H.323

August 2002

Table of Contents 3

REFERENCE

1 Technology Overview

1.1 Introduction

H.323

The H.323 standard is a set of specifications that enables real-time multimedia communication over packet-based networks.

H.323 covers the format of the data packets, coding and compression standards, signaling and flow control.

H.32x standards

The H.32x set of standards contains other standards for voice, video and data transmission in addition to H.323. It has been created by the International Telecommunications Union (ITU), an organization within the United Nations that deals with the coordination of telecommunication networks and services around the globe.

The H.32x family comprises the following:

Standard	Network
H.320	ISDN
H.321	ATM-based broadband ISDN (B-ISDN)
H.322	LAN with guaranteed quality of service
H.323	Packet-based network without guaranteed quality of service
H.324	Analog telephone network and mobile radio

Table A-1: H.32x family standards and associated networks

Advantages of H.323 standard

The H.323 standard enables modern communication equipment and facilities to be used in the accustomed working environment, e.g. ➤➤ **IP telephony**, video conferences (Microsoft NetMeeting etc.), ➤➤ **Computer Telephony Integration**, Desktop Sharing and ➤➤ **Unified Messaging**.

H.323 defines specifications for existing infrastructure. Nothing needs to be changed on existing packet-based networks. H.323 can be used on all IP-based networks such as ➤➤ **LAN**s, ➤➤ **WAN**s and the Internet.

H.323 is independent of platform, i.e. it is independent of the hardware and operating system used.

Solutions from different manufacturers can be combined using H.323 as a basis. The participants in a video conference, for example, can use different hardware. The devices are compatible as long as they are equipped with H.323.

H.323 and firewalls Corporate networks are normally hidden behind a ➤➤ **firewall** to protect sensitive corporate data against external access.

A video conference or IP telephony, however, cannot be operated so easily over a firewall. H.323 needs dynamically changing ports, whereas a firewall normally only opens certain ports for certain IP packets. An H.323 proxy solves this problem.

H.323 at BinTec BinTec Communications AG has integrated the H.323 proxy and H.323 gatekeeper features in its X-Generation products in Software Release 6.2.1. The proxy and gatekeeper features and the IPSec security solution are not available at the same time in X1000, X1200 and X3200.

BinTec’s solutions are based on version 2 of the H.323 standard.

1.2 Overview of H.323

The H.323 standard defines the components and methods used to transport voice, video and data over packet-based networks.

This chapter contains the following information:

- what components are found in an H.323 network
- what protocols are necessary for communication
- for what purpose the components use certain protocols
- the basic procedure for a call.

1.2.1 H.323 Components

A network based on the H.323 standard contains the following components:

- H.323 terminal
- Gateway (optional)
- Gatekeeper
- Multipoint Control Unit (MCU, optional).

These components provide point-to-point and point-to-multipoint connections in an IP network, i.e. it is possible to communicate with only one partner or with several partners simultaneously.

Apart from the above-mentioned components, additional components, such as firewall and proxy, can also be integrated in the network to include the security aspects that the H.323 standard does not cover.

Zone, endpoint All the terminals, gateways and MCUs administrated by a single gatekeeper are designated as an H.323 zone. A zone comprises at least one gatekeeper and one terminal and can also contain other terminals, gateways and MCUs.

Terminals, gateways and MCUs are also designated as endpoints.

Although gatekeeper, gateway and MCU are different logical components of the H.323 standard, they can be implemented in a single device.

The individual components in the H.323 network have certain properties and tasks, which are described in detail below.

Terminal

An H.323 terminal is an endpoint in the network that provides communication to another H.323 terminal, gateway or Multipoint Control Unit.

This is either a Personal Computer (PC) or another device on which H.323 protocols (see "H.323 Protocols", page 14) are available. For example, an IP telephone is a terminal in ➤➤ **Voice over IP**.

H.323 terminals can send and receive voice in real time, plus video and data as options. The H.323 standard therefore provides a basis for telephone connections over IP networks.

Gateway

A gateway can be implemented as a separate device or in software form.

An H.323 gateway connects an H.323 network to a network of another standard, e.g. to H.320 or H.324 (see table A-1, page 8). This involves translating the protocols, converting the formats, transforming the communication procedures and exchanging information between the networks.

A suitable gateway can, for example, enable communication between an H.323 network and the ➤➤ **PSTN**, i.e. set up a connection from IP telephones to telephones in the conventional telephone network.

A gateway is not necessary if communication is only to take place within a single network, e.g. within a single LAN.

Gatekeeper

The H.323 gatekeeper is always implemented as software. It is the "brain" of the network and the common point for all connections. The gatekeeper monitors all ➤➤ **calls**. Its main tasks are the admission of a call and address resolution in its zone. For this purpose, the endpoints for which a gatekeeper is to be responsible must register with this gatekeeper.

Although terminals can communicate directly, they should use the services of the gatekeeper if one is available in the network.

The gatekeeper provides important services for registered endpoints, some of which are available at every gatekeeper and some are optional.

Gatekeeper functions

The following gatekeeper functions are always available:

- Address translation: Translation of an alias or telephone number (➤➤ **E.164** address) to an IP address.
- Access control: Access control to the LAN can be provided via call authorization, the bandwidth or other criteria.

- Bandwidth control: Bandwidth can be controlled via bandwidth management according to previously defined criteria. For example, it is possible to limit the number of connections available simultaneously. This also limits the bandwidth used and the remaining bandwidth can be used for other purposes, e.g. data applications.
- Zone management: The gatekeeper provides the above functions for the terminals, gateways and MCUs registered in its zone.

The following gatekeeper functions are optional:

- Call control signaling: In a point-to-point connection, the gatekeeper either routes the Q.931 packets for call control or instructs the endpoints to communicate with each other directly.
- Call authorization: The gatekeeper can reject a request from a terminal or gateway to set up a call. The reasons can include restricted access to or from certain terminals or gateways or restricted access to certain devices at certain times.
- Bandwidth management: The gatekeeper can reject a call setup from a terminal if the bandwidth is not sufficient.
- Call management: The gatekeeper can maintain a list of the presently active calls to indicate that a called terminal is busy or to provide information for bandwidth management.
- Routing service: The gatekeeper can route calls over various paths in order to ensure even utilization of the network.

Multipoint Control Unit

Multipoint Control Units (MCUs) can be implemented as software or hardware. An MCU always contains a Multipoint Controller (MC) and optionally one or more Multipoint Processors (MP).

MCUs support a conference of three or more H.323 terminals. All terminals that take part in the conference set up a connection to the MCU. The MCU controls the conference resources and supports the negotiation of a common audio and/or video ➤➤ **CODEC** (see also "Audio", page 16 and "Video", page 16). The MCU can also control the traffic flow as an option.

There are two kinds of multipoint conferences: centralized and decentralized. A combination of both is also possible. Centralized multipoint conferences are mostly implemented, which requires an MCU. Decentralized multipoint conferences manage without an MCU, but need more computing power in the endpoints.

Proxy Server

Every corporate network is normally protected by a firewall against unauthorized access from outside, e.g. from the Internet.

Some communication services such as IP telephony or video conferencing are, however, dependent on overcoming the firewall so that partners inside and outside the corporate network can communicate with each other. The firewall should naturally not lose its function due to this process, but continue to protect the data in the corporate network.

An H.323 proxy server in combination with a firewall provides security functions for the above case. The data traffic arriving at the firewall is reflected by the proxy at the firewall. The addresses are translated by the proxy. The proxy fulfills its proxy function, but no direct connection is set up between, for example, the corporate network and the Internet. The proxy passes on the information to the respective other side, but without revealing the origin of this information.

Proxies not only protect the data, they also support bandwidth reservation or prioritization of data traffic. This ensures a reasonable quality of service for H.323 connections, although H.323 networks do not possess any guaranteed quality of service.

Advantages

A proxy has the following advantages:

- There are no direct connections between the internal and external system.
- A proxy can create comprehensive log files on data traffic and specific activities.
- A proxy supports user level authentication.
- A proxy analyzes the data packets.

- Newer proxies ensure transparency, i.e. the ➤➤ **clients** behind the firewall do not need to "know" that the proxy exists and do not need special software to communicate with the external network.

1.2.2 H.323 Protocols

Protocols control the interaction between the H.323 components.

The H.323 standard defines the following for voice, video and data transmission:

- how endpoints set up connections to each other
- how endpoints negotiate the pool of audio, video and data formats they want to use
- how voice, video and data are formatted and sent over the network
- how voice, video and data are synchronized
- how endpoints communicate with the responsible gatekeepers.

Different groups of protocols from the H.323 standard are required according to application.

H.323 uses the two transport protocols ➤➤ **TCP** and ➤➤ **UDP**, depending on what is to be transmitted.

The following protocols are defined in the H.323 standard. Some of these are always available in H.323 networks (obligatory) and some are optional:

Application	Protocols	Status	Transport protocol
Audio CODEC	G.711 G.722, G.723.1, G.726, G.728, G.729 A, G.729 B	obligatory optional	UDP UDP
Video CODEC	H.261, H.263	optional	UDP
Data	T.120	optional	TCP

Application	Protocols	Status	Transport protocol
Control	H.225 Registration, Admission and Status (RAS)	obligatory	UDP
	H.225 call signaling with Q.931	obligatory	TCP
	H.245 control signaling	obligatory	TCP
	Real-time Transfer Protocol (RTP)	obligatory	UDP
	Real-Time Control Protocol (RTCP)	obligatory	UDP
Security	H.235	optional	

Table A-2: H.323 protocols and their applications

The following diagram illustrates the protocols required for the various applications:

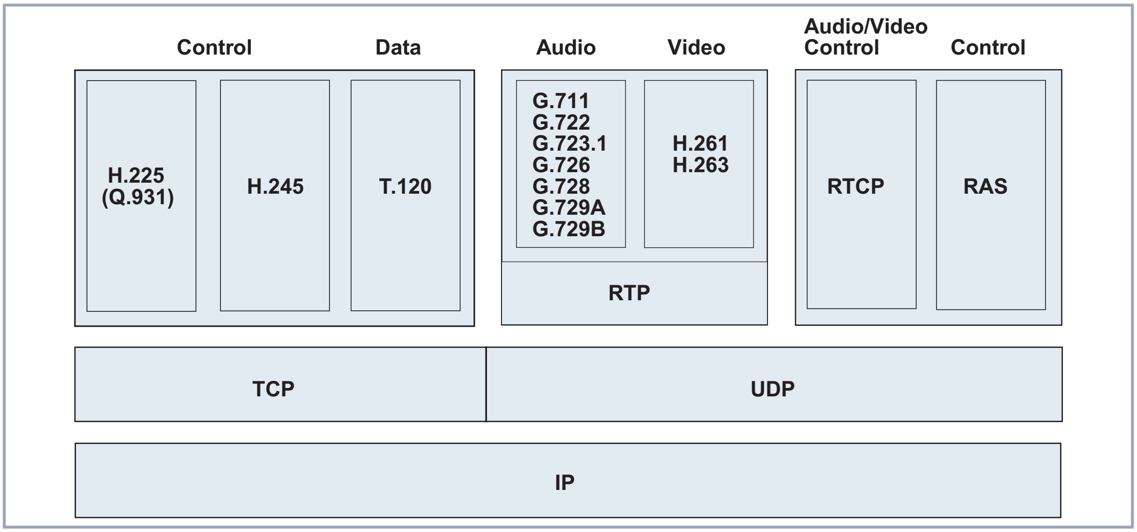


Figure A-1: H.323 protocols and their applications

Audio

An audio ➤➤ **CODEC** encodes, i.e. digitizes and compresses, an analog sound signal from the microphone to enable it to be transmitted over the network to the receiver. The transmitted signal is decoded by the CODEC at the receiver, i.e. decompressed and reconverted to an analog signal for output to a speaker.

As the transmission of sound signals is always available with H.323, all H.323 terminals must support at least one common voice coding process to be able to communicate with each other. This common voice coding process is called audio CODEC and operates to the G.711 standard at 56 kbps or 64 kbps.

The G.722 (48 kbps, 56 kbps or 64 kbps), G.723.1 (5.3 kbps or 6.3 kbps), G.726 (16 kbps, 24 kbps, 32 kbps or 40 kbps), G.728 (16 kbps) and G.729 A or G.729 B (each 8 kbps) standards can also be supported as optional standards with H.323.

Video

A video ➤➤ **CODEC** encodes a video signal before it is sent over the H.323 network. The received video code is decoded by the video CODEC and displayed on the video equipment.

H.323 provides the transmission of video signals as an option. Support for one or more video coding processes is therefore also optional. If an H.323 terminal permits video communication, it must also support a video CODEC, i.e. at least H.261 ➤➤ **QCIF**.

If the bandwidth is low, the H.263 and H.263+ video CODECs provide better video quality than H.261.

Data

The T.120 protocol is used for data transmission and is included in the H.323 standard as an option. T.120 enables applications such as shared access to a whiteboard by several users, Application Sharing, File Transfer, etc.

Microsoft NetMeeting, which also supports T.120, enables conferences to be held over the network. T.120 supports the setting up and control of the data flow, the connections and the actual conference.

Communication and Control

Apart from the protocols for coding and formatting voice, video and data, transmission over the network also requires various communication and control protocols, whose tasks are briefly described below.

H.225 Registration, Admission and Status (RAS)

The RAS (Registration, Admission and Status) protocol is required for communication between the endpoint and gatekeeper. RAS is not needed if no gatekeeper is used.

The protocol helps the endpoints to find the gatekeeper responsible for them and to register with this gatekeeper. RAS also controls the access of endpoints to the H.323 network, any bandwidth changes, the status of a connection and ending a connection between an endpoint and gatekeeper.

H.225 call signaling; Q.931

H.225 takes care of a call between H.323 endpoints.

The protocol is used for setting up and clearing a call and for call control between two endpoints. Signaling is based on the Q.931 ISDN signaling protocol. This ensures a relatively simple gateway to the public telephone network.

H.245 control signaling

H.245 is the media control protocol.

It negotiates endpoint functions, e.g. the voice coding process (audio CODEC). H.245 also controls the logical channels for the transmission of voice, video and data. The protocol controls the breakdown of the information into data packets and the synchronization of the media flows. It also contains information on flow control of the data and other control messages.

Real-time Transfer Protocol (RTP)

The Real-time Transfer Protocol (RTP) is used for transporting voice and video data.

RTP transports the audio and video traffic flow via ➤➤ **UDP**. Each UDP packet is given a header with a timestamp and sequence number. The header together with a suitable buffer is used at the receive terminal to sort the packets into the correct order, remove duplicated packets and synchronize voice, video and data.

Real-Time Control Protocol (RTCP)

The Real-Time Control Protocol (RTCP) is the counterpart to the RTP, the control protocol for the RTP as it were.

The RTCP monitors the quality of service and transfers information about the users in the network. The RTCP also informs all users about the quality of data delivery.

Security

To ensure comprehensive security for information transmitted on the basis of the H.323 standard, the traffic flows must be protected. The control protocols must also be transmitted securely.

The H.235 standard meets the following main requirements for providing secure data transmission:

- User authentication
- Data integrity check
- Data confidentiality (encryption).

Other protocols

The H.323 standard defines other protocols and additional functionality, which are not dealt with in this document.

1.2.3 Interaction between Components and Protocols

H.323 communication can be regarded as a mixture of voice, video, data and control information. Each component in the network has certain tasks, which it performs with the aid of the protocols.

A brief summary of the various protocols used by the individual components and for what purposes is given below.

This is followed by a brief description of the sequence of steps necessary for a ➤➤ **call**.

Terminal

An H.323 terminal uses the following protocols:

- H.245 is used to negotiate endpoint functions (audio CODECs, video CODECs, etc.), e.g. with another terminal. H.245 also controls the channels for transporting voice, video and data from one terminal to another terminal.
- H.225 call signaling is used for setting up and clearing a call and for call control between two endpoints, e.g. between two terminals, a terminal and a gateway or a terminal and an MCU.
- RAS is necessary for the terminal to register with a gatekeeper and for control tasks in connection with the gatekeeper.
- RTP/RTCP is used for sending and receiving audio and video data packets and for defining their order.

Gateway

A gateway supports the translation of protocols and the transfer of information between different types of networks, e.g. an IP network and an ➤➤ **SCN** network.

