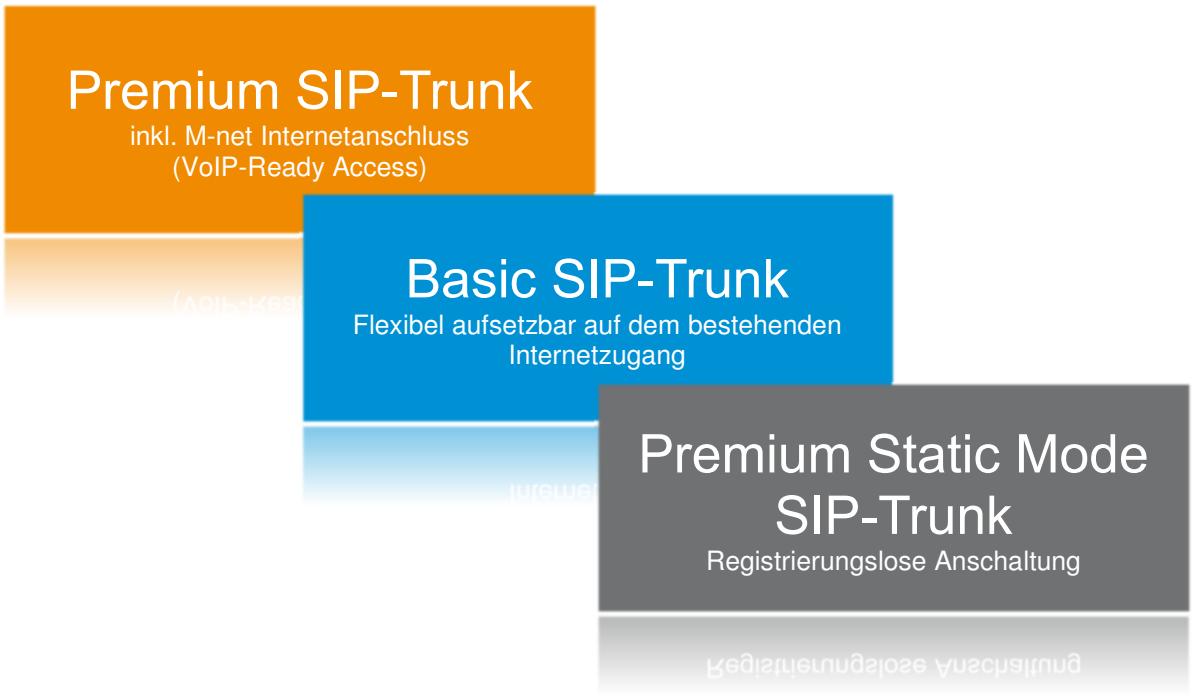
Technische Hinweise

für



Bitte leiten Sie dieses Dokument an den zuständigen Techniker bzw. Systemintegrator weiter!

Inhaltsverzeichnis

1 Dokumenteninformationen

1.1 Zweck des Dokuments

Diese technischen Informationen ergänzen die Produktbeschreibung und werden dem Kunden weitergegeben, ggf. nicht in Papierform, sondern in Internet zur Verfügung gestellt. Es handelt sich um öffentliche Informationen, also sind nicht nur dem Kunden zugänglich.

1.2 Definitionen und Abkürzungen

Abkürzung	Erklärung
M-net Vermittlungssystem	M-net VoIP-Infrastruktur (Sprachplattform)
RTP	Real Time Transport Protocol (Protokoll zur Übertragung von audiovisuellen Daten)
RTCP	Real Time Control Protocol (Zur Aushandlung von QoS-Parametern)
(IP-) PBX	Private Branch Exchange (SIP-fähige Telefonanlage)
VLAN	Virtual Local Area Network (Logisches Teilnetz)
DDI	Direct Dial In (Durchwahl)
PSTN	Public Switched Telephone Network (Öffentliches Telefonnetz)
URI	Uniform Resource Identifier (Stellt als SIP-URI die Kontaktadresse eines SIP-fähigen-Endsystems dar)
ITU	International Telecommunication Union
NAT	Network Address Translation (Adressumsetzung von IP-Adressen)
DTMF	Dual-tone multi-frequency (Mehrfrequenzwahlverfahren)
SIP	Session Initiation Protocol (Protokoll zum Aufbau einer Kommunikationsverbindung)
RFC	Requests for Comments (Sammlung technischer Dokumente der „Internet Engineering Task Force"u. a. zur Entwicklung von VoIP)
QoS	Quality of Service
SBC / E-SBC	(Enterprise-) Session Border Controller. Der Session Border Controller ist Teil des M-net Vermittlungssystems
SDP	Session Description Protocol Wird zusammen mit SIP bzw. H.323 zur Aushandlung von Codec verwendet

CPE	Customer Premises Equipment. („Ausrüstung in den Räumlichkeiten des Kunden.“ Dem Kunden zur Verfügung gestelltes Gerät z.B. Router.)
TLS	Transport Layer Security (Protokoll zur Verschlüsselung von Datenpaketen)
SRTP	Secure Real Time Protocol (Verschlüsselte RTP-Pakete)
STUN	Session Traversal Utilities for NAT (Netzwerkprotokoll zum Erkennen und durchdringen von NAT)
DSCP	Differentiated services code point

1.3 Liste der Abbildungen und Tabellen

1.3.1 Abbildungsverzeichnis:

2 Die M-net SIP-Trunk Produktvarianten

Basic Premium Static

M-net stellt mit den SIP-Trunk Produkten einen Dienst zur Verfügung, welcher eine IP-fähige Kundennebenstellenanlage (IP-PBX) über das IP-Protokoll mit dem öffentlichen Telefonnetz verbindet.

Zur Steuerung der Kommunikation mit der Gegenstelle verwendet die IP-PBX das Session Initiation Protocol (SIP). Die Sprachinformationen werden über das Real Time Protocol (RTP) übertragen.

Für die Daten zur Qualität werden optional mit dem Real Time Control Protocol (RTCP) übertragen.

Die physikalische Anschaltung der IP-PBX wird über einen IP basierten Anschluss, mit ausreichender Bandbreite realisiert. Dieser Anschluss wird für den Transport der Protokolle SIP, RTP und RTCP zwischen der IP-PBX und der M-net VoIP-Infrastruktur (nachfolgend M-net Vermittlungssystem) benötigt.

Da das M-net Vermittlungssystem georedundant aufgebaut ist, ist bei der Verwendung eines M-net VoIP Ready Access die Option „Backup“ möglich.

2.1 Premium SIP-Trunk

Der Dienst **Premium SIP-Trunk** wird über einen, von M-net bereitgestellten IP basierten Anschluss (sog. VoIP Ready Access) realisiert und betrieben. In diesem Fall wird Quality of Service (QoS) ab/zu dem M-net Router (CPE) garantiert.

2.2 Basic SIP-Trunk

Der **Basic SIP-Trunk** hingegen, wird über einen bestehenden IP basierten Anschluss realisiert und betrieben. Allerdings kann QoS beim Basic SIP-Trunk nicht garantiert werden.

Sowohl beim Premium SIP-Trunk als auch beim Basic SIP-Trunk wird die IP-PBX im registrierenden Modus betrieben.

2.3 Premium SIP-Trunk Static Mode

Beim **Premium SIP-Trunk Static Mode** handelt es sich um eine registrierungslose Anschaltung der IP-PBX an das M-net Vermittlungssystem. Der Dienst kann sowohl über einen M-net VoIP Ready Access als auch über einen bestehenden IP basierten Anschluss realisiert werden. Allerdings kann QoS nur bei Verwendung eines M-net VoIP Ready Access garantiert werden.

Da die meisten IP-PBXen den Static Mode, also die registrierungslose Anschaltung nicht unterstützen, empfehlen wir die Variante Premium SIP-Trunk.

Weitere Informationen zu QoS finden Sie im Kapitel 9.4.

3 Übersicht der M-net SIP-Trunk Produktvarianten

	Basic	Premium	Static Mode
SIPConnect 1.1 unterstützt	x	x	x
Verschlüsselung mit TLS/SRTP möglich	x	x	
Quality of Service		x	x*
Verwendung mehrerer SIP-Trunk Accounts	x	x	x
Registrierung am M-net Vermittlungssystem	x	x	
Re-Registrierung nötig?	x	x	
HD-Telefonie	x	x	x
DTMF			
nach RFC 2833 bzw. RFC 4733	x	x	x
DTMF INBAND (bei HD-Telefonie nicht möglich)	x	x	x
Faxen mit G.711a möglich	x	x	x
Redundanz der Anbindung zur IP-PBX über weiteren Access möglich		x	x*
Authentifizierung bei abgehenden Gesprächen	x	x	x
Leistungsmerkmale (z. B. CLIP -no screening)	x	x	x
Unterstützung von SIP-Methoden (z. B. INVITE, BYE etc.)	x	x	x
Feste IP-Adresse in Richtung M-net			x
Feste Portnummer in Richtung M-net			x
Transportprotkoll: UDP	x	x	x
Unterstützte IP Protokoll Version 4 (IPv 4)	x	x	x
Loadbalancing			x

* nur bei Verwendung eines M-net VoIP-ready Access

4 Allgemeine technische Infos

Da es bei den drei Produktvarianten technische Unterschiede gibt, werden diese im weiteren Verlauf gesondert beschrieben. Sie werden über jedem Hauptkapitel einen Hinweis finden, für welche Produktvariante der jeweilige Abschnitt gilt.

Die Unterkapitel in diesem Abschnitt gelten für alle drei Produktvarianten.

4.1 Der Standard: SIPconnect 1.1

Mit SIPconnect 1.1 wurde ein branchenweiter standardisierter technischer Ansatz geschaffen, um eine IP-PBX Mittels SIP-Trunk an die VoIP-Infrastruktur eines Providers anzuschalten. Dieser Standard sagt u. a. aus, wie beispielsweise die Rufnummernformate zu übermitteln sind.

Da der SIPconnect 1.1 die Anschaltung der IP-PBX vereinfacht, wird dieser Standard auch vom M-net Vermittlungssystem unterstützt.

4.2 Hinweis zu den freigegebenen IP-PBX für Premium und Basic SIP-Trunk

Obwohl M-net den SIPconnect 1.1 Standard unterstützt, prüfen wir stetig IP-PBXen unterschiedlicher Hersteller auf Kompatibilität. Nur dadurch können wir eine fehlerfreie Funktion der IP-PBXen mit den SIP-Trunk Produkten Premium und Basic von M-net garantieren.

Die hier beschriebenen Punkte beziehen sich deswegen ausschließlich auf die von M-net auf Kompatibilität getesteten IP-PBX Anlagen und die jeweiligen Softwareversionen.

4.3 Hinweis zu den freigegebenen IP-PBX für Premium SIP-Trunk Static Mode

Beachten Sie bitte, dass die Produktvariante SIP-Trunk Premium SIP-Trunk Static Mode spezielle Tests erfordert. Deswegen gelten die Angaben zu den freigegeben IP-PBXen nur für die Produktvarianten Premium und Basic SIP-Trunk.

4.4 Rufnummernformat

Die IP-PBX muss alle Rufnummern im internationalen Nummernformat entsprechend ITU-T Empfehlung E.164 und E.123 handhaben können.

Beispiel: (+)(Landeskennziffer)(Ortsnetzkennziffer)(Teilnehmer Rufnummer)

+ 49 89 189291230

4.4.1 Rufnummerndefinition

Rufnummer	Rufnummerndefinition	Beispiel
Hauptrufnummer	Mit der Hauptrufnummer registriert sich die IP-PBX am M-net Vermittlungssystem. Die Hauptrufnummer kann für die Zentrale verwendet werden. Da die Hauptrufnummer auch für den SIP-Login verwendet wird, muss bei einer Änderung der Hauptrufnummer auch der SIP-Login angepasst werden. Wird bei einem abgehenden Gespräch im FROM-Header ein ungültiger Eintrag mitgeschickt, wird dieser durch die Hauptrufnummer ersetzt und übertragen.	+4989189291230
Zentrale	Die Zentrale ist das „Eingangstor“ bzw. der Empfang. Die Zentrale kann die Hauptrufnummer sein. Die Verwendung einer Zentrale ist optional.	+4989189291230
Durchwahlnummer (DDI)	Über die Durchwahlnummern kurz DDI sind die jeweiligen Nebenstellen direkt erreichbar. **DDI Fähigkeit muss von der IP-PBX unterstützt werden.**	+49891892912312

(Angegebene Rufnummern sind Beispiele)

4.5 Notruf

Beachten Sie bitte, dass bei einem Notruf die Zielrufnummer (110/112) im lokalen Format ohne Vorwahl an das M-net Vermittlungssystem zu übermitteln ist.
Beispiel der Request-Line:

INVITE sip:112@business.mnet-voip.de

4.6 Empfohlenes Transportprotokoll: UDP

Bei UDP handelt es sich um ein Netzwerkprotokoll, dass u. a. zur Übertragung von Sprache verwendet wird. Im Gegensatz zu TCP arbeitet UDP ohne Sicherung der Datenübertragung. Durch die Sicherung bei TCP kann es zu Verzögerungen in der Sprachübertragung und somit zu Einbußen bei der Sprachqualität kommen. Ein weiterer Nachteil von TCP ist, dass die Anbindung zwischen der IP-PBX und dem M-net Vermittlungssystem dauerhaft offengehalten werden muss. Bricht die TCP-Verbindung zusammen, kann dies zu Gesprächsabbrüchen und zu einer eingeschränkten Erreichbarkeit der IP-PBX führen. Aus diesen Gründen empfehlen wir **die Verwendung von UDP.**

4.7 Aufbau einer SIP-Nachricht

Das Session Initation Protokoll (SIP) wir zur Steuerung, sowie zum Auf- und Abbau einer Kommunikationsverbindung benötigt und ist im RFC 3261 spezifiziert.

