funkwerk
enterprise communications

bintec Workshop

Router Monitoring

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

How to monitor your router is explained in the following chapters. The possible methods presented include System Logging, E-Mail Alert and Activity Monitor.

1.1 Requirements

The following are required for the configuration:

- Basic configuration of router. The basic configuration using the Wizard is recommended.
- A boot image of version 7.1.4 or later.
- The configuration requires a mail server for E-Mail Alert.
- Brickware version 7.1.4 or later for System Logging and Activity Monitor.

2 Configuration

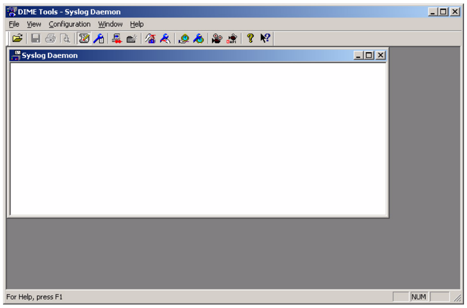
2.1 System Logging

The Syslog Daemon is used to log the debug messages and accounting information on a computer.

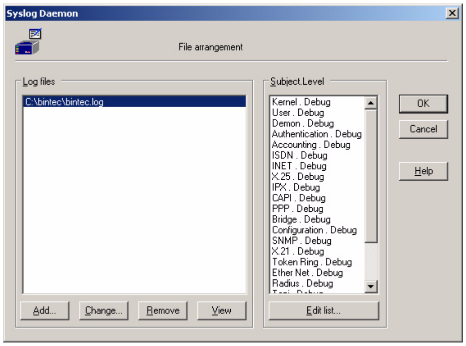
Start the **DIME Tools** under Windows in the following menu:

START -> PROGRAMME -> BRICKWARE -> DIME TOOLS.

Make sure the Syslog Daemon is running once you have opened the **DIME Tools**. Start the Syslog Daemon by pressing the key combination **CTRL** + **L** in the **DIME Tools**.



The configuration is made in the ***CONFIGURATION* ➜ *SYSLOG DAEMON*** menu.


Syslog Daemon

File arrangement

Log files

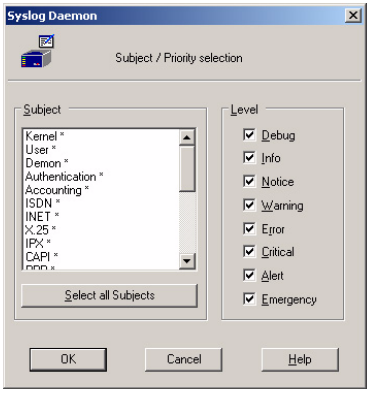
C:\bintec\bintec.log

Subject.Level

Kernel . Debug
User . Debug
Demon . Debug
Authentication . Debug
Accounting . Debug
ISDN . Debug
INET . Debug
X.25 . Debug
IPX . Debug
CAPI . Debug
PPP . Debug
Bridge . Debug
Configuration . Debug
SNMP . Debug
X.21 . Debug
Token Ring . Debug
Ether Net . Debug
Radius . Debug

Proceed as follows to configure an entry:

- Click **Add** and enter a file name, e.g. *bintec.log*.
- Go to the **Edit List** field to continue the configuration.



Syslog Daemon

Subject / Priority selection

Subject

Kernel *
User *
Demon *
Authentication *
Accounting *
ISDN *
INET *
X.25 *
IPX *
CAPI *
PPP *

Level

☑ Debug
☑ Info
☑ Notice
☑ Warning
☑ Error
☑ Critical
☑ Alert
☑ Emergency

Proceed as follows if you would like to log all the messages sent by the router:

- Click the **Select all Subjects** field.
- Tag *Debug*.
- Leave both windows by pressing **OK**.

You must add an entry in the following menu to make the router send the debug messages to the Syslog server:

SYSTEM ➜ EXTERNAL SYSTEM LOGGING ➜ ADD

```
VPN Access 25 Setup Tool                          Bintec Access Networks GmbH
[SYSTEM] [LOGGING] [ADD]                                          Head Office

          Log Host                    192.168.0.2
          Level                       debug
          Facility                    local0
          Type                        all
          Timestamp                   none


        SAVE                                CANCEL
```

The following fields are relevant:

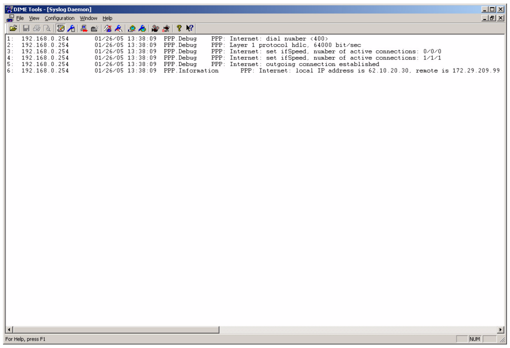
Field	Meaning
Log Host	Enter the IP address of the Syslog server.
Level	Select the type of messages you wish to send.

