IP

1 IP Menu

The *IP* menu is described below.

```
X2302w Setup Tool                         Bintec Access Networks GmbH
[IP]: IP Configuration                                      MyGateway

          Routing
          Static Settings
          Network Address Translation

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

          EXIT

```

The *IP* main menu provides access to the submenus:

■ *ROUTING*

■ *STATIC SETTINGS*

■ *NETWORK ADDRESS TRANSLATION*

■ *BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)*

■ *IP ADDRESS POOL WAN (PPP)*

■ *IP ADDRESS POOL LAN (DHCP)*

■ *SNMP*

■ *REMOTE AUTHENTICATION (RADIUS/TACACS+)*

■ *DNS*

■ *DYNDNS*

■ *ROUTING PROTOCOLS*

1 IP Menu

2 Routing Submenu

The *ROUTING* submenu is described below.

The *IP* ➜ *ROUTING* menu contains a list of all your gateway's IP routes.

FLAGS show the current status (*Up*, *Dormant*, *Blocked*) and the type of route (*Gateway Route*, *Interface Route*, *Subnet Route*, *Host Route*, *Extended Route*). The protocol with which your gateway has "learned" the routing entry is shown under *PRO*, e.g. *LOC* = local, i.e. configured manually.

```
X2302w Setup Tool                        Bintec Access Networks GmbH
[IP][ROUTING]: IP Routing                                  MyGateway


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

Destination     Gateway       Mask           Flags Met Interface Pro
192.168.0.0   192.168.0.254 255.255.255.0 US   0   en0-1     loc
192.168.1.0   192.168.100.2 255.255.255.0 DG   1   branch    loc
192.168.100.2 192.268.100.1 255.255.255.0 DH   1   branch    loc



    ADD               ADDEXT            DELETE            EXIT


```

You can add a new route with *ADD* or edit an existing entry by tagging it with the cursor and pressing *ENTER*. The following menu opens:

```
X2302w Setup Tool                        Bintec Access Networks GmbH
[IP][ROUTING][ADD]                                          MyGateway

    Route Type                  Host route
    Network                     LAN

    Destination IP Address


    Gateway IP Address
    Metric                      1



                    SAVE                            CANCEL

```

The **ROUTING** ➜ **ADD/EDIT** menu consists of the following fields:

Field	Description
Route Type	Type of route. Possible values: ■ *Host route* (default value): Route to a single host. ■ *Network route*: Route to a network. ■ *Default route*: This route is valid for all IP addresses and is only used if no other suitable route is available.
Network	Defines the type of connection (LAN, WAN). For possible values see table "Network selection options," on page 7.
Destination IP Address	Only if *ROUTE TYPE Host route* or *Network route*. IP address of the destination host or network.
Netmask	Only if *ROUTE TYPE* = *Network route*. Netmask for *DESTINATION IP ADDRESS*. If no entry is made, the gateway uses a default netmask.

Field	Description
Partner / Interface	WAN partner or interface (only if **NETWORK** = *WAN without transit network*).
Gateway IP Address	Only for **NETWORK** = *LAN* or *WAN with transit network*. IP address of the host to which your gateway should forward the IP packets.
Metric	The lower the value, the higher the priority of the route (possible values *0...15*; default value is *0*).

Table 2-1:   **ROUTING** ➜ **ADD/EDIT** menu fields

NETWORK offers the following selection options:

Description	Meaning
LAN	Route to a destination host or network that can be reached via your gateway's LAN connection.
WAN without transit network	Route to a destination host or network that can be reached via a WAN partner without including any transit network available.
WAN with transit network	Route to a destination host or network that can be reached via a WAN partner including any transit network available.
Refuse	Your gateway discards data packets using this route and sends a message to the sender saying the destination of the packet is unreachable.
Ignore	Your gateway discards data packets using this route without sending a message to the sender.

Table 2-2:   **NETWORK** selection options

In addition to the normal routing table, the gateway can also make routing decisions based on an Extended Routing Table. Apart from the source and destina-

tion address, the gateway can also include the protocol, source and destination port, type of service (TOS) and the status of the gateway interface in the decision.

Note

Entries in the Extended Routing Table are treated preferentially compared with entries in the normal routing table.

The configuration is set up in the *IP* ➜ *ROUTING* ➜ *ADDEXT* menu.

```
X2302w Setup Tool                      Bintec Access Networks GmbH
[IP][ROUTING][ADD]: IP Routing - Extended Route            MyGateway

  Route Type                 Host route
  Network                    LAN

  Destination IP Address


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



           SAVE                              CANCEL

```

This menu shows the following fields in addition to the fields of the *ROUTING* ➜ *ADD/EDIT* menu:

Field	Description
Mode	Only for *NETWORK* = *WAN without transit network*.
	Defines when the interface selected under *PARTNER / INTERFACE* is to be used. For possible values see table "Mode selection options," on page 10.

Field	Description
Source Interface	Interface over which the data packets reach the gateway. Default value is *don't verify*.
Source IP Address	Address of the source host or network.
Source Mask	Netmask for *SOURCE IP ADDRESS*.
Type of Service (TOS)	Possible values: 0..255 in binary format.
TOS Mask	Bit mask for *TYPE OF SERVICE (TOS)*.
Protocol	Defines a protocol. Possible values: *don't verify*, *icmp*, *ggp, tcp*, *egp*, *pup*, *udp*, *hmp*, *xns*, *rdp*, *rsvp*, *gre*, *esp*, *ah*, *igrp*, *ospf*, *l2tp*. Default value is *don't verify*.
Source Port	Only if *PROTOCOL* = *tcp* or *udp*. Source port number or range of source port numbers (see table "Selection options of Source Port and Destination Port," on page 10).
Destination Port	Only if *PROTOCOL* = *tcp* or *udp*. Destination port number or range of destination port numbers (see table "Selection options of Source Port and Destination Port," on page 10).

Table 2-3: *ROUTING* ➜ *ADDEXT* menu fields

MODE offers the following selection options:

Description	Meaning
always (default value)	Always use the route.
dialup wait	Route can be used if the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up".

Description	Meaning
dialup continue	Route can be used if the interface is "up". If the interface is "dormant", then select and use the alternative route (rerouting) until the interface is "up".
up only	Route can be used if the interface is "up".

Table 2-4:   *MODE* selection options

SOURCE PORT and *DESTINATION PORT* offer the following selection options:

Description	Meaning
any (default value)	The route is valid for all ➤➤ **port** numbers.
specify	Enables the entry of a port number.
specify range	Enables the entry of a range of port numbers.
priv (0...1023)	Privileged port numbers: 0 ... 1023.
server (5000....32767)	Server port numbers: 5000 ... 32767.
clients 1 (1024....4999)	Client port numbers: 1024 ... 4999.
clients 2 (32768....65535)	Client port numbers: 32768 ... 65535.
unpriv (1024...65535)	Unprivileged port numbers: 1024 ... 65535.

Table 2-5:   Selection options of *SOURCE PORT AND DESTINATION PORT*

3 Static Settings Submenu

The *STATIC SETTINGS* submenu is described below.

```
X2302w Setup Tool                              Bintec Access Networks GmbH
[IP][STATIC]: IP Static Settings                                 MyGateway

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


     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

```

The *IP* ➜ *STATIC SETTINGS* menu is for configuring the general IP settings for your gateway.

The *IP* ➜ *STATIC SETTINGS* menu consists of the following fields:

Field	Description
Domain Name	Default Domain Name of Gateway.
Primary Domain Name Server	IP address of a global Domain Name Server (DNS).
Secondary Domain Name Server	IP address of an alternative global Domain Name Server.
Primary WINS	IP address of a global Windows Internet Name Server (=WINS) or NetBIOS Name Server (=NBNS).
Secondary WINS	IP address of an alternative global WINS or NBNS.

