Benutzerhandbuch

bintec R1200 / R1200w / R3000 / R3000w / R3400 / R3800

IP

Version 2.0

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von bintec-Gateways ab Software-Release 7.4.3. 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.

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.

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.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

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 5

2 Untermenü Routing 7

3 Untermenü Static Settings 13

4 Untermenü Network Address Translation 15

4.1 Untermenü Requested from OUTSIDE/INSIDE 16

5 Untermenü Bandwidth Management (TDRC / Load Balancing / BOD) 23

5.1 Menü TCP Download Rate Control (TDRC) 23

5.2 Untermenü IP Load Balancing over Multiple Interfaces 30

5.2.1 Untermenü IP Routing List 34

5.3 Untermenü IP triggered Bandwidth on Demand (IP BOD) 37

5.3.1 Untermenü Filter 38

5.3.2 Untermenü Rules for BOD 42

5.3.3 Untermenü Configure Interfaces for BOD 44

6 Untermenü IP address pool WAN (PPP) 47

7 Untermenü IP address pool LAN (DHCP) 49

8 Untermenü SNMP 53

9 Untermenü Remote Authentication (RADIUS/TACACS+) 57

9.1 Untermenü RADIUS Authentication and Accounting 57

9.2 Untermenü TACACS+ Authentication and Authorization 64

10 Untermenü DNS 71

10.1 Untermenü Static Hosts 76

10.2 Untermenü Forwarded Domains 77

10.3 Untermenü Dynamic Cache 79
10.4 Untermenü Advanced Settings 81
10.5 Untermenü Global Statistics 82

11 Untermenü DynDNS 85

12 Untermenü Routing protocols 91

12.1 Untermenü RIP 92
12.1.1 Untermenü Static Settings 93
12.1.2 Untermenü Timer 95
12.1.3 Untermenü Filter 97
12.2 Untermenü OSPF 100
12.2.1 Untermenü Static Settings 103
12.2.2 Untermenü Interfaces 105
12.2.3 Untermenü Areas 109

Index: IP 113

1 Menü IP

Im Folgenden wird das Menü *IP* beschrieben.

```
R3000w Setup Tool                Funkwerk Enterprise Communication GmbH
[IP]: IP Configuration                                          MyGateway

         Routing
         Static Settings
         Network Address Translation

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

2 Untermenü Routing

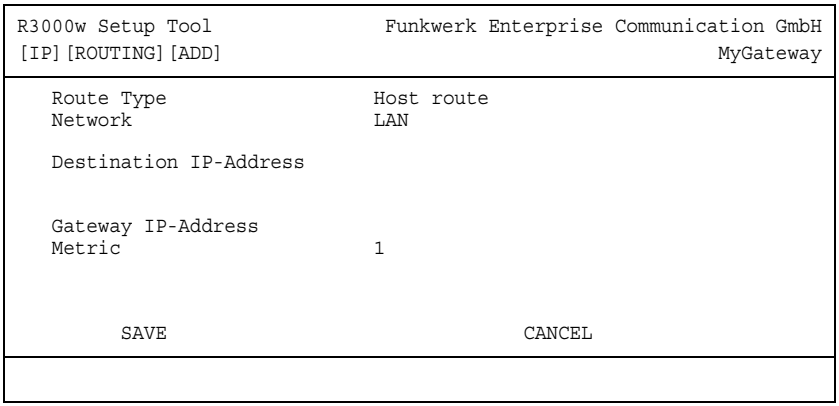
Im Folgenden wird das Untermenü *ROUTING* beschrieben.

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.

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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:



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

Feld	Wert
Route Type	Art der Route. Mögliche Werte: ■ *Host route* (Standardwert): Route zu einem einzelnen Host. ■ *Network route*: 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 10.
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*, Standardwert ist *0*).

Tabelle 2-1: 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.

Wert	Bedeutung
Local	Route zu einem Ziel-Host oder -Netzwerk, der/das über das Local Interface Ihres Gateways zu erreichen ist.

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

Zusätzlich zu der normalen Routing-Tabelle kann Ihr Gateway auch Routing-Entscheidungen aufgrund einer erweiterten Routing-Tabelle, der Extended-Routing-Tabelle, treffen. Dabei kann das 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***.

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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 12.
Source Interface	Schnittstelle, über die die Datenpakete das Gateway erreichen. Standardwert 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*. Standardwert 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 12).
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 12).

Tabelle 2-3: Felder im Menü ***ROUTING*** ➜ ***ADDEXT***

MODE enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
always (Standardwert)	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 2-4: Auswahlmöglichkeiten von ***MODE***

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

Wert	Bedeutung
any (Standardwert)	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 2-5: Auswahlmöglichkeiten von ***SOURCE PORT BZW. DESTINATION PORT***

3 Untermenü Static Settings

Im Folgenden wird das Untermenü *STATIC SETTINGS* beschrieben.

```
R3000w Setup Tool                Funkwerk Enterprise Communication GmbH
[IP][STATIC]: IP Static Settings                                MyGateway

    Domain Name
    Primary Domain Name Server
    Secondary Domain Name Server
    Primary WINS
    Secondary WINS

    Remote CAPI Server TCP port     2662
    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
Remote CAPI Server TCP port	TCP-Port-Nummer für ➤➤ **Remote-CAPI**-Verbindungen. Standardwert ist *2662*. Deaktivieren mit *0*.
Remote TRACE Server TCP port	TCP-Port-Nummer für Remote Traces. Standardwert ist *7000*. Deaktivieren mit *0*.
RIP UDP port	UDP-Port-Nummer für ➤➤ **RIP** (Routing Information Protocol). Standardwert 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. Standardwert ist *80*.

Tabelle 3-1: Felder im Menü ***STATIC SETTINGS***

4 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:

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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* (Standardwert): 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* (Standardwert): 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 4-1: Felder im Menü ***NETWORK ADDRESS TRANSLATION***

4.1 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.

```
R3000w Setup Tool                 Funkwerk Enterprise Communication 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:

```
R3000w Setup Tool                Funkwerk Enterprise Communication GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT - sessions from            MyGateway
                              OUTSIDE (Internet)

  Service                      user defined
  Protocol                     icmp

  Remote Address
  Remote Mask


  External Address
  External Mask
  External Port                any

  Internal Address
  Internal Mask                255.255.255.255
  Internal Port                any

               SAVE                                  CANCEL
```

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, Standardwert)
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.

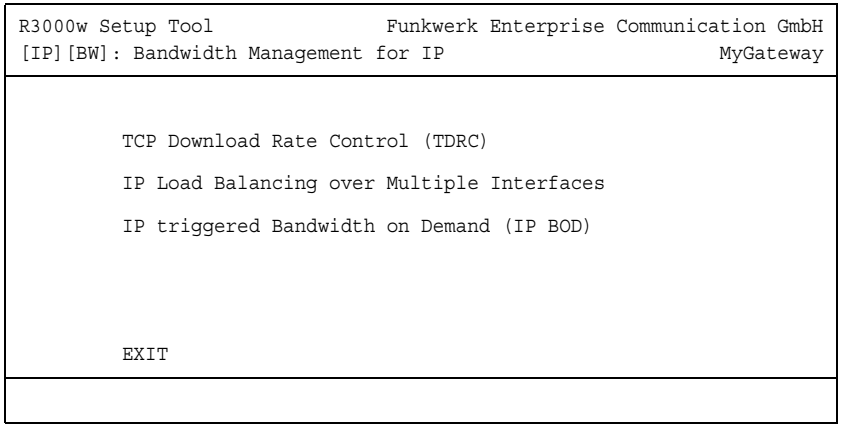
Wert	Wert
External Port Port...to Port	Nur für ***SERVICE*** = *user defined*. ■ ***REQUESTED FROM OUTSIDE*** ➜ ***ADD/EDIT***: nur für ***SERVICE*** = *user defined*; ursprünglicher Zielport der eingehenden IP-Verbindung. ■ ***REQUESTED FROM INSIDE*** ➜ ***ADD/EDIT:*** der neu gesetzte Quellport der ausgehenden IP-Verbindung. Mögliche Werte: ■ *any* (Standardwert): 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* (Standardwert): bei ***REQUESTED FROM OUTSIDE ➜ ADD/EDIT*** bedeutet dies keine Port-Umsetzung. ■ *specify*: ermöglicht die Eingabe einer Port-Nummer.

Tabelle 4-2: Felder im Menü ***REQUESTED FROM OUTSIDE/INSIDE***

5 Untermenü Bandwidth Management (TDRC / Load Balancing / BOD)

Im Folgenden wird das Menü *Bandwidth Management (TDRC / Load Balancing / BOD)* beschrieben.



Über das Menü ***Bandwidth Management (TDRC / Load Balancing / BOD)*** gelangt man in die Untermenüs:

- ***TCP Download Rate Control (TDRC)***
- ***IP Load Balancing over Multiple Interfaces***
- ***IP triggered Bandwidth on Demand (IP BOD)***

5.1 Menü TCP Download Rate Control (TDRC)

Im Folgenden wird das Menü *TCP Download Rate Control (TDRC)* beschrieben.

Das Menü ***IP*** ➜ ***Bandwidth Management (TDRC / Load Balancing / BOD)*** ➜ ***TCP Download Rate Control (TDRC)*** enthält eine Liste der Interfaces, für die

bereits der TDRC-Mechanismus konfiguriert wurde. (Der Screenshot enthält Beispielwerte.)