Table 2-1: Relevant fields in ***SYSTEM*** ➜ ***EXTERNAL SYSTEM LOGGING*** ➜ ***ADD***

Proceed as follows to configure the entry:

- Enter the IP address of the server under ***LOG HOST***, e.g. *192.168.0.2*.
- Set ***LEVEL*** to *debug*.

If the router is active, you should now receive a number of messages in the Syslog server window.



DIME Tools - [Syslog Daemon]
File View Configuration Window Help
For Help, press F1
NUM

```
1:  192.168.0.254       01/26/05 13:38:09  PPP.Debug    PPP: Internet: dial number <400>
2:  192.168.0.254       01/26/05 13:38:09  PPP.Debug    PPP: Layer 1 protocol hdlc, 64000 bit/sec
3:  192.168.0.254       01/26/05 13:38:09  PPP.Debug    PPP: Internet: set ifSpeed, number of active connections: 0/0/0
4:  192.168.0.254       01/26/05 13:38:09  PPP.Debug    PPP: Internet: set ifSpeed, number of active connections: 1/1/1
5:  192.168.0.254       01/26/05 13:38:09  PPP.Debug    PPP: Internet: outgoing connection established
6:  192.168.0.254       01/26/05 13:38:09  PPP.Information      PPP: Internet: local IP address is 62.10.20.30, remote is 172.29.209.99
```

All the messages the router sends to the Syslog server can also be requested in real time in the shell.

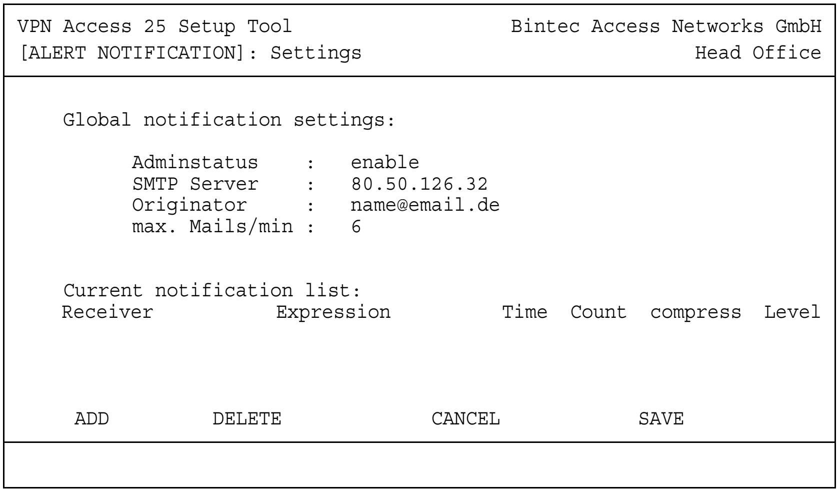
This is done by typing the following in the SNMP shell: `debug all&`

The last messages can also be seen in the following table, where the messages are saved: `biboAdmSyslogTable`

The table parameter Message is important here, which you can also request individually in the shell to clearly show the messages.

2.2 Email Alert

You can configure the router to send you an e-mail if it sends certain debug messages. Go to the following menu for the configuration: ***Monitoring and Debugging*** ➜ ***Email Alert***.



```
VPN Access 25 Setup Tool                          Bintec Access Networks GmbH
[ALERT NOTIFICATION]: Settings                                    Head Office

    Global notification settings:

          Adminstatus    :   enable
          SMTP Server    :   80.50.126.32
          Originator     :   name@email.de
          max. Mails/min :   6


    Current notification list:
    Receiver          Expression          Time  Count  compress  Level



     ADD         DELETE             CANCEL             SAVE
```

The following fields are relevant:

Field	Meaning
SMTP Server	Enter the IP address of your mail server.
Originator	Enter the sender's e-mail address.

