

Manual Workshops (Excerpt)

IP Workshops

Copyright© Version 7.0, 2011 Funkwerk Enterprise Communications GmbH

Legal Notice

Aim and purpose

This document is part of the user manual for the installation and configuration of funkwerk devices. For the latest information and notes on the current software release, please also read our release notes, particularly if you are updating your software to a higher release version. You will find the latest release notes under www.funkwerk-ec.com .

Liability

This manual has been put together with the greatest possible care. However, the information contained in this manual is not a guarantee of the properties of your product. Funkwerk Enterprise Communications GmbH is only liable within the terms of its conditions of sale and supply and accepts no liability for technical inaccuracies and/or omissions.

The information in this manual can be changed without notice. You will find additional information and also release notes for funkwerk devices under www.funkwerk-ec.com .

Funkwerk devices make WAN connections as a possible function of the system configuration. You must monitor the product in order to avoid unwanted charges. Funkwerk Enterprise Communications GmbH accepts no responsibility for data loss, unwanted connection costs and damage caused by unintended operation of the product.

Trademarks

funkwerk trademarks and the funkwerk logo, bintec trademarks and the bintec logo, artem trademarks and the artem logo, elmeg trademarks and the elmeg logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Company and product names mentioned are usually trademarks of the companies or manufacturers concerned.

Copyright

All rights reserved. No part of this manual may be reproduced or further processed in any way without the written consent of Funkwerk Enterprise Communications GmbH. The documentation may not be processed and, in particular, translated without the consent of Funkwerk Enterprise Communications GmbH.

You will find information on guidelines and standards in the declarations of conformity under www.funkwerk-ec.com .

How to reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH, Südwestpark 94, D-90449 Nuremberg, Germany,
Phone: +49 911 9673 0, Fax: +49 911 688 07 25

Funkwerk Enterprise Communications France S.A.S., 6/8 Avenue de la Grande Lande, F-33174
Gradignan, France, Phone: +33 5 57 35 63 00, Fax: +33 5 56 89 14 05

Internet: www.funkwerk-ec.com

Table of Contents

Chapter 1	IP - Network Address Translation (NAT)	1
1.1	Introduction	1
1.2	Configuration.	2
1.2.1	Enable NAT	2
1.2.2	Configuring NAT enables	3
1.3	Result.	7
1.4	Checking the connection.	7
1.5	Overview of configuration steps.	7
Chapter 2	IP - Configuration of the bintec router behind a provider router	10
2.1	Introduction	10
2.2	Configuration of the port	11
2.3	Configuring Internet access	13
2.4	Configuration of DMZ	14
2.4.1	Enabling NAT on the DMZ interface	14
2.4.2	Configuring portforwarding	15
2.5	Checking the configuration.	17
2.5.1	Checking portforwarding.	17
2.5.2	Checking the functionality	18
2.6	Overview of configuration steps.	19
Chapter 3	IP - Load balancing.	21
3.1	Introduction	21
3.2	Configuring internet access	21

3.2.1	Checking the metric	24
3.3	Configuration of load balancing groups	25
3.4	Result	26
3.5	Checking the configuration	26
3.6	Overview of configuration steps.	27
Chapter 4	IP - Internet access with T 4x4 and external DSL modem .	29
4.1	Introduction	29
4.2	Configuration.	29
4.2.1	Configure Internet access (DSL)	31
4.2.2	Control Internet access	33
4.3	Overview of configuration steps.	37
Chapter 5	IP - Internet access with T4x4 and another router in LAN .	38
5.1	Introduction	38
5.2	Configuration.	39
5.2.1	Configuration steps for the elmeg T4x4 system	40
5.3	Overview of configuration steps.	42
Chapter 6	IP - IPTV on xDSL (ADSL/VDSL) T-Home Entertainment con- nection	44
6.1	Introduction	44
6.2	Configuration.	46
6.2.1	Configuring the bintec RS120	46
6.2.2	Configuring the IPTV Multicast data access	48
6.2.3	Configuring a DHCP-IP address pool on the LAN interface	52
6.2.4	Bootable backup of the configuration	53

6.3 Overview of configuration steps 54

Chapter 1 IP - Network Address Translation (NAT)

1.1 Introduction

The configuration of Network Address Translation (NAT) is described in the chapters below.

Network Address Translation (NAT) is a function on your device for defined conversion of source and destination addresses of IP packets. If NAT is activated, IP connections are still only allowed by default in one direction, outgoing (forward) (= protective function). Exceptions can be configured in the **Portforwarding** menu.

You have a permanent 2-Mbps connection to the Internet with 8 IP addresses. Your Ethernet interface **ETH** is connected to the access router. This has the IP address `62.10.10.1/29`, whereas the remaining IPs from `62.10.10.2` to `62.10.10.6` are entered on Ethernet interface **ETH**.

You configure NAT enables for accessing your gateway over HTTP. You also want to access your terminal server and the corporate web server over the Internet.

Configuration in this scenario is carried out using the **Funkwerk Configuration Interface**.

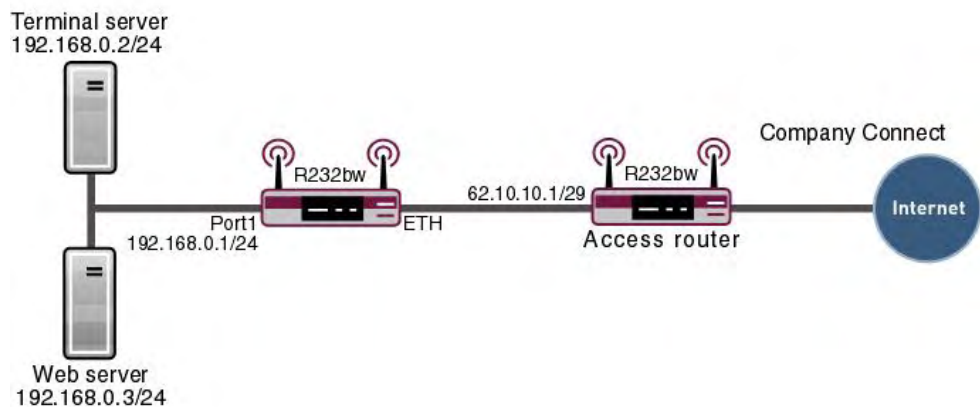


Fig. 2: Example scenario NAT

Requirements

The following are required for the configuration:

- Basic configuration of the gateway
- Boot image from version 7.8.2
- A working Internet access. For example, **Company Connect** with 8 IP addresses.

1.2 Configuration

1.2.1 Enable NAT

A list of all NAT interfaces is displayed in the NAT interface menu.

Go to the following menu to enable NAT for your interface:

- (1) Go to **Routing -> NAT -> NAT Interfaces**.

The screenshot shows the web interface for a bintec R232bw device. The top navigation bar includes 'Language English', 'Online Help', 'Express Setup Wizard', 'Logout', and the 'funkwerk' logo. The left sidebar contains a menu with categories like System Management, Physical Interfaces, LAN, Wireless LAN, Routing, WAN, VPN, Firewall, VoIP, Local Services, Maintenance, External Reporting, and Monitoring. The 'Routing' menu is expanded, showing 'Routes', 'NAT', 'RIP', 'Load Balancing', and 'Multicast'. The 'NAT' menu is further expanded to show 'NAT Interfaces' and 'Portforwarding'. The 'NAT Interfaces' page displays a table with the following data:

Interface	NAT active	Silent Deny	PPTP Passthrough	Portforwards
LAN_EN1-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN5-0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3
LAN_EN5-0-SNAP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_ETH0A50-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

At the bottom of the table, there are 'OK' and 'Cancel' buttons. The page footer indicates 'Page: 1, Items: 1 - 5'.

Fig. 3: Routing -> NAT -> NAT Interfaces

Relevant fields in the NAT Interfaces menu

Field	Meaning
NAT active	Here you can enable the NAT feature for the interface.
Silent Deny	If this function is enabled, no ICMP packets are answered.

Proceed as follows:

- (1) Select **NAT Active** for the `LAN_EN5-0` interface.

- (2) Select **Silent Deny** for the `LAN_EN5-0` interface.
- (3) Confirm with **OK**.

1.2.2 Configuring NAT enables

NAT enable for the Funkwerk Configuration Interface

It should be possible to administrate your gateway using HTTP over the Internet with the permanent IP address `62.10.10.2`. For security reasons use external port `8080`, for example, instead of port `80`.

Go to the following menu to configure NAT entries.

- (1) Go to **Routing -> NAT-> Portforwarding-> New**.

Fig. 4: Routing -> NAT ->Portforwarding -> New

Relevant fields in the Portforwarding menu

Field	Meaning
Interface	Select the interface for your NAT enable.
Service	Select a predefined service for which address mapping is defined on incoming connections.
Protocol	Only if for Services = <i>user-defined</i> is selected. Select the protocol for the entry.

Field	Meaning
External IP Address	Enter the external IP address of the gateway.
Port	Only if for Services = <i>user-defined</i> is selected. First select whether all connections are to be permitted, or whether a certain port or port range is to be defined. Now, enter the port which is reached externally on the gateway.
Map to host	Specify who is receiving the packets in the internal network. With the option <i>Local</i> your device is mapped itself.
Destination Port	Disable the option <i>Original</i> and enter a port number.

Proceed as follows:

- (1) Set the **interface** to *LAN_EN5-0*.
- (2) Leave the **Service** set to *User Defined*.
- (3) Set **Protocol** to *TCP*.
- (4) Under **External IP Address** enter the IP address, e. g. *62.10.10.2*.
- (5) Set the **Port** to *Specify Port* and enter *8080*, for example, in the first input field.
- (6) Set the **Map to host** field to *Local*.
- (7) Under **Destination Port** disable **Original** and enter *80* in the input field.
- (8) Confirm with **OK**.

NAT enable for Web Server

The internal Web server should be reached under the IP address *62.10.10.3*. External default port *80* is used as the Web server serves as a Web host for public websites.

- (1) Go to **Routing** -> **NAT**-> **Portforwarding**-> **New**.

The screenshot shows the 'bintec R232bw' web interface. The top navigation bar includes 'Language English', 'Online Help', 'Express Setup Wizard', 'Logout', and the 'funkwerk' logo. A left-hand navigation menu lists various system management options, with 'Routing' expanded to show 'NAT'. The main content area is titled 'NAT Interfaces' and 'Portforwarding'. The configuration form includes the following fields:

- Interface:** LAN_EN5-0
- Select traffic:**
 - Service:** HTTP
 - Protocol:** Any
- Corresponding NAT entry for outgoing connection:** Enabled
- External IP Address:** Auto 62.10.10.3 | 255.255.255.255
- Port:** -All- | -1 to -1
- Remote Network:** Enabled
- Forward to:**
 - Map to host:** IP Address | 192.168.0.3 | 255.255.255.255
 - Destination Port:** Original | -1

Buttons for 'OK' and 'Cancel' are located at the bottom of the form.

Fig. 5: Routing -> NAT ->Portforwarding -> New

Relevant fields in the Portforwarding menu

Field	Meaning
Interface	Select the interface for your NAT enable.
Service	Select a predefined service for which address mapping is defined on incoming connections.
External IP Address	Enter the external IP address of the gateway.
Map to host	Enter the IP address of the internal host or network.

Proceed as follows to configure the enable:

- (1) Set the **interface** to *LAN_EN5-0*.
- (2) Configure the **Service** to *HTTP*.
- (3) Under **External IP Address** enter the IP address, e. g. *62.10.10.3*.
- (4) In the **Map to host** field select *IP Address* and enter the internal IP address *192.168.0.3*.
- (5) Confirm with **OK**.

