

## Inhoudsopgave

<i>Inhoudsopgave</i> .....	1
<i>CallVoip Telefonie - Troubleshooting</i> .....	2
<i>Algemene troubleshooting vragenlijst</i> .....	3
1. Ik kan mijn VoIP-account niet registreren .....	3
2. Heeft u de juiste gegevens in de juiste velden ingevuld? .....	3
3. Is het VoIP-apparaat goed geconfigureerd? .....	3
5. Ligt het probleem in uw netwerk?.....	4
6. Mijn VoIP-account was geregistreerd maar is dat inééns niet meer! .....	4
7. Audioprobleem: als mijn nummer wordt gebeld hoort de beller niets en uiteindelijk mijn voicemail.....	4
8. Audioprobleem: ik hoor mijn gesprekspartner niet of andersom .....	5
10. Modem, router, firewall, server: hoe bouw ik het netwerk op? .....	7
11. Mijn account is wel geregistreerd maar de verbinding valt na een enige tijd weg .....	9
12. Waar vind ik handige netwerktools om te zien wat er gebeurt? .....	9
13. Mijn account is wel geregistreerd maar de verbinding is erg slecht .....	9
14. Hoe kan een SIP-verzoek door een Stateful Firewall heenkomen?.....	10
15. Toch is op de CallVoip centrale te zien wat voor client is aangemeld en wat voor client het is.....	11
16. Heb ik iets aan STUN?.....	11
17. Kan DID / DDI ook met CallVoip? .....	11
18. Ik wil niet dat er een nummer wordt meegezonden .....	11
19. Wat betekenen de termen Attended en Unattended transfer?.....	12
20. Kan ik de voicemail-files ook ontvangen in een ander formaat dan .au? .....	12
21. Ben ik ook bandbreedte kwijt voor intern bellen?.....	12
22. Loop ik ook een veiligheidsrisico als ik VoIP gebruik? .....	13
23. Belangrijk - kwetsbaarheid van OpenSource PBX-systemen .....	14
<i>Technische achtergrond: scenario's zonder/met NAT</i> .....	15
Scenario's .....	15
Scenario 1: Callvoip-naar-Callvoip zonder NAT-router.....	16
Scenario 2: Callvoip naar ander nummer/vast zonder NAT-router.....	17
Scenario 3: Callvoip-naar-Callvoip achter NAT-router.....	18
Scenario 4: Callvoip-naar-vast of vast-naar-Callvoip.....	19

## **CallVoip Telefonie - Troubleshooting**

In deze handleiding vindt u een aantal vragen en antwoorden met betrekking tot het werkend krijgen van uw VoIP-verbinding. Om via internet te kunnen bellen is een werkende internetverbinding noodzakelijk. Ook als uw internetverbinding verder goed werkt, kan het zo zijn dat uw router bepaalde poorten blokkeert, die voor VoIP-verkeer noodzakelijk zijn. In dit document vindt u enkele suggesties.

Niet alle netwerk-apparatuur is goed instelbaar voor VoIP. Mocht blijken dat uw huidige apparatuur niet of onvoldoende presteren om VoIP te kunnen gebruiken, dan adviseren wij u graag over alternatieven.

CallVoip

Tel: 050 – 526 49 33

Mail: [callvoip@callvoip.nl](mailto:callvoip@callvoip.nl)

## Algemene troubleshooting vragenlijst

Als u problemen ondervindt met de ingebruikname van uw VoIP-accounts zullen wij u altijd vragen enkele eerste checks uit te voeren. Deze checks dienen om te bepalen waar zich het probleem bevindt.

### 1. Ik kan mijn VoIP-account niet registreren

U heeft een VoIP-apparaat, u heeft uw CallVoip Accountgegevensformulier bij de hand en u bent op de telefooncentrale ingelogd. Wat u ook doet, de VoIP-account registreert niet; het VoIP-apparaat blijft zeggen [not registered].

Enkele suggesties:

- heeft u een werkende internetverbinding?
  - probeert u toch eens uit te bellen; hoort u nog iets dat van pas komt?  
Bv.: This password is not valid > u heeft een fout password gebruikt  
Bv.: This account number is not active > uw account is mogelijk verlopen/geblokkeerd.
- Neem in dit geval contact op met CallVoip.

Als dit niet het geval is, ga dan door met de onderstaande punten.

### 2. Heeft u de juiste gegevens in de juiste velden ingevuld?

Voor het registreren van een VoIP-account in een verder VoIP-ready netwerk heeft u doorgaans slechts drie gegevens nodig. U vindt deze drie gegevens geel gemarkeerd op het CallVoip Accountgegevensformulier:

- uw gebruikersnaam (31... of 777...) – dit is tevens uw telefoonnummer
- uw SIP-wachtwoord (let op dat u het SIP-wachtwoord gebruikt)
- het SIP-serveradres: **sip.sipnl.net** of **sip.callvoip.nl**
- **belangrijk!** vermeld de sip-server ook in het veld proxyserver

### 3. Is het VoIP-apparaat goed geconfigureerd?

Een eerste check is om te controleren of u het VoIP-apparaat (FRITZ!Box, IP-telefoon, etc.) goed heeft geconfigureerd. Zie ook punt 2. Zie bijvoorbeeld de handleidingen op de CallVoip Supportpagina. Wij raden u aan om ook op de CallVoip telefooncentrale in te loggen en te kijken of u daar het blauwe bolletje ziet staan, als teken dat de account geregistreerd is.

### 4. Is het VoIP-apparaat defect?

Er bestaat een (zeer) kleine kans dat uw VoIP-apparaat (FRITZ!Box, IP-telefoon, etc.) defect is. Of een apparaat defect is kunt u bv. vaststellen als alle lampjes van het product uit zijn (voeding defect), als u niet meer kunt inloggen en als het apparaat bv. elders (in een ander netwerk) ook niet werkt.

Controleer in ieder geval:

- of het product is voorzien van een recente / de laatste firmware
- of het helpt indien u het productreset naar fabrieksinstellingen

Bij IP DECT systemen is het ook mogelijk dat een handset het contact met de basis heeft verloren. Probeer de handset dan opnieuw op de basis aan te melden. Als dit niet lukt en er brandt geen lampje op de basis, dan is mogelijk de voeding van het basisstation defect.

Als het apparaat wel werkt en aan is, maar de VoIP-account niet registreert, dan is het niet waarschijnlijk dat het apparaat defect is, maar het ligt aan de wijze waarop het apparaat op uw netwerk is aangesloten en/of aan de signalen die de router(s) in het

netwerk wel of niet doorlaten.

Probeer u dan eens:

- het apparaat op een andere plaats in het netwerk aan te sluiten
- bij voorkeur zo DICHT mogelijk achter uw ADSL- of kabelmodem

#### 5. **Ligt het probleem in uw netwerk?**

Als u heeft geverifieerd dat uw VoIP-apparatuur goed is geconfigureerd, u een werkende internetverbinding heeft, de apparatuur niet defect is, maar toch nog niet werkt met uw CallVoip-account, test dan of het apparaat in een andere plaats in uw netwerk wel goed functioneert. Zet de IP Phone bv. rechtstreeks achter uw modem/router en vermijd zo switches en bekabeling die mogelijk een probleem opleveren. Blijft het probleem, probeer dan om de IP Phone of VoIP-adaptor mee te nemen naar een andere locatie (ander netwerk, bv. thuis of juist op kantoor). Functioneert het apparaat daar wel, dan weet u dat het probleem zich ergens in uw netwerk voordoet.

**In 75% van de gevallen worden problemen veroorzaakt door de netwerkrouter.** De modem-routers van het merk/type Experiabox

(SpeedTouch/Siemens, meegeleverd door KPN), ZyXEL (meegeleverd door Telfort) en Copperjet (meegeleverd door Alice) leveren vaak problemen op. Problemen hebben vaak een adhoc karakter: het ene gesprek is er geen probleem, een volgend gesprek wel. Dit is ook verklaarbaar. Zo kan het geruime tijd goed gaan en ineens na het herstarten van uw telefoon helemaal mis zijn. Het oplossen hiervan is in veel gevallen erg lastig. Omdat uw uren en die van uw systeembeheerder kostbaar zijn, raden wij aan om met ons te overleggen wat voor ander apparaat in uw situatie goed zal werken en het ongehoorzame apparaat te vervangen.

