Table 2: IP address classes*

Class C with a maximum of 254 addresses was too small, and class B with a maximum of 65534 addresses was too large for most users, as they would never require so many addresses. This resulted in ineffective usage of the class B addresses available.
Class D contains reserved multicast addresses. Class E is reserved for experimental purposes. A gateway not participating in these experiments ignores datagrams with this destination address.
The Classless Inter-Domain Routing (CIDR) provides a solution to these problems. The CIDR overcomes these class boundaries and supports classless address ranges.

With CIDR, you enter the number of bits that designate the IP address range. You represent the IP address range in binary form and count the mask bits that designate the network mask. The network mask indicates the number of bits that are identical for all IP addresses, the network part, in a given address range. Example:

| IP address, decimal | Network mask, decimal | IP address, binary |
|---|---|---|
| 149.218.112.1 | 255.255.255.128 | `10010101 11011010 01110000 00000001` |
| 149.218.112.127 | | `10010101 11011010 01110000 01111111` |
| | | 25 mask bits |

CIDR notation: 149.218.112.0/25

Mask bits

The combination of a number of class C address ranges is known as “supernetting”. This enables you to subdivide class B address ranges to a very fine degree.

Using mask bits simplifies the routing table. The router determines in that direction in which most of the mask bits match (longest prefix match).

## 2.3 Net-directed Broadcasts

A net-directed Broadcast is an IP data packet that a device sends to the network Broadcast address[1] of a network to contact all the receivers of the network. A net-directed Broadcast is sent as a MAC Unicast frame in a transfer network. If the router locally responsible for this network supports net-directed Broadcasts, then it transmits this data packet as a MAC Broadcast frame into its local network. With VLAN-based router interfaces it transmits the frame to all the ports that are members in the VLAN of the Router interface.

Thus net-directed Broadcasts can relieve your transfer network of the multiple IP Unicasts that would be necessary to replace a net-directed Broadcast.

If the router does not support net-directed Broadcasts or if you switch off this function for a router interface, the router discards IP data packets received at the network Broadcast address of the router interface. With multinetting, this also applies to the secondary IP addresses of the router interface.

[1] The network Broadcast address is the highest IP address of an IP network for which a router interface is responsible. The device determines the Broadcast address from its interface IP address and the related netmask. For example, if a router interface has the IP address 192.168.1.1 and the netmask 255.255.255.0, it is responsible for network 192.168.1.0/24. The network Broadcast address here is 192.168.1.255.

# 2.4 Multinetting

Multinetting allows you to connect a number of subnets to one router port. Multinetting provides a solution for when you want to connect existing subnets to a router within a physical medium. In this case you can use multinetting to assign a number of IP addresses for the different subnets to the routing port to which you are connecting the physical medium.

For a long-term solution, other network design strategies provide more advantages with regard to problem solving and bandwidth management.

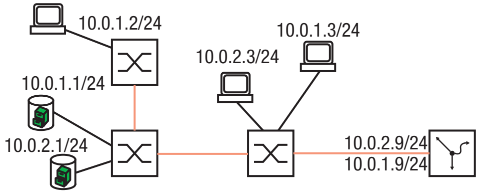


*Figure 6: Example of multinetting*

# 3 Static Routing

Static routes are user-defined routes which the Switch uses to transmit data from one subnet to another.
The user specifies to which router (next hop) the Switch forwards data for a particular subnet. Static routes are kept in a table which is permanently stored in the Switch.

Compared to dynamic routing, the advantage of this transparent route selection is offset by the increased workload involved in configuring the static routes. Static routing is therefore suited to very small networks or to selected areas of larger networks. Static routing makes the routes transparent for the administrator and can be easily configured in small networks.
If, for example, a line interruption causes the topology to change, the dynamic routing can react automatically to this, in contrast to the static routing. If you combine static and dynamic routing, you can configure the static routes in such a way that they have a higher priority than a route selected by a dynamic routing procedure.

The first step in configuring the router is to globally switch on the router function and configure the router interfaces.
The Switch allows you to define port-based and VLAN-based router interfaces (see figure 7).

Example: Connecting two production cells

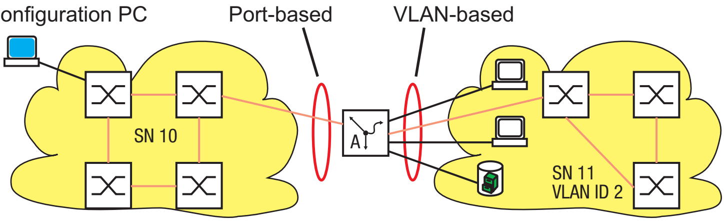


*Figure 7: Static routes*

## 3.1 Port-based Router Interface

A characteristic of the port-based router interface is that a subnet is connected to a port (see figure 7).

Special features of port-based router interfaces:

- If there is no active connection, then the entry from the routing table is omitted, because the router transmits exclusively to those ports for which the data transfer is likely to be successful.
  The entry in the interface configuration table remains.
- A port-based router interface does not recognize VLANs, which means that the router rejects tagged frames which it receives at a port-based router interface.
- A port-based router interface rejects all the non-routable packets.

Below (see figure 8) you will find an example of the simplest case of a routing application with port-based router interfaces.

### 3.1.1 Configuration of the router interfaces

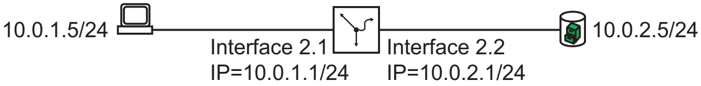


*Figure 8: Simplest case of a route*

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `ip routing` | Switch on the router function globally. |
| `interface 2/1` | Select the first port for entering the router interface IP address. |
| `ip address 10.0.1.1 255.255.255.0` | Assign the port its IP parameters. |
| `routing` | Switch on the router function at this port. |
| `exit` | Switch to the Configuration mode. |
| `interface 2/2` | Select the second port for entering the router interface IP address. |
| `ip address 10.0.2.1 255.255.255.0` | Assign the port its IP parameters. |
| `routing` | Switch on the router function at this port. |
| `ip netdirbcast` | Einschalten der Vermittlung von Netdirected Broadcasts an diesem Port. |
| `exit` | Switch to the Configuration mode. |
| `exit` | Switch to the privileged EXEC mode. |
| `show ip interface brief` | Check the entries. |

```
                                                Netdir    Multi
Interface IP Address       IP Mask              Bcast     CastFwd
--------- ---------------- ---------------- --------- ---------
2/1       10.0.1.1         255.255.255.0    Disable   Disable
2/2       10.0.2.1         255.255.255.0    Enable    Disable
```

| | |
|---|---|
| `show ip interface 2/1` | Check the remaining settings for interface 2/1. |

```
Primary IP Address.......... ............ 10.0.1.1/255.255.255.0
Routing Mode.............................  Enable
Administrative Mode...................... Enable
Forward Net Directed Broadcasts.......... Enable
Proxy ARP................................ Disable
Active State............................. Active
Link Speed Data Rate..................... 100 Full
MAC Address.............................. 00:80:63:51:74:0C
Encapsulation Type....................... Ethernet
IP MTU................................... 1500
```

```
show ip route
```

Verify the routing table:

```
Total Number of Routes......................... 2
   Network          Subnet                      Next Hop    Next Hop
   Address           Mask          Protocol      Intf      IP Address
--------------- --------------- ------------  ------   ------------
10.0.1.0        255.255.255.0   Local          2/1       10.0.1.1
10.0.2.0        255.255.255.0   Local          2/2       10.0.2.1
```

```
show ip route bestroutes
```

Check which routes the router actually uses for the transmission.

```
   Network           Subnet                      Next Hop    Next Hop
   Address            Mask          Protocol      Intf     IP Address
---------------  ---------------  -----------  ---------  --------
10.0.1.0          255.255.255.0    Local        2/1        10.0.1.1
10.0.2.0          255.255.255.0    Local        2/2        10.0.2.1

Total Number of Routes......................... 2
```

**Note:** To be able to see these entries in the routing table, you need an active connection at the ports.

# 3.2 VLAN-based Router-Interface

A characteristic of the VLAN-based router interface is that a number of devices in a VLAN are connected to different ports. The devices within a subnet belong to one VLAN (see figure 7).

Within a VLAN, the Switch exchanges data packets on layer 2.
Terminal devices address data packets with a destination address in another subnet to the router as a gateway. The router then exchanges the data packets layer 3.

Below  you will find an example of the simplest case of a routing application with VLAN-based router interfaces. For the VLAN 2, the router combines ports 3.1 and 3.2 into the VLAN router interface 9.1. A VLAN router interface remains in the routing table until at least one port of the VLAN has a connection.

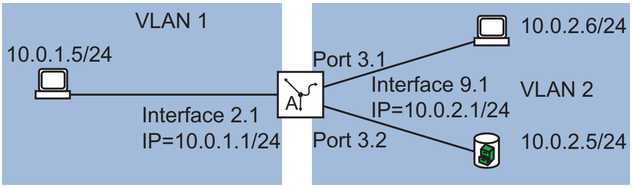


*Figure 9: VLAN-based router interface*

Configuring a VLAN router interface:

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `vlan database` | Switch to the VLAN mode. |
| `vlan 2` | Create a VLAN by entering the VLAN ID. The VLAN ID is between 1 and 4,042 (MACH 4000: 3,966). |
| `vlan name 2 Gerhard` | Assign the name “Gerhard” to VLAN 2. |
| `vlan routing 2` | Create a virtual router interface and activate the router function at this interface. |
| `exit` | Switch to the privileged EXEC mode. |

| | |
|---|---|
| `show ip vlan` | Display the virtual router interface that the router has set up for the VLAN. |

```
show ip vlan
        Logical
VLAN ID Interface  IP Address  Subnet Mask   MAC Address
------- ---------- ----------- ------------- -----------------
2       9/1        0.0.0.0     0.0.0.0       00:80:63:51:74:2C
```

| | |
|---|---|
| `show ip interface brief` | Check the entry for the virtual router interface. |

```
                                                Netdir    Multi
Interface IP Address      IP Mask         Bcast     CastFwd
--------- --------------- --------------- --------- ---------
9/1       0.0.0.0         0.0.0.0         Disable   Disable
```

| | |
|---|---|
| `configure` | Switch to the Configuration mode. |
| `interface 9/1` | Switch to the interface configuration mode of interface 9/1. |
| `ip address 10.0.2.1 255.255.255.0` | Assign the IP parameters to the router interface. |
| `routing` | Activate the router function at this interface. |
| `ip netdirbcast` | Enable the transmission of net-directed broadcasts  for this interface. |
| `exit` | Switch to the Configuration mode. |
| `interface 3/1` | Switch to the interface configuration mode of interface 3/1. |
| `vlan participation include 2` | Declare port 3.1 a member of VLAN 2. |
| `vlan participation exclude 1` | Remove port 3.1 from VLAN 1. In the state on delivery, every port is assigned to VLAN 1. |
| `vlan pvid 2` | Set the port VLAN-ID to 2, which means that data packets that are received without a tag at that port are assigned to VLAN 2 by the Switch. |
| `exit` | Switch to the Configuration mode. |
| `interface 3/2` | Switch to the interface configuration mode of interface 3/2. |
| `vlan participation include 2` | Declare port 3.2 a member of VLAN 2. |
| `vlan participation exclude 1` | Remove port 3.2 from VLAN 1. In the state on delivery, every port is assigned to VLAN 1. |
| `vlan pvid 2` | Set the port VLAN-ID to 2, which means that data packets that are received without a tag at that port are assigned to VLAN 2 by the Switch. |
| `exit` | Switch to the Configuration mode. |
| `exit` | Switch to the privileged EXEC mode. |

```
show vlan 2
```

Check your entries in the static VLAN table.

```
VLAN ID: 2
VLAN Name: Gerhard
VLAN Type: Static

Interface   Current   Configured   Tagging
---------- --------- ------------ --------
1/1         Exclude   Autodetect   Untagged
1/2         Exclude   Autodetect   Untagged
1/3         Exclude   Autodetect   Untagged
1/4         Exclude   Autodetect   Untagged
2/1         Exclude   Autodetect   Untagged
2/2         Exclude   Autodetect   Untagged
2/3         Exclude   Autodetect   Untagged
2/4         Exclude   Autodetect   Untagged
3/1         Include   Include      Untagged
3/2         Include   Include      Untagged
3/3         Exclude   Autodetect   Untagged
3/4         Exclude   Autodetect   Untagged
4/1         Exclude   Autodetect   Untagged
4/2         Exclude   Autodetect   Untagged
4/3         Exclude   Autodetect   Untagged
4/4         Exclude   Autodetect   Untagged
8/1         Exclude   Autodetect   Untagged
```

```
show vlan port all
```

Check the VLAN-specific port settings.

```
          Port    Acceptable   Ingress     Default
Interface VLAN ID Frame Types  Filtering   Priority
--------- ------- ------------ ----------- --------
1/1       1       Admit All    Disable       0
1/2       1       Admit All    Disable       0
1/3       1       Admit All    Disable       0
1/4       1       Admit All    Disable       0
2/1       1       Admit All    Disable       0
2/2       1       Admit All    Disable       0
2/3       1       Admit All    Disable       0
2/4       1       Admit All    Disable       0
3/1       2       Admit All    Disable       0
3/2       2       Admit All    Disable       0
3/3       1       Admit All    Disable       0
3/4       1       Admit All    Disable       0
4/1       1       Admit All    Disable       0
4/2       1       Admit All    Disable       0
4/3       1       Admit All    Disable       0
4/4       1       Admit All    Disable       0
8/1       1       Admit All    Disable       0
```

☐ Select the dialog `Routing:Interfaces:Configuration`.

☐ Click on “Assistant” at the bottom right to configure the VLAN router interface.

☐ Enter a number between 1 and 4,042 (MACH 4000: 3,966) as the VLAN-ID, in this example: 2.

☐ Click on “Next” at the bottom.

☐ n the “VLAN Name” line above, enter a name with which you want to identify the VLAN.

☐ In the “Member” column of the table, you select the ports which will belong to this VLAN.

☐ Click on “Next” at the bottom.

☐ In the “IP Address” line of the “Primary Address” frame, you enter the IP address for the VLAN.

☐ Enter the related network mask in the “Network mask” line.

☐ Click on “Close” to end the configuration of the VLAN-based router interface.

In the router interface table, the router interface 9.1 appears.In the static VLAN table, the VLAN appears.

☐ Tick the box in the column „net-directed broadcasts“ for the router interface 9.1.

With “Delete“, you have the opportunity to delete a selected virtual router interface from the table or to reset a physical router interface‘s entry.

**Note:** When you delete a VLAN router interface, the entry for the VLAN will remain in the VLAN table.
Deleting a VLAN deletes the VLAN router interface‘s entry in the router interface table.

## 3.3 Configuration of a Static Route

In the example below, router A requires the information that it can reach the subnet 10.0.3.0/24 via the router B (next hop). It can obtain this information via a dynamic routing protocol or via a static routing entry. With this information, router A can transmit data from subnet 10.0.1.0/24 via router B into subnet 10.0.3.0/24.

Vice versa to be able to forward data of subnet 10.0.1.0/24 router B also needs an equivalent route.

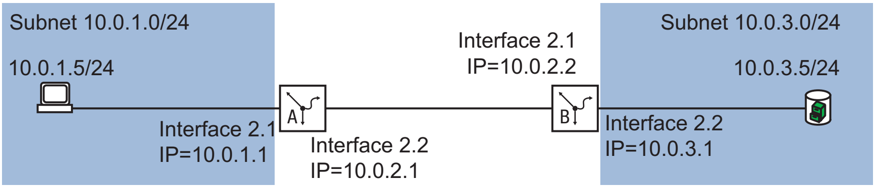


*Figure 10: Static Routing*

You can enter static routing for port-based and VLAN-based router interfaces.

## 3.3.1 Configuration of a simple static route

Enter a static route for router A based on the configuration of the router interface in the previous example (see figure 8):

```
enable                           Switch to the privileged EXEC mode.
configure                        Switch to the Configuration mode.
ip routing                       Switch on the router function globally.
ip route 10.0.3.0                Create the static routing entry
  255.255.255.0 10.0.2.2
exit                             Switch to the privileged EXEC mode.

show ip route                    Verify the routing table:

Total Number of Routes......................... 3

   Network          Subnet                       Next Hop     Next Hop
   Address           Mask          Protocol        Intf      IP Address
--------------- --------------- ------------  ------  -------------
10.0.1.0        255.255.255.0   Local            2/1        10.0.1.1
10.0.2.0        255.255.255.0   Local            2/2        10.0.2.1
10.0.3.0        255.255.255.0   Static           2/2        10.0.2.2
```

☐ Configure router B in the same way.

## 3.3.2 Configuration of a redundant static route

To ensure a reliable connection between the two routers, you can connect the two routers with two or more lines.

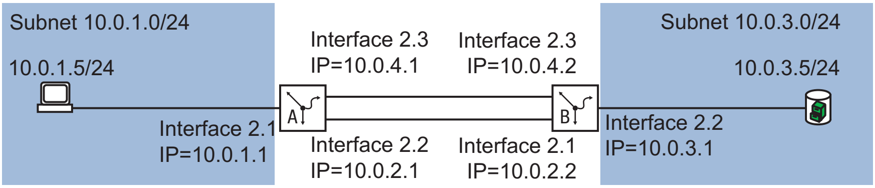


*Figure 11: Redundant static route*

You have the option of assigning importance (distance) to a route. If there are a number of routes to a destination, then the router chooses the route with the highest importance. If you do not assign a value for the importance during the configuration, the router takes the default value “1” for the importance. This is the highest importance.

□ Configure router A.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `interface 2/3` | Select the port at which you want to connect the redundant route. |
| `ip address 10.0.4.1 255.255.255.0` | Assign the port its IP parameters. |
| `routing` | Switch on the router function at this port. |
| `exit` | Switch to the Configuration mode. |
| `ip route 10.0.3.0 255.255.255.0 10.0.4.2` **`2`** | Create the static routing entry for the redundant route. The “2” at the end of the command is the importance value.<br>When both routes are available, the router uses the route via subnetwork 10.0.2.0/24, because this route has the higher importance (default value = 1) (see on page 32 “Configuration of a simple static route”). |

```
show ip route
```

Verify the routing table:

```
Total Number of Routes......................... 5

   Network           Subnet                          Next Hop     Next Hop
   Address            Mask           Protocol         Intf       IP Address
---------------- ---------------- ------------- ------  --------------
10.0.1.0         255.255.255.0    Local           2/1         10.0.1.1
10.0.2.0         255.255.255.0    Local           2/2         10.0.2.1
10.0.3.0         255.255.255.0    Static          2/2         10.0.2.2
10.0.3.0         255.255.255.0    Static          2/3         10.0.4.2
10.0.4.0         255.255.255.0    Local           2/3         10.0.4.1
```

```
show ip route bestroutes
```

Check which routes the router actually uses for the transmission.

```
   Network            Subnet                          Next Hop     Next Hop
   Address             Mask          Protocol          Intf       IP Address
----------------  ----------------  -----------  ---------  ---------
10.0.1.0          255.255.255.0     Local          2/1          10.0.1.1
10.0.2.0          255.255.255.0     Local          2/2          10.0.2.1
10.0.3.0          255.255.255.0     Static         2/2          10.0.2.2
10.0.4.0          255.255.255.0     Local          2/3          10.0.4.1

Total Number of Routes......................... 4
```

☐ Configure router B in the same way.

### 3.3.3 Configuration of a redundant static route with load sharing

The router shares the load between the two routes (load sharing), when the routes have the same importance (distance).

```
ip route 10.0.3.0
255.255.255.0 10.0.2.2 2
```

assign the importance “2” to the existing static routing entry (see on page 32 “Configuration of a simple static route”).
When both routes are available, the router uses both routes for the data transmission.

```
show ip route
```

Verify the routing table:

```
Total Number of Routes......................... 4

    Network            Subnet                         Next Hop     Next Hop
    Address             Mask          Protocol          Intf      IP Address
--------------- --------------- ------------  ------  -------------
10.0.1.0         255.255.255.0   Local           2/1       10.0.1.1
10.0.2.0         255.255.255.0   Local           2/2       10.0.2.1
10.0.3.0         255.255.255.0   Static          2/2       10.0.2.2
                                                 2/3       10.0.4.2
10.0.4.0         255.255.255.0   Local           2/3       10.0.4.1
```

```
show ip route bestroutes
```

Check which routes the router actually uses for the transmission.

```
    Network             Subnet                         Next Hop     Next Hop
    Address              Mask          Protocol          Intf      IP Address
---------------  ---------------  -----------   ---------  ---------
10.0.1.0          255.255.255.0    Local           2/1         10.0.1.1
10.0.2.0          255.255.255.0    Local           2/2         10.0.2.1
10.0.3.0          255.255.255.0    Static          2/2         10.0.2.2
                                                   2/3         10.0.4.2
10.0.4.0          255.255.255.0    Local           2/3         10.0.4.1

Total Number of Routes......................... 4
```

# 3.4 Static route tracking

## 3.4.1 Description of the static route tracking function

With static routing, if there are a number of routes to a destination, the router chooses the route with the highest importance. The router detects an existing route by the state of the router interface. While connection L 1 (see table 3) on the router interface may be fine, the connection to remote router B at location L 2 may be interrupted. In this case, the router continues transmitting via the interrupted route.

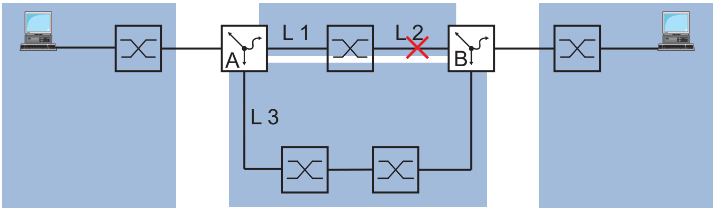


*Figure 12: Example of static route tracking*

With the static route tracking function, the router uses a tracking object such as a ping tracking object (see on page 46 “Ping tracking”) to detect the connection interruption. The active static route tracking function then deletes the interrupted route from the current routing table. If the tracking object returns to the “up” state, the router enters the static route in the current routing table again.

### 3.4.2 Application example for the static route tracking function

The figure (see figure 13) shows an example of the static route tracking function:
Router A monitors the best route via L 1 with ping tracking. If there is a connection interruption, router A transmits via redundant connection L 3.
The following is known:

| Parameter | Router A | Router B |
|---|---|---|
| IP address interface (IF) 1.1 | 10.0.4.1 | |
| IP address interface (IF) 1.2 | 10.0.2.1 | 10.0.4.2 |
| IP address interface (IF) 1.3 | | 10.0.2.53 |
| IP address interface (IF) 1.4 | 10.0.1.112 | |
| IP address interface (IF) 2.2 | | 10.0.5.1 |
| Netmask | 255.255.255.0 | 255.255.255.0 |

Prerequisites for further configuration:

- The IP parameters of the router interface are configured. (see on page 25 “Configuration of the router interfaces”)
- The router function is activated globally and at the ports/router interface.
- Ping tracking at interface 1.2 of router A is configured (see on page 51 “Application example for ping tracking”).