```
R3000w Setup Tool              Funkwerk Enterprise Communications GmbH
[IP][TDRC]: Configure TCP Download Rate Control              MyGateway

Interface        Mode                    Maximum Receive Rate

10001 DSL        TCP ACK prioritisation
50000 ehtoa50-0  static                  1024









    ADD                DELETE              EXIT
```

Eine zunehmende Anzahl von Netzwerkdiensten erfordert es, dass Daten nicht nur so schnell wie möglich, sondern auch mit konstanter Transferrate ausgetauscht werden können (so z. B. VoIP). Um dieses vor allem bei ADSL-Verbindungen zu gewährleisten, verfügt Ihr Gateway über einen entsprechenden Mechanismus.

Grundsätzlich kann man auf zwei Wegen sicherstellen, dass Datenströme, die eine geringe Latenz erfordern, nicht behindert werden.

Beide Mechanismen lassen sich im Menü ***IP*** ➜ ***Bandwidth Management (TDRC / Load Balancing / BOD)*** ➜ ***TCP Download Rate Control (TDRC)*** ➜ ***ADD/EDIT*** konfigurieren. (Die Screenshots zeigen nicht die Standardwerte.)

- Zum einen ist es möglich, die allgemein zur Verfügung gestellte Download-Rate für TCP-Verbindungen herabzusetzen, so dass eine gesicherte Bandbreite für die Daten einer High Priority QoS Queue zur Verfügung steht.

```
R3000w Setup Tool              Funkwerk Enterprise Communications GmbH
[IP][TDRC][EDIT]: Configure TCP Download Rate Control        MyGateway

  Interface             50000   ethoa50-0

  Optimize Download Rate via TCP ACK prioritisation      no
  (recommended for ADSL)

  TDRC Mode      static (fixed maximum rate for TCP download)

  Maximum TCP Download Rate (kbits/s)          1024

  Control all TCP Services                     no
  Select TCP Services >

        SAVE                                CANCEL
```

- Zum anderen ist es möglich, die zur Verfügung stehende Bandbreite optimal auszunutzen, indem man den Upload von TCP-ACK-Paketen im Upstream asynchroner DSL-Verbindungen bevorzugt. Dies stellt sicher, dass keine Verzögerungen aufgrund der geringen Upload-Bandbreite von ADSL-Verbindungen auftreten.

```
R3000w Setup Tool              Funkwerk Enterprise Communications GmbH
[IP][TDRC][EDIT]: Configure TCP Download Rate Control        MyGateway

  Interface             10001   DSL

  Optimize Download Rate via TCP ACK prioritisation      yes
  (recommended for ADSL)

        SAVE                                CANCEL
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Interface	Hier wählen Sie aus, auf welches Interface die TDRC-Konfiguration angewendet werden soll.
Optimize Download Rate via TCP ACK prioritisation	Hier wählen Sie aus, ob die Download-Rate optimiert werden soll, indem TCP-ACK-Pakete im Upstream bevorzugt behandelt werden (yes). Wenn Sie hier *yes* wählen, werden die folgenden Felder nicht mehr angezeigt. Mögliche Werte sind *yes* und *no*. Standardwert ist *no*.

Feld	Bedeutung
TDRC Mode	Nur wenn ***Optimize Download Rate via TCP ACK prioritisation*** = *no*. Hier wählen Sie den TDRC (TCP Download Rate Control) Mechanismus. Durch die Werte *dynamic (maximum rate less amount of high priority traffic)* und *static (fixed maximum rate for TCP download)* begrenzen Sie die Download-Rate für TCP-Verbindungen. Mögliche Werte: ■ *static (fixed maximum rate for TCP download)* (Standardwert) - Die Download-Rate für TCP-Verbindungen wird statisch auf den in ***Maximum TCP Download Rate (kbits/s)*** definierten Wert begrenzt. ■ *dynamic (maximum rate less amount of high priority traffic)* - Die Download-Rate wird auf einen dynamisch errechneten Wert begrenzt. Dieser errechnet sich aus dem in ***Maximum TCP Download Rate (kbits/s)*** definierten Wert, abzüglich der Bandbreite, die aktuell im Moment des Dazukommens oder Wegfallens einer TCP-Verbindung für den QoS-High-Priority-Verkehr auf diesem Interface benötigt wird. Diese Einstellung setzt eine QoS-Konfiguration für das ausgewählte Interface voraus. ■ *disabled* - Die TCP Download-Rate wird nicht begrenzt.

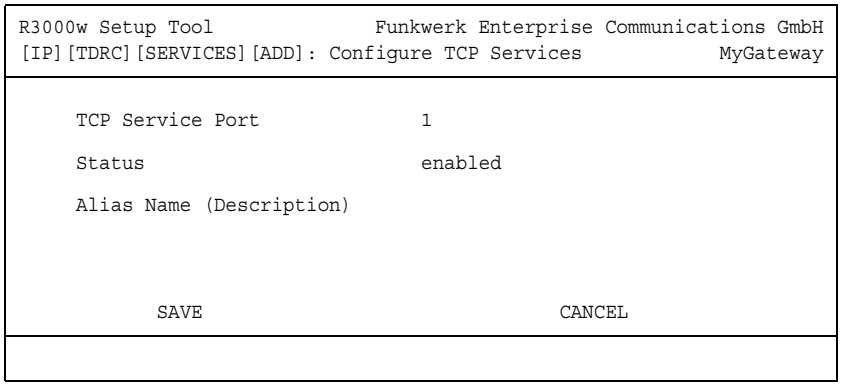
Feld	Bedeutung
Maximum TCP Download Rate (kbits/s)	Nur wenn ***Optimize Download Rate via TCP ACK prioritisation*** = *no*. Hier geben Sie die maximale Bandbreite in kbit/s für TCP-Downloads an. Mögliche Werte sind *1* bis *100000*, der Standardwert ist *1024*.
Control all TCP Services	Nur wenn ***Optimize Download Rate via TCP ACK prioritisation*** = *no*. Hier wählen Sie aus, ob die eingestellte Download-Kontrolle auf alle TCP-Verbindungen angewendet werden soll. Mögliche Werte sind *yes* und *no*. Standardwert ist *yes*.

Tabelle 5-1: ***IP ➜ Bandwidth Management (TDRC / Load Balancing / BOD) ➜ TCP Download Rate Control (TDRC) ➜ ADD/EDIT***

Wenn Sie für ***Control all TCP Services*** *no* ausgewählt haben, gelangen Sie über ***Select TCP Services*** zur Konfiguration derjenigen Dienste, die der TDRC unterstellt werden sollen (der Screenshot zeigt die voreingestellten Dienste):

```
R3000w Setup Tool                Funkwerk Enterprise Communications GmbH
[IP][TDRC][SERVICES]: Configure TCP Services                    MyGateway

 TCP Port                                  Status

    80              HTTP                     builtin
    443             HTTPS                    builtin
    20              FTP Data                 builtin
    110             POP3                     builtin
    143             IMAP2                    builtin



     ADD                 DELETE                EXIT
```

Mit ***ADD*** gelangen Sie zur Konfiguration weiterer TCP-Dienste:



Das Menü enthält folgende Felder:

Feld	Bedeutung
TCP Service Port	Hier geben Sie den TCP-Port des entsprechenden Dienstes ein, der der TDRC unterstellt werden soll. Mögliche Werte sind *1* bis *65535*, der Standardwert ist *1*.
Status	Hier wählen Sie aus, ob die Kontrolle mittels TDRC für den konfigurierten Dienst aktiviert werden soll. Mögliche Werte sind *enabled* und *disabled*, Standardwert ist *enabled*. Für die voreingestellte Dienste wird in der ***Configure TCP Services***-Liste der Status *built-in* angezeigt.
Alias Name (Description)	Hier geben Sie eine beliebige Beschreibung für den Dienst ein, die maximale Länge der Eingabe ist 20 Zeichen.

Tabelle 5-2: ***IP ➜ Bandwidth Management (TDRC / Load Balancing / BOD) ➜ TCP Download Rate Control (TDRC) ➜ ADD/EDIT ➜ Select TCP Services ➜ ADD***

5.2 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.

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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. Standardwert ist *0*.
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 34
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. (Standardwert) ■ *up-only (operational up interfaces only):* Nur Interfaces, die up sind, werden einbezogen.

Feld	Wert
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* (Standardwert): 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. ■ Für *equal for all interfaces of the group*: Hier wird angezeigt, welchen Prozentsatz des Datenverkehrs ein Interface übernehmen soll. ■ Für *individual for all interfaces of the group*: 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 5-3: 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.