Eine SIP-Nachricht ist, wie im Beispiel einer INVITE-Nachricht aufgebaut:

INVITE sip:452000@business.mnet-voip.de SIP/2.0	Request Line
Via: SIP/2.0/UDP 192.168.178.123:5060;branch=z9hG4bK_AI2016Jul14355633452008398255;rport To: sip:452000@business.mnet-voip.de From: "SIP Telefon 12" <sip:+49891892912312@business.mnet-voip.de>;tag=12345 Call-ID: AI0AD3049CEB9CEF54@192.168.178.123 CSeq: 1 INVITE Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,PUBLISH,UPDATE,REFER,PRACK Allow-Events: presence,dialog,message-summary,refer Max-Forwards: 70 User-Agent: IP-PBX Supported: 100rel Content-Type: application/sdp Privacy: none Accept: application/sdp Contact: <sip:+49891892912312@192.168.178.123:5060;line=AI31A0DBF9D4721556> Content-Length: 281	Message Header (SIP)
v=0 o=ippbx 1831823547 1831823547 IN IP4 192.168.178.123 s=call c=IN IP4 192.168.178.123 t=0 0 m=audio 3000 RTP/AVP 8 9 101 a=rtpmap:8 PCMA/8000 a=rtpmap:9 G722/8000 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 a=sendrecv a=ptime:20 a=silenceSupp:off - - - -	Message Body (SDP)

Abbildung 1: Beispiel einer abgehenden INVITE Nachricht

Die **Request Line** ist die Startzeile und enthält die Ziel-SIP-Adresse. Die Request Line besteht aus dem „Method-Name“, der „Request-URI“ und der Angabe „SIP-Version“. In der Request-URI muss das Ziel im SIP-URI Format angegeben werden:

Der **Message Header** beinhaltet u. a. Angaben in Form von sogenannten Header-Feldern (FROM, TO etc.)

Der **Message Body** ist eine optionale Angabe. Er wird beispielsweise bei einer INVITE-Nachricht benötigt, da er Daten zur Aushandlung des Medienstroms (RTP) enthält.

4.8 Unterstütze Codecs

Bei der Kommunikation über VoIP werden die Sprachdaten erst digitalisiert und dann codiert. Der zu verwendete Codec wird von den jeweiligen Endgeräten ausgehandelt. Die IP-PBX muss mindestens den **Codec G.711a** unterstützen.

Hinweis: Aktuell wird vom M-net Vermittlungssystem kein Video-Codec zugelassen.

Beim Übergang in das PSTN/Mobilfunk-Netz werden folgende Codec unterstützt:

Codec	benötigte Bandbreite pro Kanal (Brutto)	RTP Packetizing Period (ms)
G.711a (DTMF INBAND)	120 kbit/s	20
G.729	64 kbit/s	20
DTMF nach RFC 2833/4733	-	-

Innerhalb des M-net-VoIP-Netzes sind folgende Codecs zugelassen:

Codec	benötigte Bandbreite pro Kanal (Brutto)	RTP Packetizing Period (ms)
G.711a (DTMF INBAND)	120 kbit/s	20
G.729	64 kbit/s	20
G.726 32kbps	88 kbit/s	20
G.722	120 kbit/s	20
iLBC	69 kbit/s	30
DTMF nach RFC 2833/4733	-	-
Clearmode/8000	120 kbit/s	20

4.9 DTMF Töne

Die Übertragung von Dual Tone Multi Frequency (DTMF) Signalen wird z.B. für die Steuerung von Konferenzserver, Automatischer Ansagenauswahl und Voicemail benötigt. Für die Übertragung von DTMF Tönen unterstützt M-net zwei Möglichkeiten:

4.9.1 DTMF nach RFC 2833 bzw. RFC 4733

Hierbei werden die DTMF Töne in dafür spezifizierten Nachrichten übertragen. Diese Methode wird von M-net bevorzugt.

4.9.2 DTMF INBAND

Bei INBAND wird der DTMF Ton als Tonsequenz digitalisiert und im RTP übertragen. Die fehlerfreie Übertragung ist hierbei nur möglich, wenn QoS garantiert ist.

4.9.3 DTMF INBAND und HD-Codec

Bei der Verwendung des sog. HD-Codec (G.722) können DTMF Töne nur nach RFC 2833/4733 übertragen werden. Die Verwendung von DTMF INBAND ist nicht möglich.

4.10 Unterstützte Standards

Das M-net Vermittlungssystem unterstützt u. a. den SIP-Standard nach RFC 3261 und für die DTMF-Übertragung RFC 2833 bzw. 4733 (Details s. Kapitel 4.9)

4.11 Unterstützte SIP-Methoden

Für die M-net SIP-Trunk Produkte werden folgende SIP-Methoden unterstützt

SIP Methode	RFC	Unterstützte SIP-Methode innerhalb des M-net Vermittlungssystem	Unterstützte SIP-Methode bei Übergang ins PSTN	Erklärung
REGISTER	RFC 3261	ja	ja	Zur Registrierung am M-net Vermittlungssystem
INVITE	RFC 3261	ja	ja	Initiiert eine Verbindung zu einem anderen Client. Kann auch mit einem re-INVITE die Parameter verändern
ACK	RFC 3261	ja	ja	Positive Bestätigung einer endgültigen Antwort
BYE	RFC 3261	ja	ja	Beendet eine Verbindung
CANCEL	RFC 3261	ja	ja	Abbruch eines Verbindungsaufbaus
MESSAGE	RFC 3428	ja	nein	Zum Transport von Instant Messages über SIP
SUBSCRIBE	RFC 3265	ja	nein	Zur Übermittlung bestimmter Ereignisse
NOTIFY	RFC 3265	ja	nein	Wird bei Statusänderungen geschickt
PUBLISH	RFC 3903	ja	nein	Vergleichbar mit REGISTER.
OPTIONS	RFC 3261	ja	nein	Zur Bereitstellung oder Abfrage von Informationen zu den Eigenschaften von Endsystemen
PRACK	RFC 3262	ja	ja	vorläufige Bestätigung
UPDATE	RFC 3311	ja	nein	Modifizierung von Parametern während eines Verbindungsaufbaus

4.12 Vorläufige Bestätigung (Provisional Responses)

Für die SIP-Nachricht „180 Ringing“ und „183 Session Progress“ sind sogenannte „Provisional Responses“ relevant. Die Methode ist in RFC 3262 definiert und wird in einer INVITE-Nachricht im Header Field mit einem „Supported: 100rel“ angegeben. Dieser 100rel Parameter zeigt an, dass die Methode „Preliminary Acknowledgements“ (kurz PRACK) unterstützt wird.
Die SIP Funktion „Provisional Responses“ 100rel nach RFC 3262 wird vom M-net Vermittlungssystem unterstützt.

4.13 Voice Activity Detection (VAD)

Bei Voice Activity Detection (VAD) werden Sprachpausen erkannt und Sprachpakete ohne Sprachinformationen nicht übertragen. **VAD wird bei M-net nicht unterstützt.**

4.14 SIP Application Layer Gateway

Das SIP Application Layer Gateway (kurz: SIP ALG) ist in einer Vielzahl von modernen Routern zu finden. Durch die Funktion des SIP ALG sollen etwaige Probleme mit NAT umgangen werden.

Das M-net Vermittlungssystem verfügt über wirksame Methoden, die den Einsatz eines SIP ALG überflüssig machen.

Das SIP ALG ist deshalb zu deaktivieren.

Es ist nur zu aktivieren, wenn über den Inhalt und Funktion des SIP Nachrichtenverlaufes in Kombination mit NAT-traversal detaillierten Kenntnissen bestehen.

4.15 Telefax

Während bei der Übermittlung von Sprachdaten das Fehlen eines Sprachpaketes für den Empfänger nicht als störend empfunden wird, führt es beim Senden von Faxen zum Verbindungsabbruch. Faxgeräte sind aber nicht nur auf einen kontinuierlichen, sondern auch auf einen vollständigen Datenstrom angewiesen.
Kommt es zu Laufzeitschwankungen bei der Übertagung, verliert das Faxgerät die Synchronisierung und bricht die Verbindung ab.

4.15.1 Codec für Faxübertragung

Die ITU-T Empfehlung T.38 beschreibt ein Verfahren zur Übertragung von Fax über IP. Da es durch die Datenkomprimierung, verschiedenen Versionierungen und unzureichend implementierter Rückfall-Funktionen bei Übertragungen mit T.38 permanent zu Übertragungsschwierigkeiten kommt, wird T.38 bei M-net derzeit nicht unterstützt. **Für die Faxübertragung ist der Codec G.711a zu verwenden.** Mit diesem können ebenfalls G3 Faxgeräte verwendet werden.

4.15.2 ECM

Moderne Faxgeräte haben das Error Correction Mode (kurz ECM) integriert. Bei Verwendung von ECM wird das zu empfangene Dokument in Segmente zerlegt, gespeichert und auf Fehler überprüft. Mit Fehler behaftete Segmente werden beim Sender neu angefordert.

Durch die Neuanforderung von fehlerhaften Segmenten steigt die Übertragungsdauer. Das sollte vermieden werden, da bei einer längeren Übertragungsdauer die Gefahr von Laufzeitschwankungen oder Paketverlusten zunimmt. Dies kann wiederum schnell zu einem Abbruch der Übertragung führen.

Das ECM sollte bei Faxübertragung über den SIP-Trunk deaktiviert werden. Die Übertragung ist dann abhängig von der Leitungsqualität und der Qualität der verwendeten Faxgeräte.

5 Technische Details für Premium und Basic SIP-Trunk

Basic Premium

Bei den Produkten Premium SIP-Trunk und Basic SIP-Trunk muss sich die IP-PBX in bestimmten Zeitabständen zur Authentifizierung am M-net Vermittlungssystem registrieren.

Damit die SIP- und RTP-Pakete auch das M-net Vermittlungssystem erreichen, verwenden Sie bitte folgende Domains bzw. IP-Adressen und Protokollversion:

5.1 Verwendete IP-Protokollversionen, Domains, IP-Adressen und Ports

Protokolle	IP-Adressen und Ports der Domain **business.mnet-voip.de**
Signalisierung (SIP)	62.216.220.1 und 62.216.221.1 Port 5060
Mediadaten (RTP)	62.216.222.1 und 62.216.222.33 Portrange: 16384 - 65535
Verschlüsselung (TLS/SRTP)	62.216.220.1 und 62.216.221.1 Port 5061
Internet Protocol Version (IPv)	4

5.2 Registrierungsablauf der IP-PBX am M-net Vermittlungssystem

Für die Registrierung am Dafür muss die IP-PBX das **SIP Digest Authentication Verfahren nach RFC 3261** anwenden. Hierbei sendet die IP-PBX eine Registrierungsanfrage (REGISTER Request) zum M-net Vermittlungssystem. Die von der IP-PBX geschickte Registrierungs-Nachricht muss ein Request-URI enthalten.

Das M-net Vermittlungssystem antwortet darauf mit einer Aufforderung zur Authentifizierung, einer sogenannten Challenge-Message in Form einer „SIP 401 unauthorized“ worauf die IP-PBX eine weitere Registrierungsanfrage mit den Authentifizierungsdaten (REGISTER Request mit Authorization Header) sendet. Die erfolgreiche Registrierung wird vom M-net Vermittlungssystem mit „200 OK“ bestätigt.

REGISTER sip:business.mnet-voip.de SIP/2.0	Request Line
Via: SIP/2.0/UDP 192.168.178.123:5060;branch=z9hG4bK_AI2016Jul125555169+4989189291230;rport To: <sip:+4989189291230@business.mnet-voip.de> From: <sip:+4989189291230@business.mnet-voip.de>;tag=AI389FAC6CDDB154C5 Call-ID: AI3CA8881402C3CA5F@192.168.178.123 CSeq: 2 REGISTER Authorization: Digest username="+4989189291230",realm="business.mnet-voip.de",nonce="9524cbcdc63b",uri="sip:business.mnet-voip.de",qop=auth,nc=00000001,cnonce="4ff553bc1c9c5ca1",response="ed832abfdfa1a83630438faa44c437a5",algorithm=MD5 Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,PUBLISH,UPDATE,REFER,PRACK Allow-Events: presence,dialog,message-summary,refer Max-Forwards: 70 User-Agent: IP-PBX Expires: 3600 Contact: <sip:+4989189291230@192.168.178.123:5060;line=AIB634BB98E7969A90>;expires=3600 Content-Length: 0	Message Header (SIP)

Abbildung 2: Beispiel einer initialen REGISTER Request bei Registrierung auf der Domain business.mnet-voip.de

In der **Request Line** stehen der Method-Name (REGISTER) und die Request-URI (hier der Realm, an den die Registrierungsanfrage geschickt werden soll)

Im **Message Header** muss bei der Registrierung im FROM- und TO-Header jede IP-PBX-Hauptrufnummer als SIP-URI im internationalen Format mit einem führendem +, sowie im Host-Part der M-net Domain-Name enthalten sein.

Im **Contact-Header** muss im Host-Part die (private) IP-Adresse des Endpunktes, an dem der SIP-Trunk terminiert wird (z. B. die IP-PBX) eingetragen werden.

