

# Videoconferencing und Firewall / NAT – Ein Problem?

Stand: Mai 2007

## Einleitung

Als 1996 die ITU-T-Arbeitsgruppe 16 die Version 1 des H.323-Standards verabschiedete, waren Firewalls und private Adressräume eher ein theoretisches Thema. Seit 1996 hat sich in der Praxis viel getan und die heutige Version 6 des Standards beinhaltet viele Neuerungen, speziell in dem Bereich des Firewalling und NAT- (Network Address Translation) traversal. Dieses Dokument soll einen Überblick über Lösungsmöglichkeiten für das sog. H.323-Firewall-Problem geben. Dabei wird weniger auf technische Details eingegangen, denn es soll gezeigt werden, dass mit einfachen Mitteln das Problem umgangen bzw. gelöst werden kann. Im Kapitel „H.323-Videoconferencing – Ein Überblick“ wird ebenfalls kurz auf die Motivation eingegangen. Es soll die Frage beantwortet werden, wenn auch nicht in ihrer Gesamtheit, warum H.323 auch heute noch ein so wichtiger Standard ist, drängen doch andere Standards wie SIP oder Jingle auf den Markt.

## H.323-Videoconferencing – Ein Überblick

Wie bereits in der Einleitung angedeutet, ist der H.323-Standard von der Arbeitsgruppe 16 der ITU-T entwickelt und verabschiedet worden. Diese Arbeitsgruppe arbeitet auch heute noch an neuen Versionen dieses Standards. So ist zum Beispiel vor Kurzem die Version 6 dieses Standards verabschiedet worden.

Der H.323-Standard beschreibt nicht nur die Art und Weise wie Komponenten miteinander kommunizieren, er beschreibt ebenfalls die Komponenten selbst und die minimalen Voraussetzungen, damit diese voll H.323-fähig sind (H.323-compliant). H.323 selbst ist ein sog. „Dach“-Standard, der verschiedene weitere Standards vereint. Dazu gehören zum Beispiel H.245 (Signal Controlling), H.261 (Video codec), G.711 (Audio codec), um nur ein paar zu nennen. Abbildung 1 zeigt einen Überblick über die vereinten Standards.

H.323			
Verbindlich			Optional
<b>Audio</b>	<b>Video</b>	<b>Data</b>	H.263
G.711	H.261	H.225 H.245	H.264
			H.239
			H.450
			H.460
			T.120
			....

Abbildung 1: H.323-"Dach"-Standard

Heute wird H.323 fast ausschließlich als Standard für Videokonferenzen angesehen, dagegen das SIP-Protokoll meist mit Internet-Telefonie assoziiert wird. Das ist sicherlich eine Verkürzung, denn H.323 kann sowohl für Videokonferenzen, als auch für Audiokonferenzen verwendet werden. Eine heutige Analyse der Marktpenetration von Videokonferenztechnologien würde sicherlich zeigen, dass der größte Anteil H.323 zuzuordnen ist. Videoübertragung auf Basis des SIP-Protokolls ist auch möglich, derzeit aber ungebräuchlich.

Worin liegt nun das Problem im H.323-Standard bei Einsatz von Firewalls sowie privaten Adressräumen? Diese Fragestellung muss von zwei Seiten betrachtet werden, da das Firewall-Problem ein anderes ist als das NAT-Problem, auch wenn beide oft einhergehen.

### H.323 und Firewalls

Der H.323-Standard beschreibt, wie einzelne Komponenten miteinander kommunizieren. Dabei sind einige feste Ports definiert. Tabelle 1 zeigt einen Überblick der verwendeten Ports.

