IP

Bintec Benutzerhandbuch - XGeneration
Version 1.0

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Bintec-Gateways ab Software-Release 7.1.14. 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.bintec.de.

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.bintec.de.

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

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.bintec.de.

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

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

1 Menü IP 3
2 Untermenü Routing 5
3 Untermenü Static Settings 11
4 Untermenü Network Address Translation 15
4.1 Untermenü Requested from OUTSIDE/INSIDE 16
5 Untermenü Bandwidth Management (Load Balancing / BOD) . . 23
5.1 Untermenü IP Load Balancing over Multiple Interfaces 23
5.1.1 Untermenü IP Routing List 27
6 Untermenü IP address pool WAN (PPP) 31
7 Untermenü IP address pool LAN (DHCP) 33
8 Untermenü SNMP 35
9 Untermenü Remote Authentication (RADIUS/TACACS+) 37
9.1 Untermenü RADIUS Authentication and Accounting 37
9.2 Untermenü TACACS+ Authentication and Authorization 43
10 Untermenü DNS 49
10.1 Untermenü Static Hosts 54
10.2 Untermenü Forwarded Domains 55
10.3 Untermenü Dynamic Cache 57
10.4 Untermenü Advanced Settings 59
10.5 Untermenü Global Statistics 60
11 Untermenü DynDNS 63

12 Untermenü Routing protocols 69

12.1 Untermenü RIP 70

12.1.1 Untermenü Static Settings 71

12.1.2 Untermenü Timer 73

12.1.3 Untermenü Filter 75

Index: IP 79

1 Menü IP

Im Folgenden wird das Menü *IP* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP]: IP Configuration                                      MyGateway

         Routing
         Static Settings
         Network Address Translation

         Bandwidth Management (Load Balancing / BOD)
         IP address pool WAN (PPP)
         IP address pool LAN (DHCP)
         SNMP
         Remote Authentication (RADIUS/TACACS+)
         DNS
         DynDNS
         Routing Protocols

         EXIT
```

Über das Hauptmenü ***IP*** gelangt man in die Untermenüs:

- ***ROUTING***
- ***STATIC SETTINGS***
- ***NETWORK ADDRESS TRANSLATION***
- ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)***
- ***IP ADDRESS POOL WAN (PPP)***
- ***IP ADDRESS POOL LAN (DHCP)***
- ***SNMP***
- ***REMOTE AUTHENTICATION (RADIUS/TACACS+)***
- ***DNS***
- ***DYNDNS***
- ***ROUTING PROTOCOLS***

1 Menü IP

1 Untermenü Routing

Im Folgenden wird das Untermenü *ROUTING* beschrieben.

Im Menü ***IP*** ➜ ***ROUTING*** sind alle IP-Routen Ihres Gateways aufgelistet.

Unter ***FLAGS*** wird der aktuelle Status (*Up* – Aktiv, *Dormant* – Ruhend, *Blocked* – Gesperrt) und die Art der Route (*Gateway Route*, *Interface Route*, *Subnet Route*, *Host Route*, *Extended Route*) angezeigt. Unter ***PRO*** wird angezeigt, mit welchem Protokoll Ihr Gateway den Routing-Eintrag "gelernt" hat, z.B. ***LOC*** = local, d.h. manuell konfiguriert.

```
X2302 Setup Tool                              Bintec Access Networks GmbH
[IP][ROUTING]: IP Routing                                       MyGateway


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  US    0    en0-1       loc
192.168.1.0   192.168.100.2  255.255.255.0  DG    1    Filiale     loc
192.168.100.2 192.268.100.1  255.255.255.0  DH    1    Filiale     loc



     ADD                ADDEXT              DELETE              EXIT
```

Sie können eine neue Route mit ***ADD*** hinzufügen, einen bestehenden Eintrag bearbeiten Sie, indem Sie ihn mit dem Cursor markieren und mit ***ENTER*** bestätigen. Folgendes Menü öffnet sich:

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][ROUTING][ADD]                                          MyGateway

   Route Type                  Network route
   Network                     LAN

   Destination IP-Address
   Netmask

   Gateway IP-Address
   Metric                      1


                    SAVE                                CANCEL
```

Das Menü ***ROUTING*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Route Type	Art der Route. Mögliche Werte: ■ *Host route*: Route zu einem einzelnen Host. ■ *Network route* (Defaultwert): Route zu einem Netzwerk. ■ *Default route*: Gilt für alle IP-Adressen und wird nur benutzt, wenn keine andere passende Route verfügbar ist.
Network	Definiert die Art der Verbindung (LAN, WAN). Mögliche Werte, siehe Tabelle “Auswahlmöglichkeiten von Network” auf Seite 7.
Destination IP-Address	Nur für ***ROUTE TYPE*** *Host route* oder *Network route*. IP-Adresse des Ziel-Hosts oder -Netzwerks.
Netmask	nur für ***ROUTE TYPE*** = *Network route* Netzmaske zu ***DESTINATION IP-ADDRESS***. Wenn kein Eintrag erfolgt, benutzt das Gateway eine Standardnetzmaske.

Feld	Wert
Partner / Interface	WAN-Partner bzw. Schnittstelle (nur für ***NETWORK*** = *WAN without transit network*).
Gateway IP-Address	Nur für ***NETWORK*** *LAN* oder *WAN with transit network*. IP-Adresse des Hosts, an den Ihr Gateway die IP-Pakete weitergeben soll.
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0*...*15*, Default-wert ist *0*).

Tabelle 1-1: Felder im Menü ***ROUTING*** ➜ ***ADD/EDIT***

NETWORK enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
LAN	Route zu einem Ziel-Host oder -Netzwerk, das über den LAN-Anschluß Ihres Gateways zu erreichen ist.
WAN without transit network	Route zu einem Ziel-Host oder -Netzwerk, welche über einen WAN Partner zu erreichen sind ohne Berücksichtigung eines evtl. vorhandenen Transitnetzwerks.
WAN with transit network	Route zu einem Ziel-Host oder -Netzwerk, welche über einen WAN Partner zu erreichen sind unter Berücksichtigung eines vorhandenen Transitnetzwerks.
Refuse	Ihr Gateway verwirft Datenpakete, die diese Route benutzen, und übermittelt dem Absender eine Meldung, dass das Ziel des Paketes unerreichbar ist.
Ignore	Ihr Gateway verwirft Datenpakete, die diese Route benutzen ohne Rückmeldung zum Absender.

Tabelle 1-2: Auswahlmöglichkeiten von ***NETWORK***

Zusätzlich zu der normalen Routing-Tabelle kann des **XGeneration** Gateway auch Routing-Entscheidungen aufgrund einer erweiterten Routing-Tabelle, der Extended-Routing-Tabelle, treffen. Dabei kann das **XGeneration** Gateway neben der Quell- und Zieladresse u. a. auch das Protokoll, Quell- und Ziel-Port, Art des Dienstes (Type of Service, TOS) und den Status der Gateway-Schnittstelle in die Entscheidung mit einbeziehen.

Hinweis

Einträge in der Extended-Routing-Tabelle werden gegenüber den Einträgen in der normalen Routing-Tabelle bevorzugt behandelt.

Die Konfiguration erfolgt im Menü ***IP*** ➜ ***ROUTING*** ➜ ***ADDEXT***.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][ROUTING][ADD]: IP Routing - Extended Route              MyGateway


 Route Type                  Host route
 Network                     LAN

 Destination IP-Address


 Gateway IP-Address
 Metric                      1
 Source Interface            don't verify
 Source IP-Address
 Source Mask
 Type of Service (TOS)       00000000  TOS Mask  00000000
 Protocol                    don't verify


           SAVE                                  CANCEL
```

Zusätzlich zu den Feldern des Menüs ***ROUTING*** ➜ ***ADD/EDIT*** werden in diesem Menü folgende Felder angezeigt:

Feld	Wert
Mode	Nur für ***NETWORK*** = *WAN without transit network*. Definiert, wann das unter ***PARTNER*** / ***INTERFACE*** gewählte Interface benutzt werden soll. Mögliche Werte siehe Tabelle “Auswahlmöglichkeiten von Mode” auf Seite 10.
Source Interface	Schnittstelle, über die die Datenpakete das Gateway erreichen. Defaultwert ist *don’t verify*.
Source IP-Address	Adresse des Quell-Hosts bzw. -Netzwerks.
Source Mask	Netzmaske zu ***SOURCE IP-ADDRESS***
Type of Service (TOS)	Mögliche Werte: *0..255* im binären Format.
TOS Mask	Bitmaske zu ***TYPE OF SERVICE (TOS)***
Protocol	Legt ein Protokoll fest. Mögliche Werte: *don’t verify*, *icmp*, *ggp, tcp*, *egp*, *pup*, *udp*, *hmp*, *xns*, *rdp*, *rsvp*, *gre*, *esp*, *ah*, *igrp*, *ospf*, *l2tp*. Defaultwert ist *don’t verify*.
Source Port	Nur für ***PROTOCOL*** = *tcp* oder *udp*. Quell-Port-Nummer bzw. Bereich von Quell-Port-Nummern (siehe Tabelle “Auswahlmöglichkeiten von Source Port bzw. Destination Port” auf Seite 10).
Destination Port	Nur für ***PROTOCOL*** = *tcp* oder *udp*. Ziel-Port-Nummer bzw. Bereich von Ziel-Port-Nummern (siehe Tabelle “Auswahlmöglichkeiten von Source Port bzw. Destination Port” auf Seite 10).

Tabelle 1-3: Felder im Menü ***ROUTING*** ➜ ***ADDEXT***

MODE enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
always (Defaultwert)	Route immer benutzbar.
dialup-wait	Route benutzbar, wenn das Interface "up" ist. Ist das Interface "dormant", dann wählen und warten, bis das Interface "up" ist.
dialup-continue	Route benutzbar, wenn das Interface "up" ist. Ist das Interface "dormant", dann wählen und solange die Alternative Route benutzen (rerouting), bis das Interface "up" ist.
up-only	Route benutzbar, wenn das Interface "up" ist.

Tabelle 1-4: Auswahlmöglichkeiten von ***MODE***

SOURCE PORT bzw. ***DESTINATION PORT*** enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
any (Defaultwert)	Die Route gilt für alle ➤➤ **Port**-Nummern.
specify	Ermöglicht Eingabe einer Port-Nummer.
specify range	Ermöglicht Eingabe eines Bereiches von Port-Nummern.
priv (0...1023)	priviligierte Port-Nummern: 0 ... 1023.
server (5000....32767)	Server Port-Nummern: 5000 ... 32767.
clients 1 (1024....4999)	Client Port-Nummern: 1024 ... 4999.
clients 2 (32768....65535)	Client Port-Nummern: 32768 ... 65535.
unpriv (1024...65535)	unpriviligierte Port-Nummern: 1024 ... 65535.

Tabelle 1-5: Auswahlmöglichkeiten von ***SOURCE PORT BZW. DESTINATION PORT***

2 Untermenü Static Settings

Im Folgenden wird das Untermenü *STATIC SETTINGS* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][STATIC]: IP Static Settings                              MyGateway

    Domain Name
    Primary Domain Name Server
    Secondary Domain Name Server
    Primary WINS
    Secondary WINS
    Time Protocol                    TIME/UDP
    Time Offset (sec)                0
    Time Update Interval (sec)       86400
    Time Server

    Remote TRACE Server TCP port     7000
    RIP UDP port                     520
    Primary BOOTP Relay Server
    Secondary BOOTP Relay Server
    Unique Source IP Address
    HTTP TCP port                    80

          SAVE                                CANCEL
```

In ***IP*** ➜ ***STATIC SETTINGS*** konfigurieren Sie die generellen IP-Einstellungen für Ihr Gateway.

Das Menü ***IP*** ➜ ***STATIC SETTINGS*** besteht aus folgenden Feldern:

Feld	Wert
Domain Name	Default Domain Name des Gateways.
Primary Domain Name Server	IP-Adresse eines globalen Domain Name Serves (DNS).
Secondary Domain Name Server	IP-Adresse eines alternativen globalen Domain Name Servers.
Primary WINS	IP-Adresse eines globalen Windows Internet Name Servers (=WINS) oder NetBIOS Name Servers (=NBNS).
Secondary WINS	IP-Adresse eines alternativen globalen WINS oder NBNS.

