funkwerk
enterprise communications

bintec Workshop

Configuration of ISDN and Modem Backup

Version 0.9

Purpose

This document is part of the user's guide to the installation and configuration of bintec gateways running software release 7.1.4 or later. For up-to-the-minute information and instructions concerning the latest software release, you should always read our **Release Notes**, especially when carrying out a software update to a later release level. The latest **Release Notes** can be found at www.funkwerk-ec.com.

Liability

While every effort has been made to ensure the accuracy of all information in this manual, Funkwerk Enterprise Communications GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information, changes and **Release Notes** for bintec gateways can be found at www.funkwerk-ec.com.

As multiprotocol gateways, bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Funkwerk Enterprise Communications GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

bintec and the bintec logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

Copyright

Guidelines and standards

bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

You will find detailed information in the Declarations of Conformity at www.funkwerk-ec.com.

How to reach Funkwerk Enterprise Communications GmbH

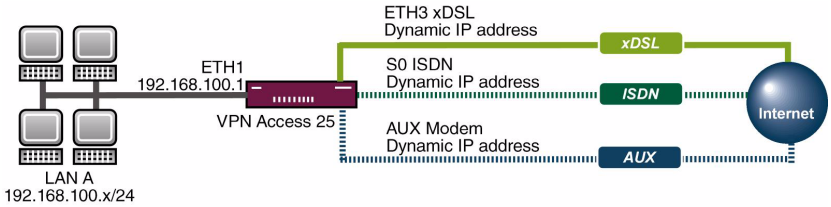
Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.funkwerk-ec.com	Bintec France 6/8 Avenue de la Grande Lande F-33174 Gradignan France Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr

1 Introduction

The configuration of backup connections over ISDN and modem using a Bintec VPN Access 25 gateway (software version 7.1.6 patch 3) is described in the following chapters. The Setup Tool is used for the configuration.

1.1 Scenario

The Internet traffic normally runs over the xDSL access. A connection is to be set up over the ISDN access if the xDSL connection fails. If the ISDN connection also fails, a backup connection is set up over the AUX interface. The dial backup is controlled via the metric variable.



1.2 Requirements

The following are required for the configuration:

- A Bintec VPN Access 25 gateway.
- xDSL Internet access.
- ISDN Internet access.
- Analog Internet access.
- Analog modem with suitable cables.
- Connect your LAN to the ETH1 interface of your gateway.

- A configured PC (see User's Guide Part **Access and Configuration**).
- Connect your modem to the AUX connection (console).

Note

Use the Bintec **User's Guide** and the Bintec FAQs to configure the Internet accesses.

2 Configuration of WAN Partners

Note

The configuration of WAN partners is not dealt with in detail here. Use the Bintec **User's Guide** or the relevant Bintec FAQs for this purpose.

Three WAN partners are configured for Internet accesses over DSL, ISDN and AUX/analog. The priority of the Internet accesses is defined by the metric of the default routes.

2.1 Changing the Metric

- Go to ***IP*** ➜ ***ROUTING*** ➜ ***INTERFACE.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][ROUTING]: IP Routing                                        vpn25

 The flags are:U (Up), D (Dormant), B (Blocked),
               G (Gateway Route), I (Interface Route),
               S (Subnet Route), H (Host Route), E (Extended Route)

 Destination  Gateway        Mask          Flags Met. Interface     Pro
 192.168.0.0  192.168.0.254 255.255.255.0       0    en0-1         loc
 default                    0.0.0.0       DI    1    T-Online      loc
 default                    0.0.0.0       DI    2    Freenet/ISDN  loc
 default                    0.0.0.0       DI    3    Freenet/Modem loc



     ADD                ADDEXT              DELETE              EXIT
```

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IP][ROUTING][EDIT]                                              vpn25

  Route Type                 Default route
  Network                     WAN without transit network


  Partner / Interface        T-Online

  Metric                     1

          SAVE                                  CANCEL
```

The following field is relevant:

Field	Meaning
Metric	Determines the priority of the route.

Table 2-1: Relevant field in ***IP*** ➜ ***ROUTING*** ➜ ***EDIT***

Proceed as follows to define the necessary settings:

- Set ***METRIC*** to *1*.
- Leave all the other settings as they are.
- Press **SAVE** to confirm your settings.

Repeat the procedure for the ISDN interface with ***METRIC*** *2* and for the modem interface with ***METRIC*** *3*.

2.2 Changing Static Short Hold

Note

The static short hold times of the ISDN and AUX WAN partners should be kept as short as possible, e.g. *120* seconds.

