

Ersetzen eines S2M/S0 Anschlusses durch einen verschlüsselten VoIP Trunk mit einem innovaphone Gateway

77. DFN Betriebstagung | 19.10.2022

S. Crump, DFN Nutzer



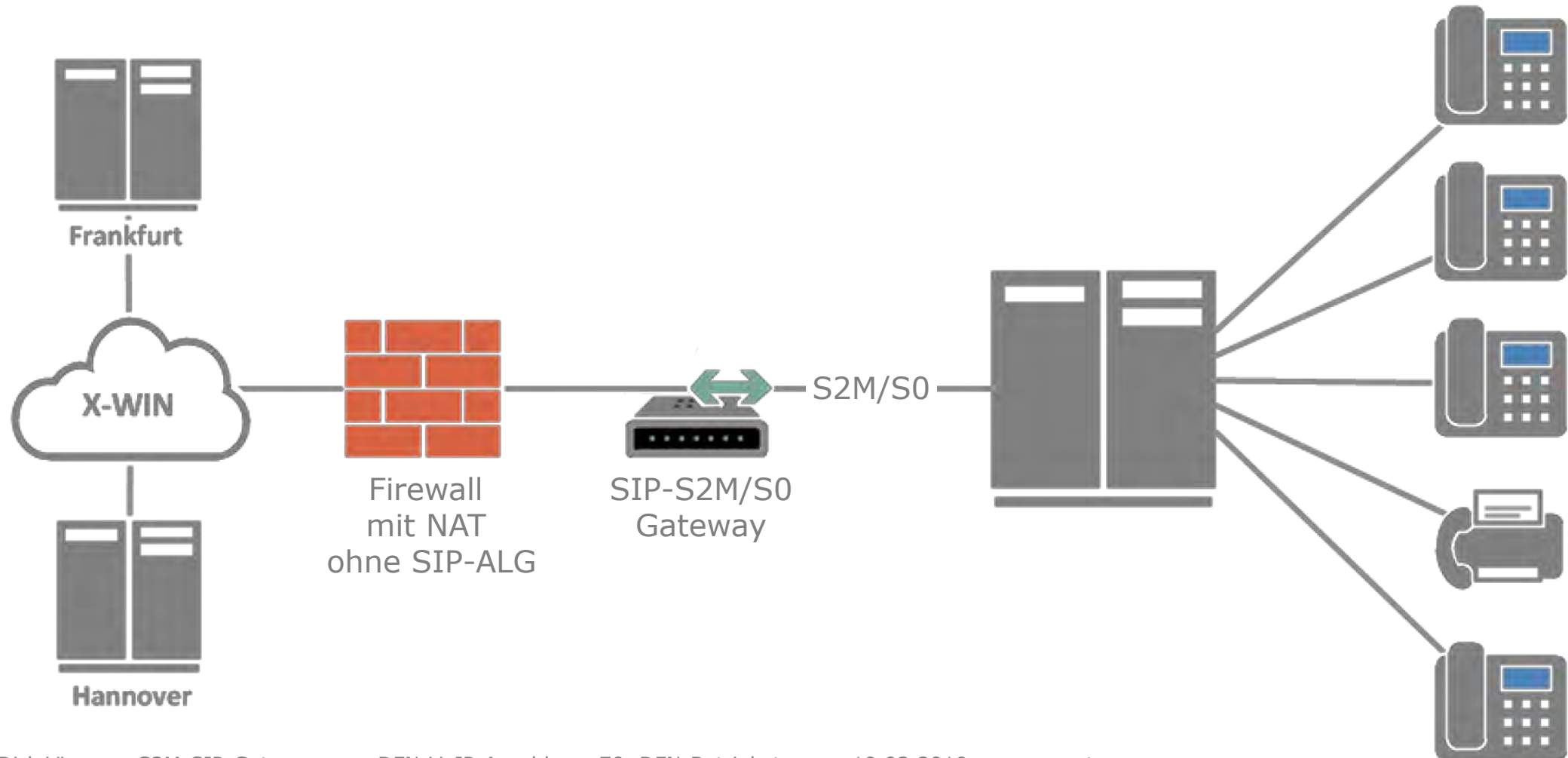
Warum ein SIP-S2M/S0 Gateway?

