

# **MONITORING AND DEBUGGING**

Copyright © 11. April 2005 Funkwerk Enterprise Communications GmbH  
Bintec Benutzerhandbuch - X2250  
Version 1.0

**Ziel und Zweck** Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Bintec-Gateways ab Software-Release 7.1.16. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter [www.funkwerk-ec.com](http://www.funkwerk-ec.com).

**Haftung** Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie **Release Notes** für Bintec-Gateways finden Sie unter [www.funkwerk-ec.com](http://www.funkwerk-ec.com).

Als Multiprotokollgateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

**Marken** Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

**Copyright** Alle Rechte sind vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

**Richtlinien und Normen** Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter [www.funkwerk-ec.com](http://www.funkwerk-ec.com).

**Wie Sie Funkwerk Enterprise Communications GmbH erreichen**

Funkwerk Enterprise Communications GmbH  
Südwestpark 94  
D-90449 Nürnberg  
Deutschland

Telefon: +49 180 300 9191 0  
Fax: +49 180 300 9193 0  
Internet: [www.funkwerk-ec.com](http://www.funkwerk-ec.com)

Bintec France  
6/8 Avenue de la Grande Lande  
F-33174 Gradignan  
Frankreich

Telefon: +33 5 57 35 63 00  
Fax: +33 5 56 89 14 05  
Internet: [www.bintec.fr](http://www.bintec.fr)



<b>1</b>	<b>Menü Monitoring and Debugging</b> .....	<b>3</b>
<b>2</b>	<b>Untermenü ISDN Monitor</b> .....	<b>5</b>
<b>3</b>	<b>Untermenü ISDN Credits</b> .....	<b>9</b>
<b>4</b>	<b>Untermenü xDSL Credits</b> .....	<b>11</b>
<b>5</b>	<b>Untermenü Interfaces</b> .....	<b>13</b>
<b>6</b>	<b>Untermenü Messages</b> .....	<b>17</b>
<b>7</b>	<b>Untermenü Email Alert</b> .....	<b>19</b>
	7.1 Untermenü Authentication Settings .....	23
<b>8</b>	<b>Untermenü TCP/IP</b> .....	<b>25</b>
<b>9</b>	<b>Untermenü IPSec</b> .....	<b>27</b>
	9.1 Untermenü Global Statistics .....	27
	9.2 Untermenü IKE Security Associations .....	29
	9.3 Untermenü IPSec SA Bundles .....	31
<b>10</b>	<b>Untermenü OPSF</b> .....	<b>33</b>
<b>11</b>	<b>Untermenü BRRP</b> .....	<b>37</b>
<b>12</b>	<b>Untermenü SSH Daemon</b> .....	<b>41</b>
	<b>Index: Monitoring and Debugging</b> .....	<b>43</b>





Menü	Bedeutung
Messages	Zeigt Systemmeldungen an, die vom Logging und Accounting Mechanismus des Gateways generiert werden.
Email Alert	Je nach Konfiguration werden dem Administrator Emails gesendet, sobald relevante Syslog Messages auftreten.
TCP/IP	In diesem Menü wird der IP Traffic der einzelnen Protokolle überwacht.
IPSec	In diesem Menü werden globale IPSec Statistiken angezeigt, sowie die <b>IKE SECURITY ASSOCIATIONS</b> und die <b>IPSEC SA BUNDLES</b> aller aktiven IPSec Tunnel aufgelistet.
OSPF	In diesem Menü werden OSPF-bezogene Informationen angezeigt.
BRRP	Dieses Menü beinhaltet statistische Informationen über die "virtuellen Router".
SSHD	In diesem Menü können Sie die aufgebauten SSH Verbindungen einsehen.

Tabelle 1-1: Untermenüs im Menü **MONITORING AND DEBUGGING**

## 2 Untermenü ISDN Monitor

Im Folgenden wird das Untermenü *ISDN MONITOR* beschrieben.

Hier wird eine Liste der bestehenden ISDN-Verbindungen (eingehend und ausgehend) angezeigt:

X2250 Setup Tool		Bintec Access Networks GmbH				
[MONITOR] [ISDN CALLS]: ISDN Monitor - Calls		MyGateway				
Dir	Remote Name/Number	charge	Duration	Stack	Channel	State
out	isdnlogind/1111		101	0	B1	active
in	isdnlogind/9999		65	0	B2	active
EXIT						
(c)alls		(h)istory		(d)etails		(s)tatistics (r)elease

Wählen Sie **c**, wenn Sie andere Optionen verwendet haben und wieder in die Liste der bestehenden ISDN-Verbindungen wechseln möchten.

Weitere Optionen stehen Ihnen in diesem Menü zur Verfügung:

- Wählen Sie **h**, um eine Liste der letzten 20 seit dem letzten Systemstart abgeschlossenen ISDN-Verbindungen (eingehend und ausgehend) anzuzeigen.

X2250 Setup Tool		Bintec Access Networks GmbH	
[MONITOR] [ISDN HISTORY]: ISDN Monitor - History		MyGateway	
Dir	Remote Number	Charge	Starttime Duration Cause
in	isdnlogind/111	06:50:11	41 (0x90) normal call clearing
out	isdnlogin/112	06:50:57	4 (0x90) normal call clearing
in	isdnlogind/113	06:52:04	110 (0x90) normal call clearing
in	isdnlogind/114	06:56:05	4 (0x90) normal call clearing
in	isdnlogind/115	06:56:11	0 (0x90) normal call clearing
in	isdnlogind/115	06:56:17	1 (0x90) normal call clearing
in	isdnlogind/115	06:56:23	1 (0x90) normal call clearing
in	isdnlogind/114	06:56:28	2 (0x90) normal call clearing
in	isdnlogind/114	06:56:32	1 (0x90) normal call clearing
in	isdnlogind/112	06:56:37	2 (0x90) normal call clearing
in	isdnlogind/111	06:56:51	4 (0x90) normal call clearing
in	isdnlogind/113	06:57:00	2 (0x90) normal call clearing
in	isdnlogind/111	06:57:06	1 (0x90) normal call clearing
EXIT			
(c)alls (h)istory (d)etails (s)tatistics (r)elease			

- Setzen Sie den Cursor auf eine bestehende oder abgeschlossene ISDN-Verbindung und wählen Sie d, um detaillierte Informationen darüber anzuzeigen.

X2250 Setup Tool		Bintec Access Networks GmbH	
[MONITOR] [ISDN DETAILS]: ISDN Monitor - Details		MyGateway	
Remote Number: 111		Direction: in State:	
Cause	(0x90) normal call clearing		
Local Cause	(0xb) chan busy		
Info	isdnlogind		
Local Number	999		
Dispatch Item	ISDN Login		
Stack	0		
Channel	B2		
Charging Info			
SIN	telephony		
EXIT			
(c)alls (h)istory (d)etails (s)tatistics (r)elease			



- Wählen Sie `s`, um eine Statistik über die Aktivität der bestehenden ein- und ausgehenden ISDN-Verbindungen anzuzeigen.