Ons advies is in de meeste gevallen: vervanging van uw apparaat door een FRITZ!Box of DrayTek. Wij adviseren u graag verder.

#### 6. **Mijn VoIP-account was geregistreerd maar is dat inééns niet meer!**

Door uiteenlopende redenen kan een VoIP-apparaat zijn registratie met de CallVoip telefooncentrale verliezen. Redenen zijn bijvoorbeeld: een korte hic-up van de internetverbinding, onderhoud van de internetprovider (bv. op DNS-vlak), een korte stroomstoring/-piek, een probleem met één van uw netwerkapparaten (router, switch, computer), onderhoud van de telefooncentrale.

Een eerste advies dat vaak ook doeltreffend is in deze situatie, is het uit- en aanschakelen van uw VoIP-apparatuur en evt. van uw modem, router, switch, IP-telefoon. Wacht ca. 15 seconden tussen het uit- en weer aandoen.

Bv: heeft u een FRITZ!Box, en is deze inééns zijn registratie kwijt, dan wil een herstart van de FRITZ! in veel gevallen het probleem oplossen.

#### 7. **Audioprobleem: als mijn nummer wordt gebeld hoort de beller niets en uiteindelijk mijn voicemail**

Deze situatie wordt veroorzaakt doordat het grootste deel van de registratie van uw account goed verloopt, maar het transport van het signaal binnen het netwerk niet. Als u op de CallVoip Telefooncentrale inlogt, ziet u een blauw bolletje achter uw account staan. De telefooncentrale denkt dat alles in orde is en stuurt een inkomend gesprek gedurende een aantal seconden (standaard: 30 seconden) naar uw apparaat. Pas bij geen gehoor gaat het gesprek naar de voicemail. Dat verklaart de stilte voordat het gesprek doorschakelt naar voicemail of naar een follow-me regel (bv. mobiel). Het signaal van het inkomende gesprek komt bij uw netwerk aan, maar wordt daar niet goed gerouteerd. Dit veroorzaakt dat er geen telefoon overgaat, dat de beller geen overgangstonen hoort. Soms gebeurt dit ook wel, en vallen andere onderdelen van de signaalstroom weg (zie ook volgende punt).

De oorzaak is uw netwerkrouter. De oplossing moet dan ook hier worden gezocht. Pas

de configuratie aan zodat de router de signalen wel goed routeert.  
→ suggesties en tips: zie de hierna volgende punten.

#### 8. **Audioprobleem: ik hoor mijn gesprekspartner niet of andersom**

Bij een zogenaamde **one-way-audio** situatie hoort u uw gesprekspartner niet en deze u wel, of andersom. Veelal zult u uw gesprekspartner niet horen: uw firewall blokkeert het inkomende VoIP-signaal dat van buiten naar binnen gaat. Dit betekent doorgaans dat uw router moeite heeft om het audiosignaal binnen uw netwerk te transporteren. Dat is nl. een ingewikkelde klus waarvoor een reeks poorten wordt gebruikt (doorgaans UDP: 30000 – 65000).

Zie de hierna volgende punten voor algemene instructies t.a.v. het instellen van uw firewall. Het is helaas niet mogelijk om een punt-voor-punt instructie voor elk merk en type router te geven, maar wij kunnen u vaak wel alternatieve apparatuur adviseren die uw probleem gaat oplossen.

#### **Enkele suggesties:**

Het is een goed streven om ervoor te zorgen dat uw firewall niet achter een kabel- of DSL-router wordt geplaatst. Is dit niet te voorkomen, stel in deze eerste router dan een DMZ in die naar de firewall erachter verwijst. Is ook dat niet mogelijk, kijk dan of u het modem als bridge kunt instellen en laat de firewall erachter via de WAN-kant de verbinding opbouwen. Het IP-adres komt dan rechtstreeks in de firewall-router en niet in de eerste router (feitelijk passeert u de eerste router).

Sommig modem-routers, bijvoorbeeld de populaire SpeedTouch-modems, kunt u configureren als bridge (IP Spoofing).

Bij de SpeedTouches is dit geen optie in het menu, maar heeft u hiervoor de configuratietool vanaf de site nodig: (<http://www.speedtouch.nl/drivers.html>).

Behoudt u een single-audio-probleem of komen inkomende gesprekken niet door, dan is dit een blokkade van de firewall of de natting van de router.

Suggestie 1: stel in dat verkeer afkomstig van de telefooncentrale (91.195.160.x en 91.195.161.x.) altijd wordt doorgelaten

Suggestie 2: plaats uw IP-telefoon of de tweede router in uw netwerk in DMZ zodat alle verkeer van buitenaf hiernaar wordt doorgelaten en NIETS wordt geblokkeerd

Suggestie 3: als uw router kennelijk zelf niet zo goed is in het maken van de juiste NAT-routeringen, maak dan in de NAT-tabel van de router een regel aan waardoor de achterliggende VoIP-apparatuur op een aantal vaste poorten naar buiten gaat. Deze poorten kunt u middels een andere NAT-regel ook weer openstellen voor inkomend verkeer.

Heeft u een Cisco router? Probeer u dan eens de volgende configuratie:

**no ip nat service sip udp port 5060**

Een **FRITZ!Box** aan het begin van uw netwerk is doorgaans een uitstekende basis voor VoIP. Heeft u ook nog een geavanceerde firewall, dan kan de volgende opstelling u van past komen: gebruik de FRITZ! als modem-router en sluit hierop uw telefoons aan (analoog, ISDN-apparatuur en IP Phones).

Via menu [Internet] > [Port Forwarding] kunt u de instelling [Exposed Host] kiezen en alle netwerkverkeer doorsturen naar het IP-adres van uw firewall.

Indien er meerdere routers achter elkaar zijn geplaatst, en u ondervindt registratie- of single audio problemen, dan kan het gebruik van een stun-server soms resultaat bieden. Gebruik bijvoorbeeld: [stun.xten.com](http://stun.xten.com).

Single-way-audio problemen bij ZyXEL modem-routers kunnen in diverse gevallen worden opgelost op de volgende manier:

- Ga naar menu **[Netwerk]** > **[NAT]** > kies tab **[ALG]**
- Vink hier **[Enable SIP ALG]** uit en sla op.
- Test u nu of het probleem zich nog steeds voordoet.

Bij het gebruik van de X-Lite softphone kunt u single-way audio problemen proberen op te lossen als volgt:

- bel met X-Lite het nummer **\*\*\*7469** > er wordt een aparte settingspagina geopend
- zoek parameter **[honor]** en stel deze in van **[0]** naar **[1]**
- test nu of het probleem zich nog steeds voordoet.

## 9. Welke poortinstellingen zijn nodig om VoIP door de NAT-router/Firewall te laten komen?

De NAT-router / firewall moet in beginsel de poorten **30000-65000 (UDP)** toelaten om een symmetrische verbinding (= audio in twee richtingen) mogelijk te maken. Hieronder een overzicht van poorten en ranges die doorgaans door VoIP worden gebruikt. Deze ranges dienen bereikbaar te zijn voor verkeer van en naar de telefonie-servers, zowel van binnenaf (vanaf IP Phones op het lokale netwerk) als van buitenaf (inkomend verkeer). De telefonieservers bevinden zich op domein **sip.sipnl.net**, netwerk 91.195.160.0/25 en 91.195.161.0/25. De router dient het verkeer goed te routeren.