NAT Enable for Terminal Server

The internal terminal server should be reached under the IP address *62.10.10.4*. When port *3389* is open attackers can easily identify that you are using a terminal server. As a result, use a different port for external access using a remote desktop, for example port

5000.

- (1) Go to **Routing -> NAT -> Portforwarding -> New**.

The screenshot shows the 'bintec R232bw' web interface. The top navigation bar includes 'Language English', 'Online Help', 'Express Setup Wizard', 'Logout', and the 'funkwerk' logo. The left sidebar contains a menu with categories like 'System Management', 'Physical Interfaces', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Local Services', 'Maintenance', 'External Reporting', and 'Monitoring'. The 'Routing' category is expanded, showing 'Routes', 'NAT', 'RIP', 'Load Balancing', and 'Multicast'. The 'NAT' category is further expanded to show 'Portforwarding'. The main content area displays the 'NAT Interfaces Portforwarding' configuration page. The form includes the following fields:

- Interface:** LAN_EN5-0
- Select traffic:** User-defined
- Service:** User-defined
- Protocol:** TCP
- Corresponding NAT entry for outgoing connection:** Enabled
- External IP Address:** Auto 62.10.10.4 | 255.255.255.255
- Port:** Specify port 5000 | to=1
- Remote Network:** Enabled
- Forward to:** IP Address 192.168.0.2 | 255.255.255.255
- Destination Port:** Original 3389

At the bottom of the form are 'OK' and 'Cancel' buttons.

Fig. 6: Routing -> NAT ->Portforwarding -> New

Relevant fields in the Portforwarding menu

Field	Meaning
Interface	Select the interface for your NAT enable.
Service	Select a predefined service for which address mapping is defined on incoming connections.
Protocol	Only if for Services = <i>user-defined</i> is selected. Select the protocol for the entry.
External IP Address	Enter the external IP address of the gateway.
Port	Only if for Services = <i>user-defined</i> is selected. First select whether all connections are to be permitted, or whether a certain port or port range is to be defined. Now, enter the port which is reached externally on the gateway.
Map to host	Enter the IP address of the internal host or network.
Destination Port	Disable the option <i>Original</i> and enter a port number.

Proceed as follows to configure the enable:

- (1) Set the **interface** to *LAN_EN5-0*.

- (2) Leave the **Service** set to *User Defined*.
- (3) Set **Protocol** to *TCP*.
- (4) Under **External IP Address** enter the IP address, e. g. *62.10.10.4*.
- (5) Set the **Port** to *Specify Port* and enter *5000*, for example, in the first input field.
- (6) In the **Map to host** field select *IP Address* and enter the internal IP address *192.168.0.2*.
- (7) Under **Destination Port** disable **Original** and enter *3389* in the input field.
- (8) Confirm with **OK**.

1.3 Result

You have configured a NAT enable so that you can access the gateway with HTTP over the Internet. You also allow access to your internal Web server and the terminal server over the Internet.

1.4 Checking the connection

To check the settings, activate debug mode in the shell with the command `debug all&`. Call up the browser on an external computer on the Internet and enter the IP address of the gateway, e.g. `http://62.10.10.2:8080`.

The following message must appear if you are from the IP address *80.65.48.135*:

```
12:14:20 DEBUG/INET: NAT: new incoming session on ifc 5000
prot 6 127.0.0.1:80/ 62.10.10.2:8080 &lt;- 80.65.48.135:1024
```

1.5 Overview of configuration steps

Enable NAT

Field	Menu	Value
NAT active	Routing -> NAT ->NAT Interfaces	Enabled for LAN_EN5-0
Silent Deny	Routing -> NAT ->NAT Interfaces	Enabled for LAN_EN5-0

Funkwerk Configuration Interface

Field	Menu	Value
Interface	Routing -> NAT ->Portforwarding -> New	<i>LAN_EN5-0</i>
Service	Routing -> NAT ->Portforwarding -> New	<i>User-defined</i>

Field	Menu	Value
Protocol	Routing -> NAT ->Portforwarding -> New	<i>TCP</i>
External IP Address	Routing -> NAT ->Portforwarding -> New	e.g. <i>62.10.10.2</i>
Port	Routing -> NAT ->Portforwarding -> New	<i>Specify Port</i> with <i>8080</i>
Map to host	Routing -> NAT ->Portforwarding -> New	<i>Local</i>
Destination Port	Routing -> NAT ->Portforwarding -> New	<i>80</i>

Web server

Field	Menu	Value
Interface	Routing -> NAT ->Portforwarding -> New	<i>LAN_EN5-0</i>
Service	Routing -> NAT ->Portforwarding -> New	<i>HTTP</i>
External IP Address	Routing -> NAT ->Portforwarding -> New	e.g. <i>62.10.10.3</i>
Map to host	Routing -> NAT ->Portforwarding -> New	<i>IP Address</i> with <i>192.168.0.3</i>

Terminal Server

Field	Menu	Value
Interface	Routing -> NAT ->Portforwarding -> New	<i>LAN_EN5-0</i>
Service	Routing -> NAT ->Portforwarding -> New	<i>User-defined</i>
Protocol	Routing -> NAT ->Portforwarding -> New	<i>TCP</i>
External IP Address	Routing -> NAT ->Portforwarding -> New	e.g. <i>62.10.10.4</i>
Port	Routing -> NAT ->Portforwarding -> New	<i>Specify Port e.g.</i> <i>5000</i>
Map to host	Routing -> NAT ->Portforwarding -> New	<i>IP Address with</i> <i>192.168.0.2</i>

Field	Menu	Value
Destination Port	Routing -> NAT ->Portforwarding -> New	<i>3389</i>

Chapter 2 IP - Configuration of the bintec router behind a provider router

2.1 Introduction

The configuration of a DMZ (Demilitarized Zone) with a **bintec R232bw** is described in the following chapters.

Configuration is performed with the **Funkwerk Configuration Interface**.

All FTP and HTTP/HTTPS requests from the Internet are to be forwarded to an FTP or Web server in the DMZ. The gateway has a leased Internet line with static public IP address, which is connected over the **ETH** port.

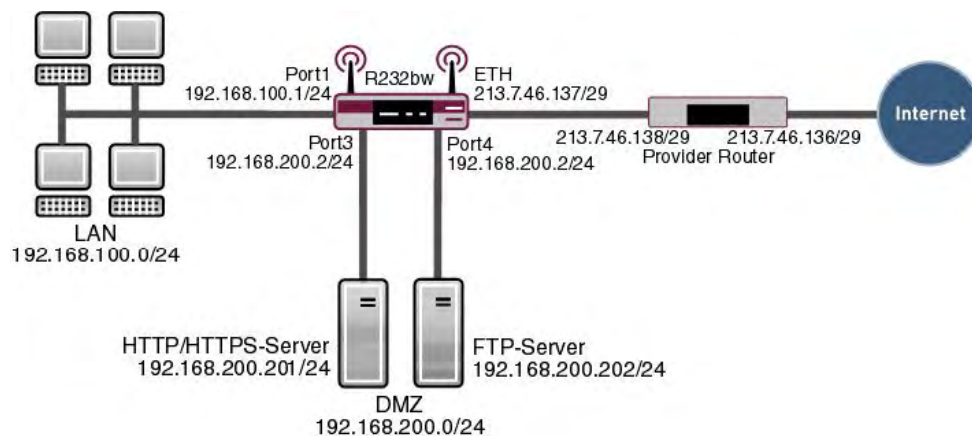


Fig. 7: Example scenario DMZ

Requirements

The following are required for the configuration:

- A **bintec R232bw** gateway
- Boot image from version 7.8.2
- Internet access with static public IP address
- An FTP and web server in the DMZ

- Your LAN is connected to port **1** or **2** (interface `en1-0`) for the gateway.
- Your DMZ is connected to port **3** or **4** (interface `en1-1`) for the gateway.
- The leased Internet line is connected to port **ETH** (`en5-0`).

2.2 Configuration of the port

The DMZ is set up by dividing the four switch ports of the **bintec R232bw** into two interfaces.

- Port **1** and **2** are assigned to the interface `en1-0`.
- Port **3** and **4** are assigned to the interface `en1-1`.

Go to the following menu to assign the ports to the interfaces:

- (1) Go to **Physical Interfaces -> Ethernet Ports-> Port Configuration**.

Fig. 8: Physical Interfaces -> Ethernet Ports-> Port Configuration

Relevant fields in Port Configuration menu

Field	Meaning
Ethernet Interface Selection	Assigns ports to specific interfaces.

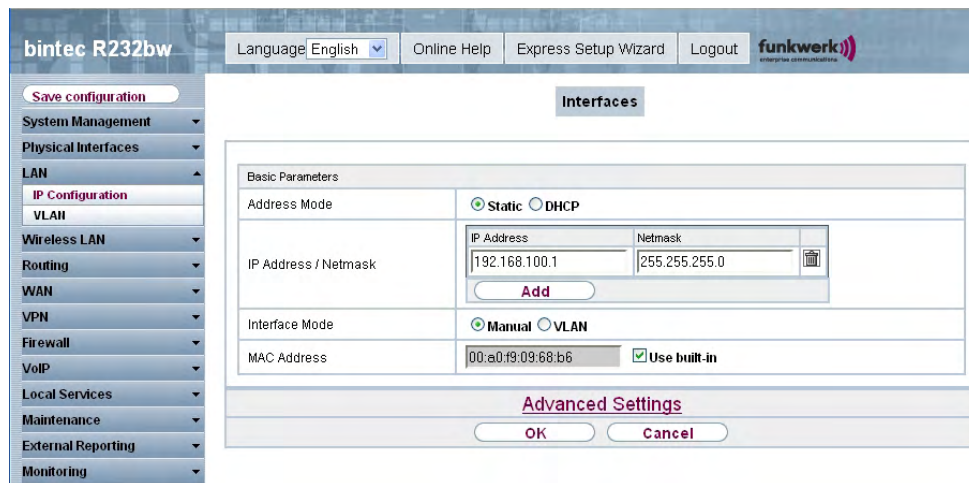
Proceed as follows to assign the ports to interfaces:

- (1) Under **Ethernet Interface Selection** select `en1-0` for the **Switch Ports 1** and **2** from the dropdown menu.
- (2) Select `en1-1` for the **Switch Ports 3** and **4**.

(3) Confirm with **OK**.

In the **IP Configuration** menu, you can assign IP addresses to the ports.

(1) Go to **LAN -> IP Configuration -> Interfaces -> <en1-0>** .



The screenshot shows the web interface for a bintec R232bw router. The left sidebar contains a navigation menu with options like System Management, Physical Interfaces, LAN, Wireless LAN, Routing, WAN, VPN, Firewall, VoIP, Local Services, Maintenance, External Reporting, and Monitoring. The 'LAN' menu is expanded, showing 'IP Configuration' as the selected option. The main content area displays the 'Interfaces' configuration page for interface 'en1-0'. The 'Basic Parameters' section includes:

- Address Mode: Static DHCP
- IP Address / Netmask: IP Address field contains '192.168.100.1' and Netmask field contains '255.255.255.0'. An 'Add' button is below these fields.
- Interface Mode: Manual VLAN
- MAC Address: '00:a0:f9:09:68:b6' with a checked 'Use built-in' option.

 At the bottom, there are 'Advanced Settings' and 'OK' / 'Cancel' buttons.

Fig. 9: **LAN -> IP Configuration -> Interfaces -> <en1-0>** .

Relevant fields in the Interfaces menu


Field	Meaning
Address mode	Select how an IP address is assigned to the interface.
IP Address/Netmask	IP address and subnet mask of the interface.
Interface Mode	Select <i>Manual</i> . The interface is not assigned for a specific purpose.

