



Manual Workshops (Excerpt)

Services Workshops

Copyright© Version 01/2020 bintec elmeg GmbH

Legal Notice

Warranty

This publication is subject to modifications.

bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH is not liable for the information in this manual. bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH accepts no liability for any direct, indirect, incidental, consequential or other damages associated with the distribution, provision or use of this manual.

Copyright © bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH

bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH reserves all rights to the data included – especially for duplication and disclosure.

Table of Contents

Chapter 1	Services - DHCP	1
1.1	Introduction	1
1.2	Configuration	3
1.2.1	Configuring as a DHCP server	3
1.2.2	Configuration as DHCP Client	6
1.2.3	Configuring a DHCP relay server	7
1.3	Overview of configuration steps	9
Chapter 2	Services - DynDNS	10
2.1	Introduction	10
2.2	Configuration.	11
2.2.1	New Provider	11
2.2.2	Configuring DynDNS	12
2.2.3	NAT entries for administration with the GUI	13
2.3	Result.	14
2.4	Checking the connection.	14
2.5	Overview of configuration steps.	14
Chapter 3	Services - Time-controlled Tasks	16
3.1	Introduction	16
3.2	Configuration.	17
3.2.1	Daily reboot	17
3.2.2	Suspending the WLAN interface	18
3.2.3	Monthly configuration backup	20
3.3	Overview of configuration steps.	21

Chapter 4	Services - Prioritisation of a VPN IPSec connection ahead of other Internet traffic	24
4.1	Introduction	24
4.2	Configuration	25
4.2.1	Configuration of gateway in head office (bintec R3002)	25
4.2.2	Configuration of Internet access via the GUI Assistant	25
4.2.3	Configuration of the VPN IPSec access of the first branch via the GUI Assistant	26
4.2.4	Configuration of gateway in head office (bintec RS120)	28
4.2.5	Configuration of Internet access via the GUI Assistant	29
4.2.6	Configuration of the VPN IPSec tunnel on the branch gateway	30
4.3	Testing the VPN connection	32
4.4	Prioritisation of the VPN tunnel on the branch gateway ahead of other Internet traffic	33
4.4.1	Creation of QoS filters	33
4.4.2	Assignment of QoS filter to QoS class or high priority class	34
4.4.3	Enabling QoS on the WAN interface	36
4.4.4	QoS Monitoring	37
4.5	Overview of Configuration Steps	37
Chapter 5	Services - Automatic Router Backup (Redundancy) with BRRP for an Internet / VPN gateway	42
5.1	Introduction	42
5.2	Configuration	43
5.2.1	Configuration of the Advertisement and Management IP address	43
5.2.2	Configuration of the virtual router	46
5.2.3	Enabling of BRRP configuration	48
5.2.4	Synchronisation of the virtual routers	50
5.3	Overview of Configuration Steps	51

Chapter 6	Services - Remote Maintenance for a bintec RS232bu+ UMTS Gateways Using GSM/GPRS Dial-In	54
6.1	Introduction	54
6.2	Configuration	55
6.3	Test the UMTS fallback with an incoming voice connection	57
6.4	Dial-in by ISDN login from a different bintec ISDN gateway	58
6.5	Overview of Configuration Steps	59

Chapter 1 Services - DHCP

1.1 Introduction

The configuration of Dynamic Host Configuration Protocol (DHCP) is described in the following chapters.

You can use your device as a DHCP server, DHCP client or DHCP relay agent.

Configuration in this scenario is carried out using the **GUI** (Graphical User Interface).

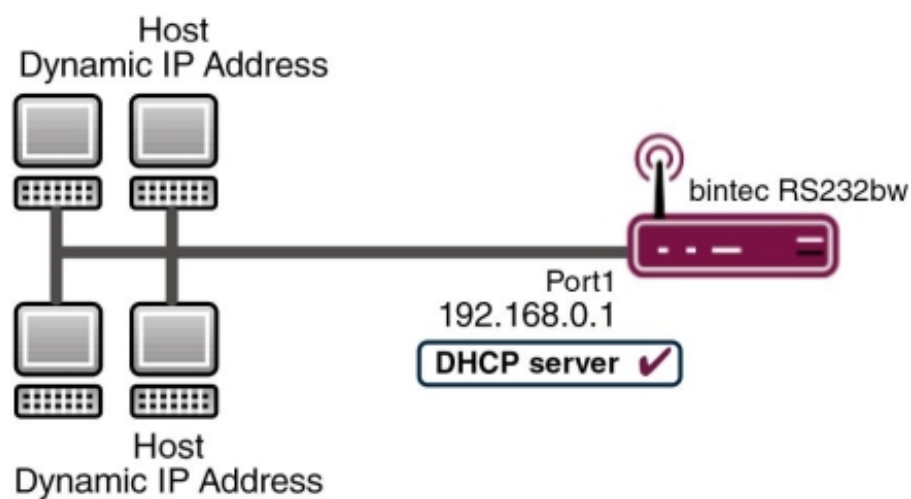


Fig. 1: Example scenario as a DHCP server

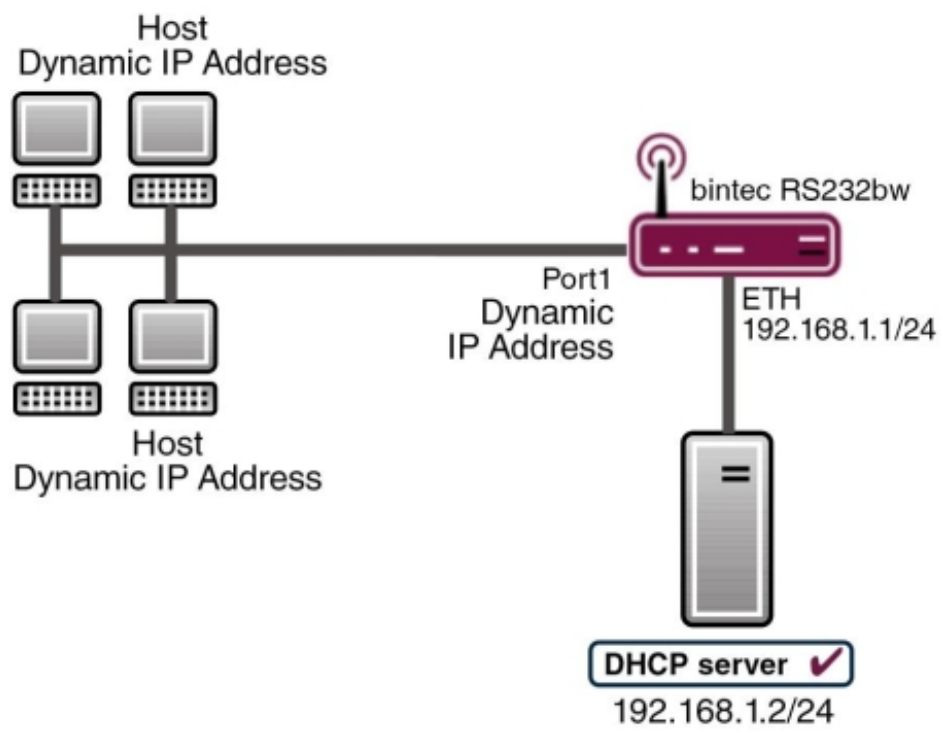


Fig. 2: Example scenario as a DHCP client

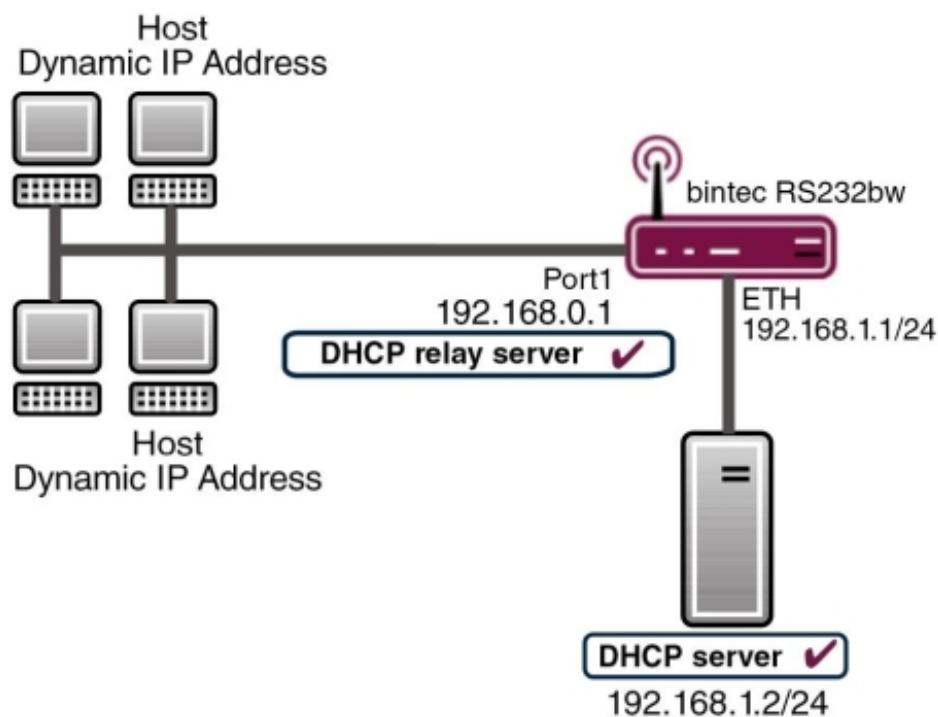


Fig. 3: Example scenario as a DHCP relay server

Requirements

The following are required for the configuration:

- Boot image from version 7.10.1
- An optional DHCP server

1.2 Configuration

1.2.1 Configuring as a DHCP server

If you wish to assign an IP address to the client computers in the network dynamically through your gateway, you must configure it as a DHCP server. To activate your device as a DHCP server, you must first define IP address pools from which the IP addresses are distributed to the requesting clients.

For this, go to the following menu:

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

Fig. 4: **Local Services** -> **DHCP Server** -> **DHCP Pool** -> **New**

Relevant fields in menu DHCP Pool

Field	Meaning
Interface	Here you select the interface via which the IP addresses are to be distributed by DHCP.
IP Address Range	Enter the first and last IP addresses to be assigned by DHCP.
Pool Usage	Specify whether the IP pool is used for DHCP requests in the same subnet or for DHCP requests that have been forwarded to your device from another subnet. In this case it is possible to define IP addresses from another network.

Additional configuration parameters can be found under **Advanced Settings**:

Relevant fields in the menu Advanced Settings

Field	Meaning
Gateway	Here you can specify whether the gateway is to be used as a default gateway or can enter a gateway IP address if the gateway is not to be used as a default gateway.
Lease Time	The length of time in minutes that the client can keep the IP address.

Proceed as follows to configure your gateway as a DHCP server:

- (1) Select your LAN interface for **Interface**, e.g. `en1-0`.
- (2) Enter the first and last IP addresses from your LAN under **IP Range**, e.g. `192.168.0.2` and `192.168.0.10`.

- (3) In **Pool Use**, select *Local*.
- (4) Under **Gateway** select *Use gateway as router*.
- (5) Leave the **Lease Time** set to *120*.
- (6) Confirm with **OK**.

The **GUI** offers a facility for checking whether or not IP addresses are assigned to clients from the DHCP pool and if so which addresses are involved. To check who has received an IP address, select the following menu options:

- (1) Go to **Local Services -> DHCP Server -> IP/MAC Binding**.

Fig. 5: **Local Services -> DHCP Server ->IP/MAC Binding**

Here you obtain all the important information concerning the issue of IP addresses from the DHCP pool.

The gateway assigns an IP address to the client as the DHCP server and not only sends the IP address of the gateway to the client, but also the IP address of the DNS server.

Use the following menu item to determine which IP address the gateway sends to the client as the DNS server address:

- (1) Go to **Local Services -> DNS -> Global Settings -> Advanced Settings**.

The screenshot shows the configuration interface for DHCP. On the left is a navigation menu with 'Local Services' expanded to 'DNS'. The main window has tabs for 'Global Settings', 'Static Hosts', 'Domain Forwarding', 'Cache', and 'Statistics'. The 'Global Settings' tab is active, showing 'Basic Parameters' and 'Advanced Settings'. In the 'Advanced Settings' section, 'Positive Cache' and 'Negative Cache' are both checked. 'Cache Size' is set to 100 entries. 'Maximum TTL for Positive Cache Entries' and 'Maximum TTL for Negative Cache Entries' are both set to 86400 seconds. 'Fallback interface to get DNS server' is set to 'Automatic'. The 'IP address to use for DNS/WINS server assignment' is set to 'Global DNS Setting'.

Fig. 6: Local Services -> DNS -> Global Settings -> Advanced Settings

Relevant fields in the Advanced Settings menu

Selection	Meaning
IP Address to use for DNS/WINS Server Assignment:	Select the most suitable method for your network environment from the following options:
As DHCP Server	<ul style="list-style-type: none"> • <i>None</i>: The gateway issues no DNS server IP addresses with this setting. • <i>Own IP address</i>: The gateway assigns its own IP address as DNS. • <i>Global DNS Setting</i>: The gateway assigns the IP addresses as DNS, which you have configured or assigned dynamically in the Local Services -> DNS -> Global Settings menu.

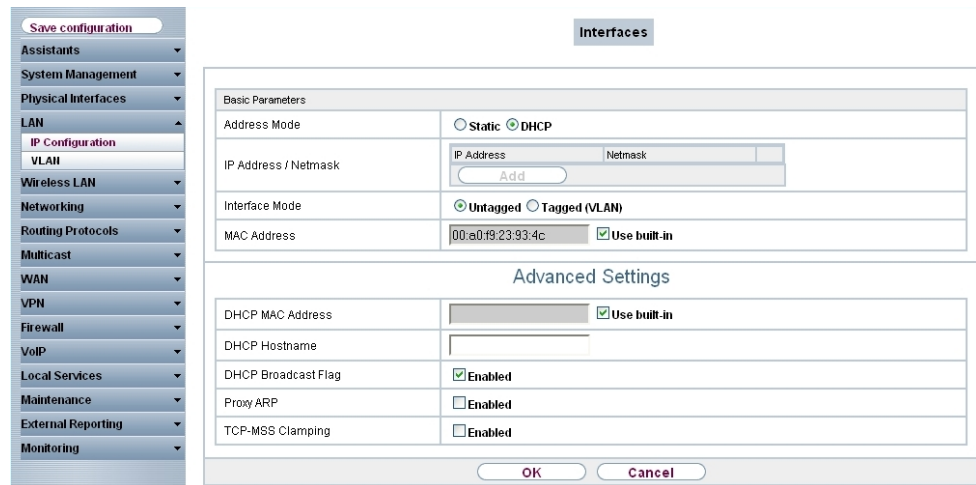
You can normally keep the *Own IP Address* setting for **As DHCP Server**.