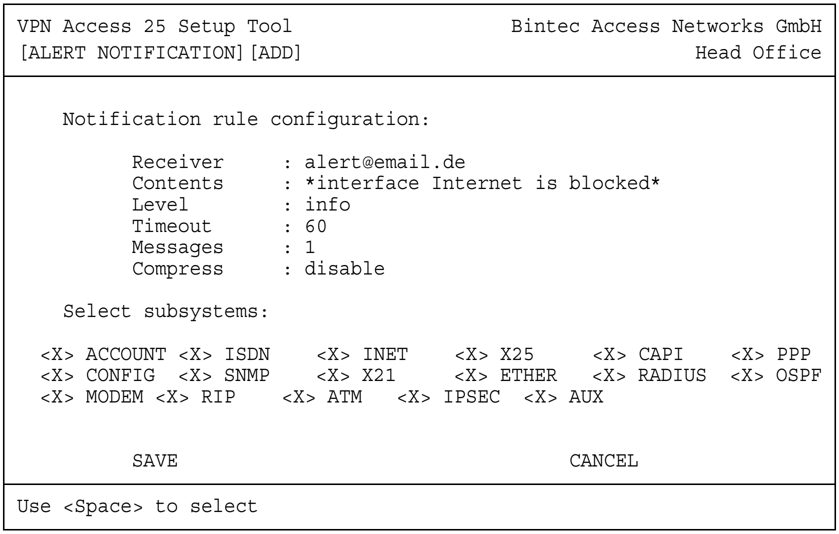
Table 2-2: Relevant fields in ***Monitoring and Debugging*** ➜ ***Email Alert***

Proceed as follows to configure the entry:

- Enter an address for ***SMTP Server***, e.g. *80.50.126.32*.
- Enter an address under ***Originator***, e.g. *name@email.de*.

Now configure a default with the critical message that is to cause a mail to be sent. Go to the following menu to create an entry for this purpose:

■ ***Monitoring and Debugging ➜ Email Alert ➜ ADD***



```
VPN Access 25 Setup Tool                   Bintec Access Networks GmbH
[ALERT NOTIFICATION][ADD]                                  Head Office

    Notification rule configuration:

          Receiver     : alert@email.de
          Contents     : *interface Internet is blocked*
          Level        : info
          Timeout      : 60
          Messages     : 1
          Compress     : disable

    Select subsystems:

  <X> ACCOUNT <X> ISDN    <X> INET    <X> X25     <X> CAPI    <X> PPP
  <X> CONFIG  <X> SNMP    <X> X21     <X> ETHER   <X> RADIUS  <X> OSPF
  <X> MODEM <X> RIP    <X> ATM   <X> IPSEC  <X> AUX


          SAVE                                    CANCEL

Use <Space> to select
```

The following fields are relevant:

Field	Meaning
Receiver	Enter the e-mail address that is to receive the alert mail.
Contents	For entering the debug message that causes the router to send a mail.
Level	This is the level at which the message appears.

Table 2-3: Relevant fields in ***Monitoring and Debugging ➜ Email Alert ➜ ADD***

Proceed as follows to configure the entry:

- Enter an address for ***Receiver***, e.g. *alert@email.de*.
- Enter a message for ***Contents***, e.g. **interface Internet is blocked**.
- Set ***Level***, e.g. to *info*.

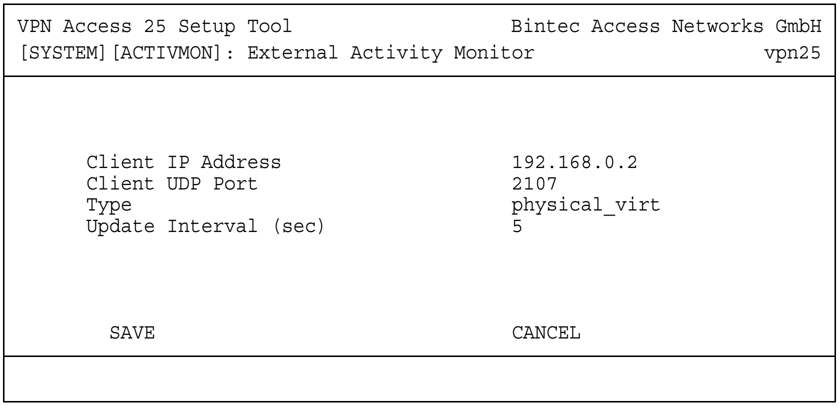
Note

Bear in mind that without the use of wildcards, e.g. "*", only those messages that correspond exactly to the entry fulfill the condition.

2.3 Activity Monitor

Brickware contains the **Activity Monitor**, which is intended for monitoring and administration of interfaces under Windows. You must first activate the **Activity Monitor** in the router before you can use it.

Go to the following menu for the configuration: ***SYSTEM* ➜ *EXTERNAL ACTIVITY MONITOR***



```
VPN Access 25 Setup Tool                   Bintec Access Networks GmbH
[SYSTEM][ACTIVMON]: External Activity Monitor                    vpn25



      Client IP Address                     192.168.0.2
      Client UDP Port                       2107
      Type                                  physical_virt
      Update Interval (sec)                 5



        SAVE                                CANCEL
```

The following fields are relevant:

Field	Meaning
Client IP Address	This is the IP address of the Windows PC.
Type	Determine which type of interface you would like to monitor.
Update Interval (sec)	The update interval in seconds.

