



# Manual Workshops (Excerpt)

Services Workshops

Copyright© Version 01/2020 bintec elmeg GmbH

#### Legal Notice

Warranty

This publication is subject to modifications.

bintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbH is not liable for the information in this manual. bintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec 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 GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbH

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

# **Table of Contents**

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

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

Chapter 6	Services - Remote Maintenance for a bintec RS232bu+ UM Gateways Using GSM/GPRS Dial-In	ГS 54
6.1		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:

Save configuration		DHCP Pool IP/MAC Binding DHCP Relay Settings
Assistants 👻		prior read occurge
System Management 🔹 👻		
Physical Interfaces 🔹 👻	Basic Parameters	
LAN 👻	IP Pool Name	
Wireless LAN 👻	Interface	
Networking 🗸 👻	Interface	
Routing Protocols 🔹 👻	IP Address Range	192.168.0.2 -  192.168.0.10
Multicast 🗸 🗸	Pool Usage	Local
WAN -		Advanced Cettings
VPN -		Advanced Settings:
Firewall 🔹	Gateway	Use router as gateway 🔽
VolP 👻	Lease Time	120 Minutes
Local Services 🔺		
DNS	DHCP Options	Option Value
HTTPS DurpDHS Client		Add
DHCP Server		OK Cancel
Web Filter		

(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.

Save configuration		DHCP Pool	IP/MAC Bindin	g DHCP Relay Setting	s
Issistants	•				-
ystem Management	•				
hysical Interfaces	View 20 per	page 🔍 🚿 Filter in 🛛 No	ne 🔽 equ	ial 🔽 (G	30
AN	IP Address	Description MAC A	ddress	Remaining Lease Time	Static Binding
ireless LAN	• 192.168.0.3	BigBoss 00:a0:	f9:09:67:6f		Enablec
tworking	▼ Page: 1, Items: 1 - 1	1			
uting Protocols	•	New	ОК	Cancel	$\overline{)}$
liticast	-				
N	•				
N	-				
wall	-				
P	•				
al Services					
NS					
TTPS					
)ynDNS Client					
OHCD Server					

#### 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.

Save configuration	Global Se	ettings S	tatic Ho	Domain Forwardi	ng <u>Cache</u>	Statistics
Assistants						
System Management 🔹 👻						
Physical Interfaces 🔹 🔻	Basic Parameters					
LAN 👻	Domain Name					
Wireless LAN 🔹	DNS Server Configuration	Oynar	nic 🔿 Stat			
Networking 👻		-				-
Routing Protocols 🔹 👻	WINS Server	Primary		0.0.0		
Multicast 🗸 🗸		Seconda	ny	D.O.O		
WAN 🔫						
VPN -			Adva	ed Settings		
Firewall 👻	Positive Cache					
VolP 🔹	Negative Cache		Frahled			
Local Services 🔺	Elenaned					
DNS	Cache Size		100	Entries		
HTTPS	Maximum TTL for Resitive Cache Entries		86400	Seconds		
DynDNS Client	Maximum TTE for Positive Cattle Entries		100 100			
DHCP Server	Maximum TTL for Negative Cache Entries		86400	Seconds		
CAPI Server	Fallback interface to get DNS server		Automatic V			
Scheduling						
Surveillance	IP address to use for DNS/WINS server assi		ignment As DHCP Server None Own IP Address Global DNS Setting			ess 🔘 Global DNS Setting
ISDN Theft Protection						ess 💿 Global DNS Setting
UPnP						
HotSpot Gateway			<b>A</b> 1/		\	
Maintenance 🔹 👻		(	ØK	Cancel	)	

#### 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 As- signment: As DHCP Server	<ul> <li>Select the most suitable method for your network environment from the following options:</li> <li><i>None</i>: The gateway issues no DNS server IP addresses with this setting.</li> </ul>
	• Own IP address: The gateway assigns its own IP address as DNS.
	• Global DNS Setting: The gateway assigns the IP ad- dresses as DNS, which you have configured or assigned dy- namically 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:

Save configuration		Interfaces	
System Management 🔹 👻			
Physical Interfaces 🔹 👻	Basic Parameters		
LAN	Address Mode	○ Static	
IP Configuration VLAN Wireless LAN	IP Address / Netmask	P Address Netmask	
Networking 🗸 🗸	Interface Mode	⊙ Untagged ○ Tagged (VLAN)	
Routing Protocols 🔹 👻	MAC Address	00:a0:f9:23:93:4c	
Multicast 🔹			
WAN -	Advanced Settings		
VPN 👻	DHCP Mac Address	Vilee built in	
Firewall 👻			
VoIP -	DHCP Hostname		
Local Services 🔹 👻	DHCP Broadcast Flag	✓ Enabled	
Maintenance 🔹 👻	Proxy ARP	Enabled	
External Reporting 🔹 👻	TCP-MSS Clamping	Enabled	
Monitoring 🗸 👻			
		OK Cancel	

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

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.

