Herzlich Willkommen zum Business-Frühstück

WWZ Telekom AG

QUICKLINE

swizzconnexx

02.05.19 / MN

swizzconnexx

Hautpsitz in Muri, AG

Tätigkeit:

- Beratung, Konzeption und Planung von Netzwerklösungen
- Konfiguration, Integration, Technische Unterstützung und Support
- Handel / Distribution

Im Bereich

- Datenkommunikation, Telefonie, Multimedia, Sicherheit, Überwachung (Monitoring), Cloud-Lösungen

Dienstleistungen

swizzconnexx

Wir unterstützen unsere Kunden in:

- **Beratung, Konzeption und Planung**
  - Gesamtheitliche Netzwerklösungen
  - Konzeption von technischen und kommerziellen Lösungen
  - Spezifikation und Ausführplanung
  - Projektleitung und –ausführung

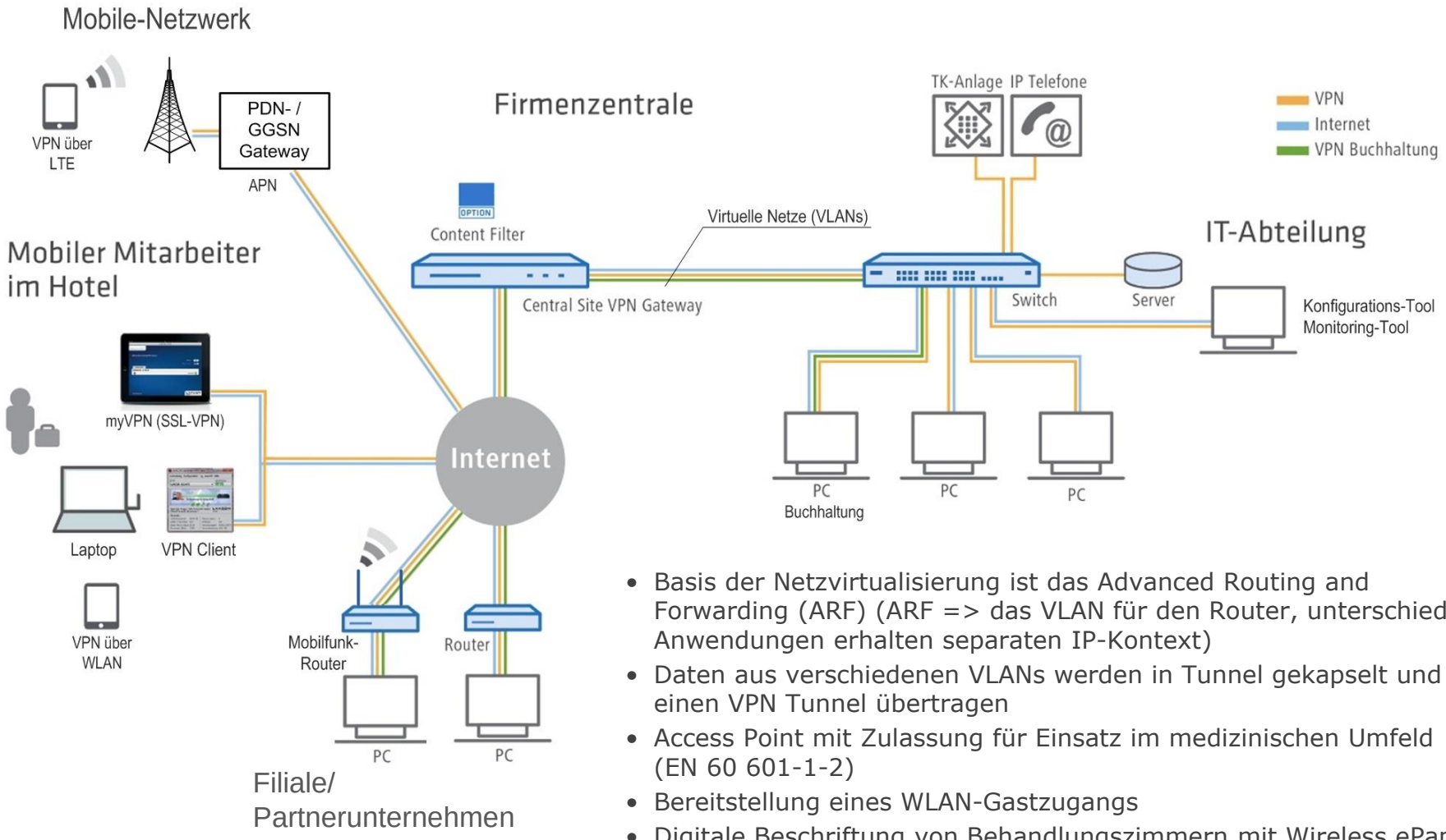
- **Engineering und technische Unterstützung**
  - Konfiguration und Integration
  - Schulung und Training
  - Wartung & Support