1.2.2 Configuration as DHCP Client

The gateway has the possibility of obtaining its own IP address dynamically from a DHCP server at an Ethernet interface.

Go to the following menu to configure your Ethernet interface to DHCP client mode:

- (1) Go to **LAN -> IP Configuration -> Interfaces -> <en1-4>** -> .



The screenshot shows a web-based configuration interface. On the left is a navigation menu with categories like Assistants, System Management, Physical Interfaces, LAN, IP Configuration, VLAN, Wireless LAN, Networking, Routing Protocols, Multicast, WAN, VPN, Firewall, VoIP, Local Services, Maintenance, External Reporting, and Monitoring. The 'LAN' section is expanded, and 'IP Configuration' is selected. The 'Interfaces' sub-menu is open, showing configuration for interface 'en1-4'. The 'Basic Parameters' section includes: Address Mode (Static/DHCP), IP Address / Netmask (with an 'Add' button), Interface Mode (Untagged/Tagged (VLAN)), and MAC Address (00:a0:f9:23:93:4c, with 'Use built-in' checked). The 'Advanced Settings' section includes: DHCP MAC Address (with 'Use built-in' checked), DHCP Hostname, DHCP Broadcast Flag (checked), Proxy ARP (unchecked), and TCP-MSS Clamping (unchecked). 'OK' and 'Cancel' buttons are at the bottom.

Fig. 7: **LAN -> IP Configuration -> Interfaces -><en1-4>** -> .

Relevant fields in the Interfaces menu

Field	Meaning
Address mode	Select DHCP to obtain an IP address as client via the interface.

Additional configuration parameters can be found under **Advanced Settings**.

Relevant fields in the menu Advanced Settings

Field	Meaning
DHCP MAC Address	If you expect an IP address from a certain DHCP server, you can enter its MAC address here.

Proceed as follows to configure the gateway as a DHCP client:

- (1) Set **Address Mode** to *DHCP*.
- (2) Confirm with **OK**.

Now you should receive all the important configuration parameters like IP address, gateway and DNS from your DHCP server.

1.2.3 Configuring a DHCP relay server

If the gateway for the local network does not distribute any IP addresses to the clients by DHCP, it can still forward the DHCP requests on behalf of the local network to a remote DHCP server.

The DHCP server then assigns the gateway an IP address from its pool, which in turn sends this to the client in the local network. The settings for a DHCP relay server can be modified in the following submenu:

- (1) Go to **Local Services -> DHCP Server -> DHCP Relay Settings**.

Fig. 8: **Local Services -> DHCP Server -> DHCP Relay Settings**

Relevant fields in the DHCP Relay Settings menu

Field	Meaning
Primary DHCP Server	Enter the IP address of the first server.
Secondary DHCP Server	Enter the IP address of the second server, if one exists.

Proceed as follows to configure the gateway as a DHCP relay agent:



- (1) Enter the server IP address, e.g. `192.168.1.2`, for the **Primary DHCP Server**.
- (2) Confirm with **OK**.

1.3 Overview of configuration steps

DHCP Server

Field	Menu	Value
Interface	Local Services -> DHCP Server -> DHCP Pool -> New	e.g. <i>en1-0</i>
IP Address Range	Local Services -> DHCP Server -> DHCP Pool -> New	e.g. <i>192.168.0.2</i> and <i>192.168.0.10</i>
Pool Usage	Local Services -> DHCP Server -> DHCP Pool -> New	<i>Local</i>
Gateway	Local Services -> DHCP Server -> DHCP Pool -> New -> Advanced Settings	<i>Use Router as Gateway</i>
Lease Time	Local Services -> DHCP Server -> DHCP Pool -> New -> Advanced Settings	e.g. <i>120</i>
IP Address to use for DNS/WINS Server Assignment: As DHCP Server	Local Services -> DNS -> Global Settings -> Advanced Settings	e.g. <i>Own IP address</i>

DHCP Client

Field	Menu	Value
Address mode	LAN -> IP Configuration -> Interfaces -> <en1-4> -> 	<i>DHCP</i>
DHCP MAC Address (optional)	LAN -> IP Configuration -> Interfaces -> <en1-4> ->  -> Advanced Configurations	MAC address for a specific DHCP server

DHCP Relay Server

Field	Menu	Value
Primary DHCP Server	Local Services -> DHCP Server -> DHCP Relay Settings	e.g. <i>192.168.1.2</i>
Secondary DHCP Server (optional)	Local Services -> DHCP Server -> DHCP Relay Settings	if one exists

Chapter 2 Services - DynDNS

2.1 Introduction

The following chapters describe the configuration of DynDNS.

You create an entry for the DynDNS provider *no-IP* and configure your DynDNS name *bintec.no-ip.com*. You then create NAT enables in order to administrate the gateway over the Internet using http.

Configuration in this scenario is carried out using the **GUI** (Graphical User Interface).

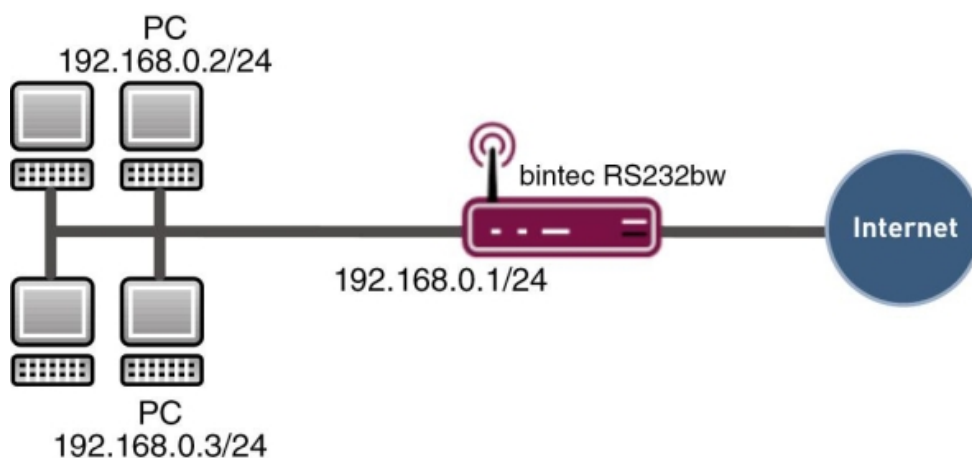


Fig. 9: Example scenario DynDNS

Requirements

The following are required for the configuration:

- Basic configuration of the gateway
- Boot image from version 7.10.1
- Configuration requires a working Internet access
- Successful registration with the DynDNS provider www.no-ip.com

2.2 Configuration

Only the following menu is used for configuring DynDNS:

- (1) Go to **Local Services** -> **DynDNS Client**.

2.2.1 New Provider

If you would like to use a DynDNS provider not yet included in the list under the menu option **Local Services** -> **DynDNS Client** -> **DynDNS Provider**, you must add this via the following menu:

- (1) Go to **Local Services** -> **DynDNS Client** -> **DynDNS Provider** -> **New**.

The screenshot shows the configuration interface for a DynDNS provider. On the left is a navigation tree with 'Local Services' expanded to 'DynDNS Client'. The main area displays a 'DynDNS Update' dialog box with the following fields:

Basic Parameters	
Provider Name	no-IP
Server	dynupdate.no-ip.com
Update Path	/nic/update
Port	80
Protocol	DynDNS
Update Interval	300 Seconds

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

Fig. 10: **Local Services** -> **DynDNS Client** -> **DynDNS Provider** -> **New**

Relevant fields in the DynDNS Provider menu

Field	Meaning
Provider Name	Give the provider a name.
Server	Enter the IP address or domain names of the update server.
Update Path	The path to the registration script.
Port	Enter the port via which the client receives the update.
Protocol	The protocol used by the DynDNS provider.

Proceed as follows:

- (1) Enter a **Provider Name**, e.g. *no-IP*.

- (2) Enter *dynupdate.no-ip.com* for **Server**.
- (3) Enter */nic/update* under **Update Path**.
- (4) Leave the **Port** set to *80*.
- (5) Select *DynDNS* for **Protocol**.
- (6) Confirm with **OK**.

2.2.2 Configuring DynDNS

Create an entry in the gateway for your registered DynDNS name. For this, go to the following menu:

- (1) Go to **Local Services -> DynDNS Client -> DynDNS Update -> New**.

The screenshot shows the configuration interface for a DynDNS Update. On the left is a navigation menu with 'Local Services' expanded to 'DynDNS Client'. The main area is titled 'DynDNS Update' and contains a form with the following fields:

- Host Name: bintec.no-ip.com
- Interface: Internet (dropdown)
- User Name: name@email.de
- Password: masked with dots
- Provider: no-IP (dropdown)
- Enable update: Enabled

At the bottom of the form are 'OK' and 'Cancel' buttons, and a link for 'Advanced Settings'.

Fig. 11: **Local Services -> DynDNS Client -> DynDNS Update -> New**

Relevant fields in the DynDNS Update menu

Field	Meaning
Hostname	Enter the complete host name you have registered.
Interface	Select the internet interface.
User Name	Enter your user name.
Password	Enter your password.
Provider	Select your DynDNS provider.
Enable update	Activate or deactivate the entry.

Proceed as follows:

- (1) Enter **Host Name**, e.g. *bintec.no-ip.com*.

- (2) Select **Interface**, e.g. *Internet*.
- (3) Enter **User Name**, e.g. *name@email.de*.
- (4) Under **Password** enter *secret* for example.
- (5) The **Provider** is *no-IP*.
- (6) Activate **Enable Update**.
- (7) Confirm with **OK**.

2.2.3 NAT entries for administration with the GUI

You should be able to administrate your gateway using HTTP over the Internet. Go to the following menu to configure the corresponding NAT enable:

- (1) Go to **Networking -> NAT -> NAT Configuration -> New**.

The screenshot shows the 'NAT Configuration' window in a web-based GUI. On the left is a navigation menu with 'Networking' expanded to show 'NAT'. The main window has two tabs: 'NAT Interfaces' and 'NAT Configuration'. The 'NAT Configuration' tab is active, showing a form for creating a new NAT rule. The form is divided into sections: 'Basic Parameters', 'Specify original traffic', and 'Replacement Values'. The 'Interface' is set to 'WAN_INTERNET', the 'Type of traffic' is 'incoming (Destination NAT)', and the 'Service' is 'http'. The 'Source IP Address/Netmask' and 'Original Destination IP Address/Netmask' are both set to 'Any'. Under 'Replacement Values', the 'New Destination IP Address/Netmask' is set to 'Host' with the value '0.0.0.0', and the 'New Destination Port' is set to 'Original' with a checked checkbox.

Fig. 12: Networking -> NAT -> NAT Configuration -> New

Relevant fields in the Portforwarding menu

Field	Meaning
Interface	This is the connection that the NAT enable should receive.
Service	This is the service you reach from outside the gateway.
Source IP Address/Net-mask	Enter the external IP address of the gateway here.
New Destination Port	The IP address to which you wish to be forwarded when you reach the gateway.

Proceed as follows to configure the NAT enable:

- (1) Set the **Interface** to *WAN_INTERNET* for example.

- (2) Configure the **Service** to `http`.
- (3) Under **Source IP Address/Netmask** select `Any`.
- (4) Leave other settings unchanged and confirm your entries with **OK**.

2.3 Result

You have entered the DynDNS provider `no-IP` and your registered a DynDNS name in the gateway. The bintec gateway can now also be administrated over the Internet.

2.4 Checking the connection

Go to the following menu to check that the current IP address is successfully registered with the DynDNS provider:

- (1) Go to **Local Services -> DynDNS Client**.

The **Status** field of this menu must be set to `up-to-date`.

If you wish to administrate the bintec gateway over the Internet, enter the following in the Browser on a remote computer:

e.g. `bintec.no-ip.com`

You should then receive the login of the **GUI** for the bintec gateway.

2.5 Overview of configuration steps

Creating new providers

Field	Menu	Value
Provider Name	Local Services -> DynDNS Client -> DynDNS Providers -> New	e.g. <code>no-IP</code>
Server	Local Services -> DynDNS Client -> DynDNS Providers -> New	<code>dynup-date.no-ip.com</code>
Update Path	Local Services -> DynDNS Client -> DynDNS Providers -> New	<code>/nic/update</code>
Port	Local Services -> DynDNS Client -> DynDNS Providers -> New	<code>80</code>
Protocol	Local Services -> DynDNS Client -> DynDNS Providers -> New	<code>DynDNS</code>

Configuring DynDNS

Field	Menu	Value
Hostname	Local Services -> DynDNS Client -> DynDNS Update -> New	e.g. <i>bintec.no-ip.com</i>
Interface	Local Services -> DynDNS Client -> DynDNS Update -> New	e.g. <i>Internet</i>
User Name	Local Services -> DynDNS Client -> DynDNS Update -> New	e.g. <i>name@email.de</i>
Password	Local Services -> DynDNS Client -> DynDNS Update -> New	e.g. <i>secret</i>
Provider	Local Services -> DynDNS Client -> DynDNS Update -> New	<i>no-IP</i>
Enable update	Local Services -> DynDNS Client -> DynDNS Update -> New	<i>Aktiviert</i>

NAT entries

Field	Menu	Value
Interface	Networking -> NAT -> NAT Configuration -> New	e.g. <i>WAN_INTERNET</i>
Service	Networking -> NAT -> NAT Configuration -> New	<i>http</i>
Source IP Address/Net-mask	Networking -> NAT -> NAT Configuration -> New	<i>Any</i>

Chapter 3 Services - Time-controlled Tasks

3.1 Introduction

The following chapters describe the configuration of time-controlled tasks.

- You want to reboot your gateway automatically overnight.
- The WLAN interface is to be suspended at the weekend.
- In addition, the configuration is to be backed up automatically once a month on a TFTP server.

Configuration in this scenario is carried out using the **GUI** (Graphical User Interface).