ssistants vystem Management vystem Management vystem Management vysteal Interfaces NN Primary DHCP Server Basic Parameters Primary DHCP Server Primary DHCP Server Basic Parameters Primary DHCP Server DI0.0.0.0 OK Cancel OK Cancel OK Cancel O Secondary DHCP Server Component Co	Save configuration			DHCP Pool IP/MAC Binding DHCP Relay Settings
ystem Management tysical Interfaces tysical Interfaces AN   Basic Parameters Primary DHCP Server ID2.168.1.2 Secondary DHCP Server ID2.168.1.2 Secondary DHCP Server OK  Cancel OK Cancel	ssistants	-		
Physical Interfaces	System Management	-		
LAN V   Wireless LAN V   Networking V   Routing Protocols 0.0.0   Winicast V   WAN V   Firewall V   VolP Local Services   Dis HTTPS   DyuDilS Client V	Physical Interfaces	-	Basic Parameters	
Wireless LAN Wireless LAN Networking Council and Protocols Walticast WAN V VPN Firewall Coal Services DIIS HTTPS DynDIIS Chient	LAN	-	Primary DHCP Server	192.168.1.2
Networking        •       ID:000       ·       ·       ID:0000       ·       ·       ·       ·       ·	Wireless LAN	-	Secondary DUCB Server	
Routing Protocols     OK     Cancel       Multicast     V       WAN     V       VPN     V       Frewall     V       Local Services       DHS       HTTPS       DHIS Client	Networking	-	Secondary Driver Server	0.0.0.0
Multicast  WAN VPN Firewall VolP Cocal Services Dils HTTPs Dils Client	Routing Protocols	-		OK Cancel
WAN  VPN VIPN VIPN VOIP VOIP VOIP VIP VIP VIP VIP VIP VIP VIP VIP VIP V	Multicast	-		
VPN  Firewall VolP VolP VolP VolP VolP VolP VolP Vo	WAN	-		
Firewall  VolP VolP Local Services DIIS HTTPS DynDIIS Client	VPN	-		
VoIP  Local Services  DHS HTTPS DynDIS Client	Firewall	-		
Local Services DHS HTTPS DynDIS Client	VolP	-		
DIIS HTTPS DynDIS Client	Local Services	•		
HTTPS UynDIS Client Uses	DNS			
DynDills Chent	HTTPS			
DM/TH Vortion	DynDNS Client	_		

#### 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 Serv- er	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	<b>e.g.</b> en1-0
IP Address Range	Local Services -> DHCP Server -> DHCP Pool -> New	e.g. 192.168.0.2 and 192.168.0.10
Pool Usage	Local Services -> DHCP Server -> DHCP Pool -> New	Local
Gateway	Local Services -> DHCP Server -> DHCP Pool -> New -> Advanced Settings	Use Router as Gateway
Lease Time	Local Services -> DHCP Server -> DHCP Pool -> New -> Advanced Settings	<b>e.g.</b> 120
IP Address to use for DNS/WINS Server As- signment: As DHCP Server	Local Services -> DNS -> Global Settings -> Advanced Settings	<b>e.g.</b> Own IP address

### **DHCP Client**

Field	Menu	Value
Address mode	LAN -> IP Configuration -> Inter- faces -> <en1-4> -&gt;</en1-4>	DHCP
DHCP MAC Address (optional)	LAN -> IP Configuration -> Inter- faces -> <en1-4> -&gt; -&gt; -&gt; Advanced Configurations</en1-4>	MAC address for a spe- cific DHCP server

### **DHCP Relay Server**

Field	Menu	Value
Primary DHCP Server	Local Services -> DHCP Server -> DHCP Relay Settings	<b>e.g.</b> 192.168.1.2
Secondary DHCP Serv- er (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.

Save configuration		DynDNS Update DynDNS Provider
Assistants 👻		
System Management 🛛 👻		
Physical Interfaces 🔹 👻	Basic Parameters	
LAN 🔫	Provider Name	no-IP
Wireless LAN 🔫	Server	dynundate no-in com
Networking 👻		
Routing Protocols 🔹 👻	Update Path	/nic/update
Multicast 🗾 👻	Port	80
WAN -	Protocol	DynDNS
VPN 🔻	Lindate Interval	300 Seconds
Firewall 👻		seconds
VoIP 🔻		OK Cancel
Local Services 🔺		
DNS		
HTTPS		
DynDNS Client		
Drice Server		



#### 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.

Save configuration				
Assistants			DynDNS Update	DynDNS Provider
Assistants				
System Management	<b>•</b>			
Physical Interfaces	Basic Pa	arameters		
LAN	<ul> <li>Host N</li> </ul>	Jame .	bintec.no-ip.com	
Wireless LAN	<ul> <li>Interfac</li> </ul>	ce	Internet 🔽	
Networking	-			
Routing Protocols	- User N	lame	name@email.de	
Multicast	<ul> <li>Passw</li> </ul>	vord	•••••	
WAN	- Provide	er	no-IP 💌	
VPN	Enable	e update	Fnabled	
Firewall	•			
VolP	-	Advanced Settings		
Local Services	•	OK Cancel		
DNS				
HTTPS				
DynDNS Client				
DHCP Server				