- ▶ **Vorhandene OpenScape 2-Draht TK Anlage** robust und ausreichend
- ▶ Weitestgehende **Trennung von TK und IT erwünscht**
- ▶ **Kostengünstiger und nachhaltiger** gegenüber einem Ersatz der vorhandenen Infrastruktur durch eine neue originäre VoIP Infrastruktur

Interne Basisanforderungen

- ▶ **Firewall mit NAT vor SIP-S2M/S0 Gateway**
- ▶ Aktuelle **Verschlüsselung mit TLS/sRTP**
- ▶ Fax, Frankit und Wählgeräte (D-/B-Kanal, DTMF) müssen weiter funktionieren

Aufbau



Quelle: Dirk Vieregg, S2M-SIP-Gateways am DFN-VoIP-Anschluss, 70. DFN-Betriebstagung 19.03.2019 - angepasst

Ablauf der VoIP Umstellung

- ▶ **15.02.2021:** **Anbieter kündigt die vorhandenen ISDN Anschlüsse**
 - ▶ 29.03.2021: Auftrag für **ersten verschlüsselten SIP-Trunk**
 - ▶ 12.04.2021: Bereitstellung Testnummern erster Trunk
 - ▶ 01.06.2021: Beginn der Inbetriebnahme des IP811 Gateways
 - ▶ 18.07.2021: erfolgreicher Abnahmetest erster Trunk
 - ▶ 14.09.2021: Rufnummernportierung **erster Trunk**
 - ▶ 05.08.2021: Auftrag für **zweiten verschlüsselten SIP-Trunk**
 - ▶ 03.09.2021: Bereitstellung Testnummern zweiter Trunk
 - ▶ 14.09.2021: Beginn der Inbetriebnahme des IP3011 Gateways
 - ▶ 06.10.2021: erfolgreicher Abnahmetest zweiter Trunk
 - ▶ **24.11.2021:** **Rufnummernportierung zweiter Trunk**
-
- fast 6 Monate
- weniger als 4 Monate
- 3 Wochen

innovaphone IP811 / IP3011 Gateways

- ▶ <https://www.innovaphone.com> (Sindelfingen) mit vielen technischen Details unter <https://wiki.innovaphone.com/>
- ▶ verschiedene Gateways verfügbar (bis 5x S0, bis 2x S2M), beliebig kaskadierbar
- ▶ IP811 / IP3011, Firmware $\geq 13r2$
 - ▶ 5x BRI (S0) / 1x PRI (S2M)
 - ▶ 2x LAN
 - ▶ PBX uvm. integriert, hier aber nicht genutzt, theoretisch sanfte Migration einzelner Teilnehmer von TK Anlage auf VoIP möglich via PBX
- ▶ Lizenzerwerb für BRI / PRI, pro Kanal usw. notwendig
- ▶ Georedundanz
- ▶ **responsiver Support** über viele Fachhändler, z.B. hier eine Firmwareanpassung innerhalb 5 Tagen
- ▶ TLS 1.2 wie benötigt unterstützt (und auch schon TLS 1.3)
- ▶ **gutes Tracing** z.B. der verschlüsselten Kommunikation über Wireshark `rpcap://nnn.nnn.nnn.nnn/trace`
- ▶ **Les- & editierbare Konfigurationsdateien**, bislang nie Probleme bei Firmwareupdate, „Reboot When Idle“ möglich
- ▶ GWs unterstützen Silent Suppression, Trunk aber nicht (wird nicht genutzt, aber könnte per `/rem-silence-sup` abgeschaltet werden)
- ▶ erfüllen alle Anforderungen des DFN-Fernsprechen T-Systems Corporate SIP Germany

Von der Beauftragung zum Abnahmetest (1/2)

- ▶ Nach Beauftragung (entgeltpflichtig verschlüsselt, Audio-Codec ausschließlich G.711a, kein T.38 o.a.!) wird in 2-4 Wochen ein Trunk mit 10 Testrufnummern eingerichtet
- ▶ dfn_PRE-Test-*_Checkliste.docx
ist nach interner Einrichtung abzuarbeiten und an T-Systems zu retournieren
- ▶ Terminvereinbarung für Abnahmetest benötigt ca. 1-2 Wochen Vorlaufzeit
- ▶ *«Der Acceptance Tests beinhaltet die Durchführung einer Reihe von einzelnen Testcases entsprechend des beigefügten Protokoll Templates.»*
- ▶ *«Die Dauer dieses Acceptance Tests beträgt im besten Fall 3-4 Stunden. Wenn Probleme auftreten verlängert sich die Dauer entsprechend der Dauer der Problemlösung. Wir planen deshalb in der Regel die Zeit von 9–16 Uhr für die Testdurchführung.»*