Proceed as follows:

- (1) Leave **Address Mode** set to *Static*.
- (2) In **IP Address / Net Mask** enter the IP address and the subnet mask, here *192.168.100.1* and *255.255.255.0*.
- (3) Leave **Interface Mode** set to *Manual*.
- (4) Confirm with **OK**.

Since your device can no longer be accessed by administration at the previous IP address, but only at the new IP address *192.168.100.1*, you must reconnect to the **Funkwerk Configuration Interface**. To do this, enter the new IP address *192.168.100.1* in the address bar of your browser and log in again.

Proceed as follows for interface *en1-1*:


- (1) For *en1-1* go to **LAN -> IP Configuration -> Interfaces -> <en1-1>**.
- (2) Click the  icon.
- (3) Leave **Address Mode** set to *Static*.
- (4) In **IP Address / Net Mask** enter the IP address and the subnet mask, here *192.168.200.2* and *255.255.255.0*.
- (5) Leave **Interface Mode** set to *Manual*.
- (6) Confirm with **OK**.

If no IP address is entered, click **Add** for the IP address / Netmask. An input field appears for the IP address where you can assign the IP address and subnet mask.

2.3 Configuring Internet access

The gateway has a leased Internet line via the provider's router. Consequently, you must define the static public IP address for the gateway and configure a default route over the provider's router.

Configure the static public IP address for the interface *en5-0* in the same way as configuring the ports in the previous section:

- (1) For *en5-0* go to **LAN -> IP Configuration -> Interfaces -> <en5-0>**.
- (2) Click the  icon.
- (3) Leave **Address Mode** set to *Static*.
- (4) In **IP Address / Net Mask** enter the IP address and the subnet mask, here *213.7.46.137* and *255.255.255.248*.
- (5) Leave **Interface Mode** set to *Manual*.
- (6) Confirm with **OK**.

Set up a default route over the provider's router.

- (1) Go to **Routing -> Routes -> IP Routes -> New** .

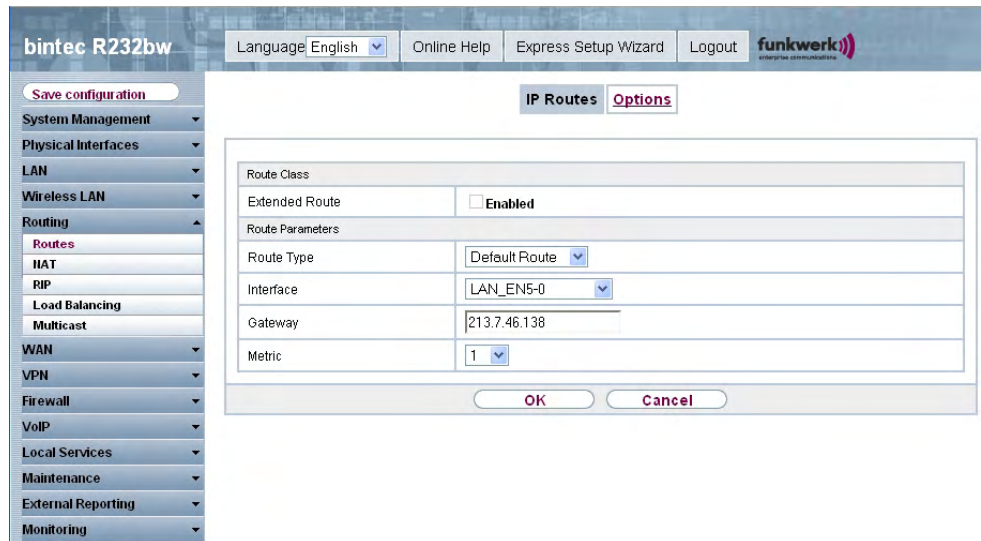


Fig. 10: Routing -> Routes-> IP Routes-> New

Relevant fields in the IP Routes menu

Field	Meaning
Route Type	Defines the type of route.
Interface	Interface over which the gateway can be accessed
Gateway	IP address of the Internet gateway.

Proceed as follows:

- (1) Leave **Extended Route** on *Disabled*.
- (2) For **Route Type** select *Standard Route*.
- (3) Set **Interface** to *LAN_EN5-0*.
- (4) Under **Gateway** enter the IP address of the Internet gateway, in this example *213.7.46.138*.
- (5) Leave **Metric** set to *1*.
- (6) Confirm with **OK**.

2.4 Configuration of DMZ

2.4.1 Enabling NAT on the DMZ interface

NAT must be enabled on the interface used to provide the Internet connection.

Go to the following menu to enable NAT for the DMZ interface:

- (1) Go to **Routing** -> **NAT**->**NAT Interfaces** .

The screenshot shows the 'bintec R232bw' web interface. The left sidebar contains a navigation menu with categories like System Management, Physical Interfaces, LAN, Wireless LAN, Routing, WAN, VPN, Firewall, VoIP, Local Services, Maintenance, External Reporting, and Monitoring. The 'Routing' menu is expanded, showing 'NAT' selected. The main content area is titled 'NAT Interfaces' and contains a table with the following data:

Interface	NAT active	Silent Deny	PPTP Passthrough	Portforwards
LAN_EN1-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN5-0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3
LAN_EN5-0-SNAP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_ETH0A50-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

At the bottom of the table, there are 'OK' and 'Cancel' buttons. The page also shows a 'View' dropdown set to 20, a 'Filter in' dropdown set to None, and a 'Go' button.

Fig. 11: Routing -> NAT ->NAT Interfaces

Relevant fields in the NAT Interfaces menu

Field	Meaning
NAT active	Enables NAT on the corresponding interface.
Silent Deny	If this function is enabled, no ICMP packets are answered.

Proceed as follows:

- (1) Under **LAN_EN5-0** select *NAT Active*.
- (2) Under **LAN_EN5-0** select *Silent Deny*.
- (3) Confirm with **OK**.

2.4.2 Configuring portforwarding

As NAT is enabled on the interface for the Internet connection, it is now no longer possible to access internal PCs from the Internet. External users must be authorised to access the FTP server over FTP and the Web server over HTTP or HTTPS. Consequently, you must set up portforwarding for these services.

Go to the following menu to forward the required ports to the FTP or Web server:

- (1) Go to **Routing** -> **NAT**-> **Portforwarding**-> **New**.

The screenshot shows the configuration page for NAT Portforwarding on a bintec R232bw router. The interface is in English and includes a 'Save configuration' button. The left sidebar lists various system management options. The main configuration area is titled 'NAT Interfaces Portforwarding' and contains the following fields:

- Interface:** LAN_EN5-0
- Select traffic:**
 - Service:** FTP
 - Protocol:** Any
- Corresponding NAT entry for outgoing connection:** Enabled
- External IP Address:** Auto 213.7.46.137 | 255.255.255.255
- Port:** -All- | -1 to -1
- Remote Network:** Enabled
- Forward to:**
 - Map to host:** IP Address | 192.168.200.202 | 255.255.255.255
 - Destination Port:** Original -1

Buttons for 'OK' and 'Cancel' are located at the bottom of the configuration area.

Fig. 12: Routing -> NAT ->Portforwarding -> New

Relevant fields in the Portforwarding menu

Field	Meaning
Interface	Interface accessed from the Internet.
Service	Service to be forwarded.
External IP Address	Public IP address of the gateway.
Map to host	IP address of the destination to which the services are passed.

Proceed as follows to set up portforwarding for FTP:

- (1) Set **Interface** to *LAN_EN5-0*.
- (2) Select the **Service** *FTP*.
- (3) Under **External IP Address**, enter the static public ISP address of the gateway, here *213.7.46.137*.
- (4) In the **Map to host** field select *IP Address* and enter the IP address of the FTP server, in this example *192.168.200.202*.
- (5) Confirm with **OK**.

Proceed as follows to set up portforwarding for HTTP:

- (1) Go to **Routing -> NAT-> Portforwarding-> New**.
- (2) Set **Interface** to *LAN_EN5-0*.

- (3) Select the **Service** *HTTP*.
- (4) Under **External IP Address**, enter the static public ISP address of the gateway, here *213.7.46.137*.
- (5) In the **Map to host** field select *IP Address* and enter the IP address of the HTTP server, in this example *192.168.200.201*.
- (6) Confirm with **OK**.

Proceed as follows to set up portforwarding for HTTPS:

- (1) Go to **Routing -> NAT-> Portforwarding-> New**.
- (2) Set **Interface** to *LAN_EN5-0*.
- (3) Select the **Service** *HTTPS*.
- (4) Under **External IP Address**, enter the static public ISP address of the gateway, here *213.7.46.137*.
- (5) In the **Map to host** field select *IP Address* and enter the IP address of the HTTPS server, in this example *192.168.200.201*.
- (6) Confirm with **OK**.

2.5 Checking the configuration

2.5.1 Checking portforwarding

The list of configured portforwarding should appear as follows:

- (1) Remain in the **Routing -> NAT-> Portforwarding** menu.

The screenshot shows the web interface for configuring NAT on a bintec R232bw router. The left sidebar contains a navigation menu with categories like System Management, Physical Interfaces, LAN, Wireless LAN, Routing, NAT, RIP, Load Balancing, Multicast, WAN, VPN, Firewall, VoIP, Local Services, Maintenance, External Reporting, and Monitoring. The main content area is titled 'NAT Interfaces' and 'Portforwarding'. It features a table with the following data:

Service / Protocol	External IP Address	Forward to	Remote IP Address	Netmask
FTP (TCP / 20)	213.7.46.137	192.168.200.202	0.0.0.0	0.0.0.0
HTTP (TCP / 80)	213.7.46.137	192.168.200.201	0.0.0.0	0.0.0.0
HTTPS (TCP / 443)	213.7.46.137	192.168.200.201	0.0.0.0	0.0.0.0

Below the table, there is a 'New' button and a 'Page: 1, Items: 1 - 3' indicator. The interface also includes a 'Save configuration' button at the top left and a 'Go' button at the top right of the table area.

Fig. 13: Routing -> NAT ->Port Forwarding

This list is used as a basis to forward all FTP requests on the public IP address of your gateway to your FTP server. HTTP and HTTPS requests are forwarded to your Web server accordingly. All other requests are rejected by the gateway.

Click **Save Configuration** and confirm with **OK** to save the configuration as the startup configuration.

2.5.2 Checking the functionality



Functionality can only be checked from the shell. To do this, enter the `debug all` command and confirm with **Return**.

```
r232bw:> debug all
01:36:27 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.201:80/213.7.46.137:80 &t;- 62.137.56.89:1050
01:36:27 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.201:80/213.7.46.137:80 &t;- 62.137.56.89:1051
01:36:27 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.201:80/213.7.46.137:80 &t;- 62.137.56.89:1052
01:36:33 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.202:21/213.7.46.137:21 &t;- 84.135.23.189:1053
```


As the debug extract shows, the HTTP requests (port 80) have been forwarded from IP address 62.137.56.89 to IP address 192.168.200.201. An FTP request (port 21) has also been forwarded from IP address 84.135.23.189 to IP address 192.168.200.202.