Feld	Wert
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.
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 34

Tabelle 5-4: Auswahlmöglichkeiten von ***Distribution Policy***

5.2.1 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***.

```
R3000w Setup Tool                 Funkwerk Enterprise Communication 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* (Standardwert): Route zu einem Netzwerk ■ *Default route*: Die Route gilt für alle IP-Adressen und wird nur benutzt, wenn keine andere passende Route verfügbar ist

Feld	Wert
Network	Definiert die Art der Verbindung (LAN, WAN). Mögliche Werte, siehe Tabelle “Auswahlmöglichkeiten von Network” auf Seite 37.
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*. Standardwert 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 Standardwert *-1* im Feld ***Port*** belässt.

Feld	Wert
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 Standardwert *-1* bedeutet, dass der Zielport beliebig ist.

Tabelle 5-5: Felder im Menü ***IP ROUTING LIST*** ➜ ***ADD/EDIT***

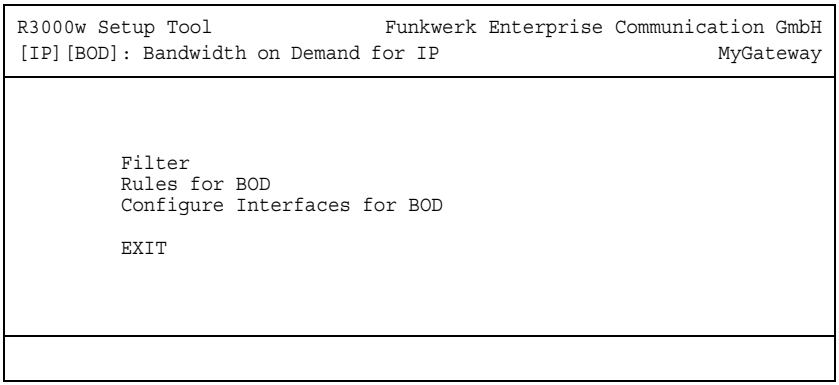
NETWORK enthält folgende Auswahlmöglichkeiten (abhängig vom Typ des Interfaces):

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 5-6: Auswahlmöglichkeiten von ***NETWORK***

5.3 Untermenü IP triggered Bandwidth on Demand (IP BOD)

Im Folgenden wird das Menü *IP TRIGGERED BANDWIDTH ON DEMAND (IP BOD)* beschrieben.



Applikationsgesteuertes Bandbreitenmanagement wird über Filter, Filterregeln und Interface-Zuweisung konfiguriert.

Filter Filter legen fest, welche IP-Pakete (und damit Applikationen) Einfluss auf die zur Verfügung stehende Bandbreite haben sollen.

Regel Regeln legen fest, ob für die per Filter erfassten IP-Pakete weitere ISDN-B-Kanäle zu einer bestehenden Verbindung hinzugefügt werden sollen.

Kette Mehrere Regeln können zu einer definierten Regelkette verknüpft werden.

Interface Sie können jedem Interface individuell eine Regelkette zuweisen.

Die Konfiguration erfolgt in den Untermenüs:

- ***FILTER***
- ***RULES FOR BOD***
- ***CONFIGURE INTERFACES FOR BOD***

5.3.1 Untermenü Filter

Im Folgenden wird das Menu *FILTER* beschrieben.

Hier wird eine Liste aller konfigurierten Filter angezeigt (einschließlich der Filter aus ***IP*** ➜ ***ACCESS LISTS*** und ***QOS***.

Die Konfiguration der Filter erfolgt in ***IP*** ➜ ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)*** ➜ ***IP TRIGGERED BANDWIDTH ON DEMAND (IP BOD)*** ➜ ***FILTER*** ➜ ***ADD/EDIT.***

```
R3000w Setup Tool                 Funkwerk Enterprise Communication GmbH
[IP][BOD][FILTER][EDIT]                                          MyGateway

  Description
  Index

  Protocol  any

  Source Address
  Source Mask



  Destination Address
  Destination Mask


  Type of Service (TOS)   00000000              TOS Mask  00000000

                    SAVE                                    CANCEL
```

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

Feld	Wert
Description	Bezeichnung des Filters. Beachten Sie, dass in anderen Menüs nur die ersten 10 bzw. 15 Zeichen sichtbar sind.
Index	Kann hier nicht verändert werden. Das Gateway vergibt hier neu definierten Filtern automatisch eine Nummer.
Protocol	Legt ein Protokoll fest. Mögliche Werte: *any, tcp/udp-port, icmp, ggp, ip, tcp, egp, igp, pup, chaos, udp, hmp, xns_idp, rdp, rsvp, gre, esp, ah, tlsp, skip, kryptolan, iso-ip, igrp, ospf, ipip, ipx-in-ip, vrrp, l2tp*. Standardwert ist *any* und passt auf jedes Protokoll.

Feld	Wert
Type	Nur bei ***PROTOCOL*** = *icmp*. Mögliche Werte: *any, echo reply, destination unreachable, source quench, redirect, echo, time exceeded, param problem, timestamp, timestamp reply, address mask, address mask reply*. Standardwert ist *any*. Siehe RFC 792.
Connection State	Bei ***PROTOCOL*** = *tcp* können Sie ein Filter definieren, das den Status der TCP-Verbindung berücksichtigt. Mögliche Werte: ■ *established*: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden. ■ *any* (Standardwert): Das Filter passt auf alle TCP-Pakete.
Source Address	Definiert die Quell-IP-Adresse der Datenpakete.
Source Mask	Netzmaske zu ***SOURCE ADDRESS***
Source Port	Nur für ***PROTOCOL*** = *tcp/udp-port*. Quell-Port-Nummer bzw. Bereich von Quell-Port-Nummern. Mögliche Werte siehe “Auswahlmöglichkeiten von Source Port bzw. Destination Port” auf Seite 42. Standardwert ist *any*.

Feld	Wert
Specify Port ..to Port	Bei ***Source Port*** bzw. ***Destination Port*** = *specify* bzw. *specify range* Port-Nummern bzw. Bereich von Port-Nummern.
Destination Address	Definiert die Ziel-IP-Adresse der Datenpaketet.
Destination Mask	Netzmaske zu ***Destination Address***
Destination Port	Nur für ***Protocol*** = *tcp/udp-port*. Ziel-Port-Nummer bzw. Bereich von Ziel-Port-Nummern, auf den das Filter passt. Mögliche Werte siehe “Auswahlmöglichkeiten von Source Port bzw. Destination Port” auf Seite 42. Standardwert ist *any*.
Type of Service (TOS)	Kennzeichnet die Priorität des IP-Pakets, vgl. RFC 1349 und RFC 1812. (Angabe im binären Format)
TOS Mask	Bitmaske für Type of Service. (Angabe im binären Format)

Tabelle 5-7: Felder im Menü ***Filter***

Source Port bzw. ***Destination Port*** enthält folgende Auswahlmöglichkeiten:

Feld	Wert
any (Standardwert)	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.

Feld	Wert
clients 2 (32768....65535)	Client Port-Nummern: 32768 ... 65535.
unpriv (1024...65535)	unpriviligierte Port-Nummern: 1024 ... 65535.

Tabelle 5-8: Auswahlmöglichkeiten von ***SOURCE PORT*** bzw. ***DESTINATION PORT***

5.3.2 Untermenü Rules for BOD

Im Folgenden wird das Menu *RULES FOR BOD* beschrieben.

In ***IP*** ➜ ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)*** ➜ ***IP TRIGGERED BANDWIDTH ON DEMAND (IP BOD)*** ➜ ***RULES FOR BOD*** werden alle konfigurierten Regeln aufgelistet.

Die Konfiguration erfolgt im Menü ***ADD/EDIT***.

```
R3000w Setup Tool                 Funkwerk Enterprise Communication GmbH
[IP][BOD][RULE][ADD]                                            MyGateway


  Action                    invoke  M

  Direction                 outgoing
  Number of Channels        0

  Filter                    Firstfilter (1)




          SAVE                                  CANCEL
```

Das Menü besteht aus folgenden Feldern:

Feld	Wert
Index	Erscheint nur bei ***EDIT***. Kann nicht verändert werden. Hier wird der ***INDEX*** von bestehenden Regeln angezeigt. Das Gateway vergibt neu definierten Regeln automatisch eine Nummer.
Insert behind Rule	Erscheint nur, bei ***ADD*** und wenn mindestens eine Regel vorhanden ist. Legt fest, hinter welche bestehende Regel die neue Regel eingefügt wird. Mit *none* beginnen Sie eine neue eigenständige Kette.
Action	Legt fest, wie mit einem gefilterten Datenpaket verfahren wird. ■ *invoke M* (Standardwert): B-Kanäle werden zugeschaltet, wenn ***FILTER*** und ***DIRECTION*** passen. ■ *invoke !M*: B-Kanäle werden zugeschaltet, wenn ***FILTER*** oder ***DIRECTION*** nicht passen. ■ *deny M*: B-Kanäle werden nicht zugeschaltet, wenn ***FILTER*** und ***DIRECTION*** passen. ■ *deny !M*: B-Kanäle werden nicht zugeschaltet, wenn ***FILTER*** oder ***DIRECTION*** nicht passen. ■ *ignore*: Nächste Regel anwenden.
Direction	Richtung der Datenpakete. Mögliche Werte: ■ *outgoing* (Standardwert): ausgehende Datenpakete ■ *incoming*: eingehende Datenpakete ■ *both*: ein- und ausgehende Datenpakete.

Feld	Wert
Number of Channels	Zahl der B-Kanäle, die zugeschaltet werden sollen. Standardwert ist *0*.
Filter	Filter, das verwendet wird.
Next Rule	Erscheint nur, wenn eine bestehende Regel editiert wird. Legt fest, welche Regel als nächste angewendet wird.

Tabelle 5-9: Felder im Menü ***RULES FOR BOD***

Im Menü ***IP*** ➜ ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)*** ➜ ***IP TRIGGERED BANDWIDTH ON DEMAND (IP BOD)*** ➜ ***RULES FOR BOD*** ➜ ***REORG*** können Sie die Indizierung der Regeln neu ordnen lassen, wobei die Reihenfolge der angelegten Regeln beibehalten wird. Im Feld ***INDEX OF RULE THAT GETS INDEX 1*** wird diejenige Regel festgelegt, die den Rule ***INDEX** 1* erhalten soll.

