H.323

Juli 2002

Inhaltsverzeichnis 3

Referenz

1 Technologieübersicht

1.1 Einführung

H.323

Der H.323-Standard, ein Satz von Spezifikationen, ermöglicht Multimedia-Kommunikation über paketorientierte Netze in Echtzeit.

H.323 umfaßt das Format der Datenpakete, Kodier- und Kompressionsstandards, Signalisierung und Flußkontrolle.

H.32x-Standards

Das H.32x-Regelwerk enthält neben H.323 noch weitere Standards für die Übertragung von Sprache, Bildern und Daten. Es wurde von der International Telecommunications Union (ITU) erstellt, einer Organisation innerhalb der Vereinten Nationen, die sich um die Koordination von Telekommunikationsnetzen und -services rund um den Globus kümmert.

Die H.32x Familie setzt sich wie folgt zusammen:

Standard	Netzwerk
H.320	ISDN
H.321	ATM-basiertes Breitband-ISDN (B-ISDN)
H.322	LAN mit garantierter Dienstgüte
H.323	paketorientiertes Netz ohne garantierte Dienstgüte
H.324	analoges Telefonnetz bzw. Mobilfunk

Tabelle A-1: Standards der H.32x-Familie in Abhängigkeit von den verwendeten Netzen

Vorteile des H.323-Standards

Mit dem H.323-Standard können moderne Kommunikationsmittel und -möglichkeiten im gewohnten Arbeitsumfeld genutzt werden, z. B. ➤➤ **IP-Telefonie**, Videokonferenz (Microsoft NetMeeting u.a.), ➤➤ **Computer Telephonie Integration**, Desktop Sharing, ➤➤ **Unified Messaging**.

H.323 legt Spezifikationen für bereits existierende Infrastruktur fest. An bestehenden paketorientierten Netzen muß nichts geändert werden. H.323 ist auf al-

len IP-basierten Netzen wie ➤➤ **LAN**s, ➤➤ **WAN**s und dem Internet einsetzbar.

H.323 ist plattformunabhängig, d.h. unabhängig von der eingesetzten Hardware und vom verwendeten Betriebssystem.

Basierend auf H.323 können Lösungen verschiedener Hersteller miteinander kombiniert werden. Teilnehmer einer Videokonferenz können zum Beispiel unterschiedliche Hardware benutzen. Die Geräte sind kompatibel solange sie mit H.323 ausgerüstet sind.

H.323 und Firewall

Firmennetzwerke werden standardmäßig hinter einer ➤➤ **Firewall** verborgen, um firmeninterne, sensible Daten vor einem Zugriff von außen zu schützen.

Eine Videokonferenz oder IP-Telefone können jedoch nicht so ohne weiteres über eine Firewall hinweg betrieben werden. H.323 benötigt dynamisch wechselnde Ports, während eine Firewall normalerweise nur bestimmte Ports für bestimmte IP-Pakete öffnet. Ein H.323-Proxy löst dieses Problem.

H.323 bei BinTec

Mit dem Software Release 6.2.1 hat BinTec Communications AG die Funktionen H.323-Proxy und H.323-Gatekeeper in die Produkte der X-Generation integriert. Bei X1000, X1200 und X3200 sind Proxy bzw. Gatekeeper und die Sicherheitslösung IPSec nicht gleichzeitig verfügbar.

BinTecs Lösungen basieren auf dem Standard H.323, Version 2.

1.2 H.323-Grundlagen

Der H.323-Standard definiert, mit Hilfe welcher Komponenten und auf welche Art und Weise Sprache, Bilder und Daten über paketorientierte Netze transportiert werden.

Dieses Kapitel enthält folgende Informationen:

- welche Komponenten es im H.323-Netzwerk gibt.
- welche Protokolle für die Kommunikation benötigt werden.
- wozu die Komponenten bestimmte Protokolle verwenden.

- wie bei einem Ruf prinzipiell vorgegangen wird.

1.2.1 H.323-Komponenten

Ein Netz mit H.323-Standard enthält folgende Komponenten:

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

Diese Komponenten stellen innerhalb eines IP-Netzwerks Punkt-zu-Punkt und Punkt-zu-Mehrpunkt Verbindungen zur Verfügung, d.h. es ist möglich, mit nur einem Partner zu kommunizieren oder mit mehreren gleichzeitig.

Abgesehen von den oben genannten Komponenten können Zusatzkomponenten, wie z. B. Firewall und Proxy, in das Netz integriert sein, um Sicherheitsaspekte zu berücksichtigen, die der H.323-Standard nicht abdeckt.

Zone, Endgerät

Die Gesamtheit aller Terminals, Gateways und MCUs, die von einem einzigen Gatekeeper verwaltet wird, bezeichnet man als H.323-Zone. Eine Zone besteht aus mindestens einem Gatekeeper und einem Terminal und kann darüber hinaus noch weitere Terminals, Gateways und MCUs enthalten.

Terminals, Gateways und MCUs werden auch als Endgeräte bezeichnet.

Obwohl Gatekeeper, Gateway und MCU unterschiedliche logische Komponenten des H.323-Standards sind, können sie in einem einzigen Gerät realisiert sein.

Die einzelnen Komponenten haben im H.323-Netz bestimmte Eigenschaften und Aufgaben, die im folgenden näher erläutert werden.

Terminal

Ein H.323-Terminal ist ein Endgerät im Netzwerk, das Kommunikation zu einem anderen H.323-Terminal, einem Gateway oder einer Multipoint Control Unit zur Verfügung stellt.

Es handelt sich dabei entweder um einen Personal Computer (PC) oder um ein anderes Gerät, auf dem H.323-Protokolle (siehe "H.323-Protokolle", Seite 12) verfügbar sind. Zum Beispiel ist bei ➤➤ **Voice over IP** ein IP-Telefon ein Terminal.

H.323-Terminals können Sprache und optional auch Bilder und Daten in Echtzeit senden und empfangen. Der H.323 Standard stellt daher eine Grundlage für Telefonverbindungen über IP-Netze zur Verfügung.

Gateway

Ein Gateway kann als separates Gerät oder in Form von Software realisiert sein.

Ein H.323 Gateway verbindet ein H.323-Netz mit einem Netz eines anderen Standards, z. B. mit H.320 oder mit H.324 (siehe Tabelle A-1, Seite 6). Dazu werden die Protokolle übersetzt, die Formate konvertiert, die Kommunikationsprozeduren umgesetzt und Informationen zwischen den Netzen ausgetauscht.

Ein entsprechendes Gateway kann z. B. die Kommunikation zwischen einem H.323-Netz und dem ➤➤ **PSTN**-Netz ermöglichen, d.h. eine Verbindung von IP-Telefonen zu Telefonen im herkömmlichen Festnetz herstellen.

Soll die Kommunikation nur innerhalb eines einzigen Netzes erfolgen, z. B. innerhalb eines einzigen LANs, so ist kein Gateway erforderlich.

Gatekeeper

Der H.323-Gatekeeper ist immer als Software realisiert. Er ist das "Gehirn" des Netzes. Hier laufen die Verbindungen zusammen. Der Gatekeeper überwacht alle ➤➤ **Rufe**. Seine Hauptaufgaben sind die Zulassung eines Rufs und die Adreßauflösung in seiner Zone. Dazu müssen sich die Endgeräte, für die der Gatekeeper zuständig sein soll, bei ihm registrieren.

Terminals können zwar direkt kommunizieren, wenn jedoch ein Gatekeeper im Netz vorhanden ist, sollten die Terminals auf die Dienste dieses Gatekeepers zurückgreifen.

Der Gatekeeper stellt für registrierte Endgeräte wichtige Dienste zur Verfügung, ein Teil der Dienste ist auf jedem Gatekeeper vorhanden, ein Teil ist optional.

Gatekeeper-Funktionen

Folgende Gatekeeper-Funktionen sind immer verfügbar:

- Adreßübersetzung: Übersetzung eines Alias oder einer Telefonnummer (➤➤ **E.164**-Adresse) in eine IP-Adresse.
- Zugangskontrolle: Die Zugangskontolle zum LAN kann mittels Rufauthorisierung, über die Bandbreite oder mittels anderer Kriterien realisiert werden.
- Bandbreitenkontrolle: Die Bandbreitenkontrolle kann über das Bandbreitenmanagement nach vorher festgelegten Kriterien geregelt werden. Es ist z. B. möglich, die Anzahl der gleichzeitigen Verbindungen zu begrenzen. Dadurch wird die benutzte Bandbreite ebenfalls begrenzt und die übrige Bandbreite kann z. B. für Datenanwendungen benutzt werden.
- Zonenmanagement: Der Gatekeeper stellt obige Funktionen für die Terminals, Gateways und MCUs zur Verfügung, die in seiner Zone registriert sind.

Folgende Gatekeeper Funktionen sind optional:

- Ruf-Kontroll-Signalisierung: Bei einer Punkt-zu-Punkt-Vebindung routet der Gatekeeper entweder die Q.931-Pakete für die Rufkontrolle oder er weist die Endgeräts an, direkt miteinander zu kommunizieren.
- Ruf-Authorisierung: Der Gatekeeper kann die Anfrage eines Terminals oder Gateways nach einem Rufaufbau zurückweisen. Die Gründe können u.a. beschränkter Zugang zu oder von bestimmten Terminals oder Gateways sein oder beschränkter Zugang zu bestimmten Geräten zu bestimmten Zeiten.
- Bandbreitenmanagement: Der Gatekeeper kann den Rufaufbau eines Terminals zurückweisen, wenn die Bandbreite nicht ausreicht.
- Rufmanagement: Der Gatekeeper kann eine Liste mit den momentan aktiven Rufen bereithalten, um anzuzeigen, daß ein angerufenes Terminal besetzt ist oder um Informationen für das Bandbreitenmanagement zur Verfügung zu stellen.
- Routing-Service: Der Gatekeeper kann Rufe über verschiedene Wege routen, um eine gleichmäßige Auslastung des Netzes zu gewährleisten.

Multipoint Control Unit

Multipoint Control Units (MCUs) können als Software oder als Hardware realisiert sein. Eine MCU enthält immer einen Multipoint Controller (MC) und optional einen oder mehrere Multipoint Prozessoren (MP).

MCUs unterstützen eine Konferenz von drei oder mehr H.323-Terminals. Alle Terminals, die an der Konferenz teilnehmen, bauen eine Verbindung zur MCU auf. Die MCU steuert die Konferenz-Ressourcen und unterstützt die Aushandlung eines gemeinsamen Audio- und/oder Video-➤➤ **CODECs** (siehe auch "Audio", Seite 14 und "Video", Seite 15). Optional regelt die MCU auch den Datenstrom.

Es gibt zwei Arten von Multipoint-Konferenzen: zentralisierte und dezentralisierte. Auch eine Kombination aus beiden ist möglich. Meist werden zentralisierte Multipoint-Konferenzen realisiert; dafür benötigt man eine MCU. Dezentralisierte Multipoint-Konferenzen kommen ohne MCU aus, sind jedoch auf mehr Rechenleistung in den Endgeräten angewiesen.

Proxy-Server

Normalerweise wird jedes Firmennetz durch eine Firewall vor unauthorisierten Zugriffen von außen, z. B. aus dem Internet, geschützt.

Manche Kommunikationsdienste, wie z. B. IP-Telefonie oder Videokonferenz sind jedoch darauf angewiesen, die Firewall zu überwinden, damit Partner innerhalb und außerhalb des Firmennetzes miteinander kommunizieren können. Natürlich soll die Firewall durch diesen Prozess ihre Funktion nicht verlieren, die Daten des Firmennetzes sollen geschützt bleiben.

Ein H.323-Proxy-Server stellt in Kombination mit einer Firewall Sicherheitsfunktionen für obigen Fall zur Verfügung. Dazu wird der Datenverkehr, der an der Firewall ankommt, vom Proxy an der Firewall gespiegelt. Die Adressen werden vom Proxy umgesetzt. Der Proxy handelt als Stellvertreter, es wird jodoch keine direkte Verbindung zwischen z. B. dem Firmennetz und dem Internet hergestellt. Der Proxy gibt die Informationen an die jeweils andere Seite weiter, ohne jedoch preiszugeben, woher diese Informationen stammen.

Proxys schützen nicht nur die Daten, sie unterstützen auch die Reservierung von Bandbreite oder die Priorisierung des Datenverkehrs. Dadurch wird eine

angemessene Dienstgüte für H.323-Verbindungen sichergestellt, obwohl H.323-Netzwerke keine garantierte Dienstgüte besitzen.

Vorteile Die Vorteile eines Proxy sind:

- Es gibt keine direkten Verbindungen zwischen dem internen und dem externen System.
- Der Proxy kann umfassende Log-Files über den Datenverkehr und über spezielle Aktivitäten anlegen.
- Der Proxy unterstützt User-Level-Authentisierung.
- Der Proxy analysiert die Datenpakete.
- Bei neueren Proxys ist für Transparenz gesorgt, d.h. die ➤➤ **Clients** hinter der Firewall müssen weder "wissen", daß der Proxy vorhanden ist, noch brauchen sie spezielle Software, um mit dem externen Netz zu kommunizieren.

1.2.2 H.323-Protokolle

Protokolle regeln die Wechselwirkung zwischen den H.323-Komponenten.