Field	Description
Remote TRACE Server TCP Port	TCP port number for remote traces. The default value is *7000*. Deactivate with *0*.
RIP UDP Port	UDP port number for ➤➤ **RIP** (Routing Information Protocol). The default value is *520*. Deactivate with *0*.
Primary BOOTP Relay Server	Here you can enter the IP address of a server to which BootP or DHCP requests are forwarded.
Secondary BOOTP Relay Server	Here you can enter the IP address of an alternative BootP or DHCP server.
Unique Source IP Address	Here you can enter an IP address that is used by the gateway as source address for locally generated IP packets. This should only be configured in special cases.
HTTP TCP Port	Here you enter the TCP port for accessing the HTTP service of the gateway (HTML start page). The default value is *80*.

Table 3-1:   *STATIC SETTINGS* menu fields

4 Network Address Translation Sub-menu

The *IP* ➜ *NETWORK ADDRESS TRANSLATION* menu is described below.

Network Address Translation (➤➤ **NAT**) is a feature of your gateway for defined conversion of source and destination addresses of IP packets (in *SESSIONS REQUESTED FROM INSIDE* and *SESSIONS REQUESTED FROM OUTSIDE*). If NAT is activated, IP connections are still only allowed as standard in one direction, outgoing (forward) (= protective function). Exceptions to the rules can be configured (in *SESSIONS REQUESTED FROM OUTSIDE*).

The *IP* ➜ *NETWORK ADDRESS TRANSLATION* menu shows a list of all interfaces of your gateway.

To edit an entry, tag the interface for which you wish to configure NAT with the cursor and press **Return**. The following menu opens:

```
X2302w Setup Tool                      Bintec Access Networks GmbH
[IP][NAT][EDIT]: NAT Configuration (Internet)            MyGateway


 Network Address Translation          off
 Silent Deny                          no
 PPTP Passthrough                     no

 Enter configuration for sessions:    requested from OUTSIDE
                                      requested from INSIDE




              SAVE                          CANCEL

```

The ***NETWORK ADDRESS TRANSLATION*** ➜ ***EDIT*** menu consists of the following fields:

Field	Description
Network Address Transla- tion	Defines the type of NAT for the selected inter- face. Possible values: ■ *off* (default value): Do not execute NAT. ■ *on*: Execute Forward NAT. ■ *reverse*: Execute Reverse NAT.
Silent Deny	Defines whether the sender of an IP packet denied by NAT is to be informed of the denial. Possible values: ■ *no* (default value): Sender is informed by a relevant ICMP message. ■ *yes*: The sender is not informed.
PPTP Passthrough	PPTP Passthrough allows setting up and oper- ation of several simultaneous outgoing PPTP connections of hosts in the network even if NAT is activated. Possible values: *yes* or *no*. If ***PPTP PASSTHROUGH*** = *yes*, the gateway itself cannot be configured as a tunnel endpoint.

Table 4-1:   ***NETWORK ADDRESS TRANSLATION*** menu fields

4.1   Requested from OUTSIDE/INSIDE Sub- menu

The *REQUESTED FROM OUTSIDE/INDSIDE* menu is described below.

For other NAT settings, the ***IP*** ➜ ***NETWORK ADDRESS TRANSLATION*** ➜ ***EDIT*** menu contains two submenus (the possible settings of the two menus differ only slightly):

- *IP* ➜ *NETWORK ADDRESS TRANSLATION* ➜ *EDIT* ➜ *REQUESTED FROM OUTSIDE*
  In this menu you can allow certain incoming IP connections.

- *IP* ➜ *NETWORK ADDRESS TRANSLATION* ➜ *EDIT* ➜ *REQUESTED FROM INSIDE*
  In this menu you can map the source IP addresses and ports for certain out-going IP connections (= address mapping).

Both menus show a list of the address mappings already configured. The ab-breviations used are explained above the list.

```
X2302w Setup Tool                      Bintec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT - sessions from           MyGateway
                               OUTSIDE (Internet)

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


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




    ADD                  DELETE                      EXIT

```

Add an entry with *ADD* or edit an existing entry by tagging it with the cursor and pressing **Return**. The following menu opens:

```
X2302w Setup Tool                          Bintec Access Networks 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

```

The *REQUESTED FROM OUTSIDE/INSIDE* ➜ *ADD/EDIT* menu consists of the following fields:

Field	Description
Service	*REQUESTED FROM OUTSIDE* ➜ *ADD/EDIT*: Service for which incoming connections are allowed.
	REQUESTED FROM INSIDE ➜ *ADD/EDIT*: Service for which address mapping is defined for outgoing connections.
	Possible values:
	ftp, telnet, smtp, domain/udp, domain/tcp, http, nntp, user defined (for other services, default value)
Protocol	Only for *SERVICE* = *user defined*. Defines the protocol.
	Possible values:
	icmp, tcp, udp, gre, esp, ah, l2tp,any

Field	Description
Remote Address	Optional.
	IP address of a host or network at the remote end.
	Enable or address mapping applies only to packets of this host or network.
Remote Mask	Netmask for **REMOTE ADDRESS**.
Remote Port Port...to Port	Only in **REQUESTED FROM INSIDE → ADD/EDIT** menu.
	Only for **SERVICE** = *user defined*.
	Entry of destination port or port range for outgoing IP connections for which address mapping is to be used.
	Possible values:
	■ *any*
	■ *specify*: Enables the entry of a port number.
	■ *specify range*: Enables the entry of a port number range *.*
External Address	External host or network IP address at the selected interface.
External Mask	Netmask for **EXTERNAL ADDRESS**.
	If you use external and internal network IP addresses, the values for **EXTERNAL MASK** and **INTERNAL MASK** must be identical.

Field	Description
External Port Port...to Port	Only for **SERVICE** = *user defined*. ■ **REQUESTED FROM OUTSIDE ➜ ADD/EDIT**: Only for **SERVICE** = *user defined*; original destination port of incoming IP connection. ■ **REQUESTED FROM INSIDE ➜ ADD/EDIT:** The newly set source port of the outgoing IP connection. Possible values: ■ *any* (default value): For **REQUESTED FROM INSIDE ➜ ADD/EDIT**; this means no port mapping. ■ *specify*: Enables the entry of a port number. ■ *specify range* (only for **REQUESTED FROM OUTSIDE ➜ ADD/EDIT**) Enables the entry of a port number range.
Internal Address	IP address of the internal host or network.
Internal Mask	Netmask for **INTERNAL ADDRESS**. If you use external and internal network IP addresses, the values for **EXTERNAL MASK** and **INTERNAL MASK** must be identical.

Field	Description
Internal Port Port	■ *REQUESTED FROM OUTSIDE* ➜*ADD/EDIT*: Newly set destination port of the incoming IP connection. ■ *REQUESTED FROM INSIDE* ➜ *ADD/EDIT:* Original source port of the outgoing IP connection. Possible values: ■ *any* (default value): For *REQUESTED FROM OUTSIDE* ➜ *ADD/EDIT*; this means no port mapping. ■ *specify*: Enables the entry of a port number.

Table 4-2: *REQUESTED FROM OUTSIDE/INSIDE* menu fields

4 Network Address Translation Submenu

5 Bandwidth Management (Load Balancing / BOD) Submenu

The *BANDWIDTH MANAGEMENT (LOAD BALANCING/ BOD)* menu is described below.

```
X2302w Setup Tool                    Bintec Access Networks GmbH
[IP][BW]: Bandwidth Management for IP                    MyGateway



          IP Load Balancing over Multiple Interfaces






          EXIT

```

The *BANDWIDTH MANAGEMENT (LOAD BALANCING / BOD)* menu provides access to the submenu:

■ *IP LOAD BALANCING OVER MULTIPLE INTERFACES*

5.1 IP Load Balancing over Multiple Interfaces Submenu

The *IP LOAD BALANCING OVER MULTIPLE INTERFACES* menu is described below.

The increasing amount of data traffic over the Internet necessitates the possibility of being able to send data over different interfaces to increase the total bandwidth available. IP load balancing enables the distribution of data traffic within a certain group of interfaces to be controlled.