2.6 Overview of configuration steps

Configuration of the port

Field	Menu	Value
Ethernet Interface Selection	Physical Interfaces -> Ethernet Ports-> Port Configuration	Switch Port 1 and 2 to <i>en1-0</i>
Ethernet Interface Selection	Physical Interfaces -> Ethernet Ports-> Port Configuration	Switch Port 3 and 4 to <i>en1-1</i>
IP Address/Netmask	LAN -> IP Configuration-> Interfaces -> <en1-0> -> 	<i>192.168.100.1</i> and <i>255.255.255.0</i>
IP Address/Netmask	LAN -> IP Configuration-> Interfaces -> <en1-1> -> 	<i>192.168.200.2</i> and <i>255.255.255.0</i>

Configuring Internet access

Field	Menu	Value
IP / Netmask	LAN -> IP Configuration -> Interfaces -> <en5-0> -> 	<i>213.7.46.137</i> and <i>255.255.255.248</i>
Route Type	Routing -> Routes-> IP Routes-> New	<i>Standard Route</i>
Interface	Routing -> Routes-> IP Routes-> New	<i>LAN_EN5-0</i>
Gateway	Routing -> Routes-> IP Routes-> New	<i>213.7.46.138</i>

NAT

Field	Menu	Value
NAT active	Routing -> NAT -> NAT Interfaces	Enabled for LAN_EN5-0
Silent Deny	Routing -> NAT -> NAT Interfaces	Enabled for LAN_EN5-0

Portforwarding

Field	Menu	Value
Interface	Routing -> NAT -> Portforwarding -> New	<i>LAN_EN5-0</i>
Service	Routing -> NAT -> Portforwarding -> New	<i>FTP</i>
External IP Address	Routing -> NAT -> Portforwarding -> New	e.g. <i>213.7.46.137</i>

Field	Menu	Value
Map to host	Routing -> NAT ->Portforwarding -> New	e.g. <i>192.168.200.202</i>
Interface	Routing -> NAT ->Portforwarding -> New	<i>LAN_EN5-0</i>
Service	Routing -> NAT ->Portforwarding -> New	<i>HTTP</i>
External IP Address	Routing -> NAT ->Portforwarding -> New	e.g. <i>213.7.46.137</i>
Map to host	Routing -> NAT ->Portforwarding -> New	e.g. <i>192.168.200.201</i>
Interface	Routing -> NAT ->Portforwarding -> New	<i>LAN_EN5-0</i>
Service	Routing -> NAT ->Portforwarding -> New	<i>HTTPS</i>
External IP Address	Routing -> NAT ->Portforwarding -> New	e.g. <i>213.7.46.137</i>
Map to host	Routing -> NAT ->Portforwarding -> New	e.g. <i>192.168.200.201</i>

Chapter 3 IP - Load balancing

3.1 Introduction

The following describes configuration of IP load balancing with a **bintec R232bw**.

Configuration is performed with the **Funkwerk Configuration Interface**.

IP load balancing allows distribution of data traffic over several available lines. If one line fails, the other line takes on the entire data traffic. The traffic can be distributed according to various criteria, e.g. half the data traffic can be distributed to each line.

In the case study configured in this workshop, the gateway has two xDSL Internet accesses. Data traffic must be balanced on both connections.

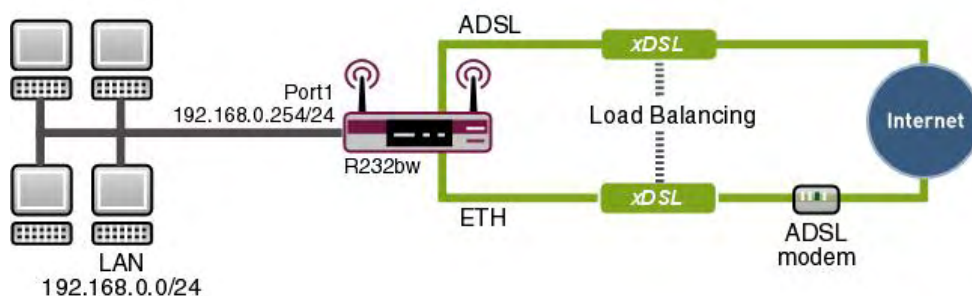


Fig. 14: Case study IP load balancing

Requirements

The following are required for the configuration:

- A **bintec R232bw** gateway
- Boot image from version 7.8.2
- xDSL Internet access connected to **ADSL** port
- xDSL Internet access connected to port **ETH** (a provider DSL modem must be available for this connection)
- Your LAN must be connected to one of ports **1** to **4** on the gateway.

3.2 Configuring internet access

You must create an internet access entry for both internet connections over xDSL.

To set up Internet access over xDSL, go to the following menu:

- (1) Go to **WAN -> Internet + Dialup -> PPPoE -> New**.

The screenshot shows the configuration interface for a bintec R232bw device. The left sidebar contains a navigation menu with categories like System Management, Physical Interfaces, LAN, Wireless LAN, Routing, WAN, ATM, Real Time Jitter Control, VPN, Firewall, VoIP, Local Services, Maintenance, External Reporting, and Monitoring. The main area is titled 'bintec R232bw' and includes a 'Save configuration' button. Below the title are tabs for 'PPPoE', 'PPTP', 'PPPoA', 'ISDN', and 'IP Pools'. The 'PPPoE' tab is active, showing a configuration form with two sections: 'Basic Parameters' and 'Advanced Settings'. The 'Basic Parameters' section includes fields for Description (xDSL_1), PPPoE Mode (Standard selected), PPPoE Ethernet Interface (ethoa50-0), User Name (t-online), Password (masked), Always on (disabled), Connection Idle Timeout (120 seconds), IP Address Mode (Get IP Address selected), Default Route (enabled), and Create NAT Policy (enabled). The 'Advanced Settings' section includes Block after connection failure for (60 seconds), Maximum Number of Dialup Retries (5), Authentication (PAP), DNS Negotiation (enabled), Prioritize TCP ACK Packets (disabled), and LCP Alive Check (disabled). At the bottom of the form are 'OK' and 'Cancel' buttons.

Fig. 15: WAN -> Internet + Dialup -> PPPoE -> New

Relevant fields in the PPPoE menu

Field	Meaning
Description	Give the connection a name. The first character in this field must not be a number and no special characters or umlauts must be used.
PPPoE ethernet interface	Specify the interface for your gateway over which the xDSL connection is to be established.

Field	Meaning
User Name	Enter the user name you received from the provider.
Password	Enter the password you received from the provider.
Always on (flat-rate mode)	This indicates that the gateway does not automatically clear the connection.
Connection Idle Timeout	Define the time in seconds after which the gateway clears the connection in the absence of data traffic.
IP address mode	Defines the mode following which the gateway receives the IP address.
Standard Route	For this connection, a standard route is automatically created.
Create NAT entry	NAT is enabled for this connection.

To set up Internet access over xDSL, proceed as follows:

- (1) In **Description** enter the description for connection `xDSL_1`.
- (2) For **PPPoE Ethernet Interface**, select `ethoa50-0`.
- (3) Under **User Name** enter your user name defined in the access data for your provider.
- (4) Under **Password** enter the password for your Internet access.
- (5) Leave the default setting *Not activated* for **Always on (flat-rate mode)** if you do not have a DSL connection with flatrate.
 If you have an Internet access without flatrate enter the time in seconds after which the gateway should clear the Internet connection when there is no further data exchange under **Connection Idle Timeout**, for example `120`.
 If you have an Internet access with flatrate, select **Always on (Flatrate Mode)**. If selected the gateway will never clear the Internet connection automatically.
- (6) Under **IP Address Mode** select *Get IP Address*.
- (7) Select **Default Route**.
- (8) Select **Create NAT Policy**.
- (9) Leave the remaining settings unchanged and confirm them with **OK**.

As for the first entry, set up a second entry for the second xDSL connection. Under **PPPoE Ethernet Interface** for this connection select `en5-0`.

- (1) Under **Description** enter the name for the connection, e.g. `xDSL_2`.
- (2) For **PPPoE Ethernet Interface**, select `en5-0`.
- (3) Under **User Name** enter your user name defined in the access data for your provider.
- (4) Under **Password** enter the password for your Internet access.
- (5) Leave the default setting *Not activated* for **Always on (flat-rate mode)** if you do not have a DSL connection with flatrate.
 If you have an Internet access without flatrate enter the time in seconds after which

the gateway should clear the Internet connection when there is no further data exchange under **Connection Idle Timeout**, for example *120*.

If you have an Internet access with flatrate, select **Always on (Flatrate Mode)**. If selected the gateway will never clear the Internet connection automatically.

- (6) Under **IP Address Mode** select *Get IP Address*.
- (7) Select **Default Route**.
- (8) Select **Create NAT Policy**.
- (9) Leave the remaining settings unchanged and confirm them with **OK**.

3.2.1 Checking the metric

IP load balancing is only enabled if the routes for both internet accesses are equal. The default routes of the two connections must have the same metric.

- (1) Go to **Routing -> Routes -> IP Routes**.

The screenshot shows the 'IP Routes' configuration page in the bintec R232bw web interface. The page includes a navigation menu on the left with options like System Management, Physical Interfaces, LAN, Wireless LAN, Routing, and WAN. The main content area displays a table of IP routes. The table has the following data:

Destination IP Address	Netmask	Gateway	Interface	Metric	Extended Route	Route Type
192.168.0.0	255.255.255.0	192.168.0.254	LAN_EN1-0	0	<input type="checkbox"/>	Network Route
0.0.0.0	0.0.0.0	0.0.0.0	WAN_XDSL_1	1	<input type="checkbox"/>	Default Route
0.0.0.0	0.0.0.0	0.0.0.0	WAN_XDSL_2	1	<input type="checkbox"/>	Default Route


Below the table, there is a 'Page: 1, Items: 1 - 3' indicator and a 'New' button.


Fig. 16: Routing -> Routes -> IP Routes

Relevant fields in the IP Routes menu

Field	Meaning
Metric	Determines the priority of the route.

Proceed as follows to adjust the metric if the two connections do not have the same metric:

- (1) Go to **Routing -> Routes -> IP Routes**.
- (2) Under **Interface <WAN_XDSL_1>** click the  icon.

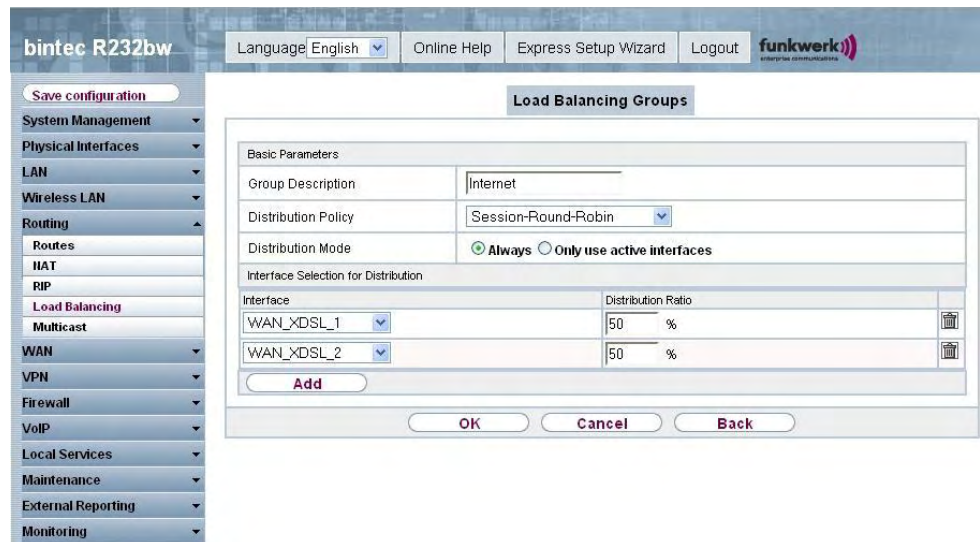
- (3) Under **Metric** select a value, e. g. 1.
- (4) Under **Interface <WAN_XDSL_2>** click the  icon.
- (5) Under **Metric** select the same value as the value for your route over **WAN_XDSL_1**, e. g. 1.
- (6) Confirm with **OK**.