Port(s)	Typ	Beschreibung
1503	TCP (statisch)	T.120
1718	TCP (statisch)	H.323 Gatekeeper Discovery
1719	TCP (statisch)	H.323 Gatekeeper RAS
1720	TCP (statisch)	H.323 Verbindungsaufbau
1024-65535	TCP (dynamisch)	H.245 Verbindungsparameter
1024-65535	UDP (dynamisch)	RTP Audio
1024-65535	UDP (dynamisch)	RTP Video
1024-65535	UDP (dynamisch)	RTCP Kontroll Information

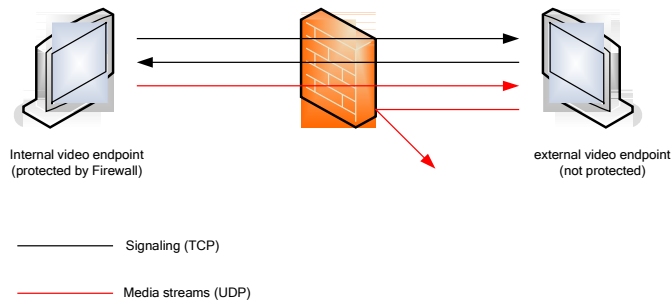
**Tabelle 1: Verwendete Ports in H.323**

Wie anhand von Tabelle 1 zu sehen ist, werden einige Ports dynamisch ausgehandelt. Während die Verbindung aufgebaut wird, betrifft das die Ports für RTP Audio, RTP Video, RTCP sowie H.245. Da diese Ports vorab nicht bekannt sind und die Ports auch aus dem gesamten oberen Portbereich (1024-65535) kommen, ist das ein Problem für Firewalls. Wie öffnet man Ports, wenn man diese nicht kennt? Die klassische Firewall-Konfiguration, das Festlegen von bestimmten Ports und IP-Adressen für eine Kommunikationsbeziehung genügen für eine H.323-Kommunikation nicht.

Eines der typischen Szenarien der Kommunikationsblockade durch Firewalls ist normalerweise, dass der externe Kommunikationspartner (außerhalb der Firewall), Audio und Video empfängt, aber der interne Kommunikationspartner (geschützt durch die Firewall), lediglich ein schwarzes Videofenster sieht, obwohl die Verbindung aufgebaut ist. Das liegt daran, dass heutige Firewalls (mit Stateful inspection) problemlos mit TCP-Verkehr umgehen können, so dass generell die Verbindung aufgebaut werden kann. Da nun aber die Medien-Ströme (Audio und Video) über dynamisch ausgehandelte UDP-Ports übertragen werden, blockt die Firewall den Verkehr von außen nach innen. Abbildung 2 zeigt ein solches Szenario.

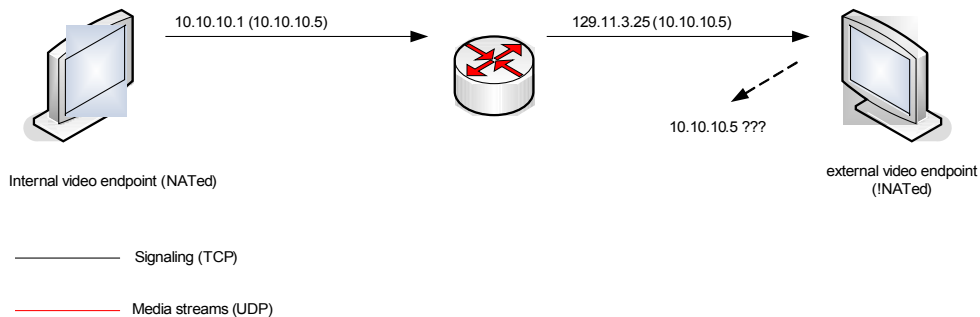
### H.323 und private Adressräume (NAT)

Private Adressräume in Netzwerken wurden in den letzten 2 bis 3 Jahren immer populärer. Als private Adressräume werden meistens die Netzadressbereiche 10.x.x.x oder 192.168.x.x verwendet. Diese speziellen Netzwerkbereiche wurden spezifiziert, um dem Mangel an IPv4-Adressen zu begegnen. Die Idee hinter privaten Adressräumen ist, dass für das interne Netzwerk ein solches privates Netz verwendet wird und der Router (Edge-Router) die privaten Adressen in öffentliche Adressen übersetzt. Die Übersetzung, auch NAT genannt, kann entweder statisch oder dynamisch sein.