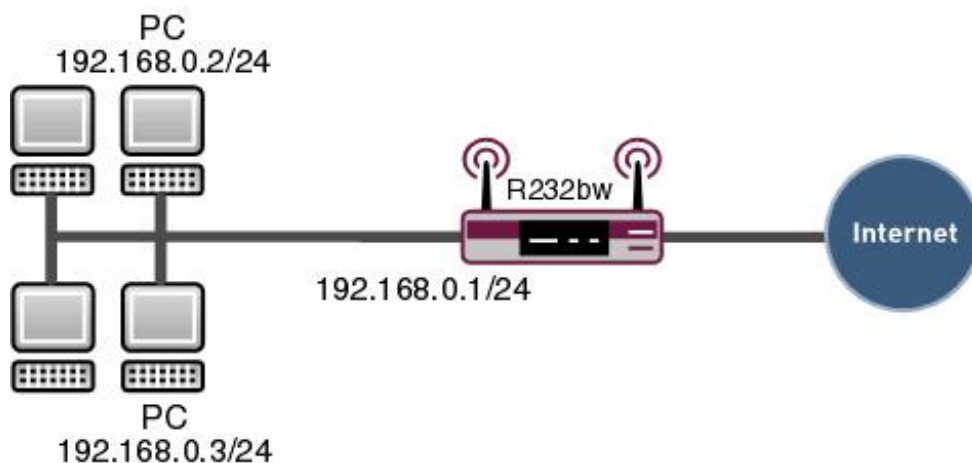


Fig. 13: Sample scenario time-controlled tasks

Requirements

The following are required for the configuration:

- Basic configuration of the gateway.
- Boot image from version 7.8.2

3.2 Configuration

Only the following menu is used for configuring time-controlled tasks:

- (1) Go to **Local Services -> Scheduling -> Time Schedule**.

3.2.1 Daily reboot

Go to the following menu to configure the gateway so that the router executes a certain action at a certain time:

- (1) Go to **Local Services -> Scheduling -> Time Schedule-> New**.

The screenshot displays the configuration interface for a Time Schedule. On the left, a navigation menu is visible with 'Local Services' expanded and 'Scheduling' selected. The main configuration area is titled 'Time Schedule' and includes an 'Options' tab. The form contains the following sections:

- Basic Parameters:** Description field containing 'Reboot'.
- Action:** Select action dropdown menu set to 'Reboot device'.
- Select time interval:** A section for defining the condition, including:
 - Condition Type:** Radio buttons for 'Weekday', 'Periods' (selected), and 'Day of Month'.
 - Condition Settings:** A sub-form with a 'Monday' dropdown, a 'Daily' dropdown, and a '1' dropdown.
- Start Time:** Fields for 'Hour' (00) and 'Minute' (00).

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

Fig. 14: **Local Services -> Scheduling-> Time Schedule-> New**

Relevant fields in the Time Schedule menu

Field	Meaning
Description	Give the entry a name.
Select action	Select the action you want the gateway to execute.
Condition Type	Select the frequency with which the action is to be executed.
Condition Settings	Select the day on which the action is to be executed.
Start Time	Specify the time at which the action is to be executed.

Proceed as follows:

- (1) Under **Description** enter *Reboot*.

- (2) Under **Select Action** select *Reboot Device*.
- (3) Select the **Condition Type** *Periods*.
- (4) In the **Condition Settings** field select *Daily*.
- (5) Enter the time under **Start Time: Hour** *00* **Minute** *00*.
- (6) Confirm with **OK**.



Note

The gateway checks the configured events only every 300 seconds. To reduce the time to every second, for example, go to the menu **Local Services -> Scheduling -> Options** and enter a **Schedule Interval**, e.g. 5. Note that checking every second may overload the gateway.

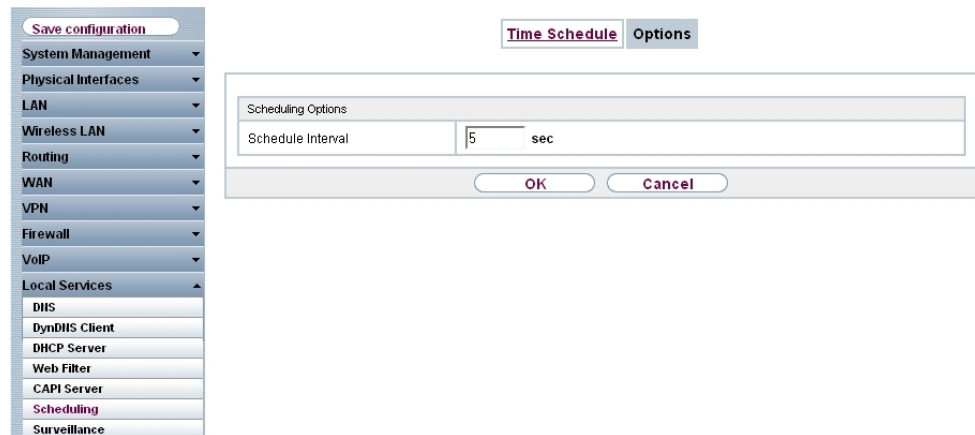


Fig. 15: **Local Services -> Scheduling-> Options**

3.2.2 Suspending the WLAN interface

Generate another entry to disable the WLAN interface on Saturday and Sunday.

Go to the following menu for this:

- (1) Go to **Local Services -> Scheduling -> Time Schedule-> New**.

Fig. 16: Local Services -> Scheduling-> Time Schedule-> New

Relevant fields in the Time Schedule menu

Field	Meaning
Description	Give the entry a name.
Select action	Select the action you want the gateway to execute.
Select interface	Select the interface you wish to enable or suspend.
Condition Type	Select the frequency with which the action is to be executed.
Condition Settings	Select the day on which the action is to be executed.
Start Time	Specify the time at which the action is to be executed.
Stop Time	Specify the time at which the action is to be terminated.

Proceed as follows:

- (1) Under **Description** enter *Wireless LAN*.
- (2) Under **Select Action** select *Deactivate WLAN*.
- (3) Under **Select Interface** choose *Funkwerk-ec (vss1-0)* for example.
- (4) Select the **Condition Type** *Periods*.
- (5) In the **Condition Settings** field, select *Saturday Sunday*.
- (6) Enter the time under **Start Time: Hour 00 Minute 00**.
- (7) Enter the time under **Stop Time** as follows: **Hour 23 Minute 59**.
- (8) Confirm with **OK**.

3.2.3 Monthly configuration backup

You want to backup your configuration on the first day of every month on a TFTP server.

Go to the following menu for this:

- (1) Go to **Local Services** -> **Scheduling** -> **Time Schedule**-> **New**.

Fig. 17: Local Services -> Scheduling-> Time Schedule-> New

Relevant fields in the Time Schedule menu

Field	Meaning
Description	Give the entry a name.
Select action	Select the action you want the gateway to execute.
TFTP Server	Enter the IP address of the TFTP server.
TFTP File Name	Enter the name of the configuration on the server.
Condition Type	Select the frequency with which the action is to be executed.
Condition Settings	Select the day on which the action is to be executed.
Start Time	Specify the time at which the action is to be executed.
Stop Time	Specify the time at which the action is to be terminated.

Proceed as follows:

- (1) Under **Description** enter *Configuration*.

- (2) Under **Select Action** select *Trigger Configuration Backup*.
- (3) Enter the IP address in the **TFTP Server** field, e.g. *192.168.0.2*.
- (4) Enter a name under **TFTP File Name**, e.g. *r232bw.cfg*.
- (5) Select the **Condition Type** *Day of Month*.
- (6) In the **Condition Settings** field select *1*.
- (7) Enter the time under **Start Time: Hour 00 Minute 00**.
- (8) Enter the time under **Stop Time: Hour 00 Minute 05**.
- (9) Confirm with **OK**.



Note

A monthly configuration backup requires an appropriately configured TFTP server.

Checking the TFTP server

The TFTP server is used to transfer files between gateway and computer, e.g. for configuration management. Make sure that the TFTP server is operating properly by opening **DIME Tools** (included in the **BRICKware**, which you can install from the bintec **Companion CD**). Start the TFTP server by pressing the key combination **CTRL + T** in **DIME Tools**.

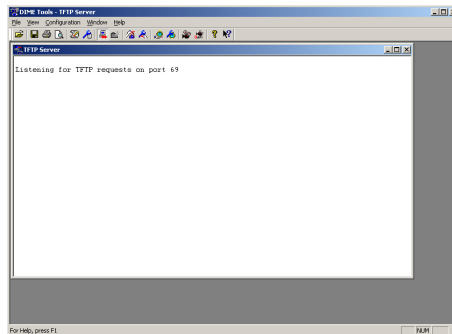


Fig. 18: DIME Tools - TFTP Server

To assign the TFTP server a directory, e.g. for saving files, you can enter your chosen path under **Configuration -> TFTP Server**.

3.3 Overview of configuration steps

Daily reboot

Field	Menu	Value
Description	Local Services -> Scheduling -> Time Schedule -> New	e.g. <i>Reboot</i>
Select action	Local Services -> Scheduling -> Time Schedule -> New	<i>Reboot device</i>
Condition Type	Local Services -> Scheduling -> Time Schedule -> New	<i>Periods</i>
Condition Settings	Local Services -> Scheduling -> Time Schedule -> New	<i>Daily</i>
Start Time	Local Services -> Scheduling-> Time Schedule-> New	Hour <i>00</i> Minute <i>00</i>
Schedule Interval	Local Services -> Scheduling-> Op-tions	5 sec

Suspending the WLAN interface

Field	Menu	Value
Description	Local Services -> Scheduling -> Time Schedule -> New	e.g. <i>Wireless LAN</i>
Select action	Local Services -> Scheduling-> Time Schedule -> New	<i>Deactivate WLAN</i>
Select interface	Local Services -> Scheduling-> Time Schedule -> New	<i>Funkwerk-ec (vss1-0)</i>
Condition Type	Local Services -> Scheduling-> Time Schedule -> New	<i>Periods</i>
Condition Settings	Local Services -> Scheduling-> Time Schedule -> New	<i>Saturday Sunday</i>
Start Time	Local Services -> Scheduling-> Time Schedule -> New	Hour <i>00</i> Minute <i>00</i>
Stop Time	Local Services -> Scheduling-> Time Schedule -> New	Hour <i>23</i> Minute <i>59</i>

Monthly configuration backup

Field	Menu	Value
Description	Local Services -> Scheduling->	e.g. <i>Configuration</i>

Field	Menu	Value
	Time Schedule -> New	
Select action	Local Services -> Scheduling-> Time Schedule -> New	<i>Trigger configuration backup</i>
TFTP Server	Local Services -> Scheduling-> Time Schedule -> New	e.g. <i>192.168.0.2</i>
TFTP File Name	Local Services -> Scheduling-> Time Schedule -> New	e.g. <i>r232bw.cfg</i>
Condition Type	Local Services -> Scheduling-> Time Schedule -> New	<i>Day of Month</i>
Condition Settings	Local Services -> Scheduling-> Time Schedule -> New	e.g. <i>1</i>
Start Time	Local Services -> Scheduling-> Time Schedule -> New	Hour <i>00</i> Minute <i>00</i>
Stop Time	Local Services -> Scheduling-> Time Schedule -> New	Hour <i>00</i> Minute <i>05</i>

Chapter 4 Services - Prioritisation of a VPN IPsec connection ahead of other Internet traffic

4.1 Introduction

A **bintec R3002** gateway is located in the head office of a company. This gateway is connected to the Internet via an Internet access with a fixed WAN IP address. The Internet access is used for the VPN IPsec connection of a company branch as well as other Internet services. If the entire bandwidth of the Internet connection is used, then the company branch should have a higher priority than the rest of the traffic and therefore continue to be usable.

In this workshop a **bintec R3002** (head office gateway) and a **bintec RS120** (branch gateway) shall be shown as examples for setting up the Internet connection and configuring the VPN IPsec connection. Then the prioritisation of the VPN IPsec connection is set for the company head office gateway.

The **GUI** (Graphical User Interface) is used for configuration.

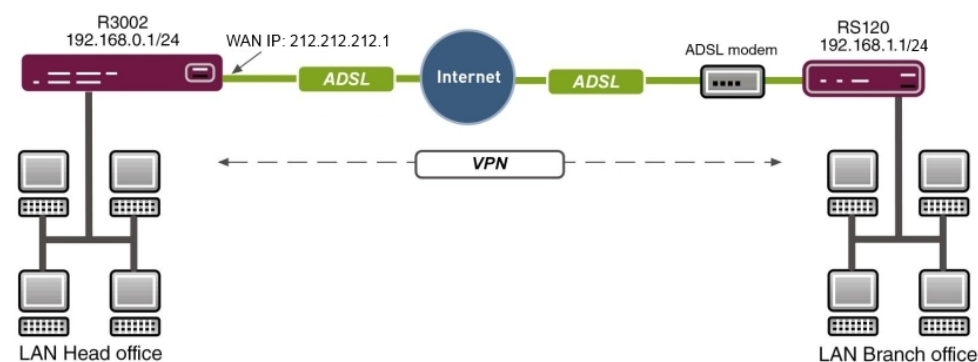


Fig. 19: Example scenario

Requirements

- A **bintec R3002** gateway (head office)
- A **bintec RS120** gateway (branch)
- A boot image of version 7.9.5 or later
- Both gateways require an independent connection to the Internet

- Head office Internet access with static WAN IP address
- **Dime Manager** software

4.2 Configuration

4.2.1 Configuration of gateway in head office (bintec R3002)

For the initial configuration the **bintec R3002** gateway can be reached via the **Dime Manager**. The LAN IP address of the gateway is changed via the shortcut menu. After you have changed the IP address, the web interface of the **bintec R3002** can be reached.