- **WLAN Planung und Messung**
  - Kapazitäts- und Versorgungsplanung
  - Versorgungsanalyse und –messung (Site Survey)

Netzwerklösung - Netzvirtualisierung

swizzconnexx

Standortvernetzung von Zentralen, Filialen und mobilen Mitarbeitern



- Basis der Netzvirtualisierung ist das Advanced Routing and Forwarding (ARF) (ARF => das VLAN für den Router, unterschiedliche Anwendungen erhalten separaten IP-Kontext)
- Daten aus verschiedenen VLANs werden in Tunnel gekapselt und über einen VPN Tunnel übertragen
- Access Point mit Zulassung für Einsatz im medizinischen Umfeld (EN 60 601-1-2)
- Bereitstellung eines WLAN-Gastzugangs
- Digitale Beschriftung von Behandlungszimmern mit Wireless ePaper-Lösungen

Themen Workshop

swizzconnexx

1. **be.IP plus, ALL-IP Business-Gateway mit TVA**
   - Technische Merkmale

2. **Anwendungsszenario be.IP plus**
   - reine Teilnehmervermittlungsanlage (TVA)
   - Gateway-Router und TVA integriert

3. **Herausforderungen VoIP**
   - VoIP (UDP) Datentransport
   - IPv4 NAT-Routing versus SIP (Session Table, Layer 5)
   - Firewall (bindings)

4. **Funktionen / Konfiguration be.IP plus**
   - Konfigurationsoberfläche
   - Assistenten
   - Inbetriebnahmehilfe-Dokument

1. be.IP plus - DAS Plus an Kommunikation und Flexibilität

swizzconnexx

Die be.IP plus ist eine konvergente ALL-IP-Kommunikationslösung, nicht nur eine Telefonanlage.

Das flexibel einsetzbare System vereint die komfortablen Telefonie-Funktionen einer TK-Anlage mit den Vorteilen eines leistungsfähigen VPN-Routers und sorgt so für eine sichere Sprach- und Datenkommunikation.

Der integrierte WLAN-Accesspoint (inkl. WLAN-Controller) unterstützt dabei das 2,4- oder 5-GHz-Band mit bis zu 300 Mbit/s Datendurchsatz.

Eigenschaften / Merkmale:

- Telefonanlage für 20 Benutzer (bis 40 erweiterbar)
- Unterstützung für analoge, ISDN und IP/IP DECT-Endgeräte
- 4 analoge und 4 ISDN-Endgeräte (2 pro S0-Schnittstelle) können eingebunden werden
- Integriertes VDSL2/ADSL2+-Modem (Annex B/J, Vectoring)
- Integrierter Business-Router mit 5 x VPN-Tunnel (max. 10)
- Integrierter WLAN Accesspoint für 2,4 oder 5 GHz mit WLAN Controller für max. 6 APs
- 5x Gigabit Ethernet Schnittstellen
- VoiceMail, TAPI und LANCAPI
- Stateful Inspection Firewall
- Professionelles Bandbreitenmanagement, QoS