#### 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.

Save configuration			NAT Interfaces NAT Configuration	
Assistants	-			
System Management	-			
Physical Interfaces	•	Basic Parameters		
LAN	-	Description		
Wireless LAN	•	Interface	WAN_INTERNET	
Networking	•	Type of traffic	incoming (Destination NAT)	
Routes	_	Type of trainc		
NAT		Specify original traffic		
Load Balancing	_	Service	http 💌	
Qos Access Rules		Source IP Address/Netmask	Any 💟	
Routing Protocols	-	Original Destination IP Address/Netmask	Any 💌	
Multicast	-	Replacement Values		
WAN	-	New Destination IP Address/Netmask	Host V 0000	
VPN	-			
Firewall	-	New Destination Port	Original 🗹	
VoIP	-		OK Cancel	
Local Services	•			



#### 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. no-IP
Server	Local Services -> DynDNS Client -> DynDNS Providers -> New	dynup- date.no-ip.com
Update Path	Local Services -> DynDNS Client -> DynDNS Providers -> New	/nic/update
Port	Local Services -> DynDNS Client -> DynDNS Providers -> New	80
Protocol	Local Services -> DynDNS Client -> DynDNS Providers -> New	DynDNS

#### **Configuring DynDNS**

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

## NAT entries

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

# **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.

Save configuration		Time Schedule	Options
System Management 🔹 👻			
Physical Interfaces 🔹 👻			
LAN 👻	Basic Parameters		
Wireless LAN 🗸	Description	Reboot	
Routing 🔹 👻	Action	,	
WAN -	Palastastian	Debestderies	
VPN 👻	Select action	Reboordevice	
Firewall 🗸	Select time interval		
VolP 👻		Condition Type	Condition Settings
Local Services		O Weekday	Monday ~
DNS	Time Condition	Periods     Day of Month	Daily 💌
DynDNS Client		C Day of Monar	1 🛛
DHCP Server			
Web Filter	Start Time	Hour 00 Minute 00	
CAPI Server	Start Time	nou oo minuce oo	
Scheduling			
Surveillance		OK C	Cancel
ISDN Theft Protection			
Funkwerk Discovery			
UPnP			

#### 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.

Save configuration
System Management 🔹 👻
Physical Interfaces 🔹 👻
LAN 👻
Wireless LAN 👻
Routing 👻
WAN -
VPN 👻
Firewall 🗸 🗸
VolP 👻
Local Services 🔺
DNS
DynDNS Client
Web Filter
CAPI Server
Scheduling
Surveillance

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.

Save configuration		Time Schedule Options	
System Management 🛛 👻			
Physical Interfaces 🔹			
LAN 👻	Basic Parameters		
Wireless LAN 🗸	Description	Wireless LAN	
Routing 👻	Action		
WAN -	Description Description With the second seco		
VPN -			
Firewall 👻	Select interface	Funkwerk-ec(vss1-0) 💌	
VolP 🗸	Select time interval		
Local Services		Condition Type Condition Settings	
DNS		O Weekday Monday V	
DynDNS Client	Time Condition	Periods     Caturday, Sunday, Marceleter	
DHCP Server		O Day of Month	
Web Filter		1 🗸	
CAPI Server			
Scheduling	Start Time	Hour 00 Minute 00	
Surveillance		11 00 11 1 50	
ISDN Theft Protection	Stop Time	Horilaa www.elaa	
Funkwerk Discovery			
UPnP		OK Cancel	

#### 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.

Save configuration	Time Schedule Options		
Physical Interfaces 🔹 👻			
LAN 👻	Basic Parameters		
Wireless LAN 👻	Description	Configuration	
Routing 🗸 🗸	Action	Teeningmann	
WAN +	Action		
VPN -	Select action	Trigger configuration backup 💌	
Firewall 🗸 🗸	TFTP Server	192.168.0.2	
VolP 👻	TFTP File Name	r232bw.cfg	
Local Services	Select time interval		
DNS		Condition Type	Condition Settings
DynDNS Client			Contaition Settings
DHCP Server		O Reviedo	Monday 👻
Web Filter	Time Condition	Day of Month	Daily
CAPI Server Seboduling		C Day of Monar	1 🗸
Surveillance			
ISDN Theft Protection	Start Time	Hour 00 Minute 00	
Funkwerk Discovery			
UPnP	Stop Time	Hour 00 Minute 05	
Maintenance 🗸 🗸			0 mm m m
External Reporting 🚽 👻		OK	Cancer

#### 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**.

DIME Tools - TETP Server	
Se Yew Configuration Window Help	
🚅 🖬 🖧 22 A 🗸 🖆 🔏 A 🧶 A 🕷 🗶 📍 😵	
TFTP Server	
Listening for TFIP requests on port 69	
ar Help, press F1	N.M 4

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

#### Suspending the WLAN interface

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

#### Monthly configuration backup

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

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

# 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 Managersoftware

# 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 Man-ager**. 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.