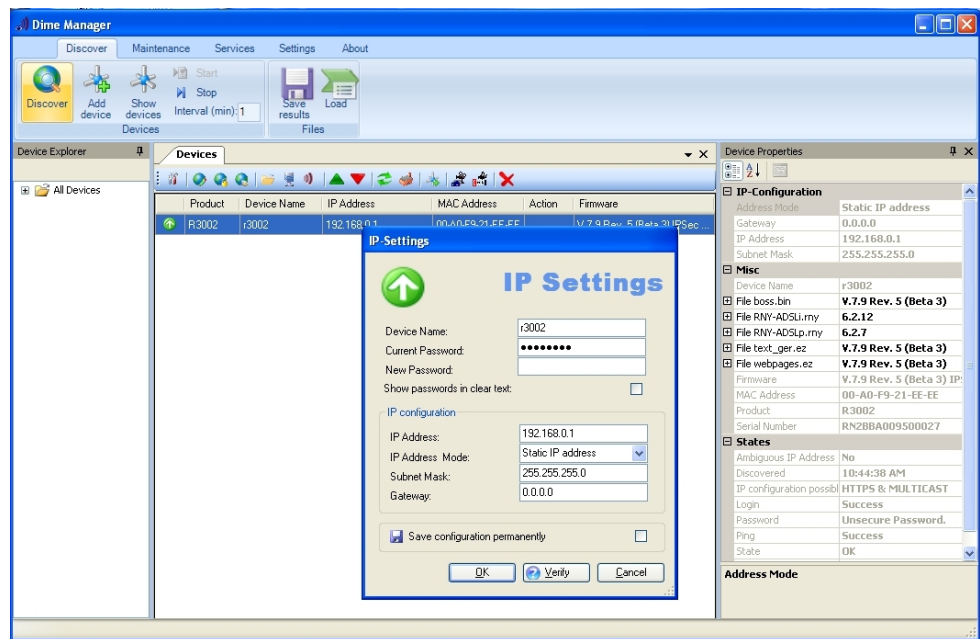


Fig. 20: Dime Manager

4.2.2 Configuration of Internet access via the GUI Assistant

Configuration of an Internet access has to be done **GUI** via an Assistant.

The gateway Internet connection can be set up in a few steps via the Assistant. For this, go to the following menu:

- (1) Go to **Assistants** -> **Internet Access**-> **Internet Connections** -> **New**.
- (2) Select the **Connector Type** e.g. *Internal ASDL Modem*.

- (3) Click on **Next** to configure a new Internet connection.

Enter the required data for the connection.

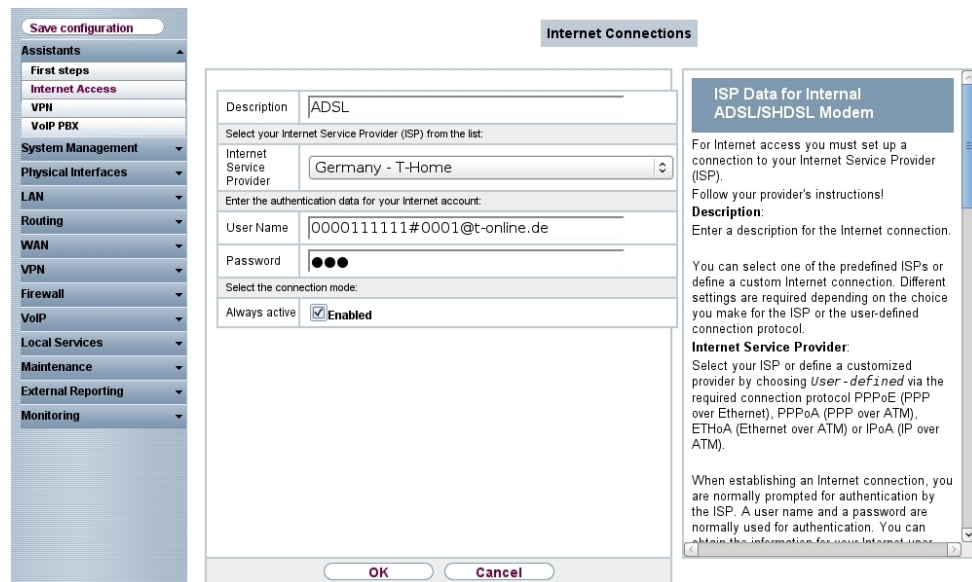


Fig. 21: Assistants -> Internet Access -> Internet Connections -> Next

Proceed as follows to configure a new Internet connection:

- (1) Under **Description** enter e.g. *ADSL* .
- (2) For the **Internet Service Provider** select e.g. *Germany-T-Home* .
- (3) Under **User Name** enter the access data you received from your provider.
- (4) Enter the **Password** you received from your provider.
- (5) So that the static WAN IP address of the head office VPN gateway can always be reached by the branch gateway, the option **Always active** must be set.
- (6) Press **OK** to confirm your entries.

4.2.3 Configuration of the VPN IPSec access of the first branch via the GUI Assistant

The VPN IPSec setup can also be configured with the Assistant in the same manner as when setting up the Internet access. For this, go to the following menu:

- (1) Go to **Assistants -> VPN -> VPN Connections -> New**.
- (2) For **VPN Scenario** select the *IPSec-LAN-LAN Connection* .
- (3) Click on **Next** to set up a new VPN connection.

Enter the required data for the connection.

The screenshot shows the 'VPN Connections' configuration window. The left sidebar has a menu with 'VPN' selected. The main window is titled 'VPN Connections' and contains a form for configuring an 'IPSec LAN-to-LAN Connection'. The form fields are as follows:

- Selected scenario: LAN-to-LAN Connection
- IPSec Scenario: LAN-to-LAN Connection
- Connection Details
- Description: filiale1
- Local IPSec ID: 212.212.212.1
- Remote IPSec ID: filiale1
- Preshared Key: [masked]
- Local IP Address: 192.168.0.1
- Define this connection as default route: Enabled
- Enter IP settings: Enabled
- IPSec Peer Address: [empty]
- IP Address of Remote Network: 192.168.1.0
- Subnet Mask: 255.255.255.0

A help window titled 'IPSec LAN-to-LAN Connection' is open on the right, providing instructions for entering data and defining the connection.

Fig. 22: Assistants -> VPN -> VPN Connections -> Next

Proceed as follows to configure a new VPN connection:

- (1) Under **Description** enter e.g. *subsidiary1*.
- (2) Under **Local IPSec ID** enter the static WAN IP address of the head office gateway, e.g. *212.212.212.1*.
- (3) Under **Remote IPSec ID** enter the local IPSec ID of the branch gateway, e.g. *filiale1*.
- (4) For the authentication enter **Preshared Key**, e.g. *supersecretgeheimkey*.
- (5) Under **Local IP Address** enter the IP address of the **bintec R3002**, e.g. *192.168.0.1*.
- (6) The VPN tunnel is always set up from the branch to the head office. As a result no **IPSec Peer Address** is set on the **bintec R3002**.
- (7) Under **IP Address of Remote Network** enter the network address of the branch, e.g. *192.168.1.0* and the **Netmask** *255.255.255.0*.
- (8) Press **OK** to confirm your entries.

After confirming the entry the VPN connection can be seen in the list.

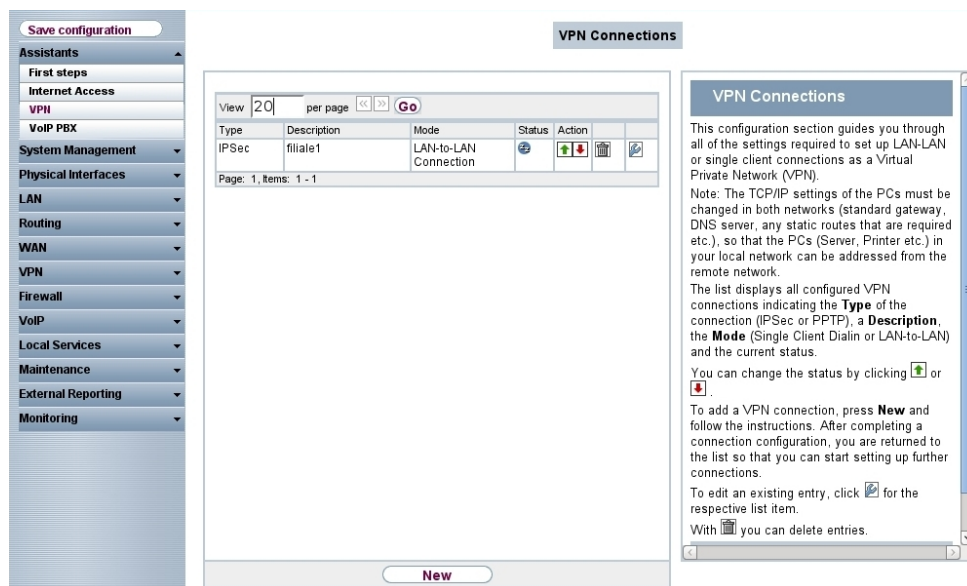


Fig. 23: Assistant-> VPN -> VPN Connections

To connect additional locations or VPN remote terminals, the Assistant can be run again.

4.2.4 Configuration of gateway in head office (bintec RS120)

The IP configuration of the branch gateway (**bintec RS120**) can be carried out again with the **Dime Manager**. The **bintec RS120** is located in the network with the aid of the **Dime Manager**. Then the LAN IP address can be set via the shortcut menu. After you have changed the IP address, the web interface **GUI** of the **bintec RS120** can be reached.

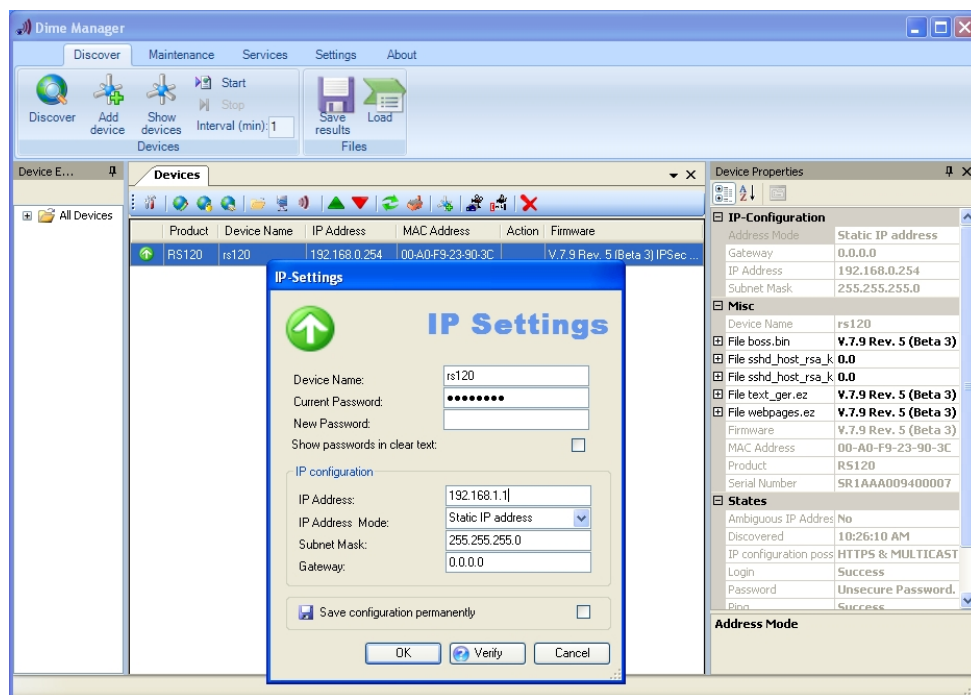


Fig. 24: Dime Manager

4.2.5 Configuration of Internet access via the GUI Assistant

The **GUI Assistant** makes it easy to configure the Internet access for the **bintec RS120** as well. For the **bintec RS120** the Internet access is done via an ADSL modem. For this, go to the following menu:

- (1) Go to **Assistants -> Internet Access-> Internet Connections -> New**.
- (2) Under **Connector Type** select e.g. *External xDSL Modem*.
- (3) Click on **Next** to configure a new Internet connection.

Enter the required data for the connection.

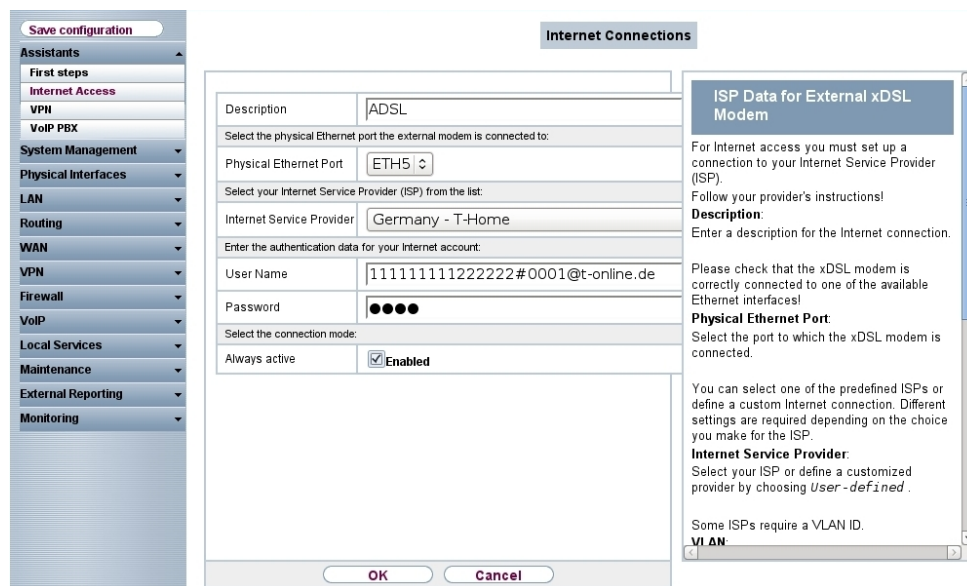


Fig. 25: Assistants -> Internet Access -> Internet Connections -> Next

Proceed as follows to configure a new Internet connection:

- (1) Under **Description** enter e.g. *ADSL* .
- (2) Under **Physical Ethernet Port** select *ETH5* .
- (3) For the **Internet Service Provider** select e.g. *Germany-T-Home* .
- (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.

4.2.6 Configuration of the VPN IPsec tunnel on the branch gateway

The **GUI Assistant** makes the VPN configuration on the branch gateway easier as well. For this, go to the following menu:

- (1) Go to **Assistants -> VPN -> VPN Connections -> New**.
- (2) For **VPN Scenario** select the *IPsec-LAN-LAN Connection* .
- (3) Click on **Next** to set up a new VPN connection.

Enter the required data for the connection.