Der H.323-Standard legt für die Übertragung von Sprache, Bildern und Daten fest:

- wie Endgeräte untereinander Verbindungen herstellen.
- wie Endgeräte einen Pool aus Audio-, Video- und Datenformaten aushandeln, den sie verwenden wollen.
- wie Sprache, Bilder und Daten formatiert und über das Netz gesendet werden.
- wie Sprache, Bilder und Daten synchronisiert werden.
- wie Endgeräte mit ihren zuständigen Gatekeepern kommunizieren.

Je nach Anwendung werden unterschiedliche Gruppen von Protokollen aus dem H.323-Standard benötigt.

H.323 nutzt die beiden Transportprotokolle ➤➤ **TCP** und ➤➤ **UDP**, abhängig davon, was übertragen werden soll.

Folgende Protokolle sind im H.323-Standard definiert. Ein Teil ist in H.323-Netzen immer vorhanden (verpflichtend), ein ist Teil optional:

Anwendung	Protokolle	Status	Transport-protokoll
Audio-CODEC	G.711 G.722, G.723.1, G.726, G.728, G.729 A, G.729 B	verpflichtend optional	UDP UDP
Video-CODEC	H.261, H.263	optional	UDP
Daten	T.120	optional	TCP
Kontrolle	H.225 Registration, Admission und Status (RAS)	verpflichtend	UDP
	H.225-Ruf-Signalisierung mit Q.931	verpflichtend	TCP
	H.245 Kontroll-Signalisierung	verpflichtend	TCP
	Real-time Transfer Protocol (RTP)	verpflichtend	UDP
	Real-time Control Protocol (RTCP)	verpflichtend	UDP
Sicherheit	H.235	optional	

Tabelle A-2: H.323-Protokolle und ihre Anwendung

Folgende Grafik veranschaulicht, welche Protokolle für welche Anwendung benötigt werden:

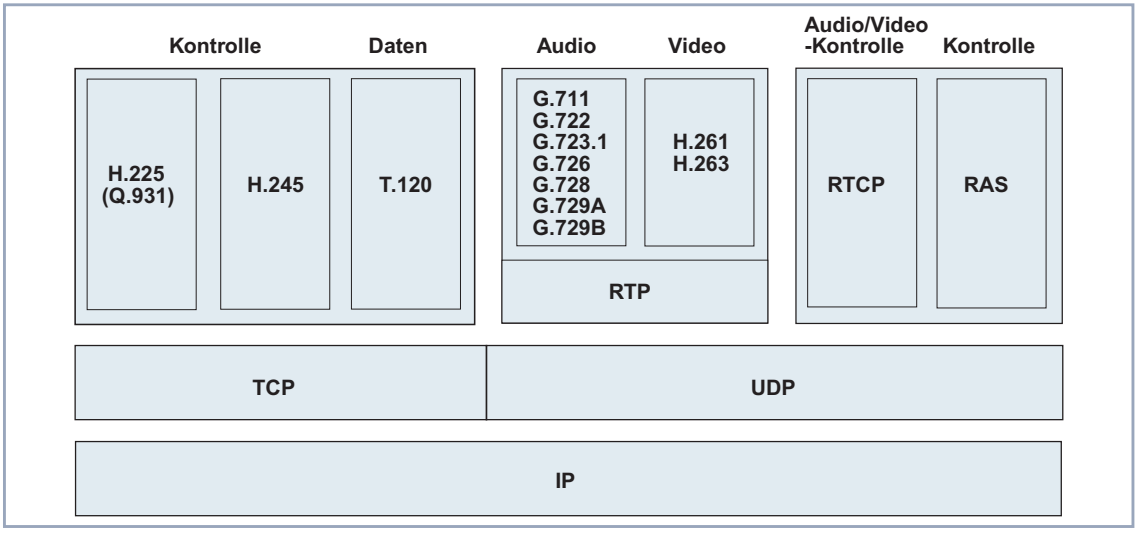

Bild A-1: H.323-Protokolle und ihre Anwendung

Audio

Ein Audio-➤➤ **CODEC** kodiert, d.h. digitalisiert und komprimiert, ein analoges Tonsignal vom Mikrofon, damit es über das Netz zum Empfänger übertragen werden kann. Das übertragene Signal wird vom CODEC dekodiert, d.h. dekomprimiert und in ein Analogsignal zurückverwandelt, und am Lautsprecher ausgegeben.

Da die Übertragung von Tonsignalen bei H.323 immer zur Verfügung steht, müssen alle H.323 Terminals mindestens ein gemeinsames Sprachkodierverfahren beherrschen, damit sie untereinander kommunizieren können. Dieses gemeinsame Sprachkodierverfahren heißt Audio-CODEC nach Standard G.711 mit 56 kBit/s oder 64 kBit/s.

Darüber hinaus können unter H.323 optional die Standards G.722 (48 kBit/s, 56 kBit/s oder 64 kBit/s), G.723.1 (5.3 kBit/s oder 6.3 kBit/s), G.726 (16 kBit/s, 24 kBit/s, 32 kBit/s oder 40 kBit/s), G.728 (16 kBit/s) und G.729 A bzw. G.729 B (jeweils 8 kBit/s) unterstützt werden.

Video

Ein Video-➤➤ **CODEC** kodiert ein Videosignal, bevor es über das H.323-Netz gesendet wird. Der empfangene Videocode wird vom Video-CODEC dekodiert und am Videogerät dargestellt.

H.323 stellt die Übertragung von Videosignalen optional zur Verfügung. Daher ist die Unterstützung eines oder mehrerer Bildkodierverfahren ebenfalls optional. Wenn ein H.323-Terminal Video-Kommunikation ermöglicht, muß es auch Video-CODEC unterstützen, d.h. mindestens H.261 ➤➤ **QCIF**.

Bei geringer Bandbreite stellen die Video-CODECs H.263 Und H.263+ bessere Videoqualität zur Verfügung als H.261.

Daten

Das Protokoll T.120 dient zur Datenübertragung, und es ist im H.323 Standard optional enthalten. T.120 ermöglicht z. B. den gemeinsamen Zugriff mehrerer Nutzer auf ein Whiteboard, Application Sharing, File Transfer u.sw.

Microsoft NetMeeting, das ebenfalls T.120 unterstützt, ermöglicht das Abhalten von Konferenzen über das Netz. T.120 unterstützt dabei den Aufbau und das Steuern des Datenflusses, der Vebindungen und der Konferenz selbst.

Verbindung und Kontrolle

Neben den Protokollen zur Kodierung und Formatierung von Sprache, Bildern und Daten sind für die Übertragung über das Netzwerk verschiedene Verbindungs- und Kontrollprotokolle nötig, deren Aufgaben im folgenden kurz erläutert werden.

H.225 Registration, Admission und Status (RAS)

Das Protokoll RAS (Registration, Admission und Status) wird für die Kommunikation zwischen Endgerät und Gatekeeper benötigt. Falls kein Gatekeeper zum Einsatz kommt, wird RAS nicht gebraucht.

Das Protokoll unterstützt die Endgeräte beim Finden des für sie zuständigen Gatekeepers und ihre Registrierung bei diesem Gatekeeper. Darüber hinaus regelt RAS die Zugangskontrolle für die Endgeräte in das H.323-Netz, eventuelle Bandbreitenänderungen, den Status und das Beenden einer Verbindung zwischen Endgerät und Gatekeeper.

H.225 Ruf-Signalisierung; Q.931

H.225 kümmert sich um die Verbindung zwischen H.323 Endgeräten.

Das Protokoll dient zum Auf- und Abbau einer Verbindung sowie zur Verbindungskontrolle zwischen zwei Endgeräten. Die Signalisierung erfolgt dabei auf der Basis von Q.931, dem Signalisierungsprotokoll von ISDN. Dadurch ist ein relativ einfacher Übergang ins öffentliche Telefonnetz gewährleistet.

H.245 Kontroll-Signalisierung

H.245 ist das Medien-Kontroll-Protokoll.

Es handelt Endgerätefunktionen aus, z. B. das Sprachkodierverfahren (Audio-CODEC). H.245 steuert darüber hinaus die logischen Kanäle für die Übertragung von Sprache, Bilder und Daten. Das Protokoll regelt die Zerlegung der Information in Datenpakete sowie die die Synchronisation der Medienströme. Es enthält außerdem Informationen zur Fluß-Kontrolle der Daten und weitere Steuerungsnachrichten.

Real-Time Transfer Protocol (RTP)

Das Real-Time Transfer Protocol (RTP) dient zum Transport von Sprach- und Bilddaten.

RTP transportiert den Audio- und Video-Datenstrom via ➤➤ **UDP**. Jedes UDP Paket wird mit einem Header mit Zeitstempel und Sequenznummer versehen. Der Header dient dazu, mit Hilfe eines entsprechenden Buffers am Empfangsterminal die Pakete in korrekter Reihenfolge zu sortieren, doppelte Pakete zu entfernen und Sprache, Bilder und Daten zu synchronisieren.

Real-Time Control Protocol (RTCP)

Das Real-time Control Protocol (RTCP) ist das Gegenstück zu RTP, quasi das Kontrollprotokoll von RTP.

RTCP überwacht die Dienstgüte und übermittelt Informationen über die Teilnehmer im Netz. RTCP informiert außerdem alle Teilnehmer über die Qualität der Datenauslieferung.

Sicherheit

Um für Informationen, die auf der Basis des H.323-Standards übertragen werden, umfassende Sicherheit zu gewährleisten, müssen die Datenströme geschützt werden. Darüber hinaus müssen aber ebenso die Kontrollprotokolle sicher übertragen werden.

Der H.235-Standard deckt folgende Hauptziele ab, um sichere Datenübertragung zu ermöglichen:

- Authentisierung der Benutzer
- Prüfung der Daten auf Integrität
- Vertraulichkeit der Daten (Verschlüsselung).

Weitere Protokolle

Der H.323-Standard spezifiziert weitere Protokolle und zusätzliche Funktionalität, auf die in diesem Dokument nicht eingegangen wird.

1.2.3 Wechselwirkung zwischen Komponenten und Protokollen

Kommunikation unter H.323 kann als Mischung aus Sprache, Bildern, Daten und Kontrollinformationen angesehen werden. Jede Komponente im Netz hat dabei bestimmt Aufgaben, die sie mit Hilfe der Protokolle wahrnimmt.

Im folgenden ist kurz zusammengefaßt, welche Protokolle die einzelnen Komponenten wofür benutzen.

Im Anschluß daran sind die Schritte szkizziert, die bei einem ➤➤ **Ruf** nacheinander stattfinden müssen.

Terminal

Ein H.323-Terminal benutzt folgende Protokolle:

- Mit H.245 handelt ein Terminal mit einem anderen Endgerät, z. B. einem weiteren Terminal, Endgerätefunktionen aus (Audio-CODECs, Video-CODECs usw.). H.245 steuert außerdem die Kanäle zum Transport von Sprache, Bildern und Daten von einem Terminal zu einem anderen Terminal.
- H.225-Ruf-Signalisierung dient zum Auf- und Abbau einer Verbindung sowie zur Verbindungskontrolle zwischen zwei Endgeräten, z. B. zwischen zwei Terminals, einem Terminal und einem Gateway oder einem Terminal und einer MCU.
- RAS wird benötigt, damit sich das Terminal bei einem Gatekeeper registrieren kann und für Kontrollaufgaben in Zusammenhang mit dem Gatekeeper.
- RTP/RTCP dient zum Senden und Empfangen von Audio- und Video-Datenpaketen sowie zur Festlegung ihrer Reihenfolge.

Gateway

Ein Gateway unterstützt die Übersetzung von Protokollen und den Transfer von Informationen zwischen verschiedenartigen Netzen, z. B. einem IP-Netz und einem ➤➤ **SCN**-Netz.

Auf H.323-Seite werden vom Gateway folgende Protokolle unterstützt:

- H.245 dient einem Gateway zum Aushandeln der Endgerätefunktionen und zum Steuern der Multimedia-Kanäle (siehe entsprechend Punkt 1 unter "Terminal", Seite 17)
- H.225-Ruf-Signalisierung dient zum Auf- und Abbau einer Verbindung sowie zur Verbindungskontrolle zwischen zwei Endgeräten, z. B. zwischen einem Gateway und einem Terminal oder einem Gateway und einer MCU.
- RAS wird benötigt, damit sich ein Gateway bei einem Gatekeeper registrieren kann und für Kontrollaufgaben in Zusammenhang mit dem Gatekeeper.

Auf ➤➤ **SCN**-Seite werden vom Gateway SCN-spezifische Protokolle unterstützt, z. B. das ➤➤ **ISDN**- und das ➤➤ **SS7**-Protokoll.

Gatekeeper

Der Gatekeeper benötigt für seine Aufgaben nur das RAS Protokoll. RAS sorgt dafür, daß sich Endgeräte beim Gatekeeper registrieren können, d.h. seiner Zone beitreten und ihre Adressen bekanntgeben. Der Gatekeeper stellt für die Endgeräte in seiner Zone verschiedene Services zur Verfügung (siehe "Gatekeeper-Funktionen", Seite 10).

Multipoint Control Unit

Innerhalb der MCU benutzt der Multipoint Controller (MC) das Protokoll H.245, um zwischen allen Terminals gemeinsame Sprach- und Bildkodierverfahren auszuhandeln.