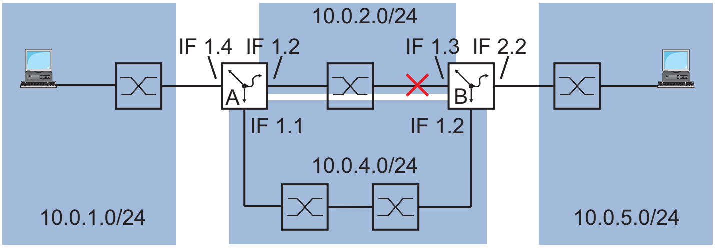


*Figure 13: Configuring static route tracking*

□ Enter the two routes to destination network 10.0.5.0/24 in the static routing table of router A.

□ Select the dialog
`Routing:Routing Table:Static.`

□ Click on “Create Entry”.
You thus open the input window for a new entry.

□ Enter the data for the first static route:

| | |
|---|---|
| “Destination Network” | `10.0.5.0` |
| “Destination Netmask” | `255.255.255.0` |
| “Next Hop” | `10.0.2.53` |
| “Track ID” | `21` |

□ Click "OK".

□ Click on “Create Entry”.
You thus open the input window for a new entry.

□ Enter the data for the first static route:

| | |
|---|---|
| “Destination Network” | `10.0.5.0` |
| “Destination Netmask” | `255.255.255.0` |
| “Next Hop” | `10.0.4.2` |
| “Track ID” | 0 |

□ Click "OK".

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `ip route 10.0.5.0 255.255.255.0 10.0.2.53 1 track 21` | Create the static routing entry with preference 1 and track ID 21. |
| `ip route 10.0.5.0 255.255.255.0 10.0.4.2 2` | Create the static routing entry with preference 2. |
| `exit` | Switch to the privileged EXEC mode. |
| `show ip route` | Verify the routing table: |

```
Total Number of Routes......................... 3

   Network          Subnet                        Next Hop     Next Hop
   Address           Mask          Protocol         Intf      IP Address
-------------- --------------- ------------  ------   -------------
10.0.1.0       255.255.255.0   Local          1/4       10.0.1.112
10.0.2.0       255.255.255.0   Local          1/2       10.0.2.1
10.0.5.0       255.255.255.0   Static         1/2       10.0.2.53
```

□ On router B, create a ping tracking object with the track ID, for example 22, for IP address 10.0.2.1.

□ Enter the two routes to destination network 10.0.1.0/24 in the static routing table of router B.

| Destination Network | Destination Netmask | Next Hop | Preference | Track ID |
|---|---|---|---|---|
| 10.0.1.0 | 255.255.255.0 | 10.0.2.1 | 1 | 22 |
| 10.0.1.0 | 255.255.255.0 | 10.0.4.1 | 2 | |

*Table 3: Static routing entries for router B*

# 3.5 Adaptation for non-IP-compliant devices

Some devices use a simplified IP stack that does not correspond to the IP standard. Without an ARP request, these devices send their responses to the MAC address contained as the source address in the requesting packet (see figure below, no MAC/IP address resolution). These devices exhibit this behavior with ping requests in particular (ICMP echo request). Some of these devices also exhibit this behavior with other data packets.
As long as the router interface of the router to which such a device is connected is itself connected to the MAC address of the physical port, the router can receive and transmit the packet.
However, if the physical port belongs to a VLAN, the VLAN router interface then has its own MAC address. Thus the router rejects packets that are being sent to the port's MAC address.

A terminal device that performs the MAC/IP address resolution according to the IP standard starts an ARP request to determine the correct MAC address before sending the reply to the determined VLAN MAC address (see figure below: MAC/IP standard address resolution using ARP).

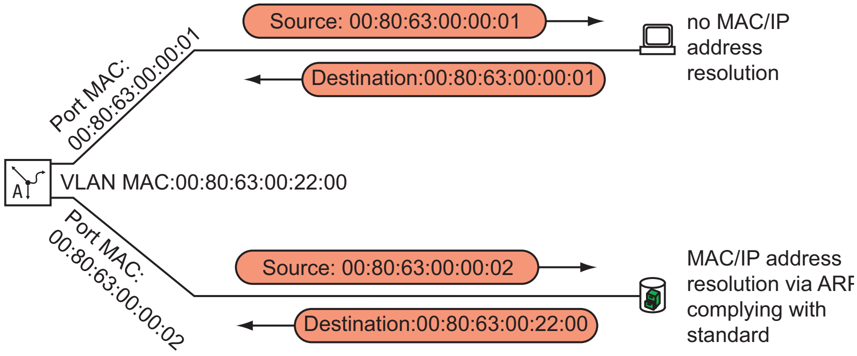

Source: 00:80:63:00:00:01
Destination:00:80:63:00:00:01
no MAC/IP address resolution
Port MAC: 00:80:63:00:00:01
VLAN MAC:00:80:63:00:22:00
Port MAC: 00:80:63:00:00:02
Source: 00:80:63:00:00:02
Destination:00:80:63:00:22:00
MAC/IP address resolution via ARF complying with standard

*Figure 14: Addressing with simplified IP stack and compliant with the standard*

For you also to be able to connect devices with a simplified IP stack to a VLAN-based router interface, the router provides you with the VLAN single MAC mode.
In the VLAN single MAC mode, all VLAN interfaces and all physical ports use the same MAC address, with the exception of the port-based router interface.

□ Activating the VLAN single MAC mode:

```
enable                         Switch to the privileged EXEC mode.
configure                      Switch to the Configuration mode.
ip vlan-single-mac             Activating the VLAN single MAC mode.
exit                           Switch to the privileged EXEC mode.

show ip vlan                   Display the VLAN IP parameters
        Logical
VLAN ID Interface IP Address     Subnet Mask    MAC Address
------- --------- -------------  -------------  -----------------
100     9/1       192.168.100.1  255.255.255.0  00:80:63:51:74:2B
200     9/2       192.168.200.1  255.255.255.0  00:80:63:51:74:2B
```

# 4 Tracking

The tracking function gives you the option of monitoring certain objects, such as the availability of an interface.
A special feature of this function is that it forwards an object status change to an application, e.g. VRRP, which previously registered as an interested party for this information.

Tracking can monitor the following objects:

- Link status of an interface (interface tracking)
- Accessibility of a device (ping tracking)
- Result of logical connections of tracking entries (logic tracking)

An object can have the following statuses:

- up (OK)
- down (not OK)

The definition of "up" and "down" depends on the type of the tracking object (e.g. interface tracking).

Tracking can forward the state changes of an object to the following applications:

- VRRP (see on page 70 “VRRP tracking”)
- Static routing (see on page 36 “Static route tracking”)

# 4.1 Interface tracking

With interface tracking the Switch monitors the link status of:

- physical ports
- link aggregation interfaces (interfaces 8.x)
- VLAN router interfaces (interfaces 9.x)

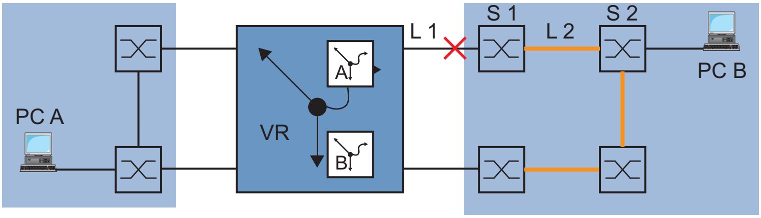


*Figure 15: Monitoring a line with interface tracking*

Ports/interfaces can have the following link statuses:

- interrupted physical link (link down) and
- existing physical link (link up).

A link aggregation interface has link status “down” if the link to all the participating ports is interrupted.

A VLAN router interface has link status “down” if the link is interrupted from all the physical ports/link aggregation interfaces that are members of the corresponding VLAN.

Setting a delay time enables you to insert a delay before informing the application about an object status change.

An interface tracking object is given the “down” status if the physical link interruption remains for longer than the “link down delay” delay time.

An interface tracking object is given the “up” status if the physical link holds for longer than the “link up delay” delay time.

State on delivery: delay times = 0 seconds.
This means that if a status changes, the registered application is informed immediately.
You can set the “link down delay” and “link up delay” delay times independently of each other in the range from 0 to 255 seconds.
You can define an interface tracking object for each interface.

# 4.2 Ping tracking

With ping tracking, the device uses ping requests to monitor the link status to other devices.

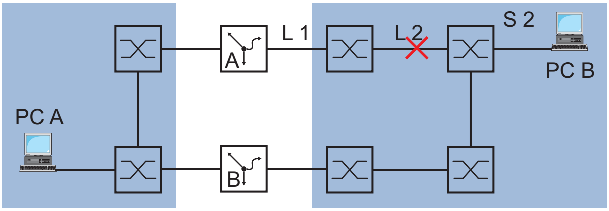


*Figure 16: Monitoring a line with ping tracking*

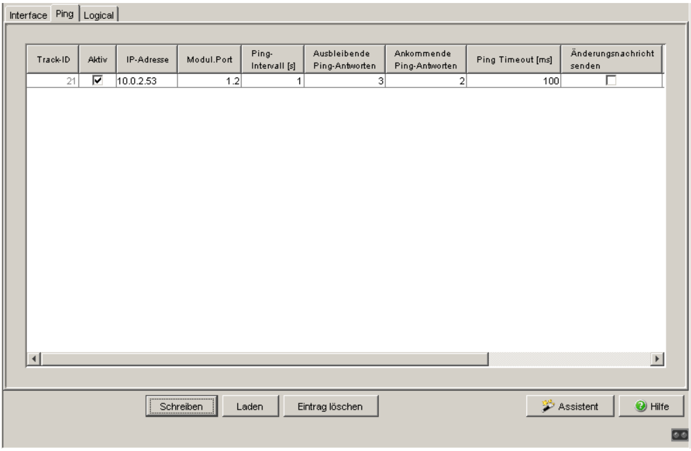
The device sends ping requests to the device with the IP address that you entered in the “IP Address” column.
The “Ping Interval” column allows you to define the frequency for sending ping requests, and thus the additional network load.
If the response comes back within the time entered in the “Ping Timeout” column, this response is a valid “Ping response received”.
If the response comes back after the time entered in the “Ping Timeout” column, or not at all, this response is evaluated as “No ping response”.

Ping tracking objects can have the following statuses:

- the number of “No ping responses” is greater than the number entered (down) and
- the number of “Ping responses received” is greater than the number entered (up).

Entering a number for unreceived or received ping responses enables you to set the sensitivity of the ping behavior of the device. The device informs the application about an object status change.

Ping tracking enables you to monitor the accessibility of defined devices. As soon as a monitored device can no longer be accessed, the device can choose to use an alternative path.



| Track-ID | Aktiv | IP-Adresse | Modul.Port | Ping-Intervall [s] | Ausbleibende Ping-Antworten | Ankommende Ping-Antworten | Ping Timeout [ms] | Änderungsnachricht senden |
|---|---|---|---|---|---|---|---|---|
| 21 | ☑ | 10.0.2.53 | 1.2 | 1 | 3 | 2 | 100 | □ |

*Figure 17: Ping Tracking dialog*

# 4.3 Logical tracking

Logical tracking enables you to logically link multiple tracking objects with each other and thus perform relatively complex monitoring tasks.
You can use logical tracking, for example, to monitor the link status for a network node to which redundant paths lead (see on page 52 “Application example for logical tracking”).

The device provides the following options for a logical link:
- AND
- OR

For a logical link, you can combine up to 8 operands with one operator.

Logical tracking objects can have the following statuses:
- The result of the logical link is incorrect (down).
- The result of the logical link is correct (up).

When a logical link delivers the result “incorrect”, the device can choose to use an alternative path.

## 4.4 Configuring the tracking

You configure the tracking by setting up tracking objects. The following steps are required to set up a tracking object:

▶ Enter the tracking object ID number (track ID).

▶ Select a tracking type, e.g. interface.

▶ Depending on the track type, enter additional options such as “port” or “link up delay” in the interface tracking.

**Note:** The registration of applications (e.g. VRRP) to which the tracking function reports status changes is performed in the application itself (see on page 70 “VRRP tracking”).

### 4.4.1 Configuring interface tracking

□ Set up interface tracking at port 1.1 with a link down delay of 0 seconds and a link up delay of 3 seconds.

□ In the `Routing:Tracking:Configuration` dialog, click on “Wizard” at the bottom right.

Select type:

□ Enter the values you desire:

| | |
|---|---|
| Track ID: | `1` |
| Type: | `interface` |

□ Click on “Continue”.

Properties:

□ Enter the values you desire:
Module.Port: 1.1
Link up delay: 3
Link down delay: 0

□ Click on “Finish” to leave the Wizard and save the entry temporarily in the configuration.

```
enable
```

Switch to the privileged EXEC mode.

```
configure
```

Switch to the Configuration mode.

```
track 1 interface 1/1
  link-down-delay 0
  link-up-delay 3
```

Enter the tracking parameters and activate this tracking object.

```
Tracking ID 1 created
  Tracking type set to Interface
  Target interface set to 1/1
  Link Down Delay for target interface set to 0 sec
  Link Up Delay for target interface set to 3 sec
Tracking ID 1 activated
```

```
exit
```

Switch to the privileged EXEC mode.

```
show track
```

Display the configured tracks

```
             Link Delay              No. of
ID Type  Intf Down  Up   Status  Mode  Changes Time since last change
-- ----  ---- ---- ----- ------ ------ -------- --------------------
1 Intf  1/1    0s    3s  DOWN  Enable      0   0 day(s), 00:00:29
Unconfigured Track-IDs with registered applications:
----------------------------------------------------
```

## 4.4.2 Application example for ping tracking

While the interface tracking monitors the directly connected link (see figure 15), the ping tracking monitors the entire link to Switch S2 (see figure 16).

□ Set up ping tracking at port 1.2 for IP address 10.0.2.53 with the preset parameters.

□ In the `Routing:Tracking:Configuration` dialog, click on "Wizard" at the bottom right.

Select type:

□ Enter the values you desire:

| | |
|---|---|
| Track ID: | `21` |
| Type: | `ping` |

□ Click on "Continue".

Properties:

□ Enter the values you desire:

| | |
|---|---|
| IP address: | `10.0.2.53` |
| Module.Port: | `1.2` |
| Ping interval [s]: | `1` |
| No ping response: | `3` |
| Ping responses received: | `2` |
| Ping timeout [ms]: | `100` |

□ Click on "Finish" to leave the Wizard and save the entry temporarily in the configuration.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `track 21 ping 10.0.2.53 interface 1/2 interval 1 miss 3 success 2 timeout 100` | Enter the tracking parameters and activate this tracking object. |

```
Tracking ID 21 created
  Tracking type set to Ping
  Target IP address set to 10.0.2.53
  Interface used for sending pings to target set to 1/2
  Ping Interval for target set to 1 sec
  Max. no. of missed ping replies from target set to 3
  Min. no. of received ping replies from target set to 2
  Timeout for ping replies from target set to 100 ms
Tracking ID 21 activated
exit                         Switch to the privileged EXEC mode.
show track                   Display the configured tracks
Ping Tracking
                                        No. of   Time since
  ID Type IP Address  Intvl Status Mode Changes  last change
 --- ---- ----------- ----- ------ ------ -------- -----------------
  21 Ping  10.0.2.53    1s  DOWN   Enable   1    0 day(s), 00:13:39
```

## 4.4.3 Application example for logical tracking

The figure (see figure 15) shows an example of monitoring the connection to a redundant ring.
By monitoring lines L 2 and L 4, you can detect a line interruption from router A to the redundant ring.
With a ping tracking object at port 1.1 of router A, you monitor the connection to Switch S2.
With an additional ping tracking object at port 1.1 of router A, you monitor the connection to Switch S4.
Only the OR link of both ping tracking objects delivers the precise result that router A has no connection to the ring.
One ping tracking object for Switch S3 could indicate an interrupted connection to the redundant ring, but in this case there could be another reason for the lack of a ping response from Switch S3. For example, there could be a power failure at Switch S3.

The following is known:

| Parameter | Value |
|---|---|
| Operand No. 1 (track ID) | 21 |
| Operand No. 2 (track ID) | 22 |

Prerequisites for further configuration:

- ▶ The ping tracking objects for operands 1 and 2 are configured (see on page 51 “Application example for ping tracking”).

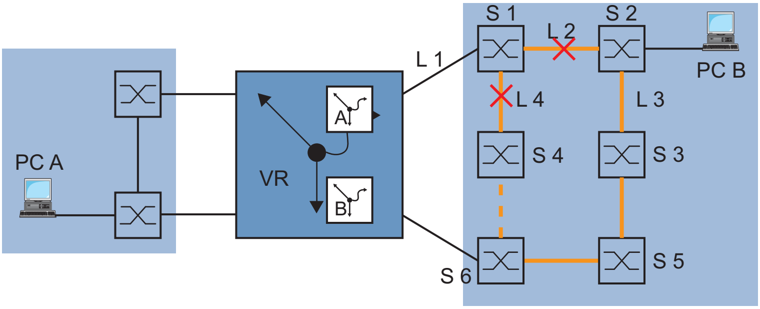


*Figure 18: Monitoring the accessibility of a device in a redundant ring*

□ Set up a logical tracking object as an OR link.

□ In the `Routing:Tracking:Configuration` dialog, click on “Wizard” at the bottom right.

Select type:

□ Enter the values you desire:
Track ID: `31`
Type: `Logical`

□ Click on “Continue”.

Properties:

☐ Enter the values you desire:

| | |
|---|---|
| Operator: | `or` |
| Operand 1 (track ID): | `21` |
| Operand 2 (track ID): | `22` |

☐ Click on “Finish” to leave the Wizard and save the entry temporarily in the configuration.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `track 31 logical or 21 22` | Enter the tracking parameters and activate this tracking object. |

```
Tracking ID 31 created
  Tracking type set to Logical
  Logical Operator set to or
  Logical Instance 21 included
  Logical Instance 1 included
Tracking ID 31 activated
```

| | |
|---|---|
| `exit` | Switch to the privileged EXEC mode. |
| `show track` | Display the configured tracks |

```
Ping Tracking
                                          No. of   Time since
  ID Type IP Address  Intvl Status Mode Changes  last change
 --- ---- ----------- ----- ------ ------ -------- -----------------
  21 Ping  10.0.2.53    1s  DOWN   Enable   1    0 day(s), 00:13:39

Ping Tracking
                                          No. of   Time since
  ID Type IP Address  Intvl Status Mode Changes  last change
 --- ---- ----------- ----- ------ ------ -------- -----------------
  22 Ping  10.0.2.54    1s  DOWN   Enable   1    0 day(s), 00:14:39

Logical Tracking
                                      No. of
 ID Type  Instances  Status  Mode    Changes Time since last change
--- ---- ----------- ------ -------- -------- ----------------------
 31  OR  21,22       DOWN   Enable      0    0 day(s), 00:04:58
```

# 5 VRRP/HiVRRP

Terminal devices usually give you the option of entering a default gateway for transmitting data packets in external subnetworks. Here the term “Gateway” applies to a router by means of which the terminal device can communicate in other subnetworks.

If this router fails, the terminal device cannot send any more data to external subnetworks.
In this case, the Virtual Router Redundancy Protocol (VRRP) provides assistance.
VRRP is a type of “gateway redundancy”. VRRP describes a process that groups multiple routers into one virtual router. Terminal devices always address the virtual router, and VRRP ensures that a physical router belonging to the virtual router takes over the data transmission.
Even if a physical router fails, VRRP ensures that another physical router takes over the distribution tasks as part of the virtual router.

VRRP has typical switching times of 3 to 4 seconds when a physical router fails.
In many cases, such as Voice over IP, Video over IP, industrial controllers, etc., these long switching times are not acceptable.

The Hirschmann company has further developed the VRRP into the Hirschmann Virtual Router Redundancy Protocol (HiVRRP).
With the appropriate configuration, HiVRRP guarantees maximum switching times of 400 milliseconds.
Thanks to this guaranteed switching time, HiVRRP enables the use of “gateway redundancy” in time-critical applications. Even in tunnel controllers that require switching times of less than one second, the user can improve the network availability with this form of “gateway redundancy”.

# 5.1 VRRP

All the routers within a network on which VRRP is active specify among themselves which router is to be the master. This router contains the IP and MAC address of the virtual router. All the devices in the network that have entered this virtual IP address as the default gateway use the master as the default gateway.

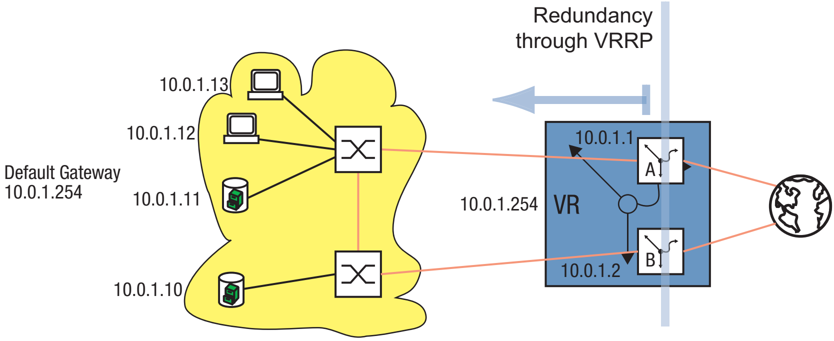


*Figure 19: Illustration of the virtual router*

If the master fails, then the remaining routers use the VRRP to specify a new master. This router then takes over the IP and MAC address of the virtual router. Thus the devices find their route via their default gateway, as before. The devices always only see the master with the virtual MAC and IP addresses, regardless of which router is actually behind this virtual address.
The virtual router IP address is assigned by the administrator.
The VRRP specifies the virtual MAC address with:
00:00:5e:00:01:<VRID>.
The first 5 octets form the fixed part in accordance with RFC 2338.
The last octet is the virtual router ID (VRID). It is a number between 1 and 255. On the basis of this, the administrator can define 255 virtual routers within a network.

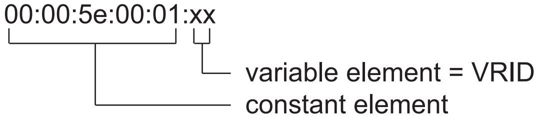


*Figure 20: Virtual MAC address*

The VRRP router sends IP Multicast messages to the IP Multicast address 224.0.0.18 in order to determine the master. The router with the highest VRRP priority becomes the master. The VRRP priority is specified by the administrator. If the VRRP priorities are the same, then the highest IP interface address of the VRRP routers is decisive. If the virtual IP address is the same as the IP address of a router interface, then this router is the IP address owner. VRRP sets the VRRP priority of an IP address owner to the value 255 and thus declares it the master. If there is no IP address owner, then VRRP declares the router with the highest VRRP priority the master.