Save configuration			Internet Connec	tions
Assistants				
First steps				
Internet Access				ISP Data for Internal
VPN		Description	ADSL	ADSL/SHDSL Modem
VoIP PBX		Select your Inter	rnet Service Provider (ISP) from the list:	
System Management	-	Internet		For Internet access you must set up a
Physical Interfaces	-	Service Provider	Germany - T-Home	(ISP).
LAN	-	Enter the auther	tication data for your Internet account:	Follow your provider's instructions!
Routing	-	User Name	0000111111#0001@t-online.de	Enter a description for the Internet connection.
WAN	-			
VPN	-	Password	$\bullet \bullet \bullet$	You can select one of the predefined ISPs or
Firewall	-	Select the conn	ection mode:	settings are required depending on the choice
VolP	-	Always active	✓Enabled	you make for the ISP or the user-defined
Local Services	-			Internet Service Provider:
Maintenance	-			Select your ISP or define a customized
External Reporting	-			provider by choosing User - defined via the required connection protocol PPPoF (PPP
Monitoring	•			over Ethernet), PPPoA (PPP over ATM), ETHoA (Ethernet over ATM) or IPoA (IP over ATM).
				When establishing an Internet connection, you are normally prompted for authentication by the ISP A user name and a password are normally used for authentication. You can c
			OK Cancel	

#### 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.

ssistants		VPN Connections	l
First steps	· · · · · · · · · · · · · · · · · · ·		
Internet Access			IPSec   AN-to-  AN Connection
VPN	Selected scenario		
oIP PBX	IPSec Scenario	LAN-to-LAN Connection	Enter the required data for the IPSec -
stem Management 🛛 👻	Connection Details		LAN-to-LAN connection scenario.
vsical Interfaces 🚽	Description	filiale1	A reminder of the selected scenario.
rting 🚽	Local IPSec ID	212.212.212.1	As you can configure several VPN
N -			be able to identify the VPN connection easily
N -	Remote IPSec ID	filiale 1	Description:
wall <del>.</del>			Enter a name for the connection.
p -	Preshared Key	••••••	The IPSec partners have to mutually identify
cal Services 🚽	Local IP Address	192.168.0.1 😂	and authenticate in order to establish an IPSec connection.
intenance -	Define this connection as default route	Enabled	The identity of the IPSec partner is proven by a unique ID (similar to user name). To
ernal Reporting 🚽	Enter IP settings:		establish an IPSec connection each IPSec
nitoring 👻	IPSec Peer Address		gateway must be able to identify the ID of the other gateway. Therefore both 'IDs' must be configured on both IPSec gateways. The ID
	IP Address of Remote Network	192.168.1.0	can be any name. In practice it is usually a name which clearly explains the connecting
	Subnet Mask	255.255.255.0	Local IPSec ID:
			Enter the ID of your own IPSec gateway.
	ОК	Cancel	

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. *fi*-*liale1*.
- (4) For the authentification 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.

Save configuration					VPN (	Coni	nection	s
Assistants	•							
First steps								
Internet Access		<u> </u>					_	VPN Connections
VPN	View 2	O per page 🔛	≥ Go					
VoIP PBX	Туре	Description	Mode	Status	Action			This configuration section guides you through
System Management	- IPSec	filiale1	LAN-to-LAN Connection	۲	<b>*</b>	窗		all of the settings required to set up LAN-LAN or single client connections as a Virtual
Physical Interfaces	▼ Page: 1,	items: 1 - 1				-	-	Private Network (VPN).
AN	•							Note: The TCP/IP settings of the PCs must be changed in both networks (standard gateway
Routing	-							DNS server, any static routes that are required
WAN	•							etc.), so that the PCs (Server, Printer etc.) in
/PN	-							remote network.
Firewall	-							The list displays all configured VPN
VolP	•							connections indicating the Type of the connection (IPSec or PPTP), a Description,
Local Services	•							the Mode (Single Client Dialin or LAN-to-LAN) and the current status.
Maintenance External Reporting	•							You can change the status by clicking 重 or
Monitoring	•							To add a VPN connection, press <b>New</b> and follow the instructions. After completing a connection configuration, you are returned to the list so that you can start setting up further connections.
								To edit an existing entry, click 🖉 for the respective list item.
								With 🗎 you can delete entries.
			New					

#### 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.

Save configuration		Internet Connecti	ons
sistants 🔺			
First steps			
Internet Access			ISP Data for External xDSL
VPN	Description	JADSL	Modem
VoIP PBX	Select the physical Ethernet	port the external modem is connected to:	<b>5</b> 11 1
stem Management 🔹 👻	Physical Ethornot Port		For Internet access you must set up a
ysical Interfaces 🛛 👻	T Hysical Ethemetr oft		(ISP).
N +	Select your Internet Service	Provider (ISP) from the list:	Follow your provider's instructions!
outing -	Internet Service Provider	Germany - T-Home	Description:
AN -	Enter the authentication data	for your Internet account:	Enter a description for the internet connection.
×N →	User Name	111111111222222#0001@t-online.de	Please check that the xDSL modern is
ewall 🗸	Password		Ethernet interfaces!
oIP 👻	T doomond		Physical Ethernet Port:
cal Services 🗸 🗸	Select the connection mode:		Select the port to which the xDSL modern is
aintenance 🗸	Always active	Enabled	connected.
ernal Reporting 🗸 🗸			You can select one of the predefined ISPs or
nitoring -			define a custom Internet connection. Different settings are required depending on the choice you make for the ISP.
			Select your ISP or define a customized provider by choosing User-defined.
			Some ISPs require a VLAN ID.
		OK Cancel	