3.3 Configuration of load balancing groups

You must configure load balancing groups to distribute existing data traffic over several interfaces. Since there are two xDSL connections with the same bandwidth, data traffic must be distributed evenly over both connections.

To consolidate both Internet connections into a single load balancing group, go to the following menu:

- (1) Go to **Routing -> Load Balancing ->Load Balancing Groups-> New**.



The screenshot shows the 'Load Balancing Groups' configuration page in the bintec R232bw web interface. The page has a navigation menu on the left and a main configuration area. The configuration area is titled 'Load Balancing Groups' and contains the following fields and options:

- Basic Parameters:**
 - Group Description: Internet
 - Distribution Policy: Session-Round-Robin
 - Distribution Mode: Always Only use active interfaces
- Interface Selection for Distribution:**

Interface	Distribution Ratio
WAN_XDSL_1	50 %
WAN_XDSL_2	50 %

At the bottom of the configuration area, there is an 'Add' button. Below the configuration area, there are three buttons: 'OK', 'Cancel', and 'Back'.

Fig. 17: Routing -> Load Sharing ->Load Sharing Groups -> New

Relevant fields in Load Balancing Groups menu

Field	Meaning
Group description	Enter a description for the load balancing group.
Distribution policy	Select the process according to which the data are distributed.
Interface	Select the interface to be added to the group.
Distribution Ratio	Enter the percentage of sessions to be transferred over the re-

Field	Meaning
	spective interface.

To consolidate both Internet connections into a single load balancing group, proceed as follows:

- (1) Under **Group Description** enter a description for the group, e.g. *Internet*.
- (2) Set **Distribution Policy** to *Session-Round-Robin*.
- (3) Click **Add** to add a member.
- (4) Select the **Interface** *WAN_XDSL_1*.
- (5) In **Distribution Ratio** enter the percentage of sessions which the interface shall handle, here *50*.
- (6) Click **Add** to add a second member.
- (7) Select the **Interface** *WAN_XDSL_2*.
- (8) In **Distribution Ratio** enter the percentage of sessions which the interface shall handle, here *50*.
- (9) Leave the remaining settings unchanged and confirm them with **OK**.

Click **Save Configuration** and confirm with **OK** to save the configuration permanently.

3.4 Result

You have now set up IP load balancing so that the data traffic is distributed evenly on the two existing xDSL connections.

3.5 Checking the configuration

By entering `iploadbiftable` on the gateway's command line, you can display statistics on the previously-defined load balancing groups. Enter the following in the command line for this purpose:

```

r232bw:> iploadbiftable
inx Index(*rw)           GroupId(rw)           Ratio(rw)
  Mode(-rw)             ActAssignedSessions(ro) TotAssignedSessions(ro)
  ActLoad(ro)           ActDownLoad(ro)      ActUpLoad(ro)

  0 10001                1                     50
    enabled              479                   487
    0                    0                     0

  1 10002                1                     50
    enabled              468                   485
    0                    0                     0

r232bw:>

```

Fig. 18: Checking the configuration

3.6 Overview of configuration steps

Internet access over the ADSL port



Field	Menu	Value
Description	WAN -> Internet + Dialup -> PPPoE -> New	e.g. <i>xDSL_1</i>
PPPoE ethernet interface	WAN -> Internet + Dialup -> PPPoE -> New	<i>ethoa50-0</i>
User Name	WAN -> Internet + Dialup -> PPPoE -> New	Your user name, e.g. <i>t-online</i>
Password	WAN -> Internet + Dialup -> PPPoE -> New	Your password
Always on (flat-rate mode)	WAN -> Internet + Dialup -> PPPoE -> New	Enabled for flatrate
IP address mode	WAN -> Internet + Dialup -> PPPoE -> New	<i>Get IP Address</i>
Standard Route	WAN -> Internet + Dialup -> PPPoE -> New	<i>Aktiviert</i>
Create NAT entry	WAN -> Internet + Dialup -> PPPoE -> New	<i>Aktiviert</i>

Internet access over the ETH port

Field	Menu	Value
Description	WAN -> Internet + Dialup -> PPPoE -> New	e.g. <i>xDSL_2</i>
PPPoE ethernet interface	WAN -> Internet + Dialup -> PPPoE -> New	<i>en5-0</i>
User Name	WAN -> Internet + Dialup -> PPPoE -> New	Your user name, e.g. <i>t-online</i>
Password	WAN -> Internet + Dialup -> PPPoE -> New	Your password
Always on	WAN -> Internet + Dialup -> PPPoE -> New	Enabled for flatrate

Field	Menu	Value
(flat-rate mode)		
IP address mode	WAN -> Internet + Dialup -> PPPoE -> New	<i>Get IP Address</i>
Standard Route	WAN -> Internet + Dialup -> PPPoE -> New	<i>Aktiviert</i>
Create NAT entry	WAN -> Internet + Dialup -> PPPoE -> New	<i>Aktiviert</i>

Check metric

Field	Menu	Value
Metric	Routing -> Routes-> IP Routes -> <WAN_xDSL_1> -> 	e.g. 1
Metric	Routing -> Routes-> IP Routes -> <WAN_xDSL_2> -> 	e.g. 1

Load Balancing Groups

Field	Menu	Value
Group description	Routing -> Load Sharing ->Load Sharing Groups -> New	e.g. <i>Internet</i>
Distribution policy	Routing -> Load Sharing ->Load Sharing Groups -> New	<i>Session-Round-Robin</i>
Interface	Routing -> Load Sharing ->Load Sharing Groups -> New	<i>WAN_XDSL_1</i>
Ratio	Routing -> Load Sharing ->Load Sharing Groups -> New	<i>50</i>
Interface	Routing -> Load Sharing ->Load Sharing Groups -> New	<i>WAN_XDSL_2</i>
Ratio	Routing -> Load Sharing ->Load Sharing Groups -> New	<i>50</i>

Chapter 4 IP - Internet access with T 4x4 and external DSL modem

4.1 Introduction

The following describes configuration of Internet access using a DSL modem. You thus are able to navigate the Internet using one or more PC's or other Internet-capable devices.

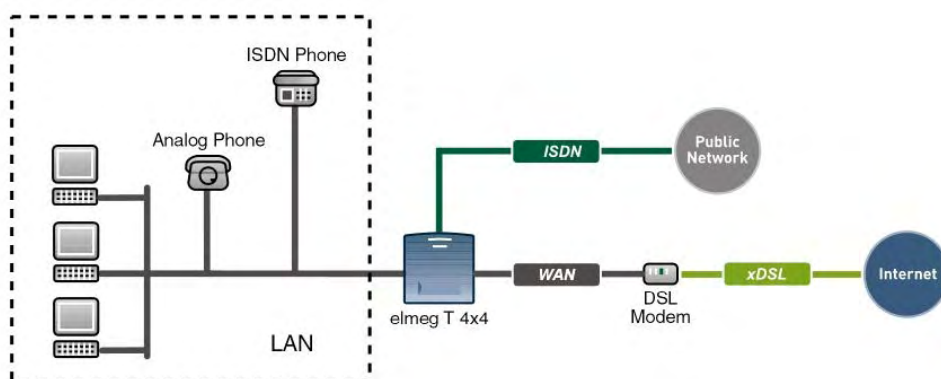


Fig. 19: Example of Internet access with DSL modem

Software version

Testing has occurred with the following software version:

- **elmeg T484** system with Firmware version 7.50
- **elmeg T444** system with Firmware version 7.50
- Win Tools **elmeg ICT system** with version 7.50

4.2 Configuration

To configure Internet access, the **Professional Configurator** version 7.50 must be installed, and an **elmeg T 484** or **elmeg T444** must be connected to the PC via a LAN- or USB cable. Launch the **Professional Configurator**; a window opens displaying the **access control**.



Fig. 20: Access control

First read out the PABX, then click **Readout** on the menu bar. After configuration readout, the system type is automatically recognised and the **Professional Configurator** correspondingly adjusted.

Relevant fields in the Access control menu

Field	Meaning
User Name	Enter <i>Service</i> for User name . Make sure you use the right notation.
Password	Also enter <i>Service</i> for Password . Make sure you use the right notation.
Interface	If the PC is connected to the PABX via a network- or USB cable, select the <i>LAN/USB</i> interface. Click LAN/USB Settings to perform TCP/IP settings.
Logon	Enable <i>Use data for a new login</i> .

Locate the PABX router with **Search**. You may have to modify the Windows XP and Windows Vista firewall! Click **OK** to launch the Configurator.

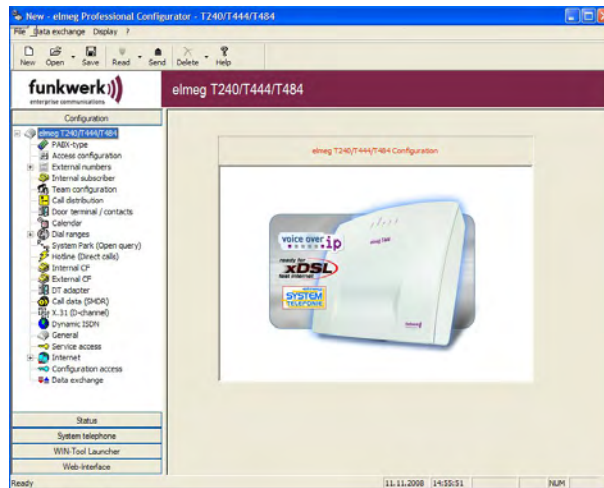


Fig. 21: elmeg Professional Configurator

4.2.1 Configure Internet access (DSL)

Go to **Network** -> **Internet access**. Here, you can select predefined providers from a list. By cancelling the window **Select predefined providers...**, you can configure an Internet provider which does not appear on the list. You can select more than one provider from the list, and configure these later. The list can be selected according to DSL Internet providers, or according to ISDN Internet providers. In the ISDN Internet provider list, you will also find several "call-by-call" entries. If **Only show call-by-call providers without login...** is selected, only providers not requiring login are displayed.

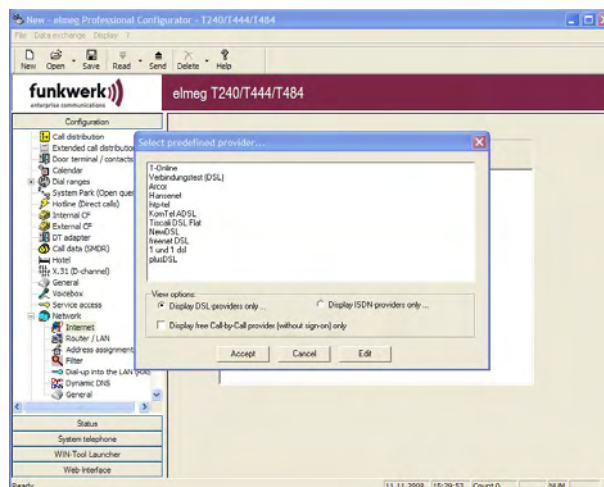


Fig. 22: Configure Internet access

If, for example, your Internet provider is **T-Online DSL**, select the entry in the list, then click on **Apply**. This entry then appears in the **Network->Internet Access** list. By double-clicking on this entry, you can now modify the **properties of the new Internet service provider**, enter your T-Online access data and password, as well as modify the dial-in parameters.