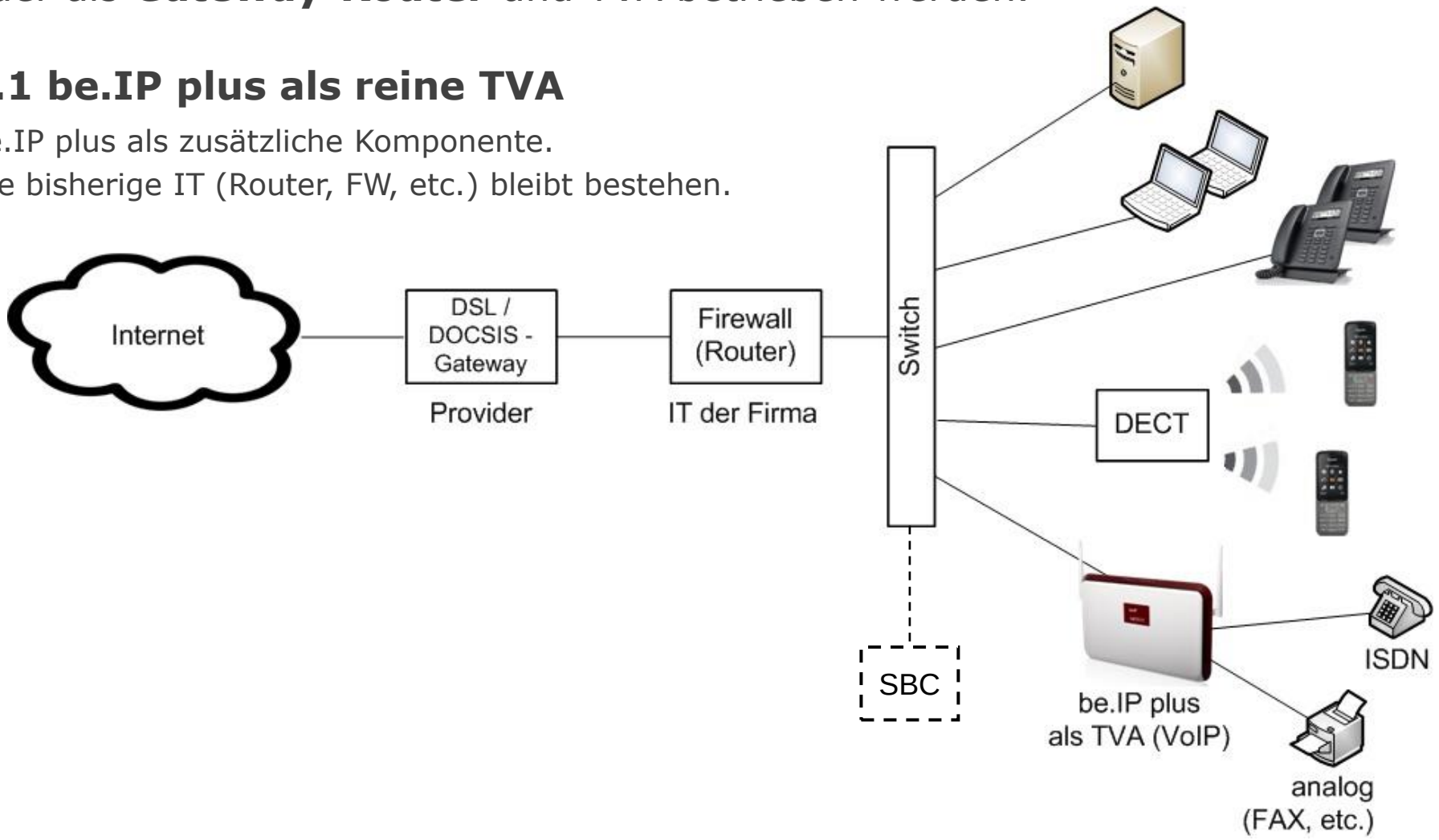
2. Betriebsarten be.IP plus

swizzconnexx

Die **be.IP plus** kann als reine **Telefonzentrale (TVA)** oder als **Gateway-Router** und TVA betrieben werden.

2.1 be.IP plus als reine TVA

be.IP plus als zusätzliche Komponente.
Die bisherige IT (Router, FW, etc.) bleibt bestehen.