Feld	Wert
Time Protocol	Protokoll, das für das Beziehen der aktuellen Zeit benutzt wird. Mögliche Werte: siehe “Auswahlmöglichkeiten von Time Protocol” auf Seite 14. Defaultwert ist *Time/UDP*.
Time Offset (sec)	Anzahl der Sekunden, die zu der bezogenen Zeit addiert oder subtrahiert wird. Wenn Sie Werte zwischen -24 und +24 eingeben, versteht das **XGeneration** Gateway die Angabe als Anzahl von Stunden und wandelt sie nach Bestätigen mit **SAVE** automatisch in die entsprechende Anzahl von Sekunden um. Beachten Sie: Eine Änderung des Time Offset (Zeit zurückstellen) im aktiven Betrieb sollte vermieden werden, da der bestehende Datenfluss dadurch gestört wird. Defaultwert ist *0*.
Time Update Interval (sec)	Zeitintervall in Sekunden, nach dem die Systemzeit überprüft und ggf. aktualisiert wird. Wenn Sie Werte zwischen *1* und *24* eingeben, versteht das **XGeneration** Gateway die Angabe als Anzahl von Stunden und wandelt sie nach dem Drücken von **SAVE** automatisch in die entsprechende Anzahl von Sekunden um. Bei ***TIME PROTOCOL*** = *TIME/UDP*, *TIME/TCP* oder *SNTP*: Aktuelle Zeit wird alle ***TIME UPDATE INTERVAL*** Sekunden überprüft. Bei ***TIME PROTOCOL*** = *ISDN*: Aktuelle Zeit wird jeweils bei der ersten ausgehenden ISDN-Verbindung nach Ablauf von ***TIME UPDATE INTERVAL*** überprüft. Defaultwert ist *86400*.
Time Server	IP-Adresse des Time-➤➤ **Servers**, den das **XGeneration** Gateway nutzt. ***TIME SERVER*** wird nicht benötigt, wenn Sie ISDN als ***TIME PROTOCOL*** einstellen.

Feld	Wert
Remote CAPI Server TCP port	TCP-Port-Nummer für ➤➤ **Remote-CAPI**-Verbindungen. Defaultwert ist *2662*. Deaktivieren mit *0*.
Remote TRACE Server TCP port	TCP-Port-Nummer für Remote Traces. Defaultwert ist *7000*. Deaktivieren mit *0*.
RIP UDP port	UDP-Port-Nummer für ➤➤ **RIP** (Routing Information Protocol). Defaultwert ist *520*. Deaktivieren mit *0*.
Primary BOOTP Relay Server	Hier können Sie die IP-Adresse eines Servers angeben, an den BootP- oder DHCP-Anfragen weitergeleitet werden.
Secondary BOOTP Relay Server	Hier können Sie die IP-Adresse eines alternativen BootP- oder DHCP-Servers angeben.
Unique Source IP Address	Hier können Sie eine IP-Adresse eingeben, die vom Gateway für lokal generierte IP-Pakete als Quelladresse verwendet wird. Dieses sollte nur in Spezialfällen konfiguriert werden.
HTTP TCP port	Hier geben Sie den TCP-Port ein, über den Sie auf den HTTP-Dienst des Gateways (HTML Startseite) zugreifen können. Defaultwert ist *80*.

Tabelle 2-1: Felder im Menü ***STATIC SETTINGS***

TIME PROTOCOL enthält folgende Auswahlmöglichkeiten:

Feld	Wert
TIME/UDP (Defaultwert)	Systemzeit (RFC 868) über ➤➤ **UDP** Port 37 beziehen.
TIME/TCP	Systemzeit (RFC 868) über ➤➤ **TCP** Port 37 beziehen.
SNTP	Systemzeit per SNTP (Simple Network Time Protocol, RFC 1769) über UDP Port beziehen.

Feld	Wert
ISDN	Systemzeit aus dem ISDN-➤➤ **D-Kanal** entnehmen.
none	Systemzeit nicht von extern beziehen.

Tabelle 2-2: Auswahlmöglichkeiten von ***TIME PROTOCOL***

3 Untermenü Network Address Translation

Im Folgenden wird das Menü *IP* ➜ *NETWORK ADDRESS TRANSLATION* beschrieben.

Network Address Translation (➤➤ **NAT**) ist eine Funktion Ihres Gateways, um Quell- und Zieladressen von IP-Paketen definiert umzusetzen (in ***SESSIONS REQUESTED FROM INSIDE*** und ***SESSIONS REQUESTED FROM OUTSIDE***). Mit aktiviertem NAT werden weiterhin IP-Verbindungen standardmässig nur noch in einer Richtung, ausgehend (forward) zugelassen (=Schutzfunktion). Ausnahmeregeln können konfiguriert werden (in ***SESSIONS REQUESTED FROM OUTSIDE***).

Das Menü ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** zeigt eine Liste aller Interfaces Ihres Gateways an.

Zum Editieren eines Eintrags markieren Sie mit dem Cursor das Interface, für das Sie NAT konfigurieren wollen, und bestätigen Sie mit der **Eingabetaste**. Folgendes Menü öffnet sich:

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][NAT][EDIT]: NAT Configuration (Internet)                MyGateway


 Network Address Translation         off
 Silent Deny                         no
 PPTP Passthrough                    no

 Enter configuration for sessions:   requested from OUTSIDE
                                     requested from INSIDE




              SAVE                              CANCEL
```

Das Menü ***NETWORK ADDRESS TRANSLATION*** ➜ ***EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Network Address Translation	Definiert die Art von NAT für die ausgewählte Schnittstelle. Mögliche Werte: ■ *off* (Defaultwert): Kein NAT ausführen. ■ *on*: Forward NAT ausführen. ■ *reverse*: Reverse NAT ausführen.
Silent Deny	Definiert, ob der Absender eines von NAT verworfenen IP-Paketes über die Ablehnung informiert wird. Mögliche Werte: ■ *no* (Defaultwert): Absender wird mit einer entsprechenden ICMP Nachricht informiert. ■ *yes*: Absender wird nicht informiert.
PPTP Passthrough	PPTP-Passthrough erlaubt auch bei aktiviertem NAT den Aufbau und Betrieb mehrerer gleichzeitiger ausgehender PPTP-Verbindungen von Hosts im Netzwerk. Mögliche Werte: *yes* oder *no*. Bei ***PPTP-PASSTHROUGH*** = *yes* darf das Gateway selber nicht als Tunnel-Endpunkt konfiguriert werden.

Tabelle 3-1: Felder im Menü ***NETWORK ADDRESS TRANSLATION***

3.1 Untermenü Requested from OUTSIDE/INSIDE

Im Folgenden wird das Menü *REQUESTED FROM OUTSIDE/INDSIDE* beschrieben.

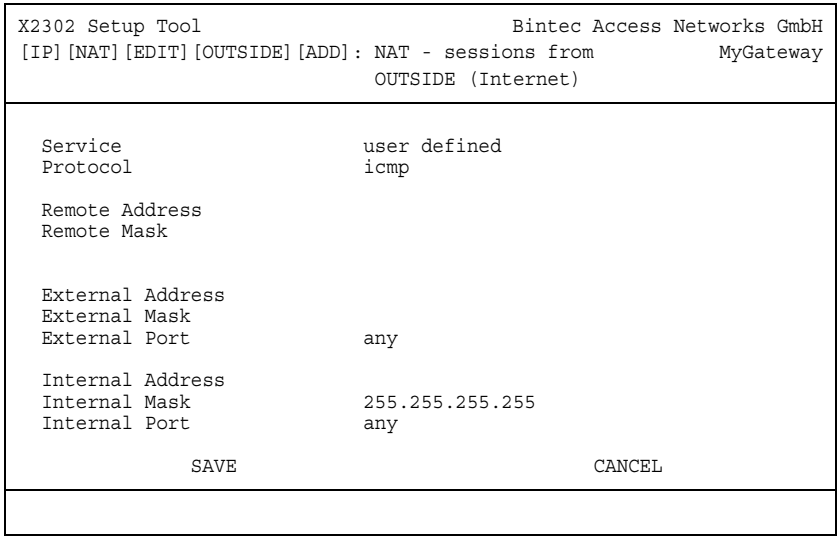
Für weitere NAT-Einstellungen enthält das Menü ***IP ➜ NETWORK ADDRESS TRANSLATION ➜ EDIT*** zwei Untermenüs (die beiden Menüs unterscheiden sich nur geringfügig in den Einstellungsmöglichkeiten):

- ***IP ➜ NETWORK ADDRESS TRANSLATION ➜ EDIT ➜ REQUESTED FROM OUTSIDE***
  In diesem Menü kann man bestimmte eingehende IP-Verbindungen zulassen.
- ***IP ➜ NETWORK ADDRESS TRANSLATION ➜ EDIT ➜ REQUESTED FROM INSIDE***
  In diesem Menü kann man für bestimmte ausgehende IP-Verbindungen die Quell-IP-Adressen bzw. -Ports definiert umsetzen (=Adressmapping).

In beiden Menüs wird eine Liste der bereits konfigurierten Adress-Mappings angezeigt. Die verwendeten Abkürzungen sind oberhalb der Liste erläutert.

```
X2302 Setup Tool                     Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT - sessions from           MyGateway
                               OUTSIDE (Internet)

Abbreviations:   r(remote) i(internal) e(external) a(address) p(port)

  Service      Conditions
  ------------------------------------------------------------
  http         ia 192.168.0.254/32, ep 80, ip 80




    ADD                 DELETE                        EXIT
```

Fügen Sie einen Eintrag mit ***ADD*** hinzu oder bearbeiten Sie einen bestehenden Eintrag, indem Sie ihn mit dem Cursor markieren und mit **Return** bestätigen. Folgendes Menü öffnet sich:



Das Menü ***REQUESTED FROM OUTSIDE/INSIDE ➜ ADD/EDIT*** besteht aus folgenden Feldern:

Wert	Wert
Service	***REQUESTED FROM OUTSIDE ➜ ADD/EDIT***: Dienst, für den eingehende Verbindungen zugelassen werden. ***REQUESTED FROM INSIDE ➜ ADD/EDIT***: Dienst, für den bei ausgehenden Verbindungen das Adress-Mapping definiert wird. Mögliche Werte: *ftp, telnet, smtp, domain/udp, domain/tcp, http, nntp, user defined* (für sonstige Dienste, Defaultwert)
Protocol	Nur für ***SERVICE*** = *user defined*. Definiert das Protokoll. Mögliche Werte: *icmp, tcp, udp, gre, esp, ah, l2tp,any*

Wert	Wert
Remote Address	Optional. IP-Adresse eines Hosts oder Netzwerks auf der entfernten Seite. Freigabe bzw. Adress-Mapping gilt nur für Pakete dieses Hosts oder Netzwerks.
Remote Mask	Netzmaske zu ***REMOTE ADDRESS***.
Remote Port Port...to Port	Nur im Menü ***REQUESTED FROM INSIDE*** ➜ ***ADD/EDIT***. Nur für ***SERVICE*** = *user defined*. Angabe des Ziel-Ports bzw. Portbereichs für ausgehende IP-Verbindungen, für die ein Adress-Mapping durchgeführt werden soll. Mögliche Werte: ■ *any* ■ *specify*: ermöglicht die Eingabe einer Port-Nummer ■ *specify range*: ermöglicht die Eingabe eines Port-Nummern-Bereichs.
External Address	Nach aussen hin wirksame (externe) Host- bzw. Netz-IP-Adresse am ausgewählten Interface.
External Mask	Netzmaske zu ***EXTERNAL ADDRESS***. Wenn Sie externe und interne Netz-IP-Adressen verwenden, müssen die Werte für ***EXTERNAL MASK*** und ***INTERNAL MASK*** identisch sind.

Wert	Wert
External Port Port...to Port	Nur für ***SERVICE*** = *user defined*. ■ ***REQUESTED FROM OUTSIDE →ADD/EDIT***: nur für ***SERVICE*** = *user defined*; ursprünglicher Zielport der eingehenden IP-Verbindung. ■ ***REQUESTED FROM INSIDE → ADD/EDIT:*** der neu gesetzte Quellport der ausgehenden IP-Verbindung. Mögliche Werte: ■ *any* (Defaultwert): bei ***REQUESTED FROM INSIDE → ADD/EDIT*** bedeutet dies keine Port-Umsetzung ■ *specify*: ermöglicht die Eingabe einer Port-Nummer ■ *specify range* (nur für ***REQUESTED FROM OUTSIDE → ADD/EDIT***) ermöglicht die Eingabe eines Port-Nummern-Bereichs.
Internal Address	IP-Adresse des internen Hosts oder Netzes.
Internal Mask	Netzmaske zu ***INTERNAL ADDRESS***. Wenn Sie externe und interne Netz-IP-Adressen verwenden, müssen die Werte für ***EXTERNAL MASK*** und ***INTERNAL MASK*** identisch sind.

Wert	Wert
Internal Port Port	■ ***REQUESTED FROM OUTSIDE ➜ ADD/EDIT***: neu gesetzter Zielport der eingehenden IP-Verbindung. ■ ***REQUESTED FROM INSIDE ➜ ADD/EDIT:*** ursprünglicher Quellport der ausgehenden IP-Verbindung. Mögliche Werte: ■ *any* (Defaultwert): bei ***REQUESTED FROM OUTSIDE ➜ ADD/EDIT*** bedeutet dies keine Port-Umsetzung. ■ *specify*: ermöglicht die Eingabe einer Port-Nummer.

Tabelle 3-2: Felder im Menü ***REQUESTED FROM OUTSIDE/INSIDE***

3 Untermenü Network Address Translation

4 Untermenü Bandwidth Management (Load Balancing / BOD)

Im Folgenden wird das Menü *BANDWIDTH MANAGEMENT (LOAD BALANCING/ BOD)* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][BW]: Bandwidth Management for IP                        MyGateway

        IP Load Balancing over Multiple Interfaces

        EXIT
```

Über das Menü ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)*** gelangt man in das Untermenü:

- ***IP LOAD BALANCING OVER MULTIPLE INTERFACES***

4.1 Untermenü IP Load Balancing over Multiple Interfaces

Im Folgenden wird das Menü *IP LOAD BALANCING OVER MULTIPLE INTERFACES* beschrieben.