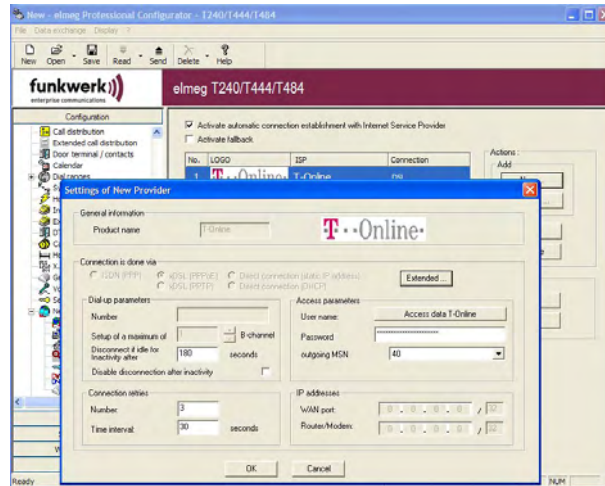


Fig. 23: Properties of the new Internet Service Provider

Release when inactive after


This value determines how much time, in seconds, elapses before the Internet connection is released in a case of inactivity. This setting is useful if the DSL access is not flat-rate, in which case the Internet connection is released after the configured time, only to be re-established if a request is sent out on the Internet (e.g., a website is called up via an Internet browser).

Disable release after inactivity

Enable this check-box if you've ordered flat-rate DSL. This means the ADSL connection is always on and is re-established each time it is terminated.

Connection attempts

The **Number** value displays the number of dialling retries, how often the attempt was made to connect to the provider. **Time** indicates the value in seconds after which there is a renewed attempt to connect to the provider.

 **Important**

If you modify these values and have entered the access data incorrectly, your access to T-Online will be blocked for 24 hours. During this interval, Internet dialin will not be possible.

T-Online access data

You receive your personal access data from your ISP. The terms used for the required access data may vary from provider to provider. However, the type of information you need for dialin is basically the same.

Enter the access data in the appropriate fields. Press **OK** to confirm your entries.

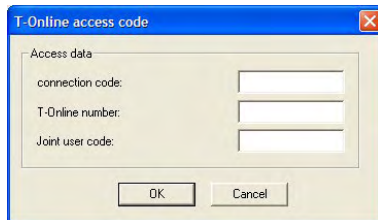


Fig. 24: T-Online access key

When all settings have been performed, send configuration to PABX. Click **Send** on the menu bar. After sending, the PABX is initialised and restarts; this process takes about 30 seconds.

4.2.2 Control Internet access

After the PABX has restarted, an Internet connection is established. To check whether there is an Internet connection, the **Control Center** program was installed during **WinTools** installation.

The **Control Center** is automatically launched when booting the computer; you'll find it in the taskbar at lower right, next to the clock. The small bar underneath it indicates the status of the Internet connection.

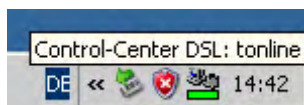







Fig. 25: Control Internet access

If the bar is...		then...
gray		there is no Internet connection.
green		there is a DSL Internet connection.
red left half		there is a 1-channel ISDN Internet connection.
red left and right half		there is a 2-channel ISDN Internet connection.
blocked		the router is blocked and there is no Internet connection.

For additional information, right-click the  symbol (DSL Control Center: tonline).



Fig. 26: Control Center

System Messages	In System messages , you will find current information concerning the system.
Set up connection	Here, you can set up the Internet connection.
Terminated connection	Here, the Internet connection is terminated.

Router Status displays information on the Internet connection.

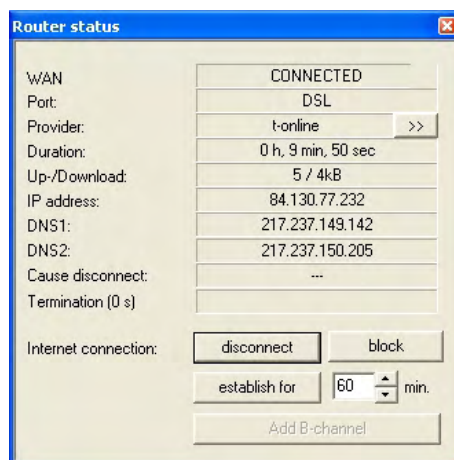


Fig. 27: Router Status

WAN	Indicates whether or not the PABX is connected to the Internet.
Port	Indicates whether the Internet connection is over DSL or ISDN.
Provider	Indicates which ISP you're currently logged in with. With the small >> button, you can switch to other ISP's, if available.
Duration	Indicates duration of the Internet connection.
Up- / Download	Displays up- and download volume.
IP Address	Displays the current IP address assigned to you by the ISP.
DNS 1	Displays the first dynamic name server address.
DNS 2	Displays the second dynamic name server address.
Release cause	In case of disconnection, the cause is displayed here.
Release (0 s)	Here, the time to automatic disconnection of the Internet connection is displayed; the relevant settings are made in the ISP configuration (release if inactive after/disable release if inactive).
Internet connection	The disconnect and establish for buttons are used for manual disconnection or establishment of the Internet connection. With lock , the PABX router is locked; the Internet connection is terminated. Via unlock , the router is unblocked (also via a reboot). The Internet connection can now be established.

4.3 Overview of configuration steps

Access control

Field	Menu	Value
User Name	Access control	<i>Service</i>
Password	Access control	<i>Service</i>
Interface	Access control	e.g. <i>LAN/USB</i>
Logon	Access control	Enable <i>Use data for a new login.</i>

Configure Internet access

Field	Menu	Value
Display only DSL providers...	Network -> Internet access	Enable
Only display call-by-call providers without login...	Network -> Internet access	poss. enable

ISP properties

Field	Menu	Value
Release when inactive after	Network -> Internet access -> T-Online DSL -> Dialin parameters	e.g. <i>180</i> seconds
Disable release when inactive	Network -> Internet access -> T-Online DSL -> Dialin parameters	poss. enable (if DSL flat-rate available)
Number	Network -> Internet access -> T-Online DSL -> Connection attempts	<i>3</i>
Interval	Network -> Internet access -> T-Online DSL -> Connection attempts	<i>30</i>

T-Online access data

Field	Menu	Value
User account	Network -> Internet access -> T-Online DSL -> Login parameters	e.g. <i>000123456789</i>
T-Online number	Network -> Internet access -> T-Online DSL -> Login parameters	e.g. <i>061112345678</i>
Joint user account	Network -> Internet access	e.g. <i>0001</i>

Field	Menu	Value
	-> T-Online DSL -> Login parameters	

Chapter 5 IP - Internet access with T4x4 and another router in LAN

5.1 Introduction

You already have an existing network on premises with several PC's connected to a router. You wish to integrate an **elmeg T444** or **elmeg T484** into your existing network.

The following describes configuration of the PABX to guarantee operation in you existing network.

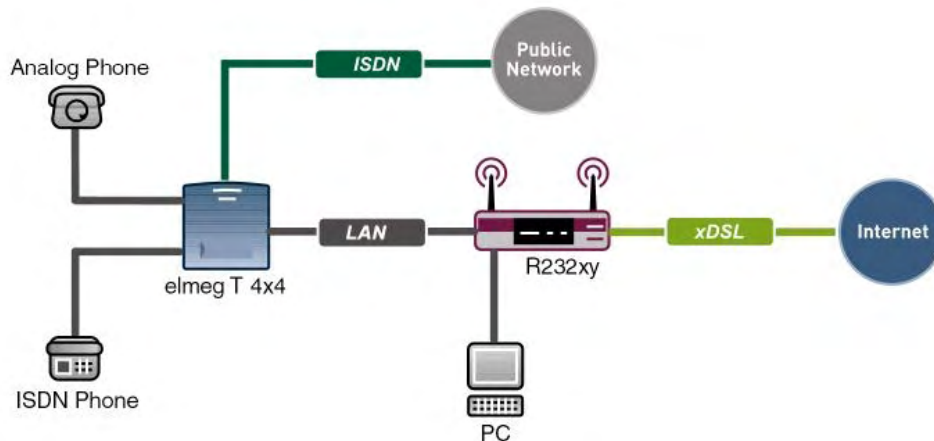


Fig. 28: Example scenario for Internet access with other router in LAN

Software version

Testing has occurred with the following software version:

- **elmeg T484** system with Firmware version 7.50
- **elmeg T444** system with Firmware version 7.50
- Win Tools **elmeg ICT system** with version 7.50

5.2 Configuration

To configure Internet access, the **Professional Configurator** version 7.50 must be installed, and an **elmeg T 484** or **elmeg T444** must be connected to the PC via a LAN- or USB cable. Launch the **Professional Configurator**; a window opens displaying the **access control**.



Fig. 29: Access control

Relevant fields in the Access control menu

Field	Meaning
User Name	Enter <i>Service</i> for User name . Make sure you use the right notation.
Password	Also enter <i>Service</i> for Password . Make sure you use the right notation.
Interface	If the PC is connected to the PABX via a network- or USB cable, select the <i>LAN/USB</i> interface. Click LAN/USB Settings to perform TCP/IP settings.
Logon	Enable <i>Use data for a new login</i> .

Locate the PABX router with **Search**. You may have to modify the Windows XP and Windows Vista firewall! Click **OK** to launch the Configurator.

5.2.1 Configuration steps for the elmeg T4x4 system

Upgrading the **elmeg T4x4** requires a built-in VOIP DSP module for VoIP telephony in LAN and over WAN (e.g., via SIP providers).



Note

The **elmeg T4x4**'s WAN port is no longer necessary, as only the LAN port is used. The system thus no longer has any NAT function! The NAT function is taken over by the upstream router.

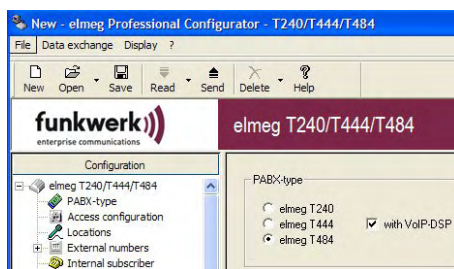


Fig. 30: System type

In the **Network-> Router / LAN** menu, the IP address and corresponding netmask are entered under **System parameters**. In the example, the fixed **IP address** `192.168.0.250` and the **Netmask** `255.255.255.0` are used. In the submenu **DNS Proxy Parameter**, *Use system as DSN proxy* is switched off for name resolution; this is taken over by the **external router in LAN**.

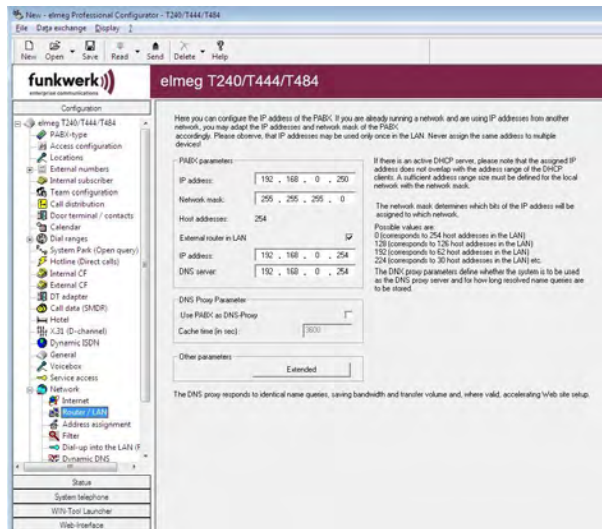


Fig. 31: Network-> Router / LAN

In the **Network->Address Assignment** menu, the DHCP server is disabled/switched off at **Parameters for dynamic IP address assignment**.

