

Installationshinweise und Konfigurationshilfe

1 Einleitung

Dieses Dokument soll Ihnen dabei helfen, jegliche SIP-fähige Hard- oder Software für die Nutzung mit ecotel sipTrunk DDI (SIP-Trunk mit SIP-DDI-Protokoll für TK-Anlagen) einzurichten und bestmöglich zu konfigurieren.

2 Konfiguration der SIP-fähigen Hard- oder Software bei SIP-Registrierung

Um über ecotel sipTrunk DDI telefonieren zu können, sind in der Konfigurationsoberfläche der Geräte, Telefonanlagen oder der Telefoniesoftware in der Regel folgende Parameter einzustellen:

1.1 SIP-Username

Der „SIP-Username“ entspricht dem im ecotel Willkommensschreiben mitgeteilten „SIP-Login-Namen“ und somit den Rumpfnummern der einzelnen Rufnummernblöcke - auch inkl. Vorwahl. Bitte verwenden Sie keine Trennstriche wie Leerzeichen, Schrägstrich „/“ oder Bindestrich „-“, da diese nicht Bestandteil des Login-Namens sind.

1.2 SIP-Passwort

Das „SIP-Passwort“ entspricht dem SIP-Login-Passwort gemäß ecotel Willkommensschreiben.

1.3 SIP-Server / SIP-Registrierer

Der SIP-Server bzw. -Registrierer lautet **sipddi.ecotel.biz**

Wichtige Bemerkungen: die IP-Adresse des für die Internettelefonie zuständigen Servers sipddi.ecotel.de kann sich von Zeit zu Zeit ändern. Solche Änderungen werden keine bestehenden Verbindungen unterbrechen.

1.4 Media-Portbereich

Hier wird der SIP-Portbereich für Media von **20000 bis 59999** angegeben.

1.5 Standard-SIP-Port

Standardmäßig wird hier der bekannte **SIP-Port 5060** eingetragen. Falls gewünscht, kann hier jedoch auch ein anderer Port verwendet werden.

1.6 STUN-Server

Dieser optionale Parameter sollte **keinen Eintrag** erhalten, weil bei den SIP-basierten Produkten von ecotel kein STUN-Server zu Einsatz kommt. Bei einigen Geräten wird auch nach „NAT Traversal“ gefragt, was mit „No“ beantwortet werden sollte.

3 NAT Expire Timer bzw. Session Expire Timer

Falls ein „NAT Expire Timer“ bzw. „Session Expire Timer“ eingestellt werden kann, sollte dieser höher als der „SIP Expire Timer“ eingestellt sein, damit die NAT-Funktion nicht die SIP-Session unterbindet. Ein guter Standardwert ist hier 30 Sekunden.

4 NAT ALG

Einige Router besitzen ein NAT- bzw. SIP-ALG (Application Level Gateway). Aufgrund der SBC-Infrastruktur sollte man aber nach Möglichkeit auf einen NAT- bzw. SIP-ALG verzichten, damit die SIP-Nachrichten möglichst unverfälscht übertragen werden.

5 SIP-Proxy oder Proxy-Server

Der Eintrag des SIP-Proxy, auch Proxy-Server genannt, kann in Einzelfällen zu Problemen führen, deshalb sollte dieses Feld grundsätzlich **frei bleiben**. Der Proxy-Server ist identisch mit dem SIP-Registrierer. Bei einigen Geräten (z. B. Auerswald-TK-Anlagen) kann es erforderlich sein, bei „Outbound-Proxy“ ebenfalls den SIP-Registrierer einzutragen.

6 SIP-URI

Falls dieser Wert abgefragt wird, ist hier <Rufnummer inkl. Vorwahl>@sipddi.ecotel.de einzutragen. Dies ist auch einzutragen, wenn das Gerät (z. B. Nokia E65) diesen Parameter „Öff. Benutzernamen“ nennt.

7 Domain

Bei einigen Geräten (z. B. Auerswald-TK-Anlagen) wird auch nach einer „Domain“ gefragt. Hier wird der SIP-Registrierer eingetragen.

8 Firewall-Einstellungen

Falls Sie eine Firewall im Datenpfad verwenden ist u. a. dies zu beachten:

- Sie brauchen die SIP-relevanten Sessions nur von „Innen nach Außen“ zu öffnen, da zu Beginn Ihr User Agent Client (UAC, dies ist das VoIP-Telefon bzw. die TK-Anlage) mit seiner SIP-Registrierung die SIP-Session von „Innen nach Außen“ startet.
- Statt einer festen Einzel-IP-Adresse zum SBC sind in der Firewall-Policy die IP-Subnetze **213.148.136.0/24** und **213.148.137.0/24** zu hinterlegen, in welchen die IP-Adressen der notwendigen VoIP-relevanten Komponenten angesiedelt sind, also auch die der SBCs.

9 Hinweise für redundanten TK-Anlagenaufbau

Bei sipTrunk DDI können Sie Kunden- bzw. TK-Anlagen-seitige Redundanz wie folgt erreichen:

Im Normalbetrieb registriert sich die primäre TK-Anlage mit dem oder den SIP-Accounts beim QSC-SIP-Proxy und bewirkt damit, dass sie alle Verbindungen bzw. Rufnummern übernimmt.