Zunehmender Datenverkehr über das Internet erfordert die Möglichkeit, Daten über unterschiedliche Interfaces senden zu können, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen. IP Load Balancing ermöglicht die geregelte Verteilung von Datenverkehr innerhalb einer bestimmten Gruppe von Interfaces.

Die Konfiguration erfolgt im Menü ***IP*** ➜ ***BANDWIDTH MANAGEMENT (LOAD BALANCING/BOD)*** ➜ ***IP LOAD BALANCING OVER MULTIPLE INTERFACES***.

Hier wird eine Liste der bereits für Load Balancing konfigurierten Interface-Gruppen angezeigt.

Über ***ADD/EDIT*** gelangen Sie in das Menü zur Konfiguration der Gruppen.

```
X2302 Setup Tool                              Bintec Access Networks GmbH
[IP][IP LOAD BALANCING][ADD]                                    MyGateway

   Description
   Interface Group ID    0

   Distribution Policy   session round-robin
   Distribution Mode     always (use operational up and
                         dormant interfaces)
   Distribution Ratio    equal for all interfaces of the
                         group

   Interface 1                                  none

   Interface 2                                  none

   Interface 3                                  none

                  SAVE              CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Description	Hier geben Sie eine beliebige Beschreibung der Interface-Gruppe ein.
Interface Group ID	Die ID der Interface-Gruppe. Sie wird vom System automatisch vergeben, kann aber auch editiert werden. Sie dient lediglich der internen Zuordnung der Gruppe. Defaultwert ist *0*.

Feld	Wert
Distribution Policy	Hier wählen Sie aus, auf welche Art der Datenverkehr auf die für die Gruppe konfigurierten Interfaces verteilt wird. Mögliche Werte: siehe “Auswahlmöglichkeiten von Distribution Policy” auf Seite 27
Distribution Mode	Hier wählen Sie aus, welchen Zustand die Interfaces der Gruppe haben dürfen, damit sie ins Load Balancing einbezogen werden dürfen. Zur Verfügung stehen: ■ *always (use operational up and dormant interfaces)*: Interfaces, die entweder up oder dormant sind, werden einbezogen. (Defaultwert) ■ *up-only (operational up interfaces only):* Nur Interfaces, die up sind, werden einbezogen.
Distribution Ratio	Nicht für ***DISTRIBUTION POLICY*** = *service/source-based routing*. Hier wählen Sie aus, ob die prozentuale Aufteilung des Datenverkehrs für alle Interfaces der Gruppe die gleiche sein oder ob sie für jedes Interface individuell konfiguriert werden soll. Zur Verfügung stehen: ■ *equal for all interfaces of the group* (Defaultwert): Allen Interfaces wird automatisch der gleiche Anteil zugewiesen. ■ *individual for all interfaces of the group*: Jedem Interface kann individuell ein Anteil zugewiesen werden.
Interface 1 - 3	Hier wählen Sie unter den zur Verfügung stehenden Interfaces diejenigen aus, die der Gruppe angehören sollen.

Feld	Wert
Distribution Fraction (in percent)	Nicht für ***DISTRIBUTION POLICY*** = *service/source-based routing*. Erscheint nur, wenn bei ***INTERFACE 1 - 3*** ein Interface ausgewählt wurde. Hier geben Sie an, welchen Prozentsatz des Datenverkehrs ein Interface übernehmen soll. Die Bedeutung unterscheidet sich je nach verwendeter ***DISTRIBUTION POLICY***: ■ für *session round robin* wird die Anzahl der zu verteilenden Sessions zugrunde gelegt. ■ für *bandwidth load-/upload-/download-dependent* ist die Datenrate maßgeblich.

Tabelle 4-1: Felder im Menü ***IP LOAD BALAMCING OVER MULTIPLE INTERFACES***

DISTRIBUTION POLICY enthält folgende Auswahlmöglichkeiten:

Feld	Wert
session round-robin	Eine neu hinzukommende Session wird je nach prozentualer Belegung der Interfaces mit Sessions einem der Gruppen-Interfaces zugewiesen. Die Anzahl der Sessions ist maßgeblich.
bandwidth load-dependent	Eine neu hinzukommende Session wird je nach Anteil der Interfaces an der Gesamtdatenrate einem der Gruppen-Interfaces zugewiesen. Maßgeblich ist die aktuelle Datenrate, wobei der Datenverkehr sowohl in Sende- als auch in Empfangsrichtung berücksichtigt wird.
bandwidth download-dependent	Eine neu hinzukommende Session wird je nach Anteil der Interfaces an der Gesamtdatenrate einem der Gruppen-Interfaces zugewiesen. Maßgeblich ist die aktuelle Datenrate, wobei nur der Datenverkehr in Empfangsrichtung berücksichtigt wird.

Feld	Wert
bandwidth upload-dependent	Eine neu hinzukommende Session wird je nach Anteil der Interfaces an der Gesamtdatenrate einem der Gruppen-Interfaces zugewiesen. Maßgeblich ist die aktuelle Datenrate, wobei nur der Datenverkehr in Senderichtung berücksichtigt wird.
service/source-based routing	Eine neu hinzukommende Session wird einem der Gruppen-Interfaces gemäß der Konfiguration des statischen Routings im Menü ***IP Load Balancing over Multiple Interfaces ➜ ADD/EDIT ➜ IP Routing List*** zugewiesen. Das Menü ist nur zugänglich, wenn Sie *service/source-based routing* ausgewählt haben. siehe “Untermenü IP Routing List” auf Seite 27

Tabelle 4-2: Auswahlmöglichkeiten von ***Distribution Policy***

4.1.1 Untermenü IP Routing List

Das Menü *IP Routing List* erscheint nur, wenn in *Distribution Policy* *service/source-based routing* und bei *Interface 1 - 3* ein Interface ausgewählt wurde.

Das Menü ***IP Load Balancing over Multiple Interfaces ➜ ADD/EDIT ➜ IP Routing List*** enthält eine Liste aller konfigurierter Routing Einträge. Die Konfiguration erfolgt in ***IP Routing List ➜ ADD/EDIT***.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][ROUTING][ADD]: Configure Service/Source-Based Routing   MyGateway

  Interface                    Internet1

  Type                         Host route
  Network                      WAN without transit network

  Destination IP-Address

  Gateway IP-Address

  Source IP-Address
  Source Mask

  Protocol                     tcp
  Service                      unlisted service     Port  -1


             SAVE                              CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Interface	Zeigt das zu bearbeitende Interface an. Dieses Feld kann nicht verändert werden.
Type	Art der Route. Mögliche Werte: ■ *Host route*: Route zu einem einzelnen Host ■ *Network route* (Defaultwert): Route zu einem Netzwerk ■ *Default route*: Die Route gilt für alle IP-Adressen und wird nur benutzt, wenn keine andere passende Route verfügbar ist
Network	Definiert die Art der Verbindung (LAN, WAN). Mögliche Werte, siehe Tabelle “Auswahlmöglichkeiten von Network” auf Seite 30.

Feld	Wert
Destination IP-Address	Nur für ***ROUTE TYPE*** *Host route* oder *Network route*. IP-Adresse des Ziel-Hosts oder -Netzwerks.
Destination Mask	nur für ***ROUTE TYPE*** = *Network route* Netzmaske zu Destination IP-Address. Wenn kein Eintrag erfolgt, benutzt das Gateway eine Standardnetzmaske.
Gateway IP-Address	Nur für ***NETWORK*** *LAN* oder *WAN with transit network*. IP-Adresse des Hosts, an den Ihr Gateway die IP-Pakete weitergeben soll.
Source IP-Address	IP-Adresse des Quell-Hosts bzw. -Netzwerks.
Source Mask	Netzmaske zu ***SOURCE IP-ADDRESS***
Protocol	Legt ein Protokoll fest. Mögliche Werte: *tcp*, *egp*, *pup*, *udp*, *hmp*, *xns*, *rdp*, *rsvp*, *gre*, *esp*, *ah*, *igrp*, *ospf*, *l2tp*, *don't verify*, *icmp*, *ggp*. Defaultwert ist *dont verify*.
Service	Hier wählen Sie einen vordefinierten Service, für dessen Datenverkehr der Eintrag gelten soll. Beim Zugriff auf das Menü wird der Wert *unlisted service* angezeigt. Dies ist lediglich ein Platzhalter. Der Datenverkehr wird durch diesen Eintrag solange nicht gefiltert, wie man den Defaultwert *-1* im Feld ***PORT*** belässt.
Port	Nur editierbar, wenn ***PROTOCOL*** = *tcp* oder *udp* und ***SERVICE*** = *unlisted service*. Eingabe des Zielports zu ***PROTOKOLL*** *tcp* oder *udp*. Zur Verfügung stehen die Werte von *-1* bis *65535*. Der Defaultwert *-1* bedeutet, dass der Zielport beliebig ist.

Tabelle 4-3: Felder im Menü ***IP ROUTING LIST*** ➜ ***ADD/EDIT***

NETWORK enthält folgende Auswahlmöglichkeiten (abhängig vom Typ des Interfaces):

Wert	Bedeutung
LAN	Route zu einem Ziel-Host oder -Netzwerk, das über den LAN-Anschluß Ihres Gateways zu erreichen ist.
WAN without transit network	Route zu einem Ziel-Host oder -Netzwerk, welche über einen WAN Partner zu erreichen sind ohne Berücksichtigung eines evtl. vorhandenen Transitnetzwerks.
WAN with transit network	Route zu einem Ziel-Host oder -Netzwerk, welche über einen WAN Partner zu erreichen sind unter Berücksichtigung eines vorhandenen Transitnetzwerks.

Tabelle 4-4: Auswahlmöglichkeiten von ***NETWORK***

5 Untermenü IP address pool WAN (PPP)

Im Folgenden wird das Menü *IP ADDRESS POOL WAN (PPP)* beschrieben.

In ***IP ➜ IP ADDRESS POOL WAN (PPP)*** können Sie einen Pool von IP-Adressen einrichten, die das **XGeneration** Gateway als dynamischer IP-Address-Server an WAN Partner vergibt, die sich einwählen.

Hier werden alle konfigurierten IP-Adress-Pools aufgelistet. Die Konfiguration erfolgt im Menü ***IP ADDRESS POOL WAN (PPP) ➜ ADD/EDIT.***

```
X2302 Setup Tool                              Bintec Access Networks GmbH
[IP][DYNAMIC][EDIT]                                              MyGateway

 Pool ID                                  0
 IP Address                               192.168.0.11
 Number of consecutive addresses          2




          SAVE                                    CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Pool ID	Eindeutige Nummer zur Identifizierung eines IP-Adress-Pools.
IP Address	Erste IP-Adresse des Bereiches.
Number of consecutive addresses	Anzahl der IP-Adressen im Bereich, einschließlich der ersten IP-Adresse. Defaultwert ist *1*.