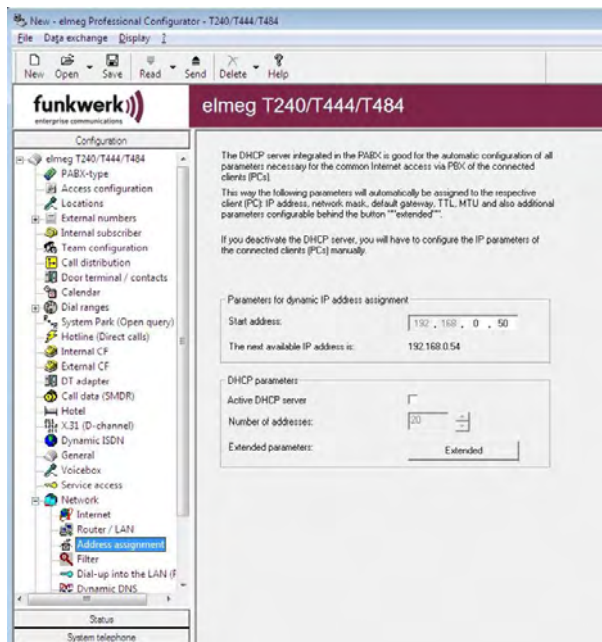


Fig. 32: Address assignment

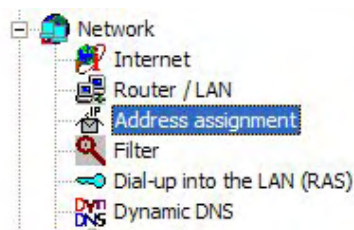


Fig. 33: Network

General settings in the **Network** menu:

Internet Access	not possible
Address assignment with DHCP	switched off
DNS	do not configure
Dynamic DNS	not possible
Filter	not possible

All above positions are administered by the upstream router.

5.3 Overview of configuration steps

Access control

Field	Menu	Value
User Name	Access control	<i>Service</i>
Password	Access control	<i>Service</i>
Interface	Access control	e.g. <i>LAN/USB</i>
Logon	Access control	Enable <i>Use data for a new login.</i>

Select system type

Field	Menu	Value
System type	Configuration -> System type	e.g. <i>elmeg T484</i>
System type	Configuration -> System type	Enable <i>with VoIP-DSP</i>

System parameters

Field	Menu	Value
IP Address	Network -> Router / LAN -> System parameters	e.g. <i>192.168.0.250</i>
Subnet Mask	Network -> Router / LAN -> System parameters	e.g. <i>255.255.255.0</i>
External router in LAN	Network -> Router / LAN -> System parameters	Enable
IP Address	Network -> Router / LAN -> System parameters	e.g. <i>192.168.0.254</i>
DNS Server	Network -> Router / LAN -> System parameters	e.g. <i>192.168.0.254</i>
Use System as DNS Proxy	Network -> Router / LAN -> DSN Proxy Parameters	Disable

Address assignment

Field	Menu	Value
DHCP Parameters	Network -> Address As- signment	<i>DHCP server enabled</i> disable

Chapter 6 IP - IPTV on xDSL (ADSL/VDSL) T-Home Entertainment connection

6.1 Introduction

This solution shows the configuration of a bintec router on a new generation xDSL T-Home Entertainment connection. On ADSL and new generation VDSL T-Home connections, the Internet data and IPTV multicast data are transmitted via separate VLAN interfaces.

The following table shows the main technical information for configuring both accesses:

Internet data access

VLAN ID	7
Network protocol	PPPoE
IP assignment via	IPCP (Internet Protocol Control Protocol)
Routing	Standard route must be configured
NAT	Active (Network Address Translation)

IPTV Multicast data access

VLAN ID	8
IP assignment via	DHCP (Dynamic Host Configuration Protocol)
IGMP proxy	Active (Internet Group Management Protocol)
Routing	Required routes are taught in via DHCP (no other configuration necessary)
NAT	Not mandatory, enabled in the example for security reasons (Network Address Translation)

In this example a VDSL connection is used. The ADSL/VDSL modem is connected to the physical Ethernet port *ETH5*. If you have a device with an integrated DSL modem, you can also use the internal modem.

Funkwerk Configuration Interface is used for configuration.

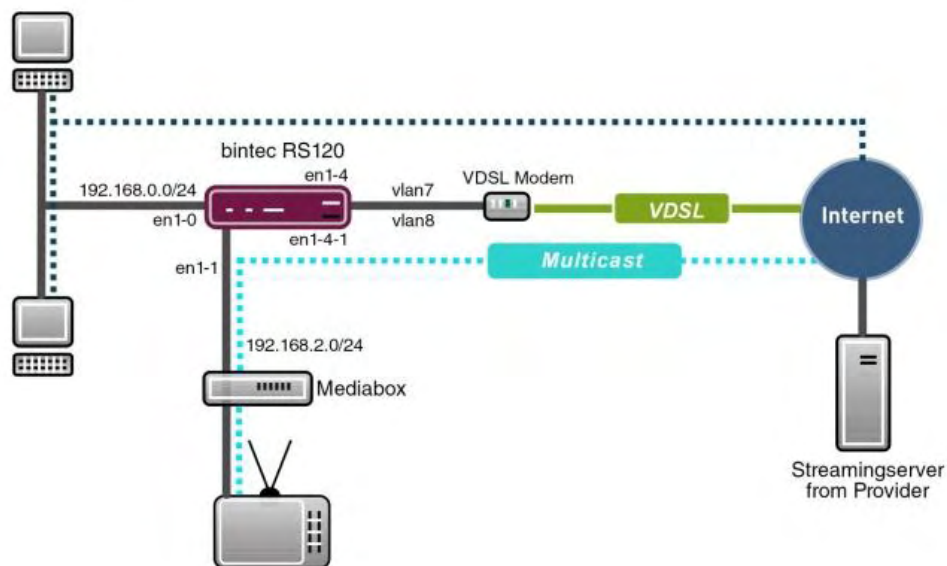


Fig. 34: Example scenario

Requirements

Provider-specific:

- New generation T-Home ADSL/VDSL with T-Home Entertainment packet
- Media Box (T-Home X301T) or similar device (generally supplied by the provider)

Funkwerk-specific:

- In this example, a **bintec RS120** with software version 7.9.4 patch 5 has been used.
- The configuration is identical for other bintec router types. The following list shows the software versions used:

TR200: 7.9.1 Patch 5

RS12x: 7.9.1 Patch 5

RS23x: 7.9.1 Patch 5

R120x: 7.9.1 Patch 5

R300x: 7.9.1 Patch 5

R400x: 7.9.1 Patch 5

- Configuration is carried out via the **Funkwerk Configuration Interface** web configuration

tool.

6.2 Configuration

6.2.1 Configuring the bintec RS120

For configuration, open an Internet browser and start a web (HTTP) connection to the **bintec RS120** router. Unless otherwise configured, use the standard IP address *192.168.0.254*. Once the HTTP connection has been established, log in using the following access data.

User *admin* **Password** *funkwerk* (default password unless otherwise configured).

Configuring VDSL Internet access

The **Funkwerk Configuration Interface** comes with a wizard for configuring VDSL Internet access. For this, go to the following menu:

- (1) Go to **Assistants -> Internet Access-> Internet Connections -> New**.

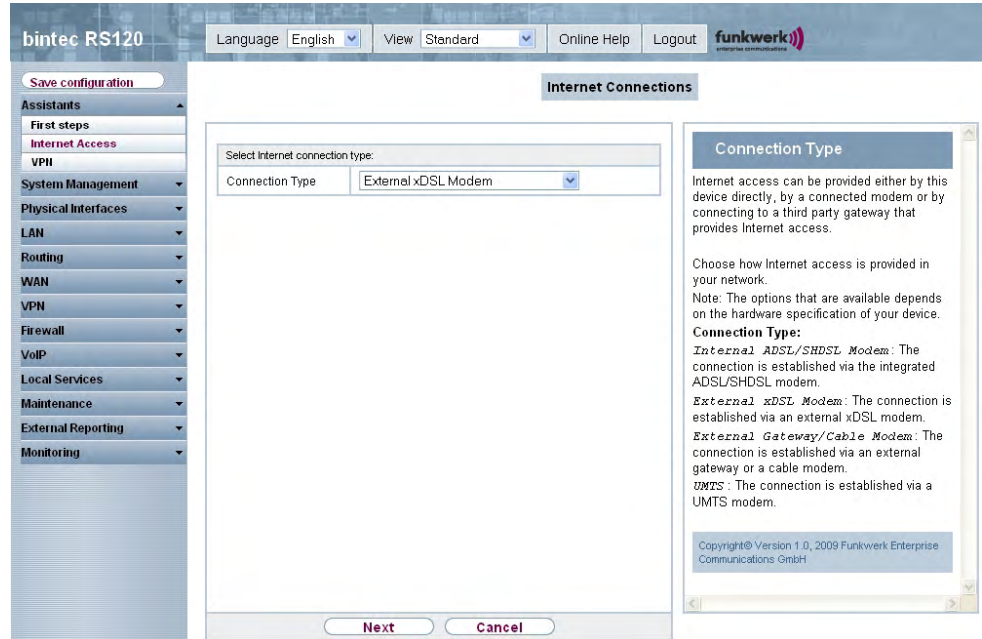


Fig. 35: **Assistants -> Internet Access-> Internet Connections -> New**

Proceed as follows:

- (1) Set the **Connection Type** to *External xDSL Modem*.
- (2) Click **Next** to configure a new Internet connection.

Enter the data required for the Internet connection.

Fig. 36: Assistants -> Internet Access -> Internet Connections -> Next

Proceed as follows to configure a new Internet connection:

- (1) Under **Description** enter a name for the Internet connection, e.g. *Internet Data*.
- (2) Under **Physical Ethernet Port**, select the physical Ethernet port to which the xDSL modem is connected, in this case *ETH5*.
- (3) Under **Internet Service Provider** select the profile *Germany - T-Home - VDSL* for our VDSL connection.
- (4) Under **User Name** enter the access data you received from your provider.
- (5) Enter the **password** you received from your provider.
- (6) In the **Always active** field, specify whether or not the Internet connection should always be on. Only activate this option if you have Internet access with a flatrate.
- (7) Press **OK** to confirm your entries.

6.2.2 Configuring the IPTV Multicast data access

To configure the virtual LAN interfaces for the multicast access, go to the following menu:

- (1) Go to **LAN -> IP Configuration -> Interfaces -> New**.

The screenshot shows the 'Interfaces' configuration page in the bintec RS120 web interface. The left sidebar contains a navigation menu with options like 'Save configuration', 'Assistants', 'System Management', 'Physical Interfaces', 'LAN', 'IP Configuration', 'VLAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Local Services', 'Maintenance', 'External Reporting', and 'Monitoring'. The main content area is titled 'Interfaces' and contains two sections: 'Basic Parameters' and 'Advanced Settings'.

Basic Parameters:

Based on Ethernet Interface	en1-4
Address Mode	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
IP Address / Netmask	<input type="text"/> IP Address <input type="text"/> Netmask <input type="button" value="Add"/>
Interface Mode	<input type="radio"/> Manual <input checked="" type="radio"/> VLAN
MAC Address	<input type="text"/> <input checked="" type="checkbox"/> Use built-in
VLAN ID	8

Advanced Settings:

DHCP MAC Address	<input type="text"/> <input checked="" type="checkbox"/> Use built-in
DHCP Hostname	<input type="text"/>
DHCP Broadcast Flag	<input type="checkbox"/> Enabled
Proxy ARP	<input type="checkbox"/> Enabled
TCP-MSS Clamping	<input type="checkbox"/> Enabled

At the bottom of the form are 'OK' and 'Cancel' buttons.

Fig. 37: LAN->IP Configuration ->Interfaces-> New

Proceed as follows:

- (1) Under **Based on Ethernet Interface** select the logical Ethernet interface that is assigned to the physical Ethernet port used above. For Ethernet port ETH5 this is the interface *en1-4* (see the explanation below).
- (2) Set the **Address Mode** to *DHCP*. An IP address is assigned to the interface dynamically via DHCP.
- (3) Set the **Interface Mode** to *VLAN*. You use this option to assign the interface to a VLAN.
- (4) In the **VLAN-ID** input field enter the VLAN-ID to be used *8*.
- (5) Click **Advanced Settings**.
- (6) Disable the **DHCP Broadcast Flag** option.
- (7) Leave the remaining settings unchanged and confirm your entries with **OK**.