The configuration is set in the *IP* ➜ *BANDWIDTH MANAGEMENT (LOAD BALANCING/BOD)* ➜ *IP LOAD BALANCING OVER MULTIPLE INTERFACES* menu.

The menu shows a list of the interface groups already configured for load balancing.

Access to the menu for configuring the groups is via *ADD/EDIT*.

```
X2302w Setup Tool                         Bintec Access Networks GmbH
[IP][IP LOAD BALANCING][ADD]                                MyGateway


   Description
   Interface Group ID    0

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

   Interface 1                              none

   Interface 2                              none

   Interface 3                              none

              SAVE               CANCEL

```

The menu contains the following fields:

Field	Description
Description	Here you enter the desired description of the interface group.
Interface Group ID	The ID of the interface group. This is assigned by the system automatically, but can also be edited. It is used only for internal assignment of the group. The default value is *0*.
Distribution Policy	Here you select in what way the data traffic is distributed to the interfaces configured for the group. Possible values: see "Distribution Policy selection options" on page 25

Field	Description
Distribution Mode	Here you select the state the interfaces in the group may have if they are to be included in load balancing. Possible settings: ■ *always (use operational up and dormant interfaces)*: Interfaces that are either up or dormant are included (default value). ■ *up-only (operational up interfaces only):* Only interfaces that are up are included.
Distribution Ratio	Not for **DISTRIBUTION POLICY** = *service/source-based routing*. Here you select whether the percentage share of data traffic is to be the same for all interfaces of the group or configured individually for each interface. Possible settings: ■ *equal for all interfaces of the group* (default value): All interfaces are automatically assigned the same share. ■ *individual for all interfaces of the group*: Each interface can be assigned a share individually.
Interface 1 - 3	Here you select the interfaces that are to belong to the group from the available interfaces.

Field	Description
Distribution Fraction (in percent)	Not for **DISTRIBUTION POLICY** = *service*/*source-based routing*. Appears only for **INTERFACE 1 - 3** if an interface has been selected. Here you enter the percentage of the data traffic to be assigned to an interface. The meaning differs according to the **DISTRIBUTION POLICY** used: ■ based on the number of sessions to be distributed for *session round-robin*. ■ based on the data rate for *bandwidth load-/upload-/download-dependent*.

Table 5-1:   **IP LOAD BALANCING OVER MULTIPLE INTERFACES** menu fields

DISTRIBUTION POLICY offers the following selection options:

Field	Description
session round-robin	A newly added session is assigned to one of the group interfaces according to the percentage assignment of sessions to the interfaces. The number of sessions is decisive.
bandwidth load-dependent	A newly added session is assigned to one of the group interfaces according to the share of the total data rate handled by the interfaces. Decisive is the current data rate based on the data traffic in both the send and receive direction.
bandwidth download-dependent	A newly added session is assigned to one of the group interfaces according to the share of the total data rate handled by the interfaces. Decisive is the current data rate based on the data traffic in the receive direction only.

Field	Description
bandwidth upload-dependent	A newly added session is assigned to one of the group interfaces according to the share of the total data rate handled by the interfaces. Decisive is the current data rate based on the data traffic in the send direction only.
service/source-based routing	A newly added session is assigned to one of the group interfaces according to the configuration of the static routing in the *IP LOAD BALANCING OVER MULTIPLE INTERFACES* ➜ *ADD/EDIT* ➜ *IP ROUTING LIST* menu. This menu is only accessible if you have selected s*ervice/source-based routing*. see "IP Routing List Submenu" on page 25

Table 5-2: *DISTRIBUTION POLICY* selection options

5.1.1 IP Routing List Submenu

The *IP ROUTING LIST* menu only appears if an interface has been selected in *DISTRIBUTION POLICY* service/source-based routing and *INTERFACE 1 - 3*.

The *IP LOAD BALANCING OVER MULTIPLE INTERFACES* ➜ *ADD/EDIT* ➜ *IP ROUTING LIST* menu contains a list of all configured routing entries. The configuration is set in *IP ROUTING LIST* ➜ *ADD/EDIT*.

```
X2302w Setup Tool                        Bintec Access Networks GmbH
[IP][ROUTING][ADD]: Configure Service/Source-Based Routing   MyGateway


  Interface                    Internet1

  Type                         Host route
  Network                      WAN without transit network

  Destination IP Address

  Gateway IP Address

  Source IP Address
  Source Mask

  Protocol                     tcp
  Service                      unlisted service     Port  -1


              SAVE                              CANCEL

```

The menu contains the following fields:

Field	Description
Interface	Shows the interface to be edited. This field cannot be changed.
Type	Type of route. Possible values: ■ *Host route*: Route to a single host ■ *Network route* (default value): Route to a network ■ *Default route*: The route is valid for all IP addresses and is only used if no other suitable route is available
Network	Defines the type of connection (LAN, WAN). For possible values see table "Network selection options," on page 28.
Destination IP Address	Only if **ROUTE TYPE** *Host route* or *Network route*. IP address of the destination host or network.

Field	Description
Destination Mask	Only if *ROUTE TYPE* = *Network route*
	Netmask for Destination IP Address. If no entry is made, the gateway uses a default netmask.
Gateway IP Address	Only for *NETWORK LAN* or *WAN with transit network*. IP address of the host to which your gateway should forward the IP packets.
Source IP Address	IP address of the source host or network.
Source Mask	Netmask for *SOURCE IP ADDRESS*.
Protocol	Defines a protocol. Possible values: *tcp*, *egp*, *pup*, *udp*, *hmp*, *xns*, *rdp*, *rsvp*, *gre*, *esp*, *ah*, *igrp*, *ospf*, *l2tp*, *don't verify*, *icmp*, *ggp*.
	The default value is *don't verify*.
Service	Here you select a predefined service for whose data traffic the entry is to apply.
	The value *unlisted service* is shown when accessing the menu. This is only a bookmark. The data traffic is not filtered by this entry as long as the default value *-1* is left in the *PORT* field.
Port	Can only be edited if *PROTOCOL* = *tcp* or *udp* and *SERVICE* = *unlisted service*.
	Entry of destination port for *PROTOCOL* *tcp* or *udp*.
	Possible settings are values from *-1* to *65535*. The default value *-1* means the destination port can be any port.

Table 5-3:   *IP ROUTING LIST* ➜ *ADD/EDIT* menu fields

NETWORK contains the following selection options (depending on type of interface):

Description	Meaning
LAN	Route to a destination host or network that can be reached via your gateway's LAN connection.
WAN without transit network	Route to a destination host or network that can be reached via a WAN partner without including any transit network available.
WAN with transit network	Route to a destination host or network that can be reached via a WAN partner including any transit network available.

Table 5-4: **NETWORK** selection options

6   IP Address Pool WAN (PPP) Sub-menu

The *IP ADDRESS POOL WAN (PPP)* menu is described below.

The *IP ➜ IP ADDRESS POOL WAN (PPP)* menu is for setting up a pool of IP addresses that your gateway as dynamic IP address server can assign to WAN partners to enable them to dial in.

All the configured IP address pools are listed here. The configuration is set up in the *IP ADDRESS POOL WAN (PPP) ➜ ADD/EDIT* menu.

```
X2302w Setup Tool                        Bintec Access Networks GmbH
[IP][DYNAMIC][EDIT]                                        MyGateway


 Pool ID                                 0
 IP Address                              192.168.0.11
 Number of Consecutive Addresses         2




          SAVE                                CANCEL

```

The menu contains the following fields:

Field	Description
Pool ID	Unique number for identifying an IP address pool.
IP Address	First IP address in the range.
Number of Consecutive Addresses	Number of IP addresses in the range, including the first IP address. The default value is *1*.

Table 6-1:   *IP ADDRESS POOL WAN (PPP)* menu fields

7 IP Address Pool LAN (DHCP) Sub-menu

The *IP ADDRESS POOL LAN (DHCP)* menu is described below.

IP ➜ *IP ADDRESS POOL LAN (DHCP)* is used for configuring the gateway as ➤➤ **DHCP** server (Dynamic Host Configuration Protocol).