Von der Beauftragung zum Abnahmetest (2/2)

- ▶ empfohlene Hardware
 - ▶ zwei Telefone (intern)
 - ▶ zwei Handys
 - ▶ zwei Faxgeräte (intern / extern)
- ▶ Bedienung von Telefon und Handy sollte klar sein
 - ▶ Halten
 - ▶ 3er-Konferenz
 - ▶ Rufumleitung
 - ▶ Rufnummernunterdrückung
- ▶ Verbindung zu den einzelnen SIP Trunk Peers muss kurzfristig trennbar sein im Gateway oder in der Firewall, um die Georedundanz checken zu können

Nach dem Abnahmetest

- ▶ Abnahmetestdokumentation 1-3 Tagen nach Test erhalten
- ▶ Rufnummernportierung dann nach frühestens 34 Werktagen möglich
- ▶ Rufnummernportierung kann schiefgehen:
 - Einmal hat der alte Anbieter das neue Routing zunächst nicht veröffentlicht
 - ⇒ wir waren nur innerhalb des Telekom-Netzes erreichbar
 - ⇒ Telekom musste dem alten Anbieter eine **Portierungsstörung** melden
 - ⇒ 2 Tage nur eingeschränkt erreichbar

Konfig: Zertifikate

- ▶ Serverzertifikate sind ausgestellt auf „han-tdg-sonus-04.telekom.de“ bzw. „fra-tdg-sonus-04.telekom.de“, haben aber keine öffentliche DNS Einträge
- ⇒ lokaler DNS / hosts Eintrag notwendig ansonsten akzeptiert das Gateway die Verbindung nicht

The screenshot shows the 'DNS' configuration page in a management interface. Under the 'Local Resource Records' section, two entries are listed:

Type	Name	Value
A	han-tdg-sonus-04.telekom.de	141.39.219.53
A	fra-tdg-sonus-04.telekom.de	141.39.219.21

The screenshot shows the 'Certificates' configuration page. It features a table of trusted certificates with columns for Subject, Issuer, Not before, Not after, and Download. The 'DFN VoIP Verschlüsselung' certificate is highlighted with an orange border.

Subject	Issuer	Not before	Not after	Download
<input type="checkbox"/> DFN-Verein Global Issuing CA	DFN-Verein Certification Authority 2	24.05.2016	22.02.2031	PEM DER
<input type="checkbox"/> DFN-Verein Certification Authority 2	T-TeleSec GlobalRoot Class 2	22.02.2016	22.02.2031	PEM DER
<input type="checkbox"/> T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	01.10.2008	01.10.2033	PEM DER
<input type="checkbox"/> DFN VoIP Verschlüsselung	DFN VoIP Verschlüsselung	07.12.2010	08.12.2030	PEM DER
<input type="checkbox"/> DFN-Verein Global Issuing CA	DFN-Verein Global Issuing CA	24.05.2016	22.02.2031	PEM DER
<input type="checkbox"/> TeleSec ServerPass Class 2 CA	T-TeleSec GlobalRoot Class 2	11.02.2014	11.02.2024	PEM DER
<input type="checkbox"/> Sectigo RSA Domain Validation Secure Server CA	USERTrust RSA Certification Authority	02.11.2018	31.12.2030	PEM DER
<input type="checkbox"/> USERTrust RSA Certification Authority	USERTrust RSA Certification Authority	01.02.2010	18.01.2038	PEM DER
<input type="checkbox"/> *.innovaphone.com	Sectigo RSA Domain Validation Secure Server CA	10.01.2022	10.02.2023	PEM DER

- ▶ Dem **Wurzelzertifikat des Trunks** unter „DFN VoIP“ https://doku.tid.dfn.de/de:dfnpki:dfnpki_root_certs muss vertraut werden
- ▶ Ein **eigenes Server-Zertifikat** der DFN-PKI mit dem Zertifikatsprofil „VoIP-Server“ muss beantragt, eingerichtet (komplette Kette) und vertraut werden