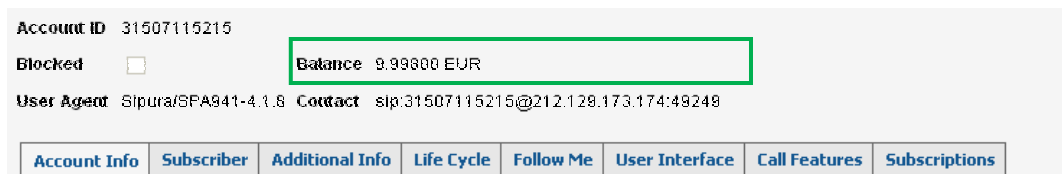
5004

5060-5069 (signaleringspoort → u ziet de registratie terug op de telefooncentrale)

10000, 16384-16482

30000-30005

35000-65000



Account ID	31507115215
Blocked	<input type="checkbox"/>
Balance	9.99800 EUR
User Agent	Sipura/SPA941-4.1.8
Contact	sip:31507115215@212.128.173.174:49248

[Account Info](#) [Subscriber](#) [Additional Info](#) [Life Cycle](#) [Follow Me](#) [User Interface](#) [Call Features](#) [Subscriptions](#)

In een lokaal netwerk kan een heel stel IP-telefoons aanwezig zijn.

De IP-telefoon registreert SIP-accounts op basis van de standaardpoort 5060. De netwerkrouter koppelt poort 5060 (registratie) voor een specifieke account aan een pseudopoort in de range 30000 t/m 65000. Zo weet de netwerkrouter welk signaal voor welke telefoon is bedoeld. Vaak ziet u het poortnummer terug in de CallVoip-telefooncentrale bij het contact-adres (loginnaam@extern-IP:poortnummer).

Als uw account geregistreerd is op uw apparatuur kunt u deze terugzien op de telefooncentrale. Hiertoe kunt u inloggen op de klantlogin, kiest u in het menu onderdeel **[Accounts]**, klikt u op **[Show accounts]**. Indien geregistreerd ziet u een blauw bolletje achter de betreffende account staan. Klik op de account door, en u ziet bij User Agent ook het merk en type apparaat vermeld staan.

Indien het u of uw systeembeheerder niet lukt om uw netwerkrouter tot orde te roepen en de routing succesvol uit te voeren, overweegt u dan de aanschaf van een router die deze mogelijkheden wel biedt. Dit kan een stuk goedkoper zijn dan doorzoeken en het probleem oplossen. Denk aan de uren van uw systeembeheerder en de frustratie van uw personeel.

Handige links:

<http://www.pc-library.com/ports/>

<http://www.chebucto.ns.ca/~rakerman/port-table.html>

#### **CallVoip adviseert het gebruik van:**

DrayTek-(modem-)routers: [http://www.tijdhof.com/index.php?manufacturers\\_id=23](http://www.tijdhof.com/index.php?manufacturers_id=23)

FRITZ!Box modem-routers: <http://www.fritzshop.nl/>

#### **10. Modem, router, firewall, server: hoe bouw ik het netwerk op?**

Het is zaak om uw VoIP-verkeer door zo weinig mogelijk zaken te laten belemmeren om daarmee uw gesprekskwaliteit te kunnen optimaliseren.

Zet uw VoIP-apparatuur daarom bij voorkeur zo DICHT mogelijk achter het kabel/ADSLodem met evt. een eenvoudige switch die de routing niet verstoort, en bij voorkeur **niet** achter een zware firewall en **niet** achter uw Windows Small Business Server of andere server met routingfunctie.

Voor de duidelijkheid: VoIP achter uw server is wel mogelijk, maar toch vaak merkbaar in termen van kwaliteit. Het goed krijgen van deze configuratie stelt meer eisen aan de vaardigheden van uw netwerkbeheerder en dit zal u in ieder geval extra werk opleveren....

Enige achtergrond: een normale FireWall die zagezegd VoIP-aware of VoIP-compatible is, zal automatisch de juiste poorten laten openen en open houden op basis van keep-alive sessies. Daarvoor hoeft u als het goed is NIETS te doen.

Als dit in een bepaalde situatie niet het geval is, zult u het apparaat even moeten helpen het gedrag aan te passen aan wat er vereist is voor VoIP. VoIP op meerdere telefoons in één netwerk is vergelijkbaar met het internetverkeer van meerdere computers in één netwerk. Als u op een computer een bepaalde website raadpleegt en daar overheen navigeert, dan is dat vergelijkbaar met een VoIP-telefoongesprek. Een verschil tussen telefoneren via internet en surfen is, dat het spraakgeluid natuurlijk zonder of met zo weinig mogelijk vertraging moet binnen komen (= realtime karakter) en dat het hier gaat om audiosignalen die door het netwerk heen moeten.

Omdat VoIP dynamisch is en dus op basis van de sessie willekeurig poorten gebruikt, is het een nachtmerrie voor ingewikkelder FireWalls. Omdat daarnaast het RTP-verkeer nogal wat eisen stelt met betrekking tot de vertraging (zo klein mogelijk), is het gebruik van een FireWall die al het verkeer via een zogenaamde "proxy" laat verlopen af te raden. Het telt immers allemaal bij elkaar op en voor je het weet is er in het gesprekspad veel vertraging, tot duidelijk merkbaar aan toe.

Deze hele combinatie aan eisen heeft ervoor gezorgd dat sommige fabrikanten ertoe zijn over gegaan om speciale VoIP-Firewall's te bouwen. Deze wordt dus parallel gezet met een bestaande FireWall, gebruikt eigen adressen en maakt dan vaak nog gebruik van een apart VLAN op het netwerk om telefoon- en dataverkeer gescheiden te houden. In deze hele combinatie wordt VoIP- en dataverkeer dus zo gescheiden mogelijk behandeld om voor beiden te kunnen voldoen aan de eisen die eraan gesteld kunnen worden. Ook kan er een tweede WAN-poort zijn om twee internetverbindingen te kunnen gebruiken.

De simpele benadering is: UDP open voor de wereld

Hiermee zou het voor iedere User Agent (VoIP-apparaat) achter de firewall dus mogelijk moeten zijn om met de buitenwereld te communiceren. Poort 5060 laat verkeer door, via poort-mappings weet de router welke User Agent welke sessie met de buitenwereld heeft en elke user agent voert zijn eigen gesprek.

Er zijn netwerk-beheerders die dit niet willen wegens mogelijke beveiligingslekken. Dit risico is minimaal omdat er weinig tot geen lekken op UDP zijn - het wordt niet gebruikt voor normaal internetverkeer.

Er is een alternatief: normaal gesproken werkt een User Agent op poort 5060. Via NAT wordt alles keurig geregeld, zodat de zogenaamde poort-mappings ervoor zorgen dat iedere User Agent kan communiceren met de buitenwereld. In de lastigere gevallen moet er dus per User Agent een set poorten gereserveerd worden om de FireWall open te houden voor het SIP-verkeer.

Bijvoorbeeld:  
5060 voor telefoon 1

Diagnostics >> NAT Sessions Table

NAT Active Sessions Table | Refresh |

Private IP :Port	#Pseudo Port	Peer IP :Port	Interface
192.168.21.64	63372	57441 83.98.222.4	5060 WAN1
192.168.21.62	56462	50019 194.120.0.198	5060 WAN1
192.168.21.111	1104	39973 72.26.207.163	80 WAN1
192.168.21.63	19632	46213 194.221.62.198	5060 WAN1
192.168.21.64	19632	46469 194.120.0.198	5060 WAN1
192.168.21.62	42708	36265 82.101.62.99	5060 WAN1
192.168.21.111	1268	40137 89.188.17.150	143 WAN1
192.168.21.4	3860	48105 192.168.22.1	53 WAN1
192.168.21.61	10998	37067 192.168.22.1	53 WAN1
192.168.21.62	65048	58605 89.188.17.150	5060 WAN1
192.168.21.64	60570	54639 83.98.222.5	5060 WAN1
192.168.21.2	123	43856 91.189.94.4	123 WAN2
192.168.21.63	40510	34323 83.98.222.4	5060 WAN1

**Bij meerdere WAN-poorten ziet u hier over welke WAN-poort het verkeer loopt.**

IP-adres v/d User Agent i/h netwerk      De pseudo-poort (soms getoond in centrale)      Poort 5060 toont VoIP-verkeer

5062 voor telefoon 2  
5064 voor telefoon 3  
etc.