#### 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.

ve configuration		VPN Conn	ections
istants 🔺			
st steps			
ernet Access	Selected scenario		IPSec LAN-to-LAN Connection
IP PBX	IPSec Scenario	LAN-to-LAN Connection	Enter the required data for the IPSec -
em Management 🔹 👻	Connection Details		LAN-to-LAN connection scenario.
cal Interfaces 👻	Description	Zentrale	IPSec Scenario: A reminder of the selected scenario.
•			
g 👻	Local IPSec ID	filiale1	As you can configure several VPN connections, you must define a description
•			be able to identify the VPN connection easi
-	Remote IPSec ID	212.212.212.1	Description:
all 👻		-	
	Preshared Key		The IPSec partners have to mutually identify
Services 👻	Local IP Address	192.168.1.1   \$	and authenticate in order to establish an IPSec connection.
enance -	Define this connection as default ro	ute Enabled	The identity of the IPSec partner is proven by a unique ID (similar to user name). To
al Reporting 🔹	Enter IP settings:		establish an IPSec connection each IPSec
ring 👻	IPSec Peer Address	212.212.212.1	gateway must be able to identify the ID of th other gateway. Therefore both 'IDs' must be configured on both IPSec gateways. The ID
	IP Address of Remote Network	192.168.0.0	can be any name. In practice it is usually a name which clearly explains the connecting
	Subnet Mask	255.255.255.0	Local IPSec ID:
			Enter the ID of your own IPSec gateway.
	ОК	Cancel	



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 authentification 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 -> ip -> Advanced Settings.

Save configuration	IPSec Peers	Phase-1 Profiles	Phase-2 Profiles	XAUTH Profiles	IP Pools	Options
Assistants 👻		I				
System Management 🛛 👻						
Physical Interfaces 🔹	Peer Parameters					
LAN 👻	Administrative Status	Op O Down				
Routing -	Description	Zentrale				
WAN -	Boor Addropp	010 010 010	1			
VPN 🔺	- Feel Address	212.212.212.	L			
IPSec	Peer ID	IPV4 Address		0		
РРТР		212.212.212.	1			
GRE	Preshared Key					-
Firewall 👻	Interface Routes					
VoIP 👻						
Local Services 👻	IP Address Assignment	Static	0			
Maintenance 👻	Default Route	Enabled				
External Reporting 👻	Local IP Address	192.168.1.1				
Monitoring 👻		Romoto IR Address		Network		Metric
		192.168.0.0		255.255.255.0	)	
	Route Entries	,				
		Add				
		Adv	anced Setting	s		
	Advanced IPSec Options					
	Phase-1 Profile	wz_ike_1	0			
	Phase-2 Profile	* Multi-Propo	sal 🗘			
	XAUTH Profile	Select one				
	Number of Admitted Connections	◉ One User ○	Multiple Users			
	Start Mode	On Demand	Always up			
	Advanced IP Options					
	Back Route Verify	Enabled				
	Proxy ARP	⊙ Inactive ○ Up	or Dormant 🔘 Up or	ily		
		ОК	Cano	el		

Fig. 27: VPN -> IPSec -> IPSec Peers -> ip> -> 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.

Save configuration			QoS Filter QoS Classification QoS Interfaces/Policies
Assistants	-		
System Management	-		
Physical Interfaces	-	Basic Parameters	
LAN	•	Description	IKE
Routing Routes	•	Protocol	udp 🗘
NAT RIP		Destination IP Address/Netmask	0.0.0.0
Load Balancing Multicast		Destination Port/Range	Specify port \$\$500 to -1
QoS		Source IP Address/Netmask	0.0.0.0
WAN	-	Source Port/Range	Specify port \$\$500 to -1
VPN	•	DSCP/TOS filter (Layer 3)	[Ignore   \$
Firewall VolP	•	COS filter (802.1p/Layer 2)	0
Local Services	-		
Maintenance	-		

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:

Save configuration				OoS Eilter OoS Cl	ssification OoS Interfac	es/Policies	
Assistants	-			403 Filter 403 Cit		es/r oncies	
ystem Management	-						
Physical Interfaces	-				QoS Filter		
		Index	Description	Source	Destination	TOS/DSCP	
.AN	•	1	IKE	0.0.0.500	0.0.0.0:500	0	龠
louting	-	2	ESP	0.0.0.0	0.0.0	0	龠
Routes		3	NAT-T 1	0000	0 0 0 0 4500	0	
NAT		4	NAT T 2	0.0.0.0:4500	0.0.0	-	
RIP		4	NAT-1_2	0.0.0.4500	0.0.0.0	U	
Load Balancing							
Multicast					New		
QoS							
BRRP							

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.

Emm configuration							
Save conliguration			QoS Filter	QoS Classification	QoS Interfaces/Policies		
Assistants	-						
System Management	-						
Physical Interfaces	•	Basic Parameters					
LAN	•	Class map	New	•			
Routing	-	Description	L (DALLID				
Routes		Description	IVPN-P	VPN-PSec			
NAT		Filter	(IKE				
RIP		FINE	IKE	IKE V			
Load Balancing		Direction	Outro				
Multicast		Direction	Ourgo	Catgoing			
QoS		High Priority Class					
BRRP							
WAN	-		Interface				
VPN	-	Interfaces	ADSL				
Firewall	-			Add			
VolP	-						
Local Senices	_			ок 🔿 🤇 с	ancel		
Local Services							

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.