X2250 Setup Tool		Bintec Access Networks GmbH	
[MONITOR] [ISDN STATS]: ISDN Monitor - Statistics		MyGateway	
Remote Number: 999		Direction: out	State: active
Duration 25			
Send:		Receive:	
Packets	107	Packets	107
Bytes	567	Bytes	5478
Errors	0	Errors	0
Packets/s	1	Packets/s	1
Bytes/s	5	Bytes/s	218
Load (%)	0	Load (%)	2
EXIT			
(c)alls	(h)istory	(d)etails	(s)tatistics
(r)elease			

- Wählen Sie `r`, um die markierte bestehende ISDN-Verbindung zu schließen.

Die Anzeige wird für die Optionen `c`, `h` und `s` im Sekundentakt aktualisiert.



### 3 Untermenü ISDN Credits

Im Folgenden wird das Untermenü *ISDN CREDITS* beschrieben.

Im Menü **MONITORING AND DEBUGGING** → **ISDN CREDITS** werden Subsystem **CAPI**, Subsystem **PPP** und Subsystem **ISDNLOGIN** und der jeweilige **SURVEILLANCE** Status angezeigt.

Wählen Sie ein Subsystem aus und bestätigen Sie mit der **Eingabetaste**.

Der aktuelle Stand des Taschengeldkontos für das ausgewählte Subsystem wird angezeigt:

X2250 Setup Tool		Bintec Access Networks GmbH		
[MONITOR] [ISDN CREDITS] [STAT]: Monitor ppp Credits		MyGateway		
	Total	Maximum	% reached	
Time till end of measure interval(sec)	82000	86400	5	
Number of Incoming Connections	1			
Number of Outgoing Connections	10	100	10	
Time of Incoming Connections	720	28800	3	
Time of Outgoing Connections	1360	28800	5	
Charge	0			
Number of Current Incoming Connections	0			
Number of Current Outgoing Connections	0			
Number of Current Connections	0			
EXIT				

Die Anzeige wird alle zwei Sekunden automatisch aktualisiert.

Das Menü besteht aus folgenden Feldern:

Feld	Wert
Time till end of measure interval (sec)	Zeitraum bis zum Ende des Messintervalls in Sekunden.
Number of Incoming Connections	Aktuelle Anzahl der bisher eingegangenen Verbindungen während <b>MEASURE TIME (SEC)</b> (siehe Menü <b>CREDITS</b> → <b>ISDN CREDITS</b> ).

Feld	Wert
Number of Outgoing Connections	Aktuelle Anzahl der bisher ausgegangenen Verbindungen während <b>MEASURE TIME (SEC)</b> .
Time of Incoming Connections	Aktuelle Gesamtdauer in Sekunden für bisher eingegangene Verbindungen während <b>MEASURE TIME (SEC)</b> .
Time of Outgoing Connections	Aktuelle Gesamtdauer in Sekunden für bisher ausgegangene Verbindungen während <b>MEASURE TIME (SEC)</b> .
Charge	Aktueller Stand der bisherigen Gebühren (Betrag, Einheiten) während <b>MEASURE TIME (SEC)</b> .
Number of Current Incoming Connections	Aktuelle Anzahl der derzeit eingehenden Verbindungen.
Number of Current Outgoing Connections	Aktuelle Anzahl der derzeit ausgehenden Verbindungen.
Number of Current Connections	Aktuelle Anzahl aller Verbindungen.

Tabelle 3-1: Felder im Menü **MONITORING AND DEBUGGING → ISDN CREDITS → PPP/ISDNLOGIN → EDIT**



#### Hinweis

Bitte beachten Sie, dass dieses Menü lediglich eine Anzeige der konfigurierten sowie der erreichten Werte darstellt.

Für eine Konfiguration der Grenzwerte benutzen Sie das Menü **CREDITS → ISDN CREDITS**.

## 4 Untermenü xDSL Credits

Im Folgenden wird das Untermenü *xDSL CREDITS* beschrieben.

Im Menü **MONITORING AND DEBUGGING** → *xDSL CREDITS* gelangt man in das Untermenü **PPPoE CREDITS**.

Der aktuelle Stand des Taschengeldkontos für das Subsystem PPPoE wird angezeigt:

X2250 Setup Tool		Bintec Access Networks GmbH		
[MONITOR] [XDSL CREDITS] : Monitor PPPoE Credits		MyGateway		
	Total	Maximum	% reached	
Time till end of measure interval (sec)	82000	86400	5	
Number of Outgoing Connections	10	1000	1	
Time of Outgoing Connections	7260	28800	26	
EXIT				

Das Menü besteht aus folgenden Feldern:

Feld	Wert
Time till end of measure interval (sec)	Zeitraum bis zum Ende des Messintervalls in Sekunden.
Number of Outgoing Connections	Aktuelle Anzahl der bisher ausgegangenen Verbindungen während <b>MEASURE TIME (SEC)</b> (siehe <b>CREDITS</b> → <i>xDSL CREDITS</i> → <b>PPPoE CREDITS</b> ).

Feld	Wert
Time of Outgoing Connections	Aktuelle Gesamtdauer in Sekunden für bisher ausgegangene Verbindungen während <b>MEASURE TIME (SEC)</b> .

Tabelle 4-1: Felder im Menü **MONITORING AND DEBUGGING** → **xDSL CREDITS** → **PPPoE CREDITS**

**Hinweis**

Bitte beachten Sie, dass dieses Menü lediglich eine Anzeige der konfigurierten sowie der erreichten Werte darstellt.

Für eine Konfiguration der Grenzwerte benutzen Sie das Menü **CREDITS** → **xDSL CREDITS** → **PPPoE CREDITS**.

## 5 Untermenü Interfaces

Im Folgenden wird das Untermenü *INTERFACES* beschrieben.

Im Menü *MONITORING AND DEBUGGING* → *INTERFACES* werden die aktuellen Werte und Aktivitäten der Gateway-Schnittstellen angezeigt.

Die Werte von zwei Schnittstellen werden nebeneinander angezeigt:

X2250 Setup Tool		Bintec Access Networks GmbH			
[MONITOR] [INTERFACE]: Interface Monitoring		MyGateway			
Interface Name	en0-1			PROVIDER	
Operational Status	up			up	
	total	per second	total	per second	
Received Packets	785	2	199	1	
Received Octets	130353	128	13429	86	
Received Errors	0		0		
Transmit Packets	295	2	89	1	
Transmit Octets	22358	169	7401	84	
Transmit Errors	0		0		
Active Connections	N/A			2	
Duration	N/A			734	
EXIT	EXTENDED			EXTENDED	

Die Anzeige aktualisiert sich im Sekundentakt.