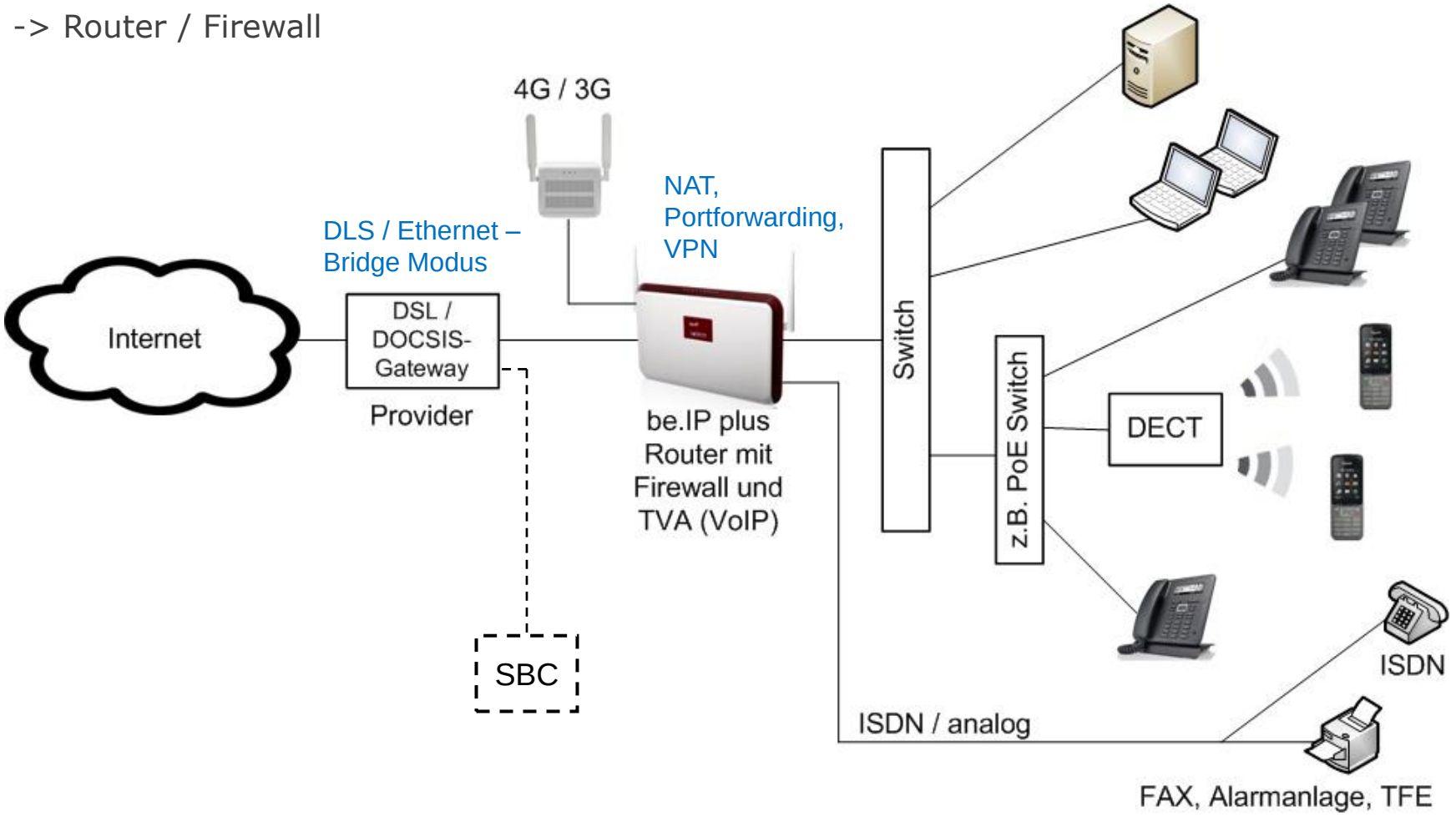


2. Betriebsarten be.IP plus

swizzconnexx

2.2 be.IP plus als Gateway-Router mit FW und TVA

be.IP plus ersetzt zusätzlich evtl. veraltete IT-Komponenten:
-> Router / Firewall