All the configured interfaces and relevant IP address pools are listed here. The configuration is set up in the *IP ADDRESS POOL LAN (DHCP)* ➜ *ADD/EDIT* menu.

```
X2302w Setup Tool                          Bintec Access Networks GmbH
[IP][DHCP][ADD]: Define Range of IP Addresses               MyGateway


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


  Gateway
  NetBT Node Type                        not specified




        SAVE                             CANCEL

```

The menu contains the following fields:

Field	Description
Interface	Interface to which the address pool is assigned. When a DHCP request is received over *INTERFACE*, one of the addresses from the address pool is assigned.
IP Address	First IP address in the address pool.

Field	Description
Number of Consecutive Addresses	Total number of IP addresses in the address pool, including the first IP address (*IP ADDRESS*). The default value is *1*.
Lease Time (Minutes)	Defines the length of time an address from the pool is assigned to a host. After the *LEASE TIME (MINUTES)* expires, the address can be reassigned. The default value is *1*20.
MAC Address	Only for *NUMBER OF CONSECUTIVE ADDRESSES* = *1* *IP ADDRESS* is only assigned to the device with *MAC ADDRESS*.
Gateway	Defines which IP address is transferred to the DHCP client as gateway. If no IP address is entered here, the IP address defined in *INTERFACE* is transferred.
NetBT Node Type	Defines how and in which order the host carries out resolution of NetBIOS names to IP addresses. Possible values: ■ *not specified* (default value) ■ *Broadcast Node* ■ *Point-to-Point Node* ■ *Mixed Node* ■ *Hybrid Node*

Table 7-1:   *IP ADDRESS POOL LAN (DHCP)* menu fields

8 SNMP Submenu

The *SNMP* menu is described below.

```
X2302w Setup Tool                          Bintec Access Networks GmbH
[IP][SNMP]: SNMP Configuration                               MyGateway


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




        SAVE                            CANCEL

```

IP ➜ *SNMP* is for changing the basic ➤➤ **SNMP** settings.

The *SNMP* menu contains the following fields:

Field	Description
SNMP listen UDP port	Here you enter the number of the udp port on which the gateway accepts SNMP requests. The default value is *161*. *0* deactivates the feature.
SNMP trap UDP port	Here you enter the number of the udp port to which the gateway sends SNMP traps. The default value is *162*. *0* deactivates the feature.
SNMP trap broadcasting	For activating SNMP trap broadcasting. The gateway then sends SNMP traps to the broadcast address of the LAN. Possible values are *on* and *off* (default value).

Field	Description
SNMP trap community	Here you can enter an SNMP ID. This must be sent by the SNMP Manager with every SNMP request so that this is accepted by your gateway. The default value is *snmp-Trap*.

Table 8-1: **SNMP** menu fields

9   Remote Authentication (RADIUS/TACACS+) Submenu

The *REMOTE AUTHENTICATION (RADIUS/TACACS+)* menu is described below.

The *IP ➜ REMOTE AUTHENTICATION (RADIUS/TACACS+)* menu offers access to the following submenus:

■   *RADIUS AUTHENTICATION AND ACCOUNTING*

■   *TACACS+ AUTHENTICATION AND AUTHORIZATION*

9.1   RADIUS Authentication and Accounting Submenu

The *RADIUS SERVER* menu is described below.

Client / Server   RADIUS (Remote Authentication Dial In User Service) is a service that enables authentication and configuration information to be exchanged between your gateway and a RADIUS server. The RADIUS server administrates a database with information about user authentication and configuration and for statistical recording of connection data.

RADIUS can be used for:

■   authentication

■   accounting

■   exchanging configuration data.

For an incoming connection, the Bintec gateway sends a request with user name and password to the RADIUS server, which then searches its database. If the user is found and can be authenticated, the RADIUS server sends corresponding confirmation to the gateway. This confirmation also contains parameters (called RADIUS attributes), which the gateway uses as WAN connection parameters.

If the RADIUS server is used for accounting, the gateway sends an accounting message at the start of the connection and a message at the end of the connection. These start and end messages also contain statistical information about the connection (IP address, user name, throughput, costs).

RADIUS packets The following types of packets are sent between the RADIUS server and Bintec gateway (client):

Type	Purpose
ACCESS_REQUEST	Client –> Server
	If an access request is received by the gateway, a request is sent to the RADIUS server if no corresponding WAN partner has been found in the gateway.
ACCESS_ACCEPT	Server –> Client
	If the RADIUS server has authenticated the information contained in the ACCESS_REQUEST, it sends an ACCESS_ACCEPT to the gateway together with the parameters used for setting up the connection.
ACCESS_REJECT	Server –> Client
	If the information contained in the ACCESS_REQUEST does not correspond to the information in the user database of the RADIUS server, it sends an ACCESS_REJECT to reject the connection.
ACCOUNTING_START	Client -> Server
	If a RADIUS server is used for accounting, the gateway sends an accounting message to the RADIUS server at the start of each connection.
ACCOUNTING_STOP	Client -> Server
	If a RADIUS server is used for accounting, the gateway sends an accounting message to the RADIUS server at the end of each connection.

All the RADIUS servers currently configured are listed in the *IP* ➜ *RADIUS SERVER* menu.

The configuration is set up in *IP* ➜ *RADIUS SERVER* ➜ *ADD/EDIT*.

```
X2302w Setup Tool                      Bintec Access Networks GmbH
[IP][RADIUS][ADD]                                        MyGateway

Protocol                 authentication

IP Address
Password

Priority                 0
Policy                   authoritative

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

          SAVE                            CANCEL

```

The menu contains the following fields:

Field	Description
Protocol	Defines whether the RADIUS server is used for authentication purposes or accounting. Possible values: ■ *authentication* (default value) - The RADIUS server is used for controlling access to a network. ■ *accounting* - The RADIUS server is used for recording statistical connection data. ■ *shell login* - The RADIUS server is used for controlling access to the SNMP shell of the gateway. ■ *IPSec* - The RADIUS server is used for sending configuration data for IPSec peers to the gateway. ■ *802.1x* - The RADIUS server is used for controlling access to a WLAN.
IP Address	The IP address of the RADIUS server.
Password	This is the common password used for communication between the RADIUS server and gateway.
Priority	Priority of the RADIUS server. If a number of RADIUS server entries exist, the server with the highest priority is used first. If this server does not answer, the server with the next lower priority is used. Possible values: Whole numbers from *0* (highest priority) to *7* (lowest priority). The default value is *0*.

Field	Description
Policy	Defines how the Bintec gateway responds if a negative answer is received to a request. Possible values: ■ *authoritative* (default value): A negative answer to a request is accepted. ■ *non authoritative*: A negative answer to a request is not accepted. A request is sent to the next RADIUS server until the gateway receives an answer from a server configured as authoritative.
Port	TCP port used for RADIUS data. RFC 2138 defines the default ports as 1812 for authentication (1645 in older RFCs) and 1813 for accounting (1645 in older RFCs). You can obtain the port to be used from the documentation for your RADIUS server. The default value is *1812*.
Timeout (ms)	Maximum waiting time in milliseconds between the ACCESS_REQUEST and answer. After timeout, the request is repeated according to *RETRIES* or the next configured RADIUS server is requested. Possible values: Whole numbers between *50* and *50000*. The default value is *1000* (1 second).

Field	Description
Retries	Number of repetitions if a request is not answered. If an answer is still not received after these retries, **STATE** is set to *inactive*. The gateway then tries to reach the server every 20 seconds; if the server answers, **STATE** is set to *active* again. Possible values: Whole numbers between *0* and *10*. The default value is *1*. To prevent **STATE** being set to *inactive*, set this value to *0*.
State	State of the RADIUS server. Possible values: ■ *active* (default value): Server answers requests. ■ *inactive*: Server does not answer (see **RETRIES**). ■ *disabled*: Requests to a certain RADIUS server are temporarily deactivated.
Validate	Possible values: ■ *enabled* (default value): The gateway checks the identity of the RADIUS server using the MD5 checksum from **PASSWORD**. This option should be activated for security purposes. ■ *disabled*: This option should only be selected in special cases.