Fällt die primäre TK-Anlage aus, kann sich eine sekundäre TK-Anlage mit dem oder den SIP-Accounts beim QSC-SIP-Proxy registrieren und so bewirken, dass sie alle Verbindungen bzw. Rufnummern übernimmt. Um diese Entscheidung zu treffen, „überwacht“ typischerweise die sekundäre TK-Anlage die primäre auf Funktionsfähigkeit.

Ist die primäre TK-Anlage wieder funktional, kann sie wiederum durch SIP-Registrierung den SIP-Trunk zurück-übernehmen.

Hier gilt: die letzte SIP-Registrierung gilt.

10 Empfohlene IP-Topologie

Gemäß der Vorgaben des TK-Anlagenherstellers und der Möglichkeiten der eingesetzten Provider-SBCs – insbesondere der Vorgabe, dass die Kunden-TK-Anlage eine feste öffentliche IP-Adresse zum SIP-Trunk besitzen muss und kein NAT bzw. kein ALG im Übertragungspfad eingesetzt werden darf – ergeben sich einige Implikationen auf die IP-WAN-Anbindung.

Nachfolgend wird ein Beispiel für eine sinnvolle IP-Topologie in Verbindung mit einem **Internet-Uplink** und einer Server- bzw. PC-basierten Kunden-TK-Anlage dargestellt. Kern der IP-Topologie ist, dass der Server der Kunden-TK-Anlage einen internen NIC (Network Interface Controller) zur Verbindung mit dem internen LAN und einen externen NIC zur Verbindung mit dem WAN besitzt. Letzterer wird am Besten mit der DMZ (Demilitarized Zone) der Firewall verbunden und kann hier eine feste, öffentliche IP-Adresse erhalten. Vom externen Netzwerkinterface der TK-Anlage (siehe NIC1 in nachfolgendem Bild) bis zum SBC darf **kein NAT- und keine ALG-Funktion** auftreten und die o. g. Ports sind freizuschalten. Da sich die SBC in zwei definierten IP-Subnetzen befinden (213.148.136.0/24 und 213.148.137.0/24), kann die Firewall gegebenenfalls so konfiguriert werden, dass die SIP-Signalisierung und -Mediadaten nur zu diesen Subnetzen zugelassen werden.

Hinweis: falls der TK-Anlagen-Server Windows-Server-basiert ist, sollte eine statische IP-Route zu den beiden QSC-IP-Subnetzen über den externen NIC des Servers gesetzt werden: Mit dem Befehl „route“ sollten zwei zusätzliche Netzwerkrouting-Tabelleneinträge erzeugt werden. Beispiel gemäß **Fehler! Verweisquelle konnte nicht gefunden werden.**:

```
route ADD 213.148.136.0 MASK 255.255.255.0 212.202.80.131 IF 1
```

```
route ADD 213.148.137.0 MASK 255.255.255.0 212.202.80.131 IF 1
```

Sofern Sie den Einsatz eines IP-VPN-Uplinks für den TK-Anlagen-Server bzw. Ihren Standort planen, wenden Sie sich bitte zur IP-Topologieplanung an einen Technical Consultant der ecotel.

11 Konfigurationsbeispiel eines ATAs für den Faxbetrieb

Nachfolgend wird die Initialisierungs-Datei eines AudioCodes ATA (Analoger Telefonie Adapter) des Typs MP-112 zum Betrieb von analogen Faxgeräten an den a/b-Schnittstellen wiedergegeben.