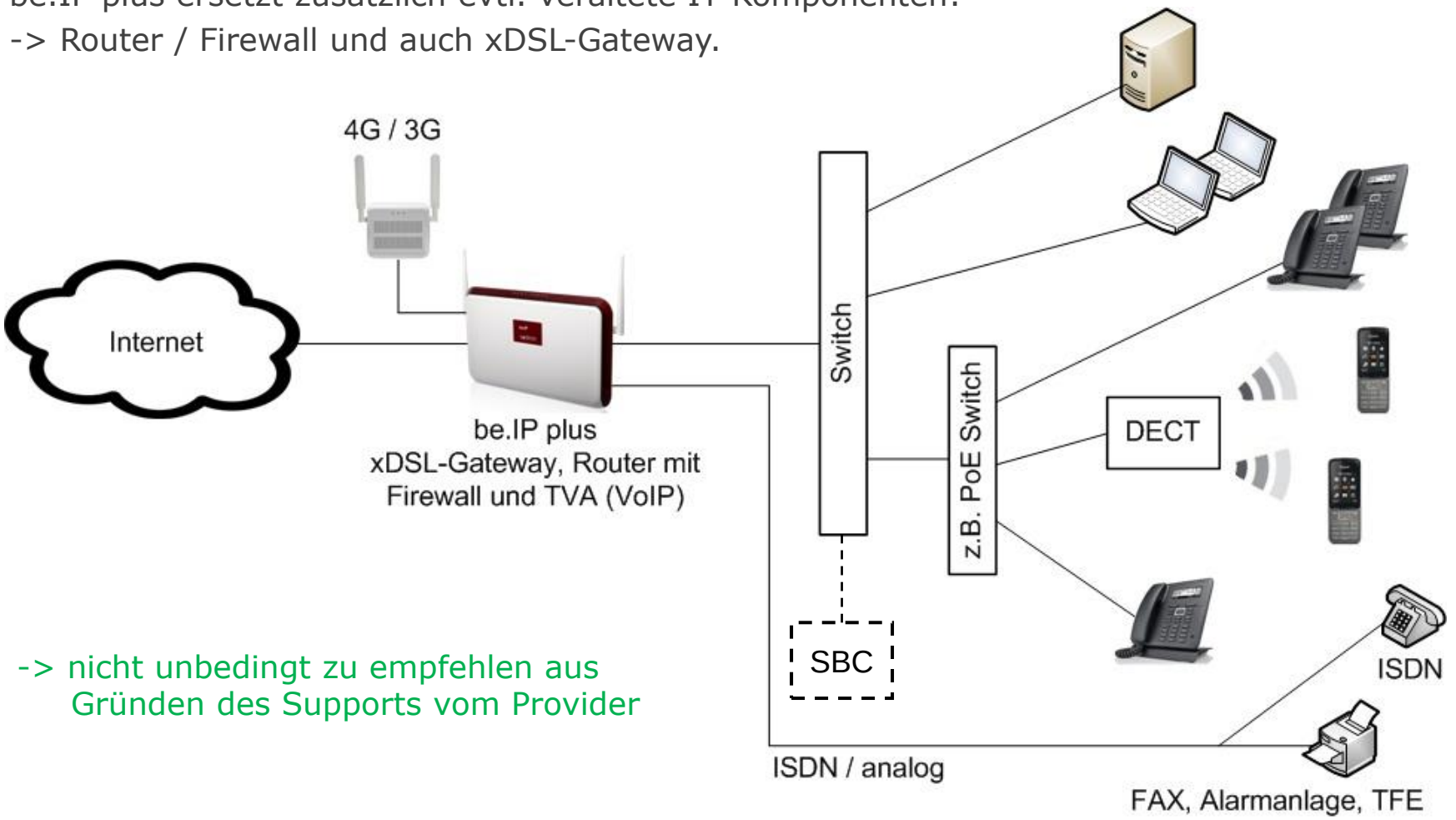


2. Betriebsarten be.IP plus

swizzconnexx

2.3 be.IP plus als VDSL-Gateway-Router mit FW und TVA

be.IP plus ersetzt zusätzlich evtl. veraltete IT-Komponenten:
-> Router / Firewall und auch xDSL-Gateway.



-> nicht unbedingt zu empfehlen aus Gründen des Supports vom Provider

3. Herausforderungen VoIP

swizzconnexx

Mit **All-IP** ist umgangssprachlich hauptsächlich gemeint, dass neu auch die Sprachdaten über das «IP-Netzwerk» gesendet werden, also **VoIP** (Voice over IP).

3.1 Datentransport

Im VoIP wurde grundsätzlich versucht die Mechanik und Logik der vermittlungsorientierten Kommunikation aus der traditionellen Telekommunikation (SDH, PDH, MPLS, ISDN, etc.) zu übernehmen.

Im IT-Netzwerk gibt es grundsätzlich 2 Transportprotokolle:

- **TCP** = verbindungsorientiert (Session), paketvermittelt
- **UDP** = verbindungslos (ohne Sicherung), sehr wenig Verzögerung

Da Sprache zeitkritische Realtimedaten sind, eignet sich aus Gründen der Latenz und Jitter nur **UDP** für **VoIP**.

3. Herausforderungen VoIP

swizzconnexx

3.2 NAT => Session Table

In IPv4 IT-Netzwerken findet aufgrund der Adressbegrenzung eine Netzwerkadressübersetzung **NAT** statt.
Bei abgehenden Datenpaketen wird vom WAN-Router (Gateway) die interne IP (z.B. 192.168.x.y) in die öffentliche IP (z.B. 178.82.50.y) umgesetzt => **Source-NAT**.

Von Extern ankommende Pakete werden nur nach Intern geleitet, wenn zuerst von Intern ein Paket gesendet wurde über dieses Port (Port-Öffnung von innen) = **NAT-Session**, oder eine spezielle Regel für die «Öffnung» von Extern definiert wurde (Destination-NAT)

VoIP **(SIP und RTP) sind UDP** => UDP baut keine Session auf. Damit die Port Öffnung in UDP für eine bidirektionale Kommunkation trotzdem stattfindet werden für UDP **logische Sessions** nachgebildet mit einem **Ablauftimer**.

3. Herausforderungen VoIP

swizzconnexx

3.3 Firewall (bindings)

Ähnlich wie beim **NAT** funktioniert auch die **Firewall**.
Von Extern ankommende Pakete werden nur nach Intern geleitet, wenn zuerst von Intern ein Paket gesendet wurde über dieses Port (Öffnung von innen) = **Session**, oder eine spezielle Regel für die «Öffnung» von Extern definiert wurde.