Save configuration	5		QoS Filter QoS Classification QoS Interfaces/Policies
Assistants	-		
System Management	-		
Physical Interfaces	-	Basic Parameters	
LAN	-	Class map	VPN-IPSec 🗢
Routing	-		
Routes		Filter	ESP
NAT		Direction	
RIP		Direction	
Load Balancing		High Priority Class	
Multicast			
QoS			
BRRP			OK Cancel

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 asigned.
- (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:

Save configuration			QoS Filt	er QoS Classifica	tion QoS Interfaces/Po	licies		
Assistants	-			-				
System Management	-							
Physical Interfaces	-			QoS Classif	fication			
		Description	Assigned Interface	Filter	Assigned Class ID	Direction		
LAN	•	VPN-IPSec	ADSL					
Routing	•			IKE	HP	Outgoing	俞	i
Routes	-			ESP	HP	Outaoina	 ) ) )	i
NAT				NATT 1	LIB	Outasing		
RIP				INAI-1_1	nr	Outgoing		J
Load Balancing				NAT-T_2	HP	Outgoing	前	·
Multicast								ļ
QoS				New				
BRRP								Î

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.

Save configuration	)	Q	oS Filter QoS Classification QoS Interfaces/Policies
Assistants	-		
System Management	-		
Physical Interfaces	-	Basic Parameters	
LAN	-	Interface	ADSL 🗘
Routing Routes	-	Priorisation algorithm	Priority Queueing
NAT RIP		Traffic shaping	Enabled
Load Balancing Multicast		Protocol Header Size below Layer 3	PPP over Ethernet
QoS			Description Type Class ID Priority Bandwidth for Traffic Shaping
BRRP		Queues/Policies	High Priority - 0 0 💼 🖉
WAN	•		Add
VPN	-		
Firewall	-		OK Cancel

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**.

sistants   term Management  siscal Interface  ting  N	Save configuration	)				0.05	0.05
tem Management  visical interface  i   CoS  i   i   i   i   i   i   i   i   i   i	Assistants	-					
sical Interfaces	System Management	-					
tting ADSL ADSL High Priority Unpriorized	Physical Interfaces	-	QoS				
ADSL           N         High Priority           unpriorized	LAN	-	Interface	QoS Queue		Send	Send Dropped
N High Priority 11 unpriorized 12	Routing	-	ADSL				
unpriorized 12611	WAN	_		High Priority	12344		0
				unpriorized	12611		11506
- V - V	/PN	-					
	wall	-					
wall 🗸	ID						
wali 👻	OIP	-					
wall + P +	ocal Services	-					
wall - p - al Services -	Maintenance	-					
wall - p - al Services - Intenance -	External Reporting	-					
wall	Monitoring	-					
wall   p  al Services  r  ennance  r  ennal Reporting  nitoring	Internal Log						
wall   p p al Services  rateanace  rateanaceanace  rateanaceanaceanaceanaceanaceanaceanacean	IPSec						
wall   p  A  p  r  al Services  r  r  nternal Reporting  r  ternal Log  Sec	ISDN/Modem						
wall   p p al Services  r al Services  r al function  r al Services  see  DMModern	Interfaces						
wall     •       p     •       ral Services     •       intenance     •       ernal Reporting     •       inforing     •       ternal Log     •       Sec     •       DiModem     •       terfaces     •	HotEnot Catoway	_					
wall •   P •   ral Services •   ratare •   ernal Reporting •   nitoring •   See •   DMModern •   terfaces •   USpot Gateway •	notspot Gateway	-					

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. 192.168.0.1

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

#### Configuration of VPN IPSec access (head office)

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

#### Configuration of gateway in branch (bintec RS120)

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

#### Configuration of Internet access (branch)

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

Field	Menu	Value
Physical Ethernet Port	Assistant -> Internet Access -> Next	<b>e.g.</b> <i>ETH5</i>
Internet Service Pro- vider	Assistant -> Internet Access -> Next	<b>e.g.</b> Germany - T- Home
User Name	Assistant -> Internet Access -> Next	<b>e.g.</b> 111111111222222#00 01@t-online.de
Password	Assistant -> Internet Access -> Next	<b>e.g.</b> supersecretge- heimkey
Always Active	Assistant -> Internet Access -> Next	Enabled

## Configuration of VPN IPSec access (branch)

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

#### Prioritisation of VPN tunnel

Field	Menu	Value
Start mode	VPN -> IPSec -> IPSec Peers ->	Always Active
	Advanced Settings	

#### **Creation of QoS filters**

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

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	<b>e.g.</b> <i>NAT-T_1</i>

Field	Menu	Value
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	<b>e.g.</b> <i>NAT-T_2</i>
Direction	Routing -> QoS -> QoS Classification - > New	Outgoing
High priority class	Routing -> QoS -> QoS Classification - > New	Enabled