Explanation of the assignment of physical Ethernet ports and logical Ether-

net interfaces

The assignment between the physical Ethernet port and the logical Ethernet interface can be configured flexibly in the routers with integrated switch. In the ex works state, the following assignment generally applies:

Physical Ethernet Port	Logical Ethernet interface
ETH1 to ETH4	en1-0
ETH5	en1-4

Detailed information on your configured assignment can be found in the **Physical Interfaces** menu. The ex works state of the **bintec RS120** router is as follows:

- (1) Go to **Physical Interfaces -> Ethernet Ports -> Port Configuration**.

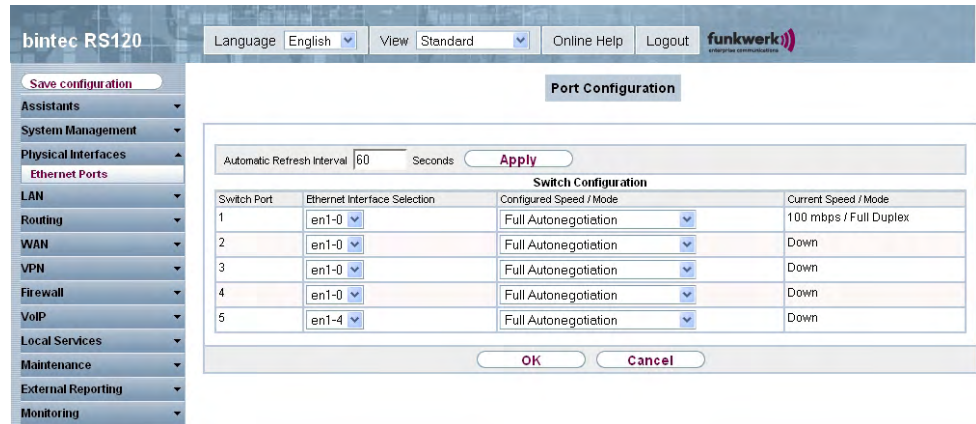


Fig. 38: Physical Interfaces->Ethernet Ports->Port Configuration

Configuring the IGMP Proxy (Internet Group Management Protocol)

In the following section, you will configure the IGMP proxy required to receive IPTV multicast data.

- (1) Go to **Routing -> Multicast -> IGMP -> New**.

The screenshot shows the configuration page for IGMP on a bintec RS120 device. The interface is in English and has a 'Standard' view. The 'IGMP' tab is selected in the top navigation bar. The 'IGMP Settings' section is configured as follows:

IGMP Settings	
Interface	LAN_EN1-0
Query Interval	125 Seconds
Maximum Response Time	10 Seconds
Robustness	2
Last Member Query Interval	1 Seconds
IGMP State Limit	0 Messages per Second
Mode	<input type="radio"/> Host <input checked="" type="radio"/> Routing

The 'Advanced Settings' section is also visible:

Advanced Settings	
IGMP Proxy	<input checked="" type="checkbox"/> Enabled
Proxy Interface	LEASED_EN1-4-1

Fig. 39: Routing -> Multicast -> IGMP -> New

Proceed as follows to configure the IGMP proxy.

- (1) Under **Interface** select the logical Ethernet interface to which the media box or client PCs are connected. In our example, these are Ethernet ports ETH1 to ETH4. Based on the assignment mentioned above, select the logical Ethernet interface `LAN_EN1-0`.
- (2) Select *Routing* under **Mode**.
- (3) Click **Advanced Settings**.
- (4) Enable the option **IGMP Proxy**.
- (5) Under **Proxy Interface** select the VLAN interface generated `LEASED_EN1-4-1`.
- (6) Leave the remaining settings unchanged and confirm your entries with **OK**.

The complete configuration appears as follows (the entry for the IGMP proxy interface (`en1-4-1`) is generated automatically):

The screenshot shows the bintec RS120 web interface. The top navigation bar includes 'Language English', 'View Standard', 'Online Help', and 'Logout'. The left sidebar contains a menu with 'Save configuration' at the top, followed by 'Assistants', 'System Management', 'Physical Interfaces', 'LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Local Services', 'Maintenance', 'External Reporting', and 'Monitoring'. The 'Routing' menu is expanded, showing 'Routes', 'NAT', 'RIP', 'Load Balancing', and 'Multicast'. The 'Multicast' menu is further expanded to show 'Forwarding', 'IGMP', and 'Options'. The 'IGMP' sub-tab is active, displaying a table with the following data:

Interface	Current IGMP Version	IGMP		
en1-0	0	<input checked="" type="checkbox"/> Enabled		
en1-4-1	0	<input checked="" type="checkbox"/> Enabled		

Buttons for 'New', 'OK', and 'Cancel' are visible at the bottom of the table.

Fig. 40: Routing -> Multicast -> IGMP

Enabling the multicast routing function

By default, the forwarding of IP multicast packets to the bintec router is disabled. In the following configuration step, you can enable the multicast routing function on the router. For this, go to the following menu:

- (1) Go to **Routing ->Multicast ->Options**.

The screenshot shows the bintec RS120 web interface. The top navigation bar is the same as in Fig. 40. The left sidebar is also the same. The 'Options' sub-tab is active, displaying a 'Basic Settings' form with the following fields:

IGMP Status	<input type="radio"/> Up <input type="radio"/> Down <input checked="" type="radio"/> Auto	
Mode	<input checked="" type="radio"/> Compatibility Mode <input type="radio"/> Version 3 only	
Maximum Groups	<input type="text" value="64"/>	
Maximum Sources	<input type="text" value="64"/>	
IGMP State Limit	<input type="text" value="0"/>	Messages per Second

Buttons for 'OK' and 'Cancel' are visible at the bottom of the form.

Fig. 41: Routing -> Multicast -> Options

Proceed as follows:

- (1) Set the **IGMP Status** to *Active* or *Auto*.
- (2) Confirm your entries with **OK**.



Note

You must confirm the configuration page with **OK** once. This also applies if the **IGMP Status** has already been set to *Auto* or *Active*.

Enabling NAT on the IGMP proxy interface

For security reasons and in order to ensure the functioning of video on demand services you need to enable the NAT function.

- (1) Go to **Routing -> NAT -> NAT Interfaces**.

Interface	NAT active	Silent Deny	PPTP Passthrough	Portforwards
LAN_EN1-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LEASED_EN1-4-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
WAN_INTERNET-DATEN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

Fig. 42: **Routing -> NAT -> NAT Interfaces**

Proceed as follows:

- (1) Enable the `LEASED_EN1-4-1` interface under **NAT Active**.
- (2) Confirm with **OK**.

6.2.3 Configuring a DHCP-IP address pool on the LAN interface

The T-Home media box requires the dynamic assignment of the IP address settings over DHCP. A DHCP-IP address pool on the LAN interface must therefore be configured for this purpose. In our example, this is the interface `en1-0`.

**Note**

Only carry out this configuration step if there are no other DHC servers in your local network. In this case, enter the LAN IP address of the **bintec RS120** router as the **Router** on the DHCP server. In our example, the LAN IP address of the **bintec RS120** is *192.168.0.254*.

If there is no DHCP server in your local network, proceed as follows:

- (1) Go to **Local Services** -> **DHCP Server** -> **DHCP Pool** -> **New**.

The screenshot shows the configuration page for a new DHCP pool on a bintec RS120 router. The interface includes a top navigation bar with 'Language English', 'View Standard', 'Online Help', and 'Logout'. A left sidebar contains a menu with categories like 'Assistants', 'System Management', 'Physical Interfaces', 'LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Local Services', 'Maintenance', 'External Reporting', and 'Monitoring'. The 'Local Services' menu is expanded to show 'DHCP Server', which is further expanded to 'DHCP Pool'. The main content area has tabs for 'DHCP Pool', 'IP/MAC Binding', and 'DHCP Relay Settings'. The 'DHCP Pool' tab is active, showing a form with the following fields: 'Interface' (en1-0), 'IP Address Range' (192.168.0.100 - 192.168.0.150), and 'Pool Usage' (Local). Below the form is an 'Advanced Settings' section with 'OK' and 'Cancel' buttons.

Fig. 43: **Local Services** -> **DHCP Server** -> **DHCP Pool** -> **New**

Proceed as follows to set up an IP address pool:

- (1) Under **Interface** select the logical interface *en1-0*.
- (2) Enter an **IP Address Range**. In our example, an IP address from *192.168.0.100* to *192.168.0.150* is configured.
- (3) Press **OK** to confirm your entries.

**Note**

The IP address range must lie within the IP network range configured on the LAN interface.

6.2.4 Bootable backup of the configuration

This concludes the configuration. If the terminal is connected correctly, the Internet data connection should function correctly and IPTV data should be received. To perform a bootable backup of the configuration, exit the **Funkwerk Configuration Interface** with **Save configuration** and confirm with **OK**.

6.3 Overview of configuration steps

Selecting a connection type

Field	Menu	Value
Interface	Assistants -> Internet Access -> Internet Connections	<i>External xDSL Modem</i>

Setting up an internet connection

Field	Menu	Value
Description	Assistants -> Internet Access -> Internet Connections -> Next	e.g. <i>Internet data</i>
Physical Ethernet Port	Assistants -> Internet Access -> Internet Connections -> Next	<i>ETH5</i>
Internet Service Provider	Assistants -> Internet Access -> Internet Connections -> Next	e.g. <i>Germany-T-Home-VDSL</i>
User Name	Assistants -> Internet Access -> Internet Connections -> Next	e.g. <i>123456789#0001@t-online.de</i>
Password	Assistants -> Internet Access -> Internet Connections -> Next	e.g. <i>secret</i>
Always Active	Assistants -> Internet Access -> Internet Connections -> Next	<i>Aktiviert</i>

Configuring the VLAN interface

Field	Menu	Value
Based on Ethernet Interface	LAN-> IP Configuration -> Interfaces -> New	<i>en1-4</i>
Address mode	LAN-> IP Configuration -> Interfaces -> New	<i>DHCP</i>
Interface Mode	LAN-> IP Configuration -> Interfaces -> New	<i>VLAN</i>

Field	Menu	Value
VLAN ID	LAN-> IP Configuration -> Interfaces -> New	8
DHCP Broadcast flag	LAN-> IP Configuration -> Interfaces -> New	Disabled

Configuring the IGMP proxy

Field	Menu	Value
Interface	Routing -> Multicast-> IGMP -> New	LAN_EN1-0
Mode	Routing -> Multicast-> IGMP -> New	Routing
IGMP Proxy	Routing -> Multicast-> IGMP -> New	Aktiviert
Proxy Interface	Routing -> Multicast-> IGMP -> New	LEASED_EN1-4-1

Enabling the multicast routing function

Field	Menu	Value
IGMP Status	Routing -> Multicast-> Options	Active or Auto

Activating NAT

Field	Menu	Value
LEASED_EN1-4-1 interface	Routing -> NAT -> NAT Interfaces	NAT active <i>Enabled</i>

Configuring the DHCP IP address pool

Field	Menu	Value
Interface	Local Services -> DHCP Server-> DHCP Pool -> New	en1-0
IP Address Range	Local Services -> DHCP Server-> DHCP Pool -> New	e.g. 192.168.0.100 - 192.168.0.150
Pool Usage	Local Services -> DHCP Server-> DHCP Pool -> New	Local