- Go to ***WAN PARTNER*** ➜ ***PARTNERNAME*** ➜ ***ADVANCED SETTINGS.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][EDIT][ADVANCED]: Advanced Settings (Freenet/Modem)          vpn25

  Callback                                  no
  Static Short Hold (sec)                   120
  Idle for Dynamic Short Hold (%)           0
  Delay after Connection Failure (sec)      10
  Layer 1 Protocol                          Modem Profile 1

  Channel Bundling                          no


  Extended Interface Settings (optional) >


  Special Interface Types                   none

            OK                                      CANCEL
```

The following field is relevant:

Field	Meaning
Static Short Hold	Time between the last data packet sent and clearing the connection.

Table 2-2: Relevant field in ***WAN PARTNER*** ➜ ***PARTNERNAME*** ➜ ***ADVANCED SETTINGS***

Proceed as follows to define the necessary settings:

- Enter a time under ***STATIC SHORT HOLD (SEC)***, e.g. *120*.
- Leave all the other settings as they are.
- Press **OK** to confirm your settings.
- Press **SAVE** to confirm your settings.

Return to the main menu and finally save your new configuration in the flash memory with **EXIT** and **Save as boot configuration and exit**.

3 PPP Table

In the ***PPPTABLE*** you can set the entry ***MAXRETRIES*** to define the number of dialing attempts before the interface changes to the *blocked* state. Enter the following in the command line of the gateway:

```
vpn25:>ppptable
```

```
inx IfIndex(ro)         Type(*rw)           Encapsulation(-rw)
    Keepalive(rw)       Timeout(rw)         Compression(rw)
    Authentication(rw)  AuthIdent(rw)       AuthSecret(rw)
    IpAddress(rw)       RetryTime(rw)       BlockTime(rw)
    MaxRetries(rw)      ShortHold(rw)       InitConn(rw)
    MaxConn(rw)         MinConn(rw)         Callback(rw)
    Layer1Protocol(rw)  LoginString(rw)     VJHeaderComp(rw)
    Layer2Mode(rw)      DynShortHold(rw)    LocalIdent(rw)
    DNSNegotiation(rw)  Encryption(rw)      LQMonitoring(rw)
    IpPoolId(rw)        SessionTimeout(rw)  Layer1DiscDelay(rw)

 01 10002               isdn_dialup         ppp
    off                 3000                none
    both
    static              4                   300
    5                   20                  1
    1                   1                   disabled
    data_64k                                disabled
    auto                0
    enabled             none                off
    0                   0                   enabled

vpn25:biboPPPTable>
```

Enter the following to change the MaxRetries value:

```
vpn25:biboPPPTable>MaxRetries:1=1
```

You have now made all the necessary settings.

4 Result

This configuration gives you two backup connections that can be activated when required.

4.1 Test

You can trace how the backup connections are set up for each type of failure by entering a `debug all` in the command line of the gateway. To simulate a failure, remove the cable for the respective connection from the interface.

Enter the following in the command line of the gateway:

```
vpn25:> debug all
```

xDSL connection

```
00:00:17 INFO/INET: dialup if 10001 prot 1 192.168.0.2:2048-
>1.1.1.1:16731
00:00:17 DEBUG/PPP: T-Online: send PPPoE Active Discovery Initiation
(PADI), interface: 300
00:00:17 DEBUG/PPP: T-Online 1/0/2/1: PPPoE call identified
00:00:18 DEBUG/PPP: T-Online 1/6523/2/5: PPPoE session established
00:00:18 DEBUG/PPP: Layer 1 protocol pppoe
00:00:18 DEBUG/PPP: T-Online: set ifSpeed, number of active connec-
tions: 0/0/0
00:00:18 DEBUG/PPP: T-Online: set ifSpeed, number of active connec-
tions: 1/1/1
00:00:18 DEBUG/PPP: T-Online: outgoing connection established
00:00:18 INFO/PPP: T-Online: local IP address is 84.128.81.243, remote
is 217.5.98.7
00:00:18 DEBUG/INET: NAT: new outgoing session on ifc 10001 prot 1
192.168.0.2:512/84.128.81.243:32769 -> 1.1.1.1:0
```

DSL link failed