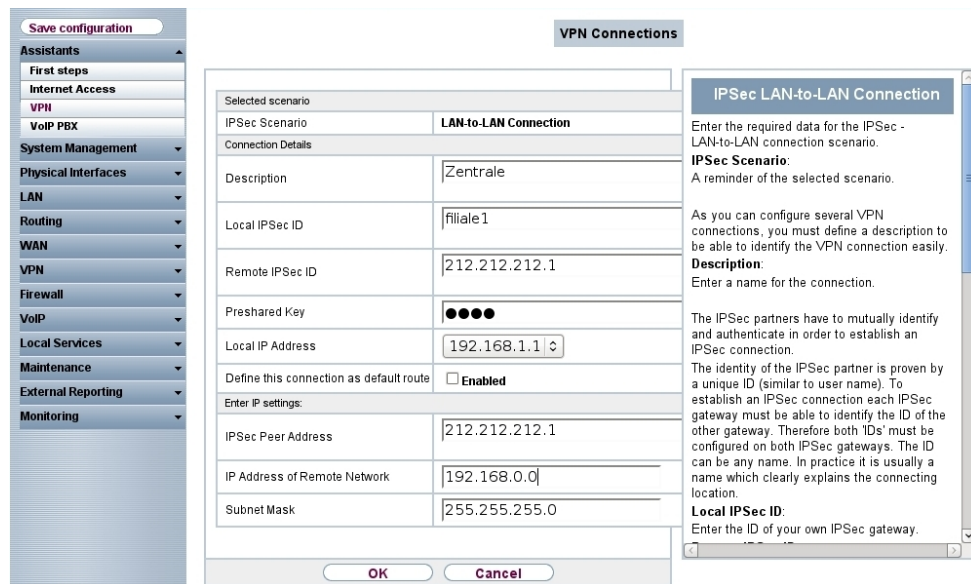


Fig. 26: Assistants -> VPN -> VPN Connections -> Next

Proceed as follows to configure a new VPN connection:

- (1) Under **Description** enter e.g. *Head Office*.
- (2) The **Local IPsec ID** enter the ID of you branch gateway appropriately to the **Remote IPsec ID** of the head office gateway, e.g. *branch1*.
- (3) Under **Remote IPsec ID** enter the local IPsec ID of the remote gateway, e.g. *212.212.212.1*.
- (4) For the authentication enter **Preshared Key**, e.g. *supersecretgeheimkey*.
- (5) Under **Local IP Address** enter the IP address of the **bintec RS120**, e.g. *192.168.1.1*.
- (6) For the **IPsec Peer Address** the WAN IP address of the **bintec R3002** must be provided, e.g. *212.212.212.1*.
- (7) Under **IP Address of Remote Network** enter the network address of the branch, e.g. *192.168.1.0* and the **Netmask** *255.255.255.0*.
- (8) Press **OK** to confirm your entries.

Due to the dynamic IP address of the **bintec RS120** the VPN IPsec tunnel can only be set up in one direction (i.e. branch -> head office). The tunnel must always be active so that the connection of both locations can be used. For this, go to the following menu:

- (1) Go to **VPN -> IPsec -> IPsec Peers** ->  -> **Advanced Settings**.

The screenshot shows a web-based configuration interface for VPN IPSec peers. On the left is a navigation menu with categories like Assistants, System Management, Physical Interfaces, LAN, Routing, WAN, VPN, IPsec, L2TP, PPTP, GRE, Firewall, VoIP, Local Services, Maintenance, External Reporting, and Monitoring. The main area has tabs for 'IPSec Peers', 'Phase-1 Profiles', 'Phase-2 Profiles', 'XAUTH Profiles', 'IP Pools', and 'Options'. The 'IPSec Peers' tab is active, showing a form for configuring a peer named 'Zentrale'. The form is divided into 'Peer Parameters', 'Interface Routes', and 'Advanced Settings'.

Peer Parameters

Administrative Status	<input checked="" type="radio"/> Up <input type="radio"/> Down
Description	Zentrale
Peer Address	212.212.212.1
Peer ID	IPv4 Address 212.212.212.1
Preshared Key	●●●●●●●●

Interface Routes

IP Address Assignment	Static						
Default Route	<input type="checkbox"/> Enabled						
Local IP Address	192.168.1.1						
Route Entries	<table border="1"><thead><tr><th>Remote IP Address</th><th>Netmask</th><th>Metric</th></tr></thead><tbody><tr><td>192.168.0.0</td><td>255.255.255.0</td><td>1</td></tr></tbody></table> <input type="button" value="Add"/>	Remote IP Address	Netmask	Metric	192.168.0.0	255.255.255.0	1
Remote IP Address	Netmask	Metric					
192.168.0.0	255.255.255.0	1					

Advanced Settings

Advanced IPSec Options

Phase-1 Profile	wz_ike_1
Phase-2 Profile	* Multi-Proposal
XAUTH Profile	Select one
Number of Admitted Connections	<input checked="" type="radio"/> One User <input type="radio"/> Multiple Users
Start Mode	<input type="radio"/> On Demand <input checked="" type="radio"/> Always up

Advanced IP Options

Back Route Verify	<input type="checkbox"/> Enabled
Proxy ARP	<input checked="" type="radio"/> Inactive <input type="radio"/> Up or Dormant <input type="radio"/> Up only

Fig. 27: VPN -> IPSec -> IPSec Peers ->  -> Advanced Settings

Proceed as follows to configure the VPN IPSec tunnel:

- (1) Set **Start Mode** to *Always active*.
- (2) Leave all other settings unchanged and confirm your entries with **OK**.

4.3 Testing the VPN connection

At the current configuration stage, the Internet access is set up on both gateways and the VPN tunnel to the location coupling can already be used. The VPN tunnel can be tested with the ping test between both gateways.

4.4 Prioritisation of the VPN tunnel on the branch gateway ahead of other Internet traffic

The **bintec R3002** Internet access (head office) is also used for other Internet services alongside the VPN tunnel. The site networking should have a higher priority than other Internet traffic. As a result the required protocols for the VPN connection (IKE, ESP, NAT Traversal) are prioritised. QoS (Quality of Service) is configured here.

4.4.1 Creation of QoS filters

At the start of the QoS configuration, filters are defined that will identify traffic that needs to be prioritised. QoS filters must be created for the prioritisation of VPN IPsec connections. For this, go to the following menu:

- (1) Go to **Routing -> QoS -> QoS Filter -> New**.

Basic Parameters	
Description	IKE
Protocol	udp
Destination IP Address/Netmask	0.0.0.0 0.0.0.0
Destination Port/Range	Specify port 500 to -1
Source IP Address/Netmask	0.0.0.0 0.0.0.0
Source Port/Range	Specify port 500 to -1
DSCP/TOS filter (Layer 3)	Ignore
COS filter (802.1p/Layer 2)	0

Fig. 28: Routing -> QoS -> QoS Filter ->New

Proceed as follows in order to configure QoS filters:

- (1) For **Description** enter the description of the filter, e.g. *IKE*.
- (2) Select the **Protocol** *udp*.
- (3) For **Destination Port/Range** select *Specify port* and enter the destination port number, e.g. *500*.
- (4) Under **Source Port/Range** select *Specify port* and enter the source port number, e.g. *500*.
- (5) Leave you **DSCP/TOS filter (Leyer 3)** to *Ignore*.
- (6) Press **OK** to confirm your entries.

Following that, create additional QoS filters for the ESP and NAT Traversal protocols by using the following tables.

Description	Protocol	Destination port/ range	Source port/range
IKE	udp	500	500
ESP	esp	-	-
NAT-T_1	udp	4500	-
NAT-T_2	udp	-	4500

The complete configuration looks like this:

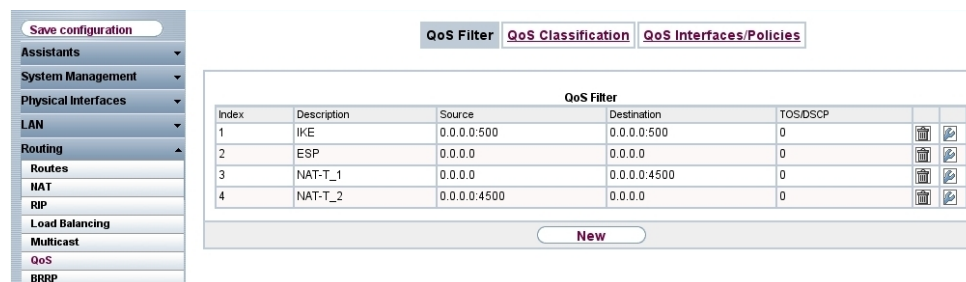


Fig. 29: Routing -> QoS -> QoS Filter

4.4.2 Assignment of QoS filter to QoS class or high priority class

In the next configuration step the created filters are assigned to the high priority class. For this, go to the following menu:

- (1) Go to **Routing -> QoS -> QoS Classification -> New**.

The screenshot shows the 'QoS Classification' configuration window. The 'Basic Parameters' section is filled with the following values:

Class map	New
Description	VPN-IPSec
Filter	IKE
Direction	Outgoing
High Priority Class	<input checked="" type="checkbox"/>
Interfaces	ADSL

Fig. 30: Routing -> QoS -> QoS Classification -> New

Proceed as follows in order to create a new class map:

- (1) For **Description** enter a description for the class map, e.g. *VPN-IPSec*.
- (2) Select **Filter** from what you have configured in the **Routing -> QoS -> QoS Filter** menu, e.g. *IKE*.
- (3) Under **Direction** select *Outgoing*.
- (4) Enable the **High Priority Class**. The data packets are then allocated to the class with the highest priority.
- (5) Select the **Interface** via which the prioritised data is to be sent, e.g. *ADSL*.
- (6) Confirm with **OK**.

For each **QoS Filter** the QoS class assignment (**High Priority Class**) must be done separately. When assigning the remaining QoS filters (ESP, NAT-T_1 and NAT-T_2) the class map is set to the newly created VPN-IPSec entry. For this, go to the following menu:

- (1) Go to **Routing -> QoS -> QoS Classification -> New**.

The screenshot shows the 'QoS Classification' configuration window. The 'Basic Parameters' section is filled with the following values:

Class map	VPN-IPSec
Filter	ESP
Direction	Outgoing
High Priority Class	<input checked="" type="checkbox"/>

Fig. 31: Routing -> QoS -> QoS Classification -> New

Proceed as follows to assign additional QoS filter to the class map:

- (1) Select the **Class map** (e.g. *VPN-IPSec*) which the QoS filter should be assigned.
- (2) Select the next **Filter** , e.g. *ESP*.
- (3) For **Direction** select *Outgoing*.
- (4) Enable the **High Priority Class**.
- (5) Press **OK** to confirm your entries.

Assign all generated QoS filters to the new class map *VPN-IPSec* .

Results:

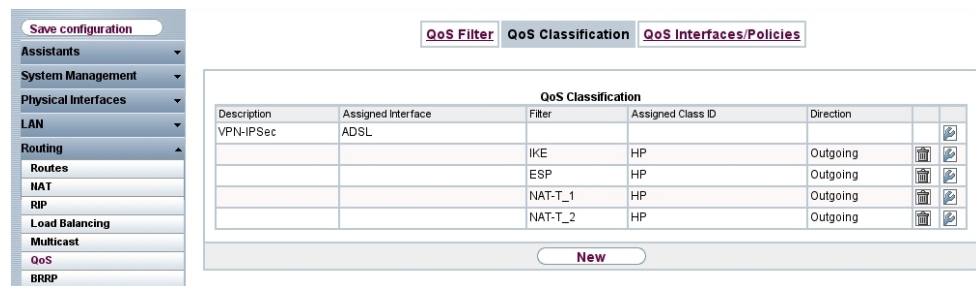


Fig. 32: Routing -> QoS -> QoS Classification

4.4.3 Enabling QoS on the WAN interface

In the last QoS configuration step, prioritisation is enabled on the WAN interface. For this, go to the following menu:

- (1) Go to **Routing -> QoS -> QoS Interfaces/Policies -> New**.

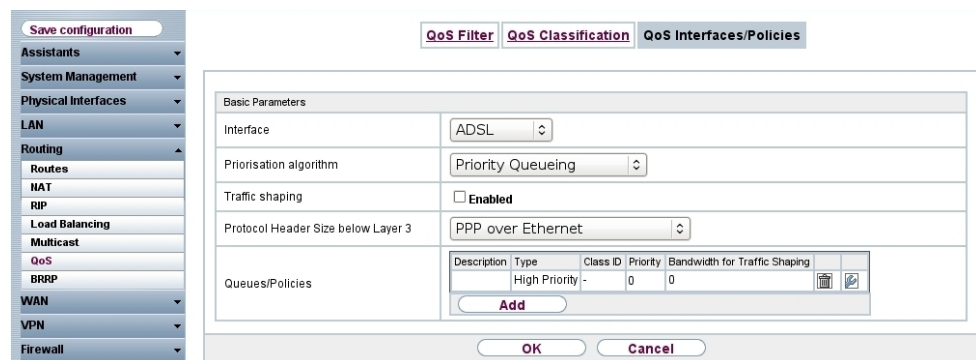


Fig. 33: Routing -> QoS -> QoS Interfaces/Policies -> New

Proceed as follows to enable prioritisation on the WAN interface:

- (1) Select the **Interface** for which the QoS is to be configured, the example here being *ADSL*.
- (2) For **Prioritisation algorithm** select *Priority Queueing*.
- (3) Under the option **Protocol Header Size below Layer 3** select *PPP over Ethernet*.
- (4) The QoS queues that are used (high priority and default) are automatically created.
- (5) Press **OK** to confirm your entries.

4.4.4 QoS Monitoring

For high priority traffic and non-prioritised traffic, queues are created for each prioritisation. The status of these queues are displayed in the **Monitoring -> QoS** menu. As soon as the bandwidth of the Internet connection for scheduled VPN data and other Internet data becomes insufficient, the non-prioritised data is deferred and preference is given to VPN data.

- (1) Go to **Monitoring -> QoS**.

QoS				
Interface	QoS Queue	Send	Dropped	Queued
ADSL	High Priority	12344	0	0
	unprioritized	12611	11506	19

Fig. 34: Monitoring -> QoS

This concludes the configuration. In order to save the configuration in a bootable manner, leave **GUI** via **Save configuration** and confirm your selection with **OK**.