Tabelle 5-1: Felder im Menü ***IP ADDRESS POOL WAN (PPP)***

5 Untermenü IP address pool WAN (PPP)

6 Untermenü IP address pool LAN (DHCP)

Im Folgenden wird das Menü *IP ADDRESS POOL LAN (DHCP)* beschrieben.

In ***IP ➜ IP ADDRESS POOL LAN (DHCP)*** konfigurieren Sie das **XGeneration** Gateway als ➤➤ **DHCP**-Server (Dynamic Host Configuration Protocol).

Hier werden alle konfigurierten Interfaces und entsprechende IP-Adresspools aufgelistet. Die Konfiguration erfolgt im Menü ***IP ADDRESS POOL LAN (DHCP) ➜ ADD/EDIT.***

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][DHCP][ADD]: Define Range of IP Addresses                MyGateway


  Interface                                 en0-1
  Type                                      Any
  IP Address
  Number of consecutive addresses           1
  Lease Time (Minutes)                      120
  MAC Address


  Gateway
  NetBT Node Type                           not specified



        SAVE                                 CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Interface	Schnittstelle, welcher der Adress-Pool zugewiesen wird. Wenn ein DHCP-Request über ***INTERFACE*** eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.
IP Address	Erste IP-Adresse des Adress-Pools.

Feld	Wert
Number of consecutive addresses	Anzahl der IP-Adressen im Adress-Pool, einschließlich der ersten IP-Adresse (***IP ADDRESS***). Defaultwert ist *1*.
Lease Time (Minutes)	Legt fest, wie lange eine Adresse aus dem Pool einem Host zugewiesen wird. Nachdem ***LEASE TIME (MINUTES)*** abgelaufen ist, kann die Adresse neu vergeben werden. Defaultwert ist *120*.
MAC Address	Nur bei ***NUMBER OF CONSECUTIVE ADDRESSES*** = *1* Nur dem Gerät mit ***MAC ADDRESS*** wird ***IP ADDRESS*** zugewiesen.
Gateway	Legt fest, welche IP-Adresse dem DHCP-Client als Gateway übermittelt wird. Wenn hier keine IP-Adresse eingetragen wird, wird die in ***INTERFACE*** definierte IP-Adresse übertragen.
NetBT Node Type	Legt fest, wie und in welcher Reihenfolge die Auflösung von NetBIOS-Namen zu IP-Adressen vom Host durchgeführt wird. Mögliche Werte: ■ *not specified* (Defaultwert) ■ *Broadcast Node* ■ *Point-to-Point Node* ■ *Mixed Node* ■ *Hybrid Node*

Tabelle 6-1: Felder im Menü ***IP ADDRESS POOL LAN (DHCP)***

7 Untermenü SNMP

Im Folgenden wird das Menü *SNMP* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][SNMP]: SNMP Configuration                              MyGateway


     SNMP listen UDP port       161
     SNMP trap UDP port         162
     SNMP trap broadcasting     off
     SNMP trap community        snmp-Trap




        SAVE                                CANCEL
```

In ***IP*** ➜ ***SNMP*** können Sie grundlegende ➤➤ **SNMP**-Einstellungen ändern.

Das Menü ***SNMP*** enthält folgende Felder:

Feld	Wert
SNMP listen UDP port	Hier geben Sie die Nummer des udp-Ports ein, unter dem das Gateway SNMP-Requests annimmt. Defaultwert ist *161*. *0* deaktiviert die Funktion.
SNMP trap UDP port	Hier geben Sie die Nummer des udp-Ports ein, zu dem das Gateway SNMP Traps sendet. Defaultwert ist *162*. *0* deaktiviert die Funktion.
SNMP trap broadcasting	Hier können Sie SNMP Trap Broadcasting aktivieren. Das Gateway sendet SNMP Traps dann an die Broadcastadresse des LANs. Mögliche Werte on und *off* (Defaultwert).

Feld	Wert
SNMP trap community	Hier können Sie eine SNMP Kennung eingeben. Diese muss vom SNMP-Manager mit jedem SNMP Request übergeben werden, damit dieser von Ihrem Gateway akzeptiert wird. Defaultwert ist *snmp-Trap*.

Tabelle 7-1: Felder im Menü ***SNMP***

8 Untermenü Remote Authentication (RADIUS/TACACS+)

Im Folgenden wird das Menü *Remote Authentication (RADIUS/TACACS+)* beschrieben.

Das Menü ***IP*** ➜ ***Remote Authentication (RADIUS/TACACS+)*** führt in folgendes Untermenü:

- ***RADIUS Authentication and Accounting***
- ***TACACS+ Authentication and Authorization***

8.1 Untermenü RADIUS Authentication and Accounting

Im Folgenden wird das Menü *Radius Server* beschrieben.

Client / Server

RADIUS (Remote Authentication Dial In User Service) ist ein Dienst, der es ermöglicht, Authentifizierungs- und Konfigurationsinformationen zwischen Ihrem Gateway und einem RADIUS Server auszutauschen. Der RADIUS Server verwaltet eine Datenbank mit Informationen zur Benutzerauthentifizierung, zur Konfiguration und für die statistische Erfassung von Verbindungsdaten.

RADIUS kann angewendet werden für:

- Authentifizierung
- Accounting
- Austausch von Konfigurationsdaten.

Bei einer eingehenden Verbindung sendet das Bintec Gateway einen Request mit Benutzername und Passwort an den RADIUS Server, woraufhin dieser seine Datenbank abfragt. Wenn der Benutzer gefunden wurde und authentifiziert werden kann, sendet der RADIUS Server eine entsprechende Bestätigung zum Gateway. Diese Bestätigung beinhaltet auch Parameter (sog. RADIUS Attribute), die das Gateway als WAN-Verbindungparameter verwendet.

Wenn der RADIUS Server für Accounting verwendet wird, sendet das Gateway eine Accounting-Meldung am Anfang der Verbindung und eine Meldung am Ende der Verbindung. Diese Anfangs- und Endmeldungen beinhalten zudem statistische Informationen zur Verbindung (IP-Adresse, Benutzername, Durchsatz, Kosten).

RADIUS Pakete

Folgende Pakettypen werden zwischen RADIUS Server und Bintec Gateway (Client) versendet:

Typ	Zweck
ACCESS_REQUEST	Client –> Server Wenn ein Verbindungs Request auf dem Gateway empfangen wird, wird beim RADIUS Server angefragt, falls im Gateway kein entsprechender WAN Partner gefunden wurde.
ACCESS_ACCEPT	Server –> Client Wenn der RADIUS Server die im ACCESS_REQUEST enthaltenen Informationen authentifiziert hat, sendet er einen ACCESS_ACCEPT zum Gateway mit den für den Verbindungsaufbau zu verwendenden Parametern.
ACCESS_REJECT	Server –> Client Wenn die im ACCESS_REQUEST enthaltenen Informationen nicht den Informationen in der Benutzerdatenbank des RADIUS Servers entsprechen, sendet er ein ACCESS_REJECT zur Ablehung der Verbindung.
ACCOUNTING_START	Client -> Server Wenn ein RADIUS Server für Accounting verwendet wird, sendet das Gateway eine Accounting-Meldung am Anfang jeder Verbindung zum RADIUS Server.

Typ	Zweck
ACCOUNTING_STOP	Client -> Server Wenn ein RADIUS Server für Accounting verwendet wird, sendet das Gateway eine Accounting-Meldung am Ende jeder Verbindung zum RADIUS Server.

Im Menü ***IP*** ➜ ***RADIUS SERVER*** werden alle aktuell konfigurierten RADIUS Server aufgelistet.

Die Konfiguration erfolgt in ***IP*** ➜ ***RADIUS SERVER*** ➜ ***ADD/EDIT***.

```
X2302 Setup Tool                              Bintec Access Networks GmbH
[IP][RADIUS][ADD]                                                MyGateway

Protocol                      authentication

IP Address
Password

Priority                      0
Policy                        authoritative

Port                          1812
Timeout (ms)                  1000
Retries                       1
State                         active
Validate                      enabled
Dialout                       disabled
Alive Check (if inactive)     enabled

          SAVE                                    CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Protocol	Definiert, ob der RADIUS Server für Authentifizierungszwecke oder zum Accounting verwendet wird. Mögliche Werte: ■ *authentication* (Defaultwert) - Der RADIUS Server wird verwendet, um den Zugang zu einem Netzwerk zu regeln. ■ *accounting* - Der RADIUS Server wird zur Erfassung statistischer Verbindungsdaten verwendet. ■ *shell login* - Der RADIUS Server wird verwendet, um den Zugang zur SNMP-Shell des Gateways zu kontrollieren. ■ *IPSec* - Der RADIUS Server wird verwendet, um Konfigurationensdaten für IPSec Peers an das Gateway zu übermitteln.
IP Address	Die IP-Adresse des RADIUS Server.
Password	Dieses ist das für die Kommunikation zwischen RADIUS Server und Gateway gemeinsam genutze Passwort.
Priority	Priorität des RADIUS Servers. Wenn mehrere RADIUS-Server-Einträge bestehen, wird der Server mit der obersten Priorität als erstes verwendet. Wenn dieser Server nicht antwortet, wird der Server mit der nächst niedrigeren Priorität verwendet usw. Mögliche Werte: Ganze Zahlen von *0* (highest priority) bis *7* (lowest priority). Defaultwert ist *0*.

Feld	Wert
Policy	Definiert wie das Bintec Gateway reagiert, wenn eine negative Antwort auf eine Anfrage eingeht. Mögliche Werte: ■ *authoritative* (Defaultwert): Eine negative Antwort auf eine Anfrage wird akzeptiert. ■ *non authoritative*: Eine negative Antwort auf eine Anfrage wird nicht akzeptiert. Der nächste RADIUS Server wird angefragt, bis das Gateway eine Antwort von einem als authoritativ konfigurierten Server erhält.
Port	Verwendeter TCP Port für RADIUS-Daten. Gemäß RFC 2138 sind die Default Ports 1812 für die Authentifizierung (1645 in älteren RFCs) und 1813 für Accounting (1645 in älterne RFCs). Der Dokumentation Ihres RADIUS Servers können Sie entnehmen, welcher Port zu verwenden ist. Defaultwert ist *1812.*
Timeout (ms)	Maximale Wartezeit zwischen ACCESS_REQUEST und Antwort in Millisekunden. Nach Ablauf dieser Zeit wird die Anfrage gemäß ***RETRIES*** wiederholt bzw. der nächste konfigurierte RADIUS Server angefragt. Mögliche Werte: Ganze Zahlen zwischen *50* und *50000*. Defaultwert ist *1000* (1 Sekunde).

Feld	Wert
Retries	Anzahl der Wiederholungen, wenn eine Anfrage nicht beantwortet wird. Falls nach diesen Versuchen dennoch keine Antwort erhalten wurde, wird der ***STATE*** auf *inactive* gesetzt. Das Gateway versucht dann alle 20 Sekunden, den Server zu erreichen, und wenn der Server antwortet, wird ***STATE*** wieder auf *active* zurückgesetzt. Mögliche Werte: Ganze Zahlen zwischen *0* und *10*. Defaultwert ist *1*. Um zu verhindern, dass ***STATE*** auf *inactive* gesetzt wird, setzen Sie diesen Wert auf *0*.
State	Status des RADIUS Servers. Mögliche Werte: ■ *active* (Defaultwert): Server beantwortet Anfragen. ■ *inactive*: Server antwortet nicht (siehe ***RETRIES***). ■ *disabled*: Anfragen an einen bestimmten RADIUS Server sind vorübergehend deaktiviert.
Validate	Mögliche Werte: ■ *enabled* (Defaultwert): Das Gateway überprüft die Identität des RADIUS Servers anhand der MD5-Prüfsumme von ***PASSWORD***. Zur Sicherheit sollte diese Option aktiviert werden. ■ *disabled*: Diese Option sollte nur in Sonderfällen gewählt werden.