Konfig: Ein paar Basiseinstellungen

- ▶ Admin Zugang absichern / anlegen unter General > Admin
- ▶ HTTPS für Zugang erzwingen
- ▶ NTP einrichten

The screenshot shows the NTP configuration page. The 'Services' menu is active, and the 'NTP' sub-menu is selected. The configuration fields are as follows:

Time Server 1	de.pool.ntp.org	de.pool.ntp.org
Time Server 2		
Interval [min]	60	60
Timezone	Europe - Central European Time (UTC+1)	
String	CET-1CEST-2,M3.5.0/2,M10.5.0/3	CET-1CEST-2,M3.5.0/2,M10.5.0/3
Current Server	de.pool.ntp.org -> 162.159.200.123	
Last sync	13.09.2022 08:33	
Default Time		

Buttons: OK

The screenshot shows the HTTP/HTTPS configuration page. The 'Services' menu is active, and the 'HTTP' sub-menu is selected. The configuration fields are as follows:

Force HTTPS	<input checked="" type="checkbox"/>
Disable HTTP basic authentication	<input type="checkbox"/>
Password protect all HTTP pages	<input type="checkbox"/>
Port	80
HTTPS-Port	443
Mutual TLS (MTLS)	<input type="checkbox"/>
no-cache	<input type="checkbox"/>

Allowed stations:

Address	Mask

Public compact flash access:

Path	Read	Write
	<input type="checkbox"/>	<input type="checkbox"/>

Active HTTP sessions:

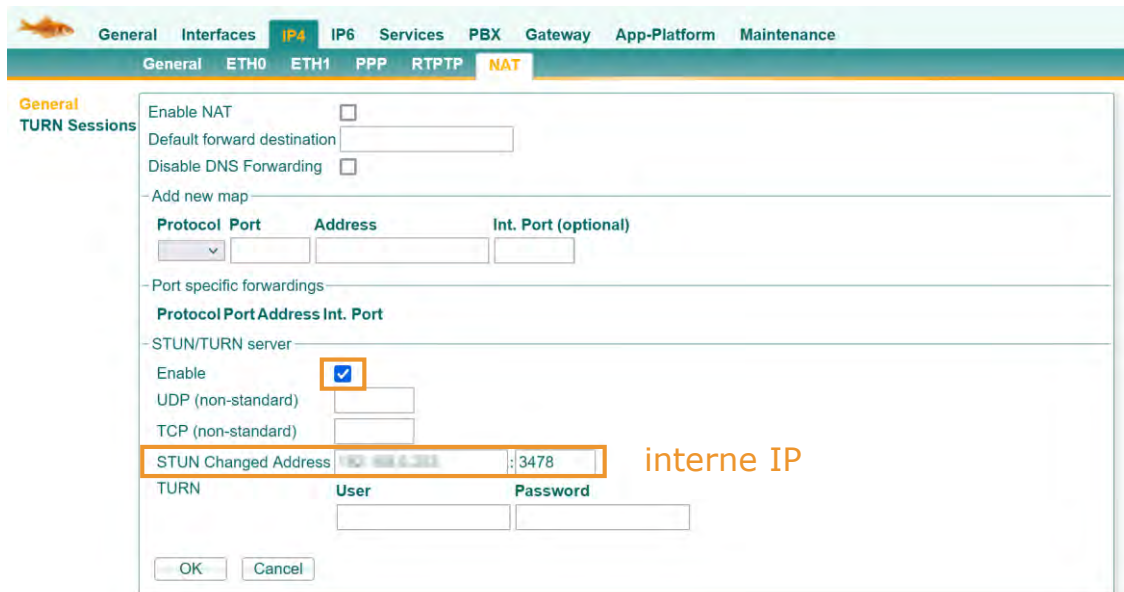
From	Protocol	To	Uptime	Idle	Requests
TEL:192.168.1.104	HTTP	192.168.1.104	0	0	0
TEL:192.168.1.104	HTTPS	192.168.1.104	0	0	0

Buttons: OK, Cancel

Konfig: Betrieb hinter Firewall mit STUN Server & NAT

Firewall Konfiguration:

- ▶ 1:1 NAT öffentliche SIP IP > interne IP
- ▶ SIP-ALG ausschalten!
- ▶ Firewall blockiert von außen alles außer:
 - ▶ TLS Signaling TCP/UDP von 1024-65535 an 5061
 - ▶ STUN Abfrage TCP/UDP von 1024-65535 an 3478 vom T-Systems Trunk, also 141.39.219.53 (Han) und 141.39.219.21 (Fra)



General Interfaces IP4 IP6 Services PBX Gateway App-Platform Maintenance

General ETH0 ETH1 PPP RTPTP NAT

General

TURN Sessions

Enable NAT

Default forward destination

Disable DNS Forwarding

Add new map

Protocol	Port	Address	Int. Port (optional)

Port specific forwardings

Protocol	Port	Address	Int. Port

STUN/TURN server

Enable

UDP (non-standard)

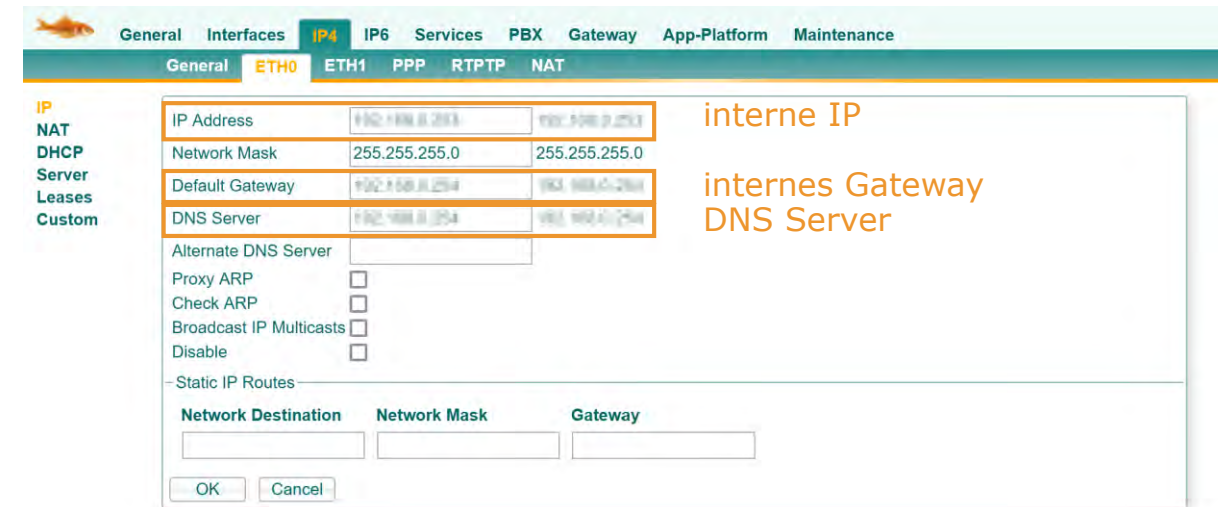
TCP (non-standard)