```
00:00:22 INFO/ETHER: en0-3: link down
00:00:22 DEBUG/PPP: T-Online 1/6523/2/6: PPPoE session terminated
00:00:22 DEBUG/PPP: T-Online: set ifSpeed, number of active connec-
tions: 0/0/0
00:00:22 INFO/PPP: T-Online: outgoing connection closed, duration 4
sec, 131 bytes received, 271 bytes sent, 0 charging units, 0 charging
amounts
00:00:22 INFO/INET: dialup if 10001 prot 1 192.168.0.2:2048-
>1.1.1.1:16475
00:00:23 DEBUG/PPP: T-Online: send PPPoE Active Discovery Initiation
(PADI), interface: 300
00:00:23 DEBUG/PPP: T-Online 2/0/2/1: PPPoE call identified
00:00:49 DEBUG/INET: NAT: delete session on ifc 10001 prot 1
192.168.0.2:512/84.128.81.243:32769 <-> 1.1.1.1:0
00:00:53 ERR/PPP: T-Online: no response to setup, dialout failed
00:00:53 INFO/PPP: interface T-Online is blocked for 120 seconds
00:00:53 ERR/PPP: delete channel in state <1>
```

ISDN connection

```
00:00:53 INFO/INET: dialup if 10002 prot 1 192.168.0.2:2048->1.1.1.1:16475
00:00:53 DEBUG/PPP: Freenet/ISDN: dial number <00101901929>
00:00:57 DEBUG/PPP: Layer 1 protocol hdlc, 64000 bit/sec
00:00:57 DEBUG/PPP: Freenet/ISDN: set ifSpeed, number of active connections: 0/0/0
00:00:57 DEBUG/PPP: Freenet/ISDN: set ifSpeed, number of active connections: 1/1/1
00:00:57 DEBUG/PPP: Freenet/ISDN: outgoing connection established
00:00:57 INFO/PPP: Freenet/ISDN: local IP address is 213.7.0.51, remote is 62.104.219.38
00:00:57 DEBUG/INET: NAT: new outgoing session on ifc 10002 prot 1
192.168.0.2:512/213.7.0.51:32770 -> 1.1.1.1:0
00:00:59 INFO/INET: NAT: refused incoming session on ifc 10002 prot 6 213.7.0.51:445 <-
213.7.19.119:3091
00:01:00 INFO/INET: NAT: refused incoming session on ifc 10002 prot 6 213.7.0.51:445 <-
213.7.19.119:3091
00:01:01 DEBUG/ISDN: stack 0: deactivate
00:01:11 ERR/ISDN: stack 0: MDL_ERROR I
00:01:15 INFO/ACCT: ISDN:
01.01.1970,00:00:54,00:01:15,18,313,729,11,21,,O,850,00101901929,7/0,0,06,Freenet/ISDN
00:01:15 ERR/ISDN: stack 0: MDL_ERROR G
00:01:15 DEBUG/PPP: Freenet/ISDN: set ifSpeed, number of active connections: 0/0/0
00:01:15 INFO/PPP: Freenet/ISDN: outgoing connection closed, duration 18 sec, 280 bytes
received, 666 bytes sent, 0 charging units, 0 charging amounts
00:01:17 DEBUG/ISDN: stack 0: TEI remove
00:01:20 INFO/INET: dialup if 10002 prot 1 192.168.0.2:2048->1.1.1.1:15195
00:01:20 DEBUG/PPP: Freenet/ISDN: dial number <00101901929>
00:01:20 DEBUG/ISDN: stack 0: TEI remove
00:01:27 DEBUG/PPP: Freenet/ISDN: dial number <00101901929>
00:01:32 DEBUG/ISDN: stack 0: TEI remove
00:01:33 DEBUG/PPP: Freenet/ISDN: dial number <00101901929>
00:01:38 DEBUG/ISDN: stack 0: TEI remove
00:01:41 DEBUG/PPP: Freenet/ISDN: dial number <00101901929>
00:01:45 DEBUG/INET: NAT: delete session on ifc 10002 prot 1 192.168.0.2:512/213.7.0.51:32770 <-
> 1.1.1.1:0
00:01:46 DEBUG/ISDN: stack 0: TEI remove
00:01:48 DEBUG/PPP: Freenet/ISDN: dial number <00101901929>
00:01:53 DEBUG/ISDN: stack 0: TEI remove
00:01:56 DEBUG/PPP: Freenet/ISDN: dial number <00101901929>
00:02:01 DEBUG/ISDN: stack 0: TEI remove
00:02:02 INFO/PPP: interface Freenet/ISDN is blocked for 120 seconds
```

Modem connection