Merk op dat dit in **even** getallen gaat! Poorten vanaf **10000 tot 65000** worden dan open gezet voor de wereld, teneinde het dynamische RTP-verkeer toe te laten.

TIP: diverse producten bieden de instelling [use random port]. Als deze optie wordt geboden, zet deze dan aan. Dit is o.a. het geval bij GrandStream IP Phones en Siemens IP DECT toestellen.

### 11. **Mijn account is wel geregistreerd maar de verbinding valt na een enige tijd (aantal seconden of minuten) weg**

Ook dit kan een symptoom zijn van uw router of telefonie-apparatuur die niet helemaal goed is ingesteld of is afgestemd op andere apparatuur in het netwerk (bv. VoIP-apparatuur tov router). Uw VoIP-apparaat (IP Phone, ATA, Gateway, PBX) houdt zich niet aan de regels voor het openhouden van een sessie (= gesprek) binnen NAT, of de NAT-router/firewall heeft last van misdragingen.

Veel routers/firewalls kennen een timer die na x tijd afloopt en waarbij een geopende poort weer gesloten wordt. Als deze poort dus 5060 is – waarop de communicatie met de CallVoip Telefooncentrale plaatsvindt, dan is uw apparatuur van buiten af niet meer bereikbaar.

Heel vaak is er sprake van **session timers** in de VoIP-apparatuur die keurig poort 5060 openhouden mits de timerwaarde wordt ingesteld **binnen de helft van de timer van de NAT-router/firewall**.

Advies: zorg ervoor dat de **session refresh timer** (er zijn verschillende termen in omloop) van uw VoIP-apparaat onder de helft van de **time-out** van de router wordt ingesteld (of zet hem gewoon heel laag) en stel de **session re-register** in op ca. 20-30 minuten. Dan blijft alles bereikbaar. Ook al wordt er 1 pakket verloren, het 2e pakket valt dan nog binnen de timer. Als u meerdere soorten VoIP-apparaten heeft, waarbij één apparaat het wel goed doet, en de andere niet, zoek dan hier de oorzaak.

**N.B.:** in de praktijk is middels tools als **Ethereal** en **Wireshark** aangetoond dat niet ieder apparaat ook werkelijk doet wat er geconfigureerd kan worden. De fabrikant van de apparatuur is er op aan te spreken dat het apparaat zich houdt aan de standaarden en samenwerkt met apparatuur die zich ook aan de standaarden houdt. Dit is slechts een schrale troost. Wij adviseren u graag met welke apparatuur wij goede ervaringen hebben.

### 12. **Waar vind ik handige netwerktools om te zien wat er gebeurt?**

Op de CallVoip Supportpagina vindt u een overzicht van handige tips, tools en (online) programma's om te zien wat de stand van zaken is.

Zo vind tu een overzicht van de SIP statuscodering, een online tool MyVoipSpeed om te beoordelen of uw netwerk geschikt is voor VoIP-verkeer (let op: dit is een momentopname!), online poortscanners, een apparaat waarmee u het MAC-adres van een apparaat in uw netwerk kunt opzoeken, etc.

Ook zeer handig is <http://www.wireshark.org/> (versies voor Windows, Linux'en, MacOS X etc.). Let op dat voor het monitoren van verkeer op een netwerk wel een hub of switch met monitor-poort vereist is.

### 13. **Mijn account is wel geregistreerd maar de verbinding is erg slecht**

CODEC - Controleert u of uw apparatuur met een bepaalde CODEC (codering - decodering) uw apparatuur werkt. CallVoip Telefonie werkt met codecs G.722, G.711 (G.711mu en G.711a) en G.729.

De **G.722-codec** biedt u een zeer hoge gesprekskwaliteit vergelijkbaar met MP3 files (wideband-codec). Deze codec wordt echter alleen gebruikt als uw apparatuur, de apparatuur van de andere beller en beide telefonie-netwerken dit ondersteunen. Belt u met ons, dan zult u deze kwaliteit behalen.

De **G.711-codec** biedt u een telefoongesprek op ISDN-kwaliteit. In veel gevallen is dit de hoogst haalbare geluidskwaliteit.

De **G.729-codec** biedt een lagere geluidskwaliteit, maar is minder zwaar. Bij een minder goede internetverbinding kan het gebruik van deze codec verbetering bieden.

Sommige apparatuur schakelt zelf terug van hoog naar de meest haalbare codec en daarmee geluidskwaliteit.

**BANDBREEDTE** - Vervolgens kunt u controleren of u voldoende bandbreedte tot uw beschikking heeft. Voor deze check bestaan er on-line tools: Wij adviseren u de volgende tools:

- <http://www.speedtest.nl>

Hier kunt u uitvinden hoeveel uploadsnelheid u heeft. Voor elk VoIP-gesprek adviseren wij als uitgangspunt ca. 100kB upload.

- <http://myvoipspeed.visualware.com/>

Een uitgebreide test van uw bandbreedte en de kwaliteit die u qua VoIP zou moeten kunnen behalen. Deze test eindigt met een conclusie en enkele tips.

**QUALITY OF SERVICE** - Indien u wel genoeg bandbreedte heeft, maar u houdt een slechte gesprekskwaliteit, dan is het mogelijk dat uw router de beschikbare bandbreedte niet effectief in uw netwerk verspreidt. Stel dat andere gebruikers in het netwerk zo nu en dan teveel bandbreedte gebruiken, dan kan dit een slechte gesprekskwaliteit opleveren.

De term **Quality of Service (QoS)** heeft betrekking op een intelligente routerfeature, waarmee uw router in staat is voorrang te geven aan bepaalde informatiestromen in het netwerk. Doorgaans is VoIP één van de informatiestromen in het netwerk die voorrang krijgen boven andere soorten netwerkverkeer. De andere netwerkgebruikers merken hier doorgaans nauwelijks tot niets van, de VoIP-bellers daarentegen wel! Een intelligente router met QoS biedt u de garantie dat VoIP voorrang krijgt, en daarmee een optimale gesprekskwaliteit.

Wij adviseren u een professionele netwerkrouter, bijvoorbeeld één van de DrayTek-producten, of een all-in-one VoIP-apparaat (bv. FRITZ!Box) dat zelf de verdeling van bandbreedte doet, dat weet dat er VoIP-verkeer is en dat daarmee rekening houdt (QoS).

Als u een FRITZ!Box in routermode gebruikt, bijvoorbeeld achter een kabelmodem, let dan op de instelling voor uploadsnelheid en downloadsnelheid bij de Account Information > deze staan default erg laag ingesteld.

#### 14. Hoe kan een SIP-verzoek door een Stateful Firewall heenkomen?

Een stateful firewall accepteert alleen requests van binnenuit, hoe kan een inkomend gesprek dan überhaupt worden gedetecteerd?

De SIP-User Agent (uw VoIP-apparaat) zet een sessie op met de CallVoip Telefooncentrale. Dat werkt via een proxy. Alle gesprekken lopen ook via die proxy, zodat een STUN-server en waslijsten open poorten niet nodig zijn.

M.a.w.: het VoIP-apparaat heeft op poort 5060 een sessie open met de CallVoip telefooncentrale. Een braaf VoIP-apparaat stuurt iedere x seconden (bv. 20-60 seconden) een refresh/keepalive-signaaltje naar de telefooncentrale die daarop ook braaf een antwoord geeft. De gemiddelde Firewall met Stateful Packet Inspection sluit een poort/sessie pas na inactiviteit tussen de 1 en 15 minuten, afhankelijk van hoe dit ingesteld is.