Bitte die u. g. Accounts „Account 1“, „Passwort 1“ sowie „Account 2“, „Passwort 2“ durch die richtigen Daten ersetzen: „Account“ ist der jeweilige „SIP-Login-Name“, wie weiter oben beschrieben und „Passwort“ ist das Passwort, dass Sie selbst in der MyQSC-Konsole für diesen Account vergeben haben.

```
; 21/08/2009 cro: Änderung 'ISFAXUSED = 3'  
; Standardkonfiguration 12/09/2008 apfe  
; Dieses sind die Defaulteinstellungen, die in der Regel funktionieren sollten  
; Modell: MP-112 FXS  
; Firmware: 5.40A.021.006 (Datei MP118_SIP_F5.40A.021.006.cmp)  
; Firmware Update, Konfigurationsupload und Konfiguration des Kennwortes  
; erfolgen über das Webinterface!  
; Zugriff via http://10.1.10.10  
; bitte den folgenden Default-Web-Login des ATAs ändern:  
; Benutzername: Admin  
; Kennwort....: Admin  
; z. B. auf:  
; Benutzername: qscadmin  
; Kennwort....: 63176141  
;  
; $cct:DeviceType=AudioCodes$  
; $cct:FirmwareFilename=MP118_SIP_F5.40A.021.006.cmp$  
; $cct:ConfigFilename=atacfg.ini$
```

```
[SYSTEM Params]  
DHCPEnable = 1  
NTPServerIP = 192.53.103.108  
NTPServerUTCOffset = 0  
NTPUpdateInterval = 86400  
SyslogServerIP =  
EnableSyslog = 0
```



```
GWDEBUGLEVEL = 5
ENABLEEARLYMEDIA = 1
PROXYNAME = 'sip.qsc.de'
USERNAME = 'Account 1'
PASSWORD = 'Passwort 1'
T38USERTPPORT = 1
ISFAXUSED = 3
HOLDFORMAT = 1
FAXCNGMODE = 1

[VXML Params]

[IPsec Params]

[Audio Staging Params]
DisableSNMP = 1
SNMPManagerIsUsed_0 = 1
SNMPManagerIsUsed_1 = 0
SNMPManagerIsUsed_2 = 0
SNMPManagerIsUsed_3 = 0
SNMPManagerIsUsed_4 = 0
SNMPManagerTableIP_0 = 0.0.0.0
SNMPManagerTableIP_1 = 0.0.0.0
SNMPManagerTableIP_2 = 0.0.0.0
SNMPManagerTableIP_3 = 0.0.0.0
SNMPManagerTableIP_4 = 0.0.0.0

; *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts

; *** TABLE CoderName ***

[ CoderName ]
FORMAT CoderName_Index = CoderName_Type, CoderName_PacketInterval, CoderName_rate, CoderName_PayloadType, CoderName_Sce;
CoderName 0 = g711Alaw64k, 20, 10, 255, 0;
CoderName 1 = g711Ulaw64k, 20, 0, 255, 0;
CoderName 2 = g729, 20, 0, 18, 0;

[ \CoderName ]

; *** TABLE TrunkGroup ***

[ TrunkGroup ]
FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum, TrunkGroup_FirstTrunkId, TrunkGroup_FirstBChannel,
TrunkGroup_LastBChannel, TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId, TrunkGroup_LastTrunkId, TrunkGroup_Module;
TrunkGroup 0 = 0, 255, 1, 1, Account 1, 0, 255, 0;
TrunkGroup 1 = 0, 255, 2, 2, Account 2, 0, 255, 0;

[ \TrunkGroup ]

; *** TABLE ProxyIp ***

[ ProxyIp ]
FORMAT ProxyIp_Index = ProxyIp_IpAddress;
ProxyIp 0 = sip.qsc.de ;
```

```
[ \ProxyIp ]

; *** TABLE TxDtmfOption ***

[ TxDtmfOption ]
FORMAT TxDtmfOption_Index = TxDtmfOption_Type;
TxDtmfOption 0 = 4;

[ \TxDtmfOption ]

; *** TABLE Authentication ***

[ Authentication ]
FORMAT Authentication_Index = Authentication_UserId, Authentication_UserPassword;
Authentication 0 = Account 1, Passwort 1;
Authentication 1 = Account 2, Passwort 2;

[ \Authentication ]
```

12 QoS

Sofern auf den Datenverbindungen von Ihren VoIP-Telefonen bzw. Ihrer VoIP-TK-Anlage zum NGN der QoS neben den VoIP-Daten auch „konkurrierende“ Computer-Daten übertragen werden, sind die VoIP-Daten auf diesen Datenverbindungen lückenlos (also auch z. B. im LAN) mit geeigneten Quality of Service-Mechanismen zu priorisieren.

Wegen der Vielfältigkeit dieses Themas, sind hier nur stichwortartige Hinweise aufgelistet:

- Besonders an Stellen des Netzwerkes, bei denen ein Bandbreitensprung vorliegt, ist ein QoS-Mechanismus zu implementieren. Im typischen Fall liegt so ein Sprung besonders bei der Standortanbindung (Internet- oder VPN-Uplink) vor.
- Netzbasierte, bidirektional wirkende QoS-Mechanismen sind hier den rein CPE-basierten vorzuziehen
- Im Fall einer ecotel Datenanbindung ist die „Dienstpriorisierung (QoS) Voice“ zu bestellen, die bidirektional die Voice-Daten von/zum ecotel-NGN priorisiert. Das Merkmal ist bereits auf vielen ecotel Datenanbindungen bestellbar (ecotel ethernet access, ecotel ethernet.VPN line, sowie »onnet« auf pure adsl und business shdsl, ethernet.VPN adsl und ethernet.VPN shdsl).
- Wird priorisiert, ist zu beachten, dass die VoIP-UACs (z. B. VoIP-Telefone oder die VoIP-TK-Anlage) die VoIP-Mediatdaten und die VoIP-Signalisierungsdaten mit den erforderlichen Markierungen versehen und keine Netzwerkkomponente diese Werte zurücksetzt.

Druckfehler / Irrtümer / technische Änderungen vorbehalten. Alle Rechte an dieser Dokumentation, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, verbleiben bei ecotel. – Stand Februar 2015 – Version 1.1
Kein Teil der Dokumentation darf in irgendeiner Form ohne vorherige schriftliche Zustimmung der ecotel communication ag reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

ecotel communication ag, Prinzenallee 11, D-40549 Düsseldorf
Tel.: +49 (0) 211 55 007 0, Fax +49 (0) 211 55 007 222
www.ecotel.de