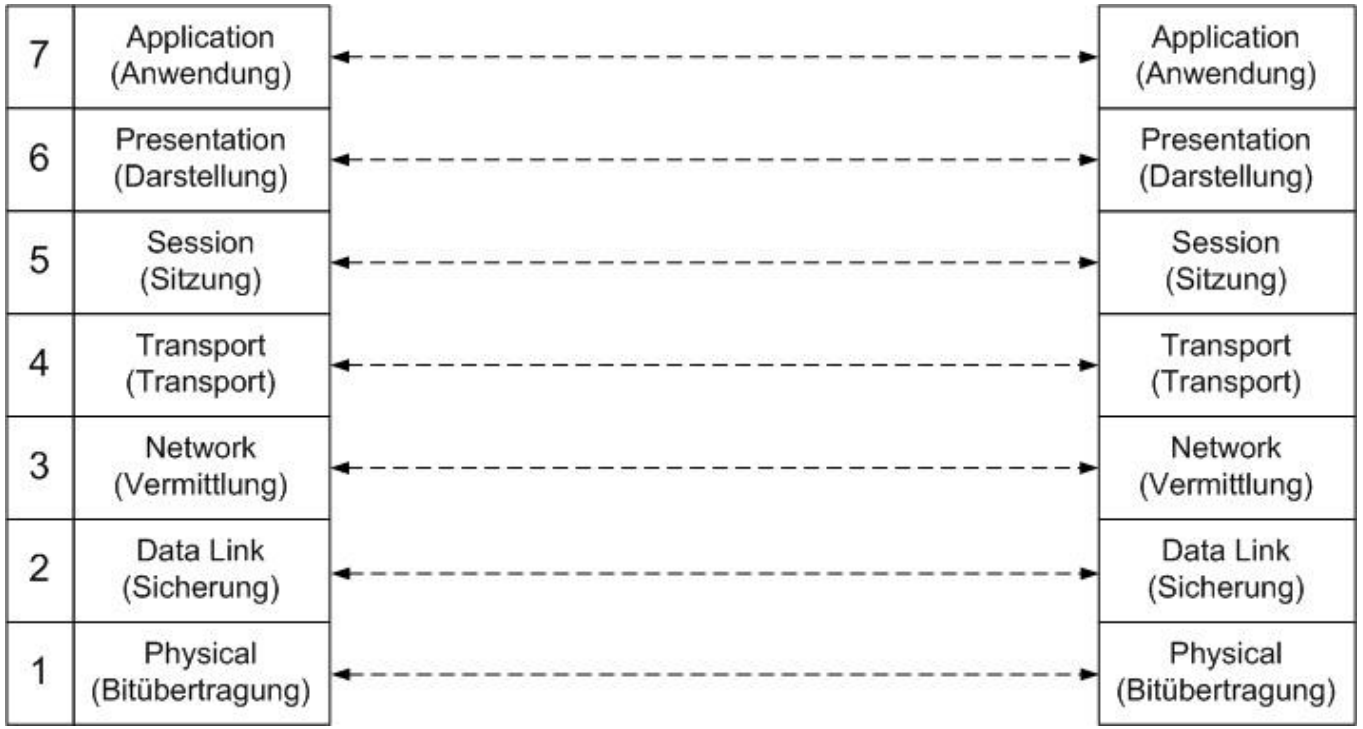
VoIP (SIP und RTP) sind UDP => UDP baut keine Session auf. Damit die Öffnung in UDP für eine bidirektionale Kommunkation trotzdem stattfindet werden für UDP **logische Sessions** nachgebildet mit einem **Ablauftimer** (oft 180s).

3. Herausforderungen VoIP

swizzconnexx

3.4 NAT => VoIP (SIP, RTP)

NAT / Routing (TCP und UDP) findet auf Layer 3 und 4 statt. SIP und RTP ist Layer 5.



DNS, HTTP, SMTP, POP, Telnet, FTP, **DHCP**, etc.

HTML, DOC, JPEG, MP3, etc.

SIP, RTP, Sockets, NetBIOS, SS7, etc.

TCP, **UDP**, SSL, **TLS**, etc.

IP, IPsec, ICMP, IGMP, NAT, RIP, BGP, etc.

Ethernet, VLAN (802.x), **ATM**, **PPP (PPPoE)**, **802.11**, etc.

RS-232, RJ45, **xDSL**, **802.11**, 802.x, SDH, **DOCSIS**, **ISDN**, etc.