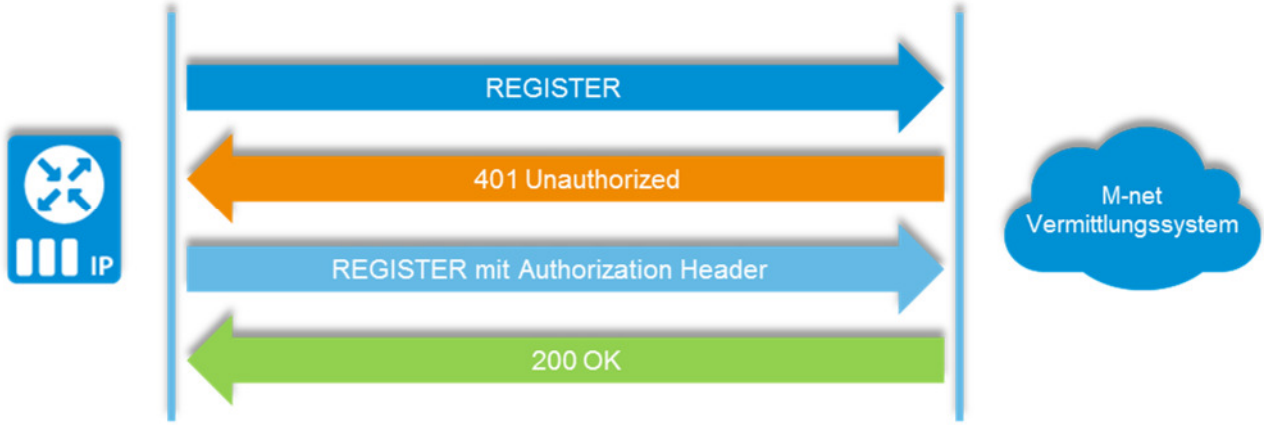
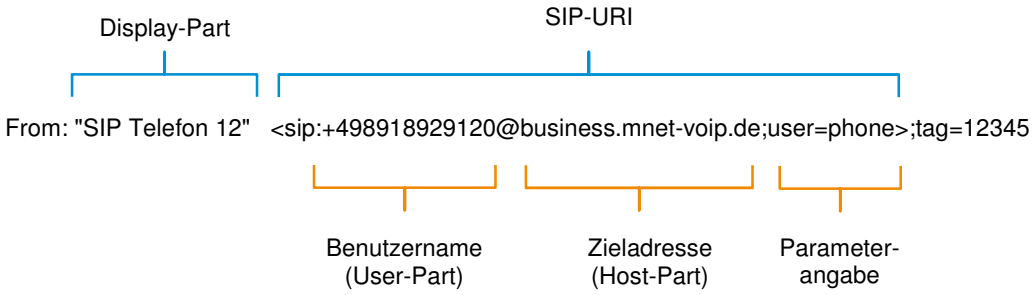


Abbildung 3: Beispiel Registrierungsablauf bei der Registrierung

5.3 Aufbau der SIP-Header Felder und SIP-URI

Das Header Field besteht aus dem Display-, User- und Host Part.
User- und Host-Part bilden wiederum den SIP-URI (auch SIP-Adresse).
Der SIP-URI dient der Adressierung von Teilnehmern auf SIP Basis und ist im RFC 3261 definiert.
Außerdem können in einer SIP-URI weitere Parameter mitgesendet werden. Im unten angegeben

Beispiel ist das „user=phone“. Mit dieser Parameterangabe wird besagt, dass es sich bei der betreffenden Zahlenkombination in der SIP-URI um eine PSTN-Rufnummer handelt.



Beispiel und Aufbau eines Header Field (hier FROM-Header).

5.4 Verwendung von DNS – Domain Name System

Das Domain Name System (kurz DNS) ist ein Internetdienst, der die Anfragen zur Namensauflösung beantwortet.
Da das M-net Vermittlungssystem aus Redundanzgründen an zwei Standorten in Betrieb ist, können bei der Auflösung der Domain business.mnet-voip.de auch zwei unterschiedliche IP-Adressen zurückgegeben werden.

5.4.1 Empfehlung: SRV-Records

Verarbeitet die IP-PBX nur A-Records, so wird jeweils eine IP-Adresse vom DNS-Server an die IP-PBX zurückgegeben.

Damit die IP-Adressen inkl. einer Priorisierung der Standorte des M-net Vermittlungssystems vom DNS-Server an die IP-PBX zurückgegeben werden, wird **die Verwendung von SRV-Records empfohlen**.

5.5 Hinweise zur Konfiguration mehrerer SIP-Trunk Accounts auf einer IP-PBX

Sie können auch mehrere M-net SIP-Trunk Accounts auf einer IP-PBX betreiben. Das M-net Vermittlungssystem bietet folgende Möglichkeiten an:

5.5.1 Unterschiedlicher Source-IP-Adresse und Source-Port

Bei dieser Möglichkeit muss die IP-PBX **für jede zu registrierende Hauptrufnummer einen anderen Source-Port oder eine andere Source-IP-Adresse mitsenden.** Dadurch wird sichergestellt, dass bei einem abgehenden Gespräch die A-Rufnummer korrekt vom M-net Vermittlungssystem übermittelt wird.

5.5.2 Verwendung von zwei Premium SIP-Trunk Accounts

Wenn die IP-PBX nur eine Source-IP-Adresse/Source-Port zulässt, können stattdessen auch unterschiedliche Outbound-Proxys verwendet werden. Hierfür konfigurieren Sie bitte folgende Domains bzw. IP-Adressen in der IP-PBX:

Hinweis zum Outbound-Proxy	Domain	IP-Adresse
Für den **ersten** SIP-Trunk Account verwenden Sie bitte den Outbound-Proxy:	business-wei.mnet-voip.de	62.216.220.1
Für den **zweiten** SIP-Trunk Account verwenden Sie bitte den Outbound-Proxy:	business-hkw.mnet-voip.de	62.216.221.1

5.5.3 Verwendung von mehr als zwei Premium SIP-Trunk Accounts

Sollen auf der IP-PBX mehr als zwei Premium SIP-Trunk Accounts betrieben werden, sind zwei Schritte nötig.

1. Wir benötigen die öffentliche IP-Adresse des M-net Access. Diese wird im M-net Vermittlungssystem hinterlegt. Wenn dies noch nicht geschehen ist, nehmen Sie bitte Kontakt zu Ihrem M-net Kundenberater auf.

2. Es müssen folgenden Konfigurationen in der IP-PBX vorgenommen werden:

Hinweis zum Outbound-Proxy	Domain	IP-Adresse
Für den **ersten** SIP-Trunk Account verwenden Sie bitte den Outbound-Proxy:	business02.mnet-voip.de	62.216.220.2
Für den **zweiten** SIP-Trunk Account verwenden Sie bitte den Outbound-Proxy:	business03.mnet-voip.de	62.216.220.3
Für den **dritten** SIP-Trunk Account verwenden Sie bitte den Outbound-Proxy:	business03.mnet-voip.de	62.216.220.4

Es können weitere SIP-Trunk Accounts auf einer IP-PBX verwendet werden. Dazu sind auch Anpassungen im M-net Vermittlungssystem notwendig. Bitte wenden Sie sich hierzu an Ihren M-net Kundenberater.

5.5.4 Verwendung von zwei oder mehr Basic SIP-Trunk Accounts

Sollen auf der IP-PBX zwei oder mehr Basic SIP-Trunk Accounts betrieben werden, sind zwei Schritte nötig.

1. Wir benötigen die öffentliche IP-Adresse des M-net Access. Diese wird im M-net Vermittlungssystem hinterlegt. Wenn dies noch nicht geschehen ist, nehmen Sie bitte Kontakt zu Ihrem M-net Kundenberater auf.

2. Es müssen folgenden Konfigurationen in der IP-PBX vorgenommen werden:

Hinweis zum Outbound-Proxy	Domain	IP-Adresse
Für den **ersten** SIP-Trunk Account verwenden Sie bitte den Outbound-Proxy:	business02.mnet-voip.de	62.216.220.2
Für den **zweiten** SIP-Trunk Account verwenden Sie bitte den Outbound-Proxy:	business03.mnet-voip.de	62.216.220.3
Für den **dritten** SIP-Trunk Account verwenden Sie bitte den Outbound-Proxy:	business03.mnet-voip.de	62.216.220.4

5.6 Verschlüsselung

Bei der Anschaltung der IP-PBX an das M-net Vermittlungssystem über einen Fremd-Access empfehlen wir die SIP- und RTP-Pakete zu verschlüsseln. Dadurch werden die Kommunikationsdaten zwischen der IP-PBX und dem M-net Vermittlungssystem gesichert übertragen.

5.6.1 TLS und SRTP

SIP-Pakete werden mit dem Transport Layer Security Protokoll, kurz TLS verschlüsselt. Als Grundlage für TLS 1.2 gilt der RFC 2246.

Für die Verschlüsselung der RTP-Pakete wird das Secure Real-Time Transport Protocol, kurz SRTP verwendet. Der Schlüsselaustausch für SRTP findet im Session Description Protocol (SDP) in Klarschrift statt. Damit der Austausch gesichert abläuft, ist zuvor eine Verschlüsselung der Signalisierung mit TLS erforderlich.

5.6.2 TLS und SRTP nur gemeinsam

Da die Verschlüsselung mit TLS und SRTP gemeinsam sinnvoll ist, lässt das M-net Vermittlungssystem auch nur eine gemeinsame Verschlüsselung von SIP und RTP (d.h. TLS und SRTP) zu.

Eine ausschließliche Verschlüsselung von RTP (SRTP) - ohne TLS - wird vom M-net Vermittlungssystem mit einem Fehlercode abgelehnt.

5.6.3 Erhöhte Sicherheit: Das Perfect Forward Secrecy Verfahren

Um die Sicherheit nochmals zu erhöhen, unterstützt M-net bei der Verschlüsselung das sogenannte **Perfect Forward Secrecy Verfahren**. Dadurch ist auch ein nachträgliches Entschlüsseln eines aufgezeichneten Nachrichtenstroms unmöglich.

5.6.4 NAT und Verschlüsselung

Es kann vorkommen, dass durch die aktive Verschlüsselung die NAT Funktion vom M-net Vermittlungssystem nicht richtig erkannt wird. Dadurch wird das Registrierungsintervall vom M-net Vermittlungssystem nicht angepasst. Was zur Folge hat, dass die IP-PBX die Registrierung verliert und für ankommende Gespräche nicht mehr erreichbar ist. Sollte dies der Fall sein, aktivieren Sie bitte in der IP-PBX die Verwendung des STUN-Servers. Weitere Informationen zum Thema STUN finden Sie in Kapitel 11.

5.6.5 Zertifikate für die Domain business.mnet-voip.de

Für die Authentifizierung sind das Root- und das Intermediate-Zertifikat der Certification Authority (CA) COMODO notwendig. Dieses Zertifikat muss in der IP-PBX hinterlegt werden.

Die Zertifikate für die Domain business.mnet-voip.de lassen sich über zwei Pfade verifizieren. Abhängig von ggf. bereits existierenden vertrauenswürdigen CA-Zertifikaten bietet sich die Verwendung von Variante A oder B an.

Details zu den genannten Varianten und weiterführende Links zu den COMODO Zertifikaten finden Sie unter: https://www.m-net.de/sip-trunk/#Verschlüsselung

5.6.6 SIPS (SIP Secure)

Normalerweise werden SIP-Pakete über UDP gesendet. Damit eine verschlüsselte Verbindung von der IP-PBX initiiert werden kann, wird allerdings das Transmission Control Protocol (TCP) und der Destination-Port 5061 verwendet.

Die Festlegung auf TCP und dem Destination-Port 5061 wird eigentlich von der IP-PBX vorgenommen, in dem in der initialen INVITE-Nachricht bei einem abgehenden Call als Request-URI eine SIPS URI eingetragen wird.

Beispiel URI (ohne SIPS):	INVITE sip:452000@business.mnet-voip.de SIP/2.0
Beispiel URI (mit SIPS):	INVITE sips:452000@business.mnet-voip.de SIP/2.0

Danach wird die Verbindung über TCP aufgebaut.

Dieses Verfahren wird allerdings z. Zt. vom M-net Vermittlungssystem nicht unterstützt. Somit muss die Umstellung von UDP auf TCP bzw. TLS und die Änderung des Ports von 5060 auf 5061 manuell in der IP-PBX vorgenommen werden.

5.6.7 Cipher Suite

Um eine gesicherte Verbindung mit TLS aufzubauen, wird im Protokoll durch die Cipher Suite festgelegt, welche Algorithmen verwendet werden sollen. Die Cipher Suite besteht aus einer Kombination von vier Algorithmen:

1. Schlüsselaustausch (Beispiel: RSA, DH etc.)
2. Authentifizierung (Beispiel: RSA, DSA etc.)
3. Hashfunktion (ausschließlich SHA)
4. Verschlüsselung (u. a. DES, IDEA, AES)

Folgende Cipher Suites werden vom M-net Vermittlungssystem unterstützt:

1. TLS_DHE_RSA_WITH_AES_256_CBC_SHA
2. TLS_DHE_DSS_WITH_AES_256_CBC_SHA
3. TLS_RSA_WITH_AES_256_CBC_SHA
4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
5. TLS_DSS_RSA_WITH_AES_128_CBC_SHA
6. TLS_RSA_WITH_AES_128_CBC_SHA

Welche Cipher Suite endgültig verwendet wird, hängt davon ab, auf welche Suite sich die IP-PBX und das M-net Vermittlungssystem einigen. Grundsätzlich wird die höchstpriorisierte Suite verwendet.

5.6.8 Der Verschlüsselungsablauf (TLS-Handshake)

Vier Schritte werden beim TLS-Handshake durchlaufen (Beispiel):

1. Bevor die eigentliche Verbindung aufgebaut wird, signalisiert die IP-PBX mit der Nachricht **„Client Hello“** den Verschlüsselungswunsch. Mit dieser Nachricht werden u. a. auch die möglichen Cipher Suites an das M-net Vermittlungssystem geschickt.

Das M-net Vermittlungssystem antwortet mit einem **„Server Hello**“. Auch in dieser Nachricht wird u. a. die zu verwendete Cipher Suite mitgesendet.

2. In diesem Schritt identifiziert sich das M-net Vermittlungssystem gegenüber der IP-PBX und sendet das von COMODO signierte Zertifikat mit (inkl. öffentlichen Schlüssel).
3. Die IP-PBX identifiziert sich gegenüber dem M-net Vermittlungssystem und verifiziert das erhaltene Zertifikat. Damit die Verifizierung durchgeführt werden kann, ist der Zertifikats-Pfad (Certificate Chain) ausschlaggebend. Die IP-PBX verschlüsselt das sogenannte „pre-master-Secret“ mit dem öffentlichen Schlüssel und sendet dieses zurück zum M-net Vermittlungssystem. Das „pre-master-Secret“ kann nur mit dem privaten Schlüssel entschlüsselt werden
4. Aus dem „pre-master-secret“ kann jetzt das „Master Secret“ abgeleitet werden. Daraus wiederum ein wird der einmalige Sitzungsschlüssel generiert. Dieser Schlüssel wird während der gesamten Verbindung zum ver- und entschlüsseln der SIP-Pakete genutzt.

Erst nach erfolgreichem TLS-Handshake wird die Verbindung aufgebaut. Tritt während des beschriebenen Vorgangs ein Fehler auf, wird die Verbindung unterbrochen.

Nun kann auch der Schlüsselaustausch für SRTP stattfindet.

5.6.9 Verschlüsselung Konfigurationsschritte für die IP-PBX

Es gibt zwei Varianten, die Zertifikate für die Domain business.mnet-voip.de verifizieren zu lassen. M-net bevorzugt die Variante A. Dabei werden die Intermediate und Root CA verwendet. Damit die SIP- und RTP-Pakete verschlüsselt übertragen werden, führen Sie bitte folgende Schritte durch:

1. Die Zertifikate müssen heruntergeladen werden (https://www.m-net.de/sip-trunk/#Verschlüsselung)
2. Beide Zertifikate sind in der IP-PBX zu hinterlegen
3. Nun muss die IP-PBX von UDP und Port 5060 auf TCP und Port 5061 umkonfiguriert werden.
4. Danach sollte die Verbindung über TCP initiiert werden.

6 Backup

Premium

Vorrausetzung für die Verwendung von Backup ist ein weiterer VoIP-Ready Access (Weitere Informationen zum Access finden Sie im Kapitel 9), der als Backup-Leitung betrieben wird. Fällt die erste Leitung aus, wird auf die Backupleitung umgeschaltet. Hierbei sind folgende Dinge zu beachten, um die Ausfallzeit seitens der IP-PBX so gering wie möglich zu halten.

Wird die IP-PBX ohne NAT betrieben, wird für die Dauer der Umschaltung kein Audio übertragen. Die aktiven SIP-Verbindungen bleiben i. d. R. in dieser Zeit bestehen. Neben den RTP-Paketen können während der Umschaltphase auch keine SIP-Nachrichten mit dem M-net Vermittlungssystem ausgetauscht werden. Sollte die IP-PBX während des Zeitraums der Umschaltung ein re-REGISTER senden, kann dies zu einem Abbruch aller aktiven SIP-Verbindungen führen, da die Anfrage vom M-net Vermittlungssystem nicht beantwortet werden kann. Die IP-PBX ist dann erst nach einer Neuregistrierung erreichbar.

Wird die IP-PBX hinter NAT betrieben, werden alle aktiven SIP-Verbindungen unterbrochen. Die IP-PBX muss nach der Umschaltung erst eine neue Registrierungsanfrage an das M-net Vermittlungssystem senden (kein re-Register).

Erst nach einer Neuregistrierung ist die IP-PBX wieder erreichbar. Dies gilt auch bei einer Umschaltung von der Backup- auf die Erstleitung. Wann die IP-PBX die Anfrage sendet, ist von Hersteller zu Hersteller unterschiedlich.

7 Technische Details für den Premium SIP-Trunk Static Mode

Static

Bei der Produktvariante Premium SIP-Trunk Static Mode ist keine Registrierung erforderlich. Die Anbindung der IP-PBX kann mittels M-net Access (VoIP-Ready) oder über einen bestehenden Internetanschluss an das M-net Vermittlungssystem realisiert werden.

Die IP-PBX muss allerdings mit einer statischen IP-Adresse und einer statischen Portnummer konfiguriert werden. Diese werden im M-net Vermittlungssystem hinterlegt. Die IP-PBX sendet wiederum SIP- und RTP-Daten nur an die statische IP-Adresse und statischen Port des M-net Vermittlungssystems. Diese Daten werden von M-net mitgeteilt und müssen in der IP-PBX oder im E-SBC hinterlegt werden. Auch die Firewall muss für die verwendeten statischen IP-Adressen und Port geöffnet werden.

Auch beim Premium SIP-Trunk Static Mode gibt es mehrere Optionen, die IP-PBX an das M-net Vermittlungssystem anzuschalten.

7.1 Verwendete IP-Protokollversionen, Domains, IP-Adressen und Ports

Protokolle	IP-Adressen und Ports, die bei der Verwendung des Premium Static Mode SIP-Trunk zu konfigurieren sind
Signalisierung (SIP)	62.216.220.10 und 62.216.221.10 Port 5060
Mediadaten (RTP)	80.81.4.186 und 80.81.4.203 Portrange: 16384 - 65535
Internet Protocol Version (IPv)	4

7.2 Anschaltung einer IP-PBX im Premium SIP-Trunk Static Mode ohne Redundanz

Bei dieser Möglichkeit der Anschaltung wird die IP-PBX über einen M-net VoIP Ready Access oder einen bestehenden Internetzugang mit einem SBC des M-net Vermittlungssystem verbunden.

Damit die IP-PBX erfolgreich VoIP-Daten (SIP/RTP) sendet und empfängt, konfigurieren Sie bitte die statische Ziel-IP-Adresse und den statischen Ziel-Port des M-net Vermittlungssystems auf der IP-PBX oder im E-SBC. Außerdem müssen der statische Port und die statischen IP-Adressen in der Firewall freigegeben werden. Gleichzeitig werden die statische IP-Adresse und Port der IP-PBX im M-net Vermittlungssystem hinterlegt.

Bei einem abgehenden INVITE muss die IP-PBX einen **P-Asserted-Identity-Header** (PAI) mit der Hauptrufnummer oder DDI aufsetzen. Weitere Informationen zur INVITE Nachricht sind im Kapitel 8.1.1 zu finden.

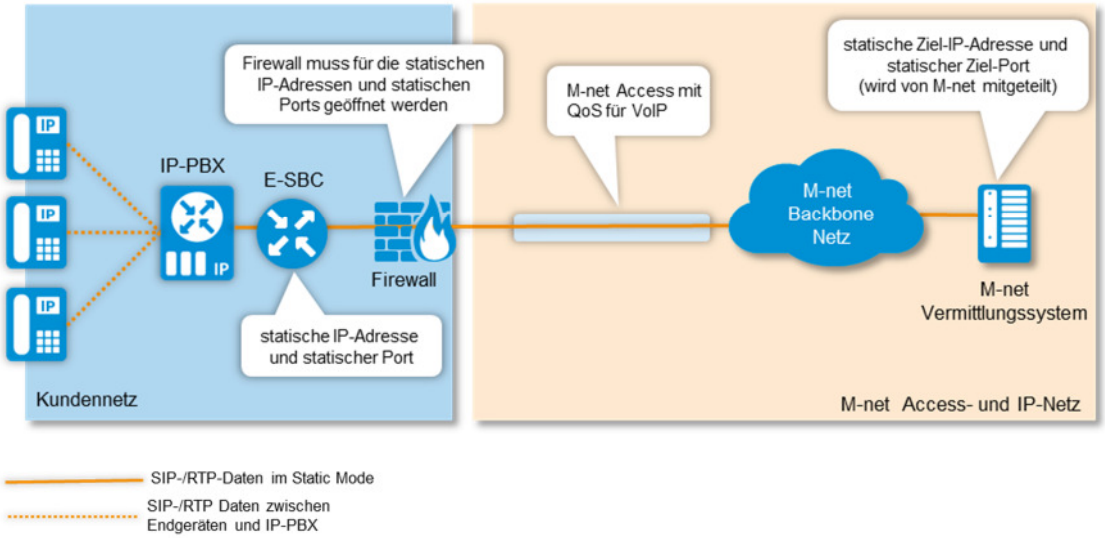


Abbildung 4: Beispiel Einfache Anschaltung einer IP-PBX im Premium SIP-Trunk Static Mode

7.3 Anschaltung einer IP-PBX im Premium SIP-Trunk Static Mode und Loadbalancing

Da das M-net Vermittlungssystem georedundant aufgebaut ist, besteht auch die Möglichkeit, den VoIP-Verkehr von der bzw. zur IP-PBX mit dem sogenannten Loadbalancing auf beide M-net Standorte gleichmäßig zu verteilen.
Ziel der SIP- und RTP-Daten, die von der IP-PBX gesendet werden, sind zwei je Standort unterschiedliche statische IP-Adressen und Ports des M-net Vermittlungssystems.

Beide statischen IP-Adressen und Ports des M-net Vermittlungssystems müssen in der IP-PBX eingetragen sein. Außerdem müssen der statische Port und die statischen IP-Adressen in der Firewall freigegeben werden. Gleichzeitig werden die statische IP-Adresse und Port der IP-PBX im M-net Vermittlungssystem hinterlegt.

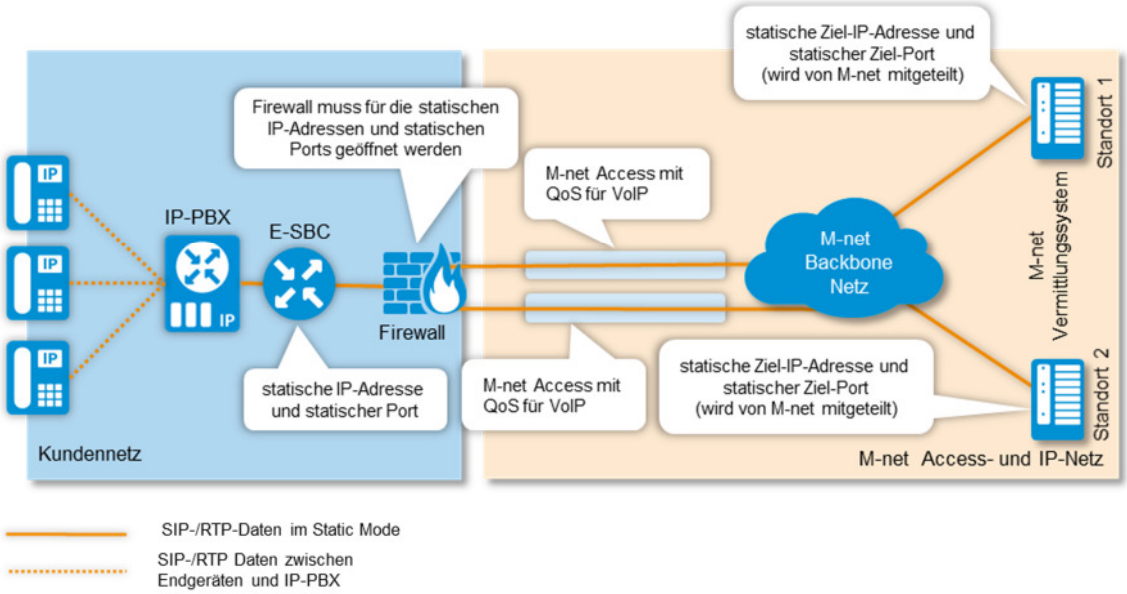


Abbildung 5: Anschaltung einer IP-PBX im Premium SIP-Trunk Static Mode und Loadbalancing

7.3.1 Anschaltung eines SIP-Trunk Accounts im Premium SIP-Trunk Static Mode mit Redundanz und Loadbalancing

Eine weitere Variante ist Redundanz inkl. Loadbalancing. Die Anschaltung wird ähnlich wie in Kapitel 7.3 realisiert. Für das Loadbalancing Verfahren werden zwei Access verwendet, die über das M-net Backbone Netz an die beiden Standorten des M-net Vermittlungssystem angebunden sind. Der Vorteil bei dieser Variante ist, dass die beiden Access unterschiedlich ausgelastet werden können (Loadbalancing). Standardmäßig ist der Standort 1 des M-net Vermittlungssystems die Hauptroute. Der Standort 2 kann als Alternativroute verwendet werden. Die Auslastung der beiden Routen wird anhand einer Gewichtung festgelegt. Die Voraussetzung für diese Variante sind zwei IP-PBX und/oder zwei E-SBC auf der Kundeseite. Diese werden jeweils mit der statischen IP-Adresse und dem statischen Port des Standortes 1 und mit der statischen IP-Adresse und dem statischen Port des Standortes 2 konfiguriert. Im M-net Vermittlungssystem werden am Standort 1 und am Standort 2 wiederum die statischen IP-Adressen und die statischen Ports der IP-PBXn bzw. der E-SBC hinterlegt.

Bei einem abgehenden INVITE muss die IP-PBX einen **P-Asserted-Identity-Header** (PAI) mit der Hauptrufnummer oder DDI aufsetzen. Weitere Informationen zur INVITE Nachricht sind im Kapitel 8.1.1 zu finden

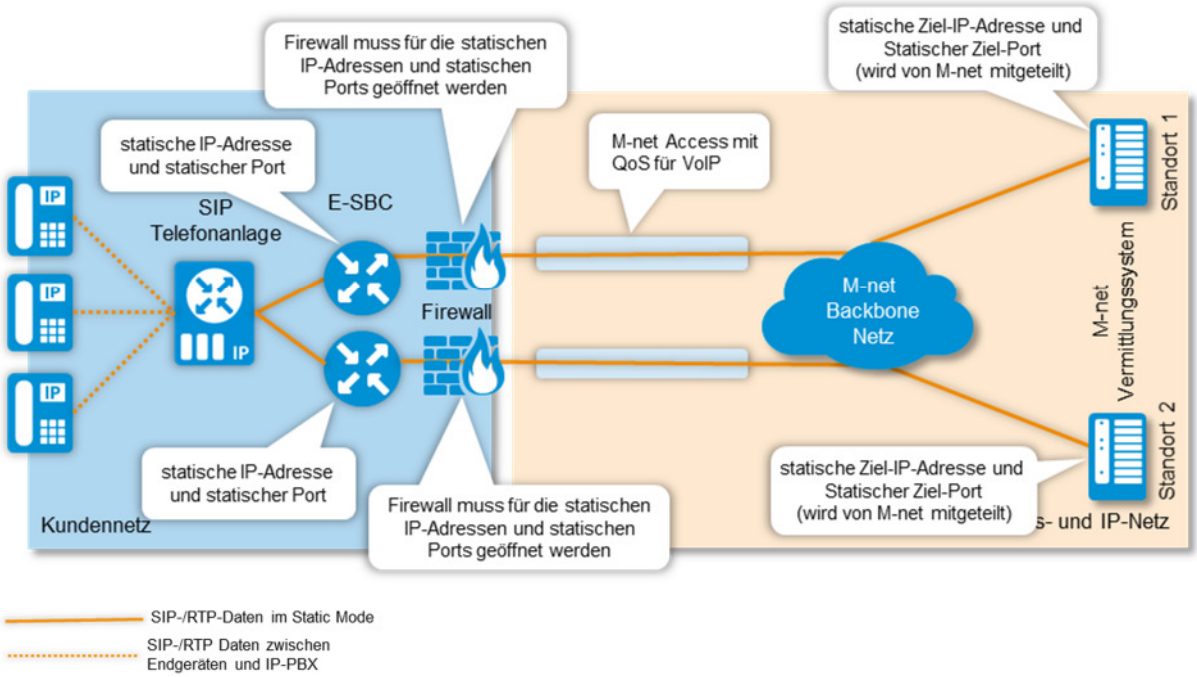


Abbildung 6: Anschaltung eines SIP-Trunk Accounts im Premium SIP-Trunk Static Mode mit Redundanz und Loadbalancing

7.4 Verwendung mehrerer SIP-Trunk Accounts im Premium SIP-Trunk Static Mode

Es besteht auch bei der Produktvariante Premium SIP-Trunk Static Mode die Möglichkeit, mehrere SIP-Trunk Accounts zu verwenden. Hierbei ist es wichtig, dass **je verwendeten SIP-Trunk Account, die IP-PBX im P-Asserted-Identity-Header** (PAI) **die Hauptrufnummer oder die DDI mitsendet**. Weitere Informationen zur INVITE Nachricht ist im Kapitel 8.1.1 zu finden.

7.4.1 Hinweis zu CLIP -no screening

Das Feature CLIP -no screening ist bei Premium SIP-Trunk Static Mode nur für eine Hauptrufnummer möglich.

7.5 Verschlüsselung bei SIP-Trunk Premium SIP-Trunk Static Mode

Leider kann bei der Produktvariante SIP-Trunk Premium SIP-Trunk Static Mode die Verschlüsselung nicht angeboten werden.

7.6 Zusammenfassung SIP-Trunk Premium SIP-Trunk Static Mode

Bitte beachten Sie die folgenden Punkte:

1. In der IP-PBX und/oder im E-SBC muss die statische IP-Adresse und der statische Port des M-net Vermittlungssystems konfiguriert werden
2. Dem M-net Vermittlungssystem muss die statische IP-Adresse und der statische Port der IP-PBX bekannt sein.
3. Die IP-Adressen und Ports müssen auch in der Firewall freigegeben werden
4. Bei abgehenden Anrufen muss die IP-PBX einen **P-Asserted-Identity-Header** (PAI) mit der Hauptrufnummer oder DDI aufsetzen

8 Telefonieren über den M-net SIP-Trunk

Basic | Premium | Static

Die folgenden Unterkapitel gelten für alle drei Produktvarianten.

8.1 Abgehendes Gespräch

Um ein abgehendes Gespräch zu initiieren, muss von der IP-PBX eine SIP Request (SIP Anfrage) in Form einer INVITE Nachricht gesendet werden.

8.1.1 INVITE Nachricht

INVITE sip:452000@business.mnet-voip.de SIP/2.0	Request Line
Via: SIP/2.0/UDP 192.168.178.123:5060;branch=z9hG4bK_AI2016Jul143556333452008398255;rport To: sip:452000@business.mnet-voip.de From: "SIP Telefon 12" <sip:+49891892912312@business.mnet-voip.de>;tag=12345 Call-ID: AI0AD3049CEB9CEF54@192.168.178.123 CSeq: 1 INVITE Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,PUBLISH,UPDATE,REFER,PRACK Allow-Events: presence,dialog,message-summary,refer Max-Forwards: 70 User-Agent: IP-PBX Supported: 100rel Content-Type: application/sdp Privacy: none Accept: application/sdp Contact: <sip:+49891892912312@192.168.178.123:5060;line=AI31A0DBF9D4721556> Content-Length: 281	Message Header (SIP)
v=0 o=ippbx 1831823547 1831823547 IN IP4 192.168.178.123 s=call c=IN IP4 192.168.178.123 t=0 0 m=audio 3000 RTP/AVP 8 9 101 a=rtpmap:8 PCMA/8000 a=rtpmap:9 G722/8000 a=rtpmap:101 telephone-event/8000 a=fmtp:101 0-15 a=sendrecv a=ptime:20 a=silenceSupp:off - - - -	Message Body (SDP)

Abbildung 7: Abgehende INVITE-Nachricht

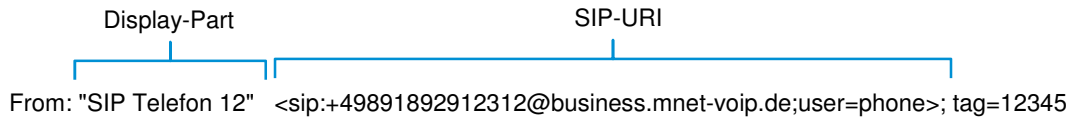
Die INVITE-Nachricht setzt sich zusammen aus der Request Line, dem Message Header und dem Message Body.

Hinweis: Die SDP-Angaben zu den Session-Attributen (a) können je nach IP-PBX von angegeben Beispiel abweichen. Die IP-PBX muss mindestens den Sprachcodec G.711a unterstützen und anbieten.

Die im **FROM-Header** mitgesendete SIP-URI enthält die Hauptrufnummer oder die Nebenstelle (DDI) des M-net SIP-Trunk Accounts und muss aus dem von M-net zugeteilten Rufnummernbereich entnommen sein. Diese Nummer muss im internationalen Format angegeben werden beginnend mit "+", entsprechend ITU-T Empfehlung E.164 und E.123. Die im FROM-Header eingetragene Rufnummer wird zur Authentifizierung und Vergebührung des Anrufes verwendet. Im Host-Part des FROM-Header muss die Domain business.mnet-voip.de eingetragen werden.
Der Display Part des FROM-Headers wird nicht übertragen.
Außerdem muss die IP-PBX den Statusparameter „user=phone“ unterstützen

Bei der Verwendung von CLIP –no screening kann eine beliebige Rufnummer im FROM-Header eingetragen werden. Hierzu bitte Kapitel 8.3.1.2 beachten.

Beispiel FROM-Header:



Im **TO-Header** kann die Zielnummer abhängig vom Zielort,
im internationalen Format mit „00“ Beispiel: 004989452000,
im internationalen Format mit führendem „+“ Beispiel: +4989452000,
im nationalen Format Beispiel: 089452000
oder im lokalen Rufnummernformat Beispiel: 452000
angegeben werden.

Ein mitgeschickter **P-preferred-identity-Header** (PPI) wird vom M-net Vermittlungssystem nicht verwendet.

Wie im SIPConnect Standard 1.1 festgelegt, muss die IP-PBX einen **P-Asserted-Identity-Header** (PAI) mit der Hauptrufnummer oder DDI aufsetzen. Da es sich bei der sog. PAI um einen „trusted“ Header handelt, wird dieser vom M-net Vermittlungssystem neu aufgesetzt. Hierfür wird die verifizierte Rufnummer des FROM-Headers verwendet. Dies gilt nicht, wenn „CLIP no screening“ im M-net Vermittlungssystem aktiviert ist.

Der **erste „via-Header“** in der INVITE-Nachricht muss mit dem „via-Header“ der REGISTER-Request übereinstimmen. Der „branch-Parameter“ ist davon ausgenommen.
(vgl. „via-Header“ in „Beispiel einer initialen REGISTER Request“ und „Beispiel einer abgehenden INVITE Nachricht“)

8.1.1.1 Message Body

Im Message Body werden - mit Hilfe des SDP – u. a. den Codec, die die IP-PBX verwendet, dem Zielendgerät angeboten. Auch die Art des Medientyps, sowie Port und Protokolle für den Transport der Medienströme werden an das Ziel übermittelt. Neben diesen Informationen beinhaltet das SDP weitere Angaben zur initiierten Session (s. Kapitel 8.1.1 Beispiel einer abgehenden INVITE Nachricht)

8.1.2 Authentifizierung bei abgehenden Gesprächen

Bei jedem abgehenden Verbindungsversuch wird die IP-PBX vom M-net Vermittlungssystem aufgefordert, diesen zu authentifizieren. Nach dem initialen INVITE schickt das M-net Vermittlungssystem ein „401 Unauthorized“ zurück. Daraufhin sendet die IP-PBX eine weitere INVITE Nachricht mit einem „Authorization-Header“.

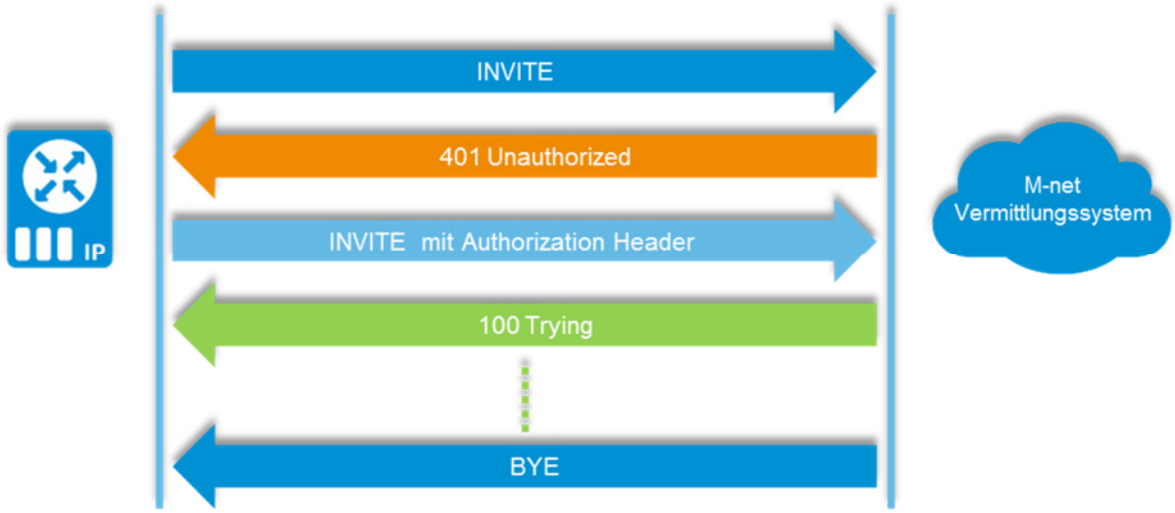


Abbildung 8: Beispiel Gesprächsauthentifizierung

Der Response 407 Proxy-Authentication Required wird vom M-net Vermittlungssystem nicht unterstützt bzw. angewendet.

8.2 Ankommendes Gespräch

Wie bei einem abgehenden Gespräch, besteht auch die INVITE Nachricht bei einem ankommenden Gespräch aus der Request Line, dem Message Header und dem Message Body.

INVITE sip:+49891892912312@192.168.178.123:5060;line=AIB634BB98E7969A90 SIP/2.0	Request Line
Via: SIP/2.0/UDP 80.81.4.125:5060;rport;branch=z9hG4bK+2cfc8627adbc7973d123fc7cbc5ed7621+sip+5+a65bcda9 From: <sip:+4989452000@business.mnet-voip.de>;tag=business.mnet-voip.de+5+c2d1a919+aba6a05a To: <sip:+49891892912312@business.mnet-voip.de> CSeq: 565355236 INVITE Expires: 180 Content-Length: 221 Supported: resource-priority, histinfo Contact: <sip:ef8656f92d319f9b5a785123456789@business.mnet-voip.de:5060> Content-Type: application/sdp Call-ID: 0gQAAC8WAAACBAAALxYAAOLRAJdoAqpYCbqX9wa2bBweOfP9ycvHJs9dK5bUAihq@business.mnet-voip.de Max-Forwards: 56 History-Info: <sip:+49891892912312@osp.mnet-voip.de;user=phone>;index=1 History-Info: <sip:d31dea775a52569fbb1fee85b22b1bc6@172.24.53.170:5060;line=AIB634BB98E7969A90>;index=1.1;rc=1 Accept: application/sdp, application/dtmf-relay	Message Header (SIP)
v=0 o=- 80742731454362 80742731454362 IN IP4 80.81.4.126 s=- c=IN IP4 80.81.4.123 t=0 0 m=audio 17424 RTP/AVP 8 18 100 110 a=rtpmap:100 telephone-event/8000 a=rtpmap:110 PCMU/8000 a=fmtp:18 annexb=no a=ptime:20	Message Body (SDP)

Abbildung 9: Beispiel einer ankommenden INVITE-Nachricht

Die SIP-URI im **TO-Header** des ankommenden SIP INVITE enthält die DDI (Hauptrufnummer + Nebenstellennummer) der IP-PBX und den M-net Domain-Namen. Der **Request-Header** beinhaltet die SIP-URI, bestehend aus der DDI der jeweiligen Nebenstelle und der IP-Adresse der IP-PBX und dem internen Port. Die Rufnummer ist im internationalen Format mit einem führendem „+“ angegeben.