Feld	Wert
Dialout	Hier können Sie festlegen, ob das Gateway vom RADIUS Server Dialout-Routen abfragt. Auf diesem Weg können automatisch temporäre Interfaces angelegt werden und das Gateway kann ausgehende Verbindungen initiieren, die nicht fest konfiguriert sind. Mögliche Werte: *enabled*, *disabled* (Default-wert).
Alive Check (if inactive)	Hier aktivieren Sie die Überprüfung der Erreichbarkeit eines RADIUS Servers im ***STATE*** *inactive*. ■ enabled (Defaultwert): Es wird regelmäßig (alle 20 Sekunden) ein Alive-Check durchgeführt durch Senden eines ACCESS_REQUESTs an die IP-Adresse des RADIUS Servers. Bei Erreichbarkeit wird ***STATE*** wieder auf *active* gesetzt. Wenn der RADIUS Server nur über eine Wählverbindung erreichbar ist, können ungewollte Kosten entstehen, wenn dieser Server längere Zeit *inactive* ist. ■ *disabled*: Alive Check wird nicht durchgeführt.

Tabelle 8-1: Felder im Menü ***RADIUS SERVER***

8.2 Untermenü TACACS+ Authentication and Authorization

Im Folgenden wird das Menü *TACACS+ AUTHENTICATION AND AUTHORIZATION* beschrieben.

Das TACACS+ Protokoll ermöglicht die Zugriffssteuerung von Gateways, Netzzugangsservern (NAS) und anderen Netzwerkkomponenten über einen oder mehrere zentrale Server. TACACS+ bietet Authentifizierungs-, Autorisierungs- und Abrechnungsdienste.

Die Konfiguration eines TACACS+ Servers wird über das Menü ***IP ➜ REMOTE AUTHENTICATION (RADIUS/TACACS+) ➜ TACACS+ AUTHENTICATION AND AUTHORIZATION ➜ ADD/EDIT*** vorgenommen.

```
X2302 Setup Tool                              Bintec Access Networks GmbH
[IP][TACACS+][ADD]                                                MyGateway

  Server's IP Address or Hostname

  Priority                                  0            TCP Port  49
  TACACS+ Key (Secret)
  Policy                                    non authoritative
  Encryption (recommended)                  enabled

  Timeout (seconds)                         3
  Block Time (seconds)                      60

  PPP Authentication                        disabled
  Login Authentication/Authorization        enabled
  TACACS+ Accounting                        disabled
  Administrative Status                     up
  TACACS+ Single-Connection                 single request

             SAVE                                   CANCEL
```

Das Menü bietet folgende Konfigurationsoptionen an:

Feld	Beschreibung
Server's IP Address or Hostname	Hier geben Sie die IP-Adresse des TACACS+ Servers ein, der für eine AAA-Anforderung (Authentifizierung, Autorisierung, Abrechnung) abgefragt werden soll.

Feld	Beschreibung
Priority	Hier weisen Sie dem aktuellen TACACS+ Server eine Priorität zu. Der Server mit dem niedrigsten Wert ist der erste, der für die TACACS+ AAA-Anforderung benutzt wird. Falls er keine Antwort gibt oder der Zugriff verweigert wurde (nur im nichtautoritativen Fall, siehe auch das Feld ***Policy***), wird der Eintrag mit der nächstniedrigeren Priorität genutzt. Verfügbare Werte sind *0* bis *9*, der Standardwert ist *0*.
TCP Port	Der für das TACACS+ Protokoll benutzte Standard-TCP-Port ist auf *49* eingestellt. Dieser Wert kann nicht verändert werden.
TACACS+ Key (Secret)	Hier geben Sie das Passwort ein, welches benutzt wird, um den Datenaustausch zwischen dem TACACS+ Server und dem Netzzugangsserver (Ihrem Gateway) zu authentifizieren und (falls zutreffend) zu verschlüsseln. Die maximale Länge des Eintrags ist 32 Zeichen.
Policy	Hier können Sie die Interpretation der TACACS+ Antwort auswählen. Verfügbare Werte sind *authoritative* und *non authoritative*. Wenn in diesem Feld *authoritative* eingetragen ist, wird eine negative Antwort auf eine Anfrage akzeptiert. Dies ist nicht notwendigerweise der Fall, wenn die Einstellung *non authoritative* (Standardwert) lautet. In diesem Fall wird der nächste TACACS+ Server abgefragt, bis eine autoritative Antwort kommt.

Feld	Beschreibung
Encryption (recommended)	Hier können Sie festlegen, ob der Datenaustausch zwischen dem TACACS+ Server und dem NAS verschlüsselt werden soll oder nicht. Verfügbare Werte sind *enabled* (Standardwert) und *disabled*. Falls *enabled* eingestellt wird, werden die TACACS+ Pakete mit MD5 verschlüsselt. Andernfalls - bei Einstellung auf *disabled* - werden die Pakete und damit alle dazugehörigen Informationen unverschlüsselt übertragen. Eine unverschlüsselte Übertragung wird nicht als Standardeinstellung empfohlen.
Timeout (seconds)	Hier geben Sie die Zeit ein, wie lange der NAS auf eine Antwort von TACACS+ wartet. Falls während der Wartezeit keine Antwort empfangen wird, wird der als nächster konfigurierte TACACS+ Server abgefragt und der aktuelle Server in einen *blocked*-Status versetzt (***TACACSPSERVEROPERSTATUS*** = *blocked*). Verfügbare Werte sind *1* bis *60*, der Standardwert ist *3*.
Block Time (seconds)	Hier geben Sie die Zeit ein, wie lange der aktuelle Server in einem blockierten Status bleibt. Nach Ende der Blockierungsdauer wird der Server in den Status versetzt, der im Feld ***ADMINISTRATIVE STATUS*** angegeben ist (siehe unten). Verfügbare Werte sind *0* bis *3600*, der Standardwert ist *60*. Der Wert *0* bedeutet, dass der Server nie in einen *blocked*-Status versetzt wird.
PPP Authentication	Diese Funktion wird von den **XGeneration** Gateways nicht unterstützt. Sie wird möglicherweise in einer späteren Version unserer Systemsoftware realisiert.

Feld	Beschreibung
Login Authentication/Authorization	Hier können Sie festlegen, ob der aktuelle TACACS+ Server für die Login-Authentifizierung zu einem Gateway benutzt werden soll. Zur Auswahl stehen *enabled* (Standardwert) und *disabled*.
TACACS+ Accounting	Diese Funktion wird von den **XGeneration** Gateways nicht unterstützt. Sie wird möglicherweise in einer späteren Version unserer Systemsoftware realisiert.
Administrative Status	Hier können Sie den Status auswählen, in den der Server versetzt werden soll: falls die Einstellung *up* lautet, wird der dazugehörige Server für Authentifizierung, Autorisierung und Abrechnung gemäß Priorität (siehe Feld ***Priority***) und aktuellem Betriebsstatus benutzt. Andernfalls wird dieser Eintrag für TACACS+ AAA-Anforderungen nicht berücksichtigt. Zur Auswahl stehen *up* (Standardwert) und *down*.
TACACS+ Single-Connection	Hier können Sie festlegen, ob mehrere TACACS+ Sitzungen (aufeinanderfolgende TACACS+ Anforderungen) gleichzeitig über eine einzige TCP-Verbindung unterstützt werden. Falls mehrere Sitzungen nicht über eine einzige TCP-Verbindung gemultiplext werden, wird für jede TACACS+ Sitzung eine neue Verbindung aufgebaut und am Ende der jeweiligen Sitzung abgebaut. Zur Auswahl stehen *multiple requests* und *single request* (Standardwert).

Tabelle 8-2: ***IP ➜ Remote Authentication (RADIUS/TACACS+) ➜ TACACS+ Authentication and Authorization ➜ ADD/EDIT***

8 Untermenü Remote Authentication (RADIUS/TACACS+)

9 Untermenü DNS

Im Folgenden wird das Menü *DNS* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][DNS]: IP Configuration - Nameservice                   MyGateway

   Positive Cache                  enabled
   Negative Cache                  enabled

   Overwrite Global Nameservers    yes
   Default Interface               none

   DHCP Assignment                 self
   IPCP Assignment                 global

   Static Hosts                    (0)
   Forwarded Domains               (0)
   Dynamic Cache                   (0 pos 0 neg)

   Advanced Settings...            Global Statistics...


              SAVE                          CANCEL
```

Namensauflösung mit dem XGeneration Gateway

Das Gateway bietet zur Namensauflösung folgende Möglichkeiten:

- DNS Proxy Funktion, um DNS-Anfragen, die an das Gateway gestellt werden, an einen geeigneten DNS-Server weiterzuleiten. Dieses schliesst auch spezifisches Forwarding bestimmter Domains (Forwarded Domains) ein.
- DNS Cache, um die positiven und negativen Ergebnisse von DNS-Anfragen zu speichern.
- Statische Einträge (Static Hosts), um Zuordnungen von IP-Adressen zu Namen manuell festzulegen oder zu verhindern.
- DNS-Monitoring, um einen Überblick über DNS-Anfragen auf dem Gateway zu ermöglichen.

Globale Name-Server

Unter ***IP*** ➜ ***STATIC SETTINGS*** werden die IP-Adressen von globalen Name-Servern eingetragen, die befragt werden, wenn das Gateway Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann.

Für lokale Anwendungen kann als globaler Name-Server die IP-Adresse des Gateways selbst oder die allgemeine Loopback-Adresse (127.0.0.1) eingetragen werden.

Die Adressen der globalen Name-Server kann das Gateway auch dynamisch von WAN Partnern erhalten bzw. diese ggf. an WAN Partner übermitteln:

Strategie zur Namensauflösung auf dem Gateway

Eine DNS-Anfrage wird vom Gateway folgendermaßen behandelt:

1. Falls möglich, wird die Anfrage aus dem statischen oder dynamischen Cache direkt beantwortet mit IP-Adresse oder negativer Antwort.
2. Ansonsten wird, falls ein passender Forwarding-Eintrag vorhanden ist, der entsprechende DNS-Server befragt, ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
3. Ansonsten werden, falls globale Name-Server eingetragen sind, der Primary Domain Name Server, danach der Secondary Domain Name Server befragt. Sind für lokale Anwendungen die IP-Adresse des Gateways oder die Loopback-Adresse eingetragen, werden diese hier ignoriert. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
4. Ansonsten werden, falls ein WAN-Partner als Default Interface ausgewählt ist, die dazugehörigen DNS-Server befragt, ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
5. Ansonsten wird, wenn das Überschreiben der Adressen der globalen Name-Server zulässig ist (***OVERWRITE GLOBAL NAMESERVER*** = *yes*), eine Verbindung zum ersten WAN-Partner ggf. kostenpflichtig aufgebaut, der so konfiguriert ist, dass DNS-Server-Adressen von DNS-Servern angefordert

werden können – soweit dies vorher noch nicht versucht wurde. Bei erfolgreicher Name-Server-Aushandlung werden diese als globale Name-Server eingetragen und stehen somit für weitere Anfragen zur Verfügung.

6. Ansonsten wird die initiale Anfrage mit Serverfehler beantwortet.

Wenn einer der DNS-Server mit "non-existent domain" antwortet, wird die initiale Anfrage sofort dementsprechend beantwortet und ein entsprechender Negativ-Eintrag in den DNS-Cache des Gateways aufgenommen.

Die Konfiguration erfolgt in ***IP*** ➜ ***DNS***.

Das Menü enthält folgende Felder:

Feld	Wert
Positive Cache	Aktivierung des positiven dynamischen Cache. Mögliche Werte: ■ *enabled* (Defaultwert): Erfolgreich aufgelöste Namen und IP-Adressen werden im Cache gespeichert. ■ *flush*: Alle positiven dynamischen Einträge im Cache werden gelöscht. ■ *disabled*: Erfolgreich aufgelöste Namen und IP-Adressen werden nicht im Cache gespeichert, bereits vorhandene dynamische positive Einträge werden gelöscht.

Feld	Wert
Negative Cache	Aktivierung des negativen dynamischen Cache. Mögliche Werte: ■ *enabled* (Defaultwert): angefragte Namen, zu denen ein DNS-Server eine negative Antwort geschickt hat, werden als negative Einträge im Cache gespeichert. ■ *flush*: Alle negativen dynamischen Einträge im Cache werden gelöscht. ■ *disabled*: Namen, die nicht aufgelöst werden konnten, werden nicht im Cache gespeichert, bereits vorhandene dynamische negative Einträge werden gelöscht.
Overwrite Global Nameservers	Legt fest, ob die Adressen der globalen Name-Server auf dem Gateway (in ***IP*** ➜ ***STATIC SETTINGS***) mit von WAN Partnern übermittelten Name-Server-Adressen überschrieben werden dürfen. Mögliche Werte: ■ *yes* (Defaultwert) ■ *no*
Default Interface	Legt den WAN Partner fest, zu dem eine Verbindung zur Name-Server-Verhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren. Defaultwert ist *none*.

Feld	Wert
DHCP Assignment	Legt fest, welche Name-Server-Adressen dem DHCP-Client übermittelt werden, wenn das Gateway als DHCP-Server genutzt wird. Mögliche Werte: ■ *none*: Es wird keine Name-Server-Adresse übermittelt. ■ *self* (Defaultwert): Es wird die Adresse des Gateways als Name-Server-Adresse übermittelt. ■ *global*: Es werden die Adressen der auf dem Gateway eingetragenen globalen Name-Server übermittelt.
IPCP Assignment	Legt fest, welche Name-Server-Adressen vom Gateway bei einer dynamischen Name-Server-Aushandlung an einen WAN Partner übermittelt werden. Mögliche Werte: ■ *none*: Es wird keine Name-Server-Adresse übermittelt. ■ *self*: Es wird die Adresse des Gateways als Name-Server-Adresse übermittelt. ■ *global* (Defaultwert): Es werden die Adressen der auf dem Gateway eingetragenen globalen Name-Server übermittelt.
Static Hosts	In Klammern wird die Anzahl der statischen Einträge angezeigt.
Forwarded Domains	In Klammern wird die Anzahl der Forwarding-Einträge angezeigt.
Dynamic Cache	In Klammern wird die Anzahl der positiven und negativen dynamischen Einträge im DNS-Cache angezeigt.

Tabelle 9-1: Felder im Menü ***DNS***

Über dieses Menü gelangen Sie in folgende Untermenüs:

- ***STATIC HOSTS***
- ***FORWARDED DOMAINS***
- ***DYNAMIC CACHE***
- ***ADVANCED SETTINGS...***
- ***GLOBAL STATISTICS...***

9.1 Untermenü Static Hosts

Im Folgenden wird das Untermenü *IP* ➜ *DNS* ➜ *STATIC HOSTS* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP] [DNS] [HOSTS] [ADD]                                   MyGateway

 Default Domain:

 Name

 Response     positive

 Address

 TTL          86400



               SAVE                                CANCEL
```