The following protocols are supported by the gateway on the H.323 side:

- H.245 is used by a gateway for negotiating the endpoint functions and for controlling the multimedia channels (see relevant item 1 under "Terminal", page 19)
- H.225 call signaling is used for setting up and clearing a call and for call control between two endpoints, e.g. between a gateway and a terminal or a gateway and an MCU.
- RAS is necessary for a gateway to register with a gatekeeper and for control tasks in connection with the gatekeeper.

On the ➤➤ **SCN** side, the gateway supports SCN-specific protocols, e.g. the ➤➤ **ISDN** protocol and the ➤➤ **SS7** protocol.

Gatekeeper

The gatekeeper requires only the RAS protocol for its tasks. RAS ensures that endpoints can register with the gatekeeper, i.e. enter its zone and announce their addresses. The gatekeeper provides various services for the endpoints in its zone (see "Gatekeeper functions", page 11).

Multipoint Control Unit

The Multipoint Controller (MC) in the MCU uses the H.245 protocol to negotiate common voice and video coding processes between all terminals.

1.2.4 Basic Procedure for H.323 Communication

The following processes take place when an H.323 terminal communicates with a second H.323 terminal:

1. Call setup

   Call setup uses the H.225 call control messages. Bandwidth is also reserved for the call.
2. Initial communication and negotiation of endpoint functions

   The endpoint functions, e.g. audio and video CODEC, are negotiated in a separate H.245 control channel or over a Q.931 call signalling channel using H.245 messages.
3. Configuring audiovisual communication

   The logical channels for the information flows are opened by H.245.
4. Services

   Various services can support the call flow during a call:

   A change in the bandwidth originally defined by the gatekeeper can be requested by the gatekeeper or a terminal at any time during a conference.

   The gatekeeper can request periodic status messages from the endpoints in order to determine if an endpoint is no longer active or if a fault has occurred.

   A point-to-point connection between two terminals can be extended into a conference, for which at least one MCU is necessary.

5. Ending the call

   Either of the endpoints involved can end an active call. This is done by ending video transmission after a complete frame, ending data and sound transmission and then closing the associated logical channels.

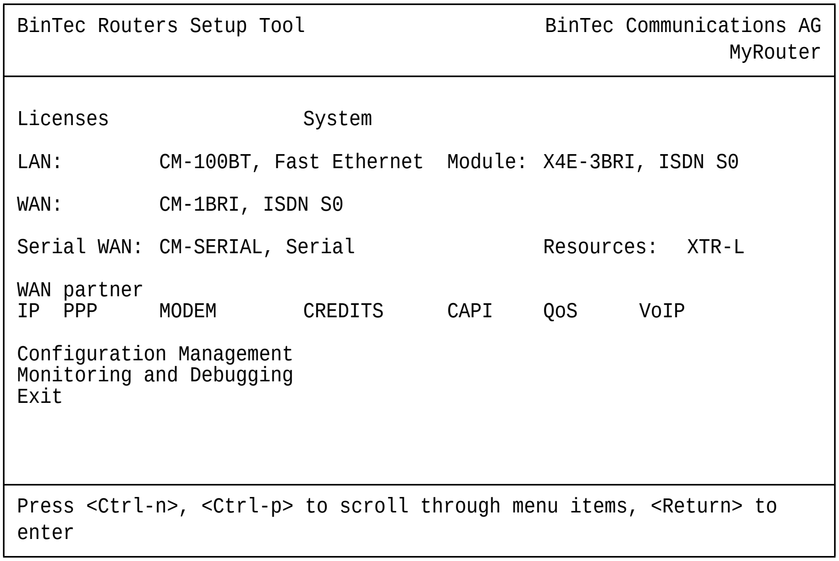
2 Configuration Overview

This chapter gives you an overview of how to configure a proxy and gatekeeper on a BinTec X-Generation router using the Setup Tool.

If a proxy and/or gatekeeper are configured and active, various monitor functions are available.

To configure a proxy and gatekeeper or use the monitor functions, activate the Setup Tool with `setup`. The main menu of the Setup Tool appears. The menu of your router may differ slightly depending on your hardware and your software configuration.

You will find the menus for configuring and monitoring a proxy and gatekeeper under ***VoIP***:

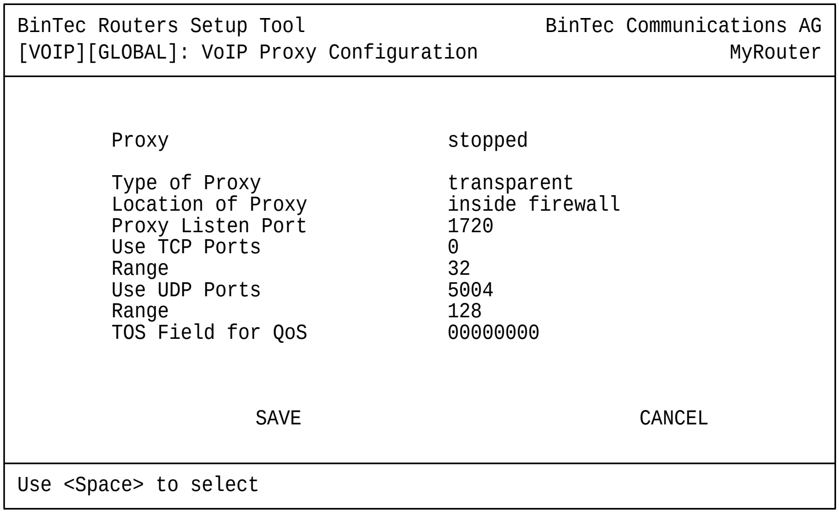


```
BinTec Routers Setup Tool                            BinTec Communications AG
                                                                     MyRouter

Licenses                 System

LAN:         CM-100BT, Fast Ethernet  Module:  X4E-3BRI, ISDN S0

WAN:         CM-1BRI, ISDN S0

Serial WAN:  CM-SERIAL, Serial                 Resources:   XTR-L

WAN partner
IP  PPP      MODEM        CREDITS      CAPI     QoS      VoIP

Configuration Management
Monitoring and Debugging
Exit



Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to
enter
```

The configuration of a proxy and gatekeeper are explained in detail using various scenarios in the "Workshop", page 35.

2.1 Configuring a Proxy

You can configure a proxy in the ***VoIP* ➜ *Proxy Settings*** menu of the Setup Tool:



```
BinTec Routers Setup Tool                              BinTec Communications AG
[VOIP][GLOBAL]: VoIP Proxy Configuration                               MyRouter


        Proxy                        stopped

        Type of Proxy                transparent
        Location of Proxy            inside firewall
        Proxy Listen Port            1720
        Use TCP Ports                0
        Range                        32
        Use UDP Ports                5004
        Range                        128
        TOS Field for QoS            00000000



                    SAVE                              CANCEL

Use <Space> to select
```

The ***VoIP* ➜ *Proxy Settings*** menu contains the following fields:

Field	Meaning
Proxy	Switches the proxy on or off. Possible values: ■ *stopped*: Proxy is switched off. ■ *running*: Proxy is switched on. Default value: *stopped.*

Field	Meaning
Type of Proxy	Defines the type of proxy. Possible values: ■ *transparent:* Proxy passes on H.323 pakkets unchanged; only the IP addresses in the packets are replaced. ■ *endpoint:* Proxy sets up two separate connections to the endpoints.
Location of Proxy	Indicates the location of the proxy in the network. Possible value: ■ *inside firewall*: Proxy is located in the LAN. ■ *outside firewall*: Proxy is located outside the LANs (not available at present).
Proxy Listen Port	TCP port for receiving the H.225 messages for ➤➤ **call** control. You should normally leave the default value *1720*. If a BinTec gatekeeper with which the endpoints are registered and which routes the H.225 call control messages is active, another port can be used. Possible values: *1024 ... 65535*
Use TCP Ports	Defines the first TCP port used for the H.245 protocol. Possible values: *0 ... 65535.* The default value *0* means that the ports for H.245 are assigned dynamically.

Field	Meaning
Range	Number of ports reserved for the H.245 protocol, starting with **Use TCP Ports**. The port range can be adapted to network-specific configurations, e.g. a separate firewall. Possible values: *0 ... 64.* Default value: *32.*
Use UDP Ports	Defines the first UDP port used for the transmission of voice and video. Possible values: *1024 ... 65535.* Default value: *5004.*
Range	Number of ports used for the transmission of voice and video. The port range can be adapted to network-specific configurations, e.g. a separate firewall. Possible values: *0 ... 256.* Default value: *128.*
TOS Field for QoS	Type of Service Field Here you can define how the proxy is to prioritize the RTP packets it sends. Possible values: *10000*: Specifies data packets that are to be delivered immediately if possible. *01000*: Specifies data packets that are to be transported at a high data throughput. *00100*: Specifies data packets that are to be delivered as reliably as possible.

Table A-3: ***VoIP*** ➧ ***Proxy Settings***

2.2 Configuring a Gatekeeper

You can configure a gatekeeper in the following menus of the Setup Tool:

- ***VoIP*** ➧ ***Gatekeeper Settings***
- ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings***
- ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table***

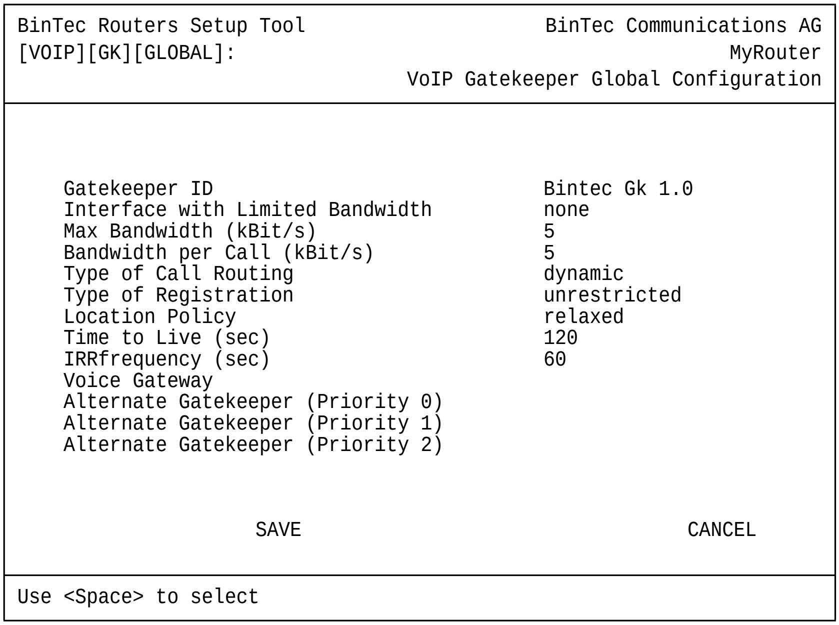
You need the ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table*** menu if you want to limit the pool of endpoints allowed to register with the gatekeeper.

The ***VoIP*** ➧ ***Gatekeeper Settings*** menu contains the following field:

Field	Meaning
Gatekeeper	Switches the gatekeeper on or off. Possible values: ■ *stopped*: Gatekeeper is switched off. ■ *running*: Gatekeeper is switched on. Default value: *stopped.*

Table A-4: ***VoIP*** ➧ ***Gatekeeper Settings***

The ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings*** menu is for defining the general settings for the gatekeeper:



```
BinTec Routers Setup Tool                     BinTec Communications AG
[VOIP][GK][GLOBAL]:                                           MyRouter
                                  VoIP Gatekeeper Global Configuration



    Gatekeeper ID                             Bintec Gk 1.0
    Interface with Limited Bandwidth          none
    Max Bandwidth (kBit/s)                    5
    Bandwidth per Call (kBit/s)               5
    Type of Call Routing                      dynamic
    Type of Registration                      unrestricted
    Location Policy                           relaxed
    Time to Live (sec)                        120
    IRRfrequency (sec)                        60
    Voice Gateway
    Alternate Gatekeeper (Priority 0)
    Alternate Gatekeeper (Priority 1)
    Alternate Gatekeeper (Priority 2)


                     SAVE                                 CANCEL

Use <Space> to select
```

The ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings*** menu contains the following fields:

Field	Meaning
Gatekeeper ID	Name of gatekeeper Default value: *Bintec Gk 1.0.*

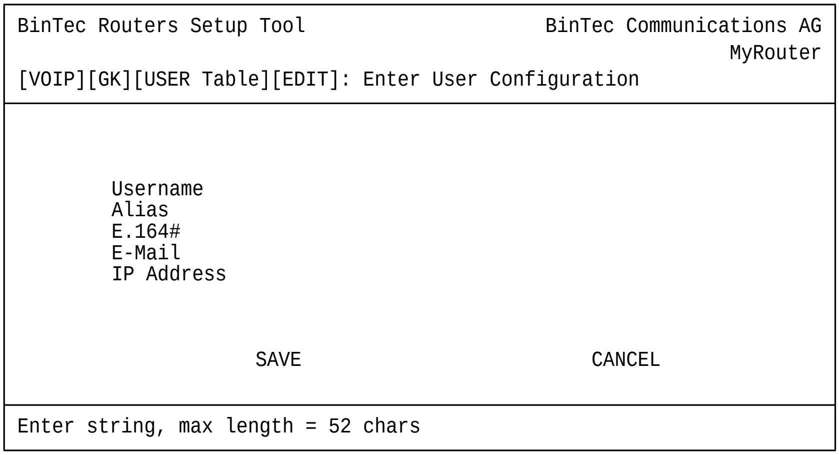
Field	Meaning
Interface with Limited Bandwidth	Defines an interface for which the bandwidth can be limited to **Max Bandwidth (kBits/s)**. You can select an interface according to the device used and WAN partner configured, e.g.: ■ *none* ■ *en1* ■ *en1-snap* ■ *t-online* Default value: *none.*
Max Bandwidth (kBits/s)	Defines the maximum bandwidth in kbps for the interface selected under **Interface with Limited Bandwidth**. Default value: *5.*
Bandwidth per Call (kBits/s)	Reserved bandwidth per call. Default value: *5.*
Type of Call Routing	Routing mode used by the gatekeeper for RTP and control packets. ■ *direct*: Packets are transmitted directly from one endpoint to the other. ■ *routed*: All packets are routed via gatekeeper or proxy. ■ *dynamic*: Network address is checked and the packets are transported in *direct* or *routed* mode in line with bandwidth management. Default value: *dynamic.*

Field	Meaning
Type of Registration	Determines if any endpoint can register with the gatekeeper or if the registered endpoints are limited to a predefined list. ■ *unrestricted*: All endpoints are allowed to register. ■ *limited to user table*: Endpoints can only register if they are entered in the user table (see table A-6, page 31). Default value: *unrestricted.*
Location Policy	Defines how the gatekeeper carries out address resolution for an endpoint. Possible values: ■ *local*: Covers only endpoints included under ***VoIP*** ➧ ***Monitoring*** ➧ ***Registered Users*** ➧ **ADD** or endpoints addressed directly via an IP address. ■ *remote*: Sends request for address resolution for an endpoint to the **Alternate Gatekeeper**. ■ *relaxed*: Tries *local* address resolution first and then *remote*. Default value: *relaxed.*
Time to Live (sec)	Time in seconds within which an endpoint already registered with the gatekeeper must register again to extend the registration period. Possible values: *60 ... 3600.* Default value: *120.*

Field	Meaning
IRRfrequency (sec)	Info Request Response Frequency Time in seconds between two Info Request Responses of an endpoint. The endpoint uses the Info Request Response to send various status and control information, plus an optional copy of the Q.931 messages. The Info Request is used for checking if a call is still active. The endpoint itself is checked with the aid of Time to Live. An Info Request is sent by the gatekeeper if the endpoint fails to send an Info Request Response in the IRRfrequency without being requested. Possible values: *60 ... 3600.* Default value: *60.*
Voice Gateway	IP address of a gateway to which calls with unresolvable addresses are passed (comparable with an IP default gateway).
Alternate Gatekeeper (Priority 0) **Alternate Gatekeeper (Priority 1)** **Alternate Gatekeeper (Priority 2)**	Here you can enter the IP addresses of three gatekeepers that can be requested in succession if your BinTec gatekeeper cannot resolve the address of an endpoint.