4.5 Overview of Configuration Steps

Configuration of gateway in head office (bintec R3002)

Field	Menu	Value
IP address	Dime Manager -> IP Settings	e.g. <i>192.168.0.1</i>

Configuration of Internet access (head office)

Field	Menu	Value
Connector Type	Assistant -> Internet Access -> New	<i>Internal ADSL Mo-dem</i>
Description	Assistant -> Internet Access -> Next	<i>ADSL</i>
Internet Service Pro-vider	Assistant -> Internet Access -> Next	<i>e.g. Germany - T-Home</i>
User Name	Assistant -> Internet Access -> Next	<i>e.g. 0000111111#0001@t-online.de</i>
Password	Assistant -> Internet Access -> Next	<i>e.g. supersecretge-heimkey</i>
Always Active	Assistant -> Internet Access -> Next	<i>Enabled</i>

Configuration of VPN IPsec access (head office)

Field	Menu	Value
Connector Type	Assistant -> VPN -> New	<i>IPsec - LAN-to-LAN connection</i>
Description	Assistant -> VPN -> Next	<i>branch1</i>
Local IPsec ID	Assistant -> VPN -> Next	<i>e.g. 212.212.212.1</i>
Remote IPsec ID	Assistant -> VPN -> Next	<i>e.g. branch1</i>
Preshared Key	Assistant -> VPN -> Next	<i>e.g. supersecretge-heimkey</i>
Local IP Address	Assistant -> VPN -> Next	<i>192.168.0.1</i>
IP Address of Re-mote Network	Assistant -> VPN -> Next	<i>192.168.1.0</i>
Netmask	Assistant -> VPN -> Next	<i>255.255.255.0</i>

Configuration of gateway in branch (bintec RS120)

Field	Menu	Value
IP address	Dime Manager -> IP Settings	<i>e.g. 192.168.1.1</i>

Configuration of Internet access (branch)


Field	Menu	Value
Connector Type	Assistant -> Internet Access -> New	<i>External xDSL Mo-dem</i>
Description	Assistant -> Internet Access -> Next	<i>ADSL</i>

Field	Menu	Value
Physical Ethernet Port	Assistant -> Internet Access -> Next	e.g. <i>ETH5</i>
Internet Service Provider	Assistant -> Internet Access -> Next	e.g. <i>Germany - T-Home</i>
User Name	Assistant -> Internet Access -> Next	e.g. <i>111111111222222#0001@t-online.de</i>
Password	Assistant -> Internet Access -> Next	e.g. <i>supersecretgeheimkey</i>
Always Active	Assistant -> Internet Access -> Next	<i>Enabled</i>

Configuration of VPN IPsec access (branch)

Field	Menu	Value
Connector Type	Assistant -> VPN -> New	<i>IPsec - LAN-to-LAN connection</i>
Description	Assistant -> VPN -> Next	<i>Head Office</i>
Local IPsec ID	Assistant -> VPN -> Next	e.g. <i>branch1</i>
Remote IPsec ID	Assistant -> VPN -> Next	e.g. <i>212.212.212.1</i>
Preshared Key	Assistant -> VPN -> Next	e.g. <i>supersecretgeheimkey</i>
Local IP Address	Assistant -> VPN -> Next	<i>192.168.1.1</i>
IPsec Peer Address	Assistant -> VPN -> Next	<i>212.212.212.1</i>
IP Address of Remote Network	Assistant -> VPN -> Next	<i>192.168.0.0</i>
Netmask	Assistant -> VPN -> Next	<i>255.255.255.0</i>

Prioritisation of VPN tunnel

Field	Menu	Value
Start mode	VPN -> IPsec -> IPsec Peers ->  -> Advanced Settings	<i>Always Active</i>

Creation of QoS filters

Field	Menu	Value
Description	Routing -> QoS -> QoS Filter -> New	<i>IKE</i>
Protocol	Routing -> QoS -> QoS Filter -> New	<i>udp</i>
Destination port/range	Routing -> QoS -> QoS Filter -> New	<i>500</i>

Field	Menu	Value
Source Port/Range	Routing -> QoS -> QoS Filter -> New	500
DSCP/TOS	Routing -> QoS -> QoS Filter -> New	Ignore
Description	Routing -> QoS -> QoS Filter -> New	ESP
Protocol	Routing -> QoS -> QoS Filter -> New	esp
Description	Routing -> QoS -> QoS Filter -> New	NAT-T_1
Protocol	Routing -> QoS -> QoS Filter -> New	udp
Destination port/ range	Routing -> QoS -> QoS Filter -> New	4500
Description	Routing -> QoS -> QoS Filter -> New	NAT-T_2
Protocol	Routing -> QoS -> QoS Filter -> New	udp
Source Port/Range	Routing -> QoS -> QoS Filter -> New	4500

Assignment of QoS filters to QoS classes

Field	Menu	Value
Description	Routing -> QoS -> QoS Classification -> New	VPN-IPSec
Filter	Routing -> QoS -> QoS Classification -> New	e.g. IKE
Direction	Routing -> QoS -> QoS Classification -> New	Outgoing
High priority class	Routing -> QoS -> QoS Classification -> New	Enabled
Interface	Routing -> QoS -> QoS Classification -> New	ADSL
Class plan	Routing -> QoS -> QoS Classification -> New	VPN-IPSec
Filter	Routing -> QoS -> QoS Classification -> New	e.g. ESP
Direction	Routing -> QoS -> QoS Classification -> New	Outgoing
High priority class	Routing -> QoS -> QoS Classification -> New	Enabled
Class plan	Routing -> QoS -> QoS Classification -> New	VPN-IPSec
Filter	Routing -> QoS -> QoS Classification -> New	e.g. NAT-T_1

Field	Menu	Value
Direction	Routing -> QoS -> QoS Classification -> New	<i>Outgoing</i>
High priority class	Routing -> QoS -> QoS Classification -> New	<i>Enabled</i>
Class plan	Routing -> QoS -> QoS Classification -> New	<i>VPN-IPSec</i>
Filter	Routing -> QoS -> QoS Classification -> New	e.g. <i>NAT-T_2</i>
Direction	Routing -> QoS -> QoS Classification -> New	<i>Outgoing</i>
High priority class	Routing -> QoS -> QoS Classification -> New	<i>Enabled</i>

Enabling QoS on the WAN interface

Field	Menu	Value
Interface	Routing -> QoS -> QoS Interfaces/ Policies -> New	<i>ADSL</i>
Priority algorithm	Routing -> QoS -> QoS Interfaces/ Policies -> New	<i>Priority Queueing</i>
Size of the protocol header below layer 3	Routing -> QoS -> QoS Interfaces/ Policies -> New	<i>PPP over Ethernet</i>

Chapter 5 Services - Automatic Router Backup (Redundancy) with BRRP for an Internet / VPN gateway

5.1 Introduction

In this workshop the configuration of BRRP (Bintec Router Redundancy Protocol) using two **bintec RT1202** is described. Two Ethernet interfaces (a LAN and WAN interface respectively) are used on both gateways. If the master gateway or the connection to the backup gateway fails, e.g. due to a hardware fault, the backup gateway takes over the functionality of the master gateway. The backup gateway remains in hot standby mode as long as the master gateway is active. How the gateways behave in the event of a failure can be defined with a configurable set of rules.

If BRRP is used, virtual IP and MAC addresses must be configured so that these IP and MAC addresses can be passed to the backup gateway if a failure occurs. The first step is to define the physical Ethernet interfaces, the BRRP advertisement interfaces and the IP address via which the master and backup gateways can communicate with each other. The gateways are configured via this interface/IP address. Then a virtual interface and virtual route is created for the LAN and WAN sides. This virtual interface and its IP address are both used for traffic.

The **GUI** (Graphical User Interface) is used for configuration.

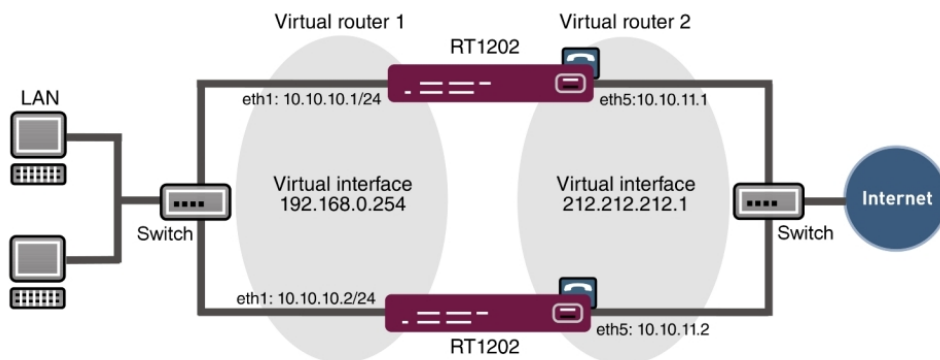


Fig. 35: Example scenario

Requirements

- Two bintec gateways with BRRP functionality (e.g. **bintec RT1202**).
- An Internet access that is made via Ethernet and a border router/gateway
- A switch to connect the Ethernet interface Eth1 (to both gateways) with the local network
- A switch to connect the Ethernet interface Eth5 (to both gateways) with the border router/gateway of the ISP

5.2 Configuration

5.2.1 Configuration of the Advertisement and Management IP address

After both networks have been connected with the local network via a switch, they can be located by using the **Dime Manager** . In this state, both gateways use the default IP address 192.168.0.254.

- (1) Go to **Dime Manager** -> **IP Settings**.

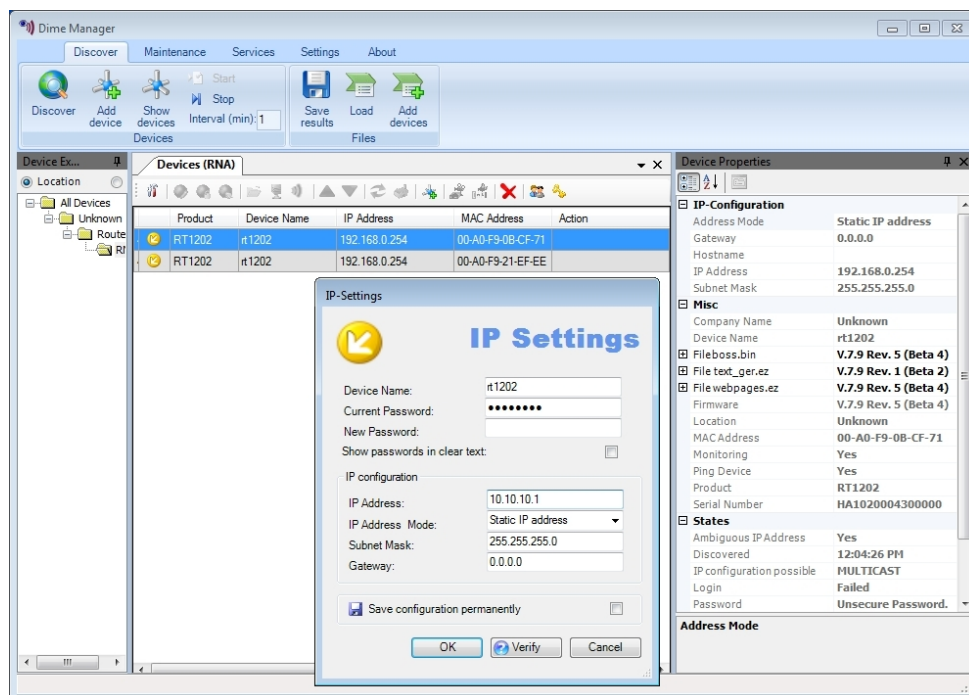


Fig. 36: Dime Manager -> IP Settings

The Advertisement and Management IP address of both gateways can be changed via the shortcut menu of the **Dime Manager**. In this workshop the address 10.10.10.1/24 shall be assigned to one network and the address 10.10.10.2/24 shall be assigned to the other network. Following successful configuration, these interfaces are used for the configuration access and for the exchange of BRRP status messages.

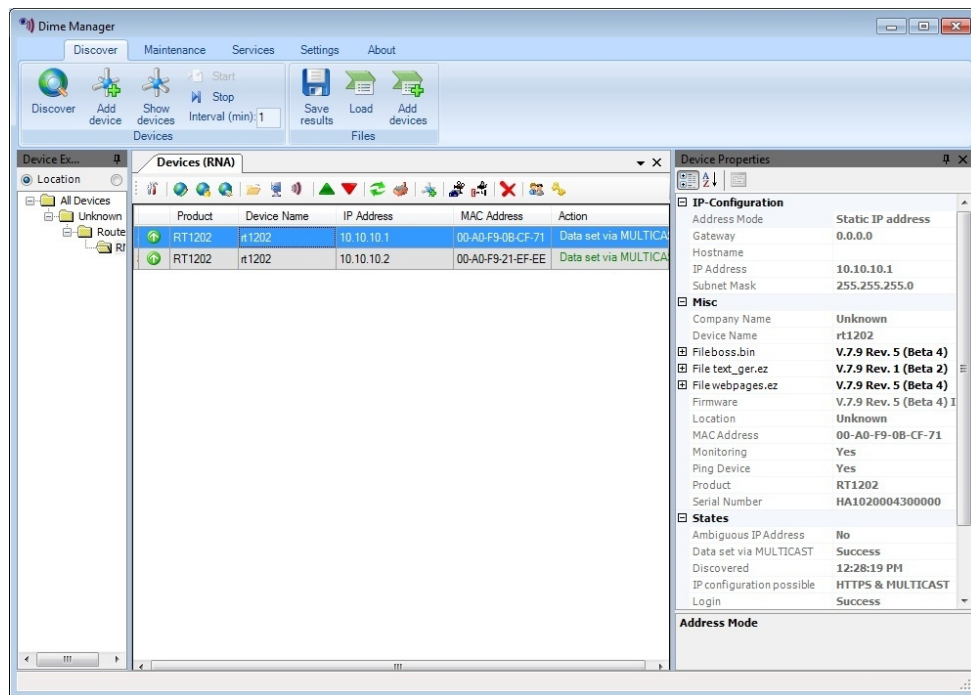


Fig. 37: Dime Manager

Then both gateways can be reached via **GUI** and the Advertisement IP addresses of the WAN interface Eth5 can be set.

In the next step the WAN Advertisement IP address is assigned to the gateway along with the netmask.

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

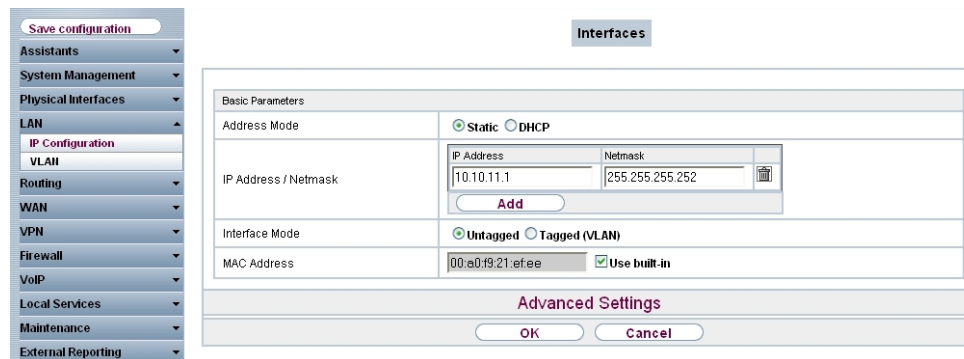


Fig. 38: **LAN -> IP Configuration -> Interfaces** ->

Proceed as follows in order to configure the ETH5 interface of the first gateway.