In diesem Menü wird eine Liste von bereits konfigurierten Static Hosts angezeigt. Dieses werden im Menü ***STATIC HOSTS*** ➜ ***ADD/EDIT*** hinzugefügt bzw. bearbeitet.

Das Menü enthält folgende Felder:

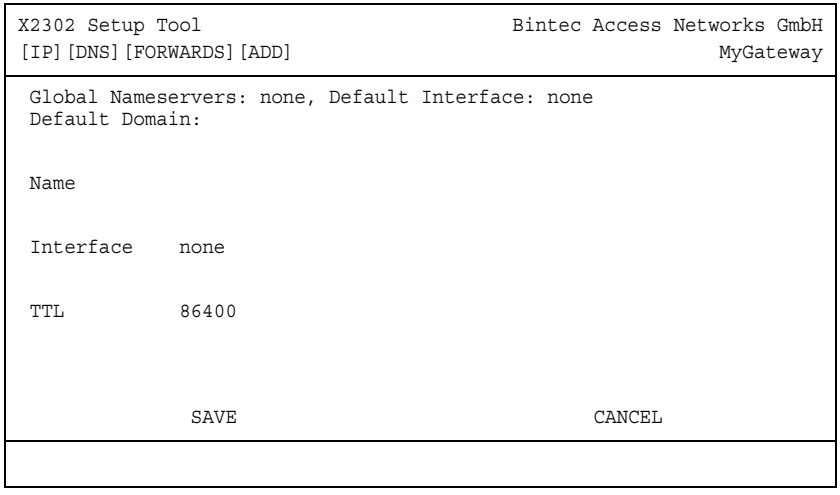
Feld	Wert
Default Domain	Anzeige des in ***IP*** ➜ ***STATIC SETTINGS*** eingetragenen Domain Names des Gateways.

Feld	Wert
Name	Host-Name, dem ***ADDRESS*** mit diesem statischen Eintrag zugeordnet wird. Kann auch mit dem Wildcard * beginnen, z. B. *.bintec.de. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit **SAVE** "***.<DEFAULT DOMAIN>.***" ergänzt.
Response	Art des statischen Eintrags. Mögliche Werte: ■ *positive* (Defaultwert): Ein DNS-Request nach ***NAME*** wird mit der dazugehörigen ***ADDRESS*** beantwortet. ■ *ignore*: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben. ■ *negative*: Ein DNS-Request nach ***NAME*** wird negativ beantwortet.
Address	nur bei ***RESPONSE*** = *positive* IP-Adresse, die ***NAME*** zugeordnet wird.
TTL	Gültigkeitsdauer der Zuordnung von ***NAME*** zu ***ADDRESS*** in Sekunden (nur relevant bei ***RESPONSE*** = *positive*), die anfragenden Hosts übermittelt wird. Defaultwert ist *86400* (= 24 h).

Tabelle 9-2: Felder im Menü ***STATIC HOSTS***

9.2 Untermenü Forwarded Domains

Im Folgenden wird das Untermenü *IP* ➜ *DNS* ➜ *FORWARDED DOMAINS* beschrieben.



In diesem Menü wird eine Liste von bereits konfigurierten Forwarded Domains angezeigt. Dieses werden im Menü ***FORWARDED DOMAINS*** ➜ ***ADD/EDIT*** hinzugefügt bzw. bearbeitet.

Das Menü enthält folgende Felder:

Feld	Wert
Global Nameservers	Anzeige der in ***IP*** ➜ ***STATIC SETTINGS*** eingetragenen globalen Name-Server.
Default Domain	Anzeige des in ***IP*** ➜ ***STATIC SETTINGS*** eingetragene Domain Names des Gateways.
Name	Host-Name, der mit diesem Forwarding-Eintrag aufgelöst werden soll. Kann auch mit dem Wildcard * beginnen, z. B. *.funkwerk.com. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit **SAVE** "***.<DEFAULT DOMAIN>.***" ergänzt.

Feld	Wert
Interface	Legt den WAN Partner fest, zu dem zur Auflösung von ***NAME*** eine Verbindung aufgebaut werden soll. Defaultwert ist *none*.
TTL	Ersatzwert für den vom DNS-Server gelieferten TTL-Wert in einer positiven Antwort, wenn dieser *0* ist oder ***MAXIMUM TTL FOR POS CACHE ENTRIES*** überschreitet. Der TTL-Wert gibt die Gültigkeitsdauer der Zuordnung Name zu IP-Adresse in Sekunden an. Defaultwert ist *86400* (=24 h).

Tabelle 9-3: Felder im Menü ***FORWARDED DOMAINS***

9.3 Untermenü Dynamic Cache

Im Folgenden wird das Untermenü *IP* ➜ *DNS* ➜ *DYNAMIC CACHE* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][DNS][DYNAMIC]: Nameservice - Dynamic Cache              MyGateway

 Name                                Address         Resp  TTL     Ref




    DELETE              STATIC              EXIT
```

Das ***Menü IP ➜ DNS ➜ Dynamic Cache*** dient der Anzeige der von DNS-Servern dynamisch gelernten DNS-Einträge. Darüber hinaus können hier dynamische Einträge in statische umgewandelt oder gelöscht werden. Die Liste enthält folgende Spalten:

Spalte	Bedeutung
Name	Host-Name, dem ***Address*** zugeordnet ist.
Address	IP-Adresse, die ***Name*** zugeordnet ist.
Resp	Art des dynamischen Eintrags. Mögliche Werte: ■ *pos* (positiv): Ein DNS-Request nach ***Name*** wird mit der dazugehörigen IP-Adresse beantwortet. ■ *neg* (negativ): Ein DNS-Request nach ***Name*** wird negativ beantwortet.
TTL	Zeigt an, wieviele Sekunden der dynamische Eintrag noch im Cache bleibt. Nach Ablauf von ***TTL*** wird der Eintrag gelöscht. Bei Speicherung eines positiven dynamischen Eintrags im Cache wird der Wert aus der Antwort des DNS-Servers übernommen. Wenn dieser Wert *0* ist oder ***Maximum TTL for Pos Cache entries*** überschreitet, wird der Wert ***Maximum TTL for Pos Cache entries*** gesetzt. Bei einem negativen dynamischen Eintrag wird ***Maximum TTL for Neg Cache entries*** gesetzt. Die Anzeige wird nicht aktualisiert.
Ref	Gibt an, wie oft der Eintrag angesprochen wurde.

Tabelle 9-4: Felder im Menü ***Dynamic Cache***

Durch Markieren eines Eintrags mit der **Leertaste** und Bestätigen mit **STATIC** wird ein dynamischer Eintrag in einen statischen umgewandelt.

Der entsprechende Eintrag verschwindet damit aus ***IP*** ➜ ***DNS*** ➜ ***DYNAMIC CACHE*** und wird in ***IP*** ➜ ***DNS*** ➜ ***STATIC HOSTS*** aufgelistet. ***TTL*** wird dabei übernommen.

9.4 Untermenü Advanced Settings

Im Folgenden wird das Untermenü *IP* ➜ *DNS* ➜ *ADVANCED SETTINGS* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][DNS][ADVANCED]: Nameservice - Advanced Settings          MyGateway


     Maximum Number of DNS Records        100



     Maximum TTL for Pos Cache entries    86400
     Maximum TTL for Neg Cache Entries    86400


     SAVE                CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Maximum Number of DNS Records	Maximale Gesamtanzahl der statischen und dynamischen Einträge. Ist dieser Wert erreicht, wird bei einem neu hinzukommenden Eintrag derjenige dynamische Eintrag gelöscht, der am längsten nicht angefragt wurde. Wird ***Maximum Number of DNS Records*** vom Benutzer heruntergesetzt, werden gegebenenfalls dynamische Einträge gelöscht. Statische Einträge werden nicht gelöscht - ***Maximum Number of DNS Records*** kann nicht kleiner als die aktuell vorhandene Anzahl von statischen Einträgen gesetzt werden. Mögliche Werte: *0* .. *1000*. Defaultwert ist *100*.
Maximum TTL for Pos Cache entries	Wird bei einem positiven dynamischen Eintrag im Cache als ***TTL*** gesetzt, wenn das TTL-Feld des erhaltenen DNS-Records den Wert *0* hat oder ***Maximum TTL for Pos Cache entries*** überschreitet. Defaultwert ist *86400*.
Maximum TTL for Neg Cache Entries	Wird bei einem negativen dynamischen Eintrag im Cache als ***TTL*** gesetzt. Defaultwert ist *86400*.

Tabelle 9-5: Felder im Menü ***Advanced Settings...***

9.5 Untermenü Global Statistics

Im Folgenden wird das Untermenü *IP* ➜ *DNS* ➜ *Global Statistics* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][DNS][STATISTICS]: Nameservice - Global Statistics       MyGateway


  Received DNS Packets                 0
  Invalid DNS Packets                  0

  DNS Requests                         0
  Cache Hits                           0
  Forwarded Requests                   0

  Cache Hitrate (%)                    0

  Successfully Answered Queries        0
  Server Failures                      0


  EXIT
```

Das enthält folgende Angaben (das Menü wird jede Sekunde aktualisiert):

Feld	Wert
Received DNS Packets	Zeigt die Anzahl der empfangenen und direkt an das Gateway adressierten DNS-Pakete an, einschließlich der Antwortpakete auf weitergeleitete Anfragen.
Invalid DNS Packets	Zeigt die Anzahl der ungültigen empfangenen und direkt an das Gateway adressierten DNS-Pakete an.
DNS Requests	Zeigt die Anzahl der gültigen empfangenen und direkt an das Gateway adressierten DNS-Requests an.
Cache Hits	Zeigt die Anzahl der Anfragen an, die mittels der statischen oder dynamischen Einträge aus dem Cache beantwortet werden konnten.
Forwarded Requests	Zeigt die Anzahl der Anfragen an, die an andere Name-Server weitergeleitet wurden.