### Enabling QoS on the WAN interface

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

# 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.

Discover Add device	Star						
	Show Interval ( devices Devices	p (min): 1 resu	ve Load Add devices Files				
Device Ex 🛛 📮	Devices (RNA	)			• ×	Device Properties	Д
Location O			▲▼ ⋧♦ ♣	2 📩 🗙 🕿	4	2↓	
All Devices	Product	Davias Name	ID Addresse	MAC Address	Action	IP-Configuration	
E- Route	Floduci	Device Name	IF Address	MAC Address	Action	Address Mode	Static IP address
	C RT1202	rt1202	192.168.0.254	00-A0-F9-0B-CF-71		Gateway	0.0.0.0
	· 🕑 RT1202	rt1202	192.168.0.254	00-A0-F9-21-EF-EE		Hostname	103 100 0 354
					)	IP Address	192.108.0.254
			IP-Settings			Subhel Mask	200.200.200.0
						Company Name	Unknown
				ID Co	44inac	Device Name	rt1202
				IF JE	tungs	Eleboss bin	V 7 9 Rev 5 (Beta 4)
						E File text, ger ez	V 7 9 Rev. 1 (Beta 2)
			Device Name:	rt1202		E File webpages.ez	V.7.9 Rev. 5 (Beta 4)
			Device Ivallie.			Firmware	V.7.9 Rev. 5 (Beta 4)
			Current Password:			Location	Unknown
			New Password:			MACAddress	00-A0-F9-0B-CF-71
			Show passwords in cle	ar text:		Monitoring	Yes
			IP configuration			Ping Device	Yes
			IF Conliguration			Product	RT1202
			IP Address:	10.10.10.1		Serial Number	HA1020004300000
			IP Address Mode:	Static IP addr	ess 👻	States	
			Subast Mask	255.255.255	0	Ambiguous IP Address	Yes
			Subriet Mask.	0.0.0.0		Discovered	12:04:26 PM
			Gateway:	0.0.0.0		IP configuration possible	MULTICAST
						Login	Failed
			📮 Save configuratio	n permanently		Password	Unsecure Password.
4				C Verify	Cancel	Address Mode	

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.

```
    Go to LAN -> IP Configuration -> Interfaces ->
```

Save configuration	<b>-</b>		Interfaces
System Management	-		
Physical Interfaces	-	Basic Parameters	
LAN	-	Address Mode	Static ○ DHCP
IP Configuration VLAN	_		IP Address Netmask
Routing	-	IP Address / Netmask	10.10.11.1 255.255.252 🗐
WAN	-		Add
VPN	-	Interface Mode	⊙ Untagged ◯ Tagged (VLAN)
Firewall	-	MAC Address	ΩΩ:a0:f9:21:efee
VolP	-		
Local Services	-		Advanced Settings
Maintenance	-		OK Cancel
External Reporting	-		

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.

Save configuration					Interfaces			
Assistants	-							
System Management	-							
Physical Interfaces	-	Interface	IP Address	Netmask	Address Mode	Status	Action	
LAN		en1-0	10.10.10.2	255.255.255.0	Static	0	14	ø
IP Configuration		en1-4	10.10.11.2	255.255.255.252	Static	0	1	
VLAN								
Routing	-			(	New			

#### 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		
Assistants 🔹				
System Management 🔹 👻				
Physical Interfaces 🔹 👻	BRRP Advertisement Interface			
LAN 🔫	Ethernet Interface	en1-0 💌		
Routing 🔺		IP Address Netmask		
Routes	IP Address	10.10.10.1 255.255.255.0		
NAT				
RIP	BRRP Monitored Interface			
Load Balancing	Virtual Router Interface	New Virtual Interface based on en1-0		
Multicast		D Address Nitreat		
QoS				
BRRP	Virtual Router IP Address	1192.168.0.254 [255.255.255.0		
NAN -		Add		
VPN -	Virtual Router ID	1 💌		
Firewall 🔹				
VolP 👻	Virtual Router Priority	254		
Local Services 🔹 👻		Advanced Settings		
Maintenance 🔹 👻				
External Reporting				

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.

Save configuration		Virtual Routers VR Synchronisation Options
Assistants 👻		
System Management 🔹 👻		
Physical Interfaces 🔹 👻	BRRP Advertisement Interface	
LAN 🔫	Ethernet Interface	en1-4
Routing		IP Address Netmask
Routes	IP Address	10.10.11.1 255.255.252
NAT	BRRP Monitored Interface	
Load Balancing	Virtual Router Interface	en1-0-1
Multicast		IP Address Netmask
QoS	Virtual Pouter IP Addrose	212 212 212 1 255 255 248
BRRP	Vinual Router IF Address	
WAN -		Add
VPN -	Virtual Router ID	2 💌
Firewall 👻	Virtual Router Priority	254 🗸
VolP 👻	· · · · · · · · · · · · · · · · · · ·	
Local Services 🔹 👻		Advanced Settings
Maintenance 🔹 👻	OK Cancel	

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.

Save configuration	5		Virtual Routers VR Synchronisation Option
Assistants	-		
System Management	-		
Physical Interfaces	-	Basic Parameters	
LAN	-	Enable BRRP	Enabled
Routing			
Routes			OK Cancel
NAT			
RIP			
Load Balancing			
Multicast			
QoS			
BRRP			

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.

Save configuration				Virtual Routers	R Synchronisation	ptions		
Assistants	-							
System Management	-							
Physical Interfaces	-			Virtua	Routers			
		VR ID	Virtual Router	Advertisement interface	IP Address	Status	Action	
LAN	•	1	en1-0-1	en1-0	10.10.10.1	master	1 4	<del></del> <b> </b>
Routing	-	2	en1-4-1	en1-4	10.10.11.1	master	11	龠
Routes								(Jane)
NAT					lew )			
RIP								
Load Balancing								
Multicast								
QoS								
RPPP								

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 0: 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_0: 212.212.212.0
19:47:54 NOTICE/BRP: 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.