The master regularly sends IP Multicast messages (default: 1 s) to the other VRRP routers in order to signal that it is ready for operation. If this message does not appear three times in a row, then the VRRP router with the highest remaining VRRP priority declares itself the new master.

| | |
|---|---|
| 1. | The IP address owner as it has the highest VRRP priority (255) by definition. |
| 2. | The VRRP router with the highest VRRP priority. |
| 3. | If the priorities are the same, the VRRP router with the highest IP address. |

*Table 4: Who shall be the master?*

**VRRP terms:**

- Virtual router
  A virtual router is a router or group of routers that act as the default gateway in a network and use the Virtual Router Redandancy Protocol.
- VRRP router
  A VRRP router is a router that uses VRRP. It can be part of one or more virtual routers.

- Master router
  The master router is the router within the virtual router that is currently responsible for forwarding data packets and responding to ARP queries. The master router periodically sends messages (advertisements) to the other VRRP routers (backup routers) to inform them about its existence.
- Ip address owner
  The IP address owner is the VRRP router whose IP address is identical to the IP address of the virtual router. By definition, it has the highest VRRP priority (255) and is thus automatically the master router.
- Backup router
  The backup router is a VRRP router that is not the master router. The backup router is ready to take over the master role, should the master fail.
- VRRP priority
  The VRRP priority is a number between 1 and 255. It is used to determine the master router. The value 255 is reserved for the IP address owner.
- VRID
  The VRID (virtual router ID) uniquely identifies a virtual router.
- Virtual router MAC address
  The virtual router MAC address is the MAC address of the virtual router (see figure 4).
- Virtual router IP address
  The virtual router IP address is the IP address of the virtual router.
- Advertisement interval
  The advertisement interval describes the frequency with which the master router sends its existence message (advertisement) to all the VRRP routers of its virtual router. The values for the advertisement interval are between 1 and 255 seconds. The default value is 1 second.
- Skew time
  The skew time is the time, dependent on the VRRP priority, that specifies the time when the backup router names itself the master router.
  Skew time = ((256 - VRRP priority) / 256) · 1 second
- Master down interval
  The master down interval specifies the time when the backup router names itself the master router.
  Master down interval = 3 · advertisement interval + skew time

## 5.1.1 Configuration of VRRP

The configuration of VRRP requires the following steps:

- Switch on routing globally (if this has not already been done).
- Switch on VRRP globally.
- Configure port - assign IP address and network mask.
- Switch on VRRP at the port.
- Create virtual router ID (VRID), because you have the option of activating a multiple virtual routers for each port.
- Assign virtual router IP address.
- Switch on virtual router.
- Assign VRRP priority.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `ip routing` | Switch on the router function globally. |
| `ip vrrp` | Switch on VRRP globally. |
| `interface 2/3` | Select the port for setting up VRRP. |
| `ip address 10.0.1.1 255.255.255.0` | Assign the port its IP parameters. |
| `routing` | Activate the router function at this interface. |
| `ip vrrp 1` | Create the VRID for the first virtual router at this port. |
| `ip vrrp 1 mode` | Switch on the first virtual router at this port. |
| `ip vrrp 1 ip 10.0.1.100` | Assign virtual router 1 its IP address. |
| `ip vrrp 1 priority 200` | Assign virtual router 1 the router priority 200. |

□ You configure every port at which VRRP will be active in the same way.

□ You also perform the same configuration on the redundant router.

## 5.2 HiVRRP

HiVRRP provides a number of mechanisms for shortening the switching times or reducing the number of Multicasts:

- shorter advertisement intervals
- link-down notification
- preempt delay
- Unicast advertisement
- domains

In compliance with RFC 2338, the master sends IP Multicast messages (advertisements) at intervals of one second to the other VRRP routers. Only if this message does not appear three times do the remaining routers select a new master.
VRRP has typical switching times of 3 to 4 seconds.

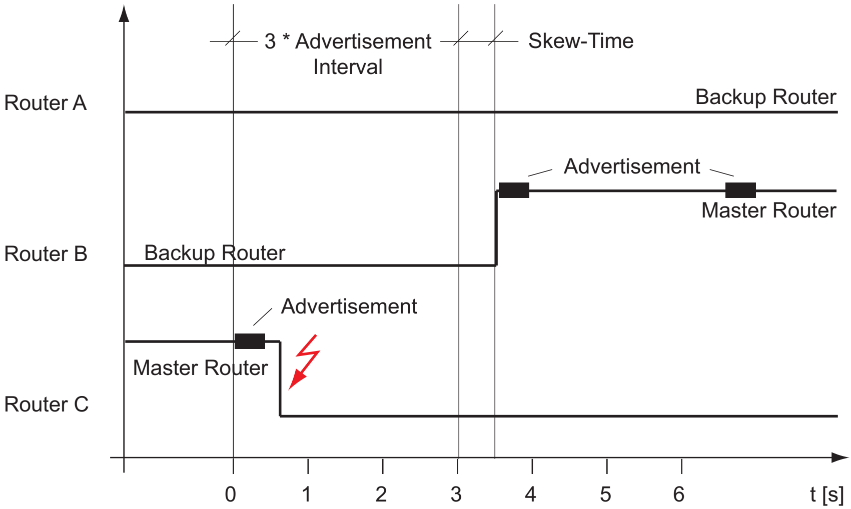


*Figure 21: Master router <-> backup router switching times according to RFC 2338*
*VRRP priority router A = 64*
*VRRP priority router B = 128*
*VRRP priority router C = 254*

To be able to achieve faster switching times, Hirschmann provides HiVRRP so that the cycle for sending the IP Multicast message can be shortened to as little as 0.1 seconds. You can thus achieve switching times that are up to 10 times as fast.

The router supports up to 16 VRRP router interfaces with this shortened sending cycle.

- HiVRRP skew time
  The HiVRRP skew time is the time, dependent on the VRRP priority, that specifies the time when the HiVRRP backup router names itself the HiVRRP master router.
  HiVRRP skew time =
  (256 - VRRP priority) / 256 · advertisement interval
  Times shown in milliseconds
- HiVRRP master down interval
  The HiVRRP master down interval specifies the time when the HiVRRP backup router names itself the HiVRRP master router.
  HiVRRP master down interval =
  3 · advertisement interval + HiVRRP skew time
  Times shown in milliseconds

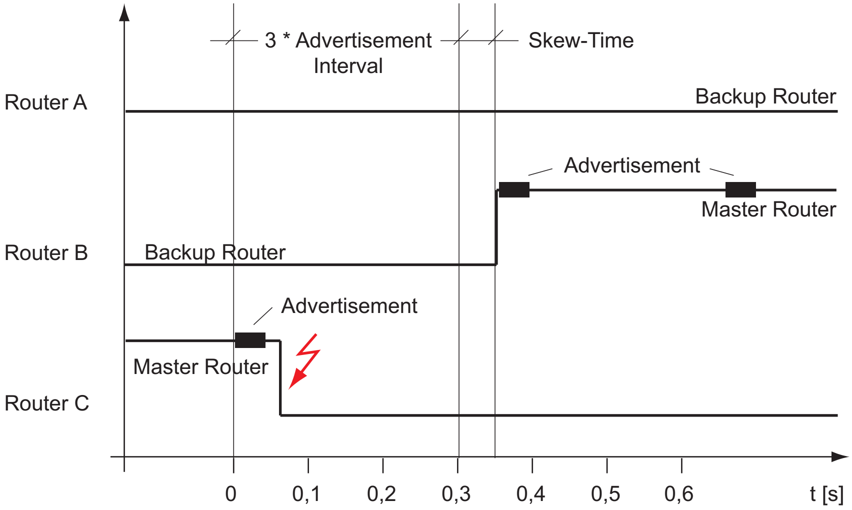


*Figure 22: Master router <-> backup router switching times according to HiVRRP*
*VRRP priority router A = 64*
*VRRP priority router B = 128*
*VRRP priority router C = 254*

Another option provided by HiVRRP for shortening the switching times dramatically is the link-down notification. You can use this function when the virtual router consists of two VRRP routers. As two VRRP routers are participating, it is sufficient to send the link-down notification in the form of a Unicast message. In contrast to the Multicast message, the Unicast message travels beyond the boundaries of the subnetwork. This means that if the link is down to your own subnetwork, the link-down notification can also travel via another subnetwork to reach the second router of the virtual router.
As soon as HiVRRP detects that the link is down, it sends the link-down notification to the second router via a different route. The second router takes over the master function immediately after receiving the link-down notification.

In the preempt mode, the backup router can take over the master function from the master router as soon as the backup router receives an advertisement from the master router for which the VRRP priority is lower than its own.
Thus the preempt mode, in collaboration with VRRP tracking (see on page 70 “VRRP tracking”) , can enable a switch to a better router. However, dynamic routing procedures take a certain amount of time to react to changed routes and refill their routing table.
To avoid the loss of packets during this time, delayed switching (preempt delay) from the master router to the backup router enables the dynamic routing procedure to fill the routing tables.

HiVRRP provides an additional advantage for networks with devices that have problems with higher volumes of Multicasts. Instead of sending advertisements in the form of Multicasts, HiVRRP can send the advertisements in the form of Unicast data packets (VRRP destination address) when using up to two HiVRRP routers.

**Note:** If you want to avail of the advantages of HiVRRP, then only use VRRP routers equipped with the HiVRRP function from Hirschmann as the virtual router.

## 5.3 HiVRRP Domains

In large, flat network structures, HiVRRP domains enable you to

- switch over all HiVRRP routers very quickly in the case of redundancy
- use the available bandwidth more effectively
- configure more than 16 VRRP router interfaces for each router using HiVRRP
- operate Multicast-sensitive terminal devices in large HiVRRP networks

A HiVRRP instance is a router interface configured as HiVRRP with functions that HiVRRP contains. In a HiVRRP domain you combine multiple HiVRRP instances of a router into one administrative unit. You nominate one HiVRRP instance as the supervisor of the HiVRRP domain. This supervisor regulates the behavior of all HiVRRP instances in its domain.

- The supervisor sends its advertisements on behalf of all HiVRRP instances in its domain.
- The supervisor puts itself and the other HiVRRP instances together into the master role or the backup role.

See figure 23 for an example of a flat network structure. All cross-VLAN data streams pass through the ring.

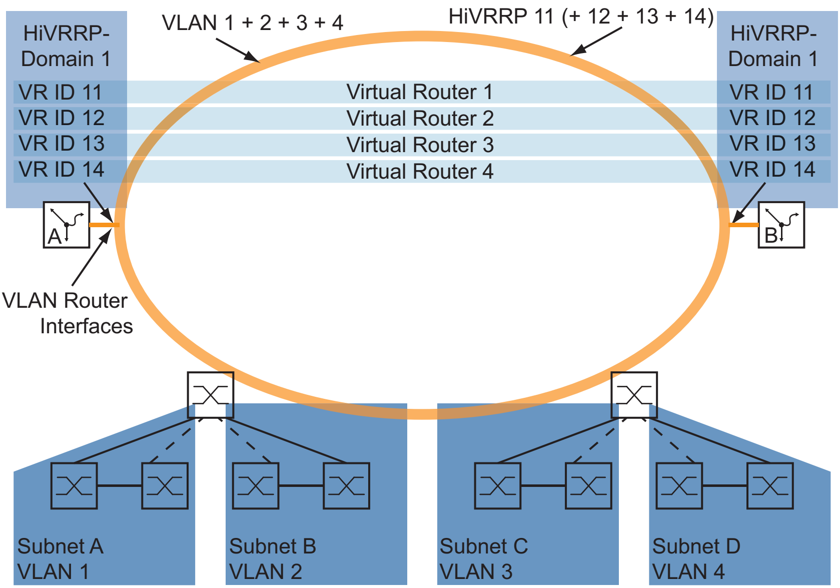


*Figure 23: Example of how a HiVRRP domain is used*

## 5.3.1 Configuration of HiVRRP domains

The configuration of HiVRRP domains consists of the following steps:

- Create VLANs
- Configure VLAN router interfaces
- Assign the IP addresses to the router interfaces
- Configure HiVRRP instances
  - Activate VRRP instance (all instances)
  - Assign IP address (all instances)
    Within a router, you either configure all instances as IP address owners, or no instance as an IP address owner.
  - Assign priority (supervisor)
    Assign the supervisors different priorities so that the VRRP routers can agree on a master router.

  - Switch on HiVRRP (all instances)
  - Assign to the domain (all instances)
  - Specify sending interval (supervisor)

- Configure HIPER-Ring (in applications as in the above example)
- Define the (Ring) ports as members of the VLANs
- Switch on routing and VRRP globally

## 5.3.2 Example of configuration of HiVRRP domains

Example of possible settings for the application in figure 23:

| Subnetwo rk | IP address range | VLAN | VLAN ID |
|---|---|---|---|
| A | 10.0.11.0/24 | 1 | 11 |
| B | 10.0.12.0/24 | 2 | 12 |
| C | 10.0.13.0/24 | 3 | 13 |
| D | 10.0.14.0/24 | 4 | 14 |

*Table 5: Configuration of the Switches in the subnetwork*

| Virtual router | VR ID | IP address of the virtual router | Router interface of router A: IP address | Router interface of router B: IP address | VLAN ID |
|---|---|---|---|---|---|
| 1 | 11 | 10.0.11.1/24 | 10.0.11.2/24 | 10.0.11.3/24 | 11 |
| 2 | 12 | 10.0.12.1/24 | 10.0.12.2/24 | 10.0.12.3/24 | 12 |
| 3 | 13 | 10.0.13.1/24 | 10.0.13.2/24 | 10.0.13.3/24 | 13 |
| 4 | 14 | 10.0.14.1/24 | 10.0.14.2/24 | 10.0.14.3/24 | 14 |

*Table 6: Configuration of the two routers*

## ☐ Configure VLAN router interface and assign IP address:

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `vlan database` | Switch to the VLAN mode. |
| `vlan 11` | Create a VLAN by entering the VLAN ID. |
| `vlan name 11 VLAN1` | Assign the name “VLAN1” to VLAN 11. |
| `vlan routing 11` | Create a virtual router interface and activate the router function at this interface. |
| `exit` | Switch to the privileged EXEC mode. |
| `show ip vlan` | Display the virtual router interface that the router has set up for the VLAN. |

```
show ip vlan          Logical
VLAN ID  Interface    IP Address    Subnet Mask     MAC Address
-------  -----------  ------------  -------------   ------------
11       9/1         0.0.0.0     0.0.0.0         00:80:63:51:74:2C
```

| | |
|---|---|
| `show ip interface brief` | Check the entry for the virtual router interface. |

```
                                           Netdir   Multi
Interface IP Address      IP Mask          Bcast    CastFwd
--------- --------------- ---------------- -------- --------
9/1       0.0.0.0         0.0.0.0          Disable  Disable
```

| | |
|---|---|
| `configure` | Switch to the Configuration mode. |
| `interface 9/1` | Switch to the interface configuration mode of interface 9/1. |
| `ip address 10.0.11.2 255.255.255.0` | Assign the interface its IP parameters. |
| `routing` | Activate the router function at this interface. |

## ☐ Set up virtual router and configure port

| | |
|---|---|
| `ip vrrp 1` | Create the VRID for the first virtual router at this port. |
| `ip vrrp 1 priority 200` | Assign virtual router 1 the router priority 200. |
| `ip vrrp 1 mode` | Switch on the first virtual router at this port. |
| `ip vrrp 1 ip 10.0.11.1` | Assign virtual router 1 its IP address. |
| `ip vrrp 1 domain 1 supervisor` | Assign the HiVRRP domain and the domain role to the interface. |

| | |
|---|---|
| `ip vrrp 1 timers advertise milliseconds 100` | Assign the HiVRRP notification interval to the interface. |
| `exit` | Switch to the Configuration mode. |
| `exit` | Switch to the privileged EXEC mode. |
| `show ip vrrp interface 9/1 1` | Display the configuration of VLAN 11 |

```
Primary IP Address............................ 10.0.11.1
VMAC Address.................................. 00:00:5e:00:01:01
Authentication Type........................... None
Base Priority................................. 200
Advertisement Interval (milliseconds)......... 100
Pre-empt Mode................................. Enable
Administrative Mode........................... Enable
State......................................... Initialized
Current Priority.............................. 200
Preemption Delay (seconds).................... 0
Link Down Notification........................ Disabled
VRRP Domain................................... 1
VRRP Domain Role.............................. Supervisor
VRRP Domain State............................ Supervisor is down
Advertisement Address......................... 224.0.0.18
```

☐ Define the (Ring) port as a member of the VLAN

| | |
|---|---|
| `interface 2/1` | Switch to the Interface Configuration mode of interface 2.1. |
| `vlan participation include 11` | Assign the interface to the VLAN. |
| `exit` | Switch to the Configuration mode. |
| `exit` | Switch to the privileged EXEC mode. |
| `show vlan 11` | Display the configuration of VLAN 11 |

```
VLAN ID           : 11
VLAN Name         : VLAN1
VLAN Type         : Static
VLAN Creation Time: 0 days, 00:00:06 (System Uptime)

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Exclude   Autodetect   Untagged
1/2         Exclude   Autodetect   Untagged
1/3         Exclude   Autodetect   Untagged
1/4         Exclude   Autodetect   Untagged
2/1         Include   Include      Untagged
2/2         Exclude   Autodetect   Untagged
2/3         Exclude   Autodetect   Untagged
2/4         Exclude   Autodetect   Untagged
3/1         Exclude   Autodetect   Untagged
3/2         Exclude   Autodetect   Untagged
9/1         Exclude   Autodetect   Untagged
```

## Switch on routing and VRRP globally

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `ip routing` | Switch on the router function globally. |
| `ip vrrp` | Switch on VRRP globally. |

# 5.4 VRRP tracking

By monitoring certain router statuses (e.g. line interruption), VRRP tracking makes it possible to switch to a better router when a link goes down.

If there is a line interruption between Switch S1 and router A (see figure 25), router B takes over the master function for virtual router 10.0.1.254.
Router A remains the master for virtual router 10.0.2.254. However, router A no longer has a link to subnetwork 10.0.1.0.
The virtual router interfaces are independent of each other.

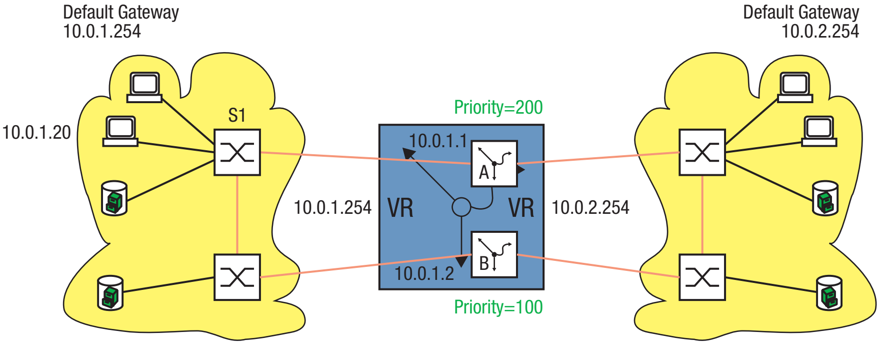


*Figure 24: Typical VRRP application*

As soon as the VRRP master router with the VRRP tracking function active detects the interruption of one of its links, it lowers its VRRP priority and informs the other VRRP routers of this.
Then another VRRP router, which now has the highest priority due to this change in the situation, can take over the master function within the skew time.

Solution without tracking:
Configure router A with a static route to router B or with a dynamic routing procedure, so that router A finds a route into subnetwork 10.0.1.0.

A direct link with preference 0 is the best route.
The static route with preference 1 is the second-best route. Then comes the dynamic route.

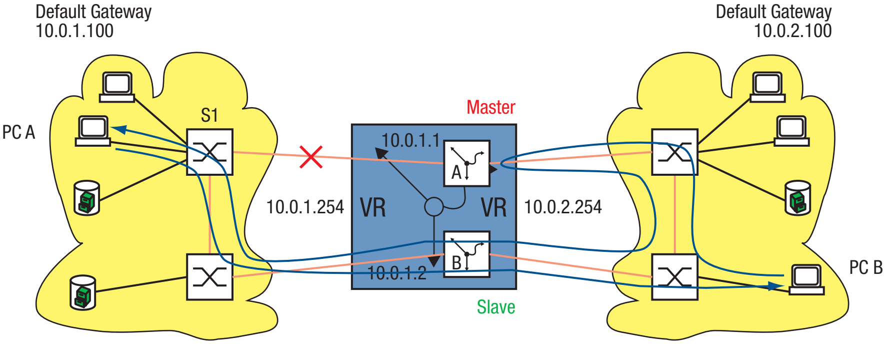


*Figure 25: Transmission path from PC B to PC A in the case of a line interruption without tracking*

The data from PC B is then transferred to PC A via router A and router B.

Solution with tracking:
For an optimal route, you can now use the tracking function to also make router B the master for virtual router 10.0.2.254.
By "tracking" the interrupted link and registering the virtual routers for this tracking object (see on page 43 “Tracking”), router A decrements its VRRP priority. Thus when router B receives the next advertisement from router A, router B detects that its own VRRP priority is higher than that of router A and takes over the master function (see figure 26).

**Note:** As the IP address owner has the fixed VRRP priority 255 by definition, the VRRP tracking function requires the IP addresses of the VRRP router interfaces to differ from the virtual router IP address.

**Note:** For the backup router to be able to take over the master function from the master router with the lower priority, the VRRP tracking function requires that the preempt mode is activated.

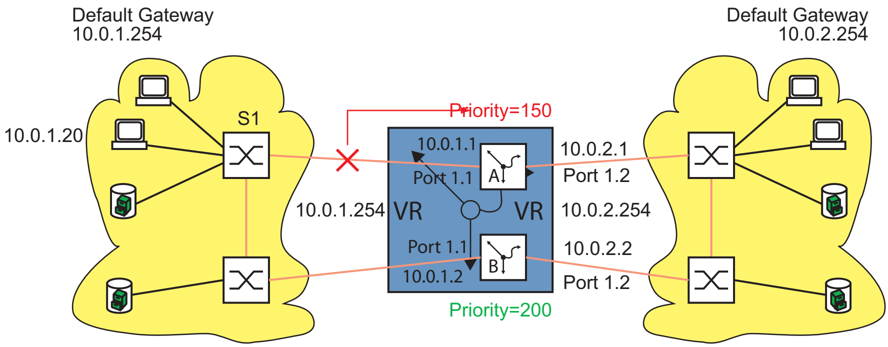


*Figure 26: VRRP tracking after a line interruption*

| | Router A | Router A | Router B | Router B |
|---|---|---|---|---|
| Interface | 1.1 | 1.2 | 1.2 | 1.1 |
| IP address | 10.0.1.1/24 | 10.0.2.1/24 | 10.0.2.2/24 | 10.0.1.2/24 |
| VRID | 1 | 2 | 2 | 1 |
| VRRP IP address | 10.0.1.254 | 10.0.2.254 | 10.0.2.254 | 10.0.1.254 |
| VRRP priority | 250 | 250 | 200 | 200 |
| VRRP preemption | Enabled | Enabled | Enabled | Enabled |
| Track ID | 2 | 1 | - | - |
| Track decrement | 100 | 100 | - | - |

*Table 7: VRRP tracking configuration for the example above*

| | Router A | Router A | Router B | Router B |
|---|---|---|---|---|
| Track ID | 1 | 2 | - | - |
| Type | Interface | Interface | - | - |
| Interface | 1.1 | 1.2 | - | - |

*Table 8: Tracking configuration for the example above*

The configuration of VRRP tracking requires the following steps:

▶ Configure the tracking object
(see on page 49 “Configuring the tracking”).