- (1) Under **IP Address/Netmask** enter the WAN Advertisement IP address `10.10.11.1` along with the netmask `255.255.255.252`.
- (2) Press **OK** to confirm your entries.

At the same time the address `10.10.11.2` along with the netmask `255.255.255.252` is configured on the ETH5 port of the second gateway.

Results:

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

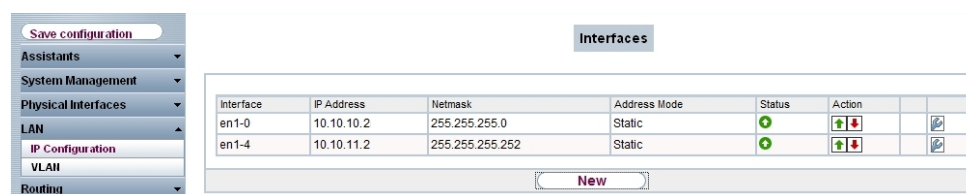


Fig. 39: **LAN -> IP Configuration -> Interfaces ->**

Both gateways exchange status messages via this interface whereby the BRRP status (master/slave) is set.

5.2.2 Configuration of the virtual router

For access to the local network (LAN) as well as for access to the Internet (WAN) a respective virtual router is created. In order to create the virtual router of the master gateway, go to the following menu:

- (1) Go to **Routing -> BRRP -> Virtual Router -> New**.

Save configuration

Virtual Routers VR Synchronisation Options

BRRP Advertisement Interface

Ethernet Interface en1-0

IP Address IP Address Netmask
10.10.10.1 255.255.255.0

BRRP Monitored Interface

Virtual Router Interface New Virtual Interface based on en1-0

Virtual Router IP Address IP Address Netmask
192.168.0.254 255.255.255.0

Virtual Router ID 1

Virtual Router Priority 254

Advanced Settings

OK Cancel

Fig. 40: Routing -> BRRP -> Virtual Router -> New

Proceed as follows for access to the local network (LAN):

- (1) Under **Ethernet Interface** select `en1-0` so that its IP address is created.
- (2) For **Router IP Address** enter the IP address and the netmask that you wish to use in the local network as the actual gateway IP address, e.g. `192.168.0.254` and `255.255.255.0`.
- (3) Under **Virtual Router ID** select the ID of the first virtual route, e.g. `1`. This ID identifies the **virtual router** in the LAN and is part of every BRRP advertisement packet that is sent by the current master.
- (4) Under **Virtual Router Priority** set the priority of the gateway that will take over the master role to `254`.
- (5) Press **OK** to confirm your entries.

To configure the virtual router to the Internet (WAN) go to the following menu:

- (1) Go to **Routing -> BRRP -> Virtual Router -> New**.

The screenshot shows the configuration page for a BRRP Monitored Interface. The interface is named 'en1-0-1'. The IP address is 212.212.212.1 and the netmask is 255.255.255.248. The virtual router ID is 2 and the priority is 254. The 'Advanced Settings' section is visible at the bottom with 'OK' and 'Cancel' buttons.

Fig. 41: Routing -> BRRP -> Virtual Router -> New

Proceed as follows for access to the Internet (WAN):

- (1) Under **Router IP Address** enter the IP address and netmask, e.g. *212.212.212.1* and *255.255.255.248*.
- (2) Select the **Virtual Router ID** , e.g. *2*.
- (3) Under **Virtual Router Priority** select *254* . By selecting priority 254, this gateway shall take over the master role following the successful configuration.
- (4) Press **OK** to confirm your entries.

The configuration steps used to create the virtual router of the backup gateway are identical to those used for the configuration of the master gateway, with the exception of **Virtual Router Priority** . On the second **bintec RT1202** (backup gateway), the value *100* is configured on both virtual routers.

5.2.3 Enabling of BRRP configuration

After creating the virtual routers on both **bintec RT1202** gateways, the BRRP function is then enabled. For this, go to the following menu:

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

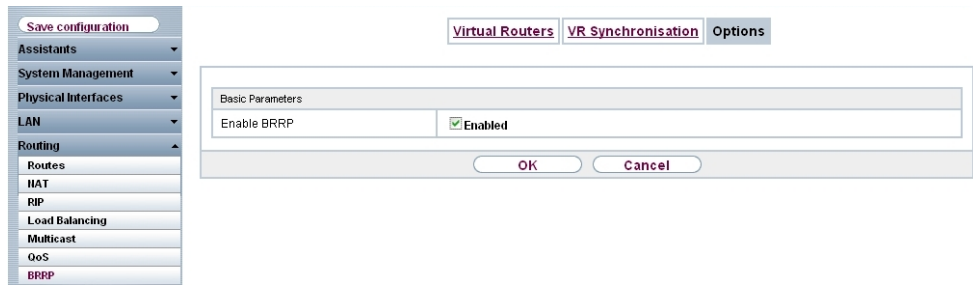


Fig. 42: Routing -> BRRP -> Options

Proceed as follows:

- (1) Enable the **Enable BRRP** function.
- (2) Confirm with **OK**.

The gateway with the higher priority is now in master status, and the gateway with the lower priority is now in backup status. You will see the configuration of the master gateway in the following menu:

- (1) Go to **Routing -> BRRP -> Virtual Routers**.

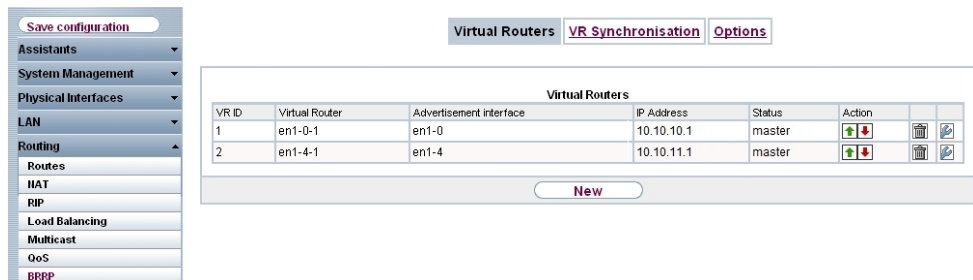


Fig. 43: Routing -> BRRP -> Virtual Routers

The following messages can be seen in the syslog:

```

19:47:54 NOTICE/BRRP: started PID 67 (compiled Aug 16 2010 17:21:34) ...
19:47:54 INFO/BRRP: create_vr(vr # 1/slot 0)
19:47:54 NOTICE/BRRP: vr # 1 - now in init state
19:47:54 INFO/BRRP: create_vr(vr # 2/slot 1)
19:47:54 NOTICE/BRRP: vr # 2 - now in init state
19:47:54 INFO/BRRP: Config VR_ID 1: Prio 254 Pre-empt mode 'true'
19:47:54 INFO/BRRP: Advertisements: ifc 1000 IP 10.10.10.1 master_down 10007
19:47:54 INFO/BRRP: Virtual Router: ifc 1004 - 1 IP address(es) assigned
19:47:54 INFO/BRRP: IP_O: 192.168.0.0
19:47:54 NOTICE/BRRP: vr # 1 - started on en1-0-1 ip 192.168.0.0 mac 00005e000101
19:47:54 NOTICE/BRRP: vr # 1 - now in backup state
19:47:54 INFO/BRRP: Config VR_ID 2: Prio 254 Pre-empt mode 'true'
19:47:54 INFO/BRRP: Advertisements: ifc 1400 IP 10.10.11.1 master_down 10007
19:47:54 INFO/BRRP: Virtual Router: ifc 1404 - 1 IP address(es) assigned
19:47:54 INFO/BRRP: IP_O: 212.212.212.0
19:47:54 NOTICE/BRRP: vr # 2 - started on en1-4-1 ip 212.212.212.0 mac 00005e000102
19:47:54 NOTICE/BRRP: vr # 2 - now in backup state
19:47:55 INFO/BRRP: vr # 1 - pre-empt master state
19:47:55 INFO/BRRP: vr # 1 - timeout in state BACKUP
19:47:55 INFO/BRRP: vr # 1 - acquire master state
19:47:55 NOTICE/BRRP: vr # 1 - now in master state
19:47:55 INFO/BRRP: vr # 1 - router-ifc en1-0-1 up
19:47:55 INFO/BRRP: vr # 2 - pre-empt master state
19:47:55 INFO/BRRP: vr # 2 - timeout in state BACKUP
19:47:55 INFO/BRRP: vr # 2 - acquire master state
19:47:55 NOTICE/BRRP: vr # 2 - now in master state
19:47:55 INFO/BRRP: vr # 2 - router-ifc en1-4-1 up

```

5.2.4 Synchronisation of the virtual routers

Up until the current configuration stage, two virtual routers were created respectively on each of the **bintec RT1202** (access to the local network and access to the Internet). The status of both routers must be synchronised per gateway. The following configuration step shall ensure that virtual router 1 always has the same status as virtual router 2. This step must be configured identically on both **bintec RT1202** . For this, go to the following menu:

- (1) Go to **Routing -> BRRP -> VR Synchronisation -> New**.

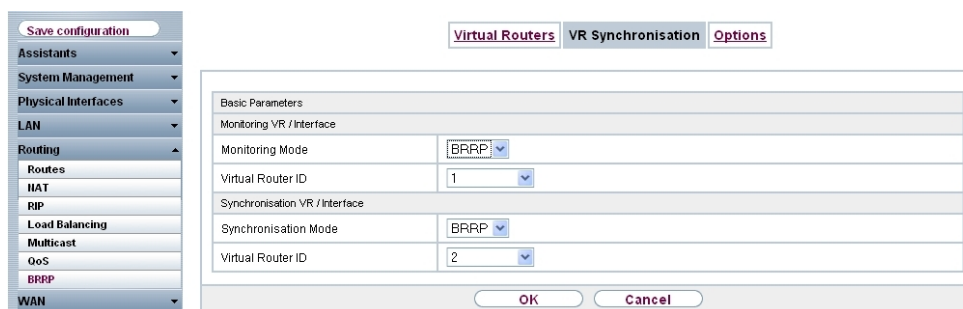


Fig. 45: Routing -> BRRP -> VR Synchronisation -> New

Proceed as follows in order to synchronise the routers:

- (1) Under **Monitoring VR/Interface** select the **Virtual Router ID 1**.
- (2) Under **Monitoring VR/Interface** select the **Virtual Router ID 2**.
- (3) Confirm with **OK**.

Following that, synchronise the second router by selecting **Routing -> BRRP -> VR Synchronisation -> New**.

- (1) Under **Monitoring VR/Interface** select the **Virtual Router ID 2**.
- (2) Under **Monitoring VR/Interface** select the **Virtual Router ID 1**.
- (3) Confirm with **OK**.

Results:

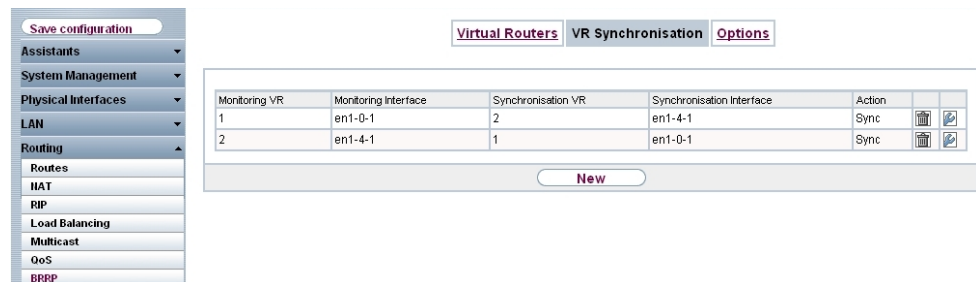


Fig. 46: **Routing -> BRRP -> VR Synchronisation -> New**

This concludes the configuration. To perform a bootable backup of the configuration, exit the **GUI** with **Save configuration** and confirm with **OK**.

5.3 Overview of Configuration Steps

Configuration of the Advertisement and Management IP address

Field	Menu	Value
IP address	Dime Manager -> IP Settings	e.g. <i>10.10.10.1</i>
IP address	Dime Manager -> IP Settings	e.g. <i>10.10.10.2</i>

IP configuration

Field	Menu	Value
IP Address/Netmask	LAN -> IP Configuration -> Interfaces -> >	e.g. <i>10.10.11.1 / 255.255.255.252</i>
IP Address/Netmask	LAN -> IP Configuration -> Interfaces -> >	e.g. <i>10.10.11.2 / 255.255.255.252</i>

Configuration of the virtual router

Field	Menu	Value
Ethernet interface	Routing -> BRRP -> Virtual Router -> New	e.g. <i>en1-0</i>
Router IP Address	Routing -> BRRP -> Virtual Router -> New	e.g. <i>192.168.0.254 / 255.255.255.0</i>
Virtual router ID	Routing -> BRRP -> Virtual Router -> New	e.g. <i>1</i>
Virtual router priority	Routing -> BRRP -> Virtual Router -> New	<i>254</i>
Ethernet interface	Routing -> BRRP -> Virtual Router -> New	e.g. <i>en1-4</i>
Router IP Address	Routing -> BRRP -> Virtual Router -> New	e.g. <i>212.212.212.11 / 255.255.255.248</i>
Virtual router ID	Routing -> BRRP -> Virtual Router -> New	e.g. <i>2</i>
Virtual router priority	Routing -> BRRP -> Virtual Router -> New	<i>254</i>
Ethernet interface	Routing -> BRRP -> Virtual Router -> New	e.g. <i>en1-0</i>
Router IP Address	Routing -> BRRP -> Virtual Router -> New	e.g. <i>192.168.0.254 / 255.255.255.0</i>
Virtual router ID	Routing -> BRRP -> Virtual Router -> New	e.g. <i>1</i>
Virtual router priority	Routing -> BRRP -> Virtual Router -> New	<i>100</i>
Ethernet interface	Routing -> BRRP -> Virtual Router -> New	e.g. <i>en1-4</i>
Router IP Address	Routing -> BRRP -> Virtual Router -> New	e.g. <i>212.212.212.11 / 255.255.255.248</i>
Virtual router ID	Routing -> BRRP -> Virtual Router -> New	e.g. <i>2</i>
Virtual router priority	Routing -> BRRP -> Virtual Router -> New	<i>100</i>

Enable BRRP configuration

Field	Menu	Value
Enable BRRP	Routing -> BRRP -> Options	<i>Enabled</i>

Synchronisation of the virtual routers

Field	Menu	Value
Monitoring mode Virtual router ID	Routing -> BRRP -> VR Synchronisation -> New	1
Synchronisation mode Virtual router ID	Routing -> BRRP -> VR Synchronisation -> New	2
Monitoring mode Virtual router ID	Routing -> BRRP -> VR Synchronisation -> New	2
Synchronisation mode Virtual router ID	Routing -> BRRP -> VR Synchronisation -> New	1

Chapter 6 Services - Remote Maintenance for a bintec RS232bu+ UMTS Gateways Using GSM/GPRS Dial-In

6.1 Introduction

This chapter will use the example of a **bintec RS232bu+** gateway to show a remote maintenance option using GSM/GPRS dial-in. The **bintec RS232bu+** gateway establishes an Internet connection using the internal UMTS (HSPA+) modem. To enable the dial-in for remote maintenance purposes (without using the Internet), you need to switch the integrated UMTS (HSPA+) modem from the UMTS service to the GSM/GPRS network. This UMTS fallback function is initiated by a remote phone call. After the integrated UMTS (HSPA+) modem has been logged into the GSM/GPRS network, a connection to the remote maintenance service from a different **bintec** ISDN gateway can be established using the ISDN login service. Alternatively, an ISDN remote access connection (PPP dial-in) can be established to the **bintec RS232bu+**. When the remote maintenance connection is ended, the **bintec RS232bu+** gateway can log back into the UMTS network and establish the Internet connection.