Save configuration			Virtual Routers VR Synchronisation Options
Assistants	-		
System Management	-		
Physical Interfaces	-	Basic Parameters	
LAN	-	Monitoring VR / Interface	
Routing	•	Monitoring Mode	BRRP
Routes	_	Virtual Router ID	1
RIP		Synchronisation VR / Interface	
Load Balancing		Synchronisation Mode	BRRP 💌
Multicast QoS	-	Virtual Router ID	2
BRRP			
WAN	•		OK Cancel

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:

Save configuration				Virtual Routers VR Svn	chronisation Options			
Assistants	-			<u> </u>				
System Management	-							
Physical Interfaces	•	Monitoring VR	Monitoring Interface	Synchronisation VR	Synchronisation Interface	Action		ĺ
-AN	-	1	en1-0-1	2	en1-4-1	Sync	窗	ľ
Routing		2	en1-4-1	1	en1-0-1	Sync	寙	
Routes				Maur				
NAT				New				
RIP								
Load Balancing								
Multicast								
QoS								
BRRP								

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. 10.10.10.1
IP address	Dime Manager -> IP Settings	e.g. 10.10.10.2

#### **IP** configuration

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

### Configuration of the virtual router

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

#### Enable BRRP configuration

Field	Menu	Value
Enable BRRP	Routing -> BRRP -> Options	Enabled

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

### Synchronisation of the virtual routers

# 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.

ave configuration		Internet Conn	ections
istants 🔺			
st steps			
ernet Access	Description	T-Mobile - UMTS	Keine Hilfe verfügbar.
DIP PBX in LAN	GPRS/UMTS Interface	Slat 6 Unit 0 UMTS 💌	
em Management 🔹 👻	Select your Internet Service	Provider (ISD) from the list	Copyright@ 2007-2010 Funkwerk Enterprise Communications GmbH
sical Interfaces 🔹 👻	Ture	Deadoficed at	
<del>ب</del> ا	туре	Predelined Y	_
working 👻	Country	Germany 💌	
ating Protocols 🛛 👻	Internet Service Provider	T-Mobile - UMTS 💌	
lticast 👻	Please enter the UMTS Provi	der data:	
IN <del>-</del>	UMTS PIN	•••••	
<del>ب</del>	Select the connection mode:		
wall 👻	Always active	Enabled	
• •			- 1
al Services 👻			
ntenance 👻			
ernal Reporting 🛛 👻			
nitoring 👻			
		OK Cancel	

#### 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:

Go to Physical Interfaces -> UMTS/HSDPA -> UMTS/HSDPA/HSUPA ->

Save configuration		UMTS/HSDPA/HSUPA		
Assistants	-			
System Management	-			
Physical Interfaces		Basic Settings		
Ethernet Ports		UMTS/HSDPA/HSUPA Status	✓ Enabled	
	-	Modem Status	Active	
Networking	-	Actual Network	UMTS	
Routing Protocols	-	Network Quality		
Multicast	-	Preferred Network Type	Automatic	
WAN	-	Incoming Service Type	◯ Disabled ⑧ ISDN Login ◯ PPP Dialin ◯ IPSec	
/PN	-	SIM Card Uses PIN	•••••	
irewall	-	Fallhack Number	+499119731414	
/oIP	-			
Local Services	-	APN (Access Point Name)	internet.t-mobile	
Maintenance	-			
External Reporting	-			



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 &
10:49:56 INFO/MODEM: usbTTY0: 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: usbTTY0: 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: usbTTY0: Registered 26201 (T-Mobile D) (AcT = GSM)
10:50:09 INFO/MODEM: usbTTY0: 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.

\_\_\_\_\_

Debug messages during the incoming ISDN login connection:

```
rs232bu+:> debug all &
10:50:41 DEBUG/USB: usbTTY0: serial state notification - ring ind.
10:50:41 DEBUG/MODEM: usbTTY0: switch state P1 -> R0
10:50:41 DEBUG/MODEM: usbTTY0: Data call from '+4991196730' - data mode state incoming
10:50:41 DEBUG/MODEM: usbTTY0: Modem incomming call from <+4991196730>
10:50:41 DEBUG/MODEM: usbTTY0: Modem incomming call from <+4991196730>
10:50:41 INFO/ISDN: isdnlogind: accept call from <+4991196730>
10:50:41 DEBUG/MODEM: usbTTY0: switch state R1 -> A0
10:50:41 DEBUG/MODEM: usbTTY0: attach to channel 1 - incoming
10:50:43 INFO/MODEM: usbTTY0: Accept call from '+4991196730' ==> (CONNECT 9600)
10:50:43 DEBUG/MODEM: usbTTY0: switch state D1 -> D1
10:50:43 DEBUG/MODEM: usbTTY0: 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	UMTS
Description	Assistant -> Internet Access -> Next	T-Mobile - UMTS
GPRS/UMTS Inter- face	Assistant -> Internet Access -> Next	Slot 6 Unit 0 UMTS
Internet Service Pro- vider	Assistant -> Internet Access -> Next	e.g. T-Mobile - UMTS
UMTS PIN	Assistant -> Internet Access -> Next	e. g. 0000

#### Configure the UMTS fallback number

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