Feld	Wert
Cache Hitrate (%)	Zeigt die Anzahl von ***CACHE HITS*** pro ***DNS REQUESTS*** in Prozent an.
Successfully Answered Queries	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.
Server Failures	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

Tabelle 9-6: Felder im Menü ***GLOBAL STATISTICS...***

10 Untermenü DynDNS

Im Folgenden wird das Menü *DynDNS* beschrieben.

Die Nutzung dynamischer IP-Adressen hat den Nachteil, dass ein Host im Netz nicht mehr aufgefunden werden kann, sobald sich seine IP-Adresse geändert hat. Dynamic DNS sorgt dafür, dass Ihr Gateway auch nach einem Wechsel der IP-Adresse noch erreichbar ist.

Folgende Schritte sind zur Einrichtung notwendig:

- Registrierung eines Host-Namens bei einem DynDNS-Provider
- Konfiguration des Gateways

Registrierung

Bei der Registrierung des Host-Namens legen Sie einen individuellen Benutzernamen für den DynDNS-Dienst fest, z. B. *dyn_client*. Dazu bieten die Service Provider unterschiedliche Domainnamen an, so dass sich ein eindeutiger Host-Name für Ihr Gateway ergibt, z. B. *dyn_client.provider.com*. Der DynDNS-Provider übernimmt es für Sie, alle DNS-Anfragen bezüglich des Hosts *dyn_client.provider.com* mit der dynamischen IP-Adresse Ihres Gateways zu beantworten.

Damit der Provider stets über die aktuelle IP-Adresse Ihres Gateways informiert ist, kontaktiert das Gateway beim Aufbau einer neuen Verbindung den Provider und propagiert seine derzeitige IP-Adresse.

Konfiguration des Gateways

Die Konfiguration erfolgt in ***IP*** ➜ ***DynDNS***. Im ersten Menüfenster finden Sie eine Aufstellung der bereits konfigurierten Einträge zur Nutzung von DynDNS-Services.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][DYNDNS]: Dynamic DNS Service                          MyGateway

  DynDNS Services:

  Host Name                  Interface       Permission     State
  dyn_client.provider.com    internet        enabled        up_to_date




 DynDNS Provider List>

     ADD                DELETE              EXIT
```

Darüber hinaus gelangen Sie von hier in das Untermenü ***IP*** ➜ ***DynDNS*** ➜ ***DynDNS Provider List***.

Im Menü ***IP*** ➜ ***DynDNS*** ➜ ***ADD/EDIT*** können Sie eine Namensauflösung über einen DynDNS-Provider konfigurieren bzw. eine bestehende Konfiguration ändern:

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][DYNDNS][ADD]                                          MyGateway

  Host Name
  Interface                  en0-1
  User
  Password

  Provider                   dyndns
  MX
  Wildcard                   off
  Permission                 enabled




           SAVE                                  CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Host Name	Vollständiger Host-Name, wie er beim DynDNS-Provider registriert ist.
Interface	WAN-Interface, dessen IP-Adresse über den DynDNS-Service propagiert werden soll (z.B. das des Internet Service Providers).
User	Benutzername, wie er beim DynDNS-Provider registriert ist.
Password	Passwort, wie es beim DynDNS-Provider registriert ist.
Provider	Auswahl eines vorkonfigurierten DynDNS-Providers. Im unkonfigurierten Zustand stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden. Defaultwert ist *dyndns*.
MX	Vollständiger Hostname eines Mailservers, an den E-Mails weitergeleitet werden, wenn der gerade konfigurierte Host keine Mail empfangen soll. Erkundigen Sie sich bei Ihrem Provider nach diesem Weiterleitungsdienst und stellen Sie sicher, dass Emails von dem als MX eingetragenen Host angenommen werden können.
Wildcard	Hier können Sie die Weiterleitung aller Unterdomänen von ***HOST NAME*** zur aktuellen IP-Adresse von ***INTERFACE*** aktivieren. Mögliche Werte: ■ *on*: Die erweiterte Namensauflösung ist aktiviert. ■ *off* (Defaultwert): Die erweiterte Namensauflösung ist deaktiviert.

Feld	Wert
Permission	Hier können Sie den soeben konfigurierten DynDNS-Eintrag ein- bzw. ausschalten. Die möglichen Werte sind: ■ *enabled* (Defaultwert): Eintrag ist aktiviert ■ *disabled*: Eintrag ist deaktiviert

Tabelle 10-1: Felder im Menü ***DynDNS***

Im Menü ***IP*** ➜ ***DynDNS*** ➜ ***DynDNS Provider List*** wird eine Liste der vorkonfigurierten Provider angezeigt. Die voreingestellten Provider können Sie nicht editieren und auch nicht löschen.

Die Konfiguration neuer Provider erfolgt im Menü ***IP*** ➜ ***DynDNS*** ➜ ***DynDNS Provider List*** ➜ ***ADD/EDIT***.

```
X2302 Setup Tool                    Bintec Access Networks GmbH
[IP] [DYNDNS] [DYNDNS PROVIDER] [ADD]                    MyGateway

 Name
 Server
 Path
 Port                        80

 Protocol                    dyndns

 Minimum Wait (sec)          300


          SAVE                                  CANCEL
```

Das Menü hat folgende Felder:

Feld	Wert
Name	Hier können Sie dem Provider einen beliebigen Namen geben.
Server	Host-Name oder IP-Adresse des Servers, auf dem der DynDNS-Service des Providers läuft.

Feld	Wert
Path	Pfad auf dem Server des Providers, auf dem das Skript zur Verwaltung der IP-Adresse Ihres Gateways zu finden ist. Fragen Sie Ihren Provider nach dem zu verwendenden Pfad.
Port	Port, auf dem Ihr Gateway den Server Ihres Providers ansprechen soll. Erfragen Sie den entsprechenden Port bei Ihrem Provider. Defaultwert: *80*.
Protocol	Hier wählen Sie eines der implementierten Protokolle aus. Es stehen zur Verfügung: ■ *dyndns* (Defaultwert) (www.dyndns.org) ■ *static dyndns* (www.dyndns.org) ■ *ods* (http://www.ods.org) ■ *hn* (http://hn.org) ■ *dyns* (http://dyns.cx) ■ *GnuDIP HTML* (http://gnudip2.sourceforge.net) ■ *GnuDIP TCP* (http://gnudip2.sourceforge.net) ■ *custom dyndns* (www.dyndns.org)

Feld	Wert
Minimum Wait (sec)	Hier geben Sie die Zeitdauer (in Sekunden) an, die das Gateway mindestens warten muss, bevor es seine aktuelle IP-Adresse erneut beim DynDNS-Provider propagieren darf. Defaultwert ist *300* Sekunden.

Tabelle 10-2: Felder im Menü ***DynDNS Provider List ➜ ADD/EDIT***

11 Untermenü Routing protocols

Im Folgenden wird das Menü *ROUTING PROTOCOLS* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][ROUTING]: Routing protocols                              MyGateway

                Routed                    running

                RIP >

                SAVE                      CANCEL
```

Die Inhalte der Routing Tabelle eines Gateways können statisch konfiguriert werden. Ein Gateway kann optional auch seine Routing Tabellen dynamisch aktualisieren, indem es Informationen mit anderen Gateways austauscht. Dieser Informationsaustausch wird in einem Routing-Protokoll spezifiziert.

Routing Protokolle erlauben dem Gateway, sich dynamisch an sich ändernde Netzwerkbedingungen anzupassen und schnell die beste Routinglösung in komplexen Netzwerken zu finden. Eines der am häufigsten verwendeten Routing-Protokolle ist ***RIP***. Dieses wird in den folgenden Kapiteln kurz erläutert.

Im Menü ***IP*** findet sich das Untermenü ***ROUTING PROTOCOLS***. Dieses zeigt den Status des Routing-Daemon (***ROUTED***) an und ermöglicht seine Aktivierung bzw. Deaktivierung (mit ***ROUTED*** = *running* bzw. *stopped*).

Die möglichen Zustände des Routing-Daemons sind:

- *running*: aktiviert RIP (abhängig von der interface-spezifischen RIP-Konfiguration).
- *stopped*: deaktiviert RIP (abhängig von der interface-spezifischen RIP-Konfiguration).

Darüber hinaus ermöglicht das Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** den Zugriff auf das Untermenü ***RIP***.

Der Einsatz der Routing-Protokolle wird global im Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***ROUTED*** aktiviert. RIP wird zudem auf dem jeweiligen Interface durch Auswahl der entsprechenden Protokollversion in ***RIP SEND*** bzw. ***RIP RECEIVE*** aktiviert.

11.1 Untermenü RIP

Im Folgenden wird das Menü *RIP* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][ROUTING][RIP]: RIP configuration                        MyGateway

      UDP port                            520

      Static Settings >

      Timer >

      Filter >


      SAVE                                CANCEL
```

Im Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***RIP*** werden globale RIP-Einstellungen vorgenommen. Die Aktivierung von RIP erfolgt interface-spezifisch in den ***IP*** ➜ ***ADVANCED SETTINGS*** des jeweiligen Interface-Menüs.

Mit RIP (Routing Information Protocol) tauscht ein Gateway Routing Informationen mit anderen Gateways aus. Ungefähr alle 30 Sekunden sendet ein Gateway Meldungen zu entfernten Netzwerken, wobei es Informationen aus seiner eigenen aktuellen Routing-Tabelle verwendet. Dabei wird immer die gesamte Routing-Tabelle ausgetauscht. Mit Triggered RIP findet nur ein Austausch statt, wenn sich Routing Informationen geändert haben. In diesem Fall werden nur die geänderten Informationen versendet.

Durch Beobachtung der Informationen, die von anderen Gateways verschickt werden, werden neue Routen und kürzere Wege für bestehende Routen in der Routing-Tabelle gespeichert. Da Zwischenrouten zwischen Netzwerken unerreichbar werden können, entfernt RIP Routen, die älter als 5 Minuten sind (d.h Routen, die in den letzten 300 Sekunden nicht verifiziert wurden). Mit Triggered RIP gelernte Routen werden jedoch nicht gelöscht.

Hinweis

Die Einstellungsmöglichkeit des ***UDP-PORT***s, der für das Senden und Empfangen von RIP-Updates verwendet wird, ist lediglich für Testzwecke von Bedeutung. Eine Veränderung der Einstellung kann dazu führen, dass das Gateway auf einem Port sendet und lauscht, auf dem keine weiteren Gateways reagieren. Der Defaultwert *520* sollte eingestellt bleiben.

Vom Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***RIP*** gelangen Sie in drei weitere Untermenüs, in denen Sie die Art und Weise, in der RIP-Updates gehandhabt werden, genau festlegen können:

- ***STATIC SETTINGS***
- ***TIMER***
- ***FILTER***.

11.1.1 Untermenü Static Settings

Im Folgenden wird das Menü *STATIC SETTINGS* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][ROUTING][RIP][STATIC]: RIP Static Settings              MyGateway

      Default Route distribution        enabled
      Poisoned Reverse                  disabled
      RFC 2453 variable timer           enabled
      RFC 2091 variable timer           disabled


      SAVE                              CANCEL
```

Im Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***RIP*** ➜ ***STATIC SETTINGS*** konfigurieren Sie grundlegende Parameter des RIP. Es enthält folgende Felder:

Feld	Wert
Default Route distribution	Hier bestimmen Sie, ob die Default-Route Ihres Gateways über RIP-Updates propagiert werden soll. Mögliche Werte: ■ *disabled* ■ *enabled* Der Defaultwert ist *enabled*.
Poisoned Reverse	Verfahren zur Verhinderung von Routing-Schleifen Bei Standard RIP werden die gelernten Routen über alle Interfaces mit aktiviertem ***RIP SEND*** propagiert. Bei ***POISENED REVERSE*** propagiert das Gateway jedoch über das Interface, über das es die Routen gelernt hat, diese mit der Metric (Next Hop Count) 16 (="Netz ist nicht erreichbar"). Mögliche Werte: ■ *disabled* ■ *enabled* Der Defaultwert ist *disabled*.
RFC 2453 variable timer	Hier können Sie bestimmen, ob für die in RFC 2453 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***RIP*** ➜ ***TIMER*** konfigurieren können. Die möglichen Werte sind: ■ *disabled* ■ *enabled* (Defaultwert) Wenn Sie den Wert *disabled* wählen, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.

Feld	Wert
RFC 2091 variable timer	Hier können Sie bestimmen, ob für die in RFC 2091 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***RIP*** ➜ ***TIMER*** konfigurieren können. Die möglichen Werte sind: ■ *disabled* (Defaultwert) ■ *enabled* Wenn Sie den Wert *disabled* belassen, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.