Wählen Sie unter *INTERFACE NAME* die anzuzeigende Schnittstelle aus.

Das Menü enthält folgende Felder:

Feld	Wert
Interface Name	Hier können Sie das Interface auswählen, für das die Daten angezeigt werden sollen.
Operational Status	Zeigt den Betriebszustand des gewählten Interfaces an.
Received Packets	Zeigt die Anzahl der erhaltenen Pakete gesamt und pro Sekunde an.

Feld	Wert
Received Octets	Zeigt die Anzahl der erhaltenen Oktetts gesamt und pro Sekunde an.
Received Errors	Zeigt die Gesamtanzahl der erhaltenen Fehler an.
Transmit Packets	Zeigt die Anzahl der gesendeten Pakete gesamt und pro Sekunde an.
Transmit Octets	Zeigt die Anzahl der gesendeten Oktetts gesamt und pro Sekunde an.
Transmit Errors	Zeigt die Gesamtanzahl der gesendeten Fehler an.
Active Connections	<p>Zeigt die Anzahl der aktuell aktiven Verbindungen über das gewählte Interface an.</p> <ul style="list-style-type: none"> <li>■ ISDN: Gesamtanzahl der aktiven B-Kanäle.</li> <li>■ DSL: <i>N/A</i> oder <i>1</i></li> </ul> <p>Der Wert <i>N/A</i> wird nur bei IPSec und Ethernet Interfaces angezeigt.</p>
Duration	Zeigt die Gesamtdauer der logischen Verbindungen über das ausgewählte Interface an.

Tabelle 5-1: Felder im Menü **INTERFACES**

Wählen Sie **EXTENDED**, um zusätzliche Informationen anzuzeigen. Anschließend können Sie unter **OPERATION** den Status der Schnittstelle verändern (mögliche Werte: *set interface down*, *set interface up*, *reset*) und die Eingabe mit **START OPERATION** bestätigen.



```

X2250 Setup Tool                               Bintec Access Networks GmbH
[MONITOR] [INTERFACE] [EXTENDED]: Extended Interface      MyGateway
                                      Monitoring (en1-0)

OperSt InPkts      InOctets      OutPkts  OutOctets  ActCalls  IP-Address
up      1158        90041        851       70922      2          213.6.255.218

Calls:
Stk Ch  Dir Remote Number  Local DspItem  RPckts  TPckts  Charge  Duration
0  B1  out  00101901929  4210  PPP      21      15      53
0  B2  out  00101901929  4210  PPP      8        3       50

IP-Sessions:
Sourceaddress Dest-Address Prot SrcPrt  DstPrt  SrcIf  DstIf  InPkt  OutPkt

EXIT      Operation >reset          START OPERATION

```



## 6 Untermenü Messages

Im Folgenden wird das Untermenü *MESSAGES* beschrieben.

Im Menü *MONITORING AND DEBUGGING* → *MESSAGES* werden alle (gemäß der Konfiguration im Menü *SYSTEM* aufgezeichneten) Syslog-Messages mit Angabe des Subsystems (*SUBJ*) und der Priorität (*LEV*) aufgelistet.

X2250 Setup Tool		Bintec Access Networks GmbH
[MONITOR] [MESSAGE]: Syslog Messages		MyGateway
Subj	Lev	Message
INET	INF	NAT: denied incoming session in ifc 10001 prot 6 213.6.125.
PPP	DEB	Layer 1 protocol hdlc, 64000 bit/sec
PPP	DEB	ISP-ISDN: set ifSpeed, number of active connections 1/1/1
PPP	DEB	ISP-ISDN: set ifSpeed, number of active connections 2/2/2
INET	INF	NAT: denied incoming session on ifc 10001 prot 6 213.6.125.
INET	INF	NAT: denied incoming session on ifc 10001 prot 6 213.6.125.
INET	INF	refuse from if 100 prot 17 172.16.72.4:137->172.16.95.255.
INET	INF	refuse from if 100 prot 17 172.16.72.37:138->172.16.95.255.
ISDN	DEB	stack 0: deactivate
ISDN	ERR	stack 0: MDL_ERROR I
ACCT	INF	ISDN: 01.01.1970,03:26:38,03:27:23,42,334,247,11,9,,0,4210,
ACCT	INF	ISDN: 01.01.1970,03:26:42,03:27:23,83,143,93,4,3,,0,4210,
ISDN	ERR	stack 0: MDL_ERROR G
EXIT	RESET	Filter:

Mittels der Schaltfläche **RESET** löschen Sie alle bestehenden Einträge.

Sie haben die Möglichkeit, die angezeigten Syslog Meldungen zu filtern. Dazu geben Sie jedes beliebige Zeichen in das Feld **FILTER**: ein. So werden nur Meldungen in der oberhalb stehenden Liste angezeigt, die die eingegebene Zeichenfolge beinhalten. Ein Wildcard (\*) wird implizit angewendet, so dass auch alle Meldungen, die die Zeichenfolge an beliebiger Stelle enthalten, angezeigt werden.

Zusätzliche Informationen zu einer bestimmten Meldung erhalten Sie, indem Sie einen Eintrag aus der Liste auswählen und die **Eingabetaste** drücken.

Es öffnet sich eine detaillierte Übersicht zu dem gewählten Listeneintrag.

```
X2250 Setup Tool                               Bintec Access Networks GmbH
[MONITOR][MESSAGE]: Syslog Messages (full view)   MyGateway

Subject      INET
Level        INFO
Timestamp     Thu Jan 15  6:18:20

Message
  refuse from if 100 prot 17 192.168.0.8:137->192.168.0.255:137 (RI 1
  FI 1)

EXIT
```

Hier wird der komplette Text der Syslog-Message (**MESSAGE**), deren Subsystem (**SUBJECT**) und der Priorität (**LEVEL**) sichtbar. Zusätzlich wird Datum und Uhrzeit (**TIMESTAMP**) der Erstellung der Meldung angegeben.

## 7 Untermenü Email Alert

Im Folgenden wird das Untermenü *EMAIL ALERT* beschrieben.

Es ist möglich, Syslog Messages vom Gateway an einen beliebigen Syslog-Host übertragen zu lassen. Zusätzlich enthält das Gateway auch eine Email Alert Funktion: Je nach Konfiguration werden dem Administrator Emails gesendet, sobald relevante Syslog Messages auftreten.