Field	Description
Dialout	Here you can define whether the gateway receives requests from RADIUS server dialout routes. This enables temporary interfaces to be configured automatically and the gateway can initiate outgoing connections that are not configured permanently. Possible values: *enabled*, *disabled* (default value).
Alive Check (if inactive)	Here you can activate a check of the reachability of a RADIUS server in *STATE inactive*. ■ *enabled* (default value): An Alive Check is carried out regularly (every 20 seconds) by sending an ACCESS_REQUEST to the IP address of the RADIUS server. If the server is reachable, *STATE* is set to *active* again. If the RADIUS server is only reachable over a dialup connection, this can cause additional costs if the server is *inactive* for a long time. ■ *disabled*: Alive Check is not carried out.

Table 9-1:   *RADIUS SERVER* menu fields

9.2   TACACS+ Authentication and Authorization Submenu

The *TACACS+ AUTHENTICATION AND AUTHORIZATION* menu is described below.

The TACACS+ protocol provides access control for gateways, network access servers and other network devices via one or more centralized servers. TACACS+ provides authentication, authorization and accounting services.

Configuration of a TACACS+ server is carried out in the ***IP*** ➜ ***REMOTE AUTHENTICATION (RADIUS/TACACS+)*** ➜ ***TACACS+ AUTHENTICATION AND AUTHORIZATION*** ➜ ***ADD/EDIT*** menu.

```
X2302w Setup Tool                          Bintec Access Networks GmbH
[IP][TACACS+][ADD]                                           MyGateway


 Server's IP Address or Hostname

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

  Timeout (seconds)                        3
  Block Time (seconds)                     60

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

          SAVE                                  CANCEL

```

It contains the following configuration options:

Field	Description
Server's IP Address or Hostname	Here you enter the IP address of the TACACS+ server that is to be queried for AAA (Authentication, Authorization, Accounting) request.
Priority	Here you assign a priority to the current TACACS+ server.
	The server with the lowest value is the first one used for a TACACS+ AAA request. If there is no response or the access was denied (in the non-authoritative case only, see also field ***POLICY***), the entry with the next lowest priority will be used.
	Available values are *0* to *9*, the default value is *0*.

Field	Description
TCP Port	Here the default TCP port used for the TACACS+ protocol is set to *49*. The value cannot be changed.
TACACS+ Key (Secret)	Here you enter the password used to authenticate and (if applicable) encrypt the data exchange between the TACACS+ server and the Network Access Server (your gateway).
	The maximum length of the entry is 32 characters.
Policy	Here you can choose the interpretation of the TACACS+ reply. Available values are *authoritative* and *non authoritative*.
	If set to *authoritative*, a negative answer to a request is accepted. This is not necessarily true when set to *non authoritative* (default value). In this case, the next TACACS+ server is queried until there is an authoritative reply.
	If **POLICY** is set to *non authoritative* and none of the servers delivers a positive reply, or if none of the servers can be reached, the locally configured SNMP communities are checked for relevant access information.
Encryption (recommended)	Here you can choose whether the data exchange between the TACACS+ server and the NAS is encrypted. Available values are *enabled* (default value) and *disabled*.
	If set to *enabled,* the TACACS+ packets are MD5 encrypted. Otherwise - if set to *disabled* - the packets and therefore all related information are sent unencrypted. Unencrypted transfer is not recommended for standard usage.

Field	Description
Timeout (seconds)	Here you enter the time the NAS waits for a TACACS+ response. If no reply is received during waiting time, the next configured TACACS+ server is queried and the current server is set into a *blocked* state (*TACACSPSERVEROPERSTATUS* = *blocked*). Available values are *1* to *60*, the default value is *3*.
Block Time (seconds)	Here you enter the amount of time for which the current server is set to a blocked state. After the Block Time has ended, the server is set to the state specified for the field *ADMINISTRATIVE STATUS* (see below). Available values are *0* to *3600*, the default value is *60*. A value of *0* means that the server is never set to a *blocked* state.
PPP Authentication	This function is not supported by **XGeneration**. It may be included in a later version of our system software.
Login Authentication/Authorization	Here you can choose whether to use the current TACACS+ server for login authentication to a gateway. Available choices are *enabled* (default value) and *disabled*.
TACACS+ Accounting	This function is not supported by **XGeneration**. It may be included in a later version of our system software.

Field	Description
Administrative Status	Here you can choose the status the server is to be put in: If set to *up* the associated server is used for authentication, authorization and accounting according to the priority (see field *PRIORITY*) and the current operational status. Otherwise this entry will not be considered for TACACS+ AAA requests. Available choices are *up* (default value) and *down*.
TACACS+ Single-Con-nection	Here you can choose if multiple TACACS+ ses-sions (subsequent TACACS+ requests) may be supported simultaneously over a single TCP connection. If multiple sessions are not being multiplexed over a single TCP connection, a new connection will be opened for each TACACS+ session and closed at the end of that session. Available choices are *multiple requests* and *single request* (*single request* is the default value and is recommended for most applica-tions).

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

9 Remote Authentication (RADIUS/TACACS+) Submenu

10   DNS Submenu

The *DNS* menu is described below.

```
X2302w Setup Tool                        Bintec Access Networks GmbH
[IP][DNS]: IP Configuration - Nameservice                  MyGateway


   Positive Cache                  enabled
   Negative Cache                  enabled

   Overwrite Global Nameservers    yes
   Default Interface               none

   DHCP Assignment                 self
   IPCP Assignment                 global

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

   Advanced Settings...            Global Statistics...


            SAVE                            CANCEL

```

Name Resolution with the Gateway

The gateway offers the following options for name resolution:

■ DNS proxy function, for forwarding DNS requests sent to the gateway to a suitable DNS server. This also includes specific forwarding of certain domains (Forwarded Domains).

■ DNS cache, for saving the positive and negative results of DNS requests.

■ Static entries (Static Hosts), for manually defining or preventing assignments of IP addresses to names.

■ DNS monitoring, for providing an overview of DNS requests in the gateway.

Global Name Server

The IP addresses of global name servers that are asked if the gateway cannot answer requests itself or by forwarding entries are entered in *IP* ➜ *STATIC SETTINGS*.

For local applications, the IP address of the gateway itself or the general loop-back address (127.0.0.1) can be entered as global name server.

The gateway can also receive the addresses of the global name servers dynamically from WAN partners or if necessary transfer these to WAN partners:

Name Resolution Strategy in the Gateway

A DNS request is handled by the gateway as follows:

1. If possible, the request is answered directly from the static or dynamic cache with IP address or negative answer.

2. Otherwise, if a suitable forwarding entry exists, the relevant DNS server is asked, if necessary by setting up a WAN connection at extra cost. If the DNS server can resolve the name, the information is forwarded and a dynamic entry created in the cache.

3. Otherwise, if global name servers are entered, the Primary Domain Name Server then the Secondary Domain Name Server are asked. If the IP address of the gateway or the loopback address is entered for local applications, these are ignored here. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

4. Otherwise, if a WAN partner is selected as default interface, the associated DNS server is asked, if necessary by setting up a WAN connection at extra cost. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

5. Otherwise, if overwriting the addresses of the global name servers is allowed (*OVERWRITE GLOBAL NAMESERVER* = *yes*), a connection is set up – if necessary at extra cost – to the first WAN partner configured to enable DNS server addresses to be requested from DNS servers, if this has not been attempted previously. If name server negotiation is successful, these are entered as global name servers and are therefore available for further requests.

6. Otherwise the initial request is answered with a server error.

If one of the DNS servers answers with "non-existent domain", the initial request is immediately answered accordingly and a corresponding negative entry is made in the DNS cache of the gateway.

The configuration is set up in *IP* ➜ *DNS*.