### 15. **Toch is op de CallVoip centrale te zien wat voor client is aangemeld en wat voor client het is**

Goed systeem he? Dat is het voordeel van het werken met een SIP-Server met proxy en de hele handel. Een SIP-telefoon kan dus, mits goed geconfigureerd en met DHCP in het netwerk op locatie, van netwerk naar netwerk meegenomen worden.

### 16. **Heb ik iets aan STUN?**

Een STUN-service kan een antwoord zijn, maar daar hoeft u in principe niet mee te werken. STUN is een 'lapmiddel' om een pad terug door een router te krijgen. Met STUN dienen er ook vaak ook nog in de configuratie van de router diverse poorten te worden geopend (herkomst ANY) naar het interne adres van het VoIP-apparaat. Dat is geen gaatje maken maar een gat in uw netwerk waar u kwetsbaar bent voor bv. een DoS attack. De methode met een RTP Proxy zoals CallVoip die gebruikt is veel veiliger dan STUN.

CallVoip werkt niet met STUN maar met een RTP proxy.

Het doel van de RTP proxy is om op een "slimme" manier om te gaan met VoIP-apparaten die achter NAT zitten. RTP staat voor Realtime Transport Protocol; een protocol waarmee audio en videoverkeer wordt gestreamd. Waar noodzakelijk zal de RTP via de proxy (= de externe SIP-telefooncentrale) gaan. Waar mogelijk, zal het gebruik van de proxy vermeden worden en zal het verkeer dus binnen het netwerk worden uitgevoerd. De User Agent die achter NAT zit, kan bijvoorbeeld in een scenario via de proxy werken en na het doorverbinden van een gesprek buiten de proxy om gaan en in het netwerk blijven.

### 17. **Kan DID / DDI ook met CallVoip?**

DID of DDI staat voor Direct Inward Dialing is in feite het gebruik van een nummer van één account dat wordt meegezonden als ID met een of meer andere accounts.

Binnen een blok van nummers op één klantenaccount is het mogelijk om het nummer van een andere account mee te zenden als CLI (Caller Line Identification). U kunt één nummer aanwijzen als hoofdnummer. Dit kan centraal worden ingesteld voor alle voipaccounts in één klantenaccount, maar kan ook individueel, per account.

Dit wordt ingesteld op tabblad [Call Features] > functie [Set CLI to Centrex]. Het veld [Set CLI to Account ID] dient dan op [no] te worden ingesteld. Dit kan CallVoip op uw verzoek voor u doen.

### 18. **Ik wil niet dat er een nummer wordt meegezonden - toestellen mogen niet van buitenaf direct te bellen zijn**

Door te kiezen voor accounts zonder nummer wordt dit goeddeels bereikt. Deze accounts zijn alleen te bellen vanaf CallVoip-accounts, niet vanaf bv. een KPN-nummer, een mobiel nummer of een VoIP-nummer van een andere provider. U kunt er wel gesprekken op ontvangen door een account mét nummer (wel te bellen vanaf andere nummers) door te verwijzen naar één of meerdere accounts zonder nummer.

Accounts zonder nummer kunnen wel gewoon naar buiten bellen.

De CallVoip centrale is standaard zó ingesteld dat u een individueel gesprek anoniem kunt uitvoeren, door 31 vóór het te draaien nummer in te toesten. Desgewenst kunnen we de centrale ook zó voor u instellen dat u altijd anoniem uitbelt.

**NB:** accounts zonder nummer zijn ook ideaal voor het vormen van groepsnummers (bv. huntgroups en callgroups). Zij kunnen niet van buitenaf gebeld worden en doorgaans wenst u dat ook niet.

## 19. Wat betekenen de termen **Attended** en **Unattended transfer**?

**Attended** Transfer of **warm** doorverbinden is het doorverbinden met ruggespraak. U heeft iemand aan de lijn, zet dit gesprek in de wacht en belt naar een ander nummer. U kondigt het gesprek aan en verbindt hem dan door. Niet alle apparatuur ondersteunt de functie attended transfer vlekkeloos – er moeten er als het ware twee gesprekken (call-legs) aan elkaar worden geknoopt. Niet alleen de IP Phones maar ook de router in het netwerk (en soms de switches) kunnen van invloed zijn op de mogelijkheid om door te verbinden. Wij hebben goede ervaringen met warm doorverbinden met o.a. de Linksys SPA-9xx IP Phones, Siemens IP DECT Phones. Ook de meeste FRITZ!Boxen ondersteunen extern doorverbinden (warm/koud) door een gesprekspartner in de wacht te zetten, een tweede te bellen en dan [R4] te kiezen (raadpleegt u de handleiding van de FRITZ!Box voor de exacte codes voor uw type box). Beide gesprekspartners worden met elkaar doorverbonden.

**Unattended** Transfer of **koud** doorverbinden is doorverbinden zonder ruggespraak: het gesprek wordt direct doorgeschoven naar degene waarnaar u doorverbindt. Dit is een technisch vrij een eenvoudige functie die werkt met de SIP-functie REFER.

## 20. Kan ik de voicemail-files ook ontvangen in een ander formaat dan .au?

Nee, dit is helaas niet mogelijk.

Het audioformaat .au is de standaardvorm voor geluidsbestanden van het type G.711a en G.711u (ISDN) en is één van de oudste audio-formaten die er zijn, oorspronkelijk ontwikkeld door SUN. Omdat VoIP-telefonie standaard G.711 gebruikt en de CallVoip Unified Messaging server (= voicemailserver) ook, ligt het voor de hand dat er van dit formaat gebruik gemaakt wordt. Conversie van de .au-bestanden naar andere formaten en ze dan per e-mail versturen, vereist een on-the-fly conversie voor verzending. Dit is in de huidige software niet mogelijk en stelt ook andere eisen aan de capaciteiten van de servers.

Nu is er toch hoop. Diverse smartphones spelen het .au formaat namelijk zonder problemen af (de meeste Nokia's) en voor veel andere smartphones zijn er converters beschikbaar. Nadeel is de extra actie die dit van u vereist. Ook Quicktime ondersteunt het .au-formaat. Windows Media Player echter weer niet (wel in een aantal versies). Uiteraard kunt u voicemail ook afluisteren door te bellen naar 020-7163716 en u dan te legitimeren met uw account ID (31--- of 777---) en uw password. Zie onze handleidingen voor meer details.

Meer informatie over het .au geluidsformaat: [http://en.wikipedia.org/wiki/Sun\\_Audio](http://en.wikipedia.org/wiki/Sun_Audio)  
Mogelijk alternatief – maar op uw op eigen risico!

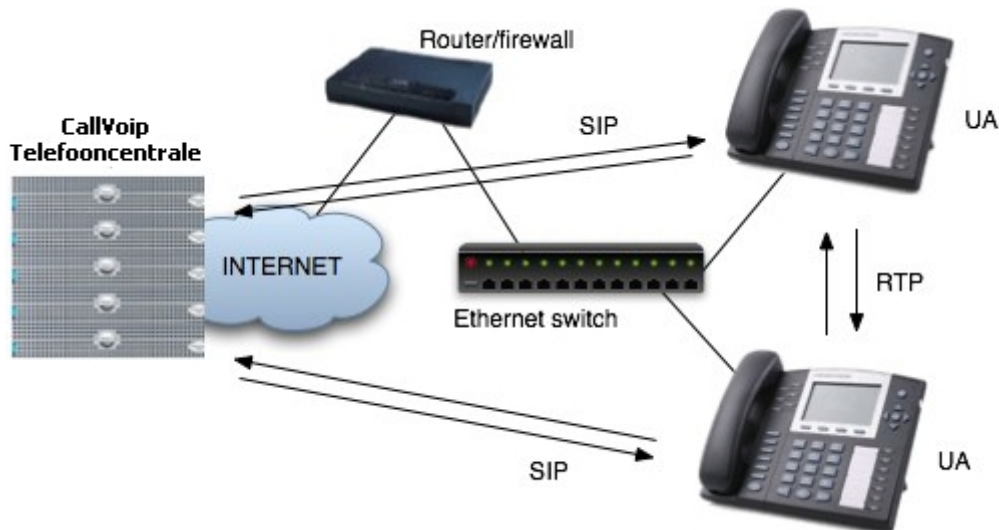
<http://www.magikinfo.com/vm2wm/default.htm> Als er ergens "bloed uit loopt". Het is iets publieks en ik weet niet of het wel 100% te vertrouwen is.