**Abbildung 2: H.323-Firewall-Problem**

Die Problematik mit H.323 ist wie folgt: IP-Pakete einer H.323-Verbindung werden entweder über TCP (Signalströme) oder UDP (Medienströme) verschickt. Die H.323-Information in der Payload des TCP/UDP-Paketes enthält aber die Adressinformationen über die privaten Adressen der Endgeräte (Terminals). Durchläuft nun ein IP-Paket NAT, wird die Absenderadresse des IP-Paketes durch die offizielle Adresse des NAT-Gateways ersetzt. Hier ist nun der Knackpunkt: H.323-Endgeräte senden Signal- und Medienströme an die aus der Payload extrahierte private Adresse, aber nicht an das NAT-Gateway zurück.



**Abbildung 3: H.323-NAT-Problem**

Das hat zur Folge, dass alle H.323-Signal- und Medienströme an die private Adresse gesendet werden, das TCP/UDP-Paket, was beim Empfänger ankommt, aber die öffentliche Adresse des NAT-Gateways trägt. Der Empfänger nimmt das Paket an und versucht auf die H.323-Information zu reagieren, zum Beispiel mit einem Alert, welcher an die private IP-Adresse geschickt wird, die in der H.323-Payload gespeichert

ist. Obwohl der Empfänger keine Routinginformation zum privaten Netz hat, versucht der Empfänger etwas an die private Absenderadresse zu senden. Die Information geht verloren, da der Router nicht weiß, wohin das Paket geschickt werden soll. Das IP-Paket wird verworfen, das Videofenster bleibt schwarz. Abbildung 3 verdeutlicht das Problem.

### **Lösungsmöglichkeiten**

Die folgenden Abschnitte sollen einen kurzen Überblick über bekannte Lösungen zu dem H.323-Firewall-Problem sowie der H.323-NAT-Problematik geben. Im ersten Abschnitt wird das Prinzip des OpenFirewalling beschrieben. Der zweite Abschnitt beschreibt das Proxy-System, anhand des bekannten GnuG-Proxy/Gatekeeper-Systems. Im dritten Abschnitt wird die Lösung mittels Session-Border-Controller beschrieben, das prinzipiell auch als H.460 bekannt ist. Im letzten Abschnitt wird MCU-Tunneling beschrieben.

### **OpenFirewalling<sup>1</sup>**

Wie bereits im Abschnitt „H.323-Videoconferencing – Ein Überblick“ beschrieben wurde, werden bei H.323-Audio-/Videokonferenzen die zu verwendenden Ports dynamisch ausgehandelt. Dieses Verhalten bringt jedoch Probleme mit sich bei der Verwendung von Firewalls.

OpenFirewalling heißt schlichtweg, dass die Firewall für das H.323-Gerät deaktiviert wird. Die Firewall-Regeln oder Access-Listen sind so gebaut, dass sämtlicher Verkehr vom und zum Gerät möglich ist.

Es ist offensichtlich, dass das Prinzip des OpenFirewalling nur bedingt verwendbar ist. Vor allem bei Software-Codecs, die auf einem lokalen PC oder Laptop installiert werden, birgt dieses Verfahren erhebliche Sicherheitsrisiken. Solche Systeme können zum einen schützenswerte Daten enthalten, zum anderen könnte dieses System kompromittiert werden und ein Hacker kann sich so Zugriff zum Netzwerk verschaffen.

Die Lösung des OpenFirewalling ist daher nur bedingt empfehlenswert. Sicherlich ist dies eine alternative Lösung für Universitäten oder kleinere Einrichtungen, die nur ein H.323-fähiges Gerät besitzen. Für solch einen Fall ist OpenFirewalling durchaus verwendbar, allerdings unter der Voraussetzung, dass der Netzwerkadministrator zusätzliche Maßnahmen bzgl. IT-Sicherheit trifft und offizielle IP-Adressen im internen Netz einsetzt.