▶ Configure the VRRP.

▶ Add the track ID to the VRRP entry (= register the VRRP entry for the tracking object).

□ Set up interface tracking at port 1.1 with a link down delay of 0 seconds and a link up delay of 3 seconds.

□ In the `Routing:Tracking:Configuration` dialog, click on “Wizard” at the bottom right.

Select type:

□ Enter the values you desire:

| | |
|---|---|
| Track ID: | `1` |
| Type: | `interface` |

□ Click on “Continue”.

Properties:

□ Enter the values you desire:

| | |
|---|---|
| Module.Port: | `1.1` |
| Link up delay: | `3` |
| Link down delay: | `0` |

□ Click on “Finish” to leave the Wizard and save the entry temporarily in the configuration.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `track 1 interface 1/1`<br>`  link-down-delay 0`<br>`  link-up-delay 3` | Enter the tracking parameters and activate this tracking object. |

□ Switch on routing and VRRP globally.

□ Select the `Routing:Global` dialog.  
□ Select “Routing”.  
□ Click "Set" to save the changes temporarily.  
□ Select the dialog `Redundancy:VRRP/HiVRRP:Configuration`.  
□ Select “Operation”.  
□ Click "Set" to save the changes temporarily.

| | |
|---|---|
| `ip routing` | Switch on the router function globally. |
| `ip vrrp` | Switch on VRRP globally. |

□ Configure the IP address and VRRP at port 1.2.

□ In the `Redundancy:VRRP/HiVRRP:Configuration` dialog, click “Wizard” at the bottom right.

Create entry:

□ Enter the values you desire:

| | |
|---|---|
| “Module”: | `1` |
| “Port”: | `2` |
| “VRID”: | `2` |

□ Click on “Continue”.

Edit entry:

□ Enter the values you desire:

| | |
|---|---|
| “VRRP IP address”: | `10.0.2.254` |
| “Priority”: | `250` |
| “Preempt mode”: | `1` |

□ Click on “Continue”.

| | |
|---|---|
| `interface 1/2` | Select the port for setting up VRRP. |
| `ip address 10.0.2.1 255.255.255.0` | Assign the port its IP parameters. |
| `routing` | Switch on the router function at this port. |
| `ip vrrp 2` | Create the VRID for the first virtual router at this port. |
| `ip vrrp 2 mode` | Switch on the first virtual router at this port. |
| `ip vrrp 2 ip 10.0.2.254` | Assign virtual router 1 its IP address. |
| `ip vrrp 2 priority 250` | Assign virtual router 1 the router priority 250. |

□ Register VRRP for the tracking object.

Tracking

□ Enter the values you desire:

| | |
|---|---|
| "Track ID": | `1` |
| "Decrement": | `100` |

□ Click on "Add".

□ Click on "Continue".

□ Click on "Finish" to leave the Wizard and save the entry temporarily in the configuration.

| | |
|---|---|
| `ip vrrp 2 track 1 decrement 100` | Register the first VRRP entry for the tracking object. |
| `exit` | Switch to the Configuration mode. |
| `exit` | Switch to the privileged EXEC mode. |
| `show track applications` | Display the registered applications. |

```
TrackId  Application              Changes  Time since last change
-------  ----------------------  -------  ---------------------
1        VRRP 1/2 VRID: 2           0      0 day(s), 00:38:24
```

□ You also perform the same configuration on the redundant router.

# 5.5 VRRP with load sharing

With the simple configuration, a router performs the gateway function for all terminal devices. The capacity of the redundant router lies idle. VRRP allows you to also use the capacity of the redundant router. By setting up a number of virtual routers, you can enter different default gateways on the connected terminal devices and thus steer the data flow.
When both routers are active, the data flows via the router on which the IP address of the default gateway has the higher VRRP priority. If a router fails, then all the data flows via the remaining routers.

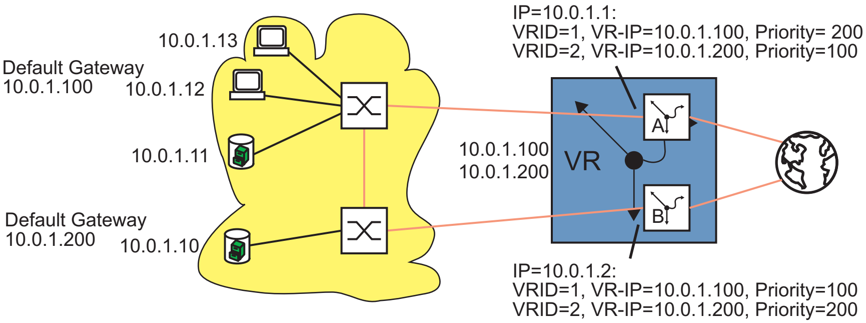

IP=10.0.1.1:
VRID=1, VR-IP=10.0.1.100, Priority= 200
VRID=2, VR-IP=10.0.1.200, Priority=100
10.0.1.13
Default Gateway
10.0.1.100
10.0.1.12
10.0.1.11
Default Gateway
10.0.1.200
10.0.1.10
10.0.1.100
10.0.1.200
VR
A
B
IP=10.0.1.2:
VRID=1, VR-IP=10.0.1.100, Priority=100
VRID=2, VR-IP=10.0.1.200, Priority=200

*Figure 27: Virtual router with load sharing*

To use load sharing, you perform the following configuration steps:

- □ Define a second VRID for the same router interface.
- □ Assign the router interface its own IP address for the second VRID.
- □ Assign the second virtual router a lower priority than the first virtual router.
- □ When configuring the redundant router, make sure that you assign the second virtual router a higher priority than the first.
- □ Give the terminal devices one of the virtual router IP addresses as a default gateway.

# 5.6 VRRP mit Multinetting

The router allows you to combine VRRP with Multinetting.

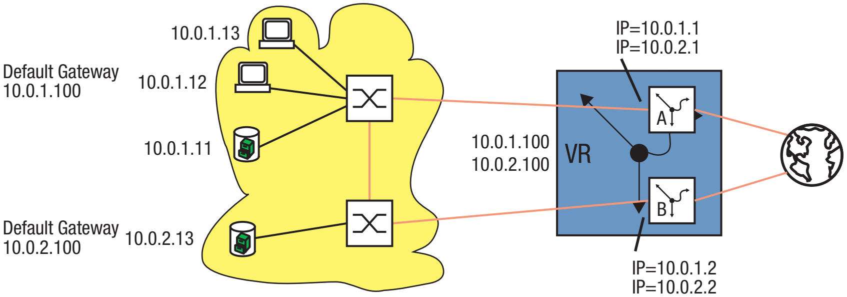


*Figure 28: Virtual router with multinetting*

To use VRRP with multinetting, you perform the following configuration steps on the basis of an existing VRRP configuration (see figure 19):

□ Assign a second (secondary) IP address to the port.

□ Assign a second (secondary) IP address to the virtual router.

| | |
|---|---|
| `interface 2/3` | Select the port at which you want to configure multinetting. |
| `ip address 10.0.2.1 255.255.255.0 secondary` | Assign the second IP address to the port. |
| `ip vrrp 1 ip 10.0.2.100 secondary` | Assign the second IP address to the virtual router with the VR-ID 1. |

□ Perform the same configuration on the redundant router also.

# 6 RIP

The Routing Information Protocol (RIP) is a routing protocol based on the distance vector algorithm. It is used for the dynamic creation of the routing table for routers.

When you start a router, the router only knows the networks directly connected to it, and it sends this routing table to the neighboring routers. At the same time, it requests the routing tables of its neighboring routers. The router adds this information to its routing table and thus learns which networks can be accessed via which routers, and how much effort is involved in this. In order to detect changes in the network (when a router fails or starts), the routers regularly repeat the exchange of all the routing tables, usually every 30 seconds. This involves a considerable bandwidth requirement in large networks.

The costs, also known as the metric, refer to the work involved in reaching a particular network. RIP uses the hop count for this, which describes the number of routers that are traversed along the path to the destination network. The name 'distance vector' is derived from the fact that the distance (metric) is the criterion for determining the route, and the direction is specified by the next hop (vector). The next hop refers to the neighboring router along the path to the destination address.

An entry in the routing table consists of the address of the next hop, the destination address and the metric. The RIP routing table always contains the most efficient route to the destination. This is the route with the smallest metric and the longest suitable network mask prefix.

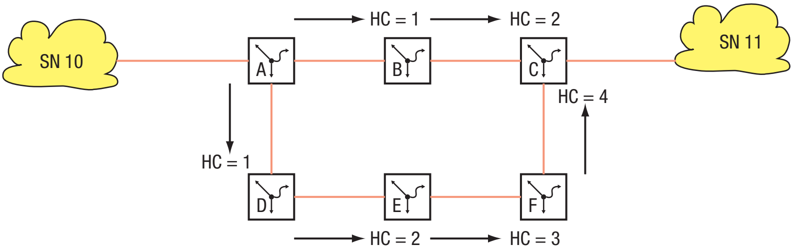


*Figure 29: Counting Hops*

| **Router A** | | | **Router B** | | | **Router D** | | |
|---|---|---|---|---|---|---|---|---|
| Destination | Next Hop | Metric | Destination | Next Hop | Metric | Destination | Next Hop | Metric |
| SN 10 | lokal | 0 | SN 10 | Router A | 1 | SN 10 | Router A | 1 |
| SN 11 | Router B | 2 | SN 11 | Router C | 1 | SN 11 | Router E | 3 |

*Table 9: Routing table to the figure above*

In contrast to OSPF, a RIP router regularly exchanges the content of its entire routing table with its direct neighbor. Every router knows only its own routes and the routes of its direct neighbor. Thus it only has a local perspective.

When changes are made in the network, it takes a while until all the routers have the same uniform view of the network. The process of achieving this condition is known as convergence.

# 6.1 Convergence

How does RIP react to changes in the topography?
In the following example of a line interruption between router B and router C, you can see the resulting changes in the address table:

Assumptions:
- The interruption occurs 5 seconds after B sent its routing table.
- The routers send their routing table every 30 seconds (= factory setting).
- There is an interval of 15 seconds between when router A sends its routing table and when router B sends its routing table.

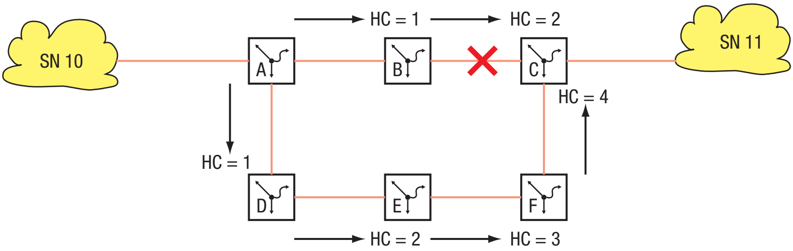


*Figure 30: Hop Count*

Time elapsing before convergence:

0 seconds:
Interruption

10 seconds
Router A sends its routing table:

| Router A | | |
|---|---|---|
| Destination | Next hop | Metric |
| SN 10 | local | 0 |
| SN 11 | Router B | 2 |

Using the routing table from router A, router B sees that router A knows a connection to destination SN 11 with a metric of 2. Because it does not have its own connection to router C as the next hop to SN 11, router B changes its entry to destination SN 11. It enters router A as the next hop and increases the metric from router A by 1 to 3 (distance = learned distance + 1).

25 secondsRouter B sends its routing table:

| **Router B** | | |
|---|---|---|
| Destination | Nex- Hop | Metrik |
| SN 10 | Router A | 1 |
| SN 11 | Router A | 3 |

Using the routing table from router B, router A sees that router B knows a connection to SN 11 with a metric of 3. So router A increases its metric for SN 11 by 1 to 4.

40 secondsRouter A sends its routing table:

| **Router A** | | |
|---|---|---|
| Destination | Next hop | Metric |
| SN 10 | local | 1 |
| SN 11 | Router B | 4 |

Using the routing table from router A, router B sees that router A knows a connection to destination SN 11 with a metric of 4. So router B increases its metric for SN 11 by 1 to 5.

55 secondsRouter B sends its routing table

| **Router B** | | |
|---|---|---|
| Destination | Next hop | Metric |
| SN 10 | Router A | 1 |
| SN 11 | Router A | 5 |

Using the routing table from router B, router A sees that router B knows a connection to SN 11 with a metric of 5. So router A increases its metric for SN 11 by 1 to 6. Because router A can see in the routing table from router D that router D has a connection to SN 11 with the smaller metric of 3, router A changes its entry for SN 11.

70 secondsRouter A sends its routing table:

| **Router A** | | |
|---|---|---|
| Destination | Next hop | Metric |

| **Router A** | | |
|---|---|---|
| SN 10 | Router A | 1 |
| SN 11 | Router D | 4 |

After 70 seconds, convergence has been achieved again.

# 6.2 Maximum Network Size

The biggest problem with RIP is that routers only know their neighbors directly. This results in long convergence times and the count-to-infinity problem. Infinity refers to the inaccessibility of a destination, and it is designated by hop count 16 in RIP. If the above example did not contain the parallel path via routers D, E and F, then routers A and B would keep sending their routing tables until the metric reached a value of 16. Then the routers recognize that the destination is inaccessible.
Using the “split horizon” approach eliminates this looping problem between two neighboring routers. Split horizon has two operating modes.

| | |
|---|---|
| Simple split horizon | Omits the entries known by a neighbor when sending the routing table to this neighbor. |
| Simple split horizon with poison reverse | Sends the routing table to a neighbor with the entries known by this neighbor, but denotes these entries with the infinity metric (=16). |

Thus the hop count 16 specifies the maximum size of a network with RIP as the routing procedure. The longest paths may use up to 15 routers.

# 6.3 General Properties of RIP

The RFC 1058 from June 1988 specifies RIP version 1. Version 1 has the following restrictions:

- Use of broadcasts for protocol messages.
- Does not support subnetworks/CIDR.
- No authentification.

The standardization of RIP version 2 in the RFC 2453 in 1998 eliminates the above restrictions.
RIP V2 sends its protocol messages as a multicast with the destination address 224.0.0.9, and supports subnetwork masks and authentication. However, the restrictions relating to the size of the network remain.

| Advantages | Disadvantages |
|---|---|
| Easy to implement | Routing tables in large networks very comprehensive |
| Easy to administrate | Routing information is distributed slowly, because there are fixed sending intervals. This applies in particular to connections that have elapsed, since the routing table only contains existing paths. |
| | Count-to-infinity |

*Table 10: Advantages and disadvantages of Vector Distance Routing*

# 6.4 Configuring the RIP

The advantage of RIP is the simple configuration. After the router interface is defined and the RIP is switched on, RIP automatically enters the required routes in the routing table.

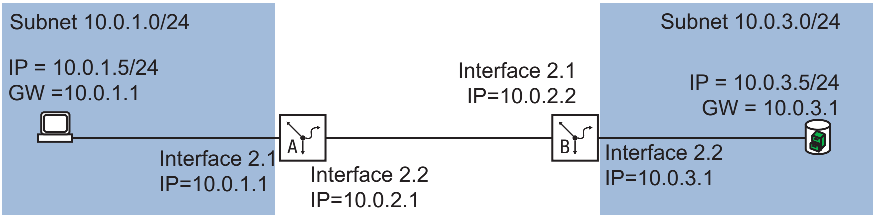


*Figure 31: Example of the configuration of RIP*

The configuration of RIP requires the following steps:

- Configure router interfaces - assign IP address and network mask.
- Switch on RIP on port.
- Switch on RIP globally.
- Switch on routing globally (if this has not already been done).

## Configuration for router B

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `interface 2/2` | Switch to the Interface Configuration mode of interface 2.2. |
| `ip address 10.0.3.1 255.255.255.0` | Assign the IP parameters to the port. |
| `routing` | Switch on the router function at this port. |
| `exit` | Switch to the Configuration mode. |

| | |
|---|---|
| `interface 2/1` | Switch to the Interface Configuration mode of interface 2.1. |
| `ip address 10.0.2.2 255.255.255.0` | Assign the IP parameters to the port. |
| `routing` | Switch on the router function at this port. |
| `ip rip` | Switch on RIP at this port. |
| `exit` | Switch to the Configuration mode. |
| `show ip rip interface brief` | Verify the settings for the RIP configuration. |

```
                                 Send         Receive       RIP         Link
Interface  IP Address          Version      Version      Mode        State
---------  -------------      -----------  ---------   ----------   -----
2/1        0.0.0.0             RIP-2        Both         Enable      Down
```

The IP address entries remain at 0.0.0.0 as long as the routing function is switched off globally.

| | |
|---|---|
| router rip | Switch to the router configuration mode |
| redistribute connected | Tell RIP to send the routes of the locally connected interfaces along with the learned routes in the RIP information |
| `enable` | Switch on RIP globally. |
| `exit` | Switch to the Configuration mode. |
| `ip routing` | Switch on the router function globally. |
| `show ip rip interface brief` | Verify the settings for the RIP configuration. |

```
                                 Send         Receive       RIP         Link
Interface  IP Address          Version      Version      Mode        State
---------  -------------      -----------  ---------   ----------   -----
2/1        10.0.2.2              RIP-2        Both          Enable      Up
```

| | |
|---|---|
| `show ip route` | Verify the routing table: |

```
Total Number of Routes......................... 3

   Network           Subnet                       Next Hop    Next Hop
   Address            Mask          Protocol       Intf      IP Address
---------------- --------------- ------------  ------   ------------
10.0.1.0         255.255.255.0   RIP            2/1        10.0.2.1
10.0.2.0         255.255.255.0   Local          2/1        10.0.2.2
10.0.3.0         255.255.255.0   Local          2/2        10.0.3.1
```

□ Also perform the corresponding configuration on the other RIP routers.

# 7 OSPF

Open Shortest Path First (OSPF) is a dynamic routing protocol based on the Link State Algorithm. This algorithm is based on the link states between the routers involved.
The significant metric in OSPF is the “OSPF costs”, which is calculated from the available bit rate of a link.

OSPF was developed by IETF. OSPF is currently specified as OSPFv2 in RFC 2328. Along with many other advantages of OSPF, the fact that it is an open standard has contributed to the wide usage of this protocol. OSPF has replaced the Routing Information Protocol (RIP) as the standard Interior Gateway Protocol (IGP) in large networks.

OSPF has a number of significant advantages to offer:

- Cost-based routing metrics: In contrast to RIP, OSPF provides clear metrics based on the bandwidth of each individual network connection. OSPF provides major flexibility in designing a network, because the user can simply change these costs.
- Routing via multiple paths (equal cost multiple path/ECMP): OSPF is able to support a number of equal paths to a given destination. OSPF thus provides efficient utilization of the network resources (load distribution) and improves the availability (redundancy).
- Hierarchical routing: By logically dividing the network into areas, OSPF shortens the time required to distribute routing information. The messages about changes in a subnetwork remain within the subnetwork, without putting any load on the rest of the network.
- Support of Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Mask (VLSM): This allows the network administrator to assign the IP address resources efficiently.
- Fast tuning time: OSPF supports the fast distribution of messages about route changes. This speeds up the tuning time for updating the network topology.

- Saving network resources / bandwidth optimization: Because OSPF, in contrast to RIP, does not exchange the routing tables at regular, short intervals, no bandwidth is unnecessarily “wasted” between the routers.
- Support of authentication: OSPF supports the authentication of all nodes that send routing information.

| Advantages | Disadvantages |
|---|---|
| Every router calculates its routes independently of the other routers. | Complicated to implement |
| All the routers have the same basic information. | Complex administration due to the large number of options. |
| Rapid detection of link interruptions and rapid calculation of alternative routes. | |
| The data volume for router information is relatively small, because information is only sent when it is required, and only the information that applies to the immediate neighbors. | |
| Optimal path selection through evaluation of the link quality. | |

*Table 11: Advantages and disadvantages of Link State Routing*

OSPF is a routing protocol based on the states of the links between the routers.
Using the link states collected from all the routers and the Shortest Path First algorithm, an OSPF router dynamically creates its routing table.

# 7.1 OSPF-Topology

OSPF is hierarchically structured in order to limit the scope of the OSPF information to be exchanged in large networks. You divide up your network using what are known as areas.

## 7.1.1 Autonomous System

An Autonomous System (AS) is a number of routers that are managed by a single administration and use the same Interior Gateway Protocol (IGP). Exterior Gateway Protocols (EGP), on the other hand, are used to connect a number of autonomous systems. OSPF is an Interior Gateway Protocol.

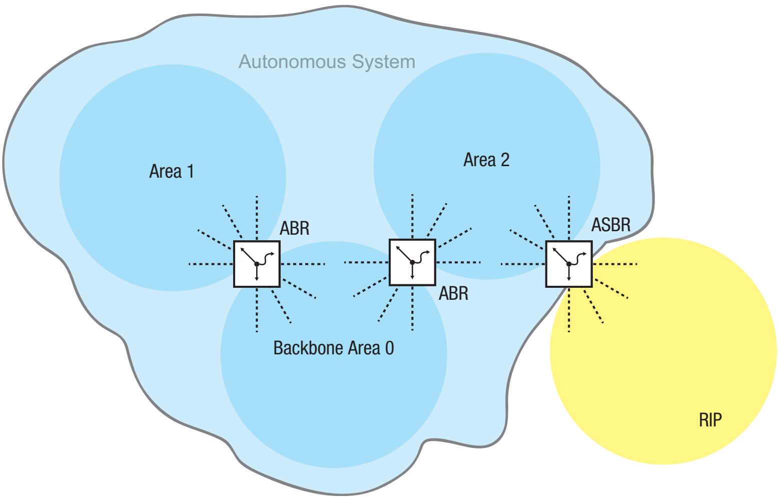


*Figure 32: Autonomous System*

An AS uses an “Autonomous System Boundary Router” (ASBR) to connect with the outside world. An ASBR understands multiple protocols and serves as a gateway to routers outside the areas. An ASBR is able to transfer routes from different protocols into the OSPF. This process is known as redistribution.

### 7.1.2 Router ID

The router ID in the form of an IP address is used to uniquely identify every router within an autonomous system. To improve the transparency, it is necessary to manually configure the router ID of every OSPF router. Thus there is no automatic function that selects the router ID from the IP interfaces of the router.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `router ospf` | Switch to the Router Configuration mode. |
| `router-id 192.168.1.0` | Assign router ID (e.g. 192.168.1.0). |
| `enable` | Switch on OSPF globally. |

### 7.1.3 Areas

Each area first forms its own database using the link states within the area. The data exchange required for this remains within the area. Each area uses an Area Border Router (ABR) to link to other areas. The routing information is summarized as much as possible between the areas (route summarization).

Every OSPF router must be a member of at least one area.
An individual router interface can only be assigned to one area. In the state on delivery, every router interface is assigned to the backbone area.