## 21. Ben ik ook bandbreedte kwijt voor intern bellen?

Als uw netwerkrouter zijn taken goed vervult en gesprekken goed routeert, dan bent u nauwelijks tot geen bandbreedte kwijt aan interne gesprekken.

CallVoip werkt met een RTP proxy. Het doel van de RTP proxy is om op een "slimme" manier om te gaan met VoIP-apparaten die achter NAT zitten. RTP staat voor Realtime Transport Protocol; een protocol waarmee audio en videoverkeer wordt gestreamd. Waar noodzakelijk zal de RTP via de proxy (= de externe SIP-telefooncentrale) gaan. Waar mogelijk, zal het gebruik van de proxy vermeden worden en zal het verkeer dus binnen het netwerk worden uitgevoerd. De User Agent die achter NAT zit, kan bijvoorbeeld in een scenario via de proxy werken en na het doorverbinden van een gesprek buiten de proxy om gaan en in het netwerk blijven.

Een voorbeeld daarvan is de RTP-mediastroom tussen twee toestellen op hetzelfde netwerk, die dus achter een NAT-router/firewall zitten. Op de CallVoip Telefooncentrale aangemeld, zal het SIP-verkeer via de SIP-server verlopen, de audio (het RTP verkeer dus) zal lokaal op het netwerk blijven. Dit is de meest effectieve methode en bovendien het meest efficiënt. Als het RTP-verkeer via de internet-verbinding wordt gerouteerd, dan bent u hier immers kostbare bandbreedte voor nodig.



#### Wat betekent dit concreet?

Stel dat van een gesprek tussen twee toestellen in één netwerk op twee bureau's tegenover elkaar alle audio via de proxy (= externe CallVoip telefooncentrale) zou verlopen. Met gebruik van de G.711a codec (ISDN) gaat er dan ruwweg 2 x 100 kb/s data upstream en dezelfde hoeveelheid dataverkeer downstream over het netwerk (= 2 audiokanalen).

Als u nu de RTP binnen het lokale netwerk blijft, is deze 200kb/s voor dit gesprek niet nodig. Als er frequent intern gebeld wordt, dan kan dit u dus een flinke hoeveelheid bandbreedte kunnen besparen!

In DrayTek routers kunt u dit terugzien in de NAT Sessions Table.

#### 22. Loop ik ook een veiligheidsrisico als ik VoIP gebruik?

Het grote voordeel van VoIP is dat het niet is gebonden aan een vaste locatie. Bij onze dienst is het gebruik van een account ook niet gebonden aan een bepaalde IP-adres. Uw VoIP-account kan dus overal ter wereld op elke internetverbinding worden gebruikt. Dit betekent dat uw VoIP-accountgegevens een open portemonnee zijn. Bescherm deze gegevens daarom goed!

Wij doen ons best om u hierbij te helpen: alleen op het CallVoip Accountgegevensformulier worden de VoIP passwords vermeld, u ziet deze ook niet terug in de telefooncentrale. Als deze dus open blijft staan, of iemand anders kan hierop inloggen, dan loopt u daardoor nog niet direct een veiligheidsrisico.

Mocht het toch gebeuren dat er onverhoopt misbruik van uw VoIP-account wordt gemaakt, dan zal de schade beperkt blijven. CallVoip monitort het gebruik en indien het gebruik opmerkelijk is (onverwacht hoog belvolume, bijzondere bestemmingen) wordt volgt een alert naar onze serviceafdeling. Deze zal u van een dergelijk alert op de hoogte brengen. Bovendien hanteren wij limieten die ervoor zorgen dat ongemerkt gebruik wordt begrensd.

Beseft u dat zowel de alerts als het aanlopen tegen een ingestelde limiet slechts

gebeuren als er reeds schade is geleden. Zonder deze mechanismen was de schade ongetwijfeld hoger uitgekomen. Tref uw voorbereidingen om deze vervelende situatie te voorkomen.

U kunt ook zelf iets doen.

- hou uw CallVoip Accountgegevens veilig en buiten bereik van onbevoegden
- meld ons diefstal van toestellen
- vraag ons passwords te wijzigen bij vertrek van een medewerker
- stel op de telefooncentrale een waarschuwinglimiet in: bij het betreffende (cumulatieve) verbelde bedrag krijgt u een notificatie per e-mail.
- bescherm uw apparatuur en netwerk goed

### 23. **Belangrijk - kwetsbaarheid van OpenSource PBX-systemen**

Gebruikt u een eigen telefooncentrale (Asterisk, Elastics, etc.) met daarop één of meer CallVoip-accounts als trunk? Weest u dan alert op een sterk toenemende trend met hack- en inbraakpogingen op OpenSource PBX-centrales zoals Asterisk. Deze trend is niet beperkt tot onze klanten, maar doet zich wereldwijd voor als randeffect van het wereldwijd toenemende gebruik van Voice over IP.

De hack begint doorgaans met het doen van belpogingen vanuit 'het Internet'. Als dat door de asterisk als 'mogelijk relevante' invite in processing wordt genomen kan e.e.a. gaan rollen. Het begint met het zetten van access-lists op de asterisk server. De meeste Linux servers hebben iptables aan boord, waarmee je een verdraaid sterke firewall kunt bouwen. Het komt erop neer dat een asterisk server van niemand een Invite toestaat, behalve van CallVoip. Dan heb je het OS van de asterisk server aangepakt, de volgende stap is iets vergelijkbaars doen in het asterisk dialplan, waarbij alleen maar calls afkomstig van de trunk (lees de CallVoip sip server) verder het dialplan in mogen. Extension 's' als ingang gebruiken naar het dialplan is gevaarlijk.

Dit vereist toch wel wat kennis van zowel Linux als asterisk.

Ontbreekt deze kennis, dan is het aan te raden gebruik te gaan maken van een firewall, zoals bijvoorbeeld Astaro appliances.

Test uw firewall met bijvoorbeeld de firewall tester op [www.grc.com](http://www.grc.com) (Shields Up).

Het meest opvallende symptoom is dat er onverwacht veel verkeer wordt gestuurd naar regio's als Noord-Korea, Somalië, Letland, Litouwen, Cuba, Eritrea en overige minder courante bestemmingen. Vaak is de misbruik terug te voeren tot het niet beheersen van algemene systeem beveiligingsprincipes. In sommige gevallen een gat in het dialplan, en in een enkel geval een hack in de webserver 'die ernaast staat' waardoor toestellen aan de binnenkant zijn gekraakt vanwege zwakke wachtwoorden.

Wij brengen hierbij graag dringend onder uw aandacht dat Open Source PBX'en van huis uit kwetsbaar zijn, en dat speciale aandacht moet worden geschonken aan de beveiliging op netwerk-, (operating)systeem en dial-plan niveau.