### **Proxy-Systeme**

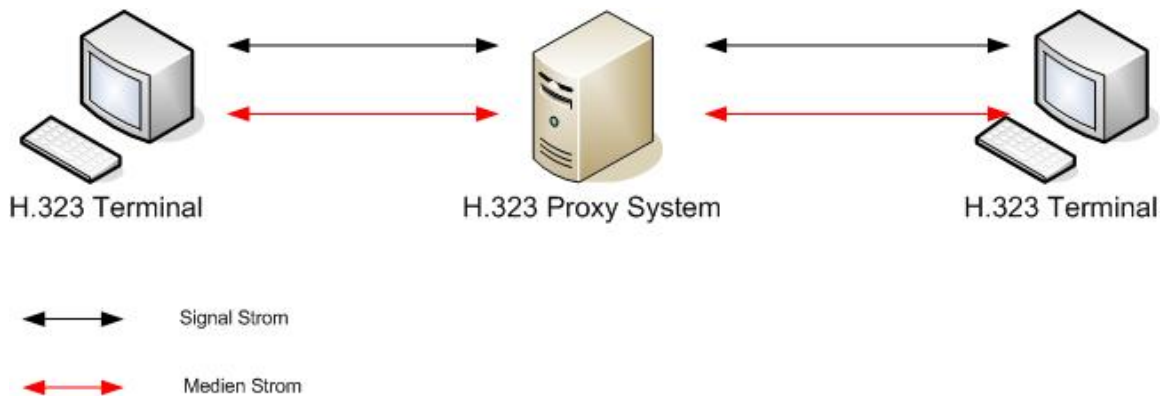
Im Gegensatz zu OpenFirewalling, sind Proxy-Systeme eine sichere und einfache Alternative. H.323-Proxy-Systeme arbeiten nach einem ähnlichen Prinzip wie Web-Proxy-Systeme.

Wie man anhand der Abbildung 4 erkennen kann, werden sämtliche Datenströme, die Signalströme (TCP) sowie die Medienströme (UDP) von einem H.323-Terminal zu

---

<sup>1</sup> Das Prinzip des OpenFirewalling geht nur bei Firewalls. Die NAT-Problematik kann damit nicht gelöst werden.

dem Proxy und von dort zum anderen H.323-Terminal übertragen.



**Abbildung 4: H.323-Videokonferenz via Proxy**

Durch diese Technologie kann gewährleistet werden, dass alle Endgeräte (Terminals), die sich im internen, geschützten Netz befinden, weiterhin durch die Firewall geschützt sind. Das Proxy-System sollte idealerweise in der DMZ<sup>2</sup> sein. Für den Fall, dass das nicht möglich ist, z.B. es existiert keine DMZ, sollte der Proxy durch eine Firewall geschützt werden. Der Proxy selbst muss allerdings eine öffentliche IP-Adresse haben.

Kann nun ein Proxy mit NAT umgehen? Ja, denn es werden 2 Verbindungen aufgebaut. Die erste Verbindung wird vom internen Gerät zum Proxy aufgebaut. Daher können im internen Netz private Adressen verwendet werden. Die zweite Verbindung zum externen Gerät wird dann vom Proxy initiiert, so dass alle H.323-Pakete, die das interne Netz verlassen, die externe IP-Adresse des Proxy beinhalten. Bei mehreren gleichzeitigen H.323-Verbindungen über einen Proxy regelt ein internes Session-Management die korrekte Verwaltung und Zuordnung der Signal- und Medienströme.

### **Session-Border-Controller / H.460**

Im Sommer 2005 hat die ITU den H.460.17/18/19-Standard verabschiedet. Dieser Standard beschreibt eine Lösung des H.323-Firewall/NAT-Problems. Verschiedene Hersteller, wie Radvision, Polycom und Tandberg, haben zu der Entwicklung beigetragen und Produkte sind nun ebenfalls erhältlich. Die untere Tabelle gibt einen kurzen Überblick über den Standard, und welche Ströme behandelt werden.