```
R3000w Setup Tool                Funkwerk Enterprise Communication GmbH
[IP][BOD][RULE][REORG]: Reorganize Rules                        MyGateway


       Index of Rule that gets Index 1      none



            REORG                                  CANCEL
```

Standardmäßig wird immer die Regelkette, die mit Rule ***INDEX** 1* anfängt, auf die Schnittstelle des Gateways (z. B. WAN-Partner) angewendet.

5.3.3 Untermenü Configure Interfaces for BOD

Im Folgenden wird das Menu *CONFIGURE INTERFACES FOR BOD* beschrieben.

Im Menü ***IP*** ➜ ***BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)*** ➜ ***IP TRIGGERED BANDWIDTH ON DEMAND (IP BOD)*** ➜ ***CONFIGURE INTERFACES FOR BOD*** werden alle WAN Partner Interfaces aufgelistet.

In ***CONFIGURE INTERFACES FOR BOD*** ➜ ***EDIT*** ordnen Sie den ausgewählten Interfaces den Beginn einer Regelkette zu.

```
R3000w Setup Tool                 Funkwerk Enterprise Communication GmbH
[IP][BOD][INTERFACES][EDIT]                                      MyGateway


 Interface                 Filiale
 First Rule                RI 1 FI 1 (Firstfilter)


            SAVE                                   CANCEL
```

Das Menü besteht aus folgenden Feldern:

Feld	Wert
Interface	Name des Interfaces, das ausgewählt wurde. Dieses Feld kann nicht bearbeitet werden.
First Rule	Definiert den Beginn der Regelkette, die auf Datenpakete, die über ***INTERFACE*** eingehen, angewendet werden soll. Mit *none* (Standardwert) legen Sie fest, dass auf ***INTERFACE*** keine Filter angewendet werden.

Tabelle 5-10: Felder im Menü ***CONFIGURE INTERFACES FOR BOD*** ➜ ***EDIT***

6 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 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.***

```
R3000w Setup Tool                 Funkwerk Enterprise Communication 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. Standardwert ist *1*.

Tabelle 6-1: Felder im Menü ***IP ADDRESS POOL WAN (PPP)***

7 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 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.***

```
R3000w Setup Tool                Funkwerk Enterprise Communication GmbH
[IP][DHCP][ADD]: Define Range of IP Addresses                  MyGateway


  Interface                                 en1-0
  Type                                      Any
  IP Address
  Number of consecutive addresses           1
  Lease Time (Minutes)                      120
  MAC Address
  Alive Test Period (seconds, 0=disabled)   0

  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.

Feld	Wert
Type	Einschränkung des DHCP-Adress-Pools auf einen bestimmten Client-Typ: ■ *IPSec*: DHCP-Adress-Pool gilt nur für IPSec Clients. ■ *Non-IPSec*: DHCP-Adress-Pool gilt nicht für IPSec Clients. ■ *Any*: DHCP-Adress-Pool gilt für alle Clients.
IP Address	Erste IP-Adresse des Adress-Pools.
Number of consecutive addresses	Anzahl der IP-Adressen im Adress-Pool, einschließlich der ersten IP-Adresse (***IP ADDRESS***). Standardwert 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. Standardwert ist *120*.
MAC Address	Nur bei ***NUMBER OF CONSECUTIVE ADDRESSES*** = *1* Nur dem Gerät mit ***MAC ADDRESS*** wird ***IP ADDRESS*** zugewiesen.
Client Identifier	Nur bei ***NUMBER OF CONSECUTIVE ADDRESSES*** = *1* Wird das Feld ***MAC ADDRESS*** markiert, kann man hierfür alternativ die Option ***CLIENT IDENTIFIER*** wählen. Dieses ist in solchen Fällen nötig, in denen keine MAC Adresse zur Verfügung steht, z.B. wenn der IPSec Client auf einem PC ohne Ethernet betrieben wird. Dazu geben Sie hier den Namen des Clients ein.

Feld	Wert
Alive Test Period (seconds, 0=disabled)	Legt einen Zeitraum (in Sekunden) fest, nach dem überprüft wird, ob die Clients, denen eine IP-Adresse aus ***IP ADDRESS POOL LAN (DHCP)*** zugewiesen wurde, noch erreichbar sind. Falls ein Client nicht mehr erreichbar ist, kann die Ip-Adresse wieder anderweitig vergeben werden. Mögliche Werte sind *0*..*65535*. Standardwert ist *0*. Wenn hier *0* gesetzt ist, wird kein Alive-Test durchgeführt.
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* (Standardwert) ■ *Broadcast Node* ■ *Point-to-Point Node* ■ *Mixed Node* ■ *Hybrid Node*

Tabelle 7-1: Felder im Menü ***IP ADDRESS POOL LAN (DHCP)***

8 Untermenü SNMP

Im Folgenden wird das Menü *IP* ➜ *SNMP* beschrieben.

```
R3000w Setup Tool                Funkwerk Enterprise Communication GmbH
[IP][SNMP]: SNMP Configuration                                  MyGateway


     SNMP versions               v1|v2c|v3

     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 versions	Dieser Parameter definiert, welche SNMP-Versionen das Gateway für das Lauschen auf externe SNMP-Zugriffe und das Senden von SNMP Traps nach extern zur Verfügung stellt. Mögliche Werte sind: ■ *v1|v2c|v3* (Standardwert) - Das Gateway akzeptiert SNMP-Zugriffe der Versionen 1, 2c und 3. ■ *off* - Das Gateway akzeptiert keine externen SNMP-Zugriffe, d. h. der SNMP-Zugriff ist nur noch auf der Konsole des Getways möglich (z. B. per SSH oder über die serielle Schnittstelle). ■ *v1|v2c* - Das Gateway akzeptiert nur SNMP-Zugriffe der Versionen 1.und 2c, die 64bit Counter und Zugriffskontrolle über SNMP Communities unterstützt. ■ *v3* - Das Gateway akzeptiert nur SNMP-Zugriffe der Version 3 mit "echter" User-Verwaltung und Zugangskontrolle durch Access Level. Weitergehende Informationen zu den SNMP-Versionen finden Sie in den entsprechenden RFCs und Drafts: ■ SNMP V. 1: RFC 1157 ■ SNMP V. 2c: RFC 1901 – 1908 ■ SNMP V. 3: RFC 3410 – 3418.

Feld	Wert
SNMP listen UDP port	Hier geben Sie die Nummer des UDP-Ports ein, an dem das Gateway SNMP-Requests annimmt. Standardwert 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. Standardwert 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* (Standardwert).
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. Standardwert ist *snmp-Trap*.

Tabelle 8-1: Felder im Menü ***IP ➜ SNMP***

9 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***

9.1 Untermenü RADIUS Authentication and Accounting

Im Folgenden wird das Menü *RADIUS Authentication and Accounting* 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***.

```
R3000w Setup Tool                 Funkwerk Enterprise Communication 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* (Standardwert) - Der RADIUS Server wird verwendet, um den Zugang zu einem Netzwerk zu regeln. ■ *accounting* - Der RADIUS Server wird zur Erfassung von 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. ■ *802.1x* - Der RADIUS Server wird verwendet, um WLAN Clients gemäß 802.1x-Standard zu authentifizieren.
IP Address	Die IP-Adresse des RADIUS Servers.
Password	Gemeinsam genutzes Passwort für die Kommunikation zwischen RADIUS Server und Gateway.

Feld	Wert
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). Standardwert ist *0*.
Policy	Definiert wie das bintec Gateway reagiert, wenn eine negative Antwort auf eine Anfrage eingeht. Mögliche Werte: ■ *authoritative* (Standardwert): 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. Standardwert ist *1812.*

Feld	Wert
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*. Standardwert ist *1000* (1 Sekunde).
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*. Standardwert 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* (Standardwert): Server beantwortet Anfragen. ■ *inactive*: Server antwortet nicht (siehe ***RETRIES***). ■ *disabled*: Anfragen an einen bestimmten RADIUS Server sind vorübergehend deaktiviert.

Feld	Wert
Validate	Mögliche Werte: ■ *enabled* (Standardwert): 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.
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* (Standardwert).

Feld	Wert
Alive Check (if inactive)	Hier aktivieren Sie die Überprüfung der Erreichbarkeit eines RADIUS Servers im ***STATE*** *inactive*. ■ enabled (Standardwert): 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 9-1: Felder im Menü ***RADIUS SERVER***

9.2 Untermenü TACACS+ Authentication and Authorization

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

Das Menü ***IP*** ➜ ***REMOTE AUTHENTICATION (RADIUS/TACACS+)*** ➜ ***TACACS+ AUTHENTICATION AND AUTHORIZATION*** enthält eine Liste aller bereits konfigurierten TACACS+ Server.