```
00:02:02 INFO/INET: dialup if 10003 prot 1 192.168.0.2:2048-
>1.1.1.1:15195
00:02:02 DEBUG/PPP: Freenet/Modem: dial number <00101901929>
00:02:02 DEBUG/TTY: Modem Dialout to 00101901929
00:02:22 DEBUG/MODEM: ASYHDLC: No HW Support for asyHDLC b->value=8
00:02:22 DEBUG/PPP: Layer 1 protocol ppp_modem, profile 1
00:02:22 DEBUG/PPP: Freenet/Modem: set ifSpeed, number of active con-
nections: 0/0/0
00:02:33 DEBUG/TTY: Modem connect (11) CONNECT
52000/ARQ/V90/LAPM/V42BIS
00:02:36 ERR/MODEM: ASYHDLC:RX FRAME TO SMALL 1
00:02:37 DEBUG/PPP: Freenet/Modem: set ifSpeed, number of active con-
nections: 1/1/1
00:02:37 DEBUG/PPP: Freenet/Modem: outgoing connection established
00:02:39 INFO/PPP: Freenet/Modem: local IP address is 213.7.46.121,
remote is 62.104.219.41
00:02:39 DEBUG/INET: NAT: new outgoing session on ifc 10003 prot 1
192.168.0.2:512/213.7.46.121:32771 -> 1.1.1.1:0
```

DSL link restored

```
00:02:41 INFO/ETHER: en0-3: (100BaseTx/halfdup) link up
00:02:42 INFO/ETHER: en0-3: (10BaseT/halfdup) link up
00:02:47 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
213.7.93.128:1954
00:02:50 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
213.7.93.128:1954
00:02:55 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:1433 <-
213.6.135.148:1801
00:02:57 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:1433 <-
213.6.135.148:1801
00:02:57 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
213.7.75.16:4017
00:02:58 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:135 <-
213.7.194.134:2274
00:03:11 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
213.7.21.129:3059
00:03:14 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
213.7.21.129:3059
00:03:25 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
213.7.9.86:1977
00:03:28 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
213.7.9.86:1977
00:03:29 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
213.7.9.86:1977
00:03:31 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
81.169.226.216:1257
00:03:31 INFO/INET: dialup if 10001 prot 1 192.168.0.2:2048->1.1.1.1:13659
00:03:31 DEBUG/PPP: T-Online: send PPPoE Active Discovery Initiation (PADI), interface: 300
00:03:31 DEBUG/PPP: T-Online 3/0/2/1: PPPoE call identified
00:03:31 DEBUG/PPP: T-Online 3/6833/2/5: PPPoE session established
00:03:31 DEBUG/PPP: Layer 1 protocol pppoe
00:03:31 DEBUG/PPP: T-Online: set ifSpeed, number of active connections: 0/0/0
00:03:32 DEBUG/PPP: T-Online: set ifSpeed, number of active connections: 1/1/1
00:03:32 DEBUG/PPP: T-Online: outgoing connection established
00:03:32 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
81.169.226.216:1257
00:03:32 INFO/PPP: T-Online: local IP address is 217.229.167.7, remote is 217.5.98.7
00:03:33 INFO/INET: NAT: refused incoming session on ifc 10003 prot 6 213.7.46.121:445 <-
81.169.226.216:1257
00:03:36 DEBUG/INET: NAT: new outgoing session on ifc 10001 prot 1
192.168.0.2:512/217.229.167.7:32772 -> 1.1.1.1:0
vpn25:>
```

Explanation:

The debug extract shows that the ISDN connection is set up when the DSL connection fails, as the ISDN connection has a higher metric (2) than the analog Internet access. After the ISDN connection failed, the analog connection was selected; the DSL connection was still not available. Once the DSL link became active again, the DSL connection was restored because of its higher metric (1). The modem connection remained set up until the static short hold expired.

4.2 Overview of Configuration Steps

Field	Menu	Description	Compulsory field
Metric	***IP*** ➜ ***ROUTING*** ➜ ***INTERFACE PARTNERNAME***	e.g. *1*	Yes
Metric	***IP*** ➜ ***ROUTING*** ➜ ***INTERFACE*** ➜ ***PARTNERNAME***	e.g. *2*	Yes
Metric	***IP*** ➜ ***ROUTING*** ➜ ***INTERFACE*** ➜ ***PARTNERNAME***	e.g. *3*	Yes
Static Short Hold (sec)	***WAN PARTNER*** ➜ ***PARTNERNAME*** ➜ ***ADVANCED SETTINGS***	e.g. *120*	