Tabelle 11-1: Felder im Menü ***STATIC SETTINGS***

Die Timer, die im Menü ***STATIC SETTINGS*** aktiviert werden können, werden im Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***RIP*** ➜ ***TIMER*** konfiguriert.

11.1.2 Untermenü Timer

Im Folgenden wird das Menü *TIMER* beschrieben.

```
X2302 Setup Tool                          Bintec Access Networks GmbH
[IP][ROUTING][RIP][TIMER]: RIP timer configuration          MyGateway


       Timer for RIP V2 (RFC 2453)
       ---------------------------
       Update Timer                       30
       Route Timeout                      180
       Garbage Collection Timer           120

       Timer for Triggered RIP (RFC 2091)
       ----------------------------------
       Hold down timer                    120
       Retransmission timer               5



              SAVE                                CANCEL
```

In diesem Menü können Sie die Timer konfigurieren, die von RFC 2091 und RFC 2453 für die unterschiedlichen Ereignisse innerhalb der Lifetime einer Route vorgesehen sind.

Das Menü gliedert sich in die Felder zur Konfiguration des ***RIP-V2-TIMERS (RFC 2453)*** und des ***TRIGGERED-RIP-TIMERS (RFC 2091)***.

Das Menü ***TIMER*** enthält folgende Felder (alle Timer werden in Sekunden angegeben):

Feld	Wert
Update Timer	Nach Ablauf dieses Zeitraums wird ein RIP-Update gesendet. Der Defaultwert ist *30*.
Route Timeout	Nach dem letzten Update einer Route wird der ***ROUTE TIMEOUT*** aktiviert. Nach dessen Ablauf wird die Route deaktiviert und der ***GARBAGE COLLECTION TIMER*** gestartet. Der Defaultwert ist *180*.
Garbage Collection Timer	Der ***GARBAGE COLLECTION TIMER*** wird gestartet, sobald der Route Timeout abgelaufen ist. Nach Ablauf dieses Zeitraums wird die ungültige Route aus der ***IPROUTETABLE*** gelöscht, sofern kein Update für die Route mehr eingeht. Der Defaultwert ist *120*.
Hold down timer	Der ***HOLD DOWN TIMER*** wird aktiviert, sobald das Gateway eine unerreichbare Route (Metric 16) erhält. Nach Ablauf dieses Zeitraums wird die Route ggf. aus der ***IPROUTETABLE*** gelöscht. Der Defaultwert ist *120*.

Feld	Wert
Retransmission timer	Nach Ablauf dieses Zeitraums werden Update-Request- bzw. Update-Response-Pakete erneut versendet, bis ein Update-Flush- bzw. Update-Acknowledge-Paket eintrifft. Der Defaultwert ist *5*.

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

11.1.3 Untermenü Filter

Im Folgenden wird das Menü *FILTER* beschrieben.

```
X2302 Setup Tool                              Bintec Access Networks GmbH
[IP][ROUTING][RIP][FILTER]: RIP Distribution Filter            MyGateway

 Interface   Direction   State    IP-Address    Netmask    Priority




   ADD                  DELETE               EXIT
```

Im Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***RIP*** ➜ ***FILTER*** können Sie exakt festlegen, welche Routen exportiert oder importiert werden sollen oder nicht.

Hierbei können Sie nach folgenden Strategien vorgehen:

- Sie deaktivieren den Import bzw. Export bestimmter Routen explizit. Der Import bzw. Export aller anderen Routen, die nicht aufgeführt werden, bleibt erlaubt.
- Sie aktivieren den Import bzw. Export bestimmter Routen explizit. Dann müssen Sie den Import bzw. Export aller anderen Routen auch explizit deaktivieren. Dieses erreichen Sie mittels eines Filters für ***IP-ADDRESS*** = kein Eintrag (dies entspricht der IP-Adresse 0.0.0.0) mit ***NETMASK*** = kein Eintrag (dies entspricht der Netzmaske 0.0.0.0) und ***DISTRIBUTION*** = *disabled*. Da-

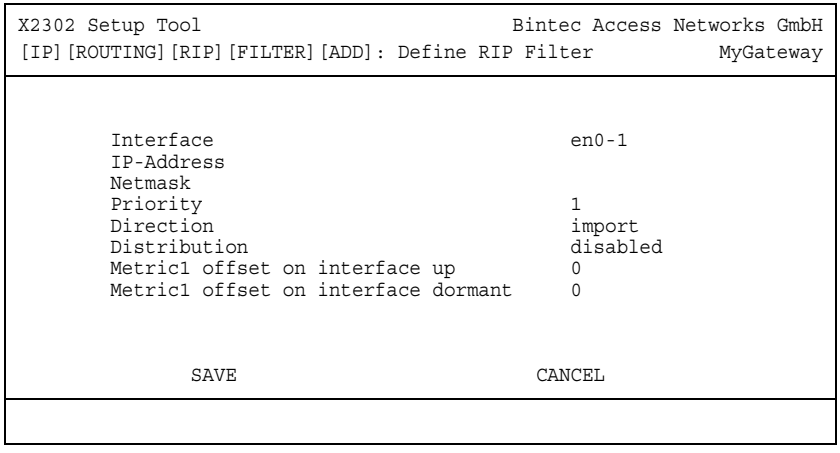
mit dieses Filter als letztes angewendet wird, muss ihm die niedrigste Priorität zugewiesen werden.

Ein Filter für eine Default-Route konfigurieren Sie mit folgenden Werten:

- ***IP-ADDRESS*** = keine Eintrag (dies entspricht der IP-Adresse 0.0.0.0) mit ***NETMASK*** = *255.255.255.255*.

Im ersten Menüfenster sehen Sie eine Auflistung der bereits konfigurierten Filter.

Die angezeigten Felder entsprechen den im Untermenü ***ADD/EDIT*** konfigurierbaren Optionen. Unter ***STATE*** wird der für die Variable ***DISTRIBUTION*** konfigurierte Wert angezeigt.



Das Menü ***FILTER*** ➜ ***ADD/EDIT*** enthält folgende Felder:

Feld	Wert
Interface	Hier bestimmen Sie, für welches Interface die zu konfigurierende Regel gilt.

Feld	Wert
IP-Address	Hier geben Sie die IP-Adresse ein, auf die die Regel angewendet werden soll. Die Adresse kann sowohl im LAN als auch im WAN liegen. Die Regeln für eingehende und ausgehende RIP-Pakete (Import oder Export) müssen für dieselbe IP-Adresse getrennt konfiguriert werden. Sie können einzelne Host-Adressen ebenso angeben wie Netzadressen.
Netmask	Hier geben Sie die Netzmaske von ***IP ADDRESS*** ein.
Priority	Hier geben Sie die Priorität ein, mit der das Filter angewendet werden soll. Gibt es unterschiedliche Filter mit sich überlappenden IP-Adressbereich, so wird dasjenige Filter zuerst ausgeführt, das die höhere Priorität hat. So lässt sich eine einzelne Host-Route aus einem eigentlich gesperrten IP-Adressbereich importieren, wenn die Regel, die dies zulässt, eine höhere Priorität hat als diejenige, die den Adressbereich sperrt. Mögliche Werte sind *1* bis *16*, wobei *1* der höchsten Priorität entspricht. Der Defaultwert ist *1*.
Direction	Hier bestimmen Sie, ob das Filter für den Export oder den Import von Routen gilt. Die möglichen Werte sind: ■ *import* ■ *export.* Defaultwert ist *import*.

Feld	Wert
Distribution	Hier bestimmen Sie, ob der Export bzw. Import vom/zum Gateway durch dieses Filter zugelassen oder gesperrt werden soll. Die möglichen Werte sind: ■ *enabled* ■ *disabled* Der Defaultwert ist *disabled*.
Metric1 offset on interface up	Hier geben Sie an, ob und in welchem Umfang die Metrik einer importierten oder exportierten Route geändert werden soll, wenn das betroffene Interface aktiv (up) ist. Die möglichen Werte sind *-16* bis *16*. Der Defaultwert ist *0*.
Metric1 offset on interface dormant	Hier geben Sie an, ob und in welchem Umfang die Metrik einer importierten oder exportierten Route geändert werden soll, wenn das betroffene Interface inaktiv (dormant) ist. Die möglichen Werte sind *-16* bis *16*. Der Defaultwert ist *0*.

Tabelle 11-3: Felder im Menü ***FILTER***

Index: IP

A

ADDEXT 8
Address 55, 58
Alive Check (if inactive) 43

B

Bandwidth Management 23
Bandwidth on Demand 23
BOD 23

C

Cache Hitrate (%) 62
Cache Hits 61
Client / Server 37

D

Default Domain 54
Default Domains 56
Default Interface 52
Default Route distribution 72
Description 24
Destination IP-Address 6
Destination Port 9, 10
DHCP Assignment 53
Dialout 43
Direction 77
Distribution 78
Distribution Fraction (in percent) 26
Distribution Mode 25
Distribution Policy 25, 26
Distribution Ratio 25
DNS 11, 49
DNS Requests 61
DNS-Proxy 11
Domain Name 11
Domain Name Server 11, 49
Dynamic Cache 53
DynDNS Registrierung 63

E

Extended Routing 8
External Address 19
External Mask 19
External Port 20

F

Flags 5
Forwarded Domains 53
Forwarded Requests 61

G

Garbage Collection Timer 74
Gateway 34
Gateway IP-Address 7

H

Hold down timer 74
Host Name 65
HTTP TCP port 13

I

Ignore 7
Interface 33, 57, 65, 76
Interface 1 - 3 25
Interface Group ID 24
Internal Address 20
Internal Mask 20
Internal Port 21
Invalid DNS Packets 61
IP Address 31, 33, 40
IP address pool LAN (DHCP) 33
IP address pool WAN (PPP) 31
IP-Address 77
IPCP Assignment 53

L

LAN 7, 30
Lease Time (Minutes) 34
Load Balancing 23
Local Nameservers 56

M

MAC Address 34
Maximum Number of DNS Records 60
Maximum TTL for Neg Cache Entries 60
Maximum TTL for Pos Cache entries 60
Metric 7
Metric1 offset on interface dormant 78
Metric1 offset on interface up 78
Minimum Wait 68
Mode 9, 10
MX 65

N

Name 55, 56, 58, 66
Namensauflösung 49
Negative Cache 52
NetBT Mode Type 34
Netmask 6, 77
Network 6
Network Address Translation 16
Number of consecutive addresses 31, 34

O

OSPF 69
Overwrite Global Nameservers 52

P

Partner / Interface 7
Password 40, 65
Path 67
Permission 66
Poisoned Reverse 72
Policy 41
Pool ID 31
Port 41, 67
Positive Cache 51
PPTP Passthrough 16
Primary BOOTP Relay Server 13
Primary Domain Name Server 11
Primary WINS 11

Priority 40, 77
Protocol 9, 18, 40, 67
Provider 65

R

RADIUS Pakete 38
Radius Server 37
Received DNS Packets 61
Ref 58
Refuse 7
Remote Address 19
Remote CAPI Server TCP port 13
Remote Mask 19
Remote Port 19
Remote TRACE Server TCP port 13
Resp 58
Response 55
Retransmission timer 75
Retries 42
RFC 2091 variable timer 73
RFC 2453 variable timer 72
RIP 69
RIP UDP port 13
Route Timeout 74
Route Type 6
Routing protocols 69
Routing-Eintrag ändern 5
Routing-Eintrag hinzufügen 5

S

Secondary BOOTP Relay Server 13
Secondary Domain Name Server 11
Secondary WINS 11
Server 66
Server Failures 62
Service 18
Silent Deny 16
SNMP 35
SNMP listen UDP port 35

SNMP trap broadcasting 35
SNMP trap community 36
SNMP trap UDP port 35
Source Interface 9
Source IP-Address 9
Source Mask 9
Source Port 9, 10
State 42
Static Hosts 53
Successfully Answered Queries 62

T
Time Offset (sec) 12
Time Protocol 12, 13
Time Server 12
Time Update Interval (sec) 12
Timeout (ms) 41
TOS Mask 9
TTL 55, 57, 58
Type of Service (TOS) 9

U
Unique Source IP Address 13
Update Timer 74
User 65

V
Validate 42

W
WAN with transit network 7, 30
WAN without transit network 7, 30
Wildcard 65
WINS 11