```
R3000w Setup Tool                 Funkwerk Enterprise Communication GmbH
[IP][TACACS+]: Configure TACACS+ Server                          MyGateway

 IP Address       Priority     AdminStatus         OperStatus

192.168.0.100     0            up                  up




    ADD                DELETE              EXIT
```

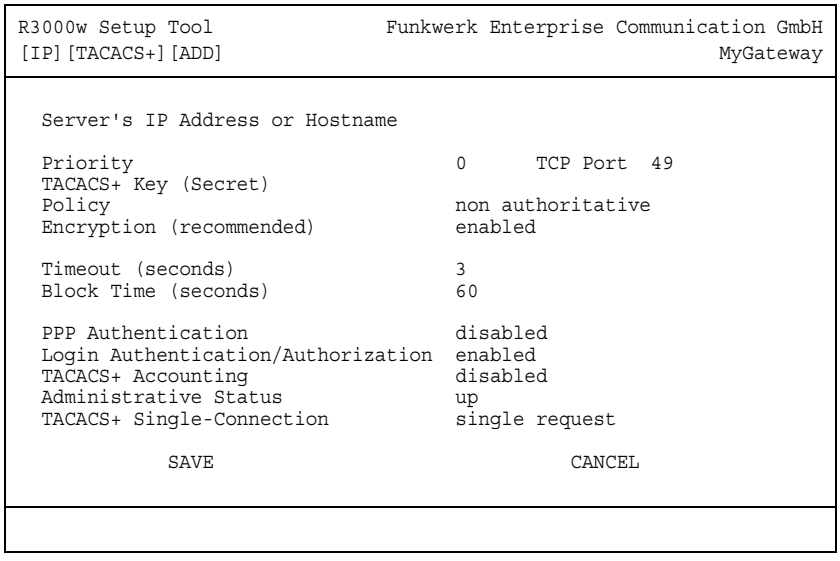
Das TACACS+ Protokoll ermöglicht die Zugriffssteuerung von Gateways, Netzzugangsservern (NAS) und anderen Netzwerkkomponenten über einen oder mehrere zentrale Server. TACACS+ ist ein AAA-Protokoll und bietet Authentifizierungs-, Autorisierungs- und Abrechnungsdienste (TACACS+ Accounting wird derzeit von bintec Gateways nicht unterstützt).

Folgende TACACS+ Funktionalitäten sind auf Ihrem bintec Gateway verfügbar:

- Authentifizierung für Login-Shell
- Authentifizierung für PPP-Verbindungen
- Kommando-Authorisierung auf der Shell (z.B. telnet, setup. show)

TACACS+ verwendet TCP Port 49 und stellt eine gesicherte und verschlüsselte Verbindung her.

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



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. (TACACS+ Accounting wird derzeit von bintec Gateways nicht unterstützt.)
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 für ***Policy*** = *non authoritative*), wird der Eintrag mit der nächstniedrigeren Priorität genutzt. Verfügbare Werte sind *0* bis *9*, der Standardwert ist *0*.

Feld	Beschreibung
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 (Verschlüsselung nur für ***ENCRYPTION (RECOMMENDED)*** = *enabled*). Die maximale Länge des Eintrags ist 32 Zeichen.
Policy	Hier können Sie die Interpretation der TACACS+ Antwort auswählen. Verfügbare Werte: ■ *authoritative*: Eine negative Antwort auf eine Anfrage wird akzeptiert, d.h. es wird kein weiterer TACACS+ Server abgefragt. ■ *non authoritative* (Standardwert): Die TACACS+ Server werden gemäß ihrer Priorität (siehe ***PRIORITY***) abgefragt, bis eine positive Antwort oder von einem authoritativen Server eine negative Antwort kommt. Die gateway-interne Benutzerverwaltung wird durch TACACS+ nicht ausgeschaltet und wird geprüft, nachdem alle TACACS+ Server abgefragt wurden.

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*. ■ *enabled*: Die TACACS+ Pakete werden mit MD5 verschlüsselt. ■ *disabled*: Die Pakete und damit alle dazugehörigen Informationen werden unverschlüsselt übertragen. Eine unverschlüsselte Übertragung wird nicht als Standardeinstellung sondern nur für Debug-Zwecke empfohlen.
Timeout (seconds)	Hier geben Sie die Zeit in Sekunden ein, die der NAS auf eine Antwort von TACACS+ wartet. Falls während der Wartezeit keine Antwort empfangen wird, wird der als nächster konfigurierte TACACS+ Server abgefragt (nur für ***POLICY*** = *non authoritative*) und der aktuelle Server in einen *blocked*-Status versetzt (siehe ***OPERSTATUS*** = *blocked* in ***IP*** ➜ ***REMOTE AUTHENTICATION (RADIUS/TACACS+)*** ➜ ***TACACS+ AUTHENTICATION AND AUTHORIZATION***). Verfügbare Werte sind *1* bis *60*, der Standardwert ist *3*.

Feld	Beschreibung
Block Time (seconds)	Hier geben Sie die Zeit in Sekunden 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, und somit keine weiteren Server angefragt werden.
PPP Authentication	Diese Funktion wird von den vorliegenden Gateways nicht unterstützt. Sie wird möglicherweise in einer späteren Version unserer Systemsoftware realisiert. Hier wird festgelegt, ob der aktuelle TACACS+ Server für die Authentifizierung der PPP-Dialin-Clients benutzt werden soll.
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 denvorliegenden Gateways nicht unterstützt. Sie wird möglicherweise in einer späteren Version unserer Systemsoftware realisiert. Hier wird festgelegt, ob die Abrechnung der PPP-Verbindungen und des Login benutzt werden soll.

Feld	Beschreibung
Administrative Status	Hier können Sie den Status auswählen, in den der Server versetzt werden soll. Mögliche Werte: ■ *up* (Standardwert): Der dazugehörige Server wird für Authentifizierung, Autorisierung und Abrechnung gemäß Priorität (siehe Feld ***PRIORITY***) und aktuellem Betriebsstatus benutzt (siehe ***OPERSTATUS*** in ***IP*** ➜ ***REMOTE AUTHENTICATION (RADIUS/TACACS+)*** ➜ ***TACACS+ AUTHENTICATION AND AUTHORIZATION***). ■ *down*: Ddieser Eintrag wird für TACACS+ AAA-Anforderungen nicht berücksichtigt.
TACACS+ Single-Connection	■ *single request* (Standardwert): Mehrere Sitzungen werden nicht über eine einzige TCP-Verbindung übertragen, für jede TACACS+ Sitzung wird eine neue Verbindung aufgebaut und am Ende der jeweiligen Sitzung abgebaut. ■ *multiple requests*: Mehrere TACACS+ Sitzungen (aufeinanderfolgende TACACS+ Anforderungen) werden gleichzeitig über eine einzige TCP-Verbindung unterstützt.

Tabelle 9-2: ***IP*** ➜ ***REMOTE AUTHENTICATION (RADIUS/TACACS+)*** ➜ ***TACACS+ AUTHENTICATION AND AUTHORIZATION*** ➜ ***ADD/EDIT***

10 Untermenü DNS

Im Folgenden wird das Menü *DNS* beschrieben.

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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 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* (Standardwert): 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* (Standardwert): 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* (Standardwert) ■ *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. Standardwert 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* (Standardwert): 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* (Standardwert): 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.

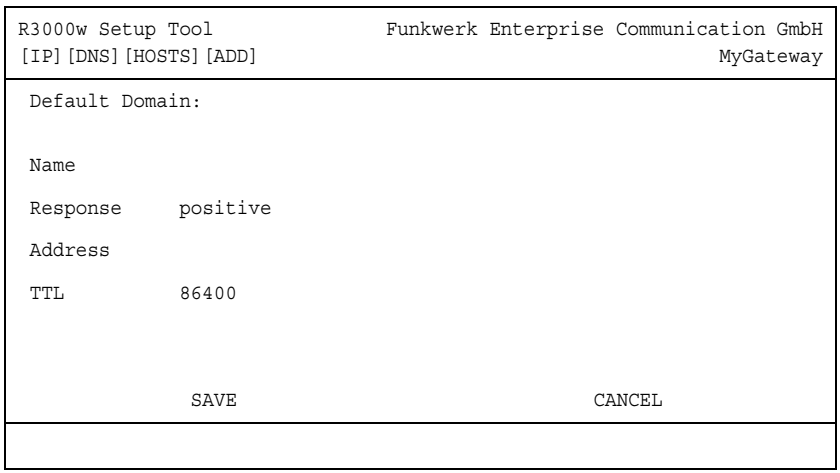
Tabelle 10-1: Felder im Menü ***DNS***

Über dieses Menü gelangen Sie in folgende Untermenüs:

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

10.1 Untermenü Static Hosts

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



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:

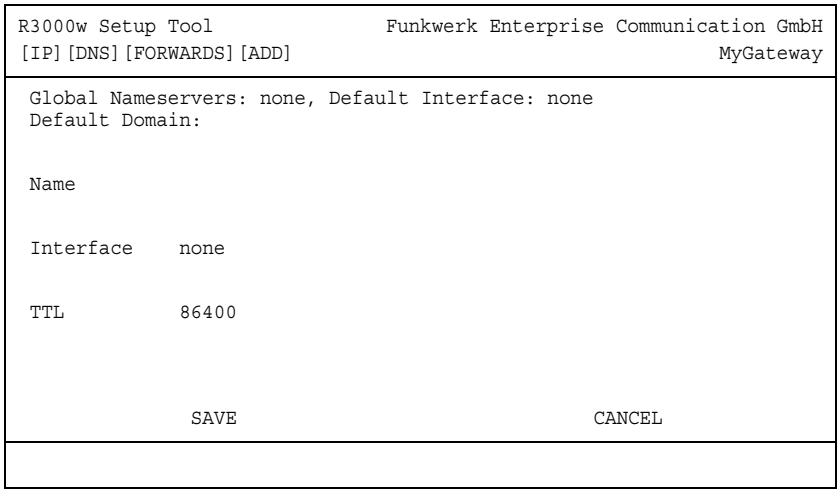
Feld	Wert
Default Domain	Anzeige des in ***IP*** ➜ ***STATIC SETTINGS*** eingetragenen Domain Names des Gateways.

Feld	Wert
Name	Host-Name, dem ***ADDRESS*** mit diesem statischen Eintrag zugeordnet wird. Kann auch mit dem Wildcard * beginnen, z. B. *.funkwerk-ec.com. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit **SAVE** "***.<DEFAULT DOMAIN>.***" ergänzt.
Response	Art des statischen Eintrags. Mögliche Werte: ■ *positive* (Standardwert): 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. Standardwert ist *86400* (= 24 h).

Tabelle 10-2: Felder im Menü ***STATIC HOSTS***

10.2 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. Standardwert 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. Standardwert ist *86400* (=24 h).

Tabelle 10-3: Felder im Menü ***FORWARDED DOMAINS***

10.3 Untermenü Dynamic Cache

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

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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 10-4: 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.

10.4 Untermenü Advanced Settings

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

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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*. Standardwert 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. Standardwert ist *86400*.
Maximum TTL for Neg Cache Entries	Wird bei einem negativen dynamischen Eintrag im Cache als ***TTL*** gesetzt. Standardwert ist *86400*.

Tabelle 10-5: Felder im Menü ***Advanced Settings...***

10.5 Untermenü Global Statistics

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

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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 10-6: Felder im Menü ***GLOBAL STATISTICS...***

11 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.

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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:

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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. Standardwert 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* (Standardwert): Die erweiterte Namensauflösung ist deaktiviert.

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

Tabelle 11-1: 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***.

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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. Standardwert: *80*.
Protocol	Hier wählen Sie eines der implementierten Protokolle aus. Es stehen zur Verfügung: ■ *dyndns* (Standardwert) (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. Standardwert ist *300* Sekunden.

Tabelle 11-2: Felder im Menü ***DynDNS Provider List*** ➜ ***ADD/EDIT***

12 Untermenü Routing protocols

Im Folgenden wird das Menü *ROUTING PROTOCOLS* beschrieben.