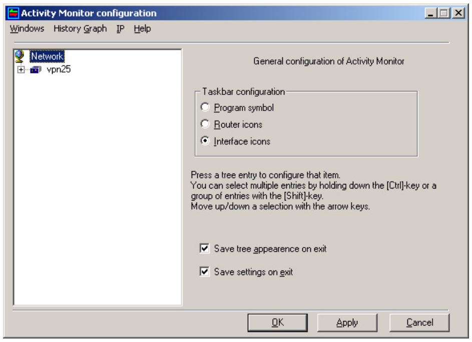
Table 2-4: Relevant fields in ***SYSTEM* ➜ *EXTERNAL ACTIVITY MONITOR***

Proceed as follows to configure the entry:

- Enter an address under ***CLIENT IP ADDRESS***, e.g. *192.168.0.2*.
- Set ***TYPE*** to *physical_virt*.
- Enter *5* for ***UPDATE INTERVAL (SEC)***.

If you have left the menu with **SAVE**, you can start the **Activity Monitor**.

You should now see your active router in the list.



General configuration of Activity Monitor

Taskbar configuration

○ Program symbol
○ Router icons
● Interface icons

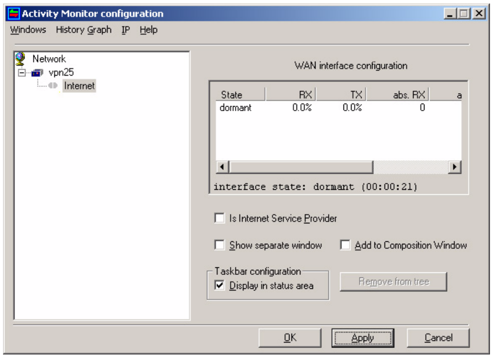
Press a tree entry to configure that item.
You can select multiple entries by holding down the [Ctrl]-key or a group of entries with the [Shift]-key.
Move up/down a selection with the arrow keys.

☑ Save tree appearence on exit

☑ Save settings on exit

Proceed as follows to show the Internet access permanently in the task bar to indicate the current status of the interface:

- Extend the view by pressing **+** before VPN25.
- Tag the Internet access.
- Place a tick against *Display in status area*.



WAN interface configuration

State	RX	TX	abs. RX	a
dormant	0.0%	0.0%	0	

```
interface state: dormant (00:00:21)
```

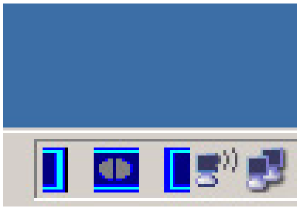
☐ Is Internet Service Provider

☐ Show separate window ☐ Add to Composition Window

Taskbar configuration

☑ Display in status area

As soon as you press the **Apply** button, your task bar changes and shows a symbol for the status of the Internet interface.



3 Overview of Configuration Steps

System Logging

Field	Menu	Description
Log Host	***SECURITY*** **➜** ***EXTERNAL SYSTEM LOGGING*** **➜** ***ADD***	e.g. *192.168.0.2*
Level	***SECURITY*** **➜** ***EXTERNAL SYSTEM LOGGING*** **➜** ***ADD***	*debug*

Email Alert

Field	Menu	Description
SMTP Server	***MONITORING AND DEBUGGING*** **➜** ***EMAIL ALERT***	e.g. *80.50.126.32*
Originator	***MONITORING AND DEBUGGING*** **➜** ***EMAIL ALERT***	e.g. *name@email.de*
Receiver	***MONITORING AND DEBUGGING*** **➜** ***EMAIL ALERT*** **➜** ***ADD***	e.g. *alert@email.de*
Contents	***MONITORING AND DEBUGGING*** **➜** ***EMAIL ALERT*** **➜** ***ADD***	e.g. *interface Internet is blocked*
Level	***MONITORING AND DEBUGGING*** **➜** ***EMAIL ALERT*** **➜** ***ADD***	e.g. info

Activity Monitor

Field	Menu	Description
Client IP Address	***SYSTEM*** **➜** ***EXTERNAL ACTIVITY MONITOR***	e.g. *192.168.0.2*
Type	***SYSTEM*** **➜** ***EXTERNAL ACTIVITY MONITOR***	e.g. *physical_virt*
Update Interval (sec)	***SYSTEM*** **➜** ***EXTERNAL ACTIVITY MONITOR***	e.g. *5*