1.2.4 Prinzipielle Vorgehensweise bei der Kommunikation unter H.323

Wenn ein H.323-Terminal mit einem zweiten H.323-Terminal kommuniziert, finden folgende Prozesse statt:

1. Rufaufbau

   Der Rufaufbau erfolgt mit Hilfe der Ruf-Kontroll-Meldungen nach H.225. Es wird auch Bandbreite für den Ruf reserviert.

2. Anfangskommunikation und Aushandlung der Endgerätefunktionen

   In einem separaten H.245-Kontroll-Kanal oder über einen Q.931-Ruf-Signalisierungskanal werden mittels H.245-Meldungen die Endgerätefunktionen ausgehandelt, z. B. Audio- und Video-CODEC.

3. Einrichten der audiovisuellen Kommunikation

   Die logischen Kanäle für die Informationsströme werden mittels H.245 geöffnet.

4. Dienste

   Während eines Rufs können verschiedene Dienste den Rufablauf unterstützen:

   Die Änderung der ursprünglich vom Gatekeeper festgelegte Bandbreite kann während einer Konferenz vom Gatekeeper oder von einem Terminal jederzeit angefordert werden.

   Der Gatekeeper kann periodische Statusmeldungen von den Endgeräten anfordern, um zu erfahren, wann ein Endgerät nicht mehr aktiv ist oder ein Fehler aufgetreten ist.

   Eine Punkt-zu-Punkt-Verbindung zwischen zwei Terminals kann zu einer Konferenz erweitert werden. Dazu ist mindestens eine MCU notwendig.

5. Beenden des Rufs

   Bei einem aktiven Ruf kann jedes der beteiligten Endgeräte den Ruf beenden. Dazu werden nacheinander die Videoübertragung am Ende eines kompletten Bildes, die Datenübertragung und dieTonübertragung beendet und die zugehörigen logischen Kanäle werden geschlossen.

2 Konfigurationsübersicht

Dieses Kapitel gibt Ihnen einen Überblick, wie Sie Proxy und Gatekeeper auf einem BinTec-Router der X-Generation anhand des Setup Tools konfigurieren.

Sind Proxy und/oder Gatekeeper konfiguriert und aktiv, so stehen Ihnen verschiedene Monitorfunktionen zur Verfügung.

Um Proxy und Gatekeeper zu konfigurieren oder um die Monitorfunktionen zu nutzen, rufen Sie das Setup Tool mit `setup` auf. Das Hauptmenü des Setup Tools erscheint. Abhängig von Ihrer Hardware und Ihrer Softwarekonfiguration kann das Menü Ihres Routers leichte Abweichungen aufweisen.

Unter ***VoIP*** finden Sie die Menüs zur Konfiguration bzw. Überwachung von Proxy und Gatekeeper.

```
BinTec-Router Setup Tool                BinTec Communications AG
                                                        MyRouter

Licenses                System

LAN:        CM-100BT, Fast EthernetModule: 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
```

Im Detail erklären wir Ihnen die Konfiguration von Proxy und Gatekeeper anhand einiger Szenarien im "Workshop", Seite 35.

2.1 Proxy konfigurieren

Sie können einen Proxy im Setup Tool im Menü ***VoIP*** ➧ ***Proxy Settings*** konfigurieren.

```
BinTec-Router 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
```

Das Menü ***VoIP*** ➧ ***Proxy Settings*** enthält folgende Felder:

Feld	Bedeutung
Proxy	Schaltet den Proxy ein oder aus. Mögliche Werte: ■ *stopped*: Proxy ist ausgeschaltet. ■ *running*: Proxy ist eingeschaltet. Voreingestellter Wert: *stopped.*

Feld	Bedeutung
Type of Proxy	Definiert den Proxy Typ. Mögliche Werte: ■ *transparent:* Proxy gibt H.323-Pakete unverändert weiter, nur die IP-Adressen in den Paketen werden ausgetauscht. ■ *endpoint:* Proxy baut zwei separate Verbindungen zu den Endgeräten auf.
Location of Proxy	Gibt an, an welcher Stelle des Netzwerks sich der Proxy befindet. Möglicher Wert: ■ *inside firewall*: Proxy befindet sich im LAN. ■ *outside firewall*: Proxy befindet sich außerhalb des LANs (momentan nicht verfügbar).
Proxy Listen Port	TCP-Port zum Annehmen der H.225 -Meldungen zur ➤➤ **Ruf**-Kontrolle. Normalerweise belassen Sie den voreingestellten Wert *1720*. Wenn ein BinTec-Gatekeeper aktiv ist, bei dem die Endgeräte registriert sind und der die H.225-Ruf-Kontollmeldungen routet, so kann ein anderer Port benutzt werden. Mögliche Werte: *1024 ... 65535*
Use TCP Ports	Legt den ersten TCP-Port fest, der für das Protokol H.245 benutzt wird. Mögliche Werte: *0 ... 65535.* Der voreingestellte Wert *0* bedeutet, daß die Ports für H.245 dynamisch zugewiesen werden.

Feld	Bedeutung
Range	Anzahl der Ports, die für das Protokol H.245 reserviert wird, beginnend mit **Use TCP Ports**. Der Port Range kann an netzwerkspezifische Konfigurationen, wie z. B. eine separate Firewall angepaßt werden. Mögliche Werte: *0 ... 64.* Voreingestellter Wert: *32.*
Use UDP Ports	Legt den ersten UDP-Port fest, der für die Übertragung von Sprache und Bildern benutzt wird. Mögliche Werte: *1024 ... 65535.* Voreingestellter Wert: *5004.*
Range	Anzahl der Ports, die für die Übertragung von Sprache und Bildern benutzt werden. Der Port Range kann an netzwerkspezifische Konfigurationen, wie z. B. eine separate Firewall angepaßt werden. Mögliche Werte: *0 ... 256.* Voreingestellter Wert: *128.*
TOS Field for QoS	Type of Service Feld In diesem Feld können Sie festlegen, wie der Proxy RTP-Pakete priorisieren soll, die er versendet. Mögliche Werte: *10000*: Kennzeichnet Datenpakete, die möglichst sofort ausgeliefert werden sollen. *01000*: Kennzeichnet Datenpakete, die mit hohem Datendurchsatz transportiert werden sollen. *00100*: Kennzeichnet Datenpakete, die möglichst zuverlässig transportiert werden sollen.

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

2.2 Gatekeeper konfigurieren

Sie konfigurieren einen Gatekeeper im Setup Tool in den folgenden Menüs:

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

Das Menü ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table*** benötigen Sie für den Fall, daß Sie den Pool der Endgeräte, die sich beim Gatekeeper registrieren dürfen, einschränken möchten.

Das Menü ***VoIP*** ➧ ***Gatekeeper Settings*** enthält folgendes Feld:

Feld	Bedeutung
Gatekeeper	Schaltet den Gatekeeper ein oder aus. Mögliche Werte: ■ *stopped*: Gatekeeper ist ausgeschaltet. ■ *running*: Gatekeeper ist eingeschaltet. Voreingestellter Wert: *stopped.*

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

Im Menü ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings*** legen Sie allgemeine Einstellungen für den Gatekeeper fest.

```
BinTec-Router 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
```

Das Menü ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings*** enthält folgende Felder:

Feld	Bedeutung
Gatekeeper ID	Name des Gatekeepers Voreingestellter Wert: *Bintec Gk 1.0.*

Feld	Bedeutung
Interface with limited Bandwidth	Legt ein Interface fest, für das die Bandbreite auf **Max Bandwidth (kBits/s)** begrenzt werden kann. Sie können, je nach eingesetztem Gerät und konfiguriertem WAN-Partner, ein Interface auswählen, z. B.: ■ *none* ■ *en1* ■ *en1-snap* ■ *t-online* Voreingestellter Wert: *none.*
Max Bandwidth (kBits/s)	Legt die maximale Bandbreite des unter **Interface with limited Bandwidth** ausgewählten Interfaces in kBit/s fest. Voreingestellter Wert: *5.*
Bandwidth per Call (kBits/s)	Reservierte Bandbreite pro Ruf. Voreingestellter Wert: *5.*
Type of Call Routing	Modus, wie der Gatekeeper RTP- und Kontrollpakete routet. ■ *direct*: Pakete werden direkt von einem Endgerät zum anderen übertragen. ■ *routed*: Alle Pakete werden über Gatekeeper bzw. Proxy geroutet. ■ *dynamic*: Netzwerkadresse wird geprüft und die Pakete werden unter Einbeziehung des Bandbreitenmanagements *direct* oder *routed* transportiert. Voreingestellter Wert: *dynamic.*

Feld	Bedeutung
Type of Registration	Legt fest, ob sich jedes beliebige Endgerät beim Gatekeeper registrieren darf oder ob die registrierten Endgeräte auf eine vordefinierte Liste beschränkt sind. ■ *unrestricted*: Alle Endgeräte dürfen sich registrieren. ■ *limited to user table*: Es dürfen sich nur die Endgeräte registrieren, die in der User Table eingetragen sind (siehe Tabelle A-6, Seite 29). Voreingestellter Wert: *unrestricted.*
Location Policy	Legt fest, wie der Gatekeeper bei der Adreßauflösung eines Endgeräts vorgeht. Mögliche Werte: ■ *local*: Berücksichtigt nur Endgeräte, die unter ***VoIP*** ➧ ***Monitoring*** ➧ ***Registered Users*** ➧ ***add*** erfaßt sind oder die über eine IP-Adresse direkt adressiert werden. ■ *remote*: Richtet Anfrage zur Adreßauflösung eines Endgeräts an die **Alternate Gatekeeper**. ■ *relaxed*: Adreßauflösung wird zuerst *local* und dann *remote* versucht. Voreingestellter Wert: *relaxed.*
Time to Live (sec)	Zeitspanne in Sekunden, innerhalb derer sich ein bereits registriertes Endgerät beim Gatekeeper erneut melden muß, um die Registrierungsdauer zu verlängern. Mögliche Werte: *60 ... 3600.* Voreingestellter Wert: *120.*

Feld	Bedeutung
IRRfrequency (sec)	Info Request Response Frequency Zeitspanne in Sekunden zwischen zwei Info Request Responses eines Endgeräts. In der Info Request Response werden vom Endgerät verschiedene Status- und Kontrollinformationen gesendet, optional auch eine Kopie der Q.931-Meldungen. Die Info Request dient zur Kontrolle, ob ein Ruf noch aktiv ist. Das Endgerät selbst wird mit Hilfe der Time to Live überprüft. Eine Info Request wird vom Gatekeeper geschickt, falls das Endgerät nicht ohne Aufforderung innerhalb der IRRfrequency eine Info Request Response sendet. Mögliche Werte: *60 ... 3600.* Voreingestellter Wert: *60.*
Voice Gateway	IP-Adresse eines Gateways, an das Rufe mit nicht auflösbarer Adresse weitergeleitet werden (vergleichbar mit einem IP Default Gateway).
Alternate Gatekeeper (Priority 0) **Alternate Gatekeeper (Priority 1)** **Alternate Gatekeeper (Priority 2)**	Hier können Sie die IP-Adressen dreier Gatekeeper angeben, die nacheinander angefragt werden, falls Ihr BinTec Gatekeeper die Adresse eines Endgeräts nicht auflösen kann.

Tabelle A-5: ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings***

Das Menü ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table*** ➧ ***add*** dient dazu, die Endgeräte festzulegen, die sich beim Gatekeeper registrieren können.

```
BinTec-Router 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
```

Das Menü enthält folgende Felder:

Feld	Bedeutung
Username	Benutzername
Alias	Spitzname des Endgeräts
E.164 #	Telefonnummer im Format ➤➤ **E.164**
E-Mail	E-Mail-Adresse
IP Address	IP-Adresse des Endgeräts

Tabelle A-6: ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table*** ➧ ***add***

2.3 Monitoring

Im Menü ***VoIP*** ➧ ***Monitoring*** ➧ ***Registered Users*** werden die Endgeräte angezeigt, die gegenwärtig beim Gatekeeper registriert sind. Wenn noch keine Endgeräte registriert sind, ist das Menü leer.

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

   Name           Alias          E.164#      IP Address




   EXIT
```

Im Menü ***VoIP*** ➧ ***Monitoring*** ➧ ***Active Calls*** werden die Endgeräte angezeigt, die gegenwärtig an einem Ruf beteiligt sind. Wenn im Moment kein Ruf stattfindet, ist das Menü leer.