```
R3000w Setup Tool                Funkwerk Enterprise Communication GmbH
[IP][ROUTING]: Routing protocols                                MyGateway

               Routed                    running

               RIP >

               OSPF >


              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.

12.1 Untermenü RIP

Im Folgenden wird das Menü *RIP* beschrieben.

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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 Standardwert *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***.

12.1.1 Untermenü Static Settings

Im Folgenden wird das Menü *Static Settings* beschrieben.

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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 Standardwert 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 Standardwert 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* (Standardwert) 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* (Standardwert) ■ *enabled* Wenn Sie den Wert *disabled* belassen, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.

Tabelle 12-1: Felder im Menü ***STATIC SETTINGS***

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

12.1.2 Untermenü Timer

Im Folgenden wird das Menü *TIMER* beschrieben.

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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 Standardwert 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 Standardwert 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 Standardwert 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 Standardwert 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 Standardwert ist *5*.

Tabelle 12-2: Felder im Menü ***TIMER***

12.1.3 Untermenü Filter

Im Folgenden wird das Menü *FILTER* beschrieben.

```
R3000w Setup Tool                Funkwerk Enterprise Communication 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.

```
R3000w Setup Tool                Funkwerk Enterprise Communication GmbH
[IP][ROUTING][RIP][FILTER][ADD]: Define RIP Filter              MyGateway


        Interface                                  en1-0
        IP-Address
        Netmask
        Priority                                   1
        Direction                                  import
        Distribution                               disabled
        Metric1 offset on interface up             0
        Metric1 offset on interface dormant        0


                SAVE                                    CANCEL
```

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 Standardwert ist *1*.
Direction	Hier bestimmen Sie, ob das Filter für den Export oder den Import von Routen gilt. Die möglichen Werte sind: ■ *import* ■ *export.* Standardwert 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 Standardwert 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 Standardwert 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 Standardwert ist *0*.

Tabelle 12-3: Felder im Menü ***FILTER***

12.2 Untermenü OSPF

Im Folgenden wird das Menü *OSPF* beschrieben.

```
R3000w Setup Tool                     Bintec Access Networks GmbH
[IP][ROUTING][OSPF]: OSPF Configuration                    MyGateway


                Static Settings
                Interfaces
                Areas

                EXIT
```

Im Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***OSPF*** werden im Unterschied zu RIP alle globalen und interface-spezifischen OSPF-Einstellungen vorgenommen.

OSPF (Open Shortest Path First) ist ein Routing Protokoll, das häufig in größeren Netzwerken als Alternative zu RIP angewendet wird. Es wurde ursprünglich dazu entwickelt, einige Einschränkungen des RIP zu umgehen (wenn es in größeren Netzwerken verwendet wird).

Einige Probleme (mit RIP), die OSPF umgeht sind:

- Verringerte Netzwerklast
  Nach einer kurzen Initialisierungsphase werden Routing Informationen nicht wie mit RIP periodisch übertragen, sondern nur geänderte Routing Informationen.
- Authentifizierung
  Zur Erhöhung der Sicherheit beim Austausch von Routing Informationen kann eine Gateway-Authentifizierung konfiguriert werden.
- Routing Traffic Kontrolle
  Um den Traffic, der durch Austausch von Routing Informationen entsteht, zu begrenzen, können Gateways zu Areas zusammengefasst werden.
- Verbindungskosten
  Im Unterschied zu RIP wird für die Kalkulation der Verbindungskosten nicht die Anzahl der Next Hops berücksichtigt, sondern die Bandbreite des jeweiligen Transportmediums.
- Keine Einschränkung der Hop-Anzahl
  Die Einschränkung der maximalen Hop-Anzahl 16 bei RIP besteht für OSPF nicht.

Obwohl das OSPF-Protokoll wesentlich komplexer ist als RIP, ist das Grundkonzept dasselbe, d.h. auch OSPF ermittelt zur Weiterleitung der Pakete den jeweils besten Weg.

Autonomous System OSPF ist ein Interior Gateway Protocol, das verwendet wird um Routing Informationen innerhalb eines autonomen Systems (Autonomous System, AS) zu verteilen. Durch Fluten werden Link State Updates zwischen den Gateways ausgetauscht. Jede Änderung der Routing Informationen wird an alle Gateways im Netzwerk weitergegeben. OSPF-Bereiche (Areas) werden definiert, um die Anzahl an Link State Updates einzugrenzen. Alle Gateways einer Area haben eine übereinstimmende Link State Datenbank.

Area Border Routers Eine Area ist interface-spezifisch. Gateways, deren Interfaces zu mehreren Areas gehören und diese an den Backbone anbinden werden Area Border Router (ABR) genannt. ABRs enthalten daher die Informationen der Backbone Area und aller angebunden Areas. Ein Gateway, dessen Interfaces alle in einer Area eingebunden sind, werden Internal Router (IR) genannt.

Link State Pakete Man unterscheidet drei Arten von Link State Paketen: Router Links geben den Status der Interfaces eines Gateways an, die zu einer bestimmt Area gehören. Summary Links werden vom ABR generiert und definiert, wie die Informationen zur Erreichbarkeit im Netzwerk zwischen Areas ausgetauscht werden. In der Regel werden alle Informationen in die Backbone-Area gesendet, welche dann die Informationen an die anderen Areas weiterleitet. Network Links werden vom Designated Router (DS) innerhalb eines Segments verschickt und propagieren alle Gateways, die an ein bestimmtes Multi-Access Segment wie Ethernet, Token Ring und FDDI (auch NBMA) angebunden sind. External Links weisen auf Netzwerke ausserhalb des AS. Diese Netzwerke werden in das OSPF mittels Redistribution eingebunden. Ein Autonomous System Border Router (ASBR) hat in diesem Falle die Aufgabe, diese externen Routen in das AS einzubinden.

Authentifizierung Zur Erhöhung der Sicherheit ist es möglich, die OSPF Pakete authentifizieren zu lassen, so dass die Gateways mittels vorgegebener Passwörter an Routing Domänen teilnehmen können.

Backbone Area In grösseren Netzwerken wird empfohlen, mehrere Areas zu definieren. Wenn mehr als eine Area angelegt wird, muss eine dieser Areas die Area ID 0.0.0.0 besitzen, die die Backbone Area definiert. Diese muss zentraler Punkt aller Areas sein, d.h. alle Areas müssen physikalisch mit der Backbone Area verbunden

sein. In seltenen Fällen können Gateways nicht direkt physikalisch an die Backbone Area angebunden werden. Dann müssen virtuelle Links eingerichtet werden.

Virtuelle Links Der Verwendungszweck von Virtuellen Links ist die Anbindung von Areas, bei denen keine physikalische Anbindung an den Backbone möglich ist und das Aufrechterhalten der Verbindung des Backbone im Falle eines Ausfalls der 0.0.0.0 Area.

Summary Links Summarizing wird die Konsolidierung verschiedener Routen zu einem einzigen Advertisment (Summary Link) genannt. Dieses geschieht in der Regel an den Area-Grenzen durch den ABR.

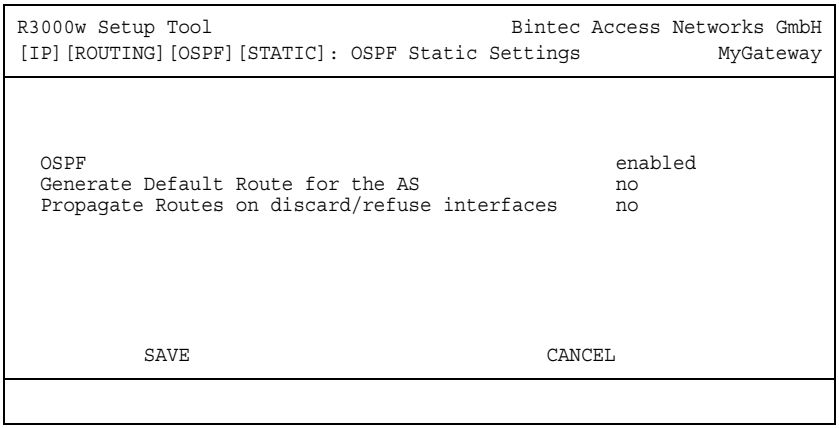
Stub Area Im OSPF können bestimmte Areas als sogenannte Stub Areas definiert werden. Dadurch wird verhindert, dass externe Netzwerke, wie z.B. solche, die aus anderen Protokollen durch Redistribution in OSPF propagiert werden, in die Stub Area hinein propagiert werden. Das Routing solcher Areas nach aussen hin wird mit einer Default Route propagiert. Die Konfiguration einer Stub Area reduziert die Datenbankgrösse innerhalb der Area und verringert die Grösse an benötigtem Speicherplatz auf den Gateways, die in die Area eingebunden sind.

Über das Menü ***IP*** ➜ ***OSPF*** gelangt man in folgende Untermenüs:

- ***STATIC SETTINGS***
- ***INTERFACES***
- ***AREAS***.

12.2.1 Untermenü Static Settings

Im Folgenden wird das Menü *STATIC SETTINGS* beschrieben.



Das Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***OSPF*** ➜ ***STATIC SETTINGS*** beinhaltet globale OSPF Parameter. Hier wird OSPF auf dem Gateway aktiviert.

Das Menü ***STATIC SETTINGS*** enthält folgende Felder:

Feld	Wert
OSPF	Aktiviert (*enabled,* Standardwert) oder deaktiviert (*disabled*) OSPF.
Generate Default Route for the AS	Wenn dieser Wert auf *yes* gesetzt ist, propagiert das Gateway eine Default Route über alle aktiven OSPF Interfaces (siehe ***ADMIN STATUS*** Feld im Menü ***IP*** ➜ ***OSPF*** ➜ ***INTERFACES***). Standardwert ist *no*.

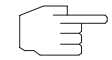
Feld	Wert
Propagate Routes on discard/refuse interfaces	Die logischen Interfaces REFUSE und IGNORE haben folgende Bedeutung: REFUSE bedeutet (wenn eine Route darauf existiert), dass Pakete von diesem Interface verworfen werden und ein ICMP Unreachable Reply generiert wird. IGNORE bedeutet (wenn eine Route darauf existiert), dass Pakete von diesem Interface kommentarlos verworfen werden. Mit *yes* werden Routen, die an die beiden discard/refuse Interfaces gebunden sind, vom OSPF in seine Datenbank übernommen. Bei *no* (Standardwert) werden diese Routen ignoriert.

Tabelle 12-4: Felder im Menü ***STATIC SETTINGS***

12.2.2 Untermenü Interfaces

Im Folgenden wird das Menü *INTERFACES* beschrieben.