The menu contains the following fields:

Field	Description
Positive Cache	Activation of the positive dynamic cache. Possible values: ■ *enabled* (default value): Successfully resolved names and IP addresses are saved in the cache. ■ *flush*: All positive dynamic entries in the cache are deleted. ■ *disabled*: Successfully resolved names and IP addresses are not saved in the cache and existing dynamic positive entries are deleted.
Negative Cache	Activation of the negative dynamic cache. Possible values: ■ *enabled* (default value): Requested names for which a DNS server has sent a negative answer are saved as negative entries in the cache. ■ *flush*: All negative dynamic entries in the cache are deleted. ■ *disabled*: Names that could not be resolved are not saved in the cache and existing dynamic negative entries are deleted.

Field	Description
Overwrite Global Nameservers	Defines whether the addresses of the global name servers in the gateway (in *IP* ➜ *STATIC SETTINGS*) may be overwritten with name server addresses sent by WAN partners. Possible values: ■ *yes* (default value) ■ *no*
Default Interface	Defines the WAN partner to which a connection is set up for name server negotiation if other name resolution attempts were not successful. The default value is *none*.
DHCP Assignment	Defines which name server addresses are sent to the DHCP client if the gateway is used as DHCP server. Possible values: ■ *none*: No name server address is sent. ■ *self* (default value): The address of the gateway is sent as name server address. ■ *global*: The addresses of the global name servers entered in the gateway are sent.
IPCP Assignment	Defines which name server addresses are sent by the gateway to a WAN partner in dynamic name server negotiation. Possible values: ■ *none*: No name server address is sent. ■ *self*: The address of the gateway is sent as name server address. ■ *global* (default value): The addresses of the global name servers entered in the gateway are sent.
Static Hosts	The number of static entries is shown in brackets.

Field	Description
Forwarded Domains	The number of forwarding entries is shown in brackets.
Dynamic Cache	The number of positive and negative dynamic entries in the DNS cache is shown in brackets.

Table 10-1:   *DNS* menu fields

This menu provides access to the following submenus:

■   *STATIC HOSTS*

■   *FORWARDED DOMAINS*

■   *DYNAMIC CACHE*

■   *ADVANCED SETTINGS...*

■   *GLOBAL STATISTICS...*

10.1   Static Hosts Submenu

The *IP* ➜ *DNS* ➜ *STATIC HOSTS* submenu is described below.

```
X2302w Setup Tool                      Bintec Access Networks GmbH
[IP][DNS][HOSTS][ADD]                                    MyGateway

 Default Domain:

 Name

 Response     positive

 Address
 TTL          86400



              SAVE                            CANCEL

```

This menu shows a list of Static Hosts already configured. This can be added to or edited in the **STATIC HOSTS → ADD/EDIT** menu.

The menu contains the following fields:

Field	Description
Default Domain	Shows the domain name of the gateway entered in **IP → STATIC SETTINGS**.
Name	Host name, which is assigned the **ADDRESS** with this static entry. Can also start with the wildcard *, e.g. *.funkwerk-ec.com. If an incomplete name is entered without a dot, this is completed with "**. <DEFAULT DOMAIN>.**" after pressing **SAVE**.
Response	Type of static entry. Possible values: ■ *positive* (default value): A DNS request for **NAME** is answered with the associated **ADDRESS**. ■ *ignore*: A DNS request is ignored; no answer is given. ■ *negative*: A DNS request for **NAME** is answered with a negative answer.
Address	Only for **RESPONSE** = *positive* IP address that is assigned to **NAME**.
TTL	Period of validity of the assignment of **NAME** to **ADDRESS** in seconds (only relevant for **RESPONSE** = *positive*), which is sent to requesting hosts. The default value is *86400* (= 24 h).

Table 10-2: **STATIC HOSTS** menu fields

10.2 Forwarded Domains Submenu

The *IP ➜ DNS ➜ FORWARDED DOMAINS* submenu is described below.

```
X2302w Setup Tool                        Bintec Access Networks GmbH
[IP][DNS][FORWARDS][ADD]                                    MyGateway

 Global Nameservers: none, Default Interface: none
 Default Domain:


 Name


 Interface     none


 TTL           86400



           SAVE                              CANCEL

```

This menu shows a list of Forwarded Domains already configured. This can be added to or edited in the *FORWARDED DOMAINS ➜ ADD/EDIT* menu.

The menu contains the following fields:

Field	Description
Global Nameservers	Shows the global name servers entered in *IP ➜ STATIC SETTINGS*.
Default Domain	Shows the domain name of the gateway entered in *IP ➜ STATIC SETTINGS*.
Name	Host name that is to be resolved with this forwarding entry. Can also start with the wildcard *, e.g. *.funkwerk.de. If an incomplete name is entered without a dot, this is completed with "*.<DEFAULT DOMAIN>.*" after pressing **SAVE**.

Field	Description
Interface	Defines the WAN partner to which a connection is to be set up for the resolution of *NAME*. The default value is *none*.
TTL	Substitute value for the TTL value supplied by the DNS server in a positive answer, if this is *0* or exceeds *MAXIMUM TTL FOR POS CACHE ENTRIES*. The TTL value indicates the period of validity of the assignment of the name to the IP address in seconds. The default value is *86400* (= 24 h).

Table 10-3:   *FORWARDED DOMAINS* menu fields

10.3   Dynamic Cache Submenu

The *IP* ➜ *DNS* ➜ *DYNAMIC CACHE* submenu is described below.

```
X2302w Setup Tool                    Bintec Access Networks GmbH
[IP][DNS][DYNAMIC]: Nameservice - Dynamic Cache           MyGateway

 Name                               Address      Resp  TTL    Ref




     DELETE              STATIC              EXIT

```

The **MENU IP ➔ DNS ➔ DYNAMIC CACHE** is used to show the DNS entries learned dynamically by the DNS servers. Here dynamic entries can also be converted to static entries or deleted. The list contains the following columns:

Column	Meaning
Name	Host name to which **ADDRESS** is assigned.
Address	IP address that is assigned to **NAME**.
Resp	Type of dynamic entry. Possible values: ■ *pos* (positive): A DNS request for **NAME** is answered with the associated IP address. ■ *neg* (negative): A DNS request for **NAME** is answered with a negative answer.
TTL	Shows how many seconds the dynamic entry still remains in the cache. The entry is deleted on expiry of **TTL**. When a positive dynamic entry is saved in the cache, the value is taken from the answer from the DNS server. If this value is *0* or exceeds **MAXIMUM TTL FOR POS CACHE ENTRIES**, the value is set to **MAXIMUM TTL FOR POS CACHE ENTRIES**. For a negative dynamic entry, the value is set to **MAXIMUM TTL FOR NEG CACHE ENTRIES**. The display is not updated.
Ref	Shows how often the entry has been called.

Table 10-4: **DYNAMIC CACHE** menu fields

A dynamic entry can be converted to a static entry by tagging the entry with the **Space** bar and confirming with **STATIC**.

The relevant entry then disappears from **IP ➔ DNS ➔ DYNAMIC CACHE** and is listed in **IP ➔ DNS ➔ STATIC HOSTS**. **TTL** is transferred in this operation.

10.4 Advanced Settings Submenu

The *IP* ➜ *DNS* ➜ *ADVANCED SETTINGS* submenu is described below.

```
X2302w Setup Tool                    Bintec Access Networks GmbH
[IP][DNS][ADVANCED]: Nameservice - Advanced Settings      MyGateway


     Maximum Number of DNS Records        100



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



     SAVE                CANCEL
```

The menu contains the following fields:

Field	Description
Maximum Number of DNS Records	Maximum total number of static and dynamic entries.
	Once this value is reached, the dynamic entry not requested for the longest period of time is deleted when a new entry is added.
	If *MAXIMUM NUMBER OF DNS RECORDS* is reduced by the user, dynamic entries are deleted if necessary.
	Static entries are not deleted; *MAXIMUM NUMBER OF DNS RECORDS* cannot be set to a lower value than the current number of existing static entries.
	Possible values: *0 .. 1000*. The default value is *100*.