```
BinTec-Router 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
```

Im Menü ***VoIP*** ➧ ***Monitoring*** ➧ ***Call History*** werden die Rufe angezeigt, die bereits beendet sind. Wenn noch keine Rufe stattgefunden haben, ist das Menü leer.

3 Glossar

Client Arbeitsplatzrechner im PC-Netz, der die Dienstleistungen des ➤➤ **Servers** nutzt.

CODEC Coder/Decoder

Computer Telefonie Integration (CTI) Telefondienst, der durch Computertechnik unterstützt wird.

Dieser Dienst kann angefangen von einfachen Anwendungen wie z. B. computergestützte Rufnummernrückwahl bis hin zu kompletten Call-Centern verschiedene Dienstleistungen anbieten.

E.164 In ISDN-Netzen verwendeter Adressierungsstandard, d.h. gebräuchliche Telefonnummer.

Firewall Bezeichnet die Summe der Schutzmechanismen für das lokale Netzwerk gegen Zugriffe von außen.

IP Internet Protocol

IP-Telefonie Telefonie über IP-Netze wie z. B. das Internet (siehe auch ➤➤ **Voice over IP**).

ISDN Integrated Services Digital Network

LAN Local Area Network (Lokales Netzwerk)

Räumlich eng begrenztes Netzwerk, das sich unter Kontrolle eines Besitzers befindet, meist innerhalb eines Gebäudes/Firmensitzes.

POTS Plain Old Telephone System

Das traditionelle, analoge Telefonnetz.

PSTN Public Switched Telephone Network

Das weltweite Telefonnetz.

QCIF Quarter Common Interchange Format

Videoformat mit176 x 144 Pixeln, das bei ISDN-Video-Konferenzen benutzt wird.

Ruf Punkt-zu-Punkt Kommunikation zwischen zwei H.323 Endgeräten.

SCN Switched Circuit Network

Öffentliches oder privates leitungsvermitteltes Telekommunikationsnetzwerk.

Server Dienstanbieter im PC-Netz

SS7 Signaling System No. 7

Signalisierungsprotokoll

TCP Transmission Control Protocol

TCP ist ein verbindungsorientiertes Transportprotokoll aus der TCP/IP-Familie. Kontrollmechanismen verhindern den Verlust von Datenpaketen.

UDP User Datagram Protocol

Ein Transportprotokoll ähnlich TCP. UDP bietet keine Kontroll-/Quitierungsmechanismen, ist dafür aber schneller als TCP. UDP ist im Gegensatz zu TCP verbindungslos.

Unified Messaging Unified Messaging vereint die drei Datentypen Sprache, Fax und E-Mail.

Alle drei sind entweder über E-Mail-Umgebung (jeder Datentyp mit entsprechender Kennung) oder über Telefon zugänglich.

Voice over IP (VoIP) Voice over IP nutzt das IP-Protokoll nicht nur zum Datentransfer sondern auch für Sprach- und Bildübertragung.

WAN Wide Area Network

Weitverkehrsdatennetz; Verbindungen z. B. über ISDN, X.25.

A Glossar

Workshop

1 Konfiguration von IP-Telefonen im lokalen Netzwerk

1.1 Einführung

In Ihrem LAN können Sie mit sehr wenig Konfigurationsaufwand IP-Telefone betreiben.

Vorteile von IP-Telefonen

IP-Telefone bieten folgende Vorteile:

Für Daten und Telefonie wird nur noch ein einziges Netzwerk benötigt, zusätzliche Infrastruktur für Telefonie im LAN wird nicht gebraucht. (Um nach "außen" telefonieren zu können, benötigen Sie ein Gateway.)

Abgesehen von der Kostenersparnis durch die Nutzung eines einzigen Netzes für die gesamte Kommunikation haben IP-Telefone einen unmittelbaren Vorteil im Arbeitsalltag: Wenn ein Mitarbeiter innerhalb der Firma seinen Arbeitsplatz dauerhaft oder vorübergehend wechselt, kann er seinen Telefonapparat mitnehmen und am neuen Arbeitsplatz anschließen. Es ist keine neuerliche Konfiguration nötig, der Mitarbeiter ist sofort unter der gewohnten Telefonnummer erreichbar.

Zusätzlich zu Ihrem BinTec-Router benötigen Sie keine weiteren Komponenten, um IP-Telefone im LAN in Betrieb zu nehmen.

Anstelle eines IP-Telefons können Sie auch einen PC mit Mikrofon bzw. Kopfhörer und Microsoft NetMeeting zur Kommunikation nutzen.

Vorgehensweise

Inbetriebnahme und Test von IP-Telefonen im LAN gliedern sich in vier Schritte:

- Registrieren der IP-Telefone beim BinTec-Gatekeeper (Abschnitt B, Kapitel 1.3.1, Seite 38)
- Überprüfen der Registrierung (Abschnitt B, Kapitel 1.3.2, Seite 42)
- Testanruf (Abschnitt B, Kapitel 1.3.3, Seite 42)
- Anrufe anzeigen lassen (Abschnitt B, Kapitel 1.3.4, Seite 43).

1.2 Voraussetzungen

Verfügbarkeit von H.323-Gatekeeper

Sie können IP-Telefone innerhalb Ihres LANs zusammen mit der Gatekeeper-Funktionalität eines BinTec-Routers der X-Generation ab Software-Release 6.2.1 nutzen. Wenn Sie die Geräte **X1000**, **X1200** oder **X3200** betreiben, so sind die Sicherheitslösung IPSec und der Gatekeeper nicht gleichzeitig verfügbar.

Um sicherzustellen, daß Ihr Router über die Gatekeeper-Funktionalität verfügt, gehen Sie folgendermaßen vor:

Routertyp

➤ Überprüfen Sie, welchen Routertyp Sie in Betrieb haben.

X1000, X1200, X3200

Bei den Routern **X1000**, **X1200** und **X3200**:

➤ Kontrollieren Sie, ob Ihr Gerät mit IPSec-System-Software betrieben wird.

Bei Software-Release 6.2.1 mit IPSec:

➤ Installieren Sie Software-Release 6.2.1 ohne IPSec oder erweben Sie einen BinTec-Router der X-Generation, der IPSec und Gatekeeper-Funktionalität gleichzeitig zur Verfügung stellt.

Bei Software-Release 6.2.1 ohne IPSec ist der Gatekeeper verfügbar.

Andere Geräte der X-Generation

Bei allen anderen Geräten der X-Generation:

➤ Überprüfen Sie, ob Software-Release 6.2.1 auf dem Router installiert ist. Falls Ihr Gerät einen älteren Software-Stand aufweist, führen Sie ein Software-Update durch. Informationen zum Software-Update finden Sie im Benutzerhandbuch zu Ihrem BinTec-Router.

1.3 Konfiguration und Monitoring

Grafische Darstellung eines LANs mit IP-Telefonen:

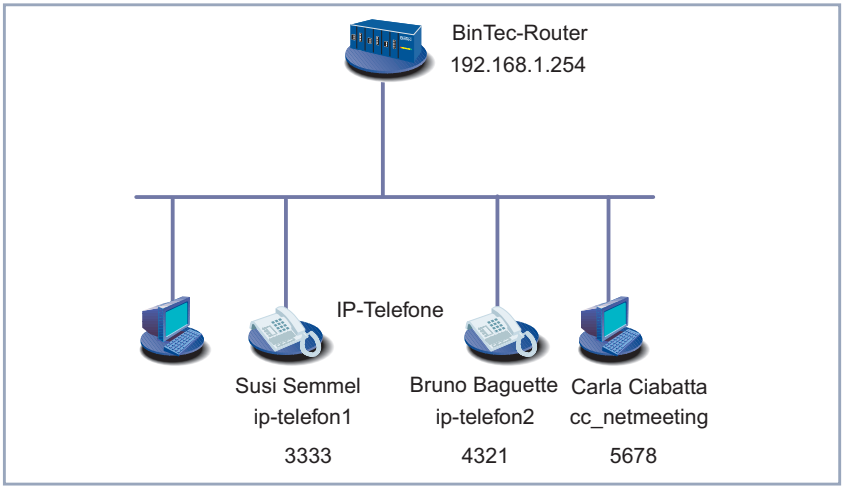

Bild B-1: IP-Telefone und PCs im LAN

1.3.1 Registrieren der IP-Telefone beim BinTec-Gatekeeper

Im folgenden erklären wir Ihnen, wie Sie Ihr IP-Telefon beim Gatekeeper Ihres BinTec-Routers registrieren. Die Registrierung wird am Beispiel des Innovaphone 200 dargestellt. IP-Telefone anderer Hersteller registrieren sich in vergleichbarer Weise.

Um sicherzustellen, daß sich nur bestimmte IP-Telefone bei Ihrem BinTec Gatekeeper registrieren können, tragen Sie die gewünschten Telefone in die ***USER TABLE*** des Gatekeepers ein. Beim IP-Telefon selbst tragen Sie den Alias des IP-Telefons und die IP-Adresse des Gatekeepers ein, bei dem sich das IP-Telefon registrieren soll. Die Registrierung selbst erfolgt automatisch.

Bevor Sie beginnen, stellen Sie sicher, daß das IP-Telefon bereits eine IP-Adresse hat bzw. daß dem IP-Telefon eine IP-Adresse zugewiesen wird. Um den Konfigurationsaufwand zu reduzieren, können Sie die IP-Adresse über ei-

nen DHCP Server beziehen. Wenn Sie Ihren BinTec-Router als DHCP Server verwenden möchten, finden Sie Hinweise zur Konfiguration im Benutzerhandbuch Ihres Geräts.

IP-Telefon in User Table eintragen

Um ein IP-Telefon in die ***USER TABLE*** Ihres BinTec-Gatekeepers einzutragen, gehen Sie im Setup Tool folgendermaßen vor:

➤ Gehen Sie zu ***VoIP*** ➧ ***GATEKEEPER SETTINGS*** ➧ ***USER TABLE*** ➧ ***ADD***.

Sie sehen folgendes Menü:

```
BinTec-Router 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 hostname)
```

➤ Geben Sie **Username** ein, z. B. ***Susi Semmel***.

➤ Geben Sie **Alias** ein, z. B. ***ip-telefon1***.

➤ Geben Sie **E.164** ein, z. B. ***3333***.

➤ Geben Sie **E-Mail** ein, z. B. ***abcde@bintec.de***.

➤ Überspringen Sie **IP Address**.

➤ Bestätigen Sie mit **SAVE**.

Die Parameter des IP-Telefons sind temporär gespeichert und aktiviert.

Beschränkung auf User Table

Um sicherzustellen, daß sich nur die Endgeräte registrieren können, die in die ***USER TABLE*** eingetragen sind, gehen Sie folgendermaßen vor:

➤ Gehen Sie zu***VoIP*** ➧ ***GATEKEEPER SETTINGS*** ➧ ***GLOBAL SETTINGS***.

Sie sehen folgendes Menü:

```
BinTec-Router 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
```

- Wählen Sie **Type of Registration** aus: *limited to user table*.
- Bestätigen Sie mit **SAVE**.

Gatekeeper einschalten

Um den Gatekeeper mit den bereits erfolgten Einstellungen zu aktivieren, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***Gatekeeper Settings***.
- Wählen Sie **Gatekeeper** aus: *running*.
- Bestätigen Sie mit **SAVE**.

  Der Gatekeeper ist jetzt aktiv.

Gatekeeper beim IP-Telefon eintragen

Um beim Innovaphone 200 den Gatekeeper Ihres BinTec-Routers einzutragen, gehen Sie folgendermaßen vor:

- Betätigen Sie die Taste **Menü** auf dem Gehäuse des Innovaphone 200.
- Gehen Sie in diesem Menü zu **Konfiguration** ➧ **Registrierung** ➧ **VoIP Gatekeeper**.

➤ Geben Sie **Gatekeeper Name** ein oder lassen Sie das Feld leer.

Wenn Sie **Gatekeeper Name** eintragen, muß der Eintrag mit **Gatekeeper ID** (siehe Tabelle A-5, Seite 28) unter ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings*** im Setup Tool übereinstimmen.

➤ Geben Sie **Gatekeeper IP Adresse** ein, z. B. ***192.168.1.254***.

➤ Schalten Sie das **RAS Protokoll** *ein*.

➤ Verlassen Sie **Konfiguration** ➧ **Registrierung** ➧ **VoIP Gatekeeper**.
Sie befinden sich in **Konfiguration** ➧**Registrierung**.

➤ Gehen Sie zu **Konfiguration** ➧ **Registrierung** ➧ **Rufnummer**.

➤ Geben Sie **Name (H323)** ein, z. B. ***ip-telefon1***.

Der **Name (H323)** beim Innovaphone 200 entspricht dem **Alias** (und nicht dem **Username**) im Setup Tool.

➤ Verlassen Sie **Konfiguration** ➧ **Registrierung** ➧ **Rufnummer** und schließen Sie alle Menüs.

Registrieren

Das Innovaphone 200 registriert sich automatisch beim Gatekeeper.

Auf dem Display des Innovaphone 200 werden **Username** und **Rufnummer** angezeigt. Außerdem symbolisiert unten rechts eine Raute den Status der Regiestrierung beim Gatekeeper: Eine gefüllte Raute steht für ein registriertes IP-Telefon. Wenn die Raute leer ist, ist das IP-Telefon nicht registriert.

Weitere IP-Telefone registrieren

➤ Gehen Sie bei allen weiteren IP-Telefonen, die sich beim Gatekeeper registrieren sollen, genauso vor.

➤ Registrieren Sie z. B. ein zweites IP-Telefon mit dem Namen ***Bruno Baguette***, dem Alias ***ip-telefon2*** und der Telefonnummer ***4321***.

1.3.2 Überprüfen der Registrierung

Um zu prüfen, ob die Registrierung der IP-Telefone beim Gatekeeper Ihres BinTec-Routers erfolgreich war, gehen Sie folgendermaßen vor:

➤ Gehen Sie im Setup-Tool-Menü zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Registered Users***.

Die beim Gatekeeper registrierten IP-Telefone werden angezeigt.

Wenn sich z. B. *ip-telefon1* und *ip-telefon2* beim Gatekeeper registriert haben, sehen Sie folgendes:

```
BinTec-Router 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
```

Sie können zu jedem Eintrag detaillierte Informationen erhalten.

➤ Wählen Sie den gewünschte Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste.

1.3.3 Testanruf

Um zu testen, ob die IP-Telefone miteinander telefonieren können, rufen Sie mit einem IP-Telefon ein anderes IP-Telefon an. Sie können die Telefonnummer, den Usernamen oder den Alias eingeben, um die Verbindung herzustellen.

Wenn alles in Ordnung ist, wird die Verbindung wie gewohnt hergestellt.

1.3.4 Anrufe anzeigen lassen

Sie können sich sowohl die momentan aktiven Anrufe als auch die bereits beendeten Anrufe anzeigen lassen.

Aktive Anrufe

Gehen Sie folgendermaßen vor, um die aktiven Anrufe anzeigen zu lassen:

➤ Gehen Sie zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Active Calls***.
Die momentan aktiven Anrufe werden angezeigt.

In unserem Beispiel ruft Susi Semmel gerade Bruno Baguette an:

```
BinTec-Router 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
```

Sie können detaillierte Informationen zu jedem Anruf erhalten:

➤ Wählen Sie den gewünschte Eintrag aus und drücken Sie **Return**.
Sie erhalten eine detaillierte Liste.

Beendete Anrufe

Gehen Sie folgendermaßen vor, um bereits beendete Anrufe anzuzeigen:

➤ Gehen Sie zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Call History***.
Die bereits beendeten Anrufe werden angezeigt.

In unserem Beispiel wurde dreimal telefoniert:

```
BinTec-Router 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
```

Sie können ebenfalls zu jedem Anruf detaillierte Informationen erhalten.

➤ Wählen Sie den gewünschte Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste. Darin werden Sie u.a. informiert, wer, wen, wie lange angerufen hat.

1.3.5 Microsoft NetMeeting im LAN

Statt mit einem IP-Telefon können Sie auch mittels PC und Mikrofon bzw. Kopfhörer und Microsoft NetMeeting mit anderen IP-Telefonen oder anderen PCs mit NetMeeting im LAN kommunizieren.

Bevor Sie beginnen, stellen Sie sicher, daß Microsoft NetMeeting ordnungsgemäß auf Ihrem PC installiert ist.

Um mit IP-Telefonen oder anderen NetMeeting-Benutzern kommunizieren zu können, muß sich NetMeeting beim Gatekeeper registrieren.

Um sicherzustellen, daß sich nur ein bestimmter PC mit NetMeeting bei Ihrem BinTec Gatekeeper registrieren kann, tragen Sie den gewünschten Kommunikationspartner in die ***USER TABLE*** des Gatekeepers ein. Bei NetMeeting selbst tragen sie nur den Alias und den Gatekeeper ein, bei dem sich NetMeeting registrieren soll. Die Registrierung selbst erfolgt automatisch.

NetMeeting in User Table eintragen

Um NetMeeting in die ***USER TABLE*** Ihres BinTec-Gatekeepers einzutragen, gehen Sie im Setup Tool folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***GATEKEEPER SETTINGS*** ➧ ***USER TABLE*** ➧ ***ADD***.
- Geben Sie **Name** ein, z. B. ***Carla Ciabatta***.
- Geben Sie **Alias** ein, z. B. ***cc_netmeeting***.
- Geben Sie **E.164** ein, z. B. ***5678***.
- Geben Sie **E-Mail** ein, z. B. ***klmno@bintec.de***.
- Überspringen Sie **IP Address**.
- Bestätigen Sie mit **SAVE**.

  Die Einträge sind temporär gespeichert und aktiviert.

Gatekeeper bei NetMeeting eintragen

Um bei NetMeeting den Gatekeeper einzutragen, gehen Sie folgendermaßen vor:

- Starten Sie NetMeeting auf Ihrem PC.
- Gehen Sie zu **Extras** ➧ **Optionen**.
- Klicken Sie auf **Erweiterte Anrufoptionen**.
- Aktivieren Sie das Kontrollkästchen **Einen Gatekeeper zum Anrufen verwenden** und geben Sie die IP-Adresse des Gatekeepers ein, z. B. ***192.168.1.254***.
- Aktivieren Sie das Kontrollkästchen **Mit Kontonamen anmelden** und geben Sie den gewünschten Namen ein, z. B. ***cc_netmeeting***.
- Schließen Sie beide Fenster mit **OK**.

  NetMeeting registriert sich beim Gatekeeper.

Überprüfung der Registrierung

In unserem Beispiel sehen Sie unter ***VoIP*** ➧ ***Monitoring*** ➧ ***Registered Users*** jetzt zusätzlich Carla Ciabatta:

```
BinTec-Router 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
```

Die Benutzer der drei Terminals können jetzt miteinander telefonieren.

Falls sich NetMeeting nicht beim Gatekeeper registriert, so hat das Programm eine ältere Konfiguration gespeichert. Starten Sie NetMeeting neu.

2 Zugang zur Firmenzentrale mit Microsoft NetMeeting

2.1 Einführung

Ein Mitarbeiter am Heimarbeitsplatz kann mit Microsoft NetMeeting von zuhause aus an einer Konferenz in der Firma teilzunehmen, wenn ihm ein Zugang zum Netzwerk der Firmenzentrale eingerichtet wird.

Der Mitarbeiter benötigt lediglich einen PC mit ISDN-Karte, auf dem Microsoft NetMeeting installiert ist, oder eine andere direkte Einwahlmöglichkeit, z. B. T-DSL mit Modem und Netzwerkkarte.

Vorgehensweise

Inbetriebnahme, Test und Anwendung von Microsoft NetMeeting gliedern sich im vorliegenden Fall in vier Schritte:

- Registrieren von NetMeeting beim BinTec-Gatekeeper (Abschnitt B, Kapitel 2.3.1, Seite 49)
- Überprüfen der Registrierung (Abschnitt B, Kapitel 2.3.2, Seite 52)
- Testverbindung zur Firmenzentrale (Abschnitt B, Kapitel 2.3.3, Seite 54)
- Verbindungen anzeigen lassen (Abschnitt B, Kapitel 2.3.4, Seite 55).

2.2 Voraussetzungen

Für die Nutzung von NetMeeting empfiehlt es sich, einen Flatrate-Zugang zum Internet zu verwenden.

Aus Sicherheitsgründen unterstützt BinTec Communications AG die NetMeeting-Funktionen "Desktop Sharing" und "Whiteboard" nicht.

Wenn Sie NetMeeting zusammen mit Gatekeeper- bzw. Proxy-Funktionalität einsetzen, können Sie den "Internet Locator Server" von Microsoft nicht nutzen.

Verfügbarkeit von H.323-Proxy und H.323-Gatekeeper

Sie können Microsoft NetMeeting zusammen mit der Gatekeeper- und Proxy-Funktionalität eines BinTec-Routers der X-Generation ab Software-Release 6.2.1 nutzen. Wenn Sie die Geräte **X1000**, **X1200** oder **X3200** betreiben, so sind die Sicherheitslösung IPSec und Gatekeeper bzw. Proxy nicht gleichzeitig verfügbar.

Um sicherzustellen, daß Ihr Router über Gatekeeper- und Proxy-Funktionalität verfügt, gehen Sie folgendermaßen vor:

Routertyp

➤ Überprüfen Sie, welchen Routertyp Sie in Betrieb haben.

X1000, X1200, X3200

Bei den Routern **X1000**, **X1200** und **X3200**:

➤ Kontrollieren Sie, ob Ihr Gerät mit IPSec-System-Software betrieben wird.

Bei Software-Release 6.2.1 mit IPSec:

➤ Installieren Sie Software-Release 6.2.1 ohne IPSec oder erweben Sie einen BinTec-Router der X-Generation, der IPSec und Gatekeeper- bzw. Proxy-Funktionalität gleichzeitig zur Verfügung stellt.

Bei Software-Release 6.2.1 ohne IPSec sind Gatekeeper und Proxy verfügbar.

Andere Geräte der X-Generation

Bei allen anderen Geräten der X-Generation:

➤ Überprüfen Sie, ob Software-Release 6.2.1 auf dem Router installiert ist. Falls Ihr Gerät einen älteren Software-Stand aufweist, führen Sie ein Software-Update durch. Informationen zum Software-Update finden Sie im Benutzerhandbuch zu Ihrem BinTec-Router.

2.3 Konfiguration und Monitoring

In der folgenden grafischen Darstellung sehen Sie einen Heimarbeitsplatz, der über das Internet an die Firmenzentrale angebunden ist:

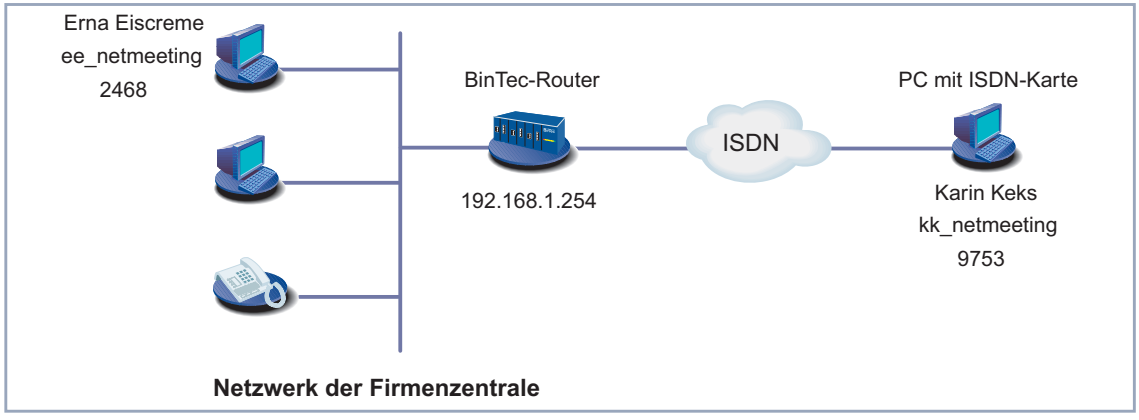

Bild B-2: Firmenzentrale und Heimarbeitsplatz verbunden durch einen BinTec-Router

2.3.1 Registrieren von NetMeeting beim BinTec-Gatekeeper

Überblick

Damit ein Mitarbeiter am Heimarbeitsplatz mit seinen Kollegen in der Firmenzentrale mittels Microsoft NetMeeting kommunizieren kann, muß sich NetMeeting beim Gatekeeper in der Zentrale registrieren. Sowohl bei NetMeeting selbst als auch beim BinTec-Router in der Firmenzentrale müssen dazu entsprechende Voraussetzungen geschaffen werden:

- Der Administrator in der Firmenzentrale muß für den Mitarbeiter am Heimarbeitsplatz einen **Username** vergeben und ihn in die ***USER TABLE*** des Gatekeepers eintragen. Er muß dafür sorgen, daß bei der Registrierung auf diesen Eintrag zurückgegriffen wird.
- Der Mitarbeiter am Heimarbeitsplatz muß NetMeeting entsprechend einrichten, so daß sich NetMeeting beim Gatekeeper des BinTec-Routers registriert.

Vorgehensweise

Der Administrator des BinTec-Routers sorgt durch Aktivierung des Proxy dafür, daß NetMeeting Zugang zum Firmennetz erhält.

Um sicherzustellen, daß der Mitarbeiter am Heimarbeitsplatz unter seinem Namen und der gewünschten Telefonnummer erreichbar ist, trägt der Administrator die entsprechenden Daten in die ***USER TABLE*** des Gatekeepers ein.

Der Mitarbeiter am Heimarbeitsplatz trägt im Programm Netmeeting nur den Alias sowie den Gatekeeper ein, bei dem sich NetMeeting registrieren soll. Die Registrierung selbst erfolgt automatisch.

Anstelle von NetMeeting können Sie auch andere H.323-fähige Endgeräte benutzen, wenn sie beim BinTec-Gatekeeper registriert werden.

Konfigurieren Ihres BinTec-Routers (Firmenzentrale)

Im folgenden erläutern wir Ihnen, welche Einstellungen Sie als Administrator bei Ihrem BinTec-Router in der Firmenzentrale vornehmen müssen, damit sich ein Außendienstmitarbeiter mit NetMeeting in das Firmennetzwerk einwählen kann.

Proxy aktivieren

Um den Proxy Ihres BinTec-Routers für einen Zugang mit NetMeeting zu konfigurieren, gehen Sie im Setup Tool folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***PROXY SETTINGS***.
- Belassen Sie die Voreinstellungen.
- Wählen Sie **Proxy** aus: *running*.
- Bestätigen Sie mit **SAVE**.
  Der Proxy ist aktiviert.

Daten für NetMeeting in User Table eintragen

Um die Daten für NetMeeting in die ***USER TABLE*** Ihres BinTec-Gatekeepers einzutragen, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***GATEKEEPER SETTINGS*** ➧ ***USER TABLE*** ➧ ***ADD***.
- Geben Sie **Username** ein, z. B. ***Karin Keks***.
- Geben Sie **Alias** ein, z. B. ***kk_netmeeting***.
- Geben Sie **E.164** ein, z. B. ***9753***.

- Geben Sie gegebenenfalls **E-Mail** ein, z. B. ***pqrst@bintec.de***.
- Überspringen Sie **IP Address**.
- Bestätigen Sie mit **SAVE**.

  Die Einträge sind temporär gespeichert und aktiviert.

Beschränkung auf User Table

Um sicherzustellen, daß sich nur die Endgeräte registrieren können, die in die ***USER TABLE*** eingetragen sind, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***GATEKEEPER SETTINGS*** ➧ ***GLOBAL SETTINGS***.

Sie sehen folgendes Menü:

```
BinTec-Router 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
```

- Wählen Sie **Type of Registration** aus: *limited to user table*.
- Bestätigen Sie mit **SAVE**.

Gatekeeper einschalten

Um den Gatekeeper mit den bereits erfolgten Einstellungen zu aktivieren, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***GATEKEEPER SETTINGS***.
- Wählen Sie **Gatekeeper** aus: *running*.

- Bestätigen Sie mit **SAVE**.

  Der Gatekeeper ist jetzt aktiv.

NetMeeting konfigurieren (Heimarbeitsplatz)

Im folgenden erklären wir Ihnen, welche Einstellungen Sie bei NetMeeting am Heimarbeitsplatz vornehmen müssen, damit sich NetMeeting beim Gatekeeper in der Firmenzentrale registrieren kann.

Bevor Sie beginnen, stellen Sie sicher, daß Microsoft NetMeeting ordnungsgemäß auf Ihrem PC installiert ist.

Gatekeeper bei NetMeeting eintragen

Um bei Ihrem Microsoft NetMeeting den Gatekeeper einzutragen, gehen Sie folgendermaßen vor:

- Starten Sie NetMeeting auf Ihrem PC.
- Gehen Sie zu **Extras** ➧ **Optionen**.
- Klicken Sie auf **Erweiterte Anrufoptionen**.
- Aktivieren Sie das Kontrollkästchen **Einen Gatekeeper zum Anrufen verwenden** und geben Sie die IP-Adresse des Gatekeepers ein, z. B. ***192.168.1.254***. Statt der IP-Adresse können Sie auch einen DNS-Namen verwenden.
- Aktivieren Sie das Kontrollkästchen **Mit Kontonamen anmelden** und geben Sie den gewünschten Namen ein, z. B. ***kk_netmeeting***.
- Schließen Sie beide Fenster mit **OK**.
- Starten Sie NetMeeting erneut.

  NetMeeting registriert sich beim Gatekeeper.

2.3.2 Überprüfen der Registrierung

Um zu prüfen, ob die Registrierung von Microsoft NetMeeting vom Heimarbeitsplatz beim Gatekeeper Ihres BinTec-Routers in der Firmenzentrale erfolgreich war, gehen Sie als Administrator folgendermaßen vor:

- Gehen Sie im Setup-Tool-Menü zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Registered Users***.

Wenn NetMeeting aus unserem Beispiel ordungsgemäß registriert ist, sehen Sie folgendes:

```
BinTec-Router 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
```

Sie können zu diesem Eintrag detaillierte Informationen erhalten:

➤ Wählen Sie den Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste:

```
BinTec-Router 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 Testverbindung zur Firmenzentrale

Um zu testen, ob Sie mit Ihrem NetMeeting am Heimarbeitsplatz mit anderen NetMeeting-Benutzern in der Firmenzentrale kommunizieren können, stellen Sie eine Verbindung zu einem anderen NetMeeting Benutzer her.

Rufen Sie z. B. Erna Eiscreme mit dem Alias ee_netmeeting und der Telefonnummer 2468 (siehe Bild B-2, Seite 49) an. Sie sollte mit diesen Daten beim Gatekeeper registriert sein. Sie können die Telefonnummer, den Usernamen oder den Alias eingeben, um die Verbindung herzustellen.

Gehen Sie folgendermaßen vor, um eine Verbindung zu Erna Eiscreme herzustellen:

Bild B-3: Herstellen einer Verbindung mit NetMeeting

➤ Geben Sie in Ihr bereits gestartetes NetMeeting die gewünschte Telefonnummer ein: *2468*.

- Alternativ zur Telefonnummer können Sie auch den Usernamen oder den Alias eingeben.
- Klicken Sie rechts neben dem Eingabefeld auf die Schaltfläche **Anrufen** (d.h. auf die Schaltfläche mit Telefonsymbol).

  Die Verbindung wird hergestellt.

Nur wenn NetMeeting am Heimarbeitsplatz bereits gestartet ist und sich beim Gatekeeper in der Firmenzentrale registriert hat, ist die Kommunikation in beide Richtungen möglich. Das bedeutet: der Mitarbeiter am Heimarbeitsplatz kann einen Kollegen in der Firmenzentrale mittels NetMeeting anrufen, es können aber auch alle Mitarbeiter in der Firmenzentrale mit Hilfe von Microsoft NetMeeting oder mittels IP-Telefon mit dem Kollegen am Heimarbeitsplatz kommunizieren.

Wenn die Verbindung zwischen Heimarbeitsplatz und Firmenzentrale steht, bleibt sie offen, bis Microsoft NetMeeting am Heimarbeitsplatz beendet wird. (Eine offene Verbindung wird wegen des Parameters **Time to Live (sec)** (siehe Tabelle A-5, Seite 28) benötigt.).

Wir empfehlen Ihnen, einen Flatrate-Zugang zum Internet zu verwenden.

2.3.4 Verbindungen anzeigen lassen

Sie können sich als Administrator des BinTec-Routers sowohl die momentan aktiven Verbindungen als auch die bereits beendeten Verbindungen anzeigen lassen.

Aktive Verbindungen

Gehen Sie folgendermaßen vor, um die aktiven Verbindungen anzeigen zu lassen:

- Gehen Sie zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Active Calls***.

  Die momentan aktiven Verbindungen werden angezeigt.

In unserem Beispiel halten Karin Keks und Erna Eiscreme gerade eine Besprechung ab:

```
BinTec-Router 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
```

Sie können detaillierte Informationen zu jeder Verbindung erhalten:

➤ Wählen Sie den gewünschte Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste:

```
BinTec-Router 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-Adress  :   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
```

Beendete Verbindungen

Gehen Sie folgendermaßen vor, um bereits beendete Verbindungen anzuzeigen:

➤ Gehen Sie zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Call History***.

Die bereits beendeten Verbindungen werden angezeigt.

In unserem Beispiel wurden zwei Besprechungen abgehalten, eine vormittags, die andere nachmittags:

```
BinTec-Router 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
```

Sie können ebenfalls zu jedem Anruf detaillierte Informationen erhalten:

➤ Wählen Sie den gewünschte Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste. Darin werden Sie u.a. informiert, wer, wen, wie lange angerufen hat.

3 NetMeeting und DynDNS mit einem BinTec-Router

3.1 Einführung

Mit Hilfe eines BinTec-Routers können Sie mittels Microsoft NetMeeting über das Internet mit einem anderen NetMeeting-Benutzer kommunizieren.

DynDNS

Ihr Router benötigt außerhalb seines LANs keine feste IP-Adresse. Die dynamische IP-Adresse wird über die BinTec-Router-Funktion "Dynamic DNS (DynDNS") bekanntgegeben, wenn Sie einen Host-Namen für Ihren Router bei einem DynDNS-Provider registriert und Ihren Router entsprechend eingerichtet haben. Detaillierte Informationen zur Funktion "DynDNS" finden Sie in den **Release Notes 6.2.2**.

Ihr Kommunikationspartner benötigt lediglich einen PC mit ISDN-Karte, auf dem Microsoft NetMeeting installiert ist, oder eine andere direkte Einwahlmöglichkeit, z. B. T-DSL mit Modem und Netzwerkkarte.

Vorgehensweise

Inbetriebnahme, Test und Anwendung von Microsoft NetMeeting gliedern sich im vorliegenden Fall in vier Schritte:

- Registrieren von NetMeeting beim BinTec-Gatekeeper (Abschnitt B, Kapitel 3.3.1, Seite 60)
- Überprüfen der Registrierung (Abschnitt B, Kapitel 3.3.2, Seite 65)
- Testverbindung (Abschnitt B, Kapitel 3.3.3, Seite 66)
- Verbindungen anzeigen lassen (Abschnitt B, Kapitel 3.3.4, Seite 68).

3.2 Voraussetzungen

Für die Nutzung von NetMeeting empfiehlt es sich, einen Flatrate-Zugang zum Internet zu verwenden.

Aus Sicherheitsgründen unterstützt BinTec Communications AG die NetMeeting-Funktionen "Desktop Sharing" und "Whiteboard" nicht.

Wenn Sie NetMeeting zusammen mit Gatekeeper- bzw. Proxy-Funktionalität einsetzen, können Sie den "Internet Locator Server" von Microsoft nicht nutzen.

Verfügbarkeit von H.323-Proxy und H.323-Gatekeeper

Sie können Microsoft NetMeeting zusammen mit der Gatekeeper- und Proxy-Funktionalität eines BinTec-Routers der X-Generation ab Software-Release 6.2.1 nutzen. Wenn Sie die Geräte **X1000**, **X1200** oder **X3200** betreiben, so sind die Sicherheitslösung IPSec und Gatekeeper bzw. Proxy nicht gleichzeitig verfügbar.

Um sicherzustellen, daß Ihr Router über Gatekeeper- und Proxy-Funktionalität verfügt, gehen Sie folgendermaßen vor:

Routertyp

➤ Überprüfen Sie, welchen Routertyp Sie in Betrieb haben.

X1000, X1200, X3200

Bei den Routern **X1000**, **X1200** und **X3200**:

➤ Kontrollieren Sie, ob Ihr Gerät mit IPSec-System-Software betrieben wird.

Bei Software-Release 6.2.1 mit IPSec:

➤ Installieren Sie Software-Release 6.2.1 ohne IPSec oder erweben Sie einen BinTec-Router der X-Generation, der IPSec und Gatekeeper- bzw. Proxy-Funktionalität gleichzeitig zur Verfügung stellt.

Bei Software-Release 6.2.1 ohne IPSec sind Gatekeeper und Proxy verfügbar.

Andere Geräte der X-Generation

Bei allen anderen Geräten der X-Generation:

- Überprüfen Sie, ob Software-Release 6.2.1 auf dem Router installiert ist. Falls Ihr Gerät einen älteren Software-Stand aufweist, führen Sie ein Software-Update durch. Informationen zum Software-Update finden Sie im Benutzerhandbuch zu Ihrem BinTec-Router.

3.3 Konfiguration und Monitoring

In der folgenden grafischen Darstellung sehen Sie zwei PCs, die in das Internet eingewählt sind. Einer von beiden ist über einen BinTec-Router an das Internet angeschlossen:

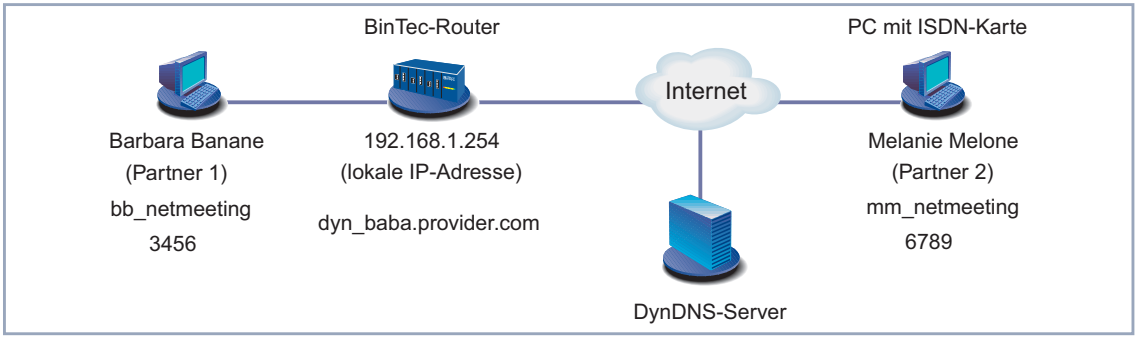

Bild B-4: Zwei PCs eingewählt in das Internet

3.3.1 Registrieren von NetMeeting beim BinTec-Gatekeeper

Überblick

Damit "Partner 1" und "Partner 2" (siehe Bild B-4, Seite 60) miteinander kommunizieren können, müssen sie beim BinTec-Gatekeeper registriert sein. Sowohl bei NetMeeting als auch beim BinTec-Router müssen dazu entsprechende Voraussetzungen geschaffen werden:

- Der Administrator des BinTec-Routers muß für beide Partner einen **Username** vergeben und ihn in die ***USER TABLE*** des Gatekeepers eintragen. Er muß dafür sorgen, daß bei der Registrierung auf diese Einträge zurückgegriffen wird.

- NetMeeting von "Partner 1" und NetMeeting von "Partner 2" (siehe Bild B-4, Seite 60) müssen entsprechend eingerichtet werden, so daß sich das jeweilige NetMeeting beim Gatekeeper des BinTec-Routers registriert.

Vorgehensweise

Der Administrator des BinTec-Routers sorgt durch Aktivierung des Proxy dafür, daß das NetMeeting von "Partner 2" Zugang zum Netz von "Partner 1" erhält.

Der Administrator trägt die gewünschten Daten der beiden Kommunikationspartner in die ***USER TABLE*** des Gatekeepers ein.

Beide Partner tragen bei ihrem NetMeeting nur den Alias sowie den Gatekeeper ein, bei dem sich NetMeeting registrieren soll. Die Registrierung selbst erfolgt automatisch.

Anstelle von NetMeeting können Sie auch andere H.323-fähige Endgeräte benutzen, wenn sie beim BinTec-Gatekeeper registriert werden.