Table A-5: ***VoIP* ➧ *GATEKEEPER SETTINGS* ➧ *GLOBAL SETTINGS***

The ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table*** ➧ **ADD** menu is used to define the endpoints that can register with the gatekeeper:



```
BinTec Routers Setup Tool                          BinTec Communications AG
                                                                   MyRouter
[VOIP][GK][USER Table][EDIT]: Enter User Configuration



        Username
        Alias
        E.164#
        E-Mail
        IP Address



                     SAVE                             CANCEL

Enter string, max length = 52 chars
```

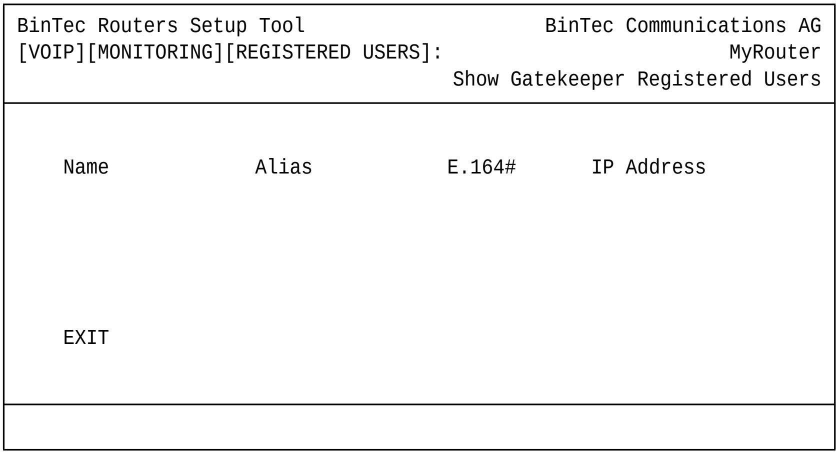
The menu contains the following fields:

Field	Meaning
User name	User name
Alias	Alias or nickname for an endpoint
E.164 #	Telephone number in ➤➤ **E.164** format
E-Mail	E-mail address
IP Address	Endpoint's IP address

Table A-6: ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table*** ➧ **ADD**

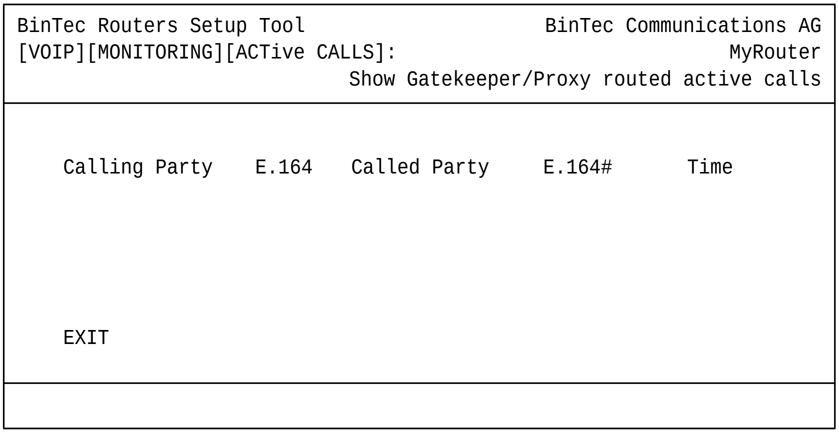
2.3 Monitoring

The ***VoIP*** ➜ ***Monitoring*** ➜ ***Registered Users*** menu displays the endpoints currently registered with the gatekeeper. The menu is empty if no endpoints are registered:



```
BinTec Routers Setup Tool                          BinTec Communications AG
[VOIP][MONITORING][REGISTERED USERS]:                              MyRouter
                                       Show Gatekeeper Registered Users


    Name             Alias            E.164#       IP Address






    EXIT


```

The ***VoIP*** ➜ ***Monitoring*** ➜ ***Active Calls*** menu displays the endpoints currently involved in a call. The menu is empty if no call is currently in progress:



```
BinTec Routers Setup Tool                          BinTec Communications AG
[VOIP][MONITORING][ACTive CALLS]:                                  MyRouter
                              Show Gatekeeper/Proxy routed active calls


    Calling Party    E.164    Called Party     E.164#      Time






    EXIT


```

The ***VoIP*** ➜ ***Monitoring*** ➜ ***Call History*** menu displays the calls already ended. The menu is empty if no calls have taken place.

3 Glossary

Call Point-to-point communication between two H.323 endpoints.

Client Workstation in the PC network that uses the services of the ➤➤ **server**.

CODEC Coder/decoder

Computer Telephony Integration (CTI) Telephony service assisted by computer systems.

CTI can offer various services ranging from simple applications like computer-aided callback to complete call centers.

E.164 Address standard used in ISDN networks, i.e. common telephone numbers.

Firewall Designates the whole range of mechanisms to protect the local network against external access.

IP Internet Protocol

IP telephony Telephony over IP networks such as the Internet (see also ➤➤ **Voice over IP**).

ISDN Integrated Services Digital Network

LAN Local Area Network

A network covering a small geographic area and controlled by its owner, usually within a building/head office.

POTS Plain Old Telephone System

The traditional analog telephone network.

PSTN Public Switched Telephone Network

The worldwide telephone network.

QCIF Quarter Common Interchange Format

Video format with 176 x 144 pixels, which is used for ISDN video conferences.

SCN Switched Circuit Network

Public or private line-switched telecommunication network.

Server Service provider in the PC network

SS7 Signaling System No. 7

Signaling protocol

TCP Transmission Control Protocol

TCP is a connection-based transport protocol from the TCP/IP family. Control mechanisms prevent the loss of data packets.

UDP User Datagram Protocol

A transport protocol similar to TCP. UDP offers no control or acknowledgment mechanisms and is therefore faster than TCP. UDP is connectionless in contrast to TCP.

Unified Messaging Unified Messaging combines the three data types of voice, fax and e-mail.

All three are accessible either via e-mail environment (with suitable identification for each data type) or via telephone.

Voice over IP (VoIP) Voice over IP uses the IP protocol for voice and video transmission and not just for data transfer.

WAN Wide Area Network

Wide area connections, e.g. over ISDN, X.25.

WORKSHOP

1 Configuration of IP Telephones in the Local Network

1.1 Introduction

You can operate IP telephones in your LAN with very little configuration effort.

Advantages of IP telephones

IP telephones offer the following advantages:

Only a single network is required for data and telephony and no additional infrastructure is needed for telephony in the LAN. (You need a gateway for telephoning to the "outside world".)

Apart from the cost savings through the use of a single network for all communication, IP telephones have a direct advantage in everyday work: If an employee changes his workplace permanently or temporarily within the company, he can take his telephone with him and connect it at his new workplace. No new configuration is necessary and the employee is immediately available under the usual telephone number.

You need no other components in addition to your BinTec router in order to operate IP telephones in the LAN.

Instead of an IP telephone, you can also use a PC with microphone or headset and Microsoft NetMeeting for communication.

Procedure

Taking IP telephones into operation in the LAN and testing them is divided into four steps:

- Registering IP telephones with the BinTec gatekeeper (section B, chapter 1.3.1, page 38)
- Checking the registration (section B, chapter 1.3.2, page 41)
- Making a test call (section B, chapter 1.3.3, page 42)
- Displaying calls (section B, chapter 1.3.4, page 42).

1.2 Requirements

Availability of H.323 gatekeeper

You can use IP telephones within your LAN together with the gatekeeper functionality of a BinTec X-Generation router with Software Release 6.2.1 or later. If you use **X1000**, **X1200** or **X3200** routers, the IPSec security solution and the gatekeeper are not available at the same time.

Proceed as follows to make sure your router has the gatekeeper functionality:

Router type

➤ Check which router type you are using.

X1000, X1200, X3200

For **X1000**, **X1200** and **X3200** routers:

➤ Check if your router is operated with the IPSec system software.

If you have Software Release 6.2.1 with IPSec:

➤ Install Software Release 6.2.1 without IPSec or purchase a BinTec X-Generation router that provides the IPSec and gatekeeper functionality at the same time.

  If you have Software Release 6.2.1 without IPSec, the gatekeeper is available.

Other X-Generation routers

For all other X-Generation routers:

➤ Check if Software Release 6.2.1 is installed on your router. If your router has an older software version, carry out a software update. You will find information about a software update in the User's Guide for your BinTec router.

1.3 Configuration and Monitoring

Diagram of a LAN with IP telephones:

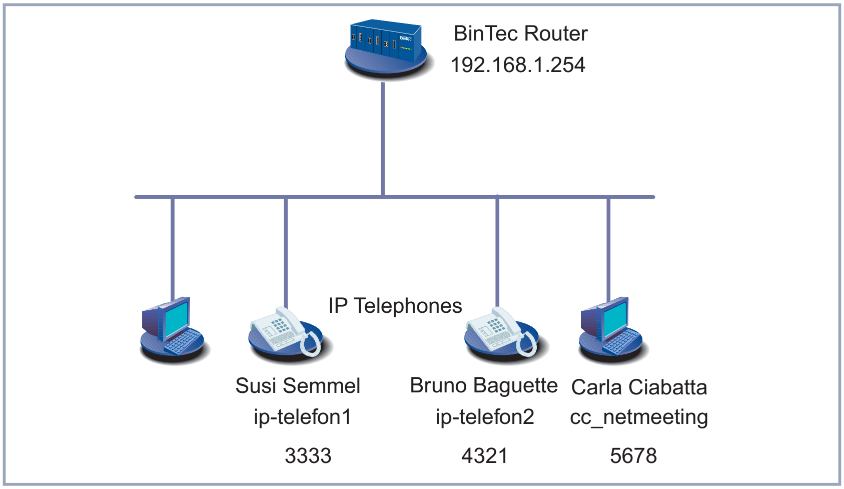


Figure B-1: IP telephones and PCs in the LAN

1.3.1 Registering IP Telephones with the BinTec Gatekeeper

How to register your IP telephone with the gatekeeper of your BinTec router is described below. The registration is described using the Innovaphone 200 as an example. IP telephones of other manufacturers are registered in a similar way.

To ensure that only certain IP telephones can register with your BinTec gatekeeper, enter the desired telephones in the ***User Table*** of the gatekeeper. At the IP telephone itself, enter the alias of the IP telephone and the IP address of the gatekeeper with which the IP telephone is to register. The actual registration takes place automatically.

Before you start, make sure the IP telephone already has an IP address or is assigned an IP address. To reduce the configuration effort, you can obtain the IP address via a DHCP server. If you would like to use your BinTec router as a

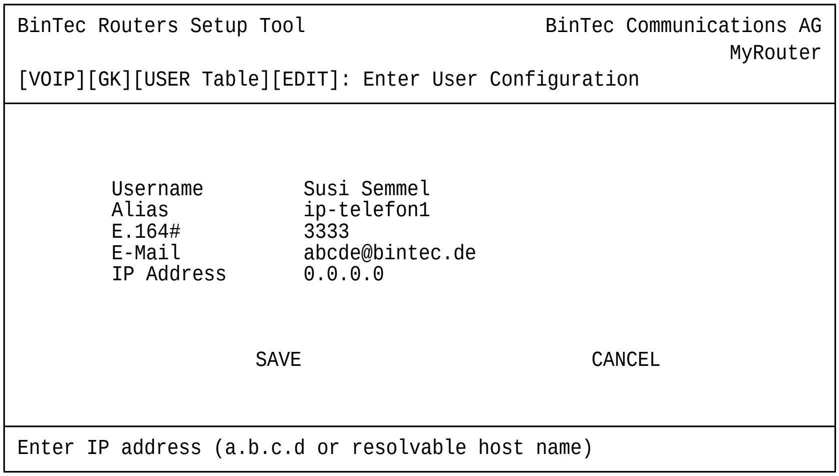
DHCP server, you will find configuration information for this in the User's Guide for your router.

Entering IP telephone in user table

To enter an IP telephone in the ***User Table*** of your BinTec gatekeeper, proceed as follows in the Setup Tool:

- Go to ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table*** ➧ **ADD**.

You see the following menu:



```
BinTec Routers Setup Tool                        BinTec Communications AG
                                                                 MyRouter
[VOIP][GK][USER Table][EDIT]: Enter User Configuration



        Username         Susi Semmel
        Alias            ip-telefon1
        E.164#           3333
        E-Mail           abcde@bintec.de
        IP Address       0.0.0.0



                     SAVE                             CANCEL


Enter IP address (a.b.c.d or resolvable host name)
```

- Enter **Username**, e.g. ***Susi Semmel***.
- Enter **Alias**, e.g. ***ip-telefon1***.
- Enter **E.164**, e.g. ***3333***.
- Enter **E-Mail**, e.g. ***abcde@bintec.de***.
- Skip **IP Address**.
- Press **SAVE**.

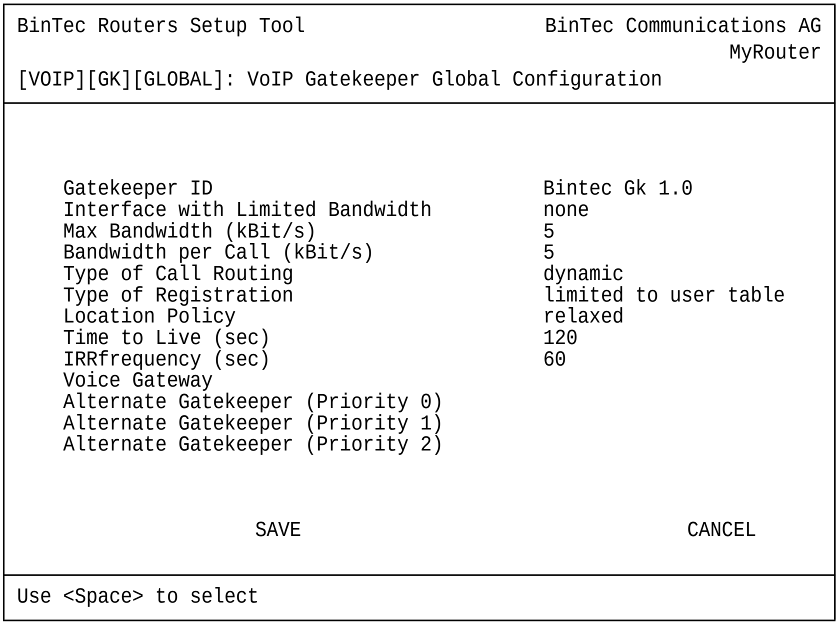
  The parameters of the IP telephone are temporarily saved and activated.

Limitation to user table

Proceed as follows to make sure that endpoints can only register if they are entered in the ***User Table***:

- Go to ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings***.

You see the following menu:



```
BinTec Routers Setup Tool                            BinTec Communications AG
                                                                     MyRouter
[VOIP][GK][GLOBAL]: VoIP Gatekeeper Global Configuration



    Gatekeeper ID                              Bintec Gk 1.0
    Interface with Limited Bandwidth           none
    Max Bandwidth (kBit/s)                     5
    Bandwidth per Call (kBit/s)                5
    Type of Call Routing                       dynamic
    Type of Registration                       limited to user table
    Location Policy                            relaxed
    Time to Live (sec)                         120
    IRRfrequency (sec)                         60
    Voice Gateway
    Alternate Gatekeeper (Priority 0)
    Alternate Gatekeeper (Priority 1)
    Alternate Gatekeeper (Priority 2)


                       SAVE                                   CANCEL

Use <Space> to select
```

- ➤ Select **Type of Registration**: *limited to user table*.
- ➤ Press **SAVE**.

Activating gatekeeper Proceed as follows to activate the gatekeeper with the settings already made:

- ➤ Go to ***VoIP*** ➧ ***Gatekeeper Settings***.
- ➤ Select **Gatekeeper**: *running*.
- ➤ Press **SAVE**.

  The gatekeeper is now active.

Entering gatekeeper for IP telephone Proceed as follows to enter the gatekeeper of your BinTec router at the Innovaphone 200 telephone:

- ➤ Press the **Menu** button on the housing of the Innovaphone 200.
- ➤ Go to **configuration** ➧ **registration** ➧ **VoIP gatekeeper** in this menu.
- ➤ Enter **gatekeeper ID** or leave the field empty.
- ➤ Enter **gatekeeper IP address**, e.g. ***192.168.1.254***.

➤ Switch the **RAS protocol** *on*.

➤ Leave the **configuration** ➧ **registration** ➧ **VoIP gatekeeper** menu.

You change to **configuration** ➧ **registration**.

➤ Go to **configuration** ➧ **registration** ➧ **telephone number**.

➤ Enter **name (H323)**, e.g. ***ip-telefon1***.