OSPF distinguishes between the following particular area types:

- Backbone-Area:
  This is by definition the area 0 or 0.0.0.0. An OSPF network consists of at least the backbone area. It is the central area, which is linked to all the other areas directly. The backbone area receives all the routing information and is responsible for forwarding this information.
- Stub Area:
  You define an area as a stub area if external LSAs are not to be flooded into the area. External means outside the autonomous system. These external LSAs are the yellow and orange links in the illustration (see figure 33). Thus the routers within a stub area only learn internal routes (blue links – e.g. no routes that are exported into OSPF from another log / redistributing). All the destinations outside the autonomous system are assigned to a default route. Stub areas are thus generally used if only one route in the area has a link to outside the area.
  The use of stub areas keeps the routing table small within the stub area.
  Totally Stubby Area:
  You define a totally stubby area if, along with the external (orange and yellow) LSAs, the LSAs of the internal (blue) routes are also not to be sent into the area. Internal means between the areas of the autonomous system. A router within a totally stubby area thus only knows the routes within its own area and the default route out of the area.

  Configuration notes:
  - For a stub area, all the routers within the stub area must be defined as stub routers.
  - A stub area does not allow passage for a virtual link.
  - The backbone area cannot be defined as a stub area.
- Not So Stubby Area (NSSA):
  You define an area as NSSA if the external (yellow) routes of a system directly connected to the NSSA that is outside your own autonomous system are to be led into the area (redistributed). These external (yellow) LSAs then also lead from the NSSA to other areas in your own autonomous system. External (orange) LSAs within your own autonomous system do not, on the other hand, lead into an NSSA.
  By using NSSAs, you can integrate ASBRs into the area without foregoing the advantage of stub areas, namely that external routes from the

backbone are not flooded into the corresponding area.
Thus NSSAs have the advantage that external routes coming from the backbone are not all entered in the routing tables of the internal routers. At the same time, however, a limited number of external networks (which can be reached across the boundaries of the NSSA) can be propagated into the backbone area.

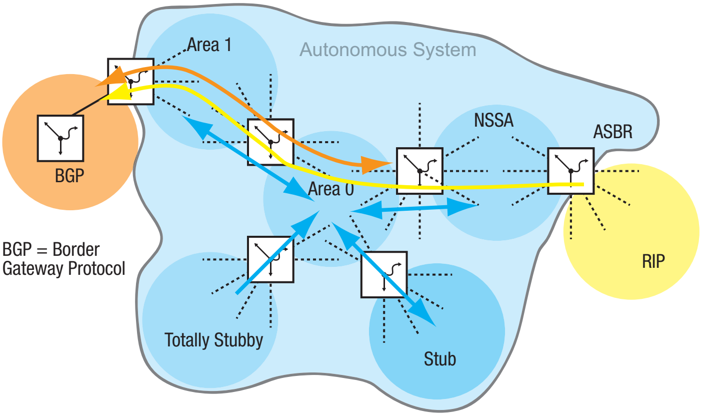


*Figure 33: LSA distribution into the area types*

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `router ospf` | Switch to the Router Configuration mode. |
| `area [area-id]` | Assign the area ID to the area. |
| `area 2 nssa` | Define area 2 as the NSSA |
| `area 3 stub` | Define area 3 as the stub area |
| `area 3 default-cost 10` | Instruct the ABR to inject the default route with the metric 10 into the stub area. |
| `no area 3 stub summerylsa` | Make stub area 3 the totally stubby area |

## 7.1.4 Virtual Link

OSPF requires that the backbone area can be passed through. However, if this is not actually possible, then OSPF provides a virtual link (VL) to connect parts of the backbone area with each other (see figure 35). A VL even allows you to connect an area that is connected with the backbone area via another area.

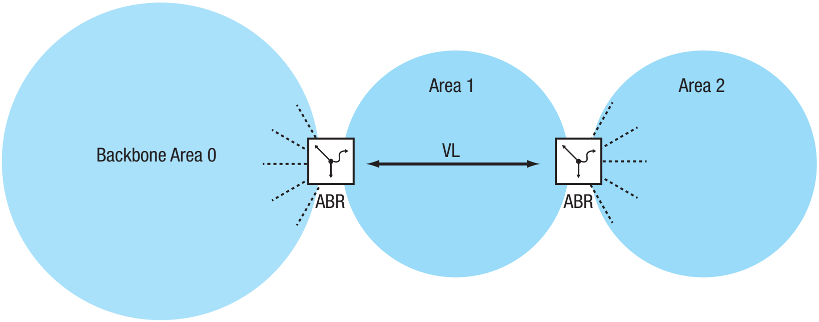


*Figure 34: Linking a remote area to the backbone area via a virtual link (VL)*

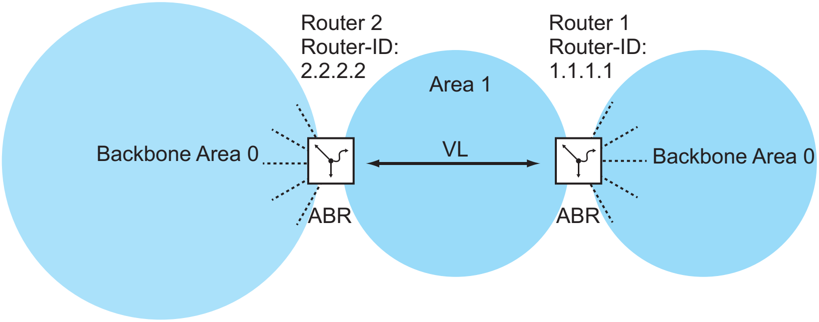


*Figure 35: Expanding the backbone area via a virtual link (VL)*

Configuration for expanding the backbone area (see figure 35):

Router 1:

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `router ospf` | Switch to the Router Configuration mode. |
| `area 1 virtual-link 2.2.2.2` | Enter the neighboring router ID for a virtual link in area 1. |

Router 2:

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `router ospf` | Switch to the Router Configuration mode. |
| `area 1 virtual-link 1.1.1.1` | Enter the neighboring router ID for a virtual link in area 1. |

### 7.1.5 OSPF Router

OSPF distinguishes between the following router types:

- Internal Router:
  All OSPF interfaces of an internal router are within the same area.
- Area Border Router (ABR):
  ABRs have OSPF interfaces in a number of areas, including the backbone area. ABRs thus participate in multiple areas. Where possible, you summarize a number of routes and send “Summary LSAs” to the backbone area.
- Autonomous System Area Border Router (ASBR):
  An ASBR is located on the boundary of an autonomous system and links OSPF to other autonomous systems / routing protocols. These external routes are transferred into OSPF using what is known as redistributing and are then summarized as “AS-external LSAs” and flooded into the area.
  Switch on the redistributing explicitly.
  If you want to use subnetting, then you enter this explicitly. In OSPF, the following “routing protocols” can be exported:
  - connected (local subnetworks on which OSPF is not switched on),
  - static (static routes),
  - RIP.

### 7.1.6 Link State Advertisement

As a basis for building up a database via the link states, OSPF uses Link State Advertisements (LSA).

An LSA contains information about

- the router,
- the connected subnets,
- the routes that can be reached,
- the network masks and
- the metrics.

OSPF unterscheidet folgende LSA-Typen:

- Router LSAs (type 1 LSAs):
  Every router sends a router LSA to all its connected areas. They describe the state and the costs of the router links (router interfaces) that the router has in the corresponding area. Router LSAs are only flooded within the area.
- Network LSAs (Type 2 LSAs):
  These LSAs are generated by the designated router, DR (see on page 100 “Setting up the Neighbor Relationship”) and are sent for every connected network/subnet within an area.
- Summary LSAs (type 3 /type 4 LSAs):
  Summary LSAs are generated by ABRs and describe inter-area destinations, meaning destinations in different areas of the same autonomous system.
  Type 3 LSAs describe targets for IP networks (individual routes or summarized routes).
  Type 4 LSAs describe routes to ASBRs.
- AS-external LSAs (type 5 LSAs):
  These LSAs are generated by ASBRs and describe routes outside the autonomous system. These LSAs are flooded everywhere apart from to stub areas and NSSAs.
- NSSA external LSAs (type 7 LSAs):
  A stub area does not flood any external routes (represented by type 5 LSAs) and therefore does not support any Autonomous System Border Routers (ASBRs) at its boundaries. Thus an ASBR cannot carry any routes from other protocols into a stub area.
  RFC 1587 specifies the functioning of NSSAs. According to RFC 1587, ASBRs send type 7 LSAs instead of type 5 LSAs for the external routes within an NSSA. These type 7 LSAs are then converted into type 5 LSAs by an ABR and flooded into the backbone area. This “translator role” is negotiated among the ABRs in an NSSA (the router with the highest router ID), but it can also be configured manually.

# 7.2 General Operation of OSPF

OSPF was specially tailored to the needs of larger networks and provides a fast convergence and minimum usage of protocol messages.

The concept of OSPF is based on the creation, maintenance and distribution of what is called the link state database. This data basis describes

- all the routers within a routing domain (area) and
- their active interfaces and routes,
- how they are linked to each other and
- the costs of these links.

All the routers within an area have an identical data basis, which means that they all know the exact topology within this area.
Every router plays its part in setting up the respective data basis by propagating its local viewpoint as Link State Advertisements (LSAs).
These LSAs are then flooded to all the other routers within an area.

OSPF supports a range of different network types such as point-to-point networks (for example, packet over SONET/SDH), broadcast networks (Ethernet) or non-broadcast networks.
Broadcast networks are distinguished by the fact that a number of systems (terminal devices, switches, routers) are connected to the same segment and thus can all be addressed simultaneously via broadcasts/multicasts.

OSPF generally performs the following three steps in carrying out its tasks in the network:

- Setting up the neighbor relationships (hello protocol)
- Synchronizing the link state database
- Route calculation

# 7.3 Setting up the Neighbor Relationship

When a router is started, it uses what are called hello packets to contact its neighboring routers. With these hello packets, an OSPF router finds out which OSPF routers are near it and whether they are suitable for setting up a neighbor relationship (adjacency).

In broadcast networks such as Ethernet, the number of neighbors increases with the number of routers connected, as does the information exchange for clarifying and maintaining the neighbor relationships. To reduce these volumes within an area, OSPF uses the “hello” protocol to determine a designated router (DR) within the corresponding segment. Thus every router in an area only sets up the neighbor relationship with its designated router, instead of with every neighbor. The designated router is responsible for the distribution of all the link state information to its neighbor routers.
For security reasons, OSPF provides for the selection of a backup designated router (BDR), which takes over the tasks of the DR if the DR fails. The OSPF router with the highest router priority is the DR. The router priority is specified by the administrator. If two routers have the same priority, the router with the higher router ID is selected. The router ID is the smallest IP address of a router interface. You configure this router ID manually when starting up the OSPF router (see on page 92 “Router ID”).

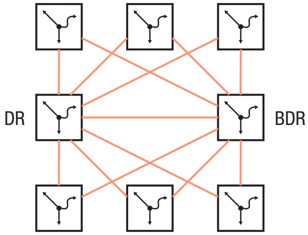


*Figure 36: LSA distribution with designated router and backup designated router*

To exchange information, OSPF uses reserved multicast addresses.

| Destination | Multicast IP address | Mapped Multicast MAC address |
|---|---|---|
| All OSPF routers | 224.0.0.5 | 01:00:5E:00:00:05 |
| Designated routers | 224.0.0.6: OSPF | 01:00:5E:00:00:06 |

*Table 12: OSPF - Multicast addresses*

Hello packets are also used to check the configuration within an area (area ID, timer values, priorities) and to monitor the neighbor relationships. Hello packets are sent cyclically (hello interval). If hello packets are not received for a specific period (dead interval), the neighbor relationship is terminated and all the corresponding routes are deleted.
The hello interval (default: 10 seconds) and the dead interval (default: 30 seconds) can be configured for each router interface, but they must be uniform within an area.

```
enable                        Switch to the privileged EXEC mode.
configure                     Switch to the Configuration mode.
interface 1/1                 Switch to the Interface Configuration mode of
                              interface 1/1.

ip ospf hello-intervall 20    Sets hello interval to 20 seconds.
ip ospf dead-intervall 60     Sets dead interval to 60 seconds.
exit                          Switch to the Configuration mode.
exit                          Switch to the privileged EXEC mode.

show ip ospf neighbor brief   Displays the neighbor relationships of the router.
all

  Router ID         IP Address    Neighbor Interface    State
------------      -----------   -------------------   --------
192.168.1.1        10.0.1.1        1/1                Full
192.168.1.2        11.0.1.1        1/2                Full
192.168.1.3        12.0.1.1        1/3                Full
192.168.1.4        13.0.1.1        1/4                Full
```

The neighbor relationships can have the following states:

| | |
|---|---|
| Down | No hello packets received yet |
| Init | Receiving hello packets |
| 2-way | Bidirectional communication, determination of the DR and the BDR |
| Exstart | Determination of master/slave for LSA exchange |
| Exchange | LSAs are exchanged or flooded |
| Loading | Completion of the LSA exchange |
| Full | Data basis complete and uniform in the area. Routes can now be calculated |

# 7.4 Synchronization of the LSD

The central part of the OSPF is the link state database (LSD). This database contains a description of the network and the states of all the routers. It is the source for calculating the routing table. It reflects the topology of the network. It is set up after the designated router or the backup designated router has been determined within an area (Broadcast networks).

To set up the LSD and update any topology changes, the OSPF router sends link status advertisements (LSA) to all the directly accessible OSPF routers. These link status advertisements consist of the interfaces and the neighbors of the sending OSPF router that can be reached via these interfaces. OSPF routers put this information into their databases and flood the information to all the ports.

If no topology changes occur, every router repeats its own LSAs every 30 minutes.

You can view the content of the Link State Database with the CLI command “show ip ospf database”, whereby the entries are output in accordance with the areas.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `show ip ospf database` | Displays the neighbor relationships of the router. |

```
Router Link States (Area 0.0.0.0)

Link Id        Adv Router     Age   Sequence Chksm  Options Rtr Opt
--------------- --------------- ----- -------- ------ ------- -----
192.168.1.1     192.168.1.1     122   80000007 0x5380 -E----  ---E-
192.169.1.1     192.169.1.1     120   80000007 0xbf0e -E----  ---E-

                Network Link States (Area 0.0.0.0)

Link Id        Adv Router     Age   Sequence Chksm  Options Rtr Opt
--------------- --------------- ----- -------- ------ ------- -----
10.0.1.2        192.169.1.1      129   80000002 0xad5a -E----
11.0.1.2        192.169.1.1      135   80000002 0xa066 -E----
12.0.1.2        192.169.1.1      137   80000002 0x9372 -E----
13.0.1.2        192.169.1.1      132   80000002 0x867e -E----

                AS External States

Link Id        Adv Router     Age   Sequence Chksm  Options Rtr Opt
--------------- --------------- ----- -------- ------ ------- -----
192.169.0.0     192.169.1.1      178   80000002 0xca1c
```

The interpretation of the link ID presented depends on the corresponding LSA type:

| | |
|---|---|
| Router Link States | Link ID corresponds to router ID of source |
| Network Link States | Link ID corresponds to interface IP address of the designated router |
| Network Summary States | Link ID corresponds to the corresponding network |
| Summary ASBR States | Link ID corresponds to router ID of described ASBR |
| AS External States | Link ID corresponds to the external network |

# 7.5 Route Calculation

After the LSDs are learned and the neighbor relationships go to the full state, every router calculates a path to every destination using the Shortest Path First (SPF) algorithm. After the optimal path to every destination has been determined, these routes are entered in the routing table. The route calculation is generally based on the accessibility of a hop and the metric (costs). The costs are added up over all the hops to the destination.

The costs of an individual router interface are based on the available bandwidth of this link. The calculation for the standard setting is based on the following formula:

Metric = 10 000 000 / bandwidth (bits/sec) .

For Ethernet, this leads to the following costs:

| | |
|---|---|
| 10 Mbit | 10 |
| 100 Mbit | 1 |
| 1000 Mbit | 1 (0.1 rounded up to 1) |

The table shows that this form of calculation in the standard configuration does not permit any distinction between Fast Ethernet and Gigabit Ethernet. You can change the standard configuration by assigning a different value for the costs to each OSPF interface. This enables you to differentiate between Fast Ethernet and Gigabit Ethernet.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `interface 1/1` | Switch to the Interface Configuration mode of interface 1/1. |
| `ip ospf cost 2` | Assigns the value 2 to port 1.1 for the OSPF costs. |

# 7.6 Configuring OSPF

In the state on delivery, the default values are selected so that you can configure simple OSPF functions in just a few steps.
After the router interface is defined and OSPF is switched on, OSPF automatically enters the required routes in the routing table.

The example (see figure 37) shows a simple OSPF configuration. Area 0 is already defined in the state on delivery. The terminal devices do not have an OSPF function, so you do not have to activate OSPF on the corresponding router interface. By activating the redistribute function, you can inject the routes to the terminal devices into the OSPF.

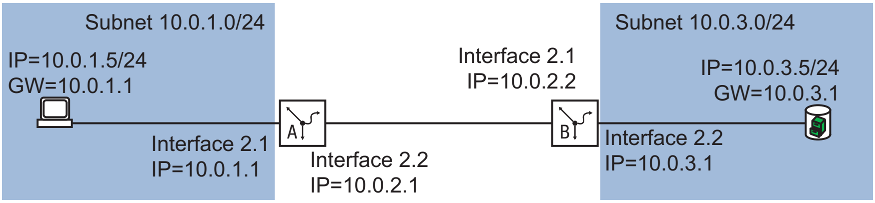


*Figure 37: Example of the configuration of OSPF*

The configuration of OSPF requires the following steps:

- Configure router interfaces – assign IP address and network mask.
- Switch on OSPF at port.
- Switch on OSPF globally.
- Switch on routing globally (if this has not already been done).

## Configuration for router B

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `interface 2/2` | Switch to the Interface Configuration mode of interface 2.2. |
| `ip address 10.0.3.1 255.255.255.0` | Assign the IP parameters to the port. |
| `routing` | Switch on the router function at this port. |
| `exit` | Switch to the Configuration mode. |
| `interface 2/1` | Switch to the interface configuration mode of interface 2.1 to set up OSPF. |
| `ip address 10.0.2.2 255.255.255.0` | Assign the IP parameters to the port. |
| `routing` | Switch on the router function at this port. |
| `ip ospf` | Switch on OSPF at this port. |
| `exit` | Switch to the Configuration mode. |
| `router ospf` | Switch to the Router Configuration mode. |
| `enable` | Switch on OSPF globally. |
| `router-id 10.0.2.2` | Assign router ID 10.0.2.2 to router B. |
| `redistribute connected subnets` | Instruct OSPF to<br>- send the routes of the locally connected interfaces along with the learned routes in the RIP information and<br>- include subnetworks without OSPF in OSPF (CIDR). |
| `exit` | Switch to the Configuration mode. |
| `exit` | Switch to the privileged EXEC mode. |
| `show ip ospf` | Check the settings for the global OSPF configuration. |

```
Router ID................................... 10.0.2.2
OSPF Admin Mode............................. Enable
ASBR Mode................................... Enable
RFC 1583 Compatibility...................... Enable
ABR Status.................................. Disable
Exit Overflow Interval...................... 0
External LSA Count.......................... 0
External LSA Checksum....................... 0
New LSAs Originated......................... 0
LSAs Received............................... 0
External LSDB Limit......................... No Limit
Default Metric.............................. Not configured

Default Route Advertise..................... Disabled
Always...................................... FALSE
Metric......................................
Metric Type................................. External Type 2
Maximum Paths............................... 4

Redistributing..............................
Source...................................... Connected
Metric...................................... Not Configured
--More-- or (q)uit
Metric Type................................. 2
Tag......................................... 0
Subnets..................................... Yes
Distribute List............................. Not configured
```

`show ip ospf interface brief` Check the settings for the OSPF interface configuration.

```
                         Router   Hello  Dead  Retrax Retrax LSAAck
Interface AdminMode Area ID    Priority Intval Intval Intval Delay
Intval
--------- --------- ----------- -------- ------ ------ ------ -----
2/1       Enable    0.0.0.0     1        10     40     5      1     1
2/2       Disable   0.0.0.0     1        10     40     5      1     1
```

`configure` Switch to the Configuration mode.

`ip routing` Switch on the router function globally.

`exit` Switch to the privileged EXEC mode.

□ Also perform the corresponding configuration on the other OSPF routers.

`show ip ospf neighbor brief` Check the OSPF neighborhood relationships.

```
   Router ID         IP Address     Neighbor Interface     State
----------------    -----------    -------------------    ---------
10.0.2.1            10.0.2.1            2/1               Full
```

```
show ip route
```

Verify the routing table:

```
Total Number of Routes......................... 3

   Network           Subnet                         Next Hop    Next Hop
   Address            Mask           Protocol        Intf     IP Address
--------------- --------------- ------------  ------  -------------
10.0.1.0        255.255.255.0   OSPF Ext T2    2/1       10.0.2.1
10.0.2.0        255.255.255.0   Local          2/1       10.0.2.2
10.0.3.0        255.255.255.0   Local          2/2       10.0.3.1
```

# 8 Protocol-based VLANs

Along with port-based VLANs based on IEEE 802.1Q, the Switch also supports protocol-based VLANs based on IEEE 802.1v.

With port-based VLANs, the Switch uses the port VLAN ID of the receiving port to determine which VLAN a data packet belongs to if it is received without a VLAN tag.

With protocol-based VLANs, the Switch uses the protocol of the received data packet to determine which VLAN a data packet belongs to if it is received without a VLAN tag. The Switch supports the protocols

- IP,
- ARP,
- IPX.

Data packets from other protocols received without a VLAN tag are assigned to a VLAN by the Switch in accordance with the port VLAN ID.

For the VLAN assignment, the Switch takes into account

- firstly, the VLAN tag,
- then the protocol the data packet belongs to,
- and finally, the port VLAN ID.

Protocol-based VLANs enable you to transfer data packets not relevant to routing across IP subnetwork boundaries. Data packets relevant to routing are IP and ARP data packets.

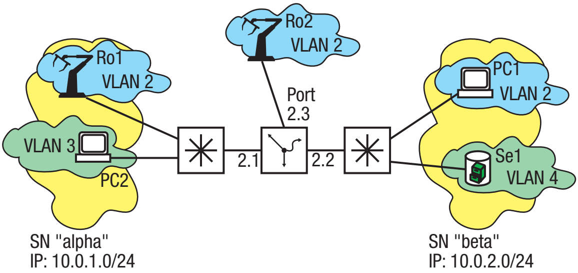


*Figure 38: Example of a protocol-based VLAN*

In the example (see figure 38), PC2 and Se1 communicate via IP. These data packets are routed.
The devices Ro1, Ro2 and PC1 communicate via other Ethernet-based protocols. These data packets are switched in VLAN 2.
Thus all IP data packets remain in their subnetworks, apart from the IP data packets that are meant for a different subnetwork.

# 8.1 General Configuration

☐ Create a VLAN protocol group for each subnetwork.