```
R3000w Setup Tool                    Bintec Access Networks GmbH
[IP][ROUTING][OSPF][INTERFACE]: Interface Configuration      MyGateway


 Interface   Area     IP Adddress  AdminStatus State Metric
 en0-1       0.0.0.0  192.16.0.181  passive    down  10
 en0-1-snap  0.0.0.0  0.0.0.0       passive    down  10
 vss8-0      0.0.0.0  0.0.0.0       passive    down  1
 vss8-0-snap 0.0.0.0  0.0.0.0       passive    down  1
 vss8-1      0.0.0.0  0.0.0.0       passive    down  1
 vss8-1-snap 0.0.0.0  0.0.0.0       passive    down  1



 EXIT
```



Hinweis

Wenn Ihre Interfaces nicht nur der Backbone Area 0.0.0.0 zugewiesen werden sollen, müssen Sie zunächst in ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***OSPF*** ➜ ***AREAS*** ➜ ***ADD*** weitere OSPF-Bereiche (Areas) definieren.

Hier werden alle OSPF-fähigen Gateway-Interfaces aufgelistet und alle interface-spezifischen Einstellungen vorgenommen.

Die Konfiguration erfolgt in ***ADD/EDIT***.

```
R3000w Setup Tool                    Bintec Access Networks GmbH
[IP][ROUTING][OSPF][INTERFACE][EDIT]: Configure Interface    MyGateway
                                      en0-1


     Admin Status               passive (propagate routes)
     Area ID                    0.0.0.0

     Metric Determination       auto (ifSpeed)
     Metric (direct routes)     10

     Authentication Type        none
     Authentication Key

     Export indirect static routes  no


               SAVE                                  CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Admin Status	Der Status eines OSPF Interfaces definiert, ob über das Interface Routen propagiert und/oder OSPF Protokoll Pakete gesendet werden. Wenn OSPF noch nicht aktiviert wurde, wird nur das ***ADMIN STATUS*** Feld angezeigt (in diesem Fall sind Änderungen irrelevant). Mögliche Werte: ■ *active (propagate routes + run OSPF)*: OSPF ist für dieses Interface aktiviert, d.h. über dieses Interface werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. ■ *passive (propagate routes)*: OSPF ist nicht für dieses Interface aktiviert, d.h. über dieses Interface werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über dieses Interface erreichbare Netze werden jedoch bei der Berechnung der Routing Informationen berücksichtigt und über aktive Interfaces propagiert. ■ *off*: OSPF ist für dieses Interface komplett deaktiviert.
Area ID	Identifiziert den Bereich, dem dieses Interface zugeordnet ist.
Metric Determination	Legt fest, wie die Metrik dieses Interfaces berechnet wird. Siehe Tabelle “Auswahlmöglichkeiten von Metric Determination” auf Seite 109.

Feld	Wert
Metric (direct routes)	Gibt den Basismetrikwert an. Die tatsächlich für eine Route verwendete Metrik beruht auf einem Base Metric Value, der sich aus der Bandbreite des Interfaces errechnet: BMV = 100.000.000 / Bandbreite in bps Das ergibt z. B. 1 für 100Mbit-Ethernet oder 1562 für Dialup ISDN Interfaces (1 B-Channel). Dieser Wert wird dann je nach gewählter ***Metric Determination*** ggf. angepasst. Wenn Sie für ***Metric Determination*** den Wert *fixed* gewählt haben, können Sie hier den Wert für die Metrik eingeben.
Authentication Type	Die Art der Authentifizierung, die angewendet wird, wenn OSPF Pakete über dieses OSPF Interface verschickt (oder eingehende geprüft) werden. Legt fest, wie der Schlüssel im Feld ***Authentication Key*** verwendet wird. Standardmäßig ist der Wert auf *none* gesetzt. Bei *simple* wird der Schlüssel als Textfolge in jedem Paket verschickt. Bei *md5* wird der Schlüssel verwendet, um einen Hash zu erstellen, der in jedem Paket mitgeschickt wird. Standardwert ist *none*.
Authentication Key	Eine Textfolge, die in Verbindung mit dem definierten ***Authentication Type*** verwendet wird.
Export indirect static routes	Wenn dieser Wert auf *no* (Standardwert) gesetzt ist, werden nur direkte Routen (d.h. Routen zu direkt über dieses Interface erreichbaren Netzen) über aktive OSPF Interfaces propagiert (siehe ***Admin Status*** Feld). Wenn der Wert auf *yes* gesetzt ist, werden auch indirekte statische Routen über aktive Interfaces propagiert.

Tabelle 12-5: Felder im Menü ***Interfaces***

METRIC DETERMINATION enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
auto (ifSpeed)	Metrik = der Wert der Basismetrik, welche auf der Bandbreite (***IFSPEED***) des Interfaces basiert.
fixed	Die im folgenden Feld definierte Metrik wird immer verwendet, d.h. es erfolgt keine automatische Berrechnung der Metrik.
auto + adjust	Wenn das Interface im *up*-Status ist, errechnet sich die tatsächlich verwendete Metrik wie folgt: Metrik = <automatisch determinierter BMV> - 10. Ansonsten wird die automatisch errechnete Metrik verwendet.
fixed + adjust	Wenn das Interface im *up*-Status ist, errechnet sich die tatsächlich verwendete Metrik wie folgt: Metrik = <fest eingestellte Metrik)> - 10. Ansonsten wird die fest eingestellte Metrik verwendet.