The **name (H323)** in the Innovaphone 200 is the same as the **Alias** (and not the **Username**) in the Setup Tool.

➤ Leave **configuration** ➧ **registration** ➧ **telephone number** and close all menus.

Registering

The Innovaphone 200 registers with the gatekeeper automatically.

The **Username** and **telephone number** are shown on the display of the Innovaphone 200. A rhomb at the bottom right shows the registration status at the gatekeeper: A filled rhomb indicates that the IP telephone is registered. The IP telephone is not registered if the rhomb is empty.

Registering other IP telephones

➤ Proceed in the same way for all the other IP telephones you wish to register with the gatekeeper.

➤ For example, register a second IP telephone with the name ***Bruno Baguette***, the alias ***ip-telefon2*** and the telephone number ***4321***.

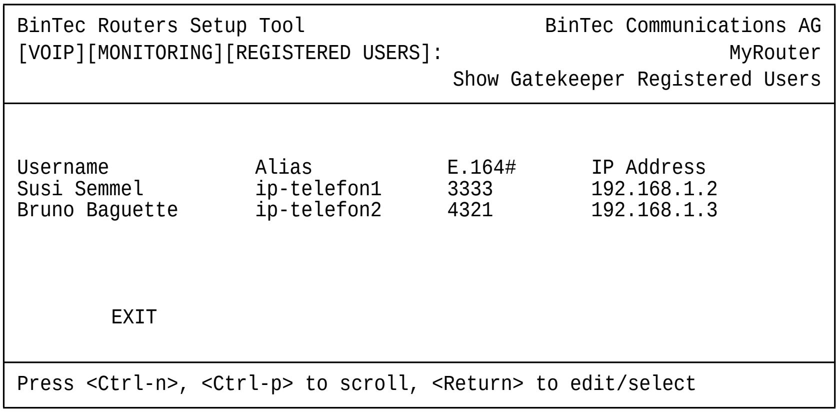
1.3.2 Checking the Registration

Proceed as follows to check that the registration of the IP telephones with the gatekeeper of your BinTec router was successful:

➤ Go to ***VoIP*** ➧ ***MONITORING*** ➧ ***REGISTERED USERS*** in the Setup Tool menu.

The IP telephones registered with the gatekeeper are displayed.

For example, if *ip-telefon1* and *ip-telefon2* have registered with the gatekeeper, you will see the following display:



```
BinTec Routers Setup Tool                              BinTec Communications AG
[VOIP][MONITORING][REGISTERED USERS]:                                  MyRouter
                                              Show Gatekeeper Registered Users


Username             Alias            E.164#       IP Address
Susi Semmel          ip-telefon1      3333         192.168.1.2
Bruno Baguette       ip-telefon2      4321         192.168.1.3



        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can obtain detailed information for each entry:

➤ Select the desired entry and press **Return**.

A detailed list is displayed.

1.3.3 Making a Test Call

To test if the IP telephones can phone each other, make a call from one IP telephone to another IP telephone. You can enter the telephone number, the user name or the alias for setting up the call.

If everything is in order, the call is set up as usual.

1.3.4 Displaying Calls

You can display both the currently active calls and the calls already cleared.

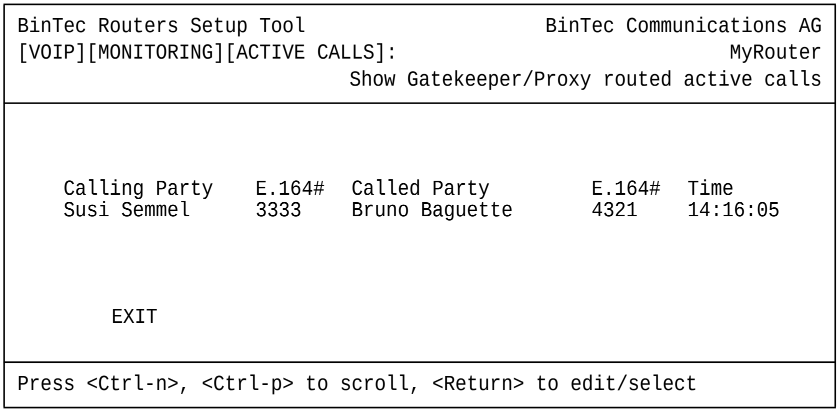
Active calls

Proceed as follows to display the active calls:

➤ Go to ***VoIP*** ➧ ***Monitoring*** ➧ ***Active Calls***.

The currently active calls are displayed.

In our example, Susi Semmel is currently speaking to Bruno Baguette:



```
BinTec Routers Setup Tool                     BinTec Communications AG
[VOIP][MONITORING][ACTIVE CALLS]:                             MyRouter
                             Show Gatekeeper/Proxy routed active calls



    Calling Party    E.164#  Called Party        E.164#  Time
    Susi Semmel      3333    Bruno Baguette      4321    14:16:05




        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can obtain detailed information for each call:

➤ Select the desired entry and press **Return**.

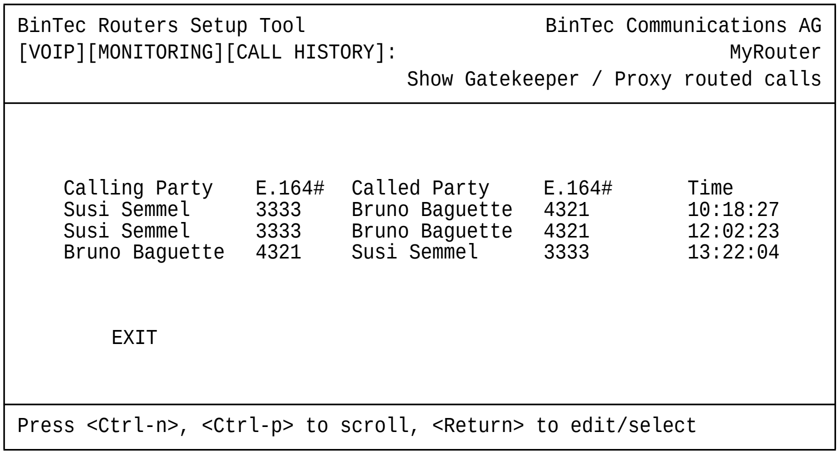
A detailed list is displayed.

Cleared calls Proceed as follows to display calls already cleared:

➤ Go to ***VoIP*** ➧ ***Monitoring*** ➧ ***Call History***.

The calls already cleared are displayed.

Three calls have been made in our example:



```
BinTec Routers Setup Tool                     BinTec Communications AG
[VOIP][MONITORING][CALL HISTORY]:                             MyRouter
                                  Show Gatekeeper / Proxy routed calls



    Calling Party    E.164#  Called Party    E.164#      Time
    Susi Semmel      3333    Bruno Baguette  4321        10:18:27
    Susi Semmel      3333    Bruno Baguette  4321        12:02:23
    Bruno Baguette   4321    Susi Semmel     3333        13:22:04



        EXIT


Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can also obtain detailed information for each call:

➤ Select the desired entry and press **Return**.

A detailed list is displayed showing information such as who called who and for how long.

1.3.5 Microsoft NetMeeting in the LAN

Instead of using an IP telephone, you can also use a PC and microphone or headphones and Microsoft NetMeeting to communicate in the LAN with other IP telephones or other PCs with NetMeeting.

Make sure Microsoft NetMeeting is properly installed on your PC before you start.

NetMeeting must register with the gatekeeper before it is possible to communicate with IP telephones or other NetMeeting users.

To ensure that only a certain PC with NetMeeting can register with your BinTec gatekeeper, enter the desired communication partner in the ***USER TABLE*** of the gatekeeper. For NetMeeting itself, enter only the alias and the gatekeeper with which NetMeeting is to register. The actual registration takes place automatically.

Entering NetMeeting in user table

To enter NetMeeting in the ***USER TABLE*** of your BinTec gatekeeper, proceed as follows in the Setup Tool:

➤ Go to ***VOIP*** ➧ ***GATEKEEPER SETTINGS*** ➧ ***USER TABLE*** ➧ **ADD**.

➤ Enter **Name**, e.g. ***Carla Ciabatta***.

➤ Enter **Alias**, e.g. ***cc_netmeeting***.

➤ Enter **E.164**, e.g. ***5678***.

➤ Enter **E-Mail**, e.g. ***klmno@bintec.de***.

➤ Skip **IP Address**.

➤ Press **SAVE**.

The entries are temporarily saved and activated.

Entering gatekeeper for NetMeeting

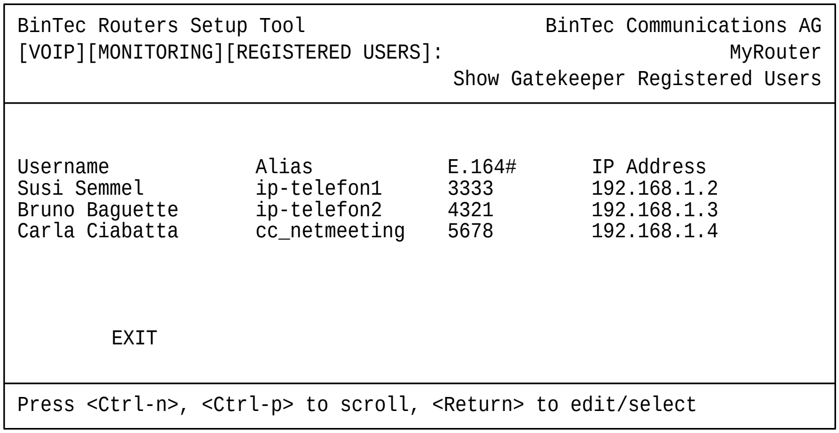
Proceed as follows to enter the gatekeeper for NetMeeting:

- Start NetMeeting on your PC.
- Go to **Tools** ➧ **Options**.
- Click **Advanced Calling**.
- Activate the control box **Use a gatekeeper to place calls** and enter the IP address of the gatekeeper, e.g. ***192.168.1.254***.
- Activate the control box **Log on using my account name** and enter the desired name, e.g. ***cc_netmeeting***.
- Close both windows by pressing **OK**.

  NetMeeting registers with the gatekeeper.

Checking the registration

In our example, you can now see Carla Ciabatta added under ***VoIP*** ➧ ***MONITORING*** ➧ ***REGISTERED USERS***:



```
BinTec Routers Setup Tool                          BinTec Communications AG
[VOIP][MONITORING][REGISTERED USERS]:                              MyRouter
                                           Show Gatekeeper Registered Users


Username             Alias            E.164#       IP Address
Susi Semmel          ip-telefon1      3333         192.168.1.2
Bruno Baguette       ip-telefon2      4321         192.168.1.3
Carla Ciabatta       cc_netmeeting    5678         192.168.1.4




        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

The users of the three terminals can now telephone each other.

If NetMeeting does not register with the gatekeeper, the program has saved an older configuration. Restart NetMeeting.

2 Access to Head Office with Microsoft NetMeeting

2.1 Introduction

An employee at a home office can use Microsoft NetMeeting to participate from home in a conference in the company if access to the network at the head office is configured for him.

The employee needs only a PC with Microsoft NetMeeting and an ISDN card, or another direct dialing in facility, e.g. T-DSL with modem and network card.

Procedure In this case, the initial operation, test and use of Microsoft NetMeeting is divided into four steps:

- Registering NetMeeting with the BinTec gatekeeper (section B, chapter 2.3.1, page 48)
- Checking the registration (section B, chapter 2.3.2, page 51)
- Making a test call to head office (section B, chapter 2.3.3, page 53)
- Displaying calls (section B, chapter 2.3.4, page 54).

2.2 Requirements

The use of flat-rate Internet access is recommended for using NetMeeting.

For security reasons, BinTec Communications AG does not support the NetMeeting functions "Desktop Sharing" and "Whiteboard".

If you use NetMeeting together with the gatekeeper or proxy functionality, you cannot use the "Internet Locator Server" from Microsoft.

Availability of H.323 proxy and H.323 gatekeeper

You can use Microsoft NetMeeting together with the gatekeeper and proxy functionality of a BinTec X-Generation router with Software Release 6.2.1 or later. If you use **X1000**, **X1200** or **X3200** routers, the IPSec security solution and the gatekeeper or proxy are not available at the same time.

Proceed as follows to make sure your router has the gatekeeper and proxy functionality:

Router type

➤ Check which router type you are using.

X1000, X1200, X3200

For **X1000**, **X1200** and **X3200** routers:

➤ Check if your router is operated with the IPSec system software.

If you have Software Release 6.2.1 with IPSec:

➤ Install Software Release 6.2.1 without IPSec or purchase a BinTec X-Generation router that provides the IPSec and gatekeeper or proxy functionality at the same time.

If you have Software Release 6.2.1 without IPSec, the gatekeeper and proxy functionality is available.

Other X-Generation routers

For all other X-Generation routers:

➤ Check if Software Release 6.2.1 is installed on your router. If your router has an older software version, carry out a software update. You will find information about a software update in the User’s Guide for your BinTec router.

2.3 Configuration and Monitoring

The diagram below shows a home office connected to the head office over the Internet:

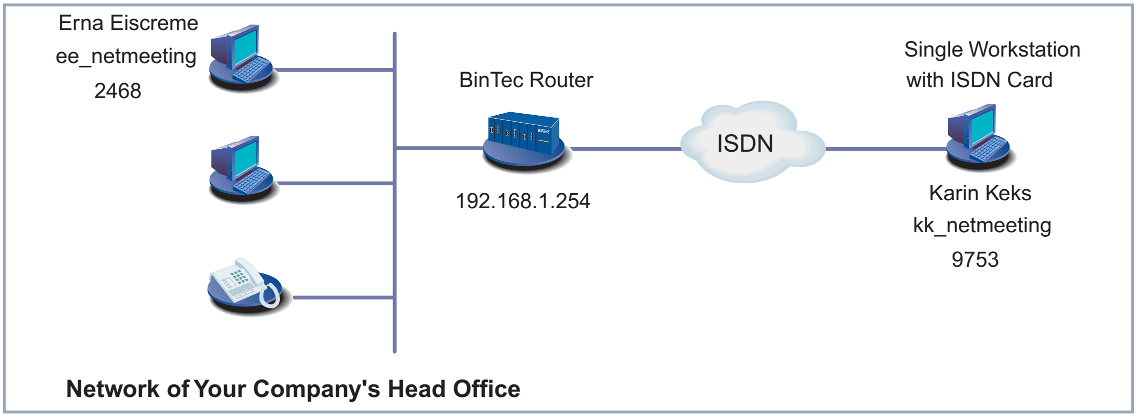


Figure B-2: Head office and home office connected by a BinTec router

2.3.1 Registering NetMeeting with the BinTec Gatekeeper

Summary Before an employee at a home office can communicate with his colleagues at head office using Microsoft NetMeeting, NetMeeting must register with the gatekeeper at the head office. The relevant requirements must be fulfilled for both NetMeeting itself and for the BinTec router at the head office:

- The administrator at the head office must assign a **Username** to the home office employee and enter him in the gatekeeper’s ***USER TABLE***. He must ensure that this entry is used for registration.
- The home office employee must configure NetMeeting so that it registers with the gatekeeper of the BinTec router.

Procedure The administrator of the BinTec router activates the proxy to ensure that NetMeeting has access to the corporate network.

To ensure that the home office employee can be reached under his name and the desired telephone number, the administrator enters the relevant data in the ***User Table*** of the gatekeeper.

The home office employee only enters in the NetMeeting program the alias and the gatekeeper with which NetMeeting is to register. The actual registration takes place automatically.

You can also use other H.323-capable endpoints instead of NetMeeting if they are registered with the BinTec gatekeeper.

Configuring Your BinTec Router (Head Office)

The settings you as administrator must make on your BinTec router at head office to enable a home office employee with NetMeeting to dial in to the corporate network are described below.

Activating a proxy

To configure the proxy of your BinTec router for access with NetMeeting, proceed as follows in the Setup Tool:

- Go to ***VoIP*** ➧ ***Proxy Settings***.
- Leave the default settings.
- Select **Proxy**: *running*.
- Press **SAVE**.

  The proxy is activated.

Entering data for NetMeeting in user table

Proceed as follows to enter the data for NetMeeting in the ***User Table*** of your BinTec gatekeeper:

- Go to ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table*** ➧ **ADD**.
- Enter **Username**, e.g. ***Karin Keks***.
- Enter **Alias**, e.g. ***kk_netmeeting***.
- Enter **E.164**, e.g. ***9753***.
- Enter **E-Mail**, if applicable, e.g. ***pqrst@bintec.de***.
- Skip **IP Address**.