☐ Assign the protocols to the VLAN protocol group for each subnetwork.

☐ Create the VLANs.

☐ Switch on the VLAN routing in the VLANs affected and thus create the virtual router interfaces.

☐ Assign the VLAN protocol groups to the VLANs.

☐ Configure the port interfaces:
- ▶ VLAN membership
- ▶ Port VLAN ID for non-ARP/IP data packets
- ▶ Port of a VLAN protocol group and thus assign to a VLAN

☐ Configure virtual router interfaces:
- ▶ Assign IP address
- ▶ Switch on routing

☐ Switch on routing globally.

# 8.2 Configuration of the Example

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `vlan protocol group alpha` | Create VLAN protocol group 1 for alpha subnetwork. |
| `vlan protocol group beta` | Create VLAN protocol group 2 for beta subnetwork. |
| `exit` | Switch to the privileged EXEC mode. |
| `show protocol all` | Display the VLAN protocol groups created. |

```
                  Group
   Group Name       ID    Protocol(s)  VLAN       Interface(s)
----------------  ------  -----------  ----  ---------------------
alpha             1                    0
beta              2                    0
```

| | |
|---|---|
| `configure` | Switch to the Configuration mode. |
| `vlan protocol group add protocol 1 ip` | Add IP of VLAN protocol group 1. |
| `vlan protocol group add protocol 1 arp` | Add ARP of VLAN protocol group 1. |
| `vlan protocol group add protocol 2 ip` | Add IP of VLAN protocol group 2. |
| `vlan protocol group add protocol 2 arp` | Add ARP of VLAN protocol group 2. |
| `exit` | Switch to the privileged EXEC mode. |
| `show protocol all` | Display the protocols assigned to the protocol groups. |

```
                  Group
   Group Name       ID    Protocol(s)  VLAN       Interface(s)
----------------  ------  -----------  ----  ------------------
alpha             1       IP,ARP       0
beta              2       IP,ARP       0
```

| | |
|---|---|
| `vlan database` | Switch to the VLAN mode. |
| `vlan 2` | Create VLAN 2. |
| `vlan 3` | Create VLAN 3. |
| `vlan 4` | Create VLAN 4. |
| `vlan routing 3` | Create a virtual router interface and activate the routing function for this interface. |

| | |
|---|---|
| `vlan routing 4` | Create a virtual router interface and activate the routing function for this interface. |
| `protocol group 1 3` | Assign VLAN protocol group 1 to VLAN 3. |
| `protocol group 2 4` | Assign VLAN protocol group 2 to VLAN 4. |
| `exit` | Switch to the privileged EXEC mode. |
| `show protocol all` | Display the protocols and VLANs assigned to the VLAN protocol groups. |

```
                     Group
   Group Name         ID     Protocol(s)  VLAN       Interface(s)
----------------  ------  -----------  ----  ----------------------
alpha              1       IP,ARP       3
beta               2       IP,ARP       4
```

| | |
|---|---|
| `show ip vlan` | Display the assignment of the virtual router interfaces to the VLANs. |

```
           Logical
VLAN ID   Interface     IP Address      Subnet Mask       MAC Address
-------  -----------  ---------------  ---------------  -----------
3        9/1         0.0.0.0         0.0.0.0          00:80:63:51:74:2C
4        9/2         0.0.0.0         0.0.0.0          00:80:63:51:74:2D
```

| | |
|---|---|
| `configure` | Switch to the Configuration mode. |
| `interface 2/1` | Switch to the Interface Configuration mode of interface 2.1. |
| `vlan participation exclude 1` | Remove port 2.1 from VLAN 1. |
| `vlan participation include 2` | Declare port 2.1 a member of VLAN 2. |
| `vlan participation include 3` | Declare port 2.1 a member of VLAN 3. |
| `vlan pvid 2` | Set the port VLAN ID to 2, which means that the Switch assigns non-IP/ARP data packets to VLAN 2. |
| `protocol vlan group 1` | Assign VLAN protocol group 1 to interface 2.1, which means that the Switch assigns IP/ARP data packets to VLAN 3. |
| `exit` | Switch to the Configuration mode. |
| `interface 2/2` | Switch to the Interface Configuration mode of interface 2.2. |
| `vlan participation exclude 1` | Remove port 2.2 from VLAN 2. |
| `vlan participation include 2` | Declare port 2.2 a member of VLAN 2. |
| `vlan participation include 4` | Declare port 2.2 a member of VLAN 4. |
| `vlan pvid 2` | Set the port VLAN ID to 2, which means that the Switch assigns non-IP/ARP data packets to VLAN 2. |

| | |
|---|---|
| `protocol vlan group 2` | Assign VLAN protocol group 2 to interface 2.2, which means that the Switch assigns IP/ARP data packets to VLAN 4. |
| `exit` | Switch to the Configuration mode. |
| `interface 2/3` | Switch to the Interface Configuration mode of interface 2.3. |
| `vlan participation exclude 1` | Remove port 2.3 from VLAN 1. |
| `vlan participation include 2` | Declare port 2.3 a member of VLAN 2. |
| `vlan pvid 2` | Set the port VLAN-ID to 2, which means that data packets that are received without a tag at that port are assigned to VLAN 2 by the Switch. |
| `exit` | Switch to the Configuration mode. |
| `interface 9/1` | Switch to the interface configuration mode of interface 9/1. |
| `ip address 10.0.1.1 255.255.255.0` | Assign the IP parameters to the router interface. |
| `routing` | Activate the router function at this interface. |
| `exit` | Switch to the Configuration mode. |
| `interface 9/2` | Switch to the interface configuration mode of interface 9/2. |
| `ip address 10.0.2.1 255.255.255.0` | Assign the IP parameters to the router interface. |
| `routing` | Activate the router function at this interface. |
| `exit` | Switch to the Configuration mode. |
| `exit` | Switch to the privileged EXEC mode. |
| `show ip interface brief` | Display the entries of the virtual router interface. |

```
                                                Netdir    Multi
Interface IP Address      IP Mask              Bcast     CastFwd
--------- --------------- --------------- -------- --------
9/1       10.0.1.1        255.255.255.0   Disable  Disable
9/2       10.0.2.1        255.255.255.0   Disable  Disable
```

| | |
|---|---|
| `configure` | Switch to the Configuration mode. |
| `ip routing` | Switch on the router function globally. |

# 9 Multicast Routing

Multicast data streams are data packets that a sender sends to multiple recipients. To reduce the network load, the sender uses a Multicast address. He thus sends each packet only once to the Multicast address instead of sending it to each recipient individually. The recipients recognize a Multicast data stream intended for them by the Multicast address.

A common reason for introducing subnetworks is the restriction of Broadcast data streams. Switches flood Broadcast/Multicast data streams to all ports, while routers block Broadcast/Multicast data streams. Multicast routing enables you to accurately transmit Multicast data streams beyond the boundaries of subnetworks. Accurate transmission means sending data streams with defined Multicast addresses exclusively to those devices that want to receive the Multicast data stream.

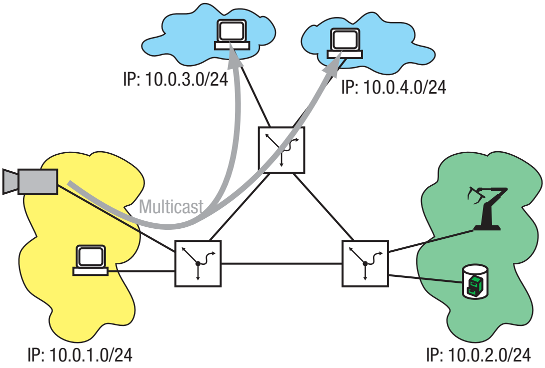


*Figure 39: Example of a Multicast application*

To the use of Multicast routing pertains:

- Defined Multicast addresses
- A protocol for Multicast group registration that organizes the exchange of information by means of Multicast data streams (e.g. IGMP). This information relates to the reporting that network participants wish to receive Multicast data streams and querying this wish by means of intermediate devices.
- A protocol that guides the Multicast data streams in accordance with the information on Multicast data streams (e.g. PIM-DM, DVMRP).

# 9.1 Multicast Addresses

## 9.1.1 IP Multicast Addresses

The IANA (Internet Assigned Numbers Authority) defines the IP addresses of the class D IP address space as Multicast addresses. IP Multicast addresses are in the range from 224.0.0.0 to 239.255.255.255.

| IP address range | Assignment |
|---|---|
| 224.0.0.0 | Base address, reserved |
| 224.0.0.1 - 224.0.0.255 | Local Network Control Block, reserved for routing protocols, IGMP, etc. For example:<br>224.0.0.1 - all hosts of a subnetwork<br>224.0.0.2 - all routers of a subnetwork<br>224.0.0.4 - all DVMRP routers<br>224.0.0.5 - all OSPF routers<br>224.0.0.6 - all OSPF DR routers<br>224.0.0.9 - all RIP v2 routers<br>224.0.0.13 - all PIM routers<br>224.0.0.18 - all VRRP routers<br>224.0.0.22 - all IGMP v3 reports |
| 224.0.1.0 - 224.0.1.255 | Internetwork Control Block |
| 224.0.2.0 - 224.0.255.255 | AD HOC Block |
| 224.1.0.0 - 238.255.255.255 | Various organizations, protocols, applications, reservations. For example:<br>232.0.0.0-232.255.255.255 - Source-specific Multicasts |
| 239.0.0.0 - 239.255.255.255 | Administratively scoped IP v4 Multicast space<br>These Multicast addresses are not transferred by any router beyond the local boundaries and into the Internet. Therefore the administrator can assign these addresses any way he wants within these local boundaries. |

*Table 13: Assignment of the IP Multicast address range*

The administratively scoped IP v4 Multicast area is subdivided further by the IANA:

| IP address range | Assignment |
|---|---|
| 239.000.000.000 - 239.191.255.255 | Reserved [IANA] |
| 239.192.000.000 - 239.251.255.255 | Organization-local scope [Meyer, RFC2365] |
| 239.252.000.000 - 239.254.255.255 | Site-local scope (reserved) [Meyer, RFC2365] |
| 239.255.000.000 - 239.255.255.255 | Site-local scope [Meyer, RFC2365] |

*Table 14: Assignment of the administratively scoped IP v4 Multicast area*

In the end, the following multicast IP adress ranges are left over for disposal by an organisation's administrator:

- 239.192.000.000 - 239.251.255.255
  for an organisation's local areas.
- 239.255.000.000 - 239.255.255.255
  for an organisation's entire area.

**Note:** When selecting the Multicast IP addresses, ensure that they can be uniquely mapped onto MAC Multicast addresses (see on page 122 “Mapping IP MAC Multicast Addresses”).

## 9.1.2 MAC Multicast Addresses

The IEEE calls the 48-bit MAC address an “Extended Unique Identifier”. It is the unique identifier of a device. The first 24 bits of the MAC address (Organizationally Unique Identifier, OUI) is assigned by the IEEE to the manufacturer. The manufacturer uses the last 24 bits to uniquely identify their device interfaces.

A number of MAC addresses are reserved for specific applications:

| MAC-Address | Type | Use |
|---|---|---|
| 01-00-5E-00-00-00 | 0800 | Internet Multicast [RFC1112] |
| 01-80-C2-00-00-00 | -802- | Spanning tree (for bridges) |
| FF-FF-FF-FF-FF-FF | 0806 | ARP (for IP and CHAOS) as needed |
| FF-FF-FF-FF-FF-FF | 8035 | Reverse ARP |

*Table 15: Examples of reserved MAC addresses*

## 9.1.3 Mapping IP MAC Multicast Addresses

When IP data packets are sent via Ethernet, the IP address is assigned to a MAC address, and therefore IP Multicast addresses are also mapped onto MAC Multicast addresses.
The 23 lower-value bits of the 32-bit IP Multicast address make up the 23 lower-value bits of the 48-bit MAC Multicast address.
Of the remaining 9 bits of the IP Multicast address, 4 bits are used as the class D identification for the Multicast address.
The remaining 5 bits ensure that 32 IP Multicast addresses can be mapped onto one and the same MAC Multicast address.

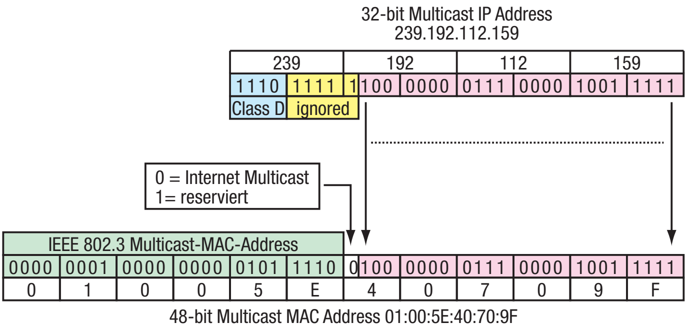


*Figure 40: Conversion of the IP address to the MAC address*

## 9.2 Multicast Group Registration

The Internet Group Management Protocol (IGMP) describes the distribution of Multicast information between routers and terminal devices on Layer 3. Routers with an active IGMP function periodically send queries to find out which IP Multicast group members are connected to the LAN, or to find out who is interested in becoming a group member.
Multicast group members reply with a Report message. This Report message contains all the parameters required by the IGMP. The router records the IP Multicast group address from the Report message in its routing table. The result of this is that it transfers frames with this IP Multicast group address in the target address field only in accordance with the routing table.
Devices which no longer want to be members of a Multicast group can cancel their membership by means of a Leave message (from IGMP version 2), and they do not transmit any more Report messages. The router removes the routing table entry if it does not receive any Report messages within a specified period of time (aging time).

If there are multiple routers with an active IGMP function in the subnetwork, then

- for IGMP version 1, all routers in this subnetwork periodically send queries
- for IGMP versions 2 and 3, the routers decide which router takes over the query function (Querier Election).

| Protocol | Standard |
|---|---|
| IGMP v1 | RFC 1112 |
| IGMP v2 | RFC 2236 |
| IGMP v3 | RFC 3376 |

*Table 16: Standards which describe the Multicast Group Membership Discovery*

An advantage that IGMP version 2 has over IGMP version 1 is that a Multicast recipient can cancel his membership in a Multicast group, thus freeing up his bandwidth more quickly. Another advantage is the introduction of the Querier Election.

IGMP version 3 provides more security with the Source Filtering option. Multicast recipients can define the sources from which they want to receive Multicast data streams. The router blocks Multicast data streams with other source addresses.

The different versions of IGMP are compatible downwards.
This means that an IGMP version 3 router can also process version 1 and version 2. If there are different IGMP versions in a subnetwork, the participating routers agree on the smallest version.

# 9.3 PIM-DM/PIM-SM/DVMRP

The DVMRP (Distance Vector Multicast Routing Protocol) is a routing protocol that uses its own distance vector algorithm to create its own Multicast routing table. DVMRP works similarly to RIP and is limited to 32 hops.
In the past, DVMRP was very widely-used, and it is used today because of its compatibility with existing applications.

PIM-DM (Protocol Independent Multicast - Dense Mode) is a routing protocol that uses the available Unicast routing table of other protocols to steer Multicast data streams.
This ability, and the fast convergence it enables, is the reason why PIM-DM is now very widely-used.

DVRP and PIM-DM use what is known as the Implicit Join method, which means that a participant who has left the Multicast data stream is not included in the data flow. To enable a participant who has left to receive Multicast data streams again, the routers transmit to all participants again after the hold time has elapsed. For DVMRP, the hold time is fixed at 2 hours. For PIM-DM, the variable hold time is set at 210 seconds. PIM-DM requires that you set the hold time to the same value for all the participating routers.

| DVMRP | PIM-DM |
|---|---|
| Knows the topology better because DVMRP uses its own protocol. | Fast convergence<br>Optimization through changeable timers |

*Table 17: Advantages of the protocols*

PIM-SM (Protocol Independent Multicast - Sparse Mode) is an extended variant of PIM-DM.
This version of PIM is mainly suitable for networks with a restricted bandwidth (e.g. WANs) and for networks with few participants from Multicast groups.

PIM-SM differs from PIM-DM and DVMRP in the following ways, as regards subscribing and unsubscribing participants:

- PIM-DM and DVMRP assume that very many participants are interested in the Multicast groups. Therefore, at the start of the communication, PIM-DM and DVMRP flood the information about available Multicast groups into the entire network. Participants who are not interested in a Multicast group unsubscribe from this group explicitly.
- In contrast, PIM-SM assumes that very few participants in the network are interested in the Multicast groups. PIM-SM waits for the participants to actively subscribe without itself sending information about available Multicast groups to the network. All participants who are interested in a Multicast group subscribe to a group explicitly. With this procedure, PIM-SM reduces the data traffic in the network.

## 9.3.1 How PIM-DM and DVMRP function

In the first step for setting up the Multicast routes, a PIM-DM/DVMRP router floods Multicast data streams to all ports, with the exception of the receiving port (= flooding).

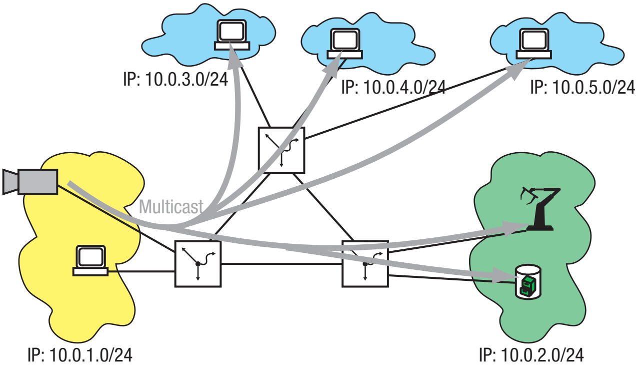


*Figure 41: Multicast Flooding*

Routers that are not interested in the Multicast data stream send what are known as prune messages so that they will not be sent any Multicast data streams from this source in the future.
The routers send the prune messages back in the direction from which they received the Multicast data streams (upstream).

A router transmits a Multicast data stream until the hold time has elapsed,

- when it is using IGMP to determine a Multicast recipient which is connected to a port directly or via a switch or
- when a router that is connected to a Multicast recipient is connected directly to a port.

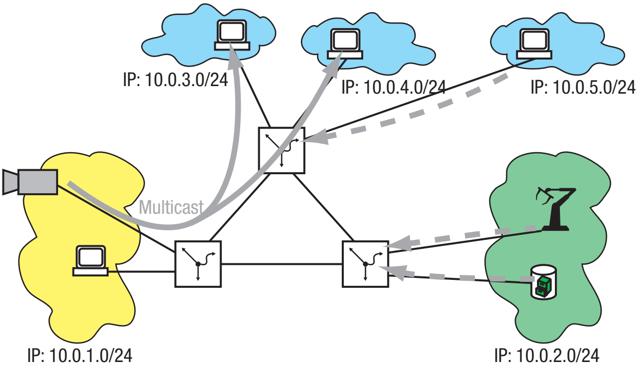


*Figure 42: Multicast Pruning*

In the second step, PIM-DM/DVMRP calculates the shortest paths (STP - Shortest Path Tree) between the Multicast source and the Multicast recipients. The result is the source-routed Multicast distribution tree. Source-routed means that the calculation method is tracing back from the recipient to the source (RPF - Reverse Path Forwarding). To avoid loops, RPF rejects all Multicast data streams received at a port that belongs to a longer path than the shortest path.

The method of the shortest paths is very efficient with regard to the data paths. However, it does have the disadvantage that, depending on the topology, the routers require a lot of memory space to store the many Multicast trees.

A participant who has unsubscribed from the Multicast data stream can subscribe to the Multicast data stream again. This procedure is known as grafting. Grafting enables the participant to receive Multicast data streams again before the hold time has elapsed.

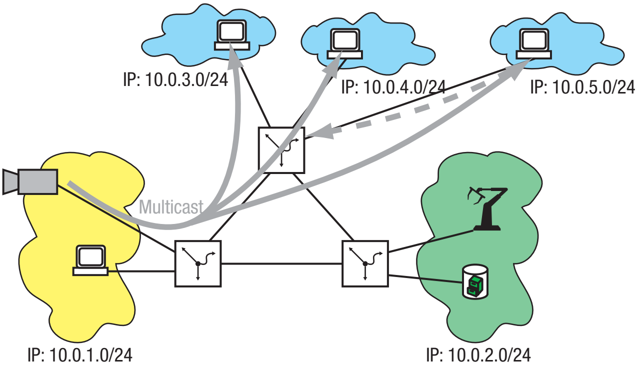


*Figure 43: Multicast Grafting*

### 9.3.2 How PIM-SM functions

PIM-SM differs from PIM-DM and DVMRP with regard to the topology of the Multicast distribution:

- PIM-DM and DVMRP always use the direct paths (SPT - Shortest Path Tree) between the Multicast source and the Multicast recipients.
- With the standard setting, PIM-SM uses the path via a central transmission point (Rendezvous Point – RP). This path is known as the Rendezvous Point Tree (RPT). At the rendezvous point, the Multicast recipients report their interest in a Multicast group. The Multicast sources register at a rendezvous point and send the data exclusively to this rendezvous point, which forwards the data to the Multicast recipients. There is exactly one rendezvous point for each group. A PIM-SM router serves as the rendezvous point for one or more Multicast groups. The rendezvous point tree extends between the rendezvous point of the Multicast group and the Multicast recipients. The recipients of a Multicast group share this RPT as a shared tree. With this procedure, PIM-SM reduces the amount of stored tree information in the routes and thus reduces the processor load for the devices.

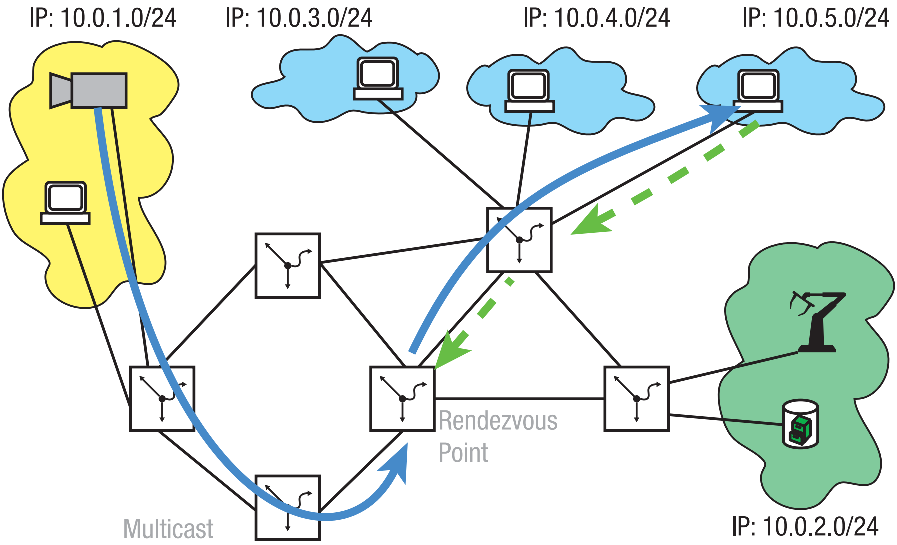


*Figure 44: Rendezvous Point in the PIM-SM protocol*

Depending on the application, there are shorter paths between the Multicast recipients and the Multicast source than the rendezvous point tree. In these cases, PIM-SM enables a switch to the direct path SPT. If the data rate for the Multicast transmission via the RPT exceeds a configurable threshold value, the router of the Multicast recipient unsubscribes from the rendezvous point. Instead, the router of the Multicast recipient creates a direct link to the last router before the Multicast source.