Die Konfiguration erfolgt im Menü **MONITORING AND DEBUGGING** → **EMAIL ALERT**:  
(Die Anzeige enthält Beispielwerte)

X2250 Setup Tool	Bintec Access Networks GmbH		
[ALERT NOTIFICATION]: Settings	MyGateway		
Global notification settings:			
Adminstatus	:	enable	
SMTP Server	:	mailserver01	
Originator	:	MyGateway@Company.org	
max. Mails/min	:	6	
Authentication Settings >			
Current notification list:			
Receiver	Expression	Time	Count compress Level
admin@Comany.org	*dialup*	60	1 disable debug
ADD	DELETE	CANCEL	SAVE

Das Menü enthält folgende Felder:

Feld	Wert
Adminstatus	Hier aktivieren bzw. deaktivieren Sie die Funktion Email Alert. Zur Verfügung stehen: <ul style="list-style-type: none"> <li>■ <i>enable</i> (Defaultwert)</li> <li>■ <i>disable</i></li> </ul>

Feld	Wert
SMTP Server	Hier geben Sie die Adresse (►► <b>IP-Adresse</b> oder gültiger ►► <b>DNS-Name</b> ) des Mailservers ein, der zum Versenden der Mails verwendet werden soll. Die Eingabe ist auf 40 Zeichen begrenzt.
Originator	Hier geben Sie die Mailadresse ein, die in das Absenderfeld der Email eingetragen werden soll.
max. Mails/min	Hier können Sie die Anzahl der ausgehenden Mails pro Minute begrenzen. Zur Verfügung stehen Werte von 1 bis 30, der Defaultwert ist 6.

Tabelle 7-1: Felder im Menü **EMAIL ALERT**

Im unteren Teil des Menüfensters werden die bereits konfigurierten Notification Rules dargestellt. Mit **ADD/EDIT** können Sie eine neue Regel konfigurieren bzw. eine bestehende editieren:

X2250 Setup Tool	Bintec Access Networks GmbH
[ALERT NOTIFICATION] [ADD]	MyGateway
Notification rule configuration:	
Receiver	: admin@Company.org
Contents	: *dialup*
Level	: debug
Timeout	: 60
Messages	: 1
Compress	: disable
Select subsystems:	
<input type="checkbox"/> ACCOUNT <input type="checkbox"/> ISDN <input type="checkbox"/> INET <input type="checkbox"/> X25 <input type="checkbox"/> CAPI <input type="checkbox"/> PPP <input type="checkbox"/> CONFIG <input type="checkbox"/> SNMP <input type="checkbox"/> X21 <input type="checkbox"/> ETHER <input type="checkbox"/> RADIUS <input type="checkbox"/> OSPF <input type="checkbox"/> MODEM <input type="checkbox"/> RIP <input type="checkbox"/> ATM <input type="checkbox"/> IPSEC <input type="checkbox"/> AUX	
SAVE	CANCEL

Das Menü besteht aus folgenden Feldern:

Feld	Wert
Receiver	Hier geben Sie die Emailadresse des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.
Contents	Hier müssen Sie eine "Regular Expression" eingeben. Ihr Vorkommen in einer Syslog Message ist die notwendige Bedingung für das Auslösen eines Alerts. Die Eingabe ist auf 55 Zeichen begrenzt. Bedenken Sie, dass ohne die Verwendung von Wildcards (z. B. "**") nur diejenigen Strings die Bedingung erfüllen, die exakt der Eingabe entsprechen. Daher wird in der Regel die eingegebene "Regular Expression" Wildcards enthalten. Um grundsätzlich über alle Syslog-Messages des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein. Bsp. Um alle Meldungen, die die Zeichenkette "dialup" enthalten, zu erfassen, geben Sie als <b>CONTENTS</b> * <i>dialup</i> * ein.
Level	Hier wählen Sie den Syslog-Level aus, auf dem der im Feld <b>CONTENTS</b> konfigurierte String vorkommen muss, damit ein Email Alert ausgelöst wird. Zur Verfügung stehen alle im Menü <b>SYSTEM</b> , Feld <b>MESSAGE LEVEL FOR THE SYSLOG TABLE</b> , verfügbaren Werte, Defaultwert ist emergency.

Feld	Wert
Timeout	<p>Hier geben Sie ein, wieviele Sekunden das Gateway nach einem entsprechenden Ereignis maximal warten darf, bevor das Versenden der Alert Mail erzwungen wird.</p> <p>Wenn <b>MESSAGES</b> konfiguriert ist, wird die Mail beim Erreichen der eingegebenen Anzahl gesendet, auch wenn die hier angegebenen Dauer noch nicht erreicht ist.</p> <p>Zur Verfügung stehen Werte von 0 bis 86400. Ein Wert von 0 deaktiviert das Timeout, Defaultwert ist 60.</p>
Messages	<p>Hier geben Sie die Anzahl an Syslog Messages ein, die erreicht sein muss, bevor eine Alert Email für diesen Fall gesendet wird. Wenn <b>TIMEOUT</b> konfiguriert ist, wird die Mail bei dessen Ablauf gesendet, auch wenn die Anzahl an Meldungen noch nicht erreicht ist.</p> <p>Zur Verfügung stehen Werte von 1 bis 99, Defaultwert ist 1.</p>
Compress	<p>Hier können Sie auswählen, ob der Text der Email Alerts verkürzt werden soll. Die Mail enthält dann Syslog-Message mit identischem Text nur einmal und zusätzlich die Anzahl der entsprechenden Ereignisse.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>disable</i> - Defaultwert</li> <li><input type="checkbox"/> <i>enable</i></li> </ul>
Select subsystems	<p>Hier wählen Sie die Subsysteme aus, die überwacht werden sollen. Wählen Sie ein Subsystem mit den Pfeiltasten und aktivieren oder deaktivieren Sie es mit der Leertaste.</p>

Tabelle 7-2: Felder im Menü **EMAIL ALERT** → **ADD/EDIT**



Das Menü bietet Zugang zum Untermenü **AUTHENTICATION SETTINGS**.

## 7.1 Untermenü Authentication Settings

Im Folgenden wird das Untermenü **AUTHENTICATION SETTINGS** beschrieben.