➤ Press **SAVE**.

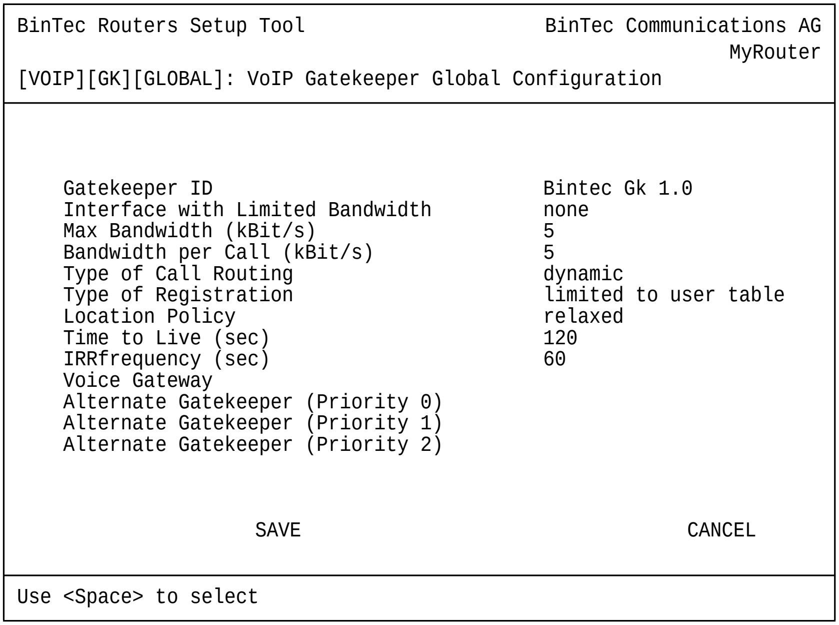
The entries are temporarily saved and activated.

Limitation to user table

Proceed as follows to make sure that endpoints can only register if they are entered in the ***User Table***:

➤ Go to ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings***.

You see the following menu:



```
BinTec Routers Setup Tool                        BinTec Communications AG
                                                                 MyRouter
[VOIP][GK][GLOBAL]: VoIP Gatekeeper Global Configuration



    Gatekeeper ID                             Bintec Gk 1.0
    Interface with Limited Bandwidth          none
    Max Bandwidth (kBit/s)                    5
    Bandwidth per Call (kBit/s)               5
    Type of Call Routing                      dynamic
    Type of Registration                      limited to user table
    Location Policy                           relaxed
    Time to Live (sec)                        120
    IRRfrequency (sec)                        60
    Voice Gateway
    Alternate Gatekeeper (Priority 0)
    Alternate Gatekeeper (Priority 1)
    Alternate Gatekeeper (Priority 2)



                  SAVE                                       CANCEL

Use <Space> to select
```

➤ Select **Type of Registration**: *limited to user table*.

➤ Press **SAVE**.

Activating gatekeeper

Proceed as follows to activate the gatekeeper with the settings already made:

➤ Go to ***VoIP*** ➧ ***Gatekeeper Settings***.

➤ Select **Gatekeeper**: *running*.

➤ Press **SAVE**.

The gatekeeper is now active.

Configuring NetMeeting (Home Office)

The settings you must make for NetMeeting at the home office to enable NetMeeting to register with the gatekeeper at the head office are described below.

Make sure Microsoft NetMeeting is properly installed on your PC before you start.

Entering gatekeeper for NetMeeting

Proceed as follows to enter the gatekeeper for your Microsoft NetMeeting:

- Start NetMeeting on your PC.
- Go to **Tools** ➧ **Options**.
- Click **Advanced Calling**.
- Activate the control box **Use a gatekeeper to place calls** and enter the IP address of the gatekeeper, e.g. ***192.168.1.254***. You can also use a DNS name instead of the IP address.
- Activate the control box **Log on using my account name** and enter the desired name, e.g. ***kk_netmeeting***.
- Close both windows by pressing **OK**.
- Restart NetMeeting.

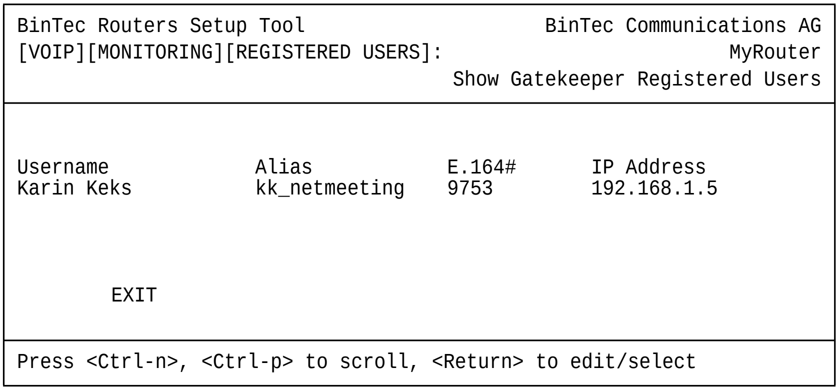
  NetMeeting registers with the gatekeeper.

2.3.2 Checking the Registration

To check if Microsoft NetMeeting at the home office has successfully registered with the gatekeeper of your BinTec router at the head office, you as administrator should proceed as follows:

- Go to ***VoIP*** ➧ ***MONITORING*** ➧ ***REGISTERED USERS*** in the Setup Tool menu.

If NetMeeting is properly registered in our example, you will see the following:

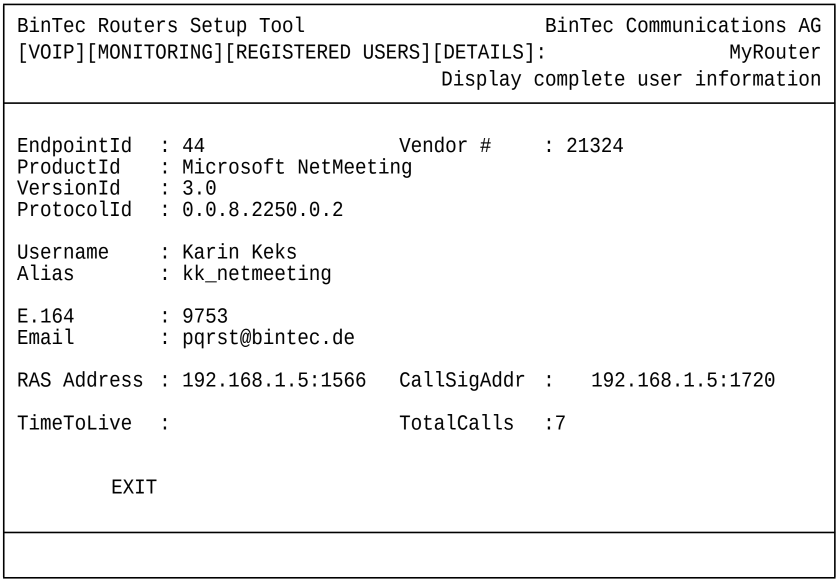


```
BinTec Routers Setup Tool                        BinTec Communications AG
[VOIP][MONITORING][REGISTERED USERS]:                            MyRouter
                                     Show Gatekeeper Registered Users


Username            Alias           E.164#       IP Address
Karin Keks          kk_netmeeting   9753         192.168.1.5




        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can obtain detailed information for this entry:

➤ Select the entry and press **Return**.

A detailed list is displayed:



```
BinTec Routers Setup Tool                        BinTec Communications AG
[VOIP][MONITORING][REGISTERED USERS][DETAILS]:                   MyRouter
                                    Display complete user information

EndpointId   : 44                 Vendor #     : 21324
ProductId    : Microsoft NetMeeting
VersionId    : 3.0
ProtocolId   : 0.0.8.2250.0.2

Username     : Karin Keks
Alias        : kk_netmeeting

E.164        : 9753
Email        : pqrst@bintec.de

RAS Address  : 192.168.1.5:1566   CallSigAddr  :   192.168.1.5:1720

TimeToLive   :                    TotalCalls   :7


        EXIT
```

2.3.3 Making a Test Call to Head Office

To test if your NetMeeting at the home office can communicate with other NetMeeting users at the head office, set up a call to another NetMeeting user.

For example, call Erna Eiscreme with the alias ee_netmeeting and the telephone number 2468 (see figure B-2, page 48). She should be registered with the gatekeeper under this data. You can enter the telephone number, the user name or the alias for setting up the call.

Proceed as follows to set up a call to Erna Eiscreme:

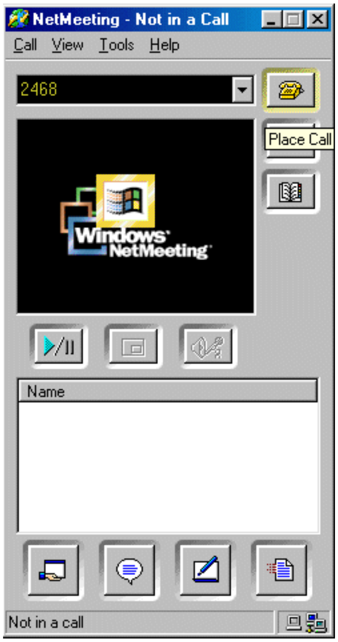


Figure B-3: Setting up a call with NetMeeting

- Enter the desired telephone number in the NetMeeting you have already started: *2468*.
- You can also enter the user name or alias as an alternative to the telephone number.

- Click the **Place Call** button to the right of the input field (i.e. the button with the telephone symbol).

  The call is set up.

Communication is only possible in both directions if NetMeeting has already been started at the home office and has registered with the gatekeeper at the head office. This means: the employee at the home office can call a colleague at the head office using NetMeeting and everyone at the head office can also communicate with the colleague at the home office using Microsoft NetMeeting or an IP telephone.

Once the connection between the home office and head office exists, it remains open until Microsoft NetMeeting is closed at the home office. (An open connection is necessary for the **Time to Live (sec)** parameter (see table A-5, page 30).

We recommend that you use flat-rate Internet access.

2.3.4 Displaying Calls

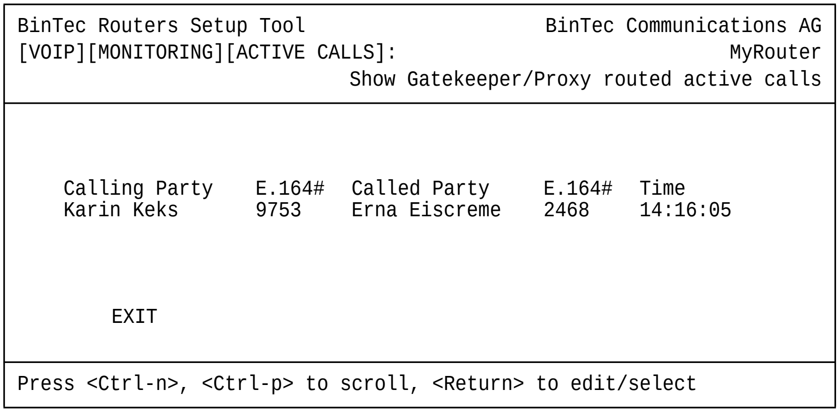
You as administrator of the BinTec router can display both the currently active calls and the calls already cleared.

Active calls Proceed as follows to display the active calls:

- Go to ***VoIP*** ➧ ***MONITORING*** ➧ ***ACTIVE CALLS***.

  The currently active calls are displayed.

In our example, Karin Keks and Erna Eiscreme are currently talking:

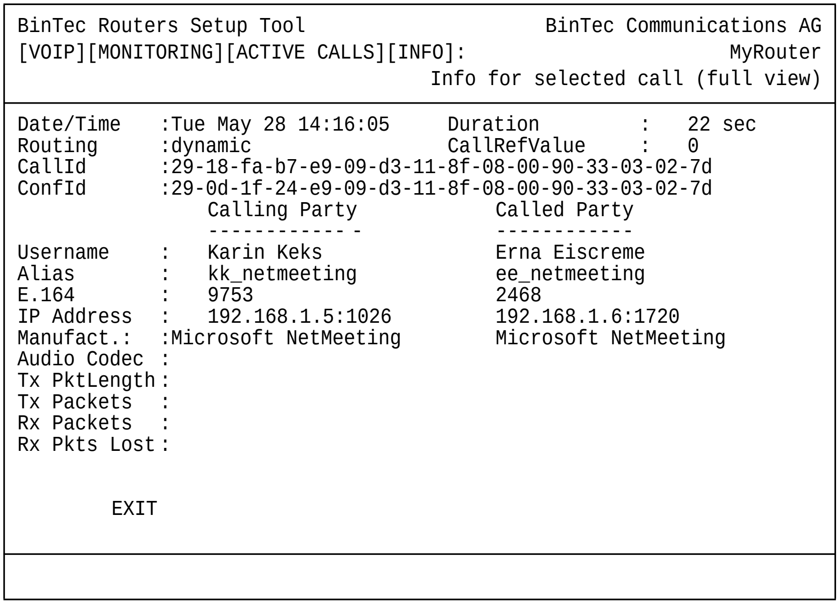


```
BinTec Routers Setup Tool                     BinTec Communications AG
[VOIP][MONITORING][ACTIVE CALLS]:                             MyRouter
                             Show Gatekeeper/Proxy routed active calls



    Calling Party    E.164#  Called Party     E.164#  Time
    Karin Keks       9753    Erna Eiscreme    2468    14:16:05




        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can obtain detailed information for each call:

➤ Select the desired entry and press **Return**.

A detailed list is displayed:



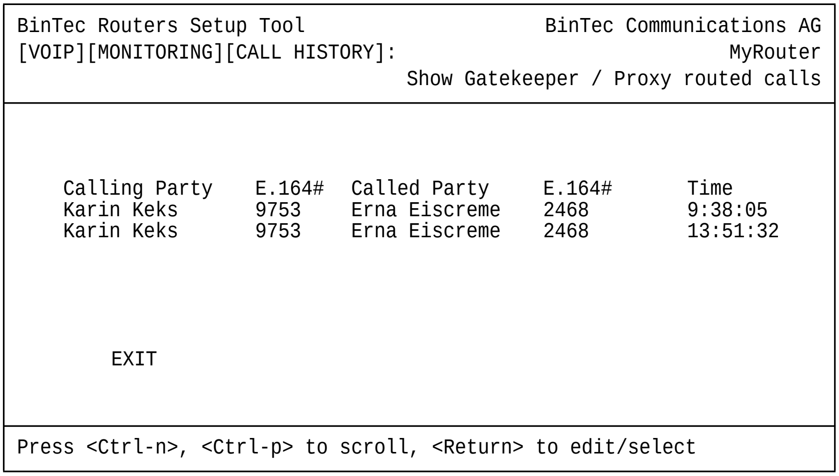
```
BinTec Routers Setup Tool                     BinTec Communications AG
[VOIP][MONITORING][ACTIVE CALLS][INFO]:                       MyRouter
                                    Info for selected call (full view)

Date/Time   :Tue May 28 14:16:05     Duration        :   22 sec
Routing     :dynamic                 CallRefValue    :   0
CallId      :29-18-fa-b7-e9-09-d3-11-8f-08-00-90-33-03-02-7d
ConfId      :29-0d-1f-24-e9-09-d3-11-8f-08-00-90-33-03-02-7d
                Calling Party            Called Party
                ------------ -           ------------
Username    :   Karin Keks               Erna Eiscreme
Alias       :   kk_netmeeting            ee_netmeeting
E.164       :   9753                     2468
IP Address  :   192.168.1.5:1026         192.168.1.6:1720
Manufact.:  :Microsoft NetMeeting        Microsoft NetMeeting
Audio Codec :
Tx PktLength:
Tx Packets  :
Rx Packets  :
Rx Pkts Lost:


        EXIT

```

Cleared calls Proceed as follows to display calls already cleared:

➤ Go to ***VoIP*** ➧ ***Monitoring*** ➧ ***Call History***.

The calls already cleared are displayed.