The **GUI** is (Graphical User Interface) used to do the configuration.

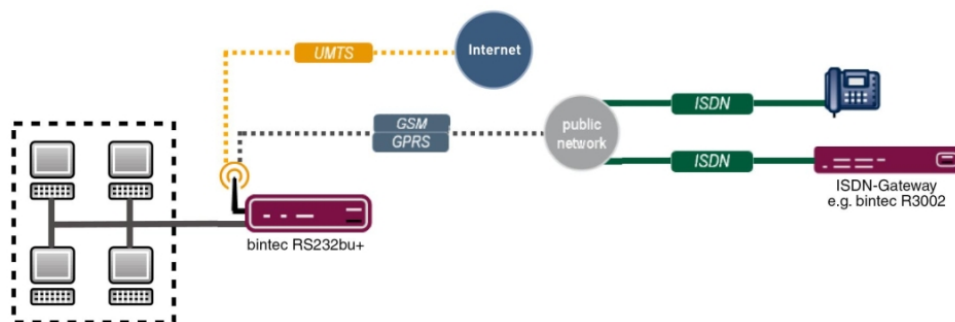


Fig. 47: Example scenario

Requirements

- A UMTS gateway in the bintec RS series (e. g. **bintec RS232bu+**)
- For this gateway, a mobile phone tariff that enables voice and data connections needs to be used

- For the UMTS gateway in the bintec RS series, a 7.10.1 or later firmware version should be used.
- For the integrated modem of the UMTS gateway in the bintec RS series, the current modem firmware must be used ([link to Release Notes](#))
- A telephone/mobile phone to remotely initiate the UMTS fallback
- A bintec ISDN gateway e. g. **bintec R3002** to start the remote maintenance connection by ISDN login
- An ISDN line with V.110 support to start the remote maintenance connection

6.2 Configuration

Configure the UMTS Internet connection

The **GUI** has an Assistant to configure the Internet connection.

With the Assistant, the **bintec RS232bu+**'s UMTS Internet connection can be set up in just a few steps. To do this, go to the following menu:

- (1) Go to **Assistants** -> **Internet Access**-> **Internet Connections** -> **New**.
- (2) For **Connection Type**, select *UMTS*.
- (3) Click on **Next** to configure a new Internet connection.
- (4) Enter the required data for the connection.

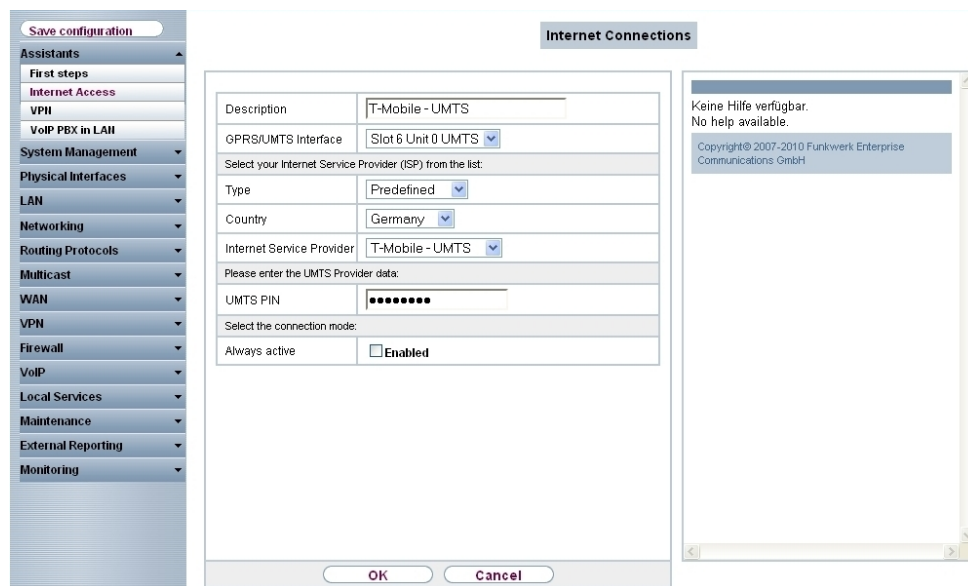


Fig. 48: Assistants -> Internet Access -> Internet Connections -> Next

Proceed as follows to configure a new UMTS Internet connection:

- (1) Under **Description** enter e.g. *T-Mobile - UMTS*.
- (2) For **GPRS/UMTS Interface**, select *Slot 6 Unit 0 UMTS*.
- (3) For **Internet Service Provider**, select *T-Mobile - UMTS*.
- (4) Enter the **UMTS PIN** that your provider has given you, e. g. *0000*.
- (5) Press **OK** to confirm your entries.

Configure the UMTS fallback number and the service for incoming data connections (ISDN login)

The **bintec RS232bu+** gateway only accepts incoming connections (ISDN login or PPP dial-in connections) in the GSM/GPRS network. Using the UMTS fallback function, the gateway can be forced to switch from the UMTS network to the GSM/GPRS network. To do this, a number needs to be created from which the UMTS fallback will be initiated. To do this, go to the following menu:

- (1) Go to **Physical Interfaces -> UMTS/HSDPA -> UMTS/HSDPA/HSUPA** -> .

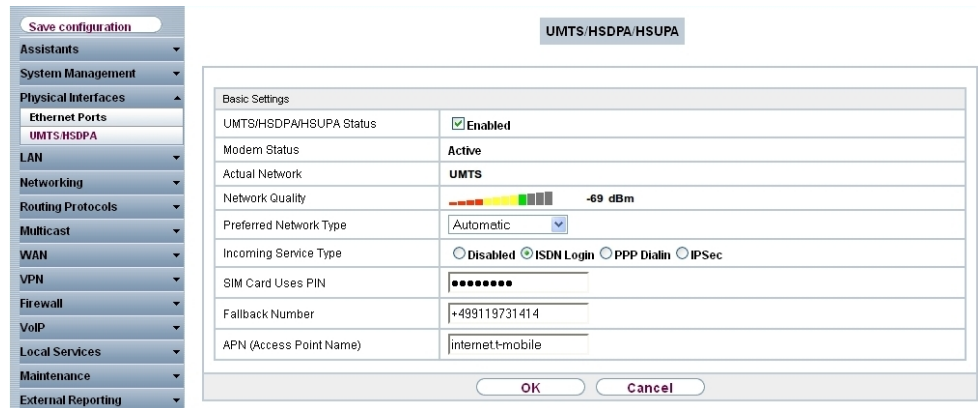


Fig. 49: Physical Interfaces -> UMTS/HSDPA -> UMTS/HSDPA/HSUPA -> 

Proceed as follows to configure the UMTS fallback number:

- (1) For **Incoming Service Type**, select *ISDN Login*. Alternatively, the *PPP Dialin* option can be used to enable an IP connection.
- (2) For **Fallback Number**, enter the telephone number from which the UMTS fallback call is to be initiated, e. g. *+4991196731550*.
- (3) Confirm with **OK**.

6.3 Test the UMTS fallback with an incoming voice connection

The default behaviour is that the **bintec RS232bu+** gateway establishes an Internet connection via the UMTS network. By means of a voice call (fallback number), the gateway logs into the GSM/GPRS network and enables incoming data connections.

Debug messages for the UMTS fallback:

```

rs232bu+> debug all 6
10:49:56 INFO/MODEM: usbTTYO: PLMN Telekom.de(Home) LAC 44B2 CID 0002AA13 AcT UMTS
10:49:59 DEBUG/MODEM: usbTTYO: switch state P1 -> RO
10:49:59 DEBUG/USB: usbTTYO: serial state notification - ring ind.
10:49:59 INFO/MODEM: usbTTYO: Voice call from '+4991196731550' - activate GSM fallback
10:49:59 DEBUG/PPP: T-Mobile - UMTS: event: "ifAdminStatus_down event",status: "initial / dormant" (dormant) ->
"interface down" (down)
10:49:59 DEBUG/MODEM: usbTTYO: Configured Access Mode 'UMTS-Pref'
10:49:59 INFO/MODEM: usbTTYO: Select PLMN 26201 ==> 26201/UMTS ==> GSM
10:49:59 DEBUG/MODEM: usbTTYO: Actual AcM 'GPRS-Only'
10:50:00 INFO/MODEM: usbTTYO: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:00 INFO/MODEM: usbTTYO: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:00 INFO/MODEM: usbTTYO: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:00 INFO/MODEM: usbTTYO: PLMN Telekom.de(Home) LAC 44B2 CID 0002AA13 AcT UMTS
10:50:00 DEBUG/PPP: T-Mobile - UMTS: event: "ifAdminStatus_up event",status: "interface down" (down) -> "initial /
dormant" (dormant)
10:50:01 DEBUG/MODEM: usbTTY3: Temperature: 52
10:50:05 INFO/MODEM: usbTTYO: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:05 INFO/MODEM: usbTTYO: PLMN Telekom.de(Home) LAC 44B2 CID 0002AA13 AcT UMTS
10:50:05 DEBUG/MODEM: usbTTYO: Network - Registration in progress
10:50:06 INFO/MODEM: usbTTYO: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:06 INFO/MODEM: usbTTYO: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:08 DEBUG/MODEM: usbTTYO: Network - Registration in progress
10:50:08 DEBUG/MODEM: usbTTYO: Network - Receive Signal Level -79 dB
10:50:08 INFO/MODEM: usbTTYO: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:08 INFO/MODEM: usbTTYO: Registered 26201 (Telekom.de) (AcT = UMTS)
10:50:09 INFO/MODEM: usbTTYO: Registered 26201 (T-Mobile D) (AcT = GSM)
10:50:09 INFO/MODEM: usbTTYO: PLMN T-Mobile D(Home) LAC 4427 CID 00001EA7 AcT GSM

```

6.4 Dial-in by ISDN login from a different bintec ISDN gateway

After the UMTS fallback has been done and the **bintec RS232bu+** gateway is registered in the GSM/GPRS network, incoming data connections can be made. To do this, an ISDN data connection must be initiated on the caller's side, using the V.110 protocol. In this chapter, an ISDN login connection to **bintec RS232bu+** remote maintenance will be established from a different bintec ISDN router. After logging in, the familiar console commands such as the Setup tool can be used for remote maintenance.

```
-----  
r3002:> isdnlogin 01713315981 v110_9600  
Trying...  
Establishing B-channel...  
Connected to 01713315981  
  
Connected to RS232bu+, rs232bu+,  
from ISDN telephonenumber +4991196730 Service modem (9600 bps)  
  
Welcome to RS232bu+ version V.7.10 Rev. 1 IPSec from 2011/08/02 00:00:00  
systemname is rs232bu+, location  
  
Login: admin  
Password:  
  
Password not changed. Call "setup" for quick configuration.  
  
rs232bu+:> setup  
-----
```

Debug messages during the incoming ISDN login connection:



```
rs232bu+:> debug all &  
10:50:41 DEBUG/USB: usbTTYO: serial state notification - ring ind.  
10:50:41 DEBUG/MODEM: usbTTYO: switch state P1 -> R0  
10:50:41 INFO/MODEM: usbTTYO: Data call from '+4991196730' - data mode state incoming  
10:50:41 DEBUG/MODEM: usbTTYO: Modem incoming call from <+4991196730>  
10:50:41 DEBUG/PPP: dialin from <+4991196730> to local number <6001> (1/2)  
10:50:41 INFO/ISDN: isdnlogind: accept call from <+4991196730>  
10:50:41 DEBUG/MODEM: usbTTYO: switch state R1 -> A0  
10:50:41 DEBUG/MODEM: usbTTYO: attach to channel 1 - incoming  
10:50:43 INFO/MODEM: usbTTYO: Accept call from '+4991196730' ==> (CONNECT 9600)  
10:50:43 DEBUG/MODEM: usbTTYO: switch state D1 -> D1  
10:50:43 DEBUG/USB: usbTTYO: get DCD on (ch 3)  
10:50:55 INFO/ACCT: LOGIN as admin from ISDNLOGIN +4991196730 at Mon Aug 1 10:50:55 2011
```

6.5 Overview of Configuration Steps

Configure the UMTS Internet connection

Field	Menu	Value
Connector Type	Assistant -> Internet Access -> New	<i>UMTS</i>
Description	Assistant -> Internet Access -> Next	<i>T-Mobile - UMTS</i>
GPRS/UMTS Interface	Assistant -> Internet Access -> Next	<i>Slot 6 Unit 0 UMTS</i>
Internet Service Provider	Assistant -> Internet Access -> Next	e. g. <i>T-Mobile - UMTS</i>
UMTS PIN	Assistant -> Internet Access -> Next	e. g. <i>0000</i>

Configure the UMTS fallback number

Field	Menu	Value
Incoming Service Type	Physical Interfaces -> UMTS/HSDPA -> UMTS/HSDPA/HSUPA -> 	<i>ISDN Login</i>
Fallback Number	Physical Interfaces -> UMTS/HSDPA -> UMTS/HSDPA/HSUPA -> 	e. g. <i>+4991196731550</i>