STUN Changed Address : **interne IP**

TURN

User	Password

OK Cancel



General Interfaces IP4 IP6 Services PBX Gateway App-Platform Maintenance

General ETH0 ETH1 PPP RTPTP NAT

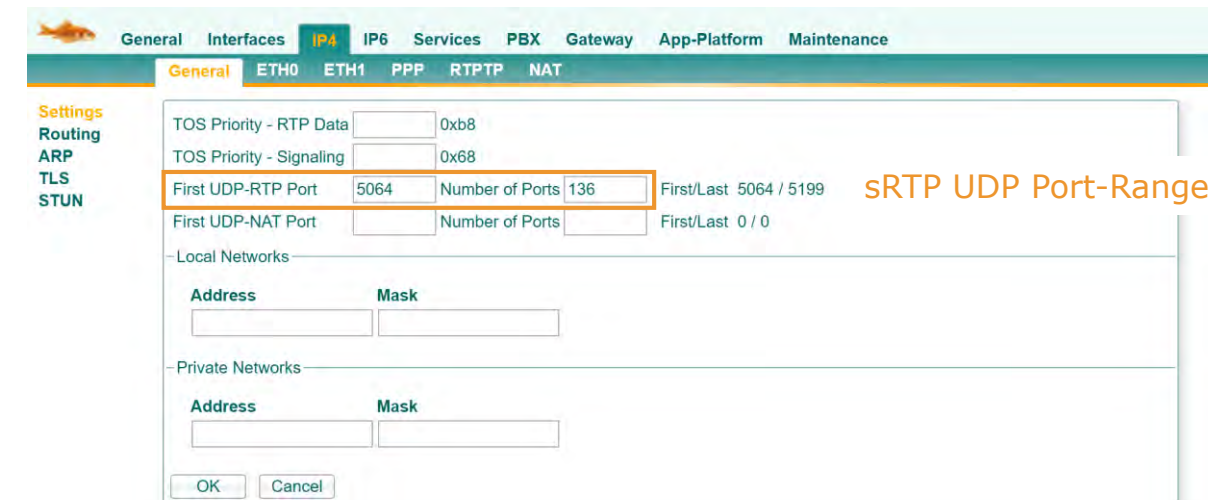
IP

IP Address	<input type="text" value="192.168.254.1"/> <input type="text" value="192.168.254.254"/>	interne IP
Network Mask	<input type="text" value="255.255.255.0"/> <input type="text" value="255.255.255.0"/>	
Default Gateway	<input type="text" value="192.168.254.1"/> <input type="text" value="192.168.254.1"/>	internes Gateway
DNS Server	<input type="text" value="192.168.254.1"/> <input type="text" value="192.168.254.1"/>	DNS Server
Alternate DNS Server	<input type="text"/>	
Proxy ARP	<input type="checkbox"/>	
Check ARP	<input type="checkbox"/>	
Broadcast IP Multicasts	<input type="checkbox"/>	
Disable	<input type="checkbox"/>	

Static IP Routes

Network Destination	Network Mask	Gateway
<input type="text"/>	<input type="text"/>	<input type="text"/>

OK Cancel



General Interfaces IP4 IP6 Services PBX Gateway App-Platform Maintenance

General ETH0 ETH1 PPP RTPTP NAT

Settings

Routing

ARP

TLS

STUN

TOS Priority - RTP Data 0xb8

TOS Priority - Signaling 0x68

First UDP-RTP Port Number of Ports First/Last 5064 / 5199 **sRTP UDP Port-Range**

First UDP-NAT Port Number of Ports First/Last 0 / 0

Local Networks

Address	Mask
<input type="text"/>	<input type="text"/>

Private Networks

Address	Mask
<input type="text"/>	<input type="text"/>

OK Cancel

Konfig: Interfaces PRI (S2M) / BRI (S0)

General Interfaces IP4 IP6 Services PBX Gateway App-Platform Maintenance

ETH0 ETH1 **PRI1**

Physical Protocol Interop State Statistics

NT Mode
Clock Mode
Swap tx/rx
Do not use for Synchronization
µ-Law
T1
CAS
No CRC4
Remote loopback
Tx attenuation for T1 mode
Send flags on FDL

OK Cancel

Physical Protocol Interop State Statistics

Protocol
Assign Channels from Top

OK Cancel

General Interfaces IP4 IP6 Services PBX Gateway App-Platform Maintenance

ETH0 ETH1 **BRI1** BRI2 BRI3 BRI4 BRI5

Physical Protocol Interop State Statistics

NT Mode
Swap tx/rx
100 Ohm Termination
µ-Law
Permanent Activation
Activate 'power-off loop' relay
Loopback

OK Cancel

Physical Protocol Interop State Statistics

Protocol
Mode

OK Cancel

Konfig: Gateway > General / Interfaces

The screenshot displays the configuration interface for a Gateway, divided into two overlapping windows.

Top Window (Gateway General Settings):

- Navigation: General, Interfaces, IP4, IP6, Services, PBX, **Gateway**, App-Platform, Maintenance
- Sub-navigation: **General**, Interfaces, SIP, GK, Routes, CDR0, CDR1, Calls
- Options:
 - No blind transfer:
 - Call Logging:
 - Route Logging:
 - Write CDRs: All (dropdown)
 - Logging Filter(GW:Nr): [] : []
- Licenses table:

Name	Count	Usage
PRIs	2	1
Channels	60	0
- Buttons: OK, Cancel

Bottom Window (Interface Configuration):

- Navigation: General, Interfaces, IP4, IP6, Services, PBX, **Gateway**, App-Platform, Maintenance
- Sub-navigation: General, **Interfaces**, SIP, GK, Routes, CDR0, CDR1, Calls
- Section: **Interface CGPN-In CDPN-In CGPN-Out CDPN-Out State Alias Registration**
- Table:

Interface	CGPN-In	CDPN-In	CGPN-Out	CDPN-Out	State	Alias	Registration
PRI1	n→0	n→0		00→i			Up
	i→00	i→00					
- Fields:
 - TEXT: []
 - TEST: []
 - TONE: []
 - HTTP: []
 - ECHO: []
 - FAX: +
 - CONF: +
 - SCNF: +
- Internal Registration:
 - Name: []
 - Disable:
 - Provisioning:
 - Tones: EUROPE-PBX (dropdown)
 - Send Date/Time:
 - Set Date/Time:
 - Ack incoming call:
 - Interface Maps: Manual (dropdown)
 - Protocol: None (dropdown)
- Buttons: OK, Cancel, Apply, Delete, Help

Konfig: Gateway > SIP

General Interfaces IP4 IP6 Services PBX **Gateway** App-Platform Maintenance

General Interfaces **SIP** GK Routes CDR0 CDR1 Calls

Interface	CGPN-In	CDPN-In	CGPN-Out	CDPN-Out	State Alias	Registration
SIP1 T-Systems Frank	i49	00→i	0049	11833→i4911833		fra-tdg-sonus-04.telekom.de
	0049	0→i49	110→i49110			
	0		112→i49112			
			115→i49115			
			00→i			
			0→i49			
			→i49			
SIP2 T-Systems Hanno	i49	00→i	0049	11833→i4911833		han-tdg-sonus-04.telekom.de
	0049	0→i49	110→i49110			
	0		112→i49112			
			115→i49115			
			00→i			
			0→i49			
			→i49			
SIP3	+					
SIP4	+					
SIP5	+					
SIP6	+					
SIP7	+					
SIP8	+					
SIP9	+					
SIP10	+					
SIP11	+					
SIP12	+					
SIP13	+					
SIP14	+					
SIP15	+					
SIP16	+					

Trunk

CGPN In

International → 00

CDPN In

International → 49

0049

0

CGPN Out

00 → International

0 → International 49

CDPN Out

0049 11833 → International 4911833

110 → International 49110

112 → International 49112

115 → International 49 115

00 → International

0 → International 49

→ International 49

Konfig: Gateway SIP > Interface

Name: T-Systems Frank
Disable:
Type: Provider
Transport: TLS Without registration
Remote Domain: fra-tdg-sonus-04.telekom.de
Local Domain:
Local Hostname:
Local Port:
Proxy: fra-tdg-sonus-04.telekom.de
STUN Server:
- Authorization -
Username:
Password: Retype:
- Media Properties -
General Coder Preference: G711A Framesize [ms]: 20 Silence Compression: Exclusive:
Local Network Coder: G711A Framesize [ms]: 20 Silence Compression:
Enable T.38: No DTMF Detection: Enable PCM: Media-Relay: On Video:
SRTP Cipher: AES128/80 SRTP Key Exchange: SDES-DTLS Unencrypted SRTCP:
No ICE: No RTCP-MUX: TURN Only:
Record to (URL):
- SIP Interop Tweaks -
Proposed Registration Interval [s]:
Accept INVITE's from Anywhere:
Enforce Sending Complete: (affects outgoing SIP calls only)
No Video:
To Header when Sending INVITE: Called Party (affects outgoing SIP calls only)
From Header when Sending INVITE: CGPN in user part of URI
Identity Header when Sending INVITE: UUI
Reliability of Provisional Responses: Supported (affects outgoing SIP calls only)
Microsoft Presence Format:
Advanced
Internal Registration
Protocol: None
Buttons: OK, Cancel, Apply, Delete, Help

bzw. T-Systems Hanno

SIP Signaling mit TLS ohne Registrierung
bzw. han-tdg-sonus-04.telekom.de
eigene öffentliche SIP IP
eigener öffentlicher SIP FQDN

bzw. han-tdg-sonus-04.telekom.de
eigener öffentlicher SIP FQDN

verschlüsselt

eigene öffentliche SIP IP: TLS-Port zum Signaling

Konfig: Gateway > Routes

General Interfaces IP4 IP6 Services PBX **Gateway** App-Platform Maintenance

General Interfaces SIP GK **Routes** CDR0 CDR1 Calls

From	To	Counter	CGPN Maps
SIP1:T-Systems Frank	PRI1		
SIP2:T-Systems Hanno			
PRI1			
	SIP1:T-Systems Frank	b	→
	SIP2:T-Systems Hanno	b	→