Konfigurieren Ihres BinTec-Routers

Im folgenden erläutern wir Ihnen, welche Einstellungen Sie als Administrator bei Ihrem BinTec-Router vornehmen müssen, damit sich NetMeeting von "außen" in Ihr Netzwerk einwählen kann.

Proxy aktivieren

Um den Proxy Ihres BinTec-Routers für einen Zugang mit NetMeeting zu konfigurieren, gehen Sie im Setup Tool folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***PROXY SETTINGS***.
- Belassen Sie die Voreinstellungen.
- Wählen Sie **Proxy** aus: *running*.
- Bestätigen Sie mit **SAVE**.
  Der Proxy ist aktiviert.

Daten für NetMeeting in User Table eintragen

Um die Daten für NetMeeting von "Partner 1" und "Partner 2" in die ***USER TABLE*** Ihres BinTec-Gatekeepers einzutragen, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***GATEKEEPER SETTINGS*** ➧ ***USER TABLE*** ➧ ***ADD***.
- Geben Sie **Username** ein, z. B. ***Barbara Banane***.
- Geben Sie **Alias** ein, z. B. ***bb_netmeeting***.

- Geben Sie **E.164** ein, z. B. ***3456***.
- Geben Sie gegebenenfalls **E-Mail** ein, z. B. ***barban@bintec.de***.
- Überspringen Sie **IP Address**.
- Bestätigen Sie mit **SAVE**.

  Sie befinden sich im Menü ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***User Table*** .
- Fügen Sie einen neuen Eintrag mit **ADD** hinzu.
- Geben Sie **Username** ein, z. B. ***Melanie Melone***.
- Geben Sie **Alias** ein, z. B. ***mm_netmeeting***.
- Geben Sie **E.164** ein, z. B. ***6789***.
- Geben Sie gegebenenfalls **E-Mail** ein, z. B. ***melmel@bintec.de***.
- Überspringen Sie **IP Address**.
- Bestätigen Sie mit **SAVE**.

  Die Einträge sind temporär gespeichert und aktiviert.

Gatekeeper Parameter einstellen

Gehen Sie folgendermaßen vor, um sicherzustellen, daß sich nur die Endgeräte registrieren können, die in die ***User Table*** eingetragen sind:

- Gehen Sie zu ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings***.

Sie sehen folgendes Menü:

```
BinTec-Router 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
```

- Wählen Sie **Type of Registration** aus: *limited to user table*.
- Bei den übrigen Parametern belassen Sie die Voreinstellungen.
- Bestätigen Sie mit **SAVE**.

Gatekeeper einschalten

Um den Gatekeeper mit den bereits erfolgten Einstellungen zu aktivieren, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***Gatekeeper Settings***.
- Wählen Sie **Gatekeeper** aus: *running*.
- Bestätigen Sie mit **SAVE**.

  Der Gatekeeper ist jetzt aktiv.

NetMeeting konfigurieren

Im folgenden erklären wir, welche Einstellungen "Partner 1" und "Partner 2" beim Programm NetMeeting vornehmen müssen, damit das jeweilige NetMeeting sich beim BinTec-Gatekeeper registrieren kann.

Bevor Sie beginnen, stellen Sie sicher, daß Microsoft NetMeeting ordnungsgemäß auf Ihrem PC installiert ist.

Gatekeeper bei NetMeeting eintragen ("Partner 1")

Um als "Partner 1" bei Ihrem Microsoft NetMeeting den BinTec-Gatekeeper einzutragen, gehen Sie folgendermaßen vor:

- Starten Sie NetMeeting auf dem PC.
- Gehen Sie zu **Extras** ➧ **Optionen**.
- Klicken Sie auf **Erweiterte Anrufoptionen**.
- Aktivieren Sie das Kontrollkästchen **Einen Gatekeeper zum Anrufen verwenden** und geben Sie die IP-Adresse des BinTec-Gatekeepers ein, z. B. ***192.168.1.254***.
- Aktivieren Sie das Kontrollkästchen **Mit Kontonamen anmelden** und geben Sie den gewünschten Namen ein, z. B. ***bb_netmeeting***.
- Schließen Sie beide Fenster mit **OK**.
- Starten Sie NetMeeting erneut.

  NetMeeting von "Partner 1" registriert sich beim Gatekeeper.

Gatekeeper bei NetMeeting eintragen ("Partner 2")

Um als "Partner 2" bei Ihrem Microsoft NetMeeting den BinTec-Gatekeeper einzutragen, gehen Sie folgendermaßen vor:

- Starten Sie NetMeeting auf dem PC.
- Gehen Sie zu **Extras** ➧ **Optionen**.
- Klicken Sie auf **Erweiterte Anrufoptionen**.
- Aktivieren Sie das Kontrollkästchen **Einen Gatekeeper zum Anrufen verwenden** und geben Sie den DynDNS-Namen des BinTec-Gatekeepers ein, z. B. ***dyn_baba.provider.com***.
- Aktivieren Sie das Kontrollkästchen **Mit Kontonamen anmelden** und geben Sie den gewünschten Namen ein, z. B. ***mm_netmeeting***.
- Schließen Sie beide Fenster mit **OK**.
- Starten Sie NetMeeting erneut.

  NetMeeting von "Partner 2" registriert sich beim Gatekeeper.

3.3.2 Überprüfen der Registrierung

Um zu prüfen, ob die Registrierung von Microsoft NetMeeting von "Partner 1" und "Partner 2" beim Gatekeeper Ihres BinTec-Routers erfolgreich war, gehen Sie als Administrator des BinTec-Routers folgendermaßen vor:

➤ Gehen Sie im Setup-Tool-Menü zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Registered Users***.

Wenn NetMeeting von "Partner 1" und von "Partner 2" aus unserem Beispiel ordungsgemäß registriert sind, sehen Sie folgendes:

```
BinTec-Router 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
```

Sie können zu jedem Eintrag detaillierte Informationen erhalten:

➤ Wählen Sie z. B. den ersten Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste:

```
BinTec-Router 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 Testverbindung

Um zu testen, ob "Partner 1" mit "Partner 2" kommunizieren kann, stellt z. B. "Partner 1" eine Verbindung zu "Partner 2" her.

Rufen Sie als "Partner 1" Melanie Melone mit dem Alias mm_netmeeting und der Telefonnummer 6789 (siehe Bild B-4, Seite 60) an. Sie können die Telefonnummer, den Usernamen oder den Alias eingeben, um die Verbindung herzustellen.

Gehen Sie folgendermaßen vor, um eine Verbindung zu Melanie Melone herzustellen:

Bild B-5: Herstellen einer Verbindung mit NetMeeting

- Geben Sie in Ihr bereits gestartetes NetMeeting die gewünschte Telefonnummer ein: *6789*.
- Alternativ zur Telefonnummer können Sie auch den Usernamen oder den Alias eingeben.
- Klicken Sie rechts neben dem Eingabefeld auf die Schaltfläche **Anrufen** (d.h. auf die Schaltfläche mit Telefonsymbol).

  Die Verbindung wird hergestellt.

Die Kommunikation ist in beide Richtungen möglich. Das bedeutet: es ist gleichgültig, ob "Partner 1" "Partner 2" anruft oder "Partner 2" "Partner 1", die Verbindung wird in jedem Fall unverzüglich hergestellt.

Wenn die Verbindung zwischen beiden Kommunikationspartnern steht, bleibt sie offen, da eine offene Verbindung wegen des Parameters **Time to Live (sec)** (siehe Tabelle A-5, Seite 28) benötig wird.

Wir empfehlen Ihnen, einen Flatrate-Zugang zum Internet zu verwenden.

3.3.4 Verbindungen anzeigen lassen

Sie können sich als Administrator des BinTec-Routers sowohl die momentan aktiven Verbindungen als auch die bereits beendeten Verbindungen anzeigen lassen.

Aktive Verbindungen

Gehen Sie folgendermaßen vor, um die aktiven Verbindungen anzeigen zu lassen:

➤ Gehen Sie zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Active Calls***.

Die momentan aktiven Verbindungen werden angezeigt.

In unserem Beispiel hat Barbara Banane gerade Kontakt zu Melanie Melone aufgenommen:

```
BinTec-Router 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
```

Sie können detaillierte Informationen zu jeder Verbindung erhalten:

➤ Wählen Sie den gewünschte Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste:

```
BinTec-Router 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-Adress  :   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
```

Beendete Verbindungen

Gehen Sie folgendermaßen vor, um bereits beendete Verbindungen anzuzeigen:

➤ Gehen Sie zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Call History***.

Die bereits beendeten Verbindungen werden angezeigt.

In unserem Beispiel haben Barbara Banane und Melanie Melone dreimal miteinander gesprochen:

```
BinTec-Router 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 Banabe 3456       14:07:45



       EXIT


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

Sie können ebenfalls zu jedem Anruf detaillierte Informationen erhalten:

➤ Wählen Sie den gewünschte Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste. Darin werden Sie u.a. informiert, wer, wen, wie lange angerufen hat.

4 NetMeeting und DynDNS mit zwei BinTec-Routern

4.1 Einführung

Als Nutzer eines BinTec-Routers können Sie mittels Microsoft NetMeeting über das Internet mit einem anderen NetMeeting-Benutzer kommunizieren, der ebenfalls über einen BinTec-Router erreichbar ist.

DynDNS Beide BinTec-Router benötigen außerhalb ihres LANs keine feste IP-Adresse. Die dynamischen IP-Adressen werden über die BinTec-Router-Funktion "Dynamic DNS (DynDNS)" bekanntgegeben, wenn für beide Router jeweils ein Host-Name bei einem DynDNS-Provider registriert ist und die Router entsprechend eingerichtet sind. Detaillierte Informationen zur Funktion "DynDNS" finden Sie in den **Release Notes 6.2.2**.

Vorgehensweise Inbetriebnahme, Test und Anwendung von Microsoft NetMeeting gliedern sich im vorliegenden Fall in vier Schritte:

- Registrieren von NetMeeting beim BinTec-Gatekeeper (Abschnitt B, Kapitel 4.3.1, Seite 73)
- Überprüfen der Registrierung (Abschnitt B, Kapitel 4.3.2, Seite 78)
- Testverbindung (Abschnitt B, Kapitel 4.3.3, Seite 79)
- Verbindungen anzeigen lassen (Abschnitt B, Kapitel 4.3.4, Seite 81).

4.2 Voraussetzungen

Für die Nutzung von NetMeeting empfiehlt es sich, einen Flatrate-Zugang zum Internet zu verwenden.

Für einen Spezialfall, den Sie ebenfalls in diesem Szenario finden (siehe "Gatekeeper Parameter einstellen", Seite 75 und "Testverbindung", Seite 79) benötigen Sie keinen Flatrate-Zugang zum Internet.

Aus Sicherheitsgründen unterstützt BinTec Communications AG die NetMeeting-Funktionen "Desktop Sharing" und "Whiteboard" nicht.

Wenn Sie NetMeeting zusammen mit Gatekeeper- bzw. Proxy-Funktionalität einsetzen, können Sie den "Internet Locator Server" von Microsoft nicht nutzen.

Verfügbarkeit von H.323-Proxy und H.323-Gatekeeper

Sie können Microsoft NetMeeting zusammen mit der Gatekeeper- und Proxy-Funktionalität eines BinTec-Routers der X-Generation ab Software-Release 6.2.1 nutzen. Wenn Sie die Geräte **X1000**, **X1200** oder **X3200** betreiben, so sind die Sicherheitslösung IPSec und Gatekeeper bzw. Proxy nicht gleichzeitig verfügbar.

Um sicherzustellen, daß Ihr Router über Gatekeeper- und Proxy-Funktionalität verfügt, gehen Sie folgendermaßen vor:

Routertyp

➤ Überprüfen Sie, welchen Routertyp Sie in Betrieb haben.

X1000, X1200, X3200

Bei den Routern **X1000**, **X1200** und **X3200**:

➤ Kontrollieren Sie, ob Ihr Gerät mit IPSec-System-Software betrieben wird.

Bei Software-Release 6.2.1 mit IPSec:

➤ Installieren Sie Software-Release 6.2.1 ohne IPSec oder erweben Sie einen BinTec-Router der X-Generation, der IPSec und Gatekeeper- bzw. Proxy-Funktionalität gleichzeitig zur Verfügung stellt.

Bei Software-Release 6.2.1 ohne IPSec sind Gatekeeper und Proxy verfügbar.

Andere Geräte der X-Generation

Bei allen anderen Geräten der X-Generation:

➤ Überprüfen Sie, ob Software-Release 6.2.1 auf dem Router installiert ist. Falls Ihr Gerät einen älteren Software-Stand aufweist, führen Sie ein Software-Update durch. Informationen zum Software-Update finden Sie im Benutzerhandbuch zu Ihrem BinTec-Router.