In our example, there were two meetings, one in the morning, the other in the afternoon:



```
BinTec Routers Setup Tool                           BinTec Communications AG
[VOIP][MONITORING][CALL HISTORY]:                                   MyRouter
                                  Show Gatekeeper / Proxy routed calls



    Calling Party     E.164#  Called Party     E.164#       Time
    Karin Keks        9753    Erna Eiscreme    2468         9:38:05
    Karin Keks        9753    Erna Eiscreme    2468         13:51:32





        EXIT


Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can also obtain detailed information for each call:

➤ Select the desired entry and press **Return**.

A detailed list is displayed showing information such as who called who and for how long.

3 NetMeeting and DynDNS with a BinTec Router

3.1 Introduction

With a BinTec router, you can use Microsoft NetMeeting to communicate with another NetMeeting user over the Internet.

DynDNS Your router does not need a fixed IP address outside its LAN. The dynamic IP address is announced via the BinTec router function "Dynamic DNS" (DynDNS), if you have registered a host name for your router with a DynDNS provider and have configured your router accordingly. Detailed information about the "DynDNS" function can be found in **Release Notes 6.2.2**.

Your communication partner needs only a PC with Microsoft NetMeeting and an ISDN card, or another direct dialing in facility, e.g. T-DSL with modem and network card.

Procedure In this case, the initial operation, test and use of Microsoft NetMeeting is divided into four steps:

- Registering NetMeeting with the BinTec gatekeeper (section B, chapter 3.3.1, page 59)
- Checking the registration (section B, chapter 3.3.2, page 63)
- Making a test call (section B, chapter 3.3.3, page 64)
- Displaying calls (section B, chapter 3.3.4, page 66).

3.2 Requirements

The use of flat-rate Internet access is recommended for using NetMeeting.

For security reasons, BinTec Communications AG does not support the NetMeeting functions "Desktop Sharing" and "Whiteboard".

If you use NetMeeting together with the gatekeeper or proxy functionality, you cannot use the "Internet Locator Server" from Microsoft.

Availability of H.323 proxy and H.323 gatekeeper

You can use Microsoft NetMeeting together with the gatekeeper and proxy functionality of a BinTec X-Generation router with Software Release 6.2.1 or later. If you use **X1000**, **X1200** or **X3200** routers, the IPSec security solution and the gatekeeper or proxy are not available at the same time.

Proceed as follows to make sure your router has the gatekeeper and proxy functionality:

Router type

➤ Check which router type you are using.

X1000, X1200, X3200

For **X1000**, **X1200** and **X3200** routers:

➤ Check if your router is operated with the IPSec system software.

If you have Software Release 6.2.1 with IPSec:

➤ Install Software Release 6.2.1 without IPSec or purchase a BinTec X-Generation router that provides the IPSec and gatekeeper or proxy functionality at the same time.

If you have Software Release 6.2.1 without IPSec, the gatekeeper and proxy functionality is available.

Other X-Generation routers

For all other X-Generation routers:

➤ Check if Software Release 6.2.1 is installed on your router. If your router has an older software version, carry out a software update. You will find information about a software update in the User's Guide for your BinTec router.

3.3 Configuration and Monitoring

The following diagram shows two PCs dialed in to the Internet. One of them is connected to the Internet via a BinTec router:

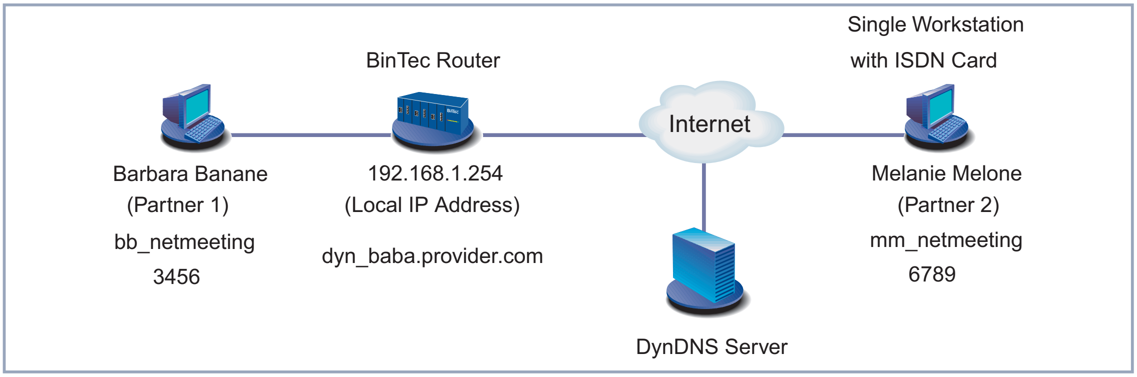


Figure B-4: Two PCs dialed in to the Internet

3.3.1 Registering NetMeeting with the BinTec Gatekeeper

Summary "Partner 1" and "partner 2" (see figure B-4, page 59) must be registered with the BinTec gatekeeper before they can communicate with each other. The relevant requirements must be fulfilled for both NetMeeting and the BinTec router:

- The administrator of the BinTec router must assign a **Username** to both partners and enter them in the ***USER TABLE*** of the gatekeeper. He must ensure that these entries are used for registration.
- NetMeeting must be suitably configured for "partner 1" and "partner 2" (see figure B-4, page 59) so that the respective NetMeeting registers with the gatekeeper of the BinTec router.

Procedure The administrator of the BinTec router activates the proxy to ensure that NetMeeting of "partner 2" has access to the network of "partner 1".

The administrator enters the desired data of the two communication partners in the ***USER TABLE*** of the gatekeeper.

Both partners enter in their own NetMeeting only the alias and the gatekeeper with which NetMeeting is to register. The actual registration takes place automatically.

You can also use other H.323-capable endpoints instead of NetMeeting if they are registered with the BinTec gatekeeper.

Configuring Your BinTec Router

The settings you as administrator must make on your BinTec router to enable NetMeeting to dial in to your network from "outside" are described below.

Activating a proxy

To configure the proxy of your BinTec router for access with NetMeeting, proceed as follows in the Setup Tool:

- Go to ***VoIP*** ➡ ***Proxy Settings***.
- Leave the default settings.
- Select **Proxy**: *running*.
- Press **SAVE**.
  The proxy is activated.

Entering data for NetMeeting in user table

Proceed as follows to enter the data for NetMeeting of "partner 1" and "partner 2" in the ***User Table*** of your BinTec gatekeeper:

- Go to ***VoIP*** ➡ ***Gatekeeper Settings*** ➡ ***User Table*** ➡ **ADD**.
- Enter **Username**, e.g. ***Barbara Banane***.
- Enter **Alias**, e.g. ***bb_netmeeting***.
- Enter **E.164**, e.g. ***3456***.
- Enter **E-Mail**, if applicable, e.g. ***barban@bintec.de***.
- Skip **IP Address**.
- Press **SAVE**.
  You change to the ***VoIP*** ➡ ***Gatekeeper Settings*** ➡ ***User Table*** menu.
- Add a new entry with **ADD**.

- Enter **Username**, e.g. ***Melanie Melone***.
- Enter **Alias**, e.g. ***mm_netmeeting***.
- Enter **E.164**, e.g. ***6789***.
- Enter **E-Mail**, if applicable, e.g. ***melmel@bintec.de***.
- Skip **IP Address**.
- Press **SAVE**.

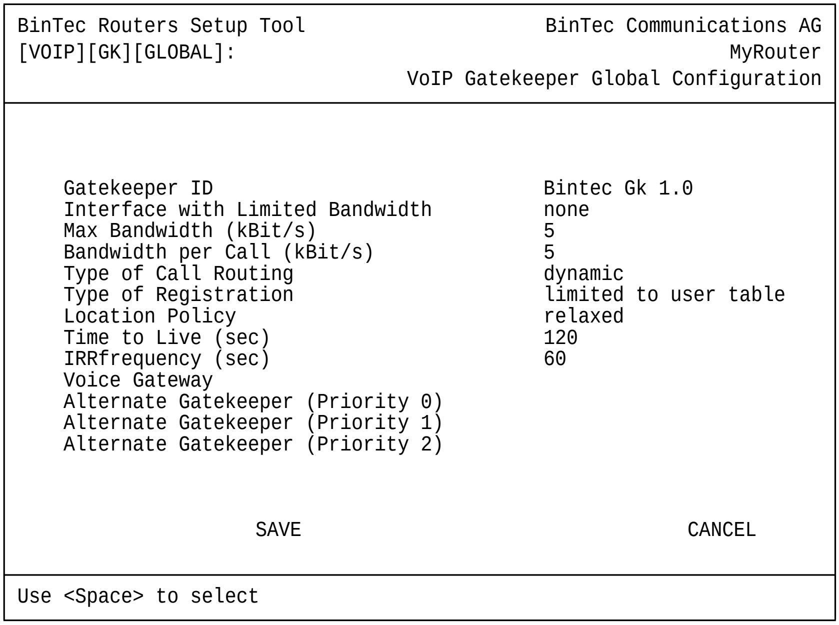
  The entries are temporarily saved and activated.

Setting gatekeeper parameters

Proceed as follows to make sure that endpoints can only register if they are entered in the ***User Table***:

- Go to ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings***.

You see the following menu:



```
BinTec Routers Setup Tool                            BinTec Communications AG
[VOIP][GK][GLOBAL]:                                                  MyRouter
                                         VoIP Gatekeeper Global Configuration


    Gatekeeper ID                              Bintec Gk 1.0
    Interface with Limited Bandwidth           none
    Max Bandwidth (kBit/s)                     5
    Bandwidth per Call (kBit/s)                5
    Type of Call Routing                       dynamic
    Type of Registration                       limited to user table
    Location Policy                            relaxed
    Time to Live (sec)                         120
    IRRfrequency (sec)                         60
    Voice Gateway
    Alternate Gatekeeper (Priority 0)
    Alternate Gatekeeper (Priority 1)
    Alternate Gatekeeper (Priority 2)


                     SAVE                                  CANCEL

Use <Space> to select
```

- Select **Type of Registration**: *limited to user table*.
- Leave the remaining parameters set to the default settings.
- Press **SAVE**.

Activating gatekeeper Proceed as follows to activate the gatekeeper with the settings already made:

- ➤ Go to ***VoIP*** ➧ ***GATEKEEPER SETTINGS***.
- ➤ Select **Gatekeeper**: *running*.
- ➤ Press **SAVE**.

  The gatekeeper is now active.

Configuring NetMeeting

The settings to be made by "partner 1" and "partner 2" in the NetMeeting program so that the respective NetMeeting can register with the BinTec gatekeeper are described below.

Make sure Microsoft NetMeeting is properly installed on your PC before you start.

Entering gatekeeper for NetMeeting ("partner 1") Proceed as follows to enter the BinTec gatekeeper for your Microsoft NetMeeting as "partner 1":

- ➤ Start NetMeeting on the PC.
- ➤ Go to **Tools** ➧ **Options**.
- ➤ Click **Advanced Calling**.
- ➤ Activate the control box **Use a gatekeeper to place calls** and enter the IP address of the BinTec gatekeeper, e.g. ***192.168.1.254***.
- ➤ Activate the control box **Log on using my account name** and enter the desired name, e.g. ***bb_netmeeting***.
- ➤ Close both windows by pressing **OK**.
- ➤ Restart NetMeeting.

  NetMeeting of "partner 1" registers with the gatekeeper.

Entering gatekeeper for NetMeeting ("partner 2") Proceed as follows to enter the BinTec gatekeeper for your Microsoft NetMeeting as "partner 2":

- ➤ Start NetMeeting on the PC.
- ➤ Go to **Tools** ➧ **Options**.
- ➤ Click **Advanced Calling**.

- ➤ Activate the control box **Use a gatekeeper to place calls** and enter the DynDNS name of the BinTec gatekeeper, e.g. ***dyn_baba.provider.com***.
- ➤ Activate the control box **Log on using my account name** and enter the desired name, e.g. ***mm_netmeeting***.
- ➤ Close both windows by pressing **OK**.
- ➤ Restart NetMeeting.

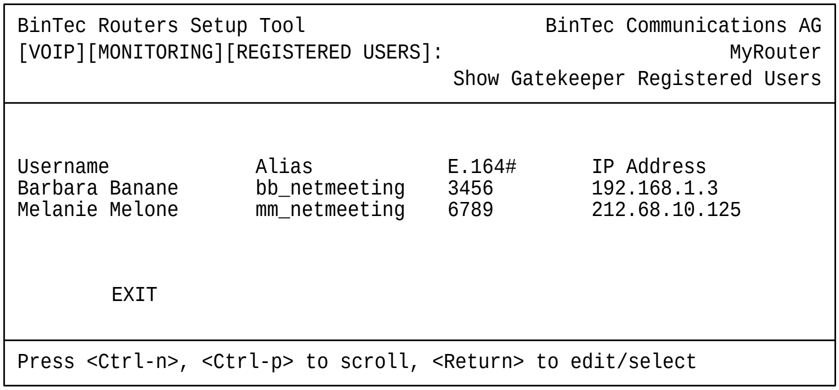
  NetMeeting of "partner 2" registers with the gatekeeper.

3.3.2 Checking the Registration

As administrator of the BinTec router, proceed as follows to check that the Microsoft NetMeeting registration of "partner 1" and "partner 2" with the gatekeeper of your BinTec router was successful:

- ➤ Go to ***VoIP*** ➧ ***Monitoring*** ➧ ***Registered Users*** in the Setup Tool menu.

Once NetMeeting is properly registered for "partner 1" and "partner 2" in our example, you see the following:

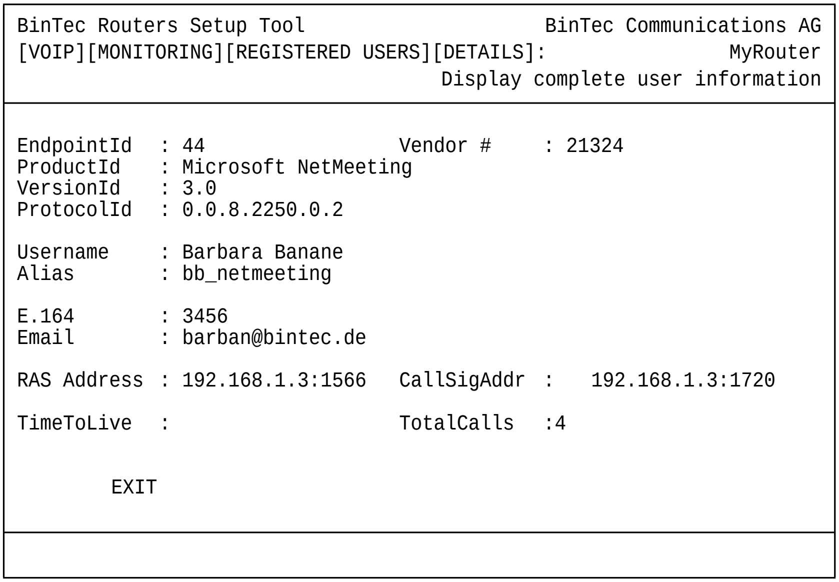


```
BinTec Routers Setup Tool                        BinTec Communications AG
[VOIP][MONITORING][REGISTERED USERS]:                            MyRouter
                                        Show Gatekeeper Registered Users


Username             Alias            E.164#      IP Address
Barbara Banane       bb_netmeeting    3456        192.168.1.3
Melanie Melone       mm_netmeeting    6789        212.68.10.125


        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can obtain detailed information for each entry:

- ➤ For example, select the first entry and press **Return**.

A detailed list is displayed:



```
BinTec Routers Setup Tool                              BinTec Communications AG
[VOIP][MONITORING][REGISTERED USERS][DETAILS]:                         MyRouter
                                             Display complete user information


EndpointId   : 44                  Vendor #     : 21324
ProductId    : Microsoft NetMeeting
VersionId    : 3.0
ProtocolId   : 0.0.8.2250.0.2

Username     : Barbara Banane
Alias        : bb_netmeeting

E.164        : 3456
Email        : barban@bintec.de

RAS Address  : 192.168.1.3:1566   CallSigAddr  :   192.168.1.3:1720

TimeToLive   :                     TotalCalls   :4


        EXIT
```

3.3.3 Making a Test Call

To check whether "partner 1" can communicate with "partner 2", "partner 1" can set up a call to "partner 2".

As "partner 1" call Melanie Melone with the alias mm_netmeeting and the telephone number 6789 (see figure B-4, page 59). You can enter the telephone number, the user name or the alias for setting up the call.