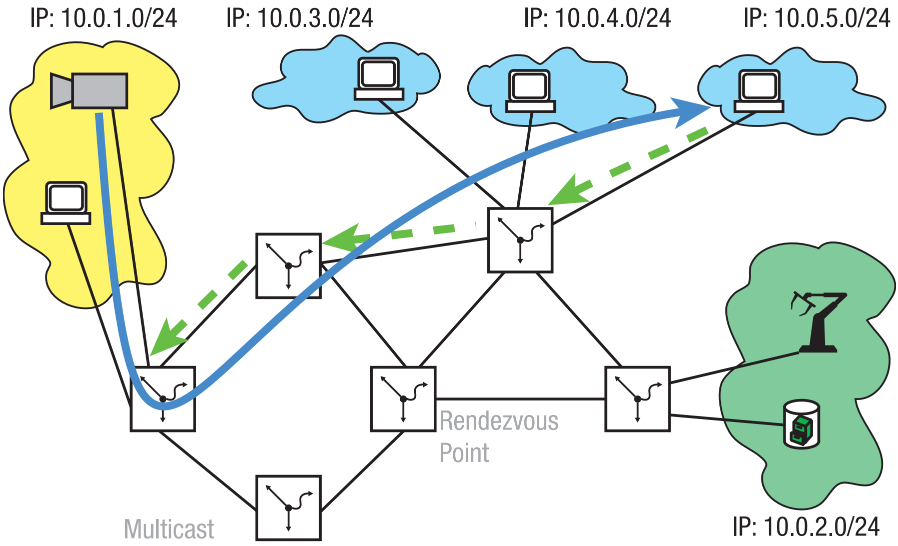


*Figure 45: Topology change from the RPT to the direct path (STP)*

- **Designated Router**
  A participant who is interested in a Multicast group sends a corresponding IGMP message to the next reachable router. This router then sends a join message in the direction of the rendezvous point. If there are additional routers between the sending router and the rendezvous point, these forward the join message. This transmission ends either at the rendezvous point itself or at an already existing branch of the RPT. After the participant subscribes, PIM-SM creates or extends the path between the rendezvous point and the participant. When a participant unsubscribes from a Multicast group, the next router reachable from the participant sends a prune message to the rendezvous point. The prune message thus removes the related branch from the RPT.
  In a network with multiple PIM-SM routers, exactly one router takes over the transmission of the join and prune messages between the Multicast recipients and the rendezvous point. In the following figure, this procedure is represented by green arrows. On the side of the Multicast sources, one of the PIM-SM routers also registers the available Multicast groups at the rendezvous point. The figure uses blue arrows to show this procedure. These routers are called designated routers (DR). In the standard setting,

the routers select the designated router using the IP address. The PIM-SM router with the highest IP address in a network segment takes over the task of the designated router. The DR selection can be controlled by setting a special priority for the designated routers. In this case, the router with the highest priority takes over the tasks of the designated router. The IP address is only used in the selection process if the priorities are the same.

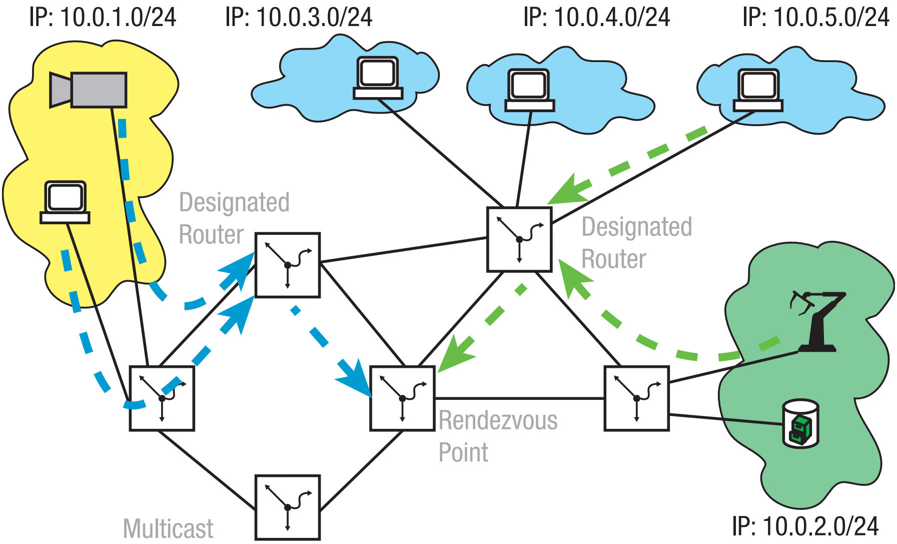


*Figure 46: Designated routers forward messages from Multicast sources and Multicast participants to the rendezvous point*

- **Bootstrap router**
  PIM-SM provides two procedures for selecting the rendezvous point for a Multicast group:

  - Static RP configuration

    In this procedure, one of the routers in the network is fixed as the rendezvous point for a Multicast group. The other routers contain the IP address of this router and the address of the related Multicast group in their configuration.

  - Dynamic RP configuration based on the Bootstrap Router procedure (BSR)

    In this procedure, the routers in the network determine the rendezvous point dynamically. A router has the option to offer itself as a candidate for the task of rendezvous point. The dynamic procedure uses bootstrap routers to select the rendezvous point for a Multicast group. The bootstrap messages also inform the other routers in the PIM-SM domain about the router selected as the rendezvous point. The PIM-SM routers forward the Bootstrap messages within the PIM-SM domain. The PIM-SM domain consists of all the reachable routers with an activated PIM-SM protocol. An active PIM-SM router has the option of limiting the domain as a BSR border. A router configured in this way drops the received BSR messages.

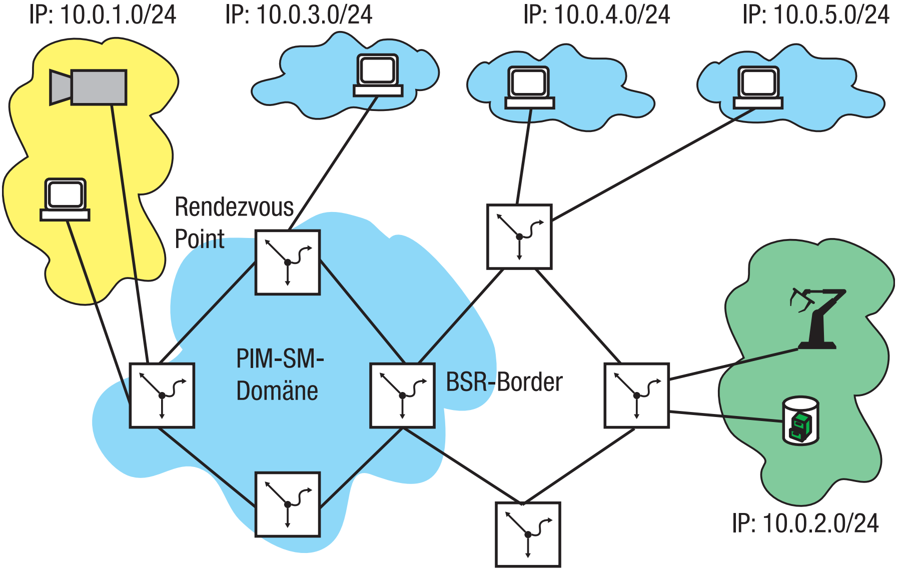


*Figure 47: Routers in the configuration as BSR borders drop bootstrap messages and limit the PIM-SM domain*

## Application example for PIM-SM

The following example shows you how you can configure PIM-SM using the Command Line Interface.

Task assignment:

- Set up a PIM-SM example configuration (see following figure).
- Configure IGMP, OSPF and PIM-SM.
- Configure RP statically.
- Use Multicast address range 239.1.0.0/16.

**Note:** The Unicast (UC) protocol used in the example is OSPF. You can also use RIP instead of OSPF.

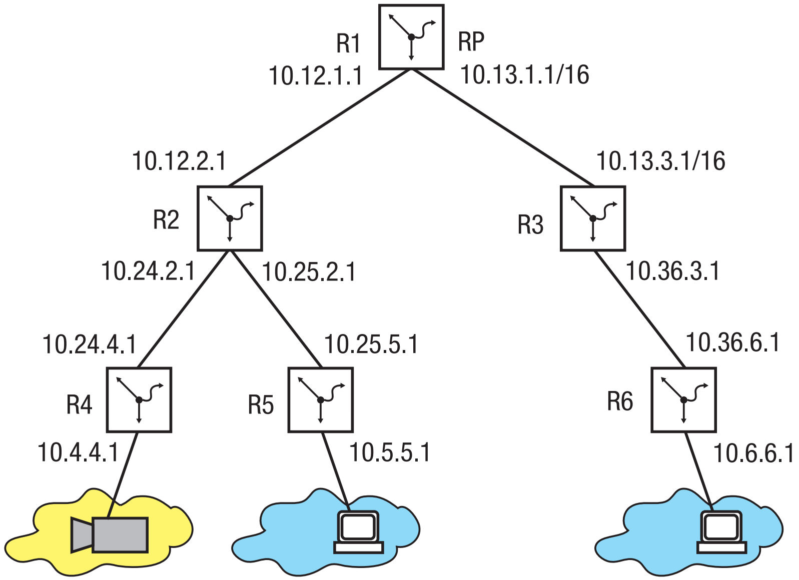


*Figure 48: Example configuration for PIM-SM*

☐ You use the following CLI command sequence to configure PIM-SM.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `# set prompt Rx` | Set input prompt for better orientation (replace x by router number) |
| # configure | Switch to the configuration mode. |
| (Config)# ip routing | Enable routing |
| (Config)# show ip brief | Display overview of IP information. |
| (Config)# router ospf | Configure UC routing protocol globally.<br>Switch to the router configuration mode for OSPF (Open Shortest Path First). |
| (Config-router)# router-id x.1.1.1 | |
| (Config-router)# enable | |
| (Config-router)# redistribute connected [subnets] | |
| (Config-router)# exit | Switch back to the configuration mode. |
| (Config)# ip igmp | Enable IGMP globally (automatically enables MC routing and IGMP snooping). |
| (Config)# ip multicast | Enable Multicast forwarding (routing). |
| (Config)# ip pimsm | Enable PIM-SM globally. |

| | |
|---|---|
| (Config)# ip pimsm rp-address <ip-@> <MC @>… | Set the static Rendezvous Point for a Multicast range. |
| (Config)# interface <s/p> | Configure routing interfaces (slot/port). |
| (Interface s/p)# ip address <ip-@> <mask> | Configure IP address and subnetwork mask for the interface. |
| (Interface s/p)# routing | Enable routing at the interface. |
| (Interface s/p)# ip ospf area-id 0.0.0.0 | Configure UC routing protocol for each interface. |
| (Interface s/p)# ip ospf | Activate OSPF on the interface. |
| (Interface s/p)# ip igmp | Enable IGMP for each interface. |
| (Interface s/p)# ip igmp version <1\|2\|3> | Optional: Change version (default: 2). |
| (Interface s/p)# ip pimsm mode | Enable PIM-SM at the corresponding interfaces. |
| (Interface s/p)# exit | Switch to the configuration mode. |
| (Config)# exit | Switch to the privileged EXEC mode. |
| # show ip pimsm | Display PIM-SM status of the router. |
| # copy system:running-config nvram:startup-config | Save current configuration to NVRAM. |
| # logout | End CLI session. |

**Note:** Configure the rendezvous point (RP) on all routers on which you have enabled PIM-SM, also on the RP itself.
Alternatively, define at least one bootstrap router (BSR) and at least one RP candidate.
If you want to use the advantages of the redundancy function, configure 2 RP candidates and 2 BSR candidates.

□ The following CLI show commands show the PIM-SM, Multicast and IGMP parameters for your current configuration.

| | |
|---|---|
| `(Interface s/p)# show` | Display the possible show commands. |
| # show ip pimsm | Display the current PIM-SM configuration. |
| # show ip mcast | Display the current Multicast configuration. |
| # show ip igmp | Display the current IGMP configuration. |

□ You can optionally perform the following configurations afterwards:

| | |
|---|---|
| `(Interface s/p)# ip pimsm dr-priority <0…2.147.483.647>` | Configure DR priority. |
| (Interface s/p)# ip pimsm hello-interval <0…18000> | Configure Hello Interval in seconds (default: 30 s). |

□ Optional: Instead of defining the RPs statically, you can configure BSR and RP candidates, from which BSR and RP are selected.

| | |
|---|---|
| `(Config)# ip pimsm bsr-candidate interface <slot/port>` | Configure BSR candidate. |
| `(Config)# ip pimsm rp-candidate interface <slot/port>` | Configure RP candidate. |

# 9.4 Scoping

In the Multicast transmission, the protocol provides two options for limiting the expansion of the Multicast data stream:

- Multicast Address Scoping / Boundary
  In the Multicast Address Scoping, the administrator assigns a Multicast IP address range to a router interface (see table 14). The router interface blocks the Multicast data streams with addresses within this address range.
  Example:
  `ip mcast boundary 239.193.122.0 255.255.255.0`
  In this example, the router interface blocks Multicast data streams with a Multicast IP address in the range 239.193.122.0-239.193.122.255.

- TTL Scoping
  Every Multicast data packet contains a TTL (Time To Live) The TTL is a counter which each router de-increments when it transmits a Multicast data packet.
  In TTL Scoping, the administrator assigns a TTL threshold to an interface. The router interface blocks every Multicast data packet for which the TTL is below the TTL threshold.
  Example:
  `ip multicast ttl-threshold 64`
  In this example, the router interface blocks Multicast data streams with a TTL whose value is less than 64.

| TTL | Range |
|---|---|
| 0 | Restricted to the same host |
| 1 | Restricted to the same subnetwork |
| < 32 | Restricted to a particular location, organization or department |
| < 64 | Restricted to the same region |
| < 128 | Restricted to the same continent |
| < 255 | Unrestricted, global |

*Table 18: Usual scope for TTLs*

# 9.5 Multicast Configuration

Select the Multicast protocol that suits your application best.
As the Multicast routing protocols use different methods for the Multicast transmission, the router prevents you from using more than one Multicast routing protocol at the same time.
When one Multicast routing protocol is activated, the router deactivates any other active Multicast routing protocol.

## 9.5.1 Example with Layer 3 Redundancy

The Multicast configuration consists of the following steps:

- Configure the routing function on the participating routers - for example, with OSPF (see on page 106 “Configuring OSPF”).
- Specify Multicast addresses, if applicable.
- Configure router interfaces. This also includes
  - specifying the Multicast boundaries
  - activating IGMP and
  - activating the selected Multicast routing protocol.
- Globally activate IGMP and therefore also IGMP Snooping.
- Globally activate the Multicast routing protocol.
- Activate Multicast transmission (forwarding).

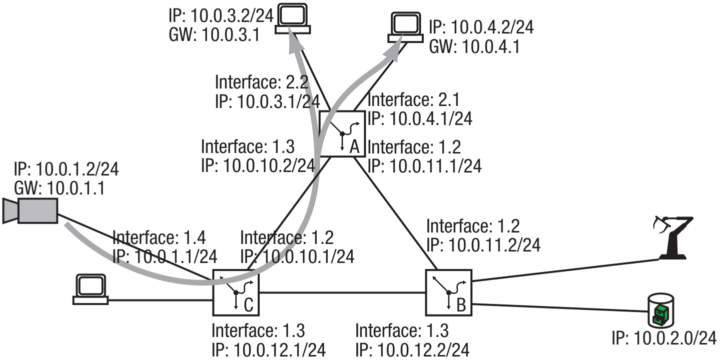


*Figure 49: Multicast example configuration*

□ Configure router interfaces using the example of router A (see figure 49):

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `interface 2/1` | Switch to the Interface Configuration mode of interface 2.1. |
| `ip multicast ttl-threshold 3` | Set threshold for Multicast expansion (see on page 139 “Scoping”). |
| `ip igmp` | Activate IGMP at port. |
| `ip pimdm mode` | Activate PIM-DM as multicast protocol. |
| `exit` | Switch to the Configuration mode. |
| `interface 2/2` | Switch to the Interface Configuration mode of interface 2.2. |
| `ip multicast ttl-threshold 3` | Set threshold for Multicast expansion (see on page 139 “Scoping”). |
| `ip igmp` | Activate IGMP at port. |
| `ip pimdm mode` | Activate PIM-DM as multicast protocol. |
| `exit` | Switch to the Configuration mode. |

| | |
|---|---|
| interface 1/3 | Switch to the Interface Configuration mode of Interface 1/3. |
| ip multicast ttl-threshold 3 | Set threshold for Multicast expansion (see on page 139 “Scoping”). |
| ip igmp | Activate IGMP at port. |
| ip pimdm mode | Activate PIM-DM as multicast protocol. |
| exit | Switch to the Configuration mode. |

□ Globally activate IGMP using the example of router A (see figure 49):

| | |
|---|---|
| ip igmp | Activate IGMP at port. |

□ Globally activate Multicast using the example of router A (see figure 49):

| | |
|---|---|
| ip pimdm | Select the Multicast routing protocol in the configuration mode. |
| ip multicast | Globally activate Multicast transmission. |
| exit | Switch to the privileged EXEC mode. |

□ Check the Multicast routing settings

```
#show ip pimdm

Admin Mode..................................... Enable

    PIM-DM INTERFACE STATUS
Interface Interface Mode  Protocol State
--------- --------------- ---------------
1/3       Enable          Operational
2/1       Enable          Operational
2/2       Enable          Operational
#show ip mcast

Admin Mode..................................... Enable
Protocol State................................. Operational
Table Max Size ................................ 256
Number Of Packets For Which Source Not Found .. 0
Number Of Packets For Which Group Not Found ... 0
Protocol....................................... PIMDM
Entry Count ................................... 0
Highest Entry Count ........................... 0
#show ip mcast mroute summary

                  Multicast Route Table Summary
                                         Incoming  Outgoing
Source IP       Group IP        Protocol Interface Interface List
--------------- --------------- -------- --------- ---------------
10.0.1.159      239.192.1.1     PIMDM    1/3       2/1
10.0.1.159      239.192.1.1     PIMDM    1/3       2/2
```

```
#show ip igmp

IGMP Admin Mode................................ Enable

    IGMP INTERFACE STATUS
Interface Interface Mode  Protocol State
--------- --------------- ---------------
1/2       Enable          Operational
1/3       Enable          Operational
2/1       Enable          Operational
2/2       Enable          Operational
#show ip igmp interface 2/1

Slot/Port...................................... 2/1
IGMP Admin Mode................................ Enable
Interface Mode................................. Enable
IGMP Version................................... 2
Query Interval (secs).......................... 125
Query Max Response Time (1/10 of a second)..... 100
Robustness..................................... 2
Startup Query Interval (secs) ................. 1
Startup Query Count............................ 2
Last Member Query Interval (1/10 of a second).. 10
Last Member Query Count........................ 2
```

□ Configure router B and router C in the same way as router A.

## 9.5.2 Example with Layer 2 redundancy (HIPER-Ring)

VLAN 1 is assigned to the HIPER-Ring.

☐ Assign other VLAN IDs to the connected VLANs and leave the HIPER-Ring exclusively in VLAN 1. You thus enable the transmission of the Multicast data streams on Layer 3.

If you assign multiple VLANs to the HIPER-Ring as transfer networks, then the Switch transmits the Multicast data streams to every transfer network during the flood and prune phase. This means that the Switch transmits the Multicast data streams to every VLAN and the network load is thus multiplied in the HIPER-Ring.

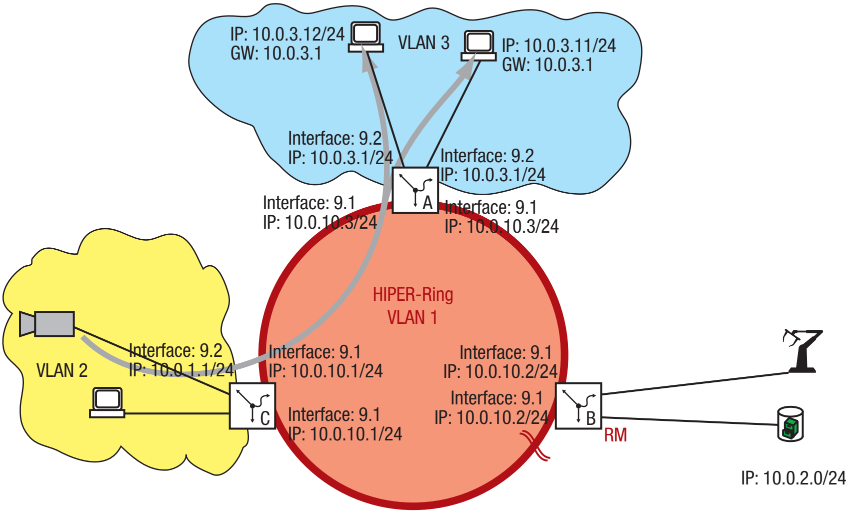


*Figure 50: Multicast example configuration with HIPER-Ring*

### 9.5.3 Tips for the configuration

- **Selection of the PIM-DM Multicast routing protocol**
  You select PIM-DM if your application requires fast switching times and is able to tolerate any packet duplications during the switching time. You set fast switching times by reducing the “Hello Time”.
  Packet duplications occur when multiple routers are connected to a subnetwork. In this case, the “Assert process” clarifies which router is permitted to send into the subnetwork. Until this is clarified, all routers send into this subnetwork.

- **Selection of the DVMRP Multicast routing protocol**
  You select DVMRP if your application does not tolerate packet duplications and is content with higher switching times.
  DVMRP provides a big advantage when you are using divided subnetworks/VLANs in a HIPER-Ring. With the Unicast table, DVMRP already knows the topology and thus prevents packet duplications.

- **Selection of the PIM-SM Multicast routing protocol**
  You select PIM-SM if your application has few participants and you can tolerate longer paths for your application.
  In this case, PIM-SM has the advantage that the data volume created in the routers remains small.