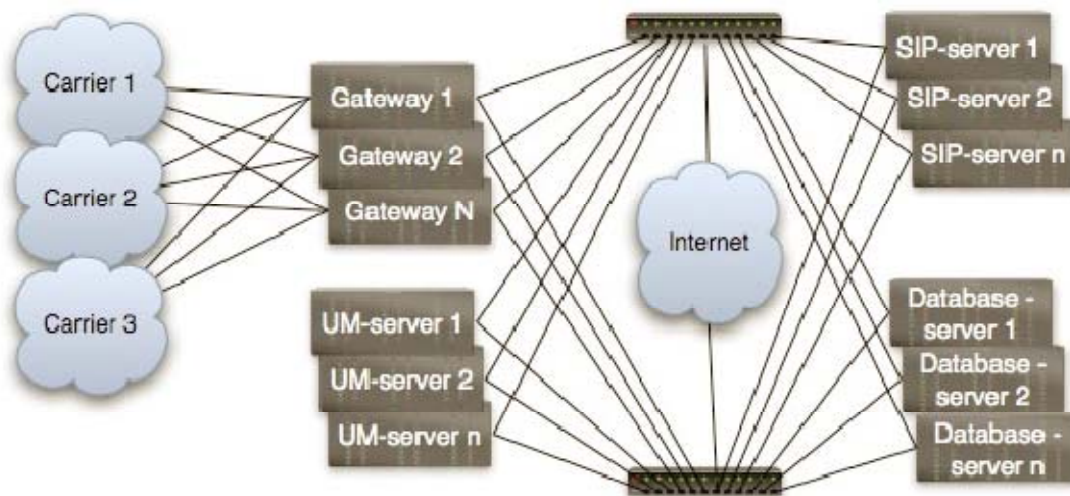
Waarschuwingssystemen en andersoortige vangnetten moeten evenwel gezien worden als last resort: als die functies worden geactiveerd, is er aan de voorkant al teveel verkeerd gegaan.

Wij raden u met klem aan om extra aandacht te besteden aan de beveiliging van uw netwerken en systemen, maar ook te bezien hoe deze omgevingen in te richten zijn ter zake van rapportage en alarmering naar uw systeem beheerder.

## Technische achtergrond: scenario's zonder/met NAT

Regelmatig krijgen wij vragen over problemen met VoIP-gesprekken, waarbij een van beide zijden de ander niet kan horen. Het doel van dit hoofdstuk is duidelijk te maken hoe de diverse call-scenario's in elkaar zitten om zodoende u wat meer hou-vast te geven om de oorzaak vna het probleem te vinden. Gebruik hierbij de informatie uit de vragen en antwoorden uit het eerste deel van deze handleidign. Dit zal uw zoektocht naar de oorzaak vereenvoudigen en u helpen uw VoIP- en netwerkapparatuur zó te configureren dat alles conform uw wensen functioneert.

De CallVoip Telefooncentrale is opgebouwd met meerdere telefooncentrales om meerdere locaties, die allemaal dubbel zijn aangesloten. Deze opzet dient een maximale beschikbaarheid te realiseren.



### Scenario's

CallVoip Telefonie werkt met het SIP-protocol als basis voor haar VoIP-diensten. Eén van de eigenschappen van het SIP-protocol is dat twee apparaten direct met elkaar verbinding kunnen krijgen. Er wordt een media-stream tussen beide apparaten opgebouwd. Dit kan echter problemen opleveren wanneer één of meer van de apparaten achter een zogenaamde **NAT-firewall** zit.

la dat het geval, dan moet er actie worden ondernomen om de audio van het éne VoIP-apparaat naar het andere VoIP-apparaat te krijgen.

### Scenario 1: Callvoip-naar-Callvoip zonder NAT-router

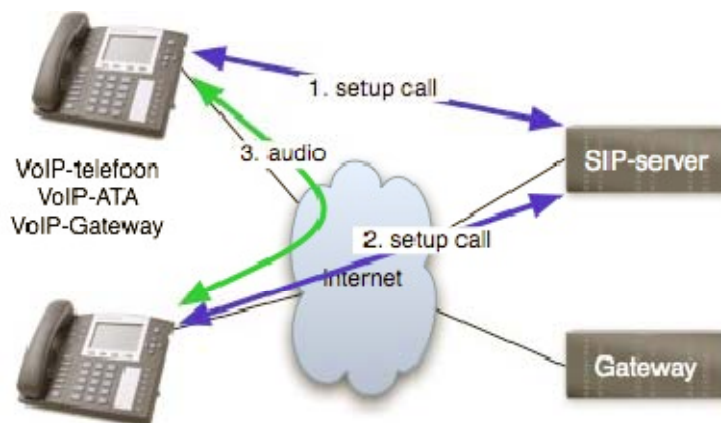
Alle VoIP-apparatuur heeft een publiek IP-adres. Deze situatie is bijvoorbeeld van toepassing als er meerdere publieke IP-adressen zijn die aan afzonderlijke apparaten in het netwerk zijn toegekend.

Vaker echter zal sprake zijn van één netwerk waarbinnen geen NAT-router actief is (alleen verkeer vanaf buiten). Deze situatie is dus ook van toepassing op intern bellen van Callvoip naar Callvoip.

Bij het opzetten en voeren van een telefoongesprek worden de volgende stappen doorlopen:

1. call setup: u draait een nummer.  
Het VoIP-apparaat meldt zich zelf aan bij de SIP-server (telefooncentrale)
2. vervolgens zoekt de SIP-server (telefooncentrale) verbinding met het nummer (een andere CallVoip-account) waarmee een gesprek moet worden opgezet en legt de verbinding (call-setup)
3. de SIP-server maakt dat de VoIP-apparaten met publieke IP-adressen elkaar kunnen vinden. Vervolgens wordt er rechtstreeks tussen de apapraten een audio-stream opgezet (dus niet via SIP-server)
4. NB: de VoIP-apparatuur kan zó worden ingesteld dat er gebruik gemaakt moet worden van een proxy-server. De SIP-server en de proxy-server kunnen hetzelfde apparaat zijn.

### Wat kan er fout gaan?



Instellingen in de VoIP-apparatuur kunnen zó zijn, dat gebruik van de Proxy geforceerd wordt door het éne apparaat, maar niet door het andere. Als dan de software van het éne danwel het andere apparaat hier niet mee omgaat conform de RFC (= een branchbrede afspraak hoe te handelen) werkt de verbinding niet of niet goed.

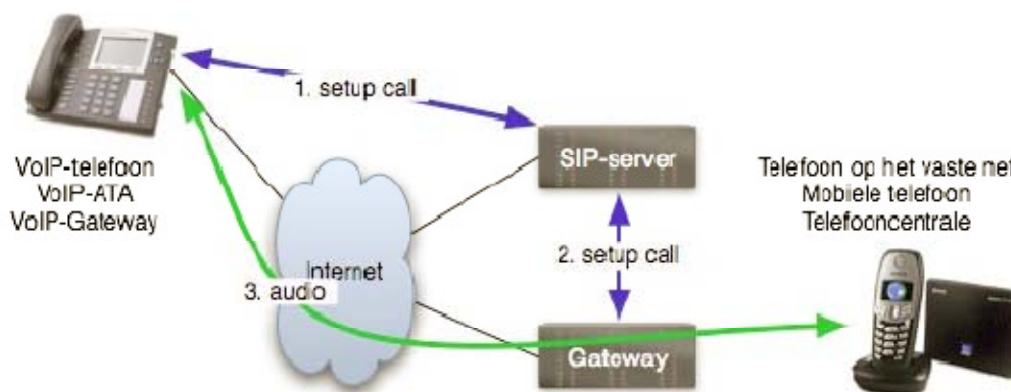
### Scenario 2: Callvoip naar ander nummer/vast zonder NAT-router

Alle VoIP-apparatuur heeft een publiek IP-adres. Deze situatie is bijvoorbeeld van toepassing als er meerdere publieke IP-adressen zijn die aan afzonderlijke apparaten in het netwerk zijn toegekend.

Vaker echter zal sprake zijn van één netwerk waarbinnen geen NAT-router actief is (alleen verkeer vanaf buiten). Deze situatie is dus ook van toepassing op intern bellen van Callvoip naar Callvoip.

Bij het opzetten en voeren van een gesprek worden de volgende stappen doorlopen:

1. call setup: u draait een nummer.  
Het VoIP-apparaat meldt zich zelf aan bij de SIP-server (telefooncentrale)
2. vervolgens zoekt de SIP-server (telefooncentrale) verbinding met het nummer waarmee een gesprek moet worden opgezet. Als dit geen CallVoip-account is maakt de telefooncentrale verbinding met de gateway en daar contact met het netwerk waar het nummer van de persoon die u wilt bellen op geregistreerd staat (bv. KPN of mobiel)
3. de VoIP-apparatuur vindt via de SIP-server en de gateway de weg naar het publieke IP-adres van de doel-telefoon. Vervolgens wordt de audio-stream direct tussen de VoIP-apparaten verstuurd, zonder tussenkomst van de SIP-server.