Tabelle 12-6: Auswahlmöglichkeiten von ***METRIC DETERMINATION***

12.2.3 Untermenü Areas

Im Folgenden wird das Menü *AREAS* beschrieben.

```
R3000w Setup Tool                    Bintec Access Networks GmbH
[IP][ROUTING][OSPF][AREA]: Area Configuration                MyGateway


  Area ID          Import External Routes
  0.0.0.0          yes


   ADD                 DELETE              EXIT
```

Bevor das Gateway-Interface einem Bereich zugeordnet werden kann, müssen zunächst OSPF-Bereiche definiert werden.

Eine Ausnahme bildet der Backbone Bereich, der automatisch beim Booten generiert wird, und auf den alle Interfacezuweisungen per Default gesetzt werden, die nicht ausdrücklich einer anderen Area zugewiesen sind.

Das Menü ***IP*** ➜ ***ROUTING PROTOCOLS*** ➜ ***OSPF*** ➜ ***AREAS*** enthält eine Liste aller konfigurierten OSPF-Bereiche (***AREAS***). Die Konfiguration erfolgt in ***ADD/EDIT***.

```
R3000w Setup Tool                    Bintec Access Networks GmbH
[[IP][ROUTING][OSPF][AREA][ADD]                              MyGateway


   Area ID                                  0.0.0.0

   Import external routes                   no
   Import summary routes                    no
   Create area default route (only ABR)     no


   Area Ranges >


          SAVE                                    CANCEL
```

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

Feld	Wert
Area ID	Identifiziert den OSPF-Bereich, zu dem dieser Eintrag gehört. Der Backbone-Bereich ist *0.0.0.0*.
Import external routes	Spezifiziert, ob das Gateway Routing Informationen, welche aus externen autonomen Systemen (nicht Areas) generiert wurden, importieren soll. *Yes* (Defaultwert) aktiviert den Import. Bei *no* wird diese Area als sog. Stub Area definiert.

Feld	Wert
Import summary routes	Nur wenn ***IMPORT EXTERNAL ROUTES*** = *no*. Definiert, ob Summary LSAs (vom Area Border Gateway generierte Routing Informationen) in die Stub Area gesendet werden sollen.
Create area default route (only ABR)	Nur wenn ***IMPORT EXTERNAL ROUTES*** = *no*. Das Area Border Gateway sendet keine LSAs in die Stub Area, sondern propagiert nur eine Default Route.

Tabelle 12-7: Felder im Menü ***AREAS***

Untermenü *AREA RANGES*

Die Optionen dieses Untermenüs sind nur für die Konfiguration des Area Border Gateways anzuwenden. Hier können Sie Netzwerkrouten zusammenfassen zu einem Gesamtsubnetz. Dieses Gesamtsubnetz wird anstelle der eigentlich gelernten Subnetze propagiert.

```
R3000w Setup Tool                    Bintec Access Networks GmbH
[IP][ROUTING][OSPF][AREA][ADD][RANGE][ADD]                  MyGateway


     Adress
     Mask

     Advertise Matching              yes




          SAVE                                   CANCEL
```

Die Konfiguration erfolgt in ***ADD/EDIT***.

Das Menü besteht aus folgenden Feldern:

Feld	Wert
Address	Geben Sie hier die IP-Adresse des Bereichs ein, der zusammengefasst werden soll.
Mask	Netzmaske zu ***ADDRESS***
Advertise Matching	Subnetze, die zu Bereichen zusammengefasst sind, lösen entweder das Propagieren des angegebenen Verbunds aus (*yes*), oder führen dazu, dass das Subnetz gar nicht ausserhalb des Bereichs propagiert wird (*no*), d.h. weder die eigentlichen Subnetzte noch das zusammengefasste Gesamtsubnetz werden propagiert. Mögliche Werte: *yes* (Defaultwert), *no*.

Tabelle 12-8: Felder im Menü ***AREA RANGE***

Index: IP

A

Action 43, 44
ADDEXT 10
Address 77, 80, 112
Admin Status 107
Administrative Status 70
Advertise Matching 112
Alias Name (Description) 29
Alive Check (if inactive) 64
Alive Test Period (seconds, 0=disabled) 51
Area ID 107, 110
Area Range 112
Authentication Key 108
Authentication Type 108

B

Bandwidth Management 23
Bandwidth on Demand 23
Block Time (seconds) 69
BOD 23

C

Cache Hitrate (%) 84
Cache Hits 83
Client / Server 57
Client Identifier 50
Connection State 40
Control all TCP Services 28

D

Default Domain 76
Default Domains 78
Default Interface 74
Default Route distribution 94
Description 31, 39
Destination Address 41
Destination IP-Address 8, 36
Destination Mask 36, 41

Destination Port 11, 12, 41
DHCP Assignment 75
Dialout 63
Direction 43, 99
Distribution 100
Distribution Fraction (in percent) 33
Distribution Mode 31
Distribution Policy 31, 33
Distribution Ratio 32
DNS 13, 71
DNS Requests 83
DNS-Proxy 13
Domain Name 13
Domain Name Server 13, 71
Dynamic Cache 75
DynDNS Registrierung 85

E

Encryption (recommended) 68
Export indirect static routes 108
Extended Routing 10
External Address 19
External Mask 19
External Port 20

F

Filter 38, 44
First Rule 45
Flags 7
Forwarded Domains 75
Forwarded Requests 83

G

Garbage Collection Timer 96
Gateway 51
Gateway IP-Address 9, 36
Generate Default Route for the AS 104

H

Hold down timer 96
Host Name 87

HTTP TCP port 14

I
Ignore 9
Import external routes 110
Index 39, 43
Insert behind Rule 43
Interface 26, 35, 38, 45, 49, 79, 87, 98
Interface 1 - 3 32
Interface Group ID 31
Internal Address 20
Internal Mask 20
Internal Port 21
Invalid DNS Packets 83
IP Address 47, 50, 60
IP address pool LAN (DHCP) 49
IP address pool WAN (PPP) 47
IP-Address 99
IPCP Assignment 75

K
Kette 38

L
LAN 9, 37
Lease Time (Minutes) 50
Load Balancing 23
Local 10
Local Nameservers 78
Login Authentication/Authorization 69

M
MAC Address 50
Mask 112
Maximum Number of DNS Records 82
Maximum TCP Download Rate (kbits/s) 28
Maximum TTL for Neg Cache Entries 82
Maximum TTL for Pos Cache entries 82
Metric 9, 108
Metric Determination 107, 109
Metric1 offset on interface dormant 100

Metric1 offset on interface up 100
Minimum Wait 90
Mode 11, 12
MX 87

N

Name 77, 78, 80, 88
Namensauflösung 71
Negative Cache 74
NetBT Mode Type 51
Netmask 8, 99
Network 8, 36
Network Address Translation 16
Next Rule 44
Number of Channels 44
Number of consecutive addresses 47, 50

O

Optimize Download Rate via TCP ACK prioritisation 26
OSPF 91, 104
Overwrite Global Nameservers 74

P

Partner / Interface 9
Password 60, 87
Path 89
Permission 88
Poisoned Reverse 94
Policy 61, 67
Pool ID 47
Port 37, 61, 89
Positive Cache 73
PPP Authentication 69
PPTP Passthrough 16
Primary BOOTP Relay Server 14
Primary Domain Name Server 13
Primary WINS 13
Priority 61, 66, 99
Propagate Routes on discard/refuse interfaces 105
Protocol 11, 18, 36, 39, 60, 89

Provider 87

R

RADIUS Pakete 58
Radius Server 57
Received DNS Packets 83
Ref 80
Refuse 9
Regel 38
Remote Address 19
Remote CAPI Server TCP port 14
Remote Mask 19
Remote Port 19
Remote TRACE Server TCP port 14
Resp 80
Response 77
Retransmission timer 97
Retries 62
RFC 2091 variable timer 95
RFC 2453 variable timer 94
RIP 91
RIP UDP port 14
Route Timeout 96
Route Type 8
Routing protocols 91
Routing-Eintrag ändern 7
Routing-Eintrag hinzufügen 7

S

Secondary BOOTP Relay Server 14
Secondary Domain Name Server 13
Secondary WINS 13
Server 88
Server Failures 84
Server's IP Address or Hostname 66
Service 18, 36
Silent Deny 16
SNMP 53
SNMP listen UDP port 55

SNMP trap broadcasting 55
SNMP trap community 55
SNMP trap UDP port 55
SNMP versions 54
Source Address 40
Source Interface 11
Source IP-Address 11, 36
Source Mask 11, 36, 40
Source Port 11, 12, 40
Specify Port 41
State 62
Static Hosts 75
Status 29
Successfully Answered Queries 84

T

TACACS+ Accounting 69
TACACS+ Key (Secret) 67
TACACS+ Single-Connection 70
TCP Port 67
TCP Service Port 29
TDRC Mode 27
Timeout (ms) 62
Timeout (seconds) 68
TOS Mask 11, 41
TTL 77, 79, 80
Type 35, 40, 50
Type of Service (TOS) 11, 41

U

Unique Source IP Address 14
Update Timer 96
User 87

V

Validate 63

W

WAN with transit network 9, 37
WAN without transit network 9, 37
Wildcard 87

WINS 13