Field	Description
Maximum TTL for Pos Cache entries	For a positive dynamic entry in the cache this is set to *TTL*, if the TTL field of the DNS record received has the value *0* or exceeds *MAXIMUM TTL FOR POS CACHE ENTRIES*. The default value is *86400*.
Maximum TTL for Neg Cache Entries	Is set to *TTL* for a negative dynamic entry in the cache. The default value is *86400*.

Table 10-5:   *ADVANCED SETTINGS...* menu fields

10.5 Global Statistics Submenu

The *IP* ➜ *DNS* ➜ *GLOBAL STATISTICS* **submenu is described below.**

```
X2302w Setup Tool                       Bintec Access Networks GmbH
[IP][DNS][STATISTICS]: Nameservice - Global Statistics      MyGateway


  Received DNS Packets               0
  Invalid DNS Packets                0

  DNS Requests                       0
  Cache Hits                         0
  Forwarded Requests                 0

  Cache Hitrate (%)                  0

  Successfully Answered Queries      0
  Server Failures                    0



  EXIT


```

Contains the following fields (the menu is updated every second):

Field	Description
Received DNS Packets	Shows the number of received DNS packets addressed direct to the gateway, including the answer packets for forwarded requests.
Invalid DNS Packets	Shows the number of invalid DNS packets received and addressed direct to the gateway.
DNS Requests	Shows the number of valid DNS requests received and addressed direct to the gateway.
Cache Hits	Shows the number of requests that were answered with static or dynamic entries from the cache.
Forwarded Requests	Shows the number of requests forwarded to other name servers.
Cache Hitrate (%)	Shows the number of *CACHE HITS* per *DNS REQUEST* in %.
Successfully Answered Queries	Shows the number of successfully answered requests (positive and negative).
Server Failures	Shows the number of requests that were not answered by any name server (either positively or negatively).

Table 10-6:   *GLOBAL STATISTICS...* menu fields

11 DynDNS Submenu

The *DYNDNS* menu is described below.

The use of dynamic IP addresses has the disadvantage that a host in the network can no longer be found once its IP address has changed. Dynamic DNS ensures that your gateway can still be reached after changing the IP address.

The following configuration steps are necessary:

■ Registration of a host name at a DynDNS provider

■ Configuration of the gateway

Registration The registration of a host name means that you define an individual user name for the DynDNS service, e.g. *dyn_client*. The service providers offer various domain names for this, so that a unique host name results for your gateway, e.g. *dyn_client.provider.com*. The DynDNS provider relieves you of the task of answering all DNS requests concerning the host *dyn_client.provider.com* with the dynamic IP address of your gateway.

To ensure that the provider always knows the current IP address of your gateway, the gateway contacts the provider when setting up a new connection and propagates its present IP address.

Configuration of the gateway The configuration is set up in *IP ➜ DYNDNS*. The first menu window contains a list of the entries already configured for using DynDNS services.

```
X2302w Setup Tool                         Bintec Access Networks GmbH
[IP][DYNDNS]: Dynamic DNS Service                            MyGateway

  DynDNS Services:


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




  DynDNS Provider List>

     ADD              DELETE            EXIT

```

From here you can also access the *IP* ➜ *DYNDNS* ➜ *DYNDNS PROVIDER LIST* submenu.

In the *IP* ➜ *DYNDNS* ➜ *ADD/EDIT* menu, you can configure name resolution over a DynDNS provider or change an existing configuration:

```
X2302w Setup Tool                        Bintec Access Networks GmbH
[IP][DYNDNS][ADD]                                           MyGateway


  Host Name
  Interface                    en0-1
  User
  Password

  Provider                     dyndns
  MX
  Wildcard                     off
  Permission                   enabled




          SAVE                             CANCEL

```

The menu contains the following fields:

Field	Description
Host Name	Full host name as registered with the DynDNS provider.
Interface	Defines the WAN interface whose IP address is to be propagated over the DynDNS service (e.g. the interface of the Internet Service Provider).
User	User name as registered with the DynDNS provider.
Password	Password as registered with the DynDNS provider.

Field	Description
Provider	Selection of a preconfigured DynDNS provider. A choice of DynDNS providers is already available in the unconfigured state and their protocols are supported. The default value is *dyndns*.
MX	Full host name of a mail server, to which e-mails are forwarded if the host currently configured is not to receive mail. Ask your provider about this forwarding service and make sure e-mails can be received from the host entered as MX.
Wildcard	Here you can activate the forwarding of all subdomains of **HOST NAME** to the current IP address of **INTERFACE**. Possible values: ■ *on*: The additional name resolution is activated. ■ *off* (default value): The additional name resolution is deactivated.
Permission	Here you can activate or deactivate the DynDNS entry just configured. Possible values are: ■ *enabled* (default value): Entry is activated. ■ *disabled*: Entry is deactivated.

Table 11-1:   **DYNDNS** menu fields

The **IP** ➜ **DYNDNS** ➜ **DYNDNS PROVIDER LIST** menu shows a list of the preconfigured providers. You cannot edit or delete the preconfigured providers.

A new provider is configured in the **IP** ➜ **DYNDNS** ➜ **DYNDNS PROVIDER LIST** ➜ **ADD/EDIT** menu.

```
X2302w Setup Tool                    Bintec Access Networks GmbH
[IP][DYNDNS][DYNDNS PROVIDER][ADD]                     MyGateway


 Name
 Server
 Path
 Port                     80

 Protocol                 dyndns

 Minimum Wait (sec)       300



         SAVE                            CANCEL

```

The menu contains the following fields:

Field	Description
Name	Here you can give the provider any name you like.
Server	Host name or IP address of the server on which the provider's DynDNS service runs.
Path	Path on the provider's server, where the script for administration of your gateway's IP address can be found. Ask your provider for the path to be used.
Port	Port at which your gateway is to reach your provider's server. Ask your provider for the relevant port. Default value: *80*.

Field	Description
Protocol	Here you select one of the protocols implemented. The following are available: ■ *dyndns* (default value) (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)
Minimum Wait (sec)	Here you enter the minimum time (in seconds) that the gateway must wait before it is allowed to propagate its current IP address to the DynDNS provider again. The default value is *300* seconds.

Table 11-2: *DYNDNS PROVIDER LIST* ➜ *ADD/EDIT* menu fields

11 DynDNS Submenu

12 Routing Protocols Submenu

The *ROUTING PROTOCOLS* menu is described below.

```
X2302w Setup Tool                          Bintec Access Networks GmbH
[IP][ROUTING]: Routing protocols                             MyGateway


             Routed                    running


             RIP >




             SAVE                      CANCEL

```

The contents of a gateway's routing table can be configured statically. A gateway also has the option of updating its routing tables dynamically by exchanging information with other gateways. This information exchange is specified in a routing protocol.

Routing protocols allow the gateway to adapt to changing network conditions dynamically and quickly find the best routing solutions in complex networks. One of the most frequently used routing protocols is *RIP*. It is explained briefly in the following chapters.

The *ROUTING PROTOCOLS* submenu is part of the *IP* menu. This shows the state of the Routing Daemon (*ROUTED*) and enables it to be activated or deactivated (with *ROUTED* = *running* or *stopped*).

The possible states of the Routing Daemon are:

■ *running*: Activates RIP (dependent on the interface-specific RIP configuration) and OSPF.

■ *stopped*: Deactivates RIP (dependent on the interface-specific RIP configuration) and OSPF.

The *IP* ➜ *ROUTING PROTOCOLS* menu also provides access to the *RIP* submenu.

The use of the routing protocols is activated globally in the *IP* ➜ *ROUTING PROTOCOLS* ➜ *ROUTED* menu. RIP is also activated on the respective interface by selecting the relevant protocol version in *RIP SEND* or *RIP RECEIVE*.