Das Gateway unterstützt die SMTP-Authentifizierung durch den Email-Alarm. Die Konfiguration erfolgt im Untermenü **MONITORING AND DEBUGGING → EMAIL ALERT → AUTHENTICATION SETTINGS** (die Anzeige enthält Beispielwerte):

X2250 Setup Tool	Bintec Access Networks GmbH
[ALERT NOTIFICATION] [SMTP]: Authentication	MyGateway
SMTP Authentication Settings:	
<pre> Server needs Authentication : SMTP after POP       POP3 Server       Username      :       Password      :       POP3 Timeout: 600           </pre>	
SAVE	CANCEL

Das Menü bietet folgende Optionen an:

Feld	Wert
Server needs Authentication	<p>Hier können Sie die gewünschte SMTP-Authentifizierung auswählen.</p> <p>Zur Auswahl stehen:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <i>none</i> (Standardwert)</li> <li><input type="checkbox"/> <i>Enhanced SMTP</i></li> <li><input type="checkbox"/> <i>SMTP after POP</i>.</li> </ul>

Feld	Wert
Username	Bei <i>Enhanced SMTP</i> -Authentifizierung: dies ist der Benutzername, den Sie benutzen, um sich direkt beim SMTP-Server einzuloggen. Bei <i>SMTP after POP</i> : dies ist der Benutzername, den Sie benutzen, um sich beim POP3-Server einzuloggen.
Password	Bei <i>Enhanced SMTP</i> -Authentifizierung: dies ist das Passwort, welches Sie benutzen, um sich direkt beim SMTP-Server einzuloggen. Bei <i>SMTP after POP</i> : dies ist das Passwort, welches Sie benutzen, um sich beim POP3-Server einzuloggen.
POP3 Server	Hier geben Sie den Domainnamen des POP3-Servers ein, der die Authentifizierung zum SMTP-Server weitergibt.
POP3 Timeout	Hier geben Sie eine Zeitsperre (Timeout) ein, nach deren Ablauf die Authentifizierung als ungültig betrachtet und wiederholt wird. Mögliche Werte sind 60 bis 3600 Sekunden, der Standardwert ist 600.

Tabelle 7-3: **MONITORING AND DEBUGGING → EMAIL ALERT → AUTHENTICATION SETTINGS**

## 8 Untermenü TCP/IP

Im Folgenden wird das Untermenü *TCP/IP* beschrieben.

Im Menü **MONITORING AND DEBUGGING** → **TCP/IP** wird eine Statistik der Verbindungen mit den ►► **Protokollen** ICMP, ►► **IP**, UDP und TCP angezeigt.

Die Statistik für IP-Verbindungen zeigt folgendes an:

X2250 Setup Tool		Bintec Access Networks GmbH	
[MONITOR] [IP]: IP Statistics		MyGateway	
InReceives	3912	OutNoRoutes	0
InHdrErrors	0	ReasmTimeout	500
InAddrErrors	0	ReasmReqds	0
ForwDatagrams	0	ReasmOKs	0
InUnknownProtos	0	ReasmFails	0
InDiscards	0	FragOKs	0
InDelivers	3321	FragFails	0
OutRequests	9	FragCreates	0
OutDiscards	0	RoutingDiscards	0
ICMP Statistics	TCP Statistics	UDP Statistics	
EXIT			
I (C)MP	(I)P	(U)DP	(T)CP

Die Bedeutung der MIB-Variablen finden Sie in der **MIB Reference**. (Diese finden Sie im Download-Bereich der Bintec-Produkte auf [www.funkwerk-ec.com](http://www.funkwerk-ec.com).)

Die jeweilige Aufstellung erhalten Sie entweder durch Auswahl der Menüs **ICMP STATISTICS**, **IP STATISTICS**, **UDP STATISTICS** und **TCP STATISTICS**, oder durch drücken der in der Hilfezeile am unteren Rand des Fensters angegebenen Tasten:

- Wählen Sie **C**, um statische Daten zu ICMP darzustellen.
- Wählen Sie **I**, um statische Daten zu IP darzustellen.
- Wählen Sie **U**, um statische Daten zu UDP darzustellen.
- Wählen Sie **T**, um statische Daten zu ICMP darzustellen.



## 9 Untermenü IPsec

Im Menü **MONITORING AND DEBUGGING** → **IPSEC** gelangt man in folgende Untermenüs:

- **GLOBAL SETTINGS**
- **IKE SECURITY ASSOCIATIONS**
- **IPSEC SA BUNDLES**

Hier können Sie sich den Status der globalen Statistiken, IKE Security Associations und IPsec Security Associations anzeigen lassen. Dementsprechend enthält es drei Untermenüs, die in den folgenden Kapiteln beschrieben werden.

### 9.1 Untermenü Global Statistics

Alle Felder im Menü **MONITORING AND DEBUGGING** → **IPSEC** → **GLOBAL STATISTICS** können nur gelesen werden, d. h. Sie können sich hier die Einstellungen und Statistiken anzeigen lassen, können jedoch keine Änderungen an der Konfiguration vornehmen.

Es sieht folgendermaßen aus (die hier aufgeführten Werte sind nur Beispiele):

X2250 Setup Tool		Bintec Access Networks GmbH	
[MONITOR] [IPSEC] [IPSEC] [STATS]: IPsec Monitoring -		Global Statistics	
		MyGateway	
Peers	Up : 10 /16	Dormant: 6	Blocked: 0
SAs	Phase 1: 10 /0	Phase 2: 10	/0
Packets	In	Out	
	Total : 850	600	
	Passed : 50	50	
	Dropped: 30	40	
	Protect: 770	510	
	Errors : 0	0	
EXIT			

Die Felder und die Bedeutung der angezeigten Werte sind folgende:

Feld	Wert
Peers Up	Zeigt die Anzahl der aktiven Peers ( <b>OPERSTATUS</b> = <i>up</i> ) von der Anzahl der konfigurierten Peers.
Peers Dormant	Zeigt die Anzahl der inaktiven Peers ( <b>OPERSTATUS</b> = <i>dormant</i> ).
Peers Blocked	Zeigt die Anzahl der blockierten Peers ( <b>OPERSTATUS</b> = <i>blocked</i> ).
SAs Phase 1	Zeigt die Anzahl der aktiven Phase-1-SAs (State = <i>established</i> ) zur Gesamtzahl der Phase-1-SAs an.
SAs Phase 2	Zeigt die Anzahl der aktiven Phase-2-SAs ( <b>STATE</b> = <i>established</i> ) zur Gesamtzahl der Phase-2-SAs an.
Packets In/Out	<p>Hier wird die Anzahl der Pakete angezeigt, die auf eine bestimmte Art und Weise behandelt worden sind:</p> <ul style="list-style-type: none"> <li>■ <i>Total</i>: Die Anzahl aller bearbeiteten Pakete.</li> <li>■ <i>Passed</i>: Die Anzahl der Pakete, die im Klartext weitergeleitet wurden.</li> <li>■ <i>Dropped</i>: Die Anzahl der verworfenen Pakete.</li> <li>■ <i>Protect</i>: Die Anzahl der durch IPsec geschützten Pakete.</li> <li>■ <i>Error</i>: Die Anzahl der Pakete, bei deren Behandlung es zu Fehlern gekommen ist.</li> </ul>