Die Rufnummer im **FROM-Header** wird vom M-net Vermittlungssystem wie im SIPconnect Standard 1.1 gefordert, im internationalen Format mit einem führendem „+“ an die IP-PBX übermittelt. Entsprechend der ITU-T Empfehlung E.164.

8.3 Leistungsmerkmale

Im folgenden Kapitel sind die für SIP-Trunk verfügbaren Leistungsmerkmale aufgelistet.
Hinweis: Bestimmte Leistungsmerkmale sind erst nach Beauftragung verfügbar.
Eine ergänzende Erklärung der einzelnen Leistungsmerkmale ist in der Leistungsbeschreibung zu finden.

8.3.1 Leistungsmerkmale des M-net Vermittlungssystems

Leistungsmerkmale, die im M-net Vermittlungssystem realisiert werden, können nur auf die gesamte IP-PBX angewendet werden.
Um die Leistungsmerkmale des M-net Vermittlungssystems per Telefon zu steuern ist es, je nach Konfiguration der IP-PBX nötig, die Amtsholungsziffer zu wählen. Die angegebenen Leistungsmerkmale können über die Nebenstellen nur dann aktiviert bzw. deaktiviert werden, wenn der jeweilige Featurecode nicht von der IP-PBX abgefangen und ausgewertet wird.

Für SIP-Trunk werden die in der folgenden Tabelle aufgeführten Leistungsmerkmale vom M-net Vermittlungssystem zur Verfügung gestellt:

Leistungsmerkmal	Aktivierung Deaktivierung	Ausführende Einheit
ACR	*52# #52#	IP-PBX*1, Vermittlungssystem*2
CLIP		Vermittlungssystem*2
CLIP -no screening	Weitere Hinweise unter Punkt 8.3.1.2	Vermittlungssystem*2
CLIR 1		Vermittlungssystem*2
CLIR 2 (CLIRREQ)	*31*RN#	Vermittlungssystem*2
CFU CFV (DIVI)	*21*RN# #21#	IP-PBX*1, Vermittlungssystem*2
CFB (DIVBY)	*67*RN# #67#	IP-PBX*1, Vermittlungssystem*2
CFNA CFDA CFNR (DIVDA)	61*RN# #61#	Vermittlungssystem*2
PR (Partial Rerouting – SIP 302)	Weitere Hinweise unter Punkt 8.3.1.1	IP-PBX*1, Vermittlungssystem*2

CFD (CFALD)		Vermittlungssystem*2
DDI		IP-PBX*1
MCID Fangen		Vermittlungssystem*2

*1 Realisierung in IP-PBX für einzelne Nebenstellen.

*2 Realisierung im M-net Vermittlungssystem für gesamte IP-PBX.

8.3.1.1 Leistungsmerkmal „Bedingte Anrufweiterleitung“ (PR)

Das Leistungsmerkmal „Bedingte Anrufweiterleitung“ (Partial Rerouting) ist aktiviert. Um dieses Leistungsmerkmal nutzen zu können, muss evtl. in der IP-PBX die Umlenkart "Rufumlenkung extern" bzw. "Bridge mode = none" aktiviert sein. Die Umlenkung wird in der Vermittlungsstelle durchgeführt. Die IP-PBX initiiert Partial Rerouting durch die SIP Message 302 Moved Temporarily. Diese muss einen Referred-By bzw. Diversion Header / History-Info enthalten welcher die umlenkende Rufnummer identifiziert. Die umlenkende Rufnummer muss in dem von M-net zugeteilten Rufnummernbereich liegen. Das Umlenkziel muss im SIP-URI Format im Contact Header der SIP-Nachricht „302 Moved Temporarily“ stehen.

Das Rufnummernformat der umlenkenden Rufnummer ist im Kapitel 0 „Message Header“ im Punkt „FROM-Header“ beschrieben.

Die SIP Message 302 kann ein Diversion-Header entsprechend RFC 5806 oder eine History-Info entsprechend RFC 4244 enthalten.

Beispiel:

Die Nebenstelle 0894622123 ist eine Nebenstelle der IP-PBX und hat eine externe Rufumleitung auf die 089452001234 konfiguriert. Bei einem Anruf auf die 0894622123 schickt die IP-PBX eine „302 Moved Temporarily“ Nachricht zurück. Das umgelenkte Ziel wird im Contact Header angegeben. Die Weiterleitung wird daraufhin in der Vermittlungsstelle aktiv.

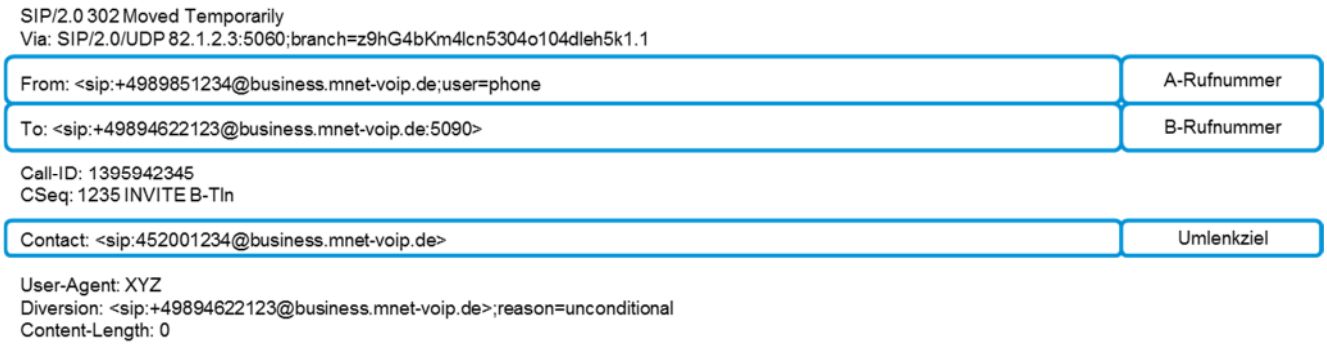


Abbildung 10: Beispiel einer „302 – Moved Temporarily“ Nachricht

8.3.1.2 Leistungsmerkmal CLIP –no screening

Bei aktivierten CLIP-no screening kann im **FROM-Header eine beliebige gültige Rufnummer, im internationalen Format mit einem führendem „+“ eingetragen werden**. Ist das Leistungsmerkmal im M-net Netz für den SIP-Trunk nicht aktiv und im FROM-Header wird eine beliebige Rufnummer mitgeschickt, wird beim Ziel die Hauptrufnummer angezeigt. Dies ist auch der Fall, wenn im FROM-Header eine fehlerhafte Rufnummer eingetragen wird.

Außerdem **muss** die IP-PBX einen PAI-Header mit der Hauptrufnummer oder der Durchwahlnummer in der INVITE Nachricht mitsenden.

Die Vergebührung von Anrufen erfolgt bei aktiviertem CLIP –no screening auf die Hauptrufnummer.

8.3.2 (Fallweise) Unterdrückung der Rufnummer (CLIR und CLIREQ)

Soll die Rufnummer des Anrufers beim Angerufenen nicht angezeigt werden (CLIR), muss entsprechend RFC 3323 und RFC 3325 die IP-PBX einen **"Privacy: id" Header** in die SIP INVITE Nachricht einfügen. Im FROM Header muss die DDI der jeweiligen Nebenstelle eingetragen werden. Diese A-Teilnehmernummer muss aus dem von M-net dem Kunden zugeteilten Rufnummernbereich entnommen sein und aus Durchwahlnummer der Nebenstelle (DDI) bestehen.

Diese Nummer muss im internationalen Format angegeben werden beginnend mit "+", entsprechend ITU-T Empfehlung E.164 und E.123.

Die A-Teilnehmernummer wird zur Vergebührung des Anrufes verwendet (z.B.: FROM: "Anonymous"<sip:+49894622123@business.mnet-voip.de).

Sendet die IP-PBX einen fehlerhaften bzw. komplett anonymisierten FROM-Header, z.B. "sip:anonymous@anonymous.invalid" kann die SIP-Request nicht authentifiziert werden und wird der Hauptrufnummer zugeordnet.

Auch durch voranstellen der *31* vor der Zielrufnummer durch die IP-PBX bzw. Nebenstelle kann die Rufnummer fallweise unterdrückt werden (CLIREQ).
Beispiel To-Header: To: <sip:*31*452000@business.mnet-voip.de>

Hinweis: Bei der Verwendung von CLIR bzw. CLIRREQ wird die IP-PBX-Hauptrufnummer mit den Gesprächsgebühren belastet.

8.3.2.1 Call Forwarding Busy

Um das Leistungsmerkmal „Call Forwarding Busy“ (CFB) nutzen zu können muss in der IP-PBX „Anklopfen“ deaktiviert sein. Dadurch schickt das Endgerät des Zielteilnehmers im Besetztfall ein „486 Busy Here“ zurück. Durch diese SIP-Message wird die Weiterleitung zu einem anderen Ziel durch das Vermittlungssystem initiiert.

8.3.3 Unterstützte IP-PBX Leistungsmerkmale

Die in den folgenden Tabellen aufgeführten Leistungsmerkmale sind Leistungsmerkmale der IP-PBX, welche ohne Mithilfe des M-net Vermittlungssystem bzw. M-net Transportnetzes realisiert werden.

Leistungsmerkmal	Erläuterung
CW	Call Waiting (Anklopfen, es werden 2 SIP-Sessions aufgebaut)
CH	Call Hold (Halten, Rückfrage und Makeln, es werden 2 SIP-Sessions aufgebaut)
MOH	Music on Hold (Wartemusik bei Call Hold)
3PTY	Three Party (Dreierkonferenz, es werden 2 SIP-Sessions aufgebaut)
CT	Call Transfer (Vermitteln in IP-PBX es werden 2 SIP-Sessions aufgebaut)

8.3.3.1 IP-PBX Leistungsmerkmale Call Forwarding (CF) und Call Transfer (CT)

Die Umlenkung wird in der IP-PBX, z.B. mit der IP-PBX-Funktion „Rufumlenkung intern“ durchgeführt. Für CF bzw. CT wird jeweils eine zweite gehende SIP-Session aufgebaut.

Hierzu muss **von der IP-PBX eine INVITE-Nachricht zur Zielrufnummer generiert werden**. In dieser zweiten INVITE wird die ursprüngliche A-Rufnummer im FROM-Header von der IP-PBX eingetragen. Diese Nummer muss im internationalen Format angegeben werden beginnend mit "+".
Ist CLIP –no screening im Netz aktiviert, wird beim Zielteilnehmer die ursprüngliche A-Rufnummer angezeigt. Die Vergebührung des Anrufes erfolgt auf die Hauptrufnummer. Ist CLIP –no screening netzseitig nicht aktiv oder der FROM-Header enthält einen fehlerhaften Eintrag, wird die Hauptrufnummer des SIP-Trunks beim Zielteilnehmer angezeigt.

8.3.4 Nicht unterstützte Leistungsmerkmale

Nicht alle Leistungsmerkmale aus der klassischen Telefonie können auf der VoIP Technologie abgebildet werden. In der folgenden Tabelle sind Leistungsmerkmale aufgeführt, die nicht unterstützt werden.

Leistungsmerkmal	Bedeutung
AOC, AOC99	Advice of charge (Übermittlung von Gebühreninformationen)
COLP	Anzeige der Nummer des Angerufenen Teilnehmer
COLR	Unterdrückung der Nummer des Angerufenen Teilnehmer
CUG	Closed User Group
SUB	Subaddressing (teilnehmerseitige Erweiterung der Rufnummer über den öffentlichen Nummerierungsplan hinaus
UUS	User to User Signaling
MSN	Multiple Subscriber Number (Mehrfachrufnummer)
TP	Terminal Portability (Parken eines Gesprächs in der Vermittlungsstelle)
CCBS, CCNR	Call Complete Busy Subscriber (Rückruf bei Besetzt), Completion of Calls on No Reply Subscriber (Automatischer Verbindungsaufbau in der Vermittlungsstelle zu einem Teilnehmer, der sich nicht meldet)
CNAP	Calling Name Presentation

9 Physikalische Anschaltung der IP-PBX am M-net VoIP-Ready Access

Premium Static

Hinweis für Premium SIP-Trunk Static Mode: Dieses Kapitel gilt nur, wenn ein M-net Access verwendet wird!

Die für den SIP-Trunk benötigte Anschlussbandbreite wird anhand der beauftragten Sprachkanäle ermittelt. Die Begrenzung der gleichzeitigen Gespräche wird vom M-net Vermittlungssystem vorgenommen. Verbindungsversuche, die über dem Limit der beauftragen Sprachkanäle liegen werden von der Begrenzungskontrolle abgewiesen.

9.1 Beispiel Anschaltung einer IP-PBX mit NAT

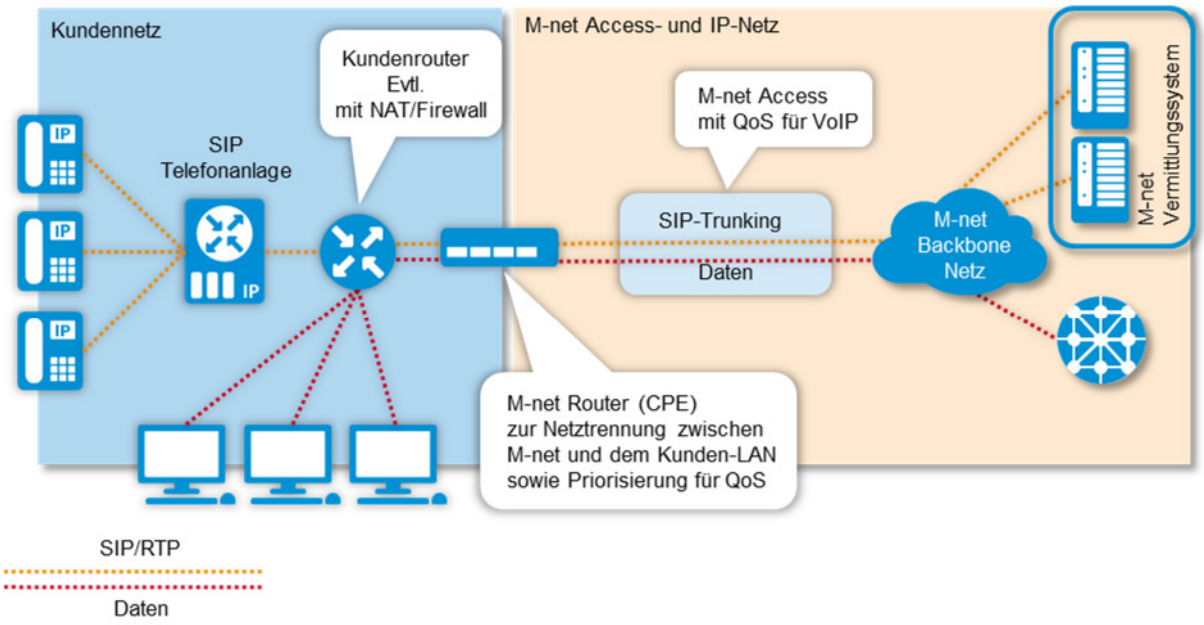


Abbildung 11: Beispiel Anschaltung der IP-PBX an die M-net Infrastruktur mit Verwendung eines Kundenrouters

Bei der **Verwendung eines kundeneigenen Routers** sollte die IP-PBX mit diesem verbunden werden. Ist NAT auf dem Kundenrouter aktiv, muss NAT im M-net Router (CPE) deaktiviert sein. Ansonsten kann es zu Problemen bei der NAT-Erkennung durch das M-net VoIP Vermittlungssystem kommen.

Die jeweiligen RTP- und SIP-Ports müssen evtl. im Kundenrouter konfiguriert werden, damit die Sprachpakete fehlerfrei übertragen werden können.

Zwischen dem Kundenrouter und der IP-PBX bzw. dem Kunden-LAN können Layer2-Geräte (Switches) liegen.

Hinweis: NAT ist im M-net Router bei den Accessvarianten SDSL, Glasfaser-SDSL und Direct Access deaktiviert und muss gesondert beauftragt werden

9.2 Beispiel Anschaltung einer IP-PBX mit Verwendung einer Firewall

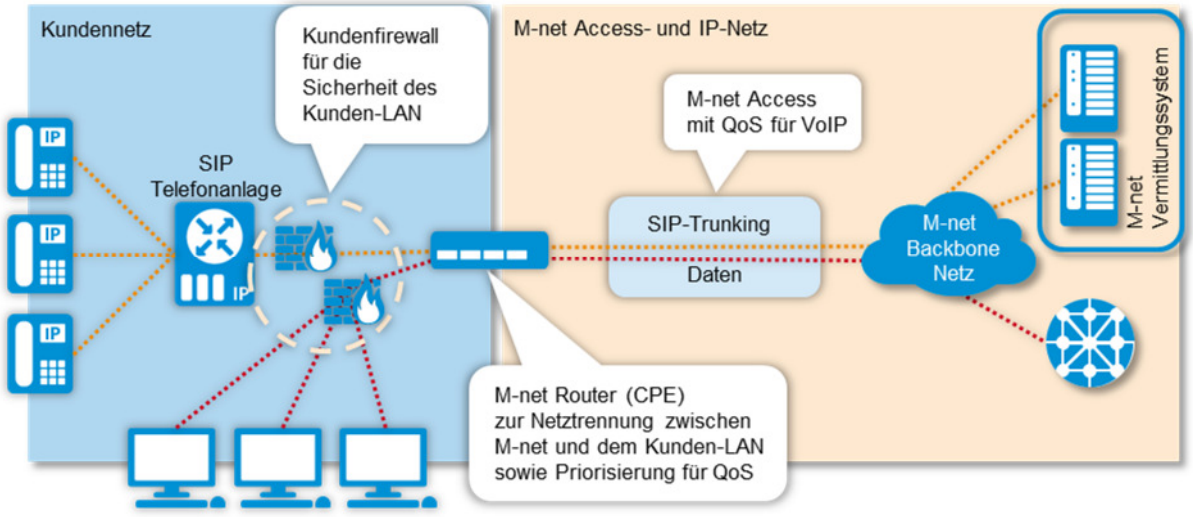


Abbildung 12: Beispiel Anschaltung der IP-PBX an die M-net Infrastruktur mit Verwendung einer Kunden-Firewall.

Die Darstellung der Firewall im Kunden LAN ist logisch als zwei Einheiten dargestellt. Physikalisch kann es sich um das selbe Gerät handeln, welches über zwei getrennte Interface oder über ein Interface mit dem M-net Router (CPE) verbunden ist.

Die Firewalls können auch über Layer2-Geräte (Switches) mit dem M-net Router verbunden werden.

Die jeweiligen RTP- und SIP-Ports müssen evtl. in der Firewall konfiguriert werden, damit die Sprachpakete fehlerfrei übertragen werden können.

Je nach Modell des M-net Routers, stehen ein oder vier FastEthernet bzw. GigabitEthernet Interfaces LAN-seitig zur Verfügung.

9.3 Anbindung des Kundennetzes

Alle vorhandenen Switchports am CPE sind als Access Ports definiert und gehören zum nativen VLAN1. Daher werden nur Datenpakete ohne 802.1q tag vom Kundennetz erwartet. Datenpakete mit 802.1q tag werden hingegen verworfen.
Die Markierung der Datenpakete für QoS in Richtung M-net Vermittlungssystem wird durch das CPE vorgenommen und ist in 9.4.3 näher beschrieben.

Eine Übergabe per VLAN wird derzeit nicht unterstützt.

9.4 Quality of Service (QoS) bei Premium SIP-Trunk

Unter Quality of Service (QoS) sind bestimmte Parameter in der ITU Empfehlung G.114 beschrieben, die für die Übertragungsqualität von Sprachdaten wichtig sind. Dazu zählen die Paketlaufzeit, die Paketlaufzeitschwankungen, die Paketverlusthäufigkeit und die Paketfehlerhäufigkeit.

Um die ITU-Empfehlungen einzuhalten, werden beim Produkt Premium SIP-Trunk die Sprachdaten (RTP Ströme) vom Kunden LAN ab dem M-net CPE (upstream) höher priorisiert und somit vorrangig übertragen. Dies geschieht anhand der IP-Adressen des M-net Vermittlungssystems.

Ebenfalls werden die Sprachdaten vom M-net Vermittlungssystem zum Kunden LAN gehend (downstream) im M-net Netzwerk, einschließlich M-net CPE, höher priorisiert.

Ab der bzw. bis zur Verkehrsübergabe im CPE ist der Kunde selbst dafür verantwortlich, dass Sprachpakete im LAN in beide Richtungen (upstream und downstream) priorisiert übertragen werden.

9.4.1 Bandbreite, Zuweisung und Begrenzung

Die Bandbreitenbegrenzung zwischen dem Kunden-LAN und dem M-net Netz bezieht sich auf die Gesamtbandbreite aller Verkehrsarten, d.h. High-Speed Internet (HSI) und VoIP. Es werden nur zwei Verkehrsarten, „Daten“ und „VoIP“ unterschieden. Um die beste Qualität für VoIP zu erzielen und gleichzeitig die optimale Auslastung der verfügbaren Bandbreite zu nutzen, wird die verfügbare Bandbreite für HSI und VoIP dynamisch aufgeteilt (siehe 9.4.4).
Zusätzlich wird die Begrenzung der möglichen gleichzeitigen Gespräche durch die Begrenzungskontrolle am M-net Vermittlungssystem vorgenommen.

9.4.2 Classification – Erkennung von Datenpakete

Unter „Classification“ versteht man die Kriterien, nach denen ein Netzelement, z.B. das CPE, die VoIP- und Daten-Pakete als solche erkennt und klassifiziert. Die Erkennung der einzelnen Datenpakete erfolgt im CPE Richtung M-net Netz (Upstream) anhand der Ziel-IP-Adresse. Wird ein Paket mit der Ziel-IP-Adresse des M-net Vermittlungssystem versehen, wird es im CPE als VoIP-Paket (SIP und RTP) klassifiziert und priorisiert an das M-net Vermittlungssystem gesendet.

Die Layer 3 Markierung (DSCP oder Precedence), die ein Netzelement in Kunden LAN setzt, wird nicht beachtet.

Alle Pakete, die nicht als VoIP-Pakete markiert sind, werden als „Daten“-Paket klassifiziert und daher nach „Best-Effort“ übertragen.

9.4.2.1 Classification im Detail

- Die Klassifizierung erfolgt anhand der oben genannten Kriterien.
- Es findet **keine Analyse der Nutzlast (Daten/Sprache) auf Applikationsebene (Deep packet Inspection) statt**, um festzustellen, ob die Datenpakete als „Daten“ oder „VoIP“ zu behandeln sind.
- Wenn ein Paket vom Kunden-LAN mit der Ziel-IP-Adresse des M-net Vermittlungssystems am CPE-Switchport ankommt, wird es als VoIP-Paket markiert, unabhängig davon, ob es sich um ein SIP- oder um ein RTP-Paket handelt. Daher wird es entsprechend priorisiert und belegt die für VoIP vorgesehene Bandbreite.
- Wird die für VoIP vorgesehene Bandbreite im Upstream überbucht (am CPE ist Bandbreite der ankommenden Pakete höher als die gesamte Produktbandbreite), werden zwangsläufig VoIP-klassifizierte Pakete verworfen. Es leidet daher die Qualität der tatsächlichen VoIP-Ströme und die der weiteren als VoIP-klassifizierten Ströme gleichermaßen darunter.
- Es erfolgt keine Klassifizierung anhand von Layer 2 Markierung (P-bit in 802.q header), da Pakete mit VLAN-Markierung im M-net CPE verworfen werden.

9.4.3 Markierung von VoIP-Paketen

Bei den Produkten SDSL und Glasfaser-SDSL erfolgt auf Layer 3 für RTP-Pakete aus dem Kunden-LAN keine erneute QoS Markierung. Daher wird die Markierung, die im Kunden LAN gesetzt wird, transparent im Upstream übertragen.
Beim Produkt „Direct Access“ mit der Option „VoIP-Ready“ hingegen erfolgt eine erneute Markierung, d.h. das DSCP-Feld im IP-Header wird immer überschrieben. Daten Pakete werden mit DSCP=0 neu markiert. VoIP-Pakete werden mit DSCP=EF markiert. D.h. es wird beim Direct-Access, im Gegensatz zu SDSL und Glasfaser-SDSL, keine DSCP Transparenz unterstützt.

Bei allen Produkten wird die vorhandene Layer 3 Markierung (DSCP- oder Precedence), wie vom Kundenequipment gesetzt, nicht beachtet.

Im Downstream (von M-net zum Kunden) werden die SIP- und RTP-Pakete vom M-net Vermittlungssystem generiert und mit DSCP = AF31 für SIP und DSCP = EF für RTP/RTCP versehen. Alle anderen Internet-Datenströme werden hinsichtlich der QoS Layer 3 Markierung transparent übertragen. Damit wird eine Implementierung der QoS-Mechanismen im Kunden-LAN erleichtert.

9.4.4 Priorisierung/scheduling des VoIP-Verkehrs

Um QoS zu gewährleisten werden VoIP-Pakete strickt priorisiert. Die Up- und Downstream-Bandbreiten betragen bei der Option „VoIP-Ready“ 66% der Produktbandbreite (s. Abbildung 13: Szenarien mit bzw. ohne Verlust bei Daten-/VoIP-Strömen). Das ist ausreichend, um die bekannten Probleme bei geringen Bandbreiten (<5Mbit/s) (z.B. serialization delay oder hoher Jitter durch große Daten-Pakete) zu umgehen. Solange die maximale Produktbandbreite nicht überschritten wird, kann für den Datenstrom so eine optimale Qualität erreicht werden.

Die Bandbreite wird dynamisch den Daten- und/oder VoIP-Strömen zugeteilt. D.h. der Datenstrom nimmt die gesamte Produktbandbreite ein, so lange keine VoIP-Telefonie aktiv ist.
Sobald SIP- bzw. RTP-Pakete gesendet bzw. empfangen werden, wird die dafür notwendige Bandbreite belegt. Wenn die Summe aller gleichzeitigen Datenströme die Produktbandbreite überschreitet, aber die

maximale VoIP-Bandbreite nicht überschritten wird, werden ausschließlich Daten-Pakete (kein VoIP-Paket) verworfen, um die Grenze einzuhalten.
Wird die VoIP-Bandbreite überschritten, werden zwangsweise auch VoIP-Pakete verworfen.
Wird die Anzahl gleichzeitiger VoIP-Gespräche (Calls) reduziert, steht die frei gewordene Bandbreite wieder für Datenströme zur Verfügung.
Die verschiedenen Szenarien sind im nachfolgenden Bild dargestellt.
Die Nutzung von stärkeren Komprimierungsverfahren (z.B. Codec G.729), sofern vom M-net Vermittlungssystem unterstützt, ist möglich. Die vertraglich festgelegte Anzahl maximaler Sprachkanäle bleibt jedoch unverändert, selbst wenn die maximale VoIP-Bandbreite nicht vollständig ausgenutzt ist, weil z.B. ein optimierter Codec ausgehandelt wird.