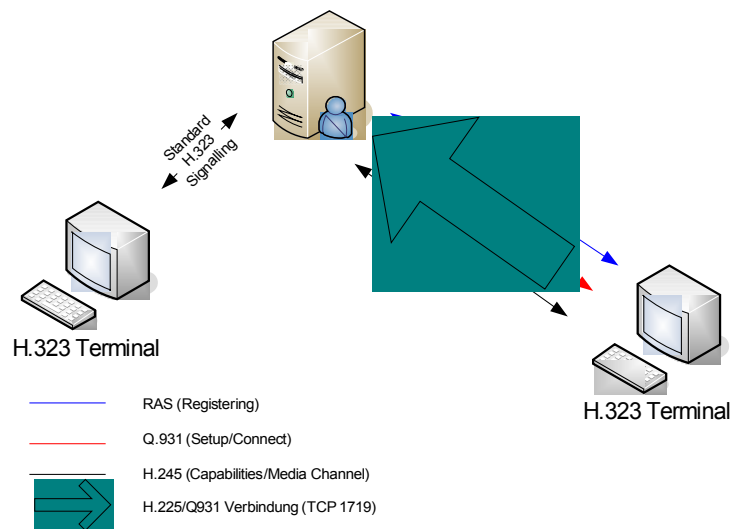
<sup>2</sup> Eine DMZ (Demilitarisierte Zone) in einem Netzwerk ist ein speziell konfigurierter Teil des Netzwerks, welcher als eine Art Puffer-Zone zwischen dem Internet und dem internen Netzwerk zu verstehen ist. Systeme in der DMZ sind oft durch spezielle Firewall-Regeln geschützt. Generell befinden sich Email- und auch Web-Server in der DMZ, da diese vom Internet her erreichbar sein müssen. Der Zugriff in ein DMZ-System ist sowohl vom internen als auch vom externen Netzwerk erlaubt. Der Zugriff von der DMZ aus ist nur zum externen Netzwerk erlaubt.

	<b>H.460.17</b>	<b>H.460.18</b>	<b>H.460.19</b>
<b>Medienströme</b>	Signal-Ströme (H.225/H.245)	Signal-Ströme (H.225/H.245)	Medien-Ströme (RTP)
<b>Hersteller / Entwickler</b>	Radvision	Tandberg Radvision Polycom	Radvision Tandberg Polycom

**Tabelle 2: H.460-Übersicht**

### H.460.17 (RAS over H.225)

Abbildung 5 verdeutlicht die Funktionsweise von H.460.17.



**Abbildung 5: Aufbau einer Verbindung via H.460.17**

Bei der Verwendung von H.460.17 wird die persistente H.225/Q.931-Verbindung genutzt, um die Verbindung aufrecht zu erhalten. Hierbei werden sog. Keep-alive-Nachrichten verwendet. Der Kanal selbst wird bei der ersten Registrierung des Endpoints am Gatekeeper geöffnet.

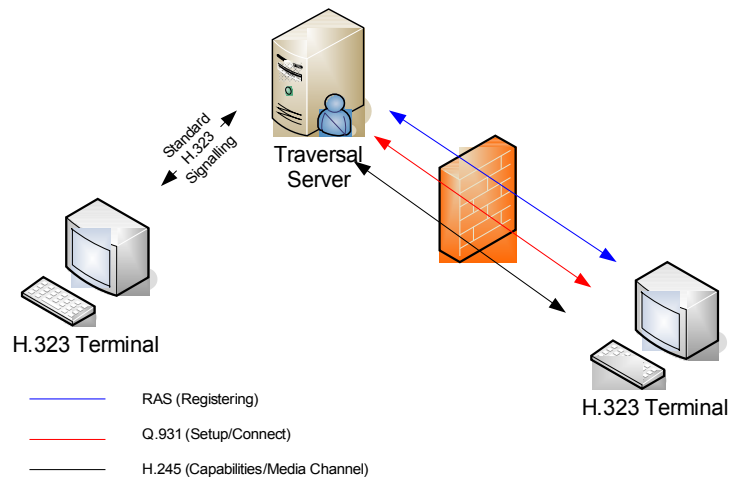
### H.460.18

Wenn H.460.18 verwendet wird, ist das Szenario etwas anders. Anstelle des Gatekeepers wird nun ein Traversal-Server verwendet. Solch ein Server verfügt über eine Gatekeeper-Funktionalität und wird ebenfalls als H.225/H.245-Signal-Proxy verwendet. Abbildung 6 veranschaulicht den Aufbau.

Der Aufbau ähnelt H.460.17, jedoch haben hier die verschiedenen Kanäle eine andere Aufgabe bzw. werden anders hergestellt.