Tabelle 9-1: **MONITORING AND DEBUGGING → IPSEC → GLOBAL STATISTICS**

## 9.2 Untermenü IKE Security Associations

Das nächste Überwachungs-Untermenü (**MONITORING AND DEBUGGING → IPSEC → IKE SECURITY ASSOCIATIONS**) zeigt Statistiken über die IKE-SAs an. Es sieht folgendermaßen aus (die aufgeführten Werte sind nur Beispiele):

```

X2250 Setup Tool                               Bintec Access Networks GmbH
[MONITOR] [IPSEC] [IPSEC] [IKE SAS]: IPsec Monitoring -
                                           IKE SAS                                           MyGateway

T: xch.-Type: B=Base      I=Id-prot.    O=auth-Only A=Aggressive
A: Auth-Meth: P=P-S-Key  D=DSA-sign. S=RSA-sign. E=RSA-encryption
R: Role      : I=Initiator R=Responder
S: State     : N=Negotiate E=Establ.    D=Delete W=Waiting-for-remove
E: Enc.-Alg  : d=DES D=3ES B=Blowfish  C=Cast R=Rijndael T=Twofish
H: Hash-Alg  : M=MD5      S=SHA1      T=Tiger      R=Ripemd160
type 'h' to toggle this help

Remote ID          Remote IP          Local ID          TARSEH
remote            192.168.0.1        local             IPIEBM

DELETE            EXIT
    
```

Die Bedeutung der Zeichen in der Spalte **TARSEH** (das ist die letzte Spalte rechts unterhalb des Hilfebereichs des Menüfensters) wird im oberen Teil des Menüfensters erläutert; somit ist das oben dargestellte Beispiel folgendermaßen zu verstehen:

Feld	Wert
Remote ID	Zeigt die ID des entfernten Peers an. Im Beispiel erfolgt die Authentifizierung mit Zertifikaten; damit besteht die entfernte ID aus Quotes aus dem Zertifikat des Peers.
Remote IP	Zeigt die IP-Adresse des entfernten Peers an.

Feld	Wert
Local ID	<p>Zeigt die lokale ID an.</p> <p>Auch hier besteht die ID aus Quotes aus dem Zertifikat welches für die Authentifizierung benutzt wurde.</p>
TARSEH	<p>Zeigt die Kombination der im Hilfebereich des Menüfensters erläuterten Parameter an.</p> <p>Das Beispiel ISREBM bedeutet somit:</p> <ul style="list-style-type: none"> <li>■ Austauschtyp: id_protect (<i>I</i>)</li> <li>■ Authentifizierungsmethode: RSA-Signatur (<i>S</i>)</li> <li>■ Rolle: Antwortender (Responder, <i>R</i>)</li> <li>■ Status: Eingerichtet (Established, <i>E</i>)</li> <li>■ Verschlüsselungsalgorithmus: Blowfish (<i>B</i>)</li> <li>■ Hash-Algorithmus: MD5 (<i>M</i>)</li> </ul>

Tabelle 9-2: **MONITORING AND DEBUGGING → IPSEC → IKE SECURITY ASSOCIATIONS**



### 9.3 Untermenü IPsec SA Bundles

Das nächste Untermenü (**MONITORING AND DEBUGGING** → **IPSEC** → **IPSEC SA BUNDLES**) zeigt die IPsec-Security Associations an, die in IKE Phase 2 ausgehandelt wurden. Das Menü sieht folgendermaßen aus:

X2250 Setup Tool		Bintec Access Networks GmbH						
[MONITOR] [IPSEC] .. [IPSEC BUNDLES]: IPsec Monitoring -		IPsec SA Bundles					MyGateway	
Local	LPort	Pto	Remote	RPort	CEA	In	Out	
192.168.0.2/32	0	all	192.168.0.1/32	0	-E-	888	1232	
DELETE		EXIT						

Die Bedeutung der Abkürzung in der Spalte **SEA** wird wieder im Hilfebereich des Menüfensters erläutert. Die Felder haben folgende Bedeutung:

Feld	Wert
Local	Zeigt die lokale ►► <b>IP-Adresse</b> , den Adressbereich oder das Netz an, welches von dieser SA geschützt wird.
LPort	Zeigt die lokale ►► <b>Portnummer</b> oder den Portnummernbereich an, die/der von dieser SA geschützt wird.
Pto	Zeigt das Schicht-4-Protokoll des durch diese SA geschützten Datenverkehrs an (0 = jedes).
Remote	Zeigt die entfernte IP-Adresse, den Adressbereich oder das Netz an, welches von dieser SA geschützt wird.

Feld	Wert
RPort	Zeigt die entfernte Portnummer oder den Portnummernbereich an, die/der von dieser SA geschützt wird.
CEA	Zeigt an, welche IPsec-Protokolle für die SA verwendet werden: <ul style="list-style-type: none"> <li>■ C = IPComp</li> <li>■ E = ESP</li> <li>■ A = AH.</li> </ul>
In	Zeigt die Anzahl der über diese SA empfangenen Bytes an.
Out	Zeigt die Anzahl der über diese SA gesendeten Bytes an.

Tabelle 9-3: **MONITORING AND DEBUGGING → IPSEC → IPSEC SECURITY ASSOCIATIONS**

## 10 Untermenü OSPF

Im Folgenden wird das Untermenü *OSPF* beschrieben.

X2250 Setup Tool		Bintec Access Networks GmbH			
[MONITOR] [OSPF]: OSPF Monitor		MyGateway			
Interface	DR	BDR	Admin Status	State	
en0-1	N/A	N/A	passive	N/A	=
en0-1-snap	N/A	N/A	passive	N/A	
en0-2	N/A	N/A	passive	N/A	
en0-2-snap	N/A	N/A	passive	N/A	v
Neighbor	Router ID	Interface	Retx Queue	State	
Area	Type	Link State ID	Router ID	Sequence	Age
EXIT					

Im Menü **MONITORING AND DEBUGGING** → **OSPF** werden Informationen zu OSPF überwacht.

Der OSPF Monitor ist horizontal in drei Bereiche gegliedert und zeigt Informationen zu OSPF Interfaces, Nachbarn und Bereichen.

**Interfaces** Im Bereich **INTERFACES** sind alle aktivierten OSPF-Interfaces aufgelistet (d.h. Interfaces, die im Menü **IP** → **OSPF** → **INTERFACES** nicht auf **OFF** gestellt wurden).

Feld	Wert
Interface	Das Gateway Interface, der zu diesem Eintrag gehört.
Designed Router (DR)	Die spezifizierte ►► <b>IP-Adresse</b> dieses Interfaces auf dem Gateway (ein DR wird für Point-To-Point Interfaces nicht angezeigt).