-> **HTTPS**: HTTP über TSL -> **SIPS**: SIP über TLS

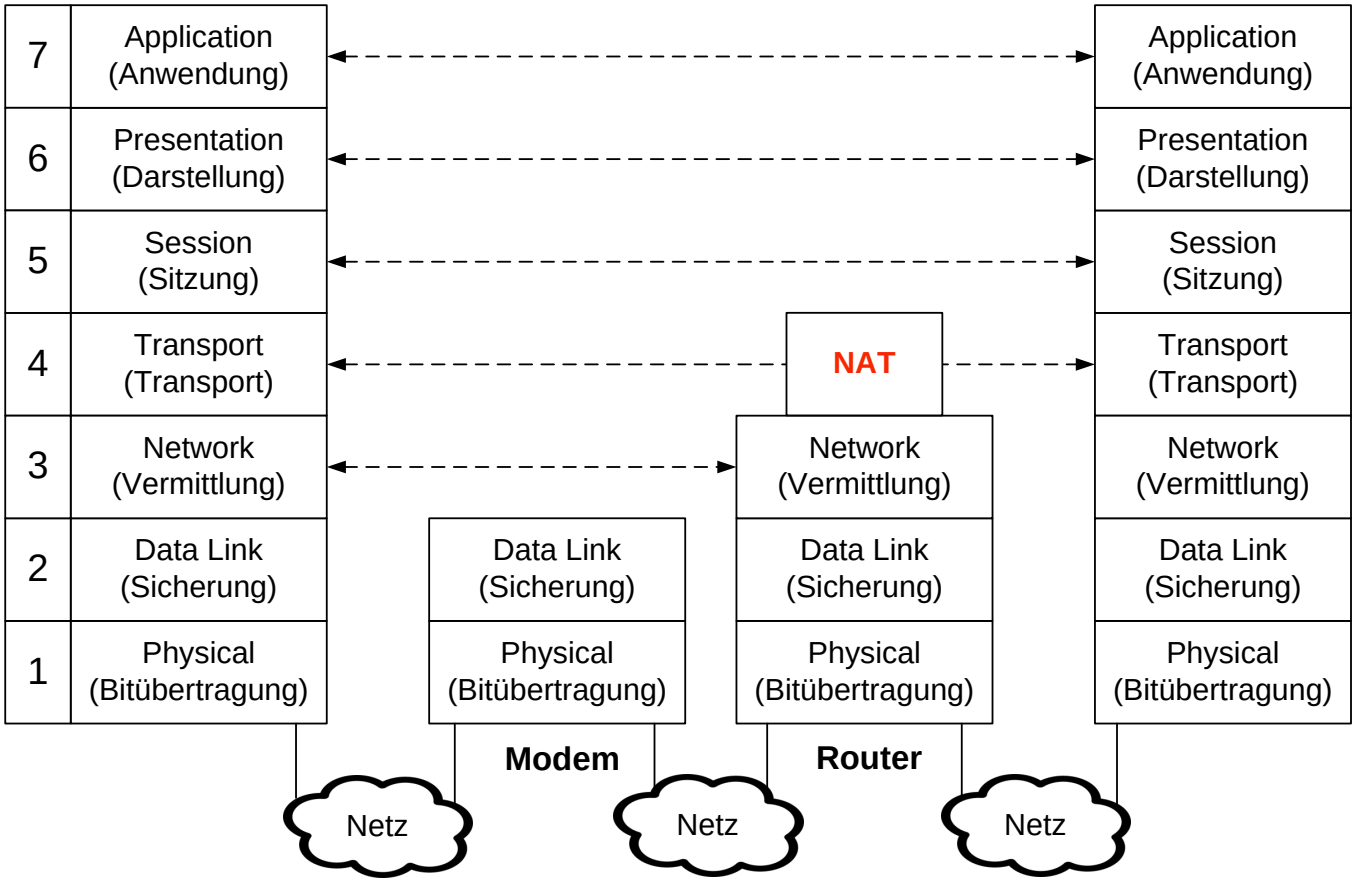
-> «**VDSL u. ADSL Übertragung**» = PPPoE / PPPoA über ATM (AAL5) über VDSL / ADSL Modulation

3. Herausforderungen VoIP

swizzconnexx

3.4 NAT => VoIP (SIP, RTP)

NAT / Routing (TCP und UDP) findet auf Layer 3 und 4 statt. SIP und RTP ist Layer 5.



DNS, HTTP, SMTP, POP, Telnet, FTP, **DHCP**, etc.

HTML, DOC, JPEG, MP3, etc.

SIP, RTP, Sockets, NetBIOS, SS7, etc.

TCP, **UDP**, SSL, **TLS**, etc.

IP, IPsec, ICMP, IGMP, **NAT**, RIP, BGP, etc.

Ethernet, VLAN (802.x), **ATM**, **PPP (PPPoE)**, **802.11**, etc.

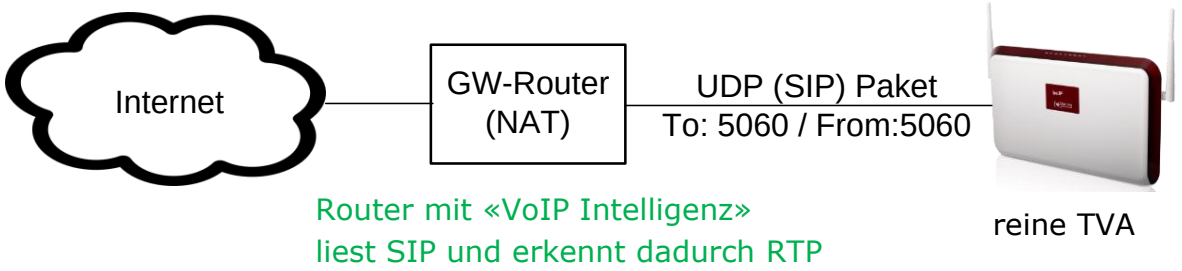
RS-232, RJ45, **xDSL**, **802.11**, 802.x, SDH, **DOCSIS**, **ISDN**, etc.