Proceed as follows to set up a call to Melanie Melone:

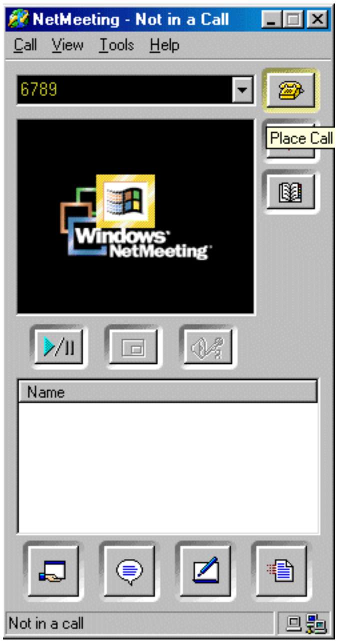


Figure B-5: Setting up a call with NetMeeting

- Enter the desired telephone number in the NetMeeting you have already started: *6789*.
- You can also enter the user name or alias as an alternative to the telephone number.
- Click the **Place Call** button to the right of the input field (i.e. the button with the telephone symbol).

  The call is set up.

Communication is possible in both directions. This means: it is immaterial if "partner 1" calls "partner 2" or "partner 2" calls "partner 1", the call is always set up without delay.

Once the connection exists between the two communication partners, it remains open, as an open connection is necessary for the **Time to Live (sec)** parameter (see table A-5, page 30).

We recommend that you use flat-rate Internet access.

3.3.4 Displaying Calls

You as administrator of the BinTec router can display both the currently active calls and the calls already cleared.

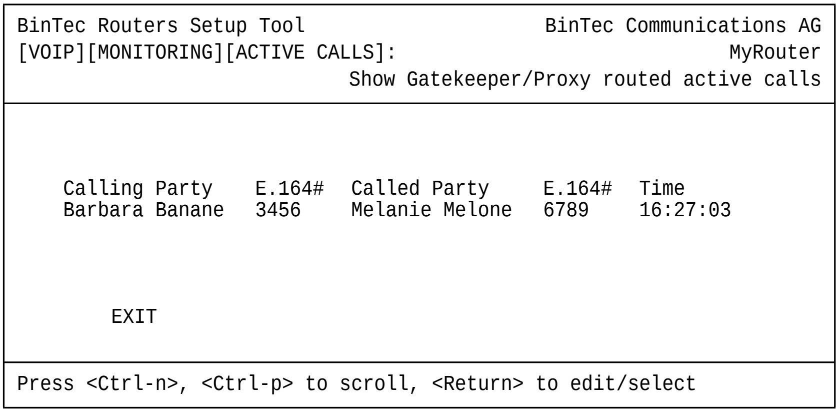
Active calls

Proceed as follows to display the active calls:

➤ Go to ***VoIP*** ➧ ***Monitoring*** ➧ ***Active Calls***.

The currently active calls are displayed.

In our example, Barbara Banane has just called Melanie Melone:

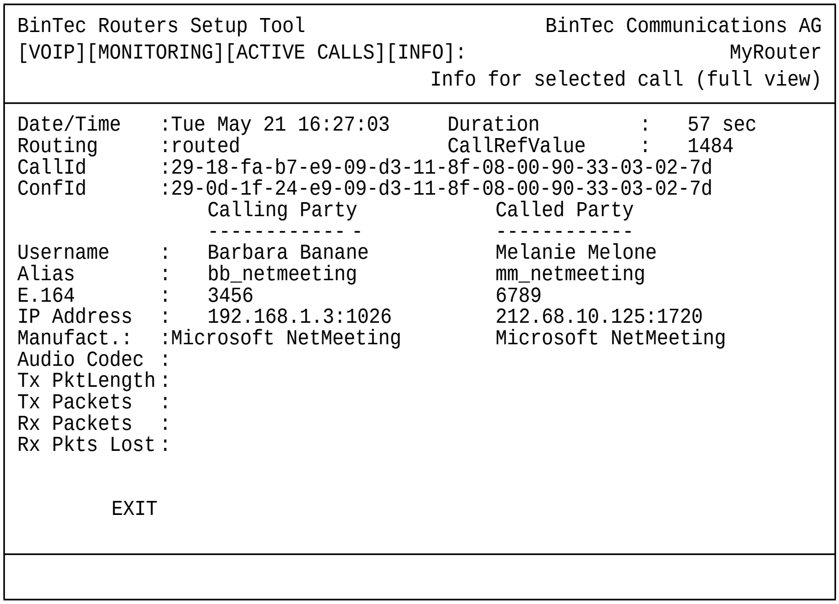


```
BinTec Routers Setup Tool                     BinTec Communications AG
[VOIP][MONITORING][ACTIVE CALLS]:                             MyRouter
                             Show Gatekeeper/Proxy routed active calls



    Calling Party    E.164#  Called Party     E.164#  Time
    Barbara Banane   3456    Melanie Melone   6789    16:27:03




        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can obtain detailed information for each call:

➤ Select the desired entry and press **Return**.

A detailed list is displayed:



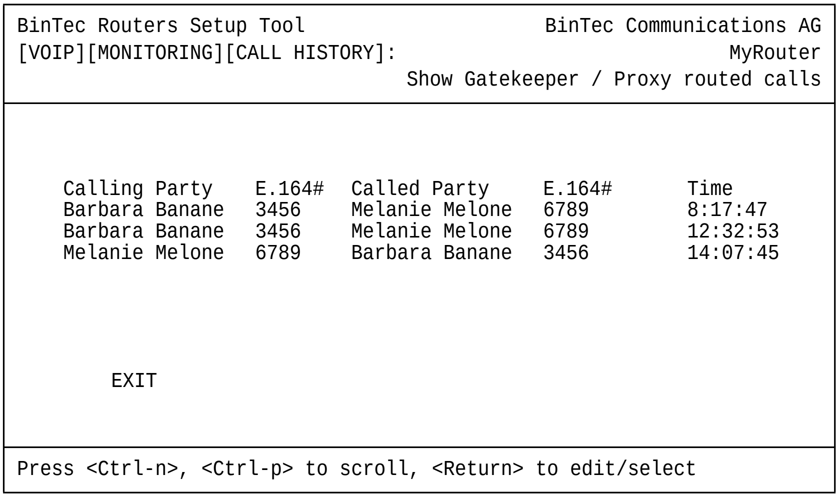
```
BinTec Routers Setup Tool                            BinTec Communications AG
[VOIP][MONITORING][ACTIVE CALLS][INFO]:                              MyRouter
                                          Info for selected call (full view)

Date/Time    :Tue May 21 16:27:03      Duration        :    57 sec
Routing      :routed                   CallRefValue    :    1484
CallId       :29-18-fa-b7-e9-09-d3-11-8f-08-00-90-33-03-02-7d
ConfId       :29-0d-1f-24-e9-09-d3-11-8f-08-00-90-33-03-02-7d
                 Calling Party             Called Party
                 ------------ -            ------------
Username     :   Barbara Banane            Melanie Melone
Alias        :   bb_netmeeting             mm_netmeeting
E.164        :   3456                      6789
IP Address   :   192.168.1.3:1026          212.68.10.125:1720
Manufact.:   :Microsoft NetMeeting         Microsoft NetMeeting
Audio Codec  :
Tx PktLength :
Tx Packets   :
Rx Packets   :
Rx Pkts Lost :


        EXIT
```

Cleared calls Proceed as follows to display calls already cleared:

➤ Go to ***VoIP*** ➧ ***Monitoring*** ➧ ***Call History***.

The calls already cleared are displayed.

In our example, Barbara Banane and Melanie Melone have spoken to each other three times:



```
BinTec Routers Setup Tool                     BinTec Communications AG
[VOIP][MONITORING][CALL HISTORY]:                             MyRouter
                                  Show Gatekeeper / Proxy routed calls



    Calling Party    E.164#   Called Party     E.164#      Time
    Barbara Banane   3456     Melanie Melone   6789        8:17:47
    Barbara Banane   3456     Melanie Melone   6789        12:32:53
    Melanie Melone   6789     Barbara Banane   3456        14:07:45





        EXIT


Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can also obtain detailed information for each call:

➤ Select the desired entry and press **Return**.

A detailed list is displayed showing information such as who called who and for how long.

4 NetMeeting and DynDNS with Two BinTec Routers

4.1 Introduction

As user of a BinTec router, you can use Microsoft NetMeeting to communicate over the Internet with another NetMeeting user also reachable via a BinTec router.

DynDNS

Neither of the BinTec routers needs a fixed IP address outside its LAN. The dynamic IP addresses are announced via the BinTec router function "Dynamic DNS" (DynDNS), if you have registered a host name for each of the two routers with a DynDNS provider and have configured the routers accordingly. Detailed information about the "DynDNS" function can be found in **Release Notes 6.2.2**.

Procedure

In this case, the initial operation, test and use of Microsoft NetMeeting is divided into four steps:

- Registering NetMeeting with the BinTec gatekeeper (section B, chapter 4.3.1, page 71)
- Checking the registration (section B, chapter 4.3.2, page 76)
- Making a test call (section B, chapter 4.3.3, page 77)
- Displaying calls (section B, chapter 4.3.4, page 79).

4.2 Requirements

The use of flat-rate Internet access is recommended for using NetMeeting.

For a special case, which you will also find in this scenario (see "Setting gatekeeper parameters", page 73 and "Making a Test Call", page 77), you do not need flat-rate access to the Internet.

For security reasons, BinTec Communications AG does not support the NetMeeting functions "Desktop Sharing" and "Whiteboard".

If you use NetMeeting together with the gatekeeper or proxy functionality, you cannot use the "Internet Locator Server" from Microsoft.

Availability of H.323 proxy and H.323 gatekeeper

You can use Microsoft NetMeeting together with the gatekeeper and proxy functionality of a BinTec X-Generation router with Software Release 6.2.1 or later. If you use **X1000**, **X1200** or **X3200** routers, the IPSec security solution and the gatekeeper or proxy are not available at the same time.

Proceed as follows to make sure your router has the gatekeeper and proxy functionality:

Router type

➤ Check which router type you are using.

X1000, X1200, X3200

For **X1000**, **X1200** and **X3200** routers:

➤ Check if your router is operated with the IPSec system software.

If you have Software Release 6.2.1 with IPSec:

➤ Install Software Release 6.2.1 without IPSec or purchase a BinTec X-Generation router that provides the IPSec and gatekeeper or proxy functionality at the same time.

  If you have Software Release 6.2.1 without IPSec, the gatekeeper and proxy functionality is available.

Other X-Generation routers

For all other X-Generation routers:

➤ Check if Software Release 6.2.1 is installed on your router. If your router has an older software version, carry out a software update. You will find information about a software update in the User's Guide for your BinTec router.

4.3 Configuration and Monitoring

The following diagram shows two PCs, each dialed in to the Internet via a BinTec router:

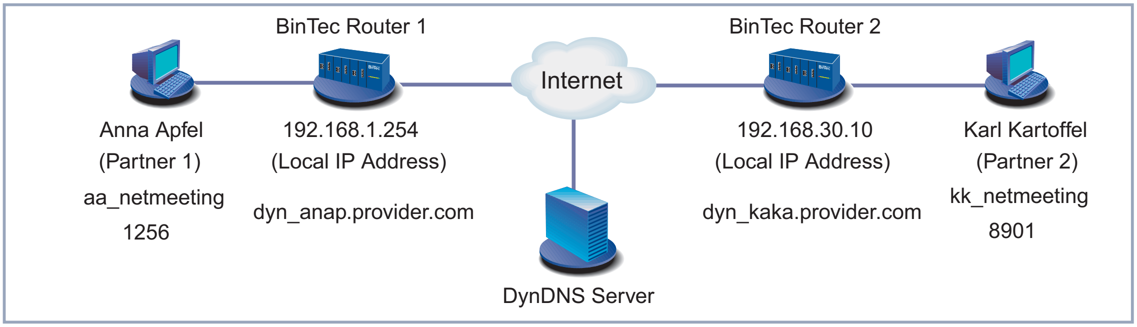


Figure B-6: Communication of two PCs over BinTec router and Internet

4.3.1 Registering NetMeeting with the BinTec Gatekeeper

Summary

"Partner 1" and "partner 2" must be registered with the gatekeeper of their respective BinTec router before they can communicate with each other. The relevant requirements must be fulfilled for both NetMeeting and the BinTec router:

- The administrator of the respective BinTec router must assign a **Username** to "his" user and enter it in the ***USER TABLE*** of the gatekeeper. He must ensure that this entry is used for registration.
- "Partner 1" and "partner 2" must configure their NetMeeting program so that NetMeeting of "partner 1" is registered with the gatekeeper of "BinTec

router 1" and NetMeeting of "partner 2" is registered with the gatekeeper of "BinTec router 2".

- The two gatekeepers must "know" each other.

Procedure

The administrators of the BinTec routers activate the proxy to ensure that the far side obtains access to their network.

Each administrator enters the desired data of "his" user in the ***User Table*** of his gatekeeper.

Each user enters in his NetMeeting only the alias and the gatekeeper with which NetMeeting is to register. The actual registration takes place automatically.

To ensure that each user "knows" of the existence of the other, both administrators enter the gatekeeper of the "other end" as alternative gatekeeper in their BinTec routers.

You can also use other H.323-capable endpoints instead of NetMeeting if they are registered with the BinTec gatekeeper.

Configuring Your BinTec Router (Administrator)

The settings you as administrator must make on your BinTec router are described below.

Activating a proxy

To configure the proxy of your BinTec router for access with NetMeeting, proceed as follows in the Setup Tool:

➤ Go to ***VoIP*** ➧ ***Proxy Settings***.

➤ Leave the default settings.

➤ Select **Proxy**: *running*.

➤ Press **SAVE**.

The proxy is activated.

Entering data for NetMeeting in user table ("partner 1")

As administrator of "BinTec router 1", proceed as follows to enter the data for NetMeeting of "partner 1" in the ***User Table*** of your gatekeeper:

➤ Go to ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table*** ➧ **ADD**.

- Enter **Username**, e.g. ***Anna Apfel***.
- Enter **Alias**, e.g. ***aa_netmeeting***.
- Enter **E.164**, e.g. ***1256***.
- Enter **E-Mail**, if applicable, e.g. ***annapf@bintec.de***.
- Skip **IP Address**.
- Press **SAVE**.

  The entries are temporarily saved and activated.

Entering data for NetMeeting in user table ("partner 2")

As administrator of "BinTec router 2", proceed as follows to enter the data for NetMeeting of "partner 2" in the ***User Table*** of your gatekeeper:

- Enter **Username**, e.g. ***Karl Kartoffel***.
- Enter **Alias**, e.g. ***kk_netmeeting***.
- Enter **E.164**, e.g. ***8901***.
- Enter **E-Mail**, if applicable, e.g. ***karkar@bintec.de***.
- Skip **IP Address**.
- Press **SAVE**.

  The entries are temporarily saved and activated.

Setting gatekeeper parameters

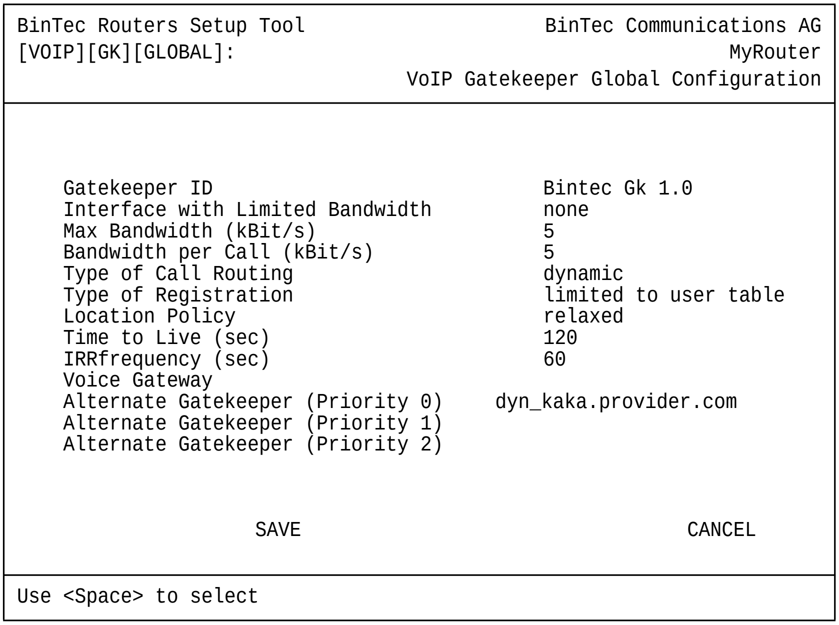
How you as administrator of "BinTec router 1" ensure that endpoints can only register if they are entered in the ***User Table*** and how you enter the alternative gatekeeper are described below. The administrator of "BinTec router 2" must carry out the same procedure at his router.