12.1 RIP Submenu

The *RIP* menu is described below.

```
X2302w Setup Tool                    Bintec Access Networks GmbH
[IP][ROUTING][RIP]: RIP configuration                  MyGateway


       UDP port                        520

       Static Settings >

       Timer >

       Filter >



       SAVE                            CANCEL

```

The *IP* ➜ *ROUTING PROTOCOLS* ➜ *RIP* menu is used for making global RIP settings. The activation of RIP is set specific to interface in *IP* ➜ *ADVANCED SETTINGS* of the respective interface menu.

A gateway exchanges routing information with other gateways using the RIP (Routing Information Protocol). A gateway sends messages to remote networks every 30 seconds using information from its own current routing table. The complete routing table is always exchanged in this process. If triggered RIP is used, information is only exchanged if the routing information has changed and only the changed information is sent.

Observing the information sent by other gateways enables new routes and shorter paths for existing routes to be saved in the routing table. As intermediate routes between networks can become unreachable, RIP removes routes that

are older than 5 minutes (i.e. routes not verified in the last 300 seconds). Routes learnt are not deleted if triggered RIP is used.

Note

The setting option *UDP PORT*, which is used for sending and receiving RIP updates, is only for test purposes. If the setting is changed, this can mean that the gateway sends and listens at a port to which no other gateways react. The default value *520* should be retained.

The *IP* ➜ *ROUTING PROTOCOLS* ➜ *RIP* menu provides access to three other submenus, in which you can define exactly how RIP updates are handled:

■ *STATIC SETTINGS*

■ *TIMER*

■ *FILTER*.

12.1.1 Static Settings Submenu

The *STATIC SETTINGS* menu is described below.

```
X2302w Setup Tool                    Bintec Access Networks GmbH
[IP][ROUTING][RIP][STATIC]: RIP Static Settings          MyGateway


     Default Route distribution      enabled

     Poisoned Reverse                disabled

     RFC 2453 variable timer         enabled

     RFC 2091 variable timer         disabled



     SAVE                            CANCEL

```

The **IP ➜ ROUTING PROTOCOLS ➜ RIP ➜ STATIC SETTINGS** menu is for configuring basic RIP parameters. It contains the following fields:

Field	Description
Default Route distribution	Here you determine whether the default route of your gateway is to be propagated via RIP updates. Possible values: ■ *disabled* ■ *enabled* The default value is *enabled*.
Poisoned Reverse	Procedure for preventing routing loops With standard RIP, the routes learnt are propagated over all interfaces with **RIP SEND** activated. With **POISONED REVERSE**, the gateway propagates over the interface over which it learnt the routes, with the metric (Next Hop Count) 16 (="Network is not reachable"). Possible values: ■ *disabled* ■ *enabled* The default value is *disabled*.
RFC 2453 variable timer	Here you can determine whether the timers described in RFC 2453 are to use the values you can configure in the **IP ➜ ROUTING PROTOCOLS ➜ RIP ➜ TIMER** menu. Possible values are: ■ *disabled* ■ *enabled* (default value) If you select *disabled*, the times defined in RFC are retained for the timeouts.

Field	Description
RFC 2091 variable timer	Here you can determine whether the timers described in RFC 2091 are to use the values you can configure in the **IP ➜ ROUTING PROTOCOLS ➜ RIP ➜ TIMER** menu. Possible values are: ■ *disabled* (default value) ■ *enabled* If you keep the *disabled* setting, the times defined in RFC are retained for the timeouts.

Table 12-1:   *STATIC SETTINGS* menu fields

The timers that can be activated in the **STATIC SETTINGS** menu are configured in the **IP ➜ ROUTING PROTOCOLS ➜ RIP ➜ TIMER** menu.

12.1.2   Timer Submenu

The *TIMER* menu is described below.

```
X2302w Setup Tool                         Bintec Access Networks GmbH
[IP][ROUTING][RIP][TIMER]: RIP timer configuration          MyGateway


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

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



              SAVE                              CANCEL

```

In this menu you can configure the timers defined by RFC 2091 and RFC 2453 for the various events in the lifetime of a route.

The menu is divided into fields for configuration of the *RIP-V2 TIMER (RFC 2453)* and *TRIGGERED-RIP TIMER (RFC 2091)*.

The *TIMER* menu contains the following fields (all timers are stated in seconds):

Field	Description
Update Timer	An RIP update is sent on expiry of this period of time. The default value is *30*.
Route Timeout	The *ROUTE TIMEOUT* is activated after the last update of a route. After timeout, the route is deactivated and the *GARBAGE COLLECTION TIMER* is started. The default value is *180*.
Garbage Collection Timer	The *GARBAGE COLLECTION TIMER* is started as soon as the route timeout has expired. After this timeout, the invalid route is deleted from the *IPROUTETABLE* if no further update is received for the route. The default value is *120*.
Hold down timer	The *HOLD DOWN TIMER* is activated as soon as the gateway contains an unreachable route (metric 16). After this timeout, the route is deleted from the *IPROUTETABLE*, if applicable. The default value is *120*.

Field	Description
Retransmission timer	After this timeout, update request or update response packets are sent again until an update flush or update acknowledge packet arrives.
	The default value is *5*.

Table 12-2:   *TIMER* menu fields

12.1.3   Filter Submenu

The *FILTER* menu is described below.

```
X2302w Setup Tool                           Bintec Access Networks GmbH
[IP][ROUTING][RIP][FILTER]: RIP Distribution Filter            MyGateway


 Interface   Direction   State    IP Address    Netmask    Priority




    ADD              DELETE            EXIT

```

In the *IP* ➜ *ROUTING PROTOCOLS* ➜ *RIP* ➜ *FILTER* menu, you can define exactly which routes are to be exported or imported.

You can use the following strategies for this:

■ You explicitly deactivate the import or export of certain routes. The import or export of all other routes that are not listed is still allowed.

■ You explicitly activate the import or export of certain routes. In this case, you must also explicitly deactivate the import or export of all other routes. You can do this using a filter for *IP ADDRESS* = no entry (this corresponds to the IP address 0.0.0.0) with *NETMASK* = no entry (this corresponds to the netmask 0.0.0.0) and *DISTRIBUTION* = *disabled*. To make sure this filter is used last, you must assign it the lowest priority.

You configure a filter for a default route with the following values:

- **IP ADDRESS** = no entry (this corresponds to the IP address 0.0.0.0) with **NETMASK** = *255.255.255.255*.

The first menu window shows a list of the filters already configured.

The fields shown correspond to the options configurable in the **ADD/EDIT** sub-menu. The value for the **DISTRIBUTION** variable is shown under **STATE**.

```
X2302w Setup Tool                    Bintec Access Networks 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

```

The **FILTER ➔ ADD/EDIT** menu contains the following fields:

Field	Description
Interface	Here you define the interface to which the rule to be configured applies.
IP Address	Here you enter the IP address to which the rule is to be applied. This address can be in the LAN or WAN.
	The rules for incoming and outgoing RIP packets (import or export) for the same IP address must be separately configured.
	You can enter individual host addresses or network addresses.
Netmask	Here you enter the netmask of **IP ADDRESS**.

Field	Description
Priority	Here you enter the priority with which the filter is to be used. If different filters with overlapping IP address range exist, the filter with the higher priority is used first. This enables a single host route to be imported from an IP address range that is actually disabled, if the rule that allows this has a higher priority than the rule that disables the address range. Possible values are *1* to *16*, where *1* corresponds to the highest priority. The default value is *1*.
Direction	Here you define whether the filter applies to the export or import of routes. Possible values are: ■ *import* ■ *export.* The default value is *import*.
Distribution	Here you define whether this filter allows or denies export or import from/to the gateway. Possible values are: ■ *enabled* ■ *disabled* The default value is *disabled*.
Metric1 offset on interface up	Here you enter whether and to what extent the metric of an imported or exported route is to be changed if the interface concerned is active (up). Possible values are *-16* to *16*. The default value is *0*.

Field	Description
Metric1 offset on interface dormant	Here you enter whether and to what extent the metric of an imported or exported route is to be changed if the interface concerned is inactive (dormant). Possible values are *-16* to *16*. The default value is *0*.

Table 12-3:   *FILTER* menu fields

Index: IP