### Wat kan er fout gaan?

Eigenlijk hetzelfde als het voorgaande scenario. Het gaat om instellingen en het volgen van de standaarden.

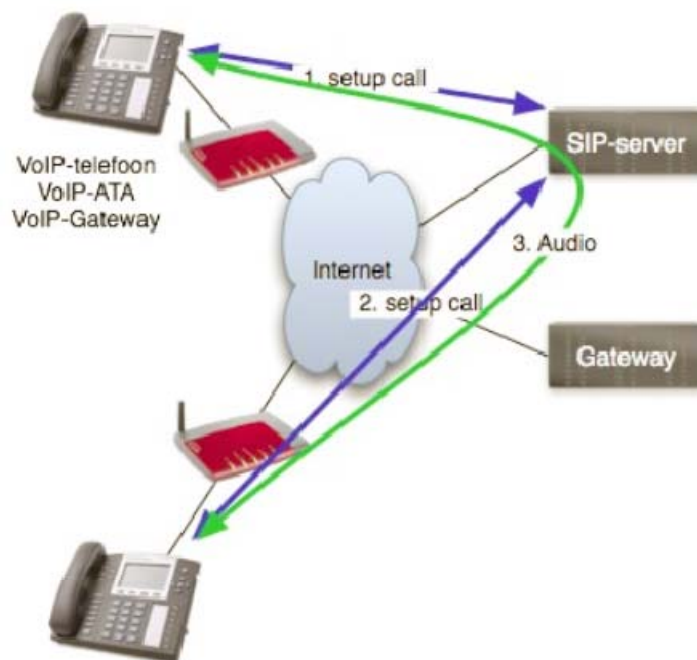
### Scenario 3: Callvoip-naar-Callvoip achter NAT-router

Alle uw VoIP-apparatuur is via een NAT router verbonden met het internet (vaak een gecombineerde modem-router-firewal met NAT-routing). Een FRITZ!Box of een DrayTek zijn voorbeelden van NAT-routers. De VoIP-apparaten hebben in dit geval geen eigen publiek IP-adres. Bij het opzetten en voeren van een gesprek worden de volgende stappen doorlopen:

1. call setup: u draait een nummer. Het VoIP-apparaat meldt zich zelf aan bij de SIP-server (telefooncentrale)
2. vervolgens zoekt de SIP-server (telefooncentrale) verbinding met het nummer waarmee een gesprek moet worden opgezet. Als dit een CallVoip-account is vindt de SIP-server dit nummer op de eigen server.
3. De VoIP-apparatuur 'weet' dat ze achter een NAT-router zit en de CallVoip SIP-server/proxy weet dat ook. De audio-stream verloopt dan via de SIP-server (telefooncentrale), en in dit geval dus niet rechtstreeks tussen de twee VoIP-apparaten.

### Waarom verloopt het gesprek via de SIP-server?

Omdat de NAT-router / firewall niet weet waar de audio van het telefoongesprek vandaan gaat komen, behalve dat dit van de SIP-server (telefooncentrale) komt. De SIP-server speelt daarom intermediair in het gesprek. Dit mechanisme zorgt ervoor dat ook bij moeilijker werkende NAT-routers / firewalls er telefoonverkeer mogelijk is. De VoIP-apparatuur praat dus voor alles direct met de SIP-server (telefooncentrale).



### Wat kan er fout gaan?

Eén van de VoIP-apparaten en/of de NAT-routers / firewalls meldt zich niet aan conform de RFC's, waardoor de CallVoip Telefooncentrale niet ziet dat de account achter een NAT-router zit. Eén van de VoIP-apparaten kan de audio-stream dan rechtstreeks versturen naar het externe IP-adres van de andere partij. De NAT-router / firewall ziet verkeer aankomen vanaf een verkeerd adres en blokkeert dit.

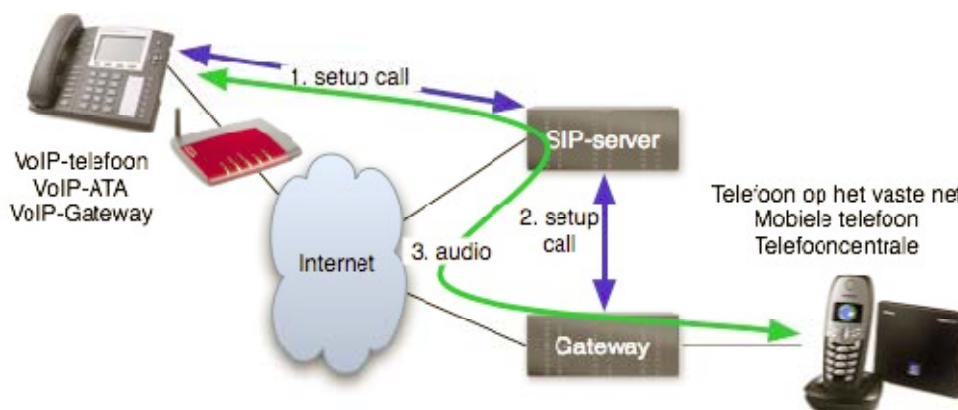
#### Scenario 4: Callvoip-naar-vast of vast-naar-Callvoip

Alle uw VoIP-apparatuur is via een NAT router verbonden met het internet (vaak een gecombineerde modem-router-firewal met NAT-routing). Een FRITZ!Box of een DrayTek zijn voorbeelden van NAT-routers. De VoIP-apparaten hebben in dit geval geen eigen publiek IP-adres. Bij het opzetten en voeren van een gesprek worden de volgende stappen doorlopen:

1. call setup: u draait een nummer. Het VoIP-apparaat meldt zich zelf aan bij de SIP-server (telefooncentrale)
2. vervolgens zoekt de SIP-server (telefooncentrale) verbinding met het nummer waarmee een gesprek moet worden opgezet. Als dit geen CallVoip-account is maakt de telefooncentrale verbinding met de gateway en daar contact met het netwerk waar het nummer van de persoon die u wilt bellen op geregistreerd staat (bv. KPN of mobiel)
3. De VoIP-apparatuur 'weet' dat ze achter een NAT-router zit en de CallVoip SIP-server/proxy weet dat ook. De audio-stream verloopt dan via de telefooncentrale SIP-server, en in dit geval dus niet rechtstreeks tussen de twee VoIP-apparaten.

#### Waarom verloopt het gesprek via de SIP-server?

Omdat de NAT-router / firewall niet weet waar de audio van het telefoongesprek vandaan gaat komen, behalve dat dit van de SIP-server (telefooncentrale) komt. De SIP-server speelt daarom intermediair in het gesprek. Dit mechanisme zorgt ervoor dat ook bij moeilijker werkende NAT-routers / firewalls er telefoonverkeer mogelijk is. De VoIP-apparatuur praat dus voor alles direct met de SIP-server (telefooncentrale).



#### Wat kan er fout gaan?

Eén van de VoIP-apparaten en/of de NAT-routers / firewalls meldt zich niet aan conform de RFC's aan, waardoor de CallVoip Telefooncentrale niet ziet dat de account achter een NAT-router zit.

Een inkomend gesprek vanaf het vaste net wil bijvoorbeeld de audio-stream rechtstreeks van de gateway naar het externe adres van de te bellen partij doorzetten. Eén van de VoIP-apparaten kan de audio-stream dan rechtstreeks versturen naar het externe IP-adres van de andere partij. De NAT-router / firewall ziet verkeer aankomen vanaf een verkeerd (niet-toegelaten) adres en blokkeert dit. Van de VoIP-apparatuur naar de gateway (= uitbellen) komt de audio-stream doorgaans **wel** aan omdat het initiatief van **binnen naar buiten** is – en dat wordt door de NAT-router wel toegestaan.