> You do not need to enter an alternative gatekeeper if you use an address with the format name@DynDNSname for NetMeeting for reaching your communication partner, e.g. ***karl@dyn_kaka.provider.com*** (see figure B-6, page 71 and "Making a Test Call", page 77).

Proceed as follows for "BinTec router 1":

- Go to ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings***.

You see the following menu:



```
BinTec Routers Setup Tool                          BinTec Communications AG
[VOIP][GK][GLOBAL]:                                                MyRouter
                                   VoIP Gatekeeper Global Configuration


    Gatekeeper ID                             Bintec Gk 1.0
    Interface with Limited Bandwidth          none
    Max Bandwidth (kBit/s)                    5
    Bandwidth per Call (kBit/s)               5
    Type of Call Routing                      dynamic
    Type of Registration                      limited to user table
    Location Policy                           relaxed
    Time to Live (sec)                        120
    IRRfrequency (sec)                        60
    Voice Gateway
    Alternate Gatekeeper (Priority 0)     dyn_kaka.provider.com
    Alternate Gatekeeper (Priority 1)
    Alternate Gatekeeper (Priority 2)


                     SAVE                                  CANCEL

Use <Space> to select
```

- Select **Type of Registration**: *limited to user table*.
- Enter **Alternate Gatekeeper (Priority 0)**, e.g. ***dyn_kaka.provider.com***.
- Leave the remaining parameters set to the default settings.
- Press **SAVE**.

Activating gatekeeper

Proceed as follows to activate the gatekeeper with the settings already made:

- Go to ***VoIP*** ➧ ***GATEKEEPER SETTINGS***.
- Select **Gatekeeper**: *running*.
- Press **SAVE**.

  The gatekeeper is now active.

Configuring NetMeeting (PC User)

The settings you must make for the NetMeeting program to enable NetMeeting to register with the gatekeeper of the BinTec router are described below.

Make sure Microsoft NetMeeting is properly installed on your PC before you start.

Entering gatekeeper for NetMeeting ("partner 1")

Proceed as follows to enter the gatekeeper of "BinTec router 1" for your Microsoft NetMeeting as "partner 1" (see figure B-6, page 71):

- Start the NetMeeting program on your PC.
- Go to **Tools** ➧ **Options**.
- Click **Advanced Calling**.
- Activate the control box **Use a gatekeeper to place calls** and enter the IP address of the gatekeeper, e.g. ***192.168.1.254***.
- Activate the control box **Log on using my account name** and enter the desired name, e.g. ***aa_netmeeting***.
- Close both windows by pressing **OK**.
- Restart NetMeeting.

  NetMeeting of "partner 1" registers with the gatekeeper of "BinTec router 1".

Entering gatekeeper for NetMeeting ("partner 2")

Proceed as follows to enter the gatekeeper of "BinTec router 2" for your Microsoft NetMeeting as "partner 2" (see figure B-6, page 71):

- Start the NetMeeting program on your PC.
- Go to **Tools** ➧ **Options**.
- Click **Advanced Calling**.
- Activate the control box **Use a gatekeeper to place calls** and enter the IP address of the gatekeeper, e.g. ***192.168.30.10***.
- Activate the control box **Log on using my account name** and enter the desired name, e.g. ***kk_netmeeting***.
- Close both windows by pressing **OK**.
- Restart NetMeeting.

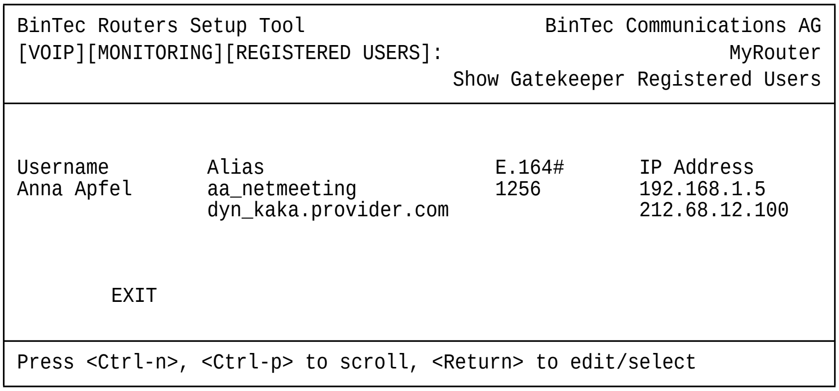
  NetMeeting of "partner 2" registers with the gatekeeper of "BinTec router 2".

4.3.2 Checking the Registration

The administrators of "BinTec router 1" and "BinTec router 2" check the registration with the gatekeeper as follows:

➤ Go to ***VoIP*** ➧ ***Monitoring*** ➧ ***Registered Users*** in the Setup Tool menu.

If NetMeeting of "partner 1" in our example is properly registered, you see the following (similar for NetMeeting of "partner 2"):

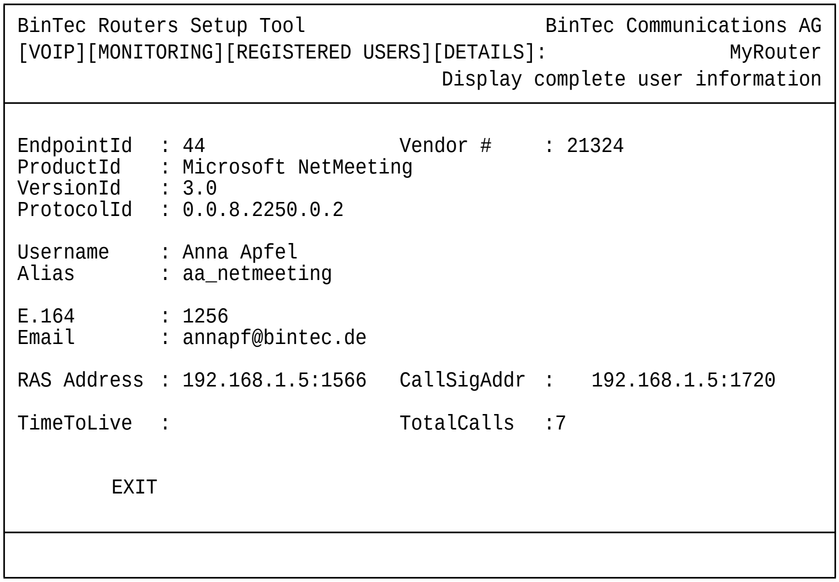


```
BinTec Routers Setup Tool                            BinTec Communications AG
[VOIP][MONITORING][REGISTERED USERS]:                                MyRouter
                                       Show Gatekeeper Registered Users


Username        Alias                    E.164#      IP Address
Anna Apfel      aa_netmeeting            1256        192.168.1.5
                dyn_kaka.provider.com                212.68.12.100



        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can obtain detailed information for each entry:

➤ Select an entry and press **Return**.

A detailed list is displayed:



```
BinTec Routers Setup Tool                                 BinTec Communications AG
[VOIP][MONITORING][REGISTERED USERS][DETAILS]:                            MyRouter
                                                      Display complete user information


EndpointId   : 44                  Vendor #     : 21324
ProductId    : Microsoft NetMeeting
VersionId    : 3.0
ProtocolId   : 0.0.8.2250.0.2

Username     : Anna Apfel
Alias        : aa_netmeeting

E.164        : 1256
Email        : annapf@bintec.de

RAS Address  : 192.168.1.5:1566   CallSigAddr  :   192.168.1.5:1720

TimeToLive   :                    TotalCalls   :7


        EXIT
```

4.3.3 Making a Test Call

To check whether "partner 1" can communicate with "partner 2", "partner 1" can set up a call to "partner 2".

As "partner 1" call Karl Kartoffel with the alias kk_netmeeting and the telephone number 8901 (see figure B-6, page 71). You can enter the telephone number, the user name or the alias for setting up the call.

You can also enter an address with the format name@DynDNSname, e.g. ***karl@dyn_kaka.provider.com***. The part after the @ symbol is interpreted as DynDNS name.

Proceed as follows to set up a call to Karl Kartoffel:

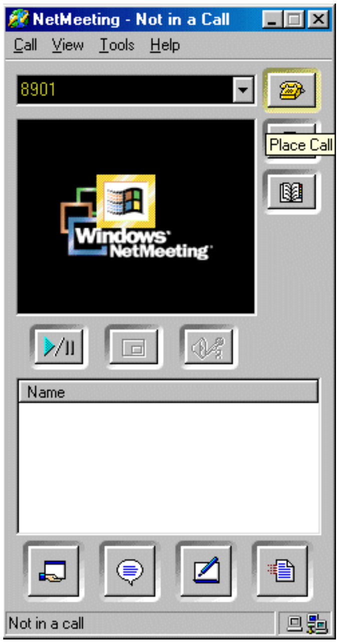


Figure B-7: Setting up a call with NetMeeting

- Enter the desired telephone number in the NetMeeting you have already started: *8901*.
- You can also enter the user name, the alias or an address with the format name@DynDNSname as an alternative to the telephone number.
- Click the **Place Call** button to the right of the input field (i.e. the button with the telephone symbol).

  The call is set up.

Communication is possible in both directions. This means: it is immaterial if "partner 1" calls "partner 2" or "partner 2" calls "partner 1", the call is always set up without delay.

If alternative gatekeepers are entered, the connection between the two routers always remains open, as an open connection is necessary for the **Time to Live (sec)** parameter (see table A-5, page 30).

We recommend that you use flat-rate Internet access.

4.3.4 Displaying Calls

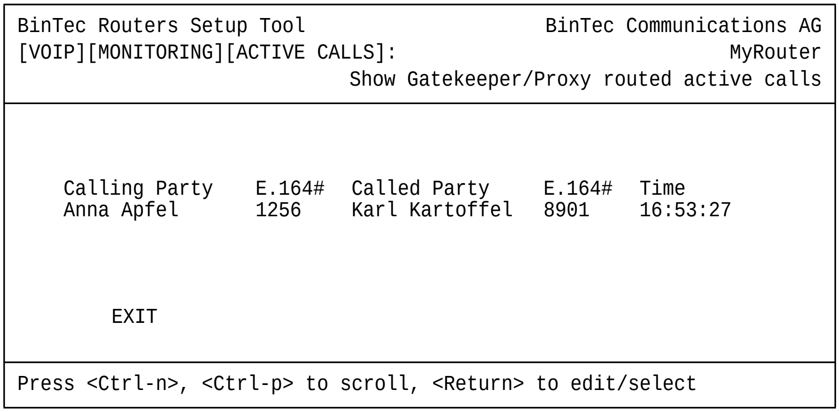
You as administrator of a BinTec router can display both the currently active calls and the calls already cleared.

Active calls Proceed as follows to display the active calls:

- Go to ***VoIP*** ➧ ***Monitoring*** ➧ ***Active Calls***.

  The currently active calls are displayed.

In our example, Anna Apfel has just called Karl Kartoffel:

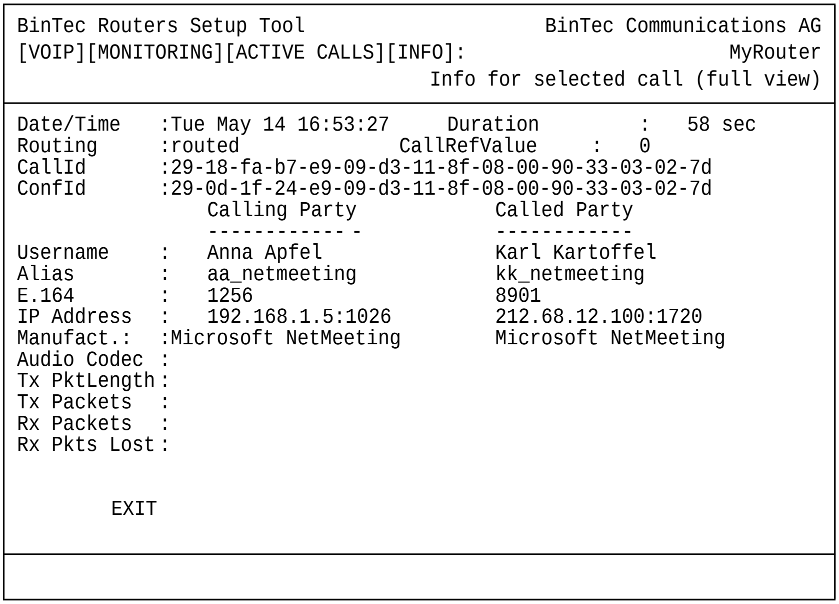


```
BinTec Routers Setup Tool                          BinTec Communications AG
[VOIP][MONITORING][ACTIVE CALLS]:                                  MyRouter
                           Show Gatekeeper/Proxy routed active calls



    Calling Party    E.164#   Called Party    E.164#   Time
    Anna Apfel       1256     Karl Kartoffel  8901     16:53:27



        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can obtain detailed information for each call:

- Select the desired entry and press **Return**.

A detailed list is displayed:



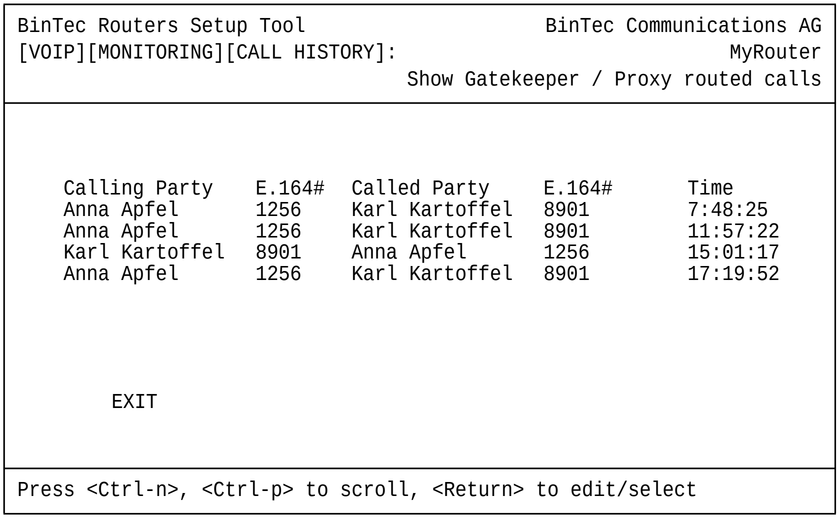
```
BinTec Routers Setup Tool                     BinTec Communications AG
[VOIP][MONITORING][ACTIVE CALLS][INFO]:                       MyRouter
                                    Info for selected call (full view)

Date/Time   :Tue May 14 16:53:27     Duration        :   58 sec
Routing     :routed             CallRefValue    :   0
CallId      :29-18-fa-b7-e9-09-d3-11-8f-08-00-90-33-03-02-7d
ConfId      :29-0d-1f-24-e9-09-d3-11-8f-08-00-90-33-03-02-7d
                Calling Party            Called Party
                ------------ -           ------------
Username    :   Anna Apfel               Karl Kartoffel
Alias       :   aa_netmeeting            kk_netmeeting
E.164       :   1256                     8901
IP Address  :   192.168.1.5:1026         212.68.12.100:1720
Manufact.:  :Microsoft NetMeeting        Microsoft NetMeeting
Audio Codec :
Tx PktLength:
Tx Packets  :
Rx Packets  :
Rx Pkts Lost:


        EXIT
```

Cleared calls Proceed as follows to display calls already cleared:

➤ Go to ***VoIP*** ➧ ***Monitoring*** ➧ ***Call History***.

The calls already cleared are displayed.

In our example, four calls were set up on this day:



```
BinTec Routers Setup Tool                       BinTec Communications AG
[VOIP][MONITORING][CALL HISTORY]:                               MyRouter
                                  Show Gatekeeper / Proxy routed calls


    Calling Party    E.164#   Called Party     E.164#       Time
    Anna Apfel       1256     Karl Kartoffel   8901         7:48:25
    Anna Apfel       1256     Karl Kartoffel   8901         11:57:22
    Karl Kartoffel   8901     Anna Apfel       1256         15:01:17
    Anna Apfel       1256     Karl Kartoffel   8901         17:19:52




        EXIT


Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

You can also obtain detailed information for each call:

➤ Select the desired entry and press **Return**.

A detailed list is displayed showing information such as who called who and for how long.