Feld	Wert
Backup Designed Router (BDR)	Die IP-Adresse des Interfaces für das spezifizierte Backup Gateway (ein BDR wird für Point-To-Point Interfaces nicht angezeigt).
Admin Status	Hier werden nur aktive und passive Interfaces angezeigt.
State	<p>Der hier angezeigte OSPF Status (<i>OSPFIFSTATE</i>) des Interfaces kann folgende Werte annehmen:</p> <ul style="list-style-type: none"> <li>■ <i>down</i>: OSPF läuft nicht auf diesem Interface.</li> <li>■ <i>wait</i>: Die Initialphase des OSPF, in der DR und BDR bestimmt werden.</li> <li>■ <i>PTP</i>: Das Interface ist ein Point-To-Point Interface. DR oder BDR werden nicht angezeigt.</li> <li>■ <i>DR</i>: Das Gateway ist das spezifizierte Gateway für dieses Interface.</li> <li>■ <i>BDR</i>: Das Gateway ist das spezifizierte Backup-Gateway für dieses Interface.</li> <li>■ <i>DRouter</i>: Ein anderes Gateway ist DR/BDR für dieses Interface.</li> </ul>

Tabelle 10-1: Der OSPF Monitor Bereich **INTERFACE**

**Neighbor** Im Bereich **NEIGHBOR** werden die Nachbar-Gateways aufgelistet, die über das HELLO Protokoll identifiziert wurden.

Feld	Wert
Neighbor	Die Adresse des Nachbar-Gateways auf diesem Interface.
Router ID	Die systemweite Router ID des Nachbargateways.

Feld	Wert
Interface	Das Gateway Interface, über das dieses Gateway identifiziert wurde.
Retx Queue	Die Größe der Retransmission Queue dieses Nachbarn. Es handelt sich um die Anzahl der Advertisements, die zu diesem Nachbarn geschickt (und angenommen) werden müssen.
State	<p>Der OSPF Status mit diesem Nachbargateway kann folgende Werte annehmen:</p> <ul style="list-style-type: none"> <li>■ <i>init</i>: Die Initialphase. Ein HELLO Paket wird vom Nachbarn empfangen.</li> <li>■ <i>twoWay</i>: Bidirektionale Kommunikation mit dem Nachbarn. Die übermittelten HELLO Pakete sind vom Nachbargateway angenommen worden (mit korrekten Parametern).</li> <li>■ <i>EXstart</i>: Der Austausch von Database Description Paketen zwischen den Gateways hat begonnen.</li> <li>■ <i>exchange</i>: Aktiver Austausch von Database Description Paketen mit dem Nachbarn.</li> <li>■ <i>loading</i>: Das Gateway tauscht nun Link State Advertisements mit dem Nachbarn aus.</li> <li>■ <i>full</i>: Die Link State Datenbanken des Gateways und seines Nachbarn sind nun synchronisiert.</li> </ul>

Tabelle 10-2: Bereich **NEIGHBOR**

**LSDB** Im Bereich für die Link State Database werden die Headers aller Link State Advertisements (LSA) aufgelistet.

Feld	Wert
Area	Die Bereichsdatenbank, der das LSA zugeordnet ist.
Type	Der LSA-Typ. Es gibt fünf LSA-Typen: Router Link, Network Link, Summary Link, Summary ASBR, and AS External.
Link State ID	Die Link State ID des LSA. Die Bedeutung der Link State ID hängt vom Typ des Advertisements ab.
Router ID	Identifiziert das Gateway, das dieses LSA generiert hat.
Sequence	Die Sequenznummer des Advertisements. Sequenznummern ermöglichen es dem Gateway, zu bestimmen, ob seine Datenbank aktuell ist oder ob es ein Update anfordern muss.
Age	Das Alter des LSA (in Sekunden)

Tabelle 10-3: Bereich **LSDB**

# 11 Untermenü BRRP

Im Folgenden wird das Untermenü *BRRP* beschrieben.

VrID	Prio	State	Interface	Master-IP-Addr	Errors
1	100	down	en0-1-1	0.0.0.0	0
2	100	down	en0-1-2	0.0.0.0	0

EXIT

Das Menü **MONITORING AND DEBUGGING** → **BRRP** zeigt eine Liste aller "virtuellen Router".

Die Liste enthält folgende Einträge (siehe auch Handbuch Kapitel **BRRP**):

Spalte	Bedeutung
VrID	ID des konfigurierten "virtuellen Routers"
Prio	Konfigurierte Priorität: <ul style="list-style-type: none"> <li>■ 255 = Master</li> <li>■ &lt;255 = Slave</li> </ul>
State	Der aktuelle Status des BRRP Gateways innerhalb des "virtuellen Routers".
Interface	Interface, das am "virtuellen Router" teilnimmt
Master-IP-Addr	IP-Adresse des virtuellen Interfaces des Masters

Spalte	Bedeutung
Errors	Gesamtanzahl der empfangenen fehlerhaften Pakete

Tabelle 11-1: Virtual Router Monitoring Liste

Detaillierte statistische Informationen über die einzelnen "virtuellen Router" erhält man, indem man mit den Pfeiltasten auf den gewünschten Listeneintrag geht und diesen durch Drücken der **Return**-Taste auswählt.

X2250 Setup Tool		Bintec Access Networks GmbH	
[MONITOR] [BRRP] [DETAILS]: Virtual Router Details		MyGateway	
Virtual Router ID	1		
Virtual Router State	backup		
Become Master	2		
Advertisements Received	23536		
Advertisement Interval Errors	0		
Version Errors	0		
Authentication Errors	0		
Authentication Type Mismatch	0		
Invalid Authentication Type	30		
Invalid Type Packets Received	0		
Packet Length Errors	0		
IP TTL Errors	0		
Checksum Errors	0		
EXIT			

Hier werden folgende Werte angezeigt:

Feld	Wert
Virtual Router ID	ID des "virtuellen Routers", dessen Statistik Sie einsehen.