Der RAS-Kanal (blaue Linie) öffnet die Firewall mittels RRQ. Die Verbindung selbst verwendet symmetrisches UDP, und weitere RRQ werden als Keep-alive verwendet. Die Q.931- und H.245-Kanäle werden dann erst bei einem Anruf aufgebaut. Q931 verwendet Port 1720 TCP. H.245 ist ebenfalls TCP, aber der Port wird dynamisch

ausgehandelt. Beide Protokolle verwenden allerdings leere TPKT- (Transport Packet) Nachrichten für das Keep-alive.



**Abbildung 6: Aufbau einer Verbindung mittels H.460.18**

Neben den Kanälen spielt hier allerdings auch der Ruf-Aufbau eine Rolle. Für eingehende Rufe auf dem externen H.323-Terminal sendet der Traversal-Server ein RAS SCI (Incoming Call Indicator) zum externen Gerät via Q.931. Daraufhin wird ein Rückkanal zwischen dem externen Teilnehmer und dem Traversal-Server aufgebaut. Für den H.245-Kanal sendet der Traversal-Server eine so genannte StartH245-Nachricht an den externen Teilnehmer. Diese Nachricht öffnet automatisch einen neuen TCP-Datenkanal der ausschließlich für H.245 verwendet wird.

### H.460.19

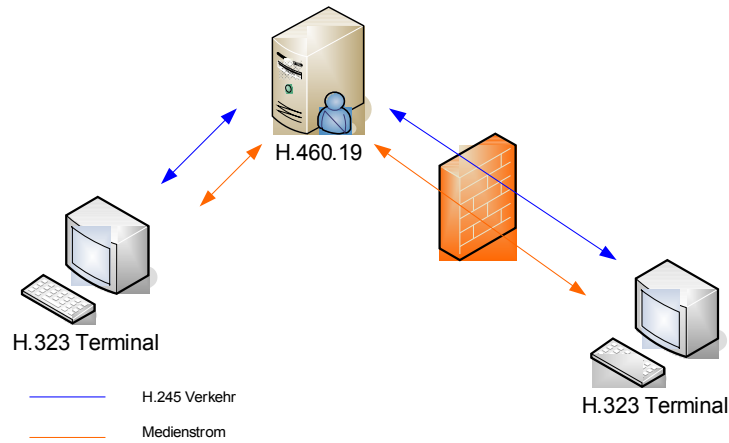
Dieser Standard bezieht sich vor allem auf den Medienstrom selbst, den RTP-Strom. Ähnlich wie bei H.323-Proxy-Systemen wird in der H.245-Nachricht der RTP-Adresse geändert, so dass der gesamte Verkehr durch den H.460.19-Server muss.

Wie Abbildung 7 zeigt gleicht der Verlauf der Signal- und Medienströme dem bei der Verwendung eines H.323-Proxy (siehe Proxy-Systeme).

Im Allgemeinen ist H.460.19 der akzeptierte Standard für H.323-Firewall und NAT. Ebenfalls identisch zu den Proxy-Systemen ist das klare Client/Server-Modell. Hier muss keine Punkt-zu-Punkt-Firewall/NAT-Auflösung wie beispielsweise bei ICE aufgebaut werden.

Ein großer Vorteil von H.460.17/18/19 ist auch das Far-end/Near-end-Traversal. Hierbei kann sich eine Firewall im eigenen Netz oder auf der Gegenseite befinden. Befindet sich die Firewall in einem entfernten Netz, dann müssen allerdings die Klienten dort H.460 verstehen, andernfalls kann eine Verbindung nicht aufgebaut werden.