Description Disable

PRI1
 TEXT
 TEST
 TONE
 HTTP
 ECHO
 FAX
 CONF
 SCNF

SIP1 T-Systems Frank
 SIP2 T-Systems Hanno

SIP3
 SIP4
 SIP5
 SIP6
 SIP7
 SIP8
 SIP9
 SIP10
 SIP11
 SIP12
 SIP13
 SIP14
 SIP15
 SIP16

Add UUI
Final Route
Final Map
No Reroute on wrong No
Verify CGPN or DGPN
Interworking(QSIG,SIP)
Rerouting as Deflection
Routing on Diverting No
Force enblock after ms
Add #
Disable Echo Canceler
Emergency
No DGPN Mapping
Call Counter max

OK Cancel Apply Help

GK Reg. Name	Number In	Number Out
<input type="text"/>	<input type="text"/>	<input type="text"/> → <input type="text"/> <input type="text"/>

OK Cancel Apply Help

Konfig: Gateway > Routes

From	To	Counter	CGPN	Maps
SIP1:T-Systems Frank	PRI1			→
SIP2:T-Systems Hanno	PRI1			→
PRI1	SIP1:T-Systems Frank	b		→
	SIP2:T-Systems Hanno	b		→

Description: Disable:

PRI1 SIP1 T-Systems Frank SIP2 T-Systems Hanno

TEXT TEST TONE HTTP ECHO FAX CONF SCNF

SIP3 SIP4 SIP5 SIP6 SIP7 SIP8 SIP9 SIP10 SIP11 SIP12 SIP13 SIP14 SIP15 SIP16

Add UUI:

Final Route: Final Map:

No Reroute on wrong No: Verify CGPN: or DGP:

Interworking(QSIG,SIP): Rerouting as Deflection:

Routing on Diverting No: Force enblock: after 4000 ms

Add #: Disable Echo Canceler:

Emergency: No DGP Mapping:

Call Counter: max:

OK Cancel Apply Delete Help

bzw. T-Systems Hanno
eigene öffentliche SIP IP

GK Reg. Name:

Number In: → Number Out:

OK Cancel Apply Help

Zusammenfassung

IP811 / IP3011 überzeugen als verlässliche SIP-S0/S2M Gateways mit gutem Support:

- ▶ Bisher stets problemlose Aktualisierung auf neue Firmware
- ▶ Telefon, Fax und Frankit funktionierten ad hoc
- ▶ Wählgeräte mit D-Kanal Euro-ISDN (DSS1) X.31 und B-Kanal HDLC X.75 SLP transparent funktionierte ebenfalls ad hoc, aber Protokolle gehören *«nicht zum versprochenen Produkt(-umfang) DFN-C.SIP.G. (...) keinen Support (...) Es ist möglich, dass die Protokolle bei einem Update seitens der Deutsche Telekom-Plattform C.SIP.G. nicht mehr funktionieren.»*
- ▶ Wählgeräte mit DTMF funktionieren seit einem Firmware Update des Wählgeräteherstellers, durch das die Steuergeräte nun auf Rückantworten etwas länger wartet
- ▶ Bereits eingebaute Unified Communications Funktionen wie PBX, myApps bieten Skalierbarkeit

Einen großen Dank an die tolle Unterstützung von DFN Fernsprechen, innovaphone, Telekom & T-Systems – man steht nicht einsam vor Hürden, auch wenn man mitdenken muss ...

Wunsch an DFN & innovaphone: *«Automatic Certificate Management Environment (ACME)»*

Nützliche Abkürzungen

- ▶ STUN Session Traversal Utilities for NAT
- ▶ TLS Transport Layer Security
- ▶ sSIP secure Session Initiation Protocol
- ▶ sRTP secure Real-Time Transport Protocol
- ▶ SIP-ALG SIP Application Layer Gateway
- ▶ DTMF Dual Tone Multi-Frequency,
Mehrfrequenzwahlverfahren (MFV)
- ▶ PBX Private Branch Exchange, Telefonanlage