4.3 Konfiguration und Monitoring

In der folgenden grafischen Darstellung sehen Sie zwei PCs, die jeweils über einen BinTec-Router in das Internet eingewählt sind:

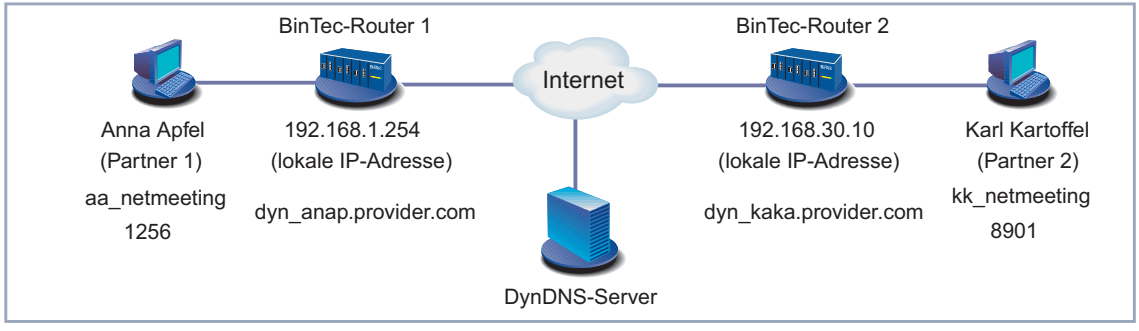

Bild B-6: Kommunikation zweier PCs über BinTec-Router und Internet

4.3.1 Registrieren von NetMeeting beim BinTec-Gatekeeper

Überblick

Damit "Partner 1" und "Partner 2" miteinander kommunizieren können, müssen sie beim Gatekeeper ihres jeweiligen BinTec-Routers registriert sein. Sowohl bei NetMeeting als auch beim BinTec-Router müssen dazu entsprechende Voraussetzungen geschaffen werden:

- Der Administrator des jeweiligen BinTec-Routers muß für "seinen" Nutzer einen **Username** vergeben und ihn in die ***USER TABLE*** des Gatekeepers eintragen. Er muß dafür sorgen, daß bei der Registrierung auf diesen Eintrag zurückgegriffen wird.

- "Partner 1" und "Parner 2" müssen das Programm NetMeeting jeweils so einrichten, daß NetMeeting von "Partner 1" beim Gatekeeper des "BinTec-Routers 1" und NetMeeting von "Partner 2" beim Gatekeeper des "BinTec-Routers 2" registriert wird.
- Die beiden Gatekeepern müssen einander "kennen".

Vorgehensweise

Die Administratoren der BinTec-Router sorgen durch Aktivierung des Proxy dafür, daß die jeweils "andere Seite" Zugang zu ihrem Netz erhält.

Jeder Administrator trägt die gewünschten Daten "seines" Nutzers in die ***USER TABLE*** seines Gatekeepers ein.

Jeder Nutzer trägt bei seinem NetMeeting nur den Alias sowie den Gatekeeper ein, bei dem sich NetMeeting registrieren soll. Die Registrierung selbst erfolgt automatisch.

Damit jeder Nutzer von der Existenz des jeweils anderen "weiß", tragen beide Administratoren den Gatekeeper der "anderen Seite" als alternativen Gatekeeper in ihren BinTec-Router ein.

Anstelle von NetMeeting können Sie auch andere H.323-fähige Endgeräte benutzen, wenn sie beim BinTec-Gatekeeper registriert werden.

Konfigurieren Ihres BinTec-Routers (Administrator)

Im folgenden erläutern wir Ihnen, welche Einstellungen Sie als Administrator bei Ihrem BinTec-Router vornehmen müssen.

Proxy aktivieren

Um den Proxy Ihres BinTec-Routers für einen Zugang mit NetMeeting zu konfigurieren, gehen Sie im Setup Tool folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***PROXY SETTINGS***.
- Belassen Sie die Voreinstellungen.
- Wählen Sie **Proxy** aus: *running*.
- Bestätigen Sie mit **SAVE**.
  Der Proxy ist aktiviert.

Daten für NetMeeting in User Table eintragen ("Partner 1")

Um als Administrator des "BinTec-Routers 1" die Daten für NetMeeting von "Partner 1" in die ***USER TABLE*** Ihres Gatekeepers einzutragen, gehen Sie folgendermaßen vor:

- Gehen Sie zu ***VoIP*** ➧ ***GATEKEEPER SETTINGS*** ➧ ***USER TABLE*** ➧ ***ADD***.
- Geben Sie **Username** ein, z. B. ***Anna Apfel***.
- Geben Sie **Alias** ein, z. B. ***aa_netmeeting***.
- Geben Sie **E.164** ein, z. B. ***1256***.
- Geben Sie gegebenenfalls **E-Mail** ein, z. B. ***annapf@bintec.de***.
- Überspringen Sie **IP Address**.
- Bestätigen Sie mit **SAVE**.

  Die Einträge sind temporär gespeichert und aktiviert.

Daten für NetMeeting in User Table eintragen ("Partner 2")

Um als Administrator des "BinTec-Routers 2" die Daten für NetMeeting von "Partner 2" in die ***USER TABLE*** Ihres Gatekeepers einzutragen, gehen Sie folgendermaßen vor:

- Geben Sie **Username** ein, z. B. ***Karl Kartoffel***.
- Geben Sie **Alias** ein, z. B. ***kk_netmeeting***.
- Geben Sie **E.164** ein, z. B. ***8901***.
- Geben Sie gegebenenfalls **E-Mail** ein, z. B. ***karkar@bintec.de***.
- Überspringen Sie **IP Address**.
- Bestätigen Sie mit **SAVE**.

  Die Einträge sind temporär gespeichert und aktiviert.

Gatekeeper Parameter einstellen

Im folgenden erklären wir Ihnen, wie Sie als Administrator von "BinTec-Router 1" sicherstellen, daß sich nur die Endgeräte registrieren können, die in die ***USER TABLE*** eingetragen sind und wie Sie den alternativen Gatekeeper eintragen. Der Administrator von "BinTec-Router 2" muß bei seinem Router entsprechend vorgehen.

Der Eintrag des alternativen Gatekeepers entfällt, wenn Sie bei NetMeeting eine Adresse im Format Name@DynDNSName benutzen, z. B. ***karl@dyn_kaka.provider.com*** (siehe Bild B-6, Seite 73 bzw. "Testverbindung", Seite 79), um Ihren Kommunikationspartner zu erreichen.

Gehen Sie für "BinTec-Router 1" folgendermaßen vor:

➤ Gehen Sie zu ***VoIP*** ➧ ***Gatekeeper Settings*** ➧ ***Global Settings***.

Sie sehen folgendes Menü:

```
BinTec-Router 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
```

➤ Wählen Sie **Type of Registration** aus: *limited to user table*.

➤ Geben Sie **Alternate Gatekeeper (Priority 0)** ein, z. B. ***dyn_kaka.provider.com***.

➤ Bei den übrigen Parametern belassen Sie die Voreinstellungen.

➤ Bestätigen Sie mit **SAVE**.

Gatekeeper einschalten

Um den Gatekeeper mit den bereits erfolgten Einstellungen zu aktivieren, gehen Sie folgendermaßen vor:

➤ Gehen Sie zu ***VoIP*** ➧ ***Gatekeeper Settings***.

➤ Wählen Sie **Gatekeeper** aus: *running*.

➤ Bestätigen Sie mit **SAVE**.

Der Gatekeeper ist jetzt aktiv.

NetMeeting konfigurieren (PC-Benutzer)

Im folgenden erklären wir Ihnen, welche Einstellungen Sie beim Programm NetMeeting vornehmen müssen, damit NetMeeting sich beim Gatekeeper des BinTec-Routers registrieren kann.

Bevor Sie beginnen, stellen Sie sicher, daß Microsoft NetMeeting ordnungsgemäß auf Ihrem PC installiert ist.

Gatekeeper bei NetMeeting eintragen ("Partner 1")

Um als "Partner 1" bei Ihrem Microsoft NetMeeting den Gatekeeper des "BinTec-Router 1" einzutragen (siehe Bild B-6, Seite 73), gehen Sie folgendermaßen vor:

- Starten Sie das Programm NetMeeting auf Ihrem PC.
- Gehen Sie zu **Extras** ➧ **Optionen**.
- Klicken Sie auf **Erweiterte Anrufoptionen**.
- Aktivieren Sie das Kontrollkästchen **Einen Gatekeeper zum Anrufen verwenden** und geben Sie die IP-Adresse des Gatekeepers ein, z. B. ***192.168.1.254***.
- Aktivieren Sie das Kontrollkästchen **Mit Kontonamen anmelden** und geben Sie den gewünschten Namen ein, z. B. ***aa_netmeeting***.
- Schließen Sie beide Fenster mit **OK**.
- Starten Sie NetMeeting erneut.

  NetMeeting von "Partner 1" registriert sich beim Gatekeeper von "BinTec-Router 1".

Gatekeeper bei NetMeeting eintragen (Partner 2)

Um als "Partner 2" bei Ihrem Microsoft NetMeeting den Gatekeeper des "BinTec-Router 2" einzutragen (siehe Bild B-6, Seite 73), gehen Sie folgendermaßen vor:

- Starten Sie das Programm NetMeeting auf Ihrem PC.
- Gehen Sie zu **Extras** ➧ **Optionen**.
- Klicken Sie auf **Erweiterte Anrufoptionen**.
- Aktivieren Sie das Kontrollkästchen **Einen Gatekeeper zum Anrufen verwenden** und geben Sie die IP-Adresse des Gatekeepers ein, z. B. ***192.168.30.10***.

- Aktivieren Sie das Kontrollkästchen **Mit Kontonamen anmelden** und geben Sie den gewünschten Namen ein, z. B. ***kk_netmeeting***.
- Schließen Sie beide Fenster mit **OK**.
- Starten Sie NetMeeting erneut.

  NetMeeting von "Partner 2" registriert sich beim Gatekeeper von "BinTec-Router 2".

4.3.2 Überprüfen der Registrierung

Der Administrator von "BinTec-Router 1" bzw. "BinTec-Router 2" überprüft die Registrierung beim Gatekeeper folgendermaßen:

- Gehen Sie im Setup-Tool-Menü zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Registered Users***.

Wenn NetMeeting von "Partner 1" aus unserem Beispiel ordungsgemäß registriert ist, sehen Sie folgendes (bei NetMeeting von "Partner 2" entsprechend):

```
BinTec-Router 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
```

Sie können zu jedem Eintrag detaillierte Informationen erhalten.

- Wählen Sie einen Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste:

```
BinTec-Router 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 Testverbindung

Um zu testen, ob "Partner 1" mit "Partner 2" kommunizieren kann, stellt z. B. "Partner 1" eine Verbindung zu "Partner 2" her.

Rufen Sie als "Partner 1" Karl Kartoffel mit dem Alias kk_netmeeting und der Telefonnummer 8901 (siehe Bild B-6, Seite 73) an. Sie können die Telefonnummer, den Usernamen oder den Alias eingeben, um die Verbindung herzustellen.

Sie können auch eine Adresse im Format Name@DynDNSName eingeben, z. B. ***karl@dyn_kaka.provider.com***. Der Teil nach dem @-Zeichen wird dabei als DnyDNS-Name interpretiert.

Gehen Sie folgendermaßen vor, um eine Verbindung zu Karl Kartoffel herzustellen:

Bild B-7: Herstellen einer Verbindung mit NetMeeting

- Geben Sie in Ihr bereits gestartetes NetMeeting die gewünschte Telefonnummer ein: *8901*.
- Alternativ zur Telefonnummer können Sie auch den Usernamen, den Alias oder eine Adresse im Format Name@DynDNSName eingeben.
- Klicken Sie rechts neben dem Eingabefeld auf die Schaltfläche **Anrufen** (d.h. auf die Schaltfläche mit Telefonsymbol).

  Die Verbindung wird hergestellt.

Die Kommunikation ist in beide Richtungen möglich. Das bedeutet: es ist gleichgültig, ob "Partner 1" "Partner 2" anruft oder "Partner 2" "Partner 1", die Verbindung wird in jedem Fall unverzüglich hergestellt.

Wenn alternative Gatekeeper eingetragen sind, bleibt die Verbindung zwischen beiden Routern immer offen, da eine offene Verbindung wegen des Parameters **Time to Live (sec)** (siehe Tabelle A-5, Seite 28) benötig wird.

Wir empfehlen Ihnen, einen Flatrate-Zugang zum Internet zu verwenden.

4.3.4 Verbindungen anzeigen lassen

Sie können sich als Administrator eines BinTec-Routers sowohl die momentan aktiven Verbindungen als auch die bereits beendeten Verbindungen anzeigen lassen.

Aktive Verbindungen

Gehen Sie folgendermaßen vor, um die aktiven Verbindungen anzeigen zu lassen:

➤ Gehen Sie zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Active Calls***.

Die momentan aktiven Verbindungen werden angezeigt.

In unserem Beispiel hat Anna Apfel gerade Verbindung zu Karl Kartoffel aufgenommen:

```
BinTec-Router 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
```

Sie können detaillierte Informationen zu jeder Verbindung erhalten:

➤ Wählen Sie den gewünschte Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste:

```
BinTec-Router 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-Adress  :   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
```

Beendete Verbindungen

Gehen Sie folgendermaßen vor, um bereits beendete Verbindungen anzuzeigen:

➤ Gehen Sie zu ***VoIP*** ➧ ***Monitoring*** ➧ ***Call History***.

Die bereits beendeten Verbindungen werden angezeigt.

In unserem Beispiel wurde an diesem Tag vier Verbindungen hergestellt:

```
BinTec-Router 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
```

Sie können ebenfalls zu jeder Verbindung detaillierte Informationen erhalten.

➤ Wählen Sie den gewünschte Eintrag aus und drücken Sie **Return**.

Sie erhalten eine detaillierte Liste. Darin werden Sie u.a. informiert, wer, wen, wie lange angerufen hat.