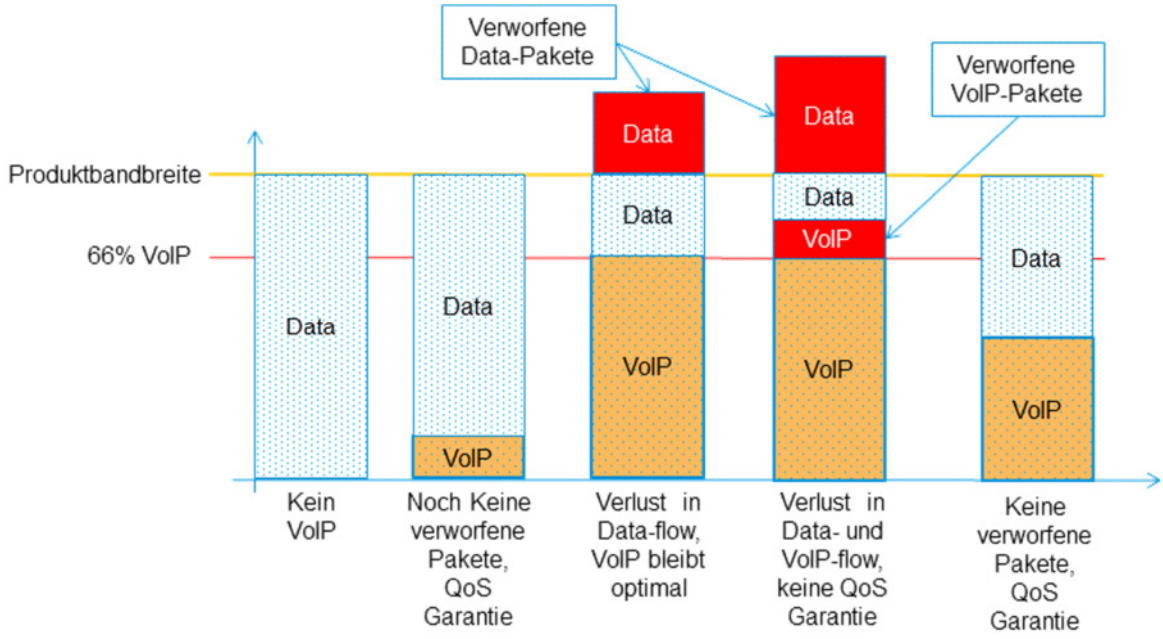


Abbildung 13: Szenarien mit bzw. ohne Verlust bei Daten-/VoIP-Strömen

9.5 Weitere Real-Time-Ströme (z.B. Video)

RTP-Pakete, die Video-Nutzdaten enthalten, haben andere Eigenschaften als RTP-Pakete einer VoIP-Verbindung (z.B. kein konstanter Datenstrom bzw. sehr unterschiedliche Paketgröße). Es ist prinzipiell möglich (vorausgesetzt die Funktion wird vom M-net Vermittlungssystem unterstützt) eine Multimedia-Verbindung statt einer VoIP-Verbindung zwischen SIP-Telefonen oder Softphones aufzubauen. Wenn der Videostrom als VoIP-Strom klassifiziert wird, (vgl. 9.4.2) wird die entsprechende Bandbreite belegt. Um QoS zu gewährleisten, ist dafür Sorge zu tragen, dass die maximal reservierte Bandbreite von 66% der Produktbandbreite, für VoIP-Gespräche und Video-Verbindungen, nicht überschritten wird. Die QoS-Option VoIP-Ready für M-net Accessprodukte ist so dimensioniert, dass die vertraglich festgelegte Anzahl von gleichzeitigen Gesprächen (Sprachkanäle) mit QoS-Garantie durchgeführt werden können, sofern erlaubte Codecs verwendet werden.
Ähnliches gilt für VoIP-Verbindungen, die mehrere gleichzeitige SIP- bzw. RTP-Ströme erzeugen (z.B. Stereo) oder Codecs nutzen, die eine höhere Bandbreite als G.711 (z.B. High-Fidelity Audio) benötigen.

10 NAT (Network Address Translation)

Basic Premium

10.1 NAT traversal

RTP-Ströme und die dazugehörende RTP-Signalisierung (RTCP) müssen nach der IETF-SIP-Architektur direkt zwischen den Endpunkten fließen. Pro Richtung jeweils ein Strom wie z.B. zwischen IP-fähigen Telefonen oder Softphones. Daher müssen die Endpunkte die routbaren IP-Adressen der jeweils anderen Seite kennen. Wird NAT genutzt, kennt ein Endpunkt nur die private (und damit nicht routbare) Adresse und fügt diese der SIP-Signalisierung hinzu. Ohne weitere Maßnahmen wird diese private Adresse dann von der Gegenstelle adressiert. Somit kann das jeweilige Ziel nicht erreicht werden. Unter NAT-traversal versteht man verschiedene technische Lösungen für dieses Problem.

10.1.1 Symmetrisches RTP im SIP-UA

Vom SIP-UA (SIP-User Agent) der Endpunkte werden die VoIP-Pakete zum NAT gesendet bzw. vom NAT empfangen.
Ein Endpunkt kann sein:

- ein Telefon oder Softphone, wenn die IP-PBX den Ende-zu-Ende RTP-Strom zulässt
- eine IP-PBX (SIP-Telefonanlage)
- ein E-SBC (Enterprise Session Border Controller)

Bei symmetrischem RTP werden auf dem gleichen RTP/RTCP-Port Pakete gesendet und empfangen. Durch die ersten Pakete die vom SIP-UA durch das NAT gehen, entsteht das sogenannte Binding. Das gleiche Binding wird genutzt, um Pakete vom M-net Vermittlungssystem zu empfangen. Die meisten SIP-UA unterstützen symmetrisches RTP/RTCP.

10.1.2 Far-End NAT Erkennung

M-net unterstützt die Far-End NAT Erkennung (symmetrisches RTP). Sofern der SIP-UA ebenso „symmetrisches RTP“ unterstützt, ist das Problem mit NAT traversal gelöst.

Die Far-End NAT Erkennung im M-net Vermittlungssystem erkennt NAT sowohl auf der SIP- als auch auf RTP-Ebene.
Das M-net Vermittlungssystem vergleicht dafür bei der Registrierung die Source-IP im IP-Header und die IP-Adresse im obersten via Header. Sind diese beiden IP-Adressen unterschiedlich, wird NAT verwendet. Daraufhin wird das Zeitintervall bis zur Re-Registrierung vom M-net Vermittlungssystem auf einen Wert von 30 Sekunden angepasst.

Um NAT auf RTP-Ebene zu erkennen, werden die Source-IP und der Source-Port des ersten RTP-Paketes, das von der IP-PBX beim M-net Vermittlungssystem eintrifft verwendet, um den Mediastrom an diese IP-Adresse und Port zu senden.

Ausnahme: Zwei symmetrische NATs liegen zwischen der IP-PBX des Kunden und dem M-net Vermittlungssystem. Auch wenn der SIP-UA „symmetrisches RTP“ unterstützt, kann er nur die bekannte private IP-Adresse routen und ist damit von außen nicht mehr erreichbar. Ohne Far-End NAT Erkennung, wäre eine Alternative die Anwendung eines STUN-Servers. Der STUN-Server ermöglicht dem SIP-UA Pakete mit der öffentlichen IP-Adresse zu generieren (in Kapitel 11 erklärt).

10.1.3 Symmetrisches NAT

Symmetrisches NAT stellt die größte Schwierigkeit für NAT-traversal dar. Es erzeugt ein neues Binding für jede Verbindung, die vom gleichen SIP-UA erstellt wird. Da die SIP-Signalisierung und die RTP-

Pakete zu unterschiedlichen Adresse-Port Paaren gesendet werden, behandelt symmetrisches NAT diese als unterschiedliche Verbindungen und weist ein neues Binding zu. Dies führt das M-net Vermittlungssystem mit Far-End NAT Erkennung zur falschen Manipulation der SIP Nachrichten, da die Port-Nummer im SDP vom M-net Vermittlungssystem nicht geändert wird.
Hinweis: Von der Anwendung eines symmetrischen NATs wird daher abgeraten.

10.2 Firewall (FW)

10.2.1 FW in CPE

Das CPE bietet keine Firewall-Funktion. Der Zugriff auf Funktionen für Management und Administration des CPEs sind M-net vorbehalten. Die NAT-Funktion, wenn vorhanden, bietet keine ausreichende Sicherheit.

10.2.2 FW im Kunden-LAN

Genau wie für NAT im Kunden-LAN, muss durch den Kunden sichergestellt werden, dass die Ports für die VoIP-Kommunikation (RTP, RTPC und SIP) in beide Richtungen geöffnet sind. Das CPE sperrt keine Ports zu IP-Adressen in dem Bereich, der dem Kunden zugewiesen ist.

11 Verwendung eines STUN-Servers

Basic Premium

Beim Einsatz von NAT kann es zu Problemen durch die Umsetzung der privaten auf eine öffentliche IP-Adresse kommen. Durch die Umsetzung wird dem Zielteilnehmer (In diesem Fall dem M-net Vermittlungssystem) als Source-IP-Adresse die öffentliche IP-Adresse der IP-PBX mitgeteilt und nicht die private IP-Adresse, die eigentlich als Zieladresse verwendet werden muss.

Durch die Verwendung eines STUN-Servers (Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)) kann diese Problematik umgangen werden.
Der STUN-Server ermöglicht es, dass u. a. IP-PBXen ihre öffentliche IP-Adresse und den öffentlichen internet-seitigen Port ermitteln.
Das STUN-Protokoll ist im RFC 3489 beschrieben und definiert.

Bei der Registrierung auf der Domain business.mnet-voip.de bitte den STUN Server stun.mnet-voip.de und den STUN- Standardport 3478 für UDP und TCP verwenden.

Das Erneuern der Verbindung zum STUN Server sollte alle 240 Sekunden (4 Minuten) durchgeführt werden.
Bei Verwendung eines STUN-Servers muss die IP-PBX alle 20 Sekunden ein OPTIONS-Paket an das M-net Vermittlungssystem schicken. Nur so ist gewährleistet, dass die IP-PBX erreichbar ist.

Bei der Verwendung eines STUN-Servers werden im REGISTER Request die private Source-IP-Adresse und der private Source-Port im ersten via-Header und im Contact-Header durch die öffentliche Source-IP-Adresse und den öffentlichen Source-Port ersetzt:

REGISTER sip:business.mnet-voip.de SIP/2.0	Request Line
Via: SIP/2.0/UDP **83.111.222.333:62345**;branch=z9hG4bK802d2cf8d27ce611b7e6fde19d2be330;rport From: <sip:+4989189291230@business.mnet-voip.de> To: <sip:+4989189291230@business.mnet-voip.de> Call-ID: 802D2CF8-D27C-E611-B7E4-FDE19D2BE330@83.111.222.333 CSeq: 1 REGISTER Contact: <sip:+4989189291230@**83.111.222.333:62345**>;+sip.instance="<urn:uuid:001D3E01-C415-E611-8F16-FE123456789>" Allow: INVITE, ACK, BYE, CANCEL, INFO, MESSAGE, NOTIFY, OPTIONS, REFER, UPDATE Max-Forwards: 70 Allow-Events: presence,dialog,message-summary,refer User-Agent: IP-PBX Supported: replaces, timer, from-change, gruu Expires: 3600 Content-Length: 0	Message Header (SIP)

Abbildung 14: Beispiel einer REGISTER-Request bei Verwendung eines STUN-Server

Bei einem abgehenden Gespräch wird in der ersten INVITE-Nachricht, dass von der IP-PBX gesendet wird zusätzlich die private Source IP-Adresse im SDP durch die öffentliche Source IP-Adresse ersetzt:

INVITE sip:+4989452000@business.mnet-voip.de SIP/2.0	Request Line
Via: SIP/2.0/UDP **83.111.222.333**:**62345**;branch=z9hG4bK80ec8849d47ce611b7eafde19d123330;rport From: <sip:+4989189291230@business.mnet-voip.de>;tag=1732903747 To: <sip:+4989452000@business.mnet-voip.de> Call-ID: 80EC8849-D47C-E611-B7E9-FDE19D233333@83.111.222.333 CSeq: 4 INVITE Contact: <sip:+4989189291230@**83.111.222.333**:**62345**> Content-Type: application/sdp Allow: INVITE, ACK, BYE, CANCEL, INFO, MESSAGE, NOTIFY, OPTIONS, REFER, UPDATE Max-Forwards: 70 Supported: 100rel, replaces, from-change P-Early-Media: supported User-Agent: IP-PBX P-Preferred-Identity: <sip:+4989189291230@business.mnet-voip.de> Content-Length: 179	Message Header (SIP)
v=0 o=- 19054385611 IN IP4 **83.111.222.333** s=SIPPER for PhonerLite c=IN IP4 83.111.222.333 t=0 0 m=audio 62432 RTP/AVP 8 a=rtpmap:8 PCMA/8000 a=ssrc:505132282 a=sendrecv	Message Body (SDP)

Abbildung 15: Beispiel einer INVITE-Nachricht eines bei einem abgehenden Gespräch bei Verwendung eines STUN-Servers

Detaillierte Beschreibungen zu REGISTER-Request und INVITE-Nachrichten finden Sie im Kapitel 5.2.