3. Herausforderungen VoIP

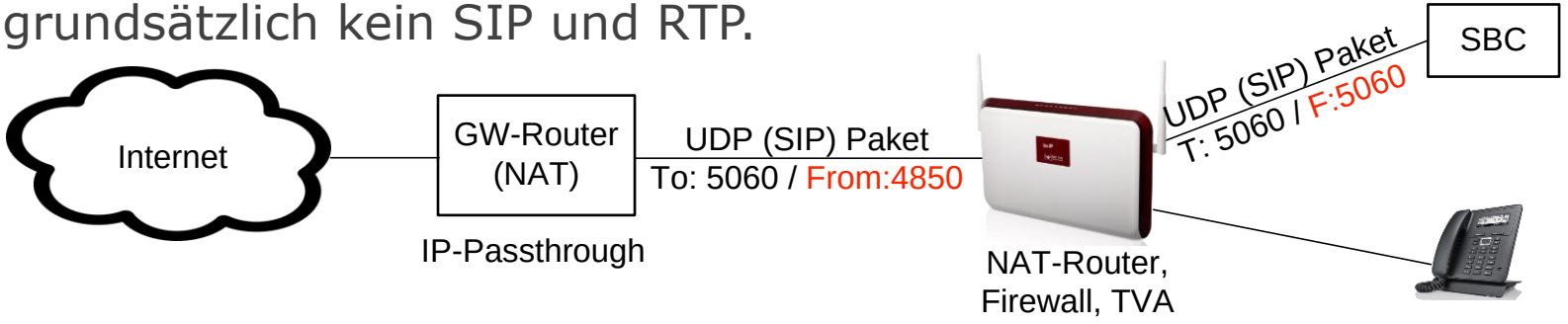
swizzconnexx

3.4 NAT => VoIP (SIP, RTP)

Fazit: Ein normaler NAT-Router (Gateway) weiss bei UDP:5060 dass er SIP routet, hat aber keine Kenntnis über den Inhalt.
Das RTP-Port (UDP:Port > 10’000) erkennt er nicht.



Wird eine DMZ oder Passthrough auf dem GW eingerichtet, erkennt der GW grundsätzlich kein SIP und RTP.



Mögliche Lösung: SNAT Definition mit fixem 5060 Port. VoIP Intelligenz hält SIP «offen» solange RTP gesendet wird.

3. Herausforderungen VoIP

swizzconnexx

SIP / RTP

SIP Invite (Datenauszug): *gesendetes Paket (WAN)*

Internet Protocol Version 4, Src: 178.197.234.226, Dst: 84.73.156.236
User Datagram Protocol, Src Port: 35206, Dst Port: 5060
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:83@tel.swizzconnexx.ch:5060 SIP/2.0
Message Header
Via: SIP/2.0/UDP 10.128.115.223:5060;branch=z9hG4bKe973aefa818c249a6;rport
From: "71" <sip:71@tel.swizzconnexx.ch:5060>;tag=2beb427efc
To: <sip:83@tel.swizzconnexx.ch:5060>
Call-ID: 52b2cf27b7066c3b
Contact: <sip:71@10.128.115.223:5060>;audio
Session-Expires: 1800; refresher=uas
Content-Type: application/sdp
Message Body
Session Description Protocol
Owner/Creator, Session Id (o): - 305065757297 305065757297 IN IP4 10.128.115.223
Connection Information (c): IN IP4 10.128.115.223
Session Attribute (a): sendrecv
Media Description, name and address (m): audio 12100 RTP/AVP 0 8
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): sendrecv

SIP-Client teilt lokale IP mit, der NAT-Router ändert jedoch IP und Port

Nach Session Initierung soll RTP direkt an 10.128.115.223:12100 senden.

=> Provider hat Medien-Proxy mit symmetric response routing

3. Herausforderungen VoIP

swizzconnexx

Übersicht

1. **Datentransport UDP** (verbindungslos ohne Sicherung)
   - «Fire and Forget», keine Rückmeldung, keine Wiederholung
     korrekte MAC-Tabellen sind die einzige Gewährleistung (=>ARP)
   - Wenn Latenz zu gross => gedropt
   - Wenn Jitter (Schwankungen) zu gross => unbrauchbar

   Bisher nur für Daten (TCP) benutztes LAN (auch WAN) muss nun richtig und gut funktionieren (=> evtl. VLAN, MTU, QoS, etc.)

2. **NAT-Sessions:** logische Sessions UDP mit **Ablauftimer (TTL)**
   - Wenn «Port-Öffnung» von innen abläuft keine Anrufe mehr von Extern
   - Innerhalb eines SIP-Dialogs (SIP:Invite, dann RTP) muss Session nach ca. 12-14 Min. erneuert werden mit Re-Invite oder SIP:Update. Nach Ablauf der Session, nicht mehr möglich von Extern.

   SIP:Option- oder leere UDP-Pakete senden (Keep-Alive), VoIP-Intelligenz (RTP->SIP), DNAT, bestimmte ALG Features

3. **Firewall Bindings: TTL** (siehe 2. NAT-Sessions)
   zusätzlich: Zugriffsregeln, VoIP-Intelligenz, bestimmte ALG Features

3. Herausforderungen VoIP

swizzconnexx

Übersicht

4. **NAT-VoIP: Erkennt SIP und RTP nicht**
   - kann SDP im SIP nicht lesen => RTP Port nicht offen
   - SIP:Option- oder leere UDP-Pakete haben keinen Nutzen, weil jeder SIP-Dialog (z.B. SIP:Invite, dann RTP) einen neuen S