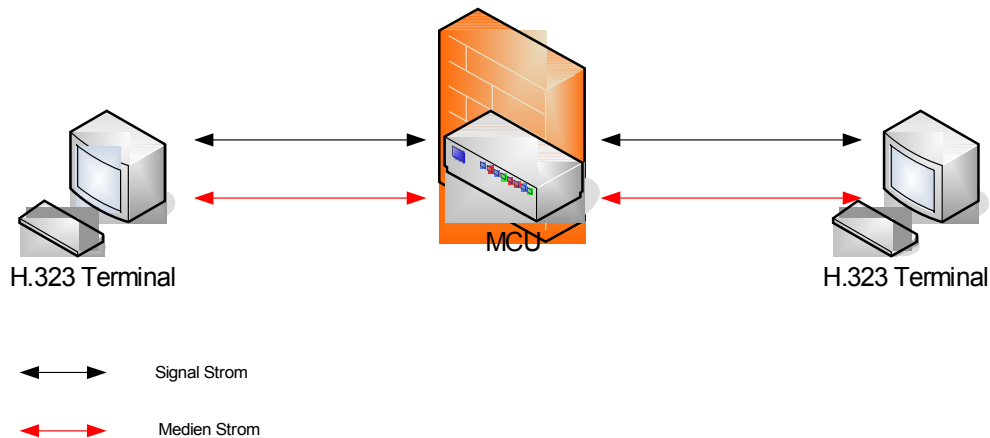
Ein häufiges Problem bei der Verwendung von H.460.17/18/19 ist das „h323 fixup“ der CiscoPIX, u. U. wird der Verbindungsaufbau komplett verhindert.



**Abbildung 7: Aufbau einer H.460.19-Verbindung**

### MCU-Tunneling

MCU-Tunneling verwendet ein ähnliches Prinzip wie ein H.323-Proxy. Auch hier befindet sich ein System, in diesem Fall eine MCU (Multipoint Control Unit) zwischen den H.323-Klienten. Die beiden Endgeräte wählen sich in eine MCU-Konferenz ein. Das funktioniert für Teilnehmer aus dem internen Netz und für Teilnehmer aus dem externen Netz, da die MCU über eine Verbindung sowohl zum externen als auch zum internen Netz verfügt.



**Abbildung 8: MCU-Tunneling**

Man kann sich das auch als virtuellen Konferenzraum auf der MCU vorstellen, in dem sich die Teilnehmer treffen.

Da die MCU sowohl das interne als auch das externe Netzwerk kennt, kann das MCU-Tunneling auch für NAT-traversal verwendet werden. In diesem Fall muss die MCU über zwei unterschiedliche Netzwerkverbindungen/Interfaces verfügen. Weiterhin müssen sog. Forwarding-Rules gesetzt sein.

### **Zusammenfassung**

Wie dieser kurze Artikel zeigt, gibt es heute einige zuverlässige Lösungsmöglichkeiten für das H.323-Firewall-Problem. Sicherlich bietet jede Vorgehensweise ihre individuellen Vor- und Nachteile, eine „General“-Lösung gibt es nicht.

Eine der preiswertesten Alternativen ist GnuGK, eine OpenSource-Gatekeeper/Proxy-Lösung. Diese jedoch funktioniert nur mit H.323. Session-Border-Controller und seit neuestem auch verschiedene MCUs verstehen auch das SIP-Protokoll. Dadurch bedingt bieten diese Lösungen eine größere Vielfalt.

Sicherlich gibt es auch OpenSource-Lösungen für SIP, diese werden hier allerdings nicht besprochen.

OpenFirewalling wird eher selten und nur für einzelne Systeme eingesetzt. Wer bereits mehrere Systeme oder eine größere H.323-Infrastruktur besitzt, steht dann vor der Entscheidung, welche Lösungsmöglichkeit die beste für das abzubildende Szenario ist.

### **Literatur**

- [1] ITU Study group 16, <http://www.itu.int/ITU-T/studygroups/com16/index.asp>
- [2] <http://www.packetizer.com>
- [3] Stöckigt, K.; Videokonferenzen aus sicheren Netzwerken, Bachelor Arbeit, GWDG Göttingen
- [3] Schwenn, U.; H.323 Videoconferencing, EFDA Remote Participation workshop, Budapest, Ungarn, 2004
- [4] Stöckigt, K.; Traversing H.323 audio/video through firewalls, EFDA Remote Participation Wotkshop, Budapest, Ungarn, 2004
- [5] Schwenn, U.; Video over IP – Videoconferencing Infrastructure, KFKI Budapest
- [6] Schlatter, C.; The new H.460.17/18/19 Protocols for H.323 Firewall and NAT Traversal, 8<sup>th</sup> SURA/ViDe conference, Atlanta, USA, 2006

Verfasser: Kewin Stöckigt

VIKTAS, Mai 2007