Feld	Wert
Virtual Router State	<p>Der aktuelle Status des BRRP Gateways innerhalb des "virtuellen Routers". Dieses Feld kann folgende Werte annehmen:</p> <ul style="list-style-type: none"> <li>■ <i>initialize</i>: Das BRRP Gateway wartet auf ein Startup-Event.</li> <li>■ <i>backup</i>: Das BRRP Gateway überwacht die Erreichbarkeit des Master Routers.</li> <li>■ <i>master</i>: Das BRRP Gateway leitet Pakete weiter an ►► <b>IP-Adressen</b>, die mit diesem Router verknüpft sind.</li> </ul>
Become Master	Die Gesamtanzahl der Statusübergänge des BRRP Gateways zu <i>master</i> .
Advertisements Received	Die Gesamtanzahl der BRRP Advertisements, die vom BRRP Gateway empfangen wurden.
Advertisement Interval Errors	Die Gesamtanzahl der empfangenen BRRP-Advertisement-Pakete, deren Advertisement Interval sich von dem, der auf dem lokalen BRRP Gateway konfiguriert ist, unterscheidet.
Version Errors	Die Gesamtanzahl der empfangenen BRRP-Pakete mit unbekannter oder nicht-unterstützter Versionsnummer.
Authentication Errors	Die Gesamtanzahl der empfangenen BRRP-Pakete mit falschem <b>AUTHENTICATION KEY</b> .
Authentication Type Mismatch	Die Gesamtanzahl der empfangenen Pakete, bei denen der <b>AUTHENTICATION TYPE</b> zwar bekannt ist, aber nicht der lokal konfigurierten Authentifizierungsmethode entspricht.
Invalid Authentication Type	Die Gesamtanzahl der empfangenen Pakete, die einen völlig unbekanntem Authentifizierungstypen haben.

Feld	Wert
Invalid Type Packets Received	Die Anzahl der vom "virtuellen Router" empfangenen BRRP-Pakete, die einen ungültigen Wert im 'type'-Feld des BRRP Headers haben. Der korrekte Wert für 'type' ist '1' ('advertisement').
Packet Length Errors	Die Gesamtanzahl der empfangenen Pakete mit einer kleineren Paketlänge als der Länge, die im BRRP Header spezifiziert wird.
IP TTL Errors	Die Gesamtanzahl der vom "virtuellen Router" empfangenen BRRP-Pakete mit IP TTL (Time-To-Live) ungleich 255.
Checksum Errors	Die Gesamtanzahl der empfangenen BRRP-Pakete mit einer ungültigen BRRP Checksum.

Tabelle 11-2: Felder im Menü **MONITORING**

## 12 Untermenü SSH Daemon

Im Folgenden wird das Untermenü *SSH DAEMON* beschrieben.

Im Menü *MONITORING AND DEBUGGING* → *SSH DAEMON* können Sie die aufgebauete SSH-Client Verbindung einsehen.

X2302 Setup Tool		Bintec Access Networks GmbH	
[MONITOR] [SSHD] [SESSIONS]: SSH Daemon active Sessions		MyGateway	
User	IP-Address	State	Connect-Time
admin	192.168.1.1:2013	active	Thu Jan 1 4:51:07 2005
EXIT			

Wenn Sie die Verbindung durch Drücken der **Bestätigungstaste** auswählen, werden folgende Details sichtbar:

X2302 Setup Tool		Bintec Access Networks GmbH	
[MONITOR] [SSHD] [SESSIONS] [] [DETAILS]: SSH Daemon		MyGateway	
Session Details			
Account	admin		
Connection State	active		
Remote IP-Address	192.168.1.1:2013		
Negotiated Cipher	aes128-cbc		
Negotiated MAC	hmac-sha1		
Negotiated Compression	none		
Established Time	00:06:02		
Total Bytes IN	26616		
Total Bytes OUT	31180		
EXIT			

Die Details geben Auskunft über folgende Werte:

Feld	Wert
Account	Der Benutzername, der für den Client Login verwendet wird.
Connection State	Der Status der Client-Verbindung.
Remote IP-Address	Die IP-Adresse und der Port des verbundenen Clients.
Negotiated Cipher	Mit dem Client vereinbarter Verschlüsselungsalgorithmus.
Negotiated MAC	Der mit dem Client vereinbarte MAC (Message Authentication Code).
Negotiated Compression	Der mit dem Client vereinbarte Kompressionsalgorithmus.
Established Time	Dauer der SSH-Verbindung.
Total Bytes IN	Anzahl der von diesem Client empfangenen Bytes.
Total Bytes OUT	Anzahl der an diesen Client gesendeten Bytes.

Tabelle 12-1: Felder im Menü **MONITORING AND DEBUGGING** → **SSH DAEMON** → **EDIT**

# Index: Monitoring and Debugging

<b>A</b>	Active Connections	14
	Admin Status	34
	Adminstatus	19
	Advertisement Interval Errors	39
	Advertisements Received	39
	Age	36
	Area	36
	Authentication Errors	39
	Authentication Type Mismatch	39
<b>B</b>	Backup Designed Router (BDR)	34
	Become Master	39
	BRRP	4
<b>C</b>	CEA	32
	Charge	10
	Checksum Errors	40
	Compress	22
	Contents	21
<b>D</b>	Designed Router (DR)	33
	Duration	14
<b>E</b>	Email Alert	4
	EXTENDED	14
<b>I</b>	In	32
	Interface	33, 35
	Interface Name	13
	Interfaces	3, 33
	Invalid Authentication Type	39
	Invalid Type Packets Received	40
	IP TTL Errors	40
	IPSec	4

	ISDN Credits	3
	ISDN Monitor	3
<b>L</b>	Level	21
	Link State ID	36
	Local	31
	Local ID	30
	LPort	31
	LSDB	36
<b>M</b>	max. Mails/min	20
	Messages	4, 22
<b>N</b>	Neighbor	34
	Number of Current Connections	10
	Number of Current Incoming Connections	10
	Number of Current Outgoing Connections	10
	Number of Incoming Connections	9
	Number of Outgoing Connections	10, 11
<b>O</b>	Operation	14
	Operational Status	13
	Originator	20
	OSPF	4
	Out	32
<b>P</b>	Packet Length Errors	40
	Packets In	28
	Peers Blocked	28
	Peers Dormant	28
	Peers Up	28
	Pto	31
<b>R</b>	Received Errors	14
	Received Octets	14
	Received Packets	13
	Receiver	21



	Remote	31
	Remote ID	29
	Remote IP	29
	Retx Queue	35
	Router ID	34, 36
	RPort	32
<b>S</b>	SAs Phase 1	28
	SAs Phase 2	28
	SEA	31
	Select subsystems	22
	Sequence	36
	SMTP Server	20
	SSH Daemon	4
	START OPERATION	14
	State	34, 35
<b>T</b>	TARSEH	29, 30
	TCP/IP	4
	Time for Incoming Connections	10
	Time for Outgoing Connections	10
	Time for Outgoing Connections (sec)	12
	Time till end of measure interval (sec)	9, 11
	Timeout	22
	Transmit Errors	14
	Transmit Octets	14
	Transmit Packets	14
	Type	36
<b>V</b>	Version Errors	39
	Virtual Router ID	38
	Virtual Router State	39
<b>X</b>	xDSL Credits	3