- **Configuration as Rendezvous Point for PIM-SM**
  When using PIM-SM, you have the option of defining a router as a rendezvous point candidate for a Multicast group. To do this, you specify the Multicast group for which the router can be used as the rendezvous point.

| | |
|---|---|
| `enable` | Switch to the Privileged EXEC mode. |
| `configure` | Switch to the configuration mode. |

| | |
|---|---|
| `ip pimsm rp-candidate interface 1/1 225.1.1.1 255.255.255.0` | Activate the router as the potential rendezvous point for group 225.1.1.1/24. |
| `no ip pimsm rp-candidate interface 1/1 225.1.1.1 255.255.255.0` | Deactivate the router as a potential rendezvous point. |

### Configuration of the limit for the switch to SPT

When using PIM-SM, you have the option of defining the limit for the switch to SPT on the last routers for the Multicast recipients. To do this, you specify the limit for the data throughput in Kbit/s, and when this limit is reached the router switches to the shortest path SPT.

| | |
|---|---|
| `enable` | Switch to the Privileged EXEC mode. |
| `configure` | Switch to the configuration mode. |
| `ip pimsm spt-threshold 1000` | Activate the limit of 1000 Kbit/s for the switch to the SPT. |
| `no ip pimsm spt-threshold` | Deactivate the limit for the switch to the SPT. |

### Configuration as Designated Router for PIM-SM

When using PIM-SM, you have the option of defining a router as the designated router candidate. To do this, you specify the priority with which the router offers itself as the designated router.

| | |
|---|---|
| `enable` | Switch to the Privileged EXEC mode. |
| `configure` | Switch to the configuration mode. |
| `ip pimsm dr-priority 2/1 priority 2000` | Activate the router as the potential designated router with the priority 2000. |
| `no ip pimsm dr-priority 2/1` | Deactivate the router as a potential designated router. |

### Configuration as Bootstrap Router for PIM-SM

When using PIM-SM, you have the option of defining a router as the bootstrap router candidate. To do this, you specify the priority with which the router offers itself as the bootstrap router.

| | |
|---|---|
| `enable` | Switch to the Privileged EXEC mode. |
| `configure` | Switch to the configuration mode. |

| | |
|---|---|
| `ip pimsm bsr-candidate 2/1 priority 20` | Activate the router as the potential bootstrap router with the priority 20. |
| `no ip pimsm bsr-candidate 2/1` | Deactivate the router as a potential bootstrap router. |

### Limiting the PIM-SM domain

When you define an interface of the device as a BSR border, the router does not forward any BSR messages via this interface. In this way, the router limits the PIM-SM domain.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `interface 2/1` | Switch to the interface configuration mode of interface 2.1. |
| `ip pimsm bsr-border` | Deactivate the forwarding of BSR messages via interface 2.1. |
| `no ip pimsm bsr-border` | Allow the forwarding of BSR messages via interface 2.1. |

### Reducing the switching times

With both DVMRP and PIM-DM you can reduce the switching times by reducing the IGMP querier interval on the router interface. This reduction becomes effective when an inactive router to which Multicast recipients are connected becomes active again.

| | |
|---|---|
| `enable` | Switch to the privileged EXEC mode. |
| `configure` | Switch to the Configuration mode. |
| `interface 2/1` | Switch to the Interface Configuration mode of interface 2.1. |
| `ip igmp query-max-response-time 10` | Set the Query Max Response Time smaller than the Query Interval<br>In this example: 1 second<br>Default setting: 10 seconds |
| `ip igmp query-interval 5` | Set Query Interval<br>In this example: 5 seconds<br>Default setting: 125 seconds. |

With PIM-DM, if you reduce the Hello Time, a router can detect more quickly when a downstream router becomes inactive or active again.

```
ip pimdm query-interval 1
```

Set the PIM-DM Query Interval (Hello Time)
In this example: 1 second
Default setting: 30 seconds

With PIM-DM, using a default route that has been entered can reduce the switching time. While the router is gathering information about the path to the source (RPF), the router can use a default route that has been entered.

```
ip route 10.0.3.0
  255.255.255.0 10.0.2.2
```

Create the static default route.

```
exit
```

Switch to the Configuration mode.

### Special feature of VLAN routing

The router floods a Multicast data stream to all ports of a VLAN routing interface if

- the Multicast data stream comes from another subnetwork and
- at least one recipient on this VLAN interface has registered via IGMP for this Multicast data stream.

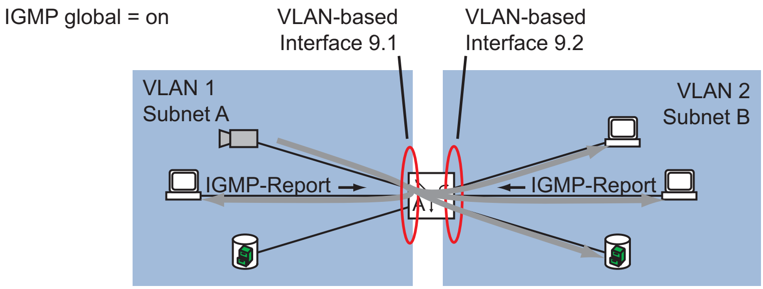


*Figure 51: Registered Multicast data stream on the VLAN routing interface*

# A Appendix

# A.1 Abbreviations used

| | |
|---|---|
| ABR | Area Border Router |
| ACA | AutoConfiguration Adapter |
| AS | Autonomous System |
| ASBR | Autonomous System Border Router |
| BC | Broadcast |
| BDR | Backup designated Router |
| BGP | Border Gateway Protocol |
| BOOTP | Bootstrap Protocol |
| CIDR | Classless Inter Domain Routing |
| CLI | Command Line Interface |
| DHCP | Dynamic Host Configuration Protocol) |
| DR | Designated Router |
| DVMRP | Distance Vector Multicast Routing Protocol |
| EUI | Extended Unique Identifier |
| FDB | Forwarding Database |
| GARP | General Attribute Registration Protocol |
| GMRP | GARP Multicast Registration Protocol |
| http | Hypertext Transfer Protocol |
| HiVRRP | Hirschmann Virtual Router Redundancy Protocol |
| IANA | Internet Assigned Numbers Authority |
| ICMP | Internet Control Message Protocol |
| IGMP | Internet Group Management Protocol |
| IGP | Interior Gateway Protocol |
| IP | Internet Protocoll |
| LED | Light Emitting Diode |
| LLDP | Link Layer Discovery Protocol |
| LSA | Link Status Advertisement |
| LSD | Link State Database |
| F/O | Optical Fiber |
| MAC | Media Access Control |
| MC | Multicast |
| MICE | Modular Industrial Communication Equipment |
| NSSA | Not So Stubby Area |
| NTP | Network Time Protocol |
| OSPF | Open Shortest Path First |
| OUI | Organizationally Unique Identifier |
| PC | Personal Computer |
| PIM-DM | Protocol Independent Multicast-Dense Mode |

| | |
|---|---|
| PIM-SM | Protocol Independent Multicast-Sparse Mode |
| PTP | Precision Time Protocol |
| RFC | Request For Comment |
| RM | Redundancy Manager |
| RS | Rail Switch |
| RSTP | Rapid Spanning Tree Protocol |
| RIP | Routing Information Protocol |
| RPF | Reverse Path Forwarding |
| SFP | Small Form-factor Pluggable |
| SNMP | Simple Network Management Protocol |
| SNTP | Simple Network Time Protocol |
| SPT | Shortest Path Tree |
| TCP | Transfer Control Protocol |
| tftp | Trivial File Transfer Protocol |
| TP | Twisted Pair |
| TTL | Time-to-live |
| UDP | User Datagramm Protocol |
| URL | Uniform Resourve Locator |
| UTC | Coordinated Universal Time |
| VL | Virtual Link |
| VLAN | Virtual Local Area Network |
| VLSM | Variable Length Subnet Mask |
| VRID | Virtual Router Identification |
| VRRP | Virtual Router Redundancy Protocol |

# A.2 Underlying IEEE Standards

- IEEE 802.1AB
  Topology Discovery (LLDP)
- IEEE 802.1D
  Switching, GARP, GMRP, Spanning Tree (Supported via 802.1S implementation)
- IEEE 802.1D-1998
  Media Access Control (MAC) Bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
- IEEE 802.1Q-1998
  Virtual Bridged Local Area Networks (VLAN Tagging, Port Based VLANs, GVRP)
- IEEE 802.1S
  Multiple Spanning Tree
- IEEE 802.1v
  Protocol Based VLANs
- IEEE 802.1 w.2001
  Rapid Reconfiguration, Supported via 802.1S implementation
- IEEE 802.1 X
  Port Authentication
- IEEE 802.3 - 2002
  Ethernet
- IEEE 802.3 ac
  VLAN Tagging
- IEEE 802.3 ad
  Link Aggregation with Static LAG and LACP support
- IEEE 802.3 x
  Flow Control

# A.3 List of RFCs

- RFC 768 (UDP)
- RFC 783 (TFTP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 855 (Telnet Option)
- RFC 951 (BOOTP)
- RFC 1112 (Host Extensions for IP Multicasting)
- RFC 1155 (SMIv1)
- RFC 1157 (SNMPv1)
- RFC 1212 (Concise MIB Definitions)
- RFC 1213 (MIB2)
- RFC 1493 (Dot1d)
- RFC 1542 (BOOTP-Extensions)
- RFC 1643 (Ethernet-like -MIB)
- RFC 1757 (RMON)
- RFC 1867 (HTML/2.0 Forms w/ file upload extensions)
- RFC 1901 (Community based SNMP v2)
- RFC 1905 (Protocol Operations for SNMP v2)
- RFC 1906 (Transport Mappings for SNMP v2)
- RFC 1907 (Management Information Base for SNMP v2)
- RFC 1908 (Coexistence between SNMP v1 and SNMP v2)
- RFC 1945 (HTTP/1.0)
- RFC 2068 (HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03)
- RFC 2131 (DHCP)
- RFC 2132 (DHCP-Options)
- RFC 2233 The Interfaces Group MIB using SMI v2
- RFC 2236 (IGMPv2)
- RFC 2246 (The TLS Protocol, Version 1.0)
- RFC 2271 (SNMP Framework MIB)
- RFC 2346 (AES Ciphersuites for Transport Layer Security)
- RFC 2362 (PIM-SM)
- RFC 2365 (Administratively Scoped Boundaries)
- RFC 2570 (Introduction to SNMP v3)
- RFC 2571 (Architecture for Describing SNMP Management Frameworks)

- RFC 2572 (Message Processing and Dispatching for SNMP)
- RFC 2573 (SNMP v3 Applications)
- RFC 2574 (User Based Security Model for SNMP v3)
- RFC 2575 (View Based Access Control Model for SNMP)
- RFC 2576 (Coexistence between SNMP v1,v2 & v3)
- RFC 2578 (SMI v2)
- RFC 2579 (Textual Conventions for SMI v2)
- RFC 2580 (Conformance statements for SMI v2)
- RFC 2613 (SMON)
- RFC 2618 (RADIUS Authentication Client MIB)
- RFC 2620 (RADIUS Accounting MIB)
- RFC 2674 (Dot1p/Q)
- RFC 2818 (HTTP over TLS)
- RFC 2851 (Internet Addresses MIB)
- RFC 2865 (RADIUS Client)
- RFC 2866 (RADIUS Accounting)
- RFC 2868 (RADIUS Attributes for Tunnel Protocol Support)
- RFC 2869 (RADIUS Extensions)
- RFC 2869bis (RADIUS support for EAP)
- RFC 2933 (IGMP MIB)
- RFC 3164 (The BSD Syslig Protocol)
- RFC 3376 (IGMPv3)
- RFC 3580 (802.1X RADIUS Usage Guidelines)
- RFC 4330 (SNTP, obsoletes RFCs 1769 and 2330)

- **Routing**
  - RFC 826 Ethernet ARP
  - RFC 894 Transmission of IP Datagrams over Ethernet Networks
  - RFC 896 Congestion Control in IP/TCP Networks
  - RFC 919 IP Broadcast
  - RFC 922 IP Broadcast in the presence of subnets
  - RFC 950 IP Subnetting
  - RFC 1027 Using ARP to implement Transparent Subnet Gateways (Proxy ARP)
  - RFC 1256 ICMP Router Discovery Messages
  - RFC 1321 Message Digest Algorithm
  - RFC 1519 CIDR
  - RFC 1724 RIP v2 MIB Extension
  - RFC 1765 OSPF Database Overflow
  - RFC 1812 Requirements for IP Version 4 Routers

- RFC 1850 OSPF MIB Draft-ietf-ipv6-rfc2096-update-07.txt IP Forwarding Table MIB
- RFC 2082 RIP-2 MD5 Authentication
- RFC 2131 DHCP Relay
- RFC 2328 OSPF Version 2
- RFC 2453 RIP v2
- RFC 2787 VRRP MIB
- RFC 2863 The Interfaces Group MIB
- RFC 2932 IPv4 Multicast Routing MIB
- RFC 2934 PIM MIB for IPv4
- RFC 3046 DHCP/BootP Relay
- RFC 3101 The OSPF "Not So Stubby Area" (NSSA) Option
- RFC 3376 IGMPV3
- RFC 3768 VRRP, Virtual Router Redundancy Protocol
- Draft-holbrook-idmr-igmpv3-ssm-08.txt – IGMPv3 / MLDv2 for SSM
- Draft-ietf-idmr-dvmrp-mib-11.txt – DVMRP MIB
- Draft-ietf-idmr-dvmrp-v3-10 – DVMRP
- Draft-ietf-magma-igmpv3-and-routing-05.txt – IGMPv3 an Multicast Routing Protocol Interaction
- Draft-ietf-magma-mgmd-mib-03.txt – Multicast Group Membership Discovery MIB
- Draft-ietf-pim-v2-dm-03 – PIM-DM
- Draft-ietf-smm-arch-06.txt – Source -Specific Multicast for IP

# A.4 Entering the IP Parameters

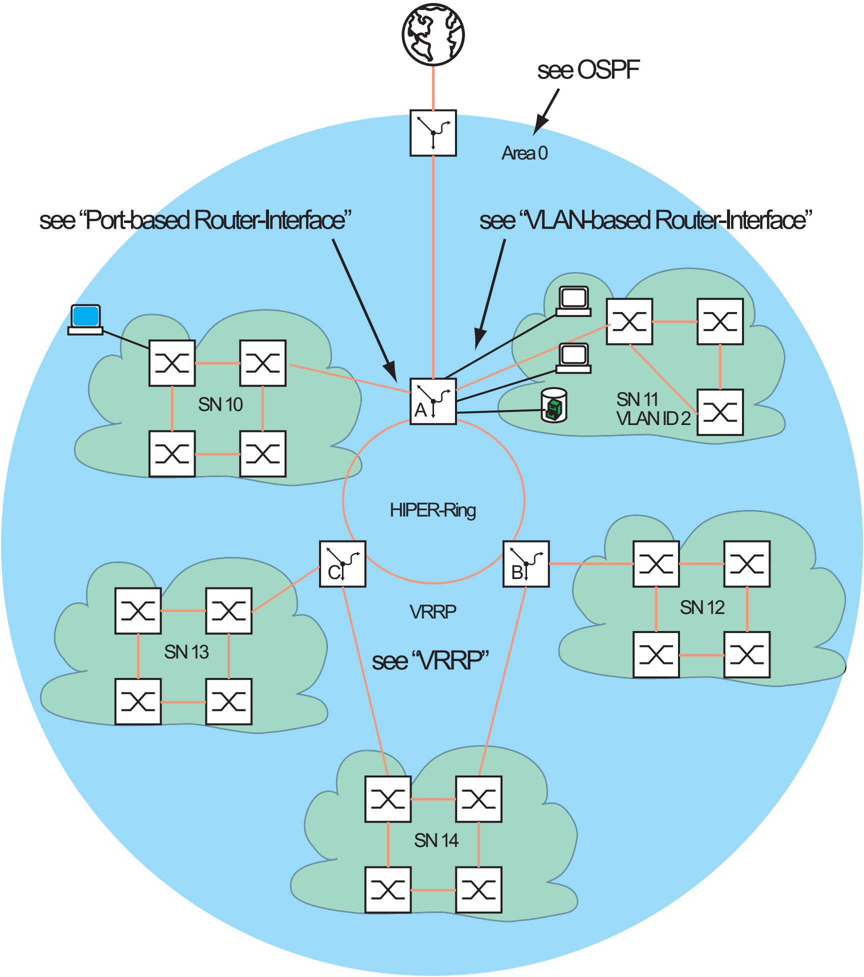


*Figure 52: Network plan*

To configure the layer 3 function, you require access to the management of the Switch, as described in the “Basic Configuration” user manual. Depending on your own application, you will find many options for assigning IP addresses to the devices. The following example describes one option that often arises in practice. Even if you have other prerequisites, this example shows the general method for entering the IP parameters and points out important things that you should note.

The prerequisites for the following example are:

- All layer 2 and layer 3 switches have the IP address 0.0.0.0 (= state on delivery)
- The IP addresses of the switches and router interfaces and the gateway IP addresses are defined in the network plan.
- The devices and their connections are installed.
- Redundant connections are open (see VRRP and HIPER-Ring). To avoid loops in the configuration phase, close the redundant connections only after the configuration phase.

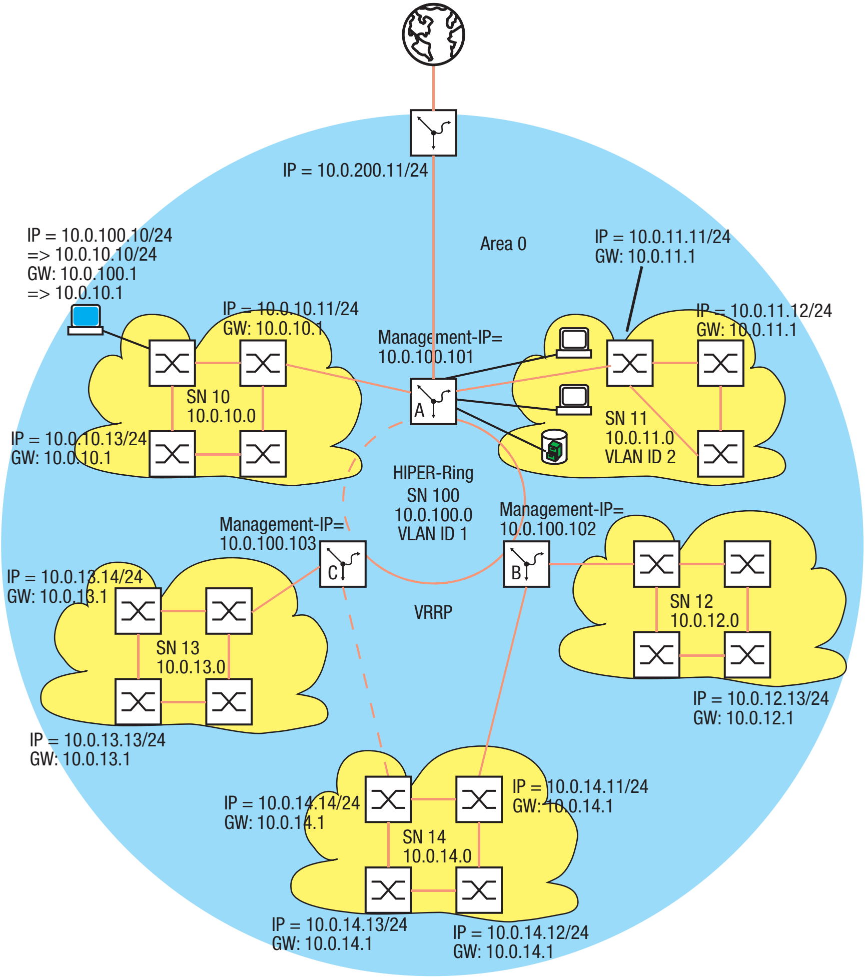


*Figure 53: Network plan with management IP addresses*

□ Assign the IP parameters to your configuration computer. During the configuration phase, the configuration computer is located in subnet 100. This is necessary, so that the configuration computer has access to the layer 3 switches throughout the entire configuration phase.

□ Start HiDiscovery on your configuration computer.

□ Give all the layer 2 and layer 3 switches their IP parameters in accordance with the network plan.
You can access the devices in subnets 10 to 14 again when you have completed the following router configuration.

□ Configure the router function for the layer 3 switches.
Note the sequence:
1. Layer 3 switch C
2. Layer 3 switch B
The sequence is important; you thus retain access to the devices.
As soon as you assign an IP address from the subnet of the management IP address (= SN 100) to a router interface, the Switch deletes the management IP address. You access the Switch via the IP address of the router interface.

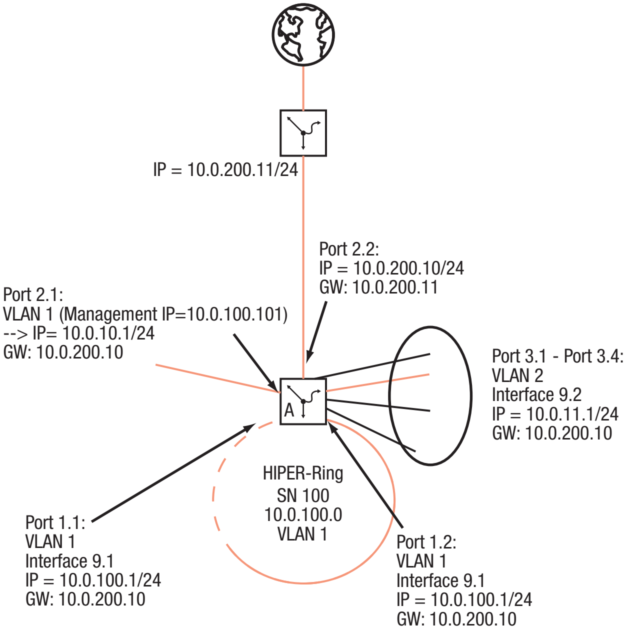


*Figure 54: IP parameters for layer 3 switch A*

□ Configure the router function for layer 3 switch A.
You first configure the router interface at a port to which the configuration computer is connected. The result of this is that in future you will access the layer 3 switch via subnet 10.

□ Change the IP parameters of your configuration computer to the values for subnet 10. You thus access layer 3 switch A again, namely via the IP address of the router interface set up beforehand.

□ Finish the router configuration for layer 3 switch A (see figure 54).

After the configuration of the router function on all layer 3 switches, you have access to all the devices.

# A.5 Copyright of Integrated Software

## A.5.1 Bouncy Castle Crypto APIs (Java)

The Legion Of The Bouncy Castle
Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle
(http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## A.5.2 Broadcom Corporation

(c) Copyright 1999-2007 Broadcom Corporation. All Rights Reserved.

# B Readers’ Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

| | Very Good | Good | Satisfactory | Mediocre | Poor |
|---|---|---|---|---|---|
| Precise description | O | O | O | O | O |
| Readability | O | O | O | O | O |
| Understandability | O | O | O | O | O |
| Examples | O | O | O | O | O |
| Structure | O | O | O | O | O |
| Comprehensive | O | O | O | O | O |
| Graphics | O | O | O | O | O |
| Drawings | O | O | O | O | O |
| Tables | O | O | O | O | O |

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- per mail to

  Hirschmann Automation and Control GmbH
  Department 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

# C Index

# D Further Support

## Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at http://www.hirschmann.com

Contact our support at https://hirschmann-support.belden.eu.com

You can contact us

in the EMEA region at
- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at
- Tel.: +1 (717) 217-2270
- E-mail: inet-support.us@belden.com

in the Asia-Pacific region at
- Tel.: +65 6854 9860
- E-mail: inet-ap@belden.com

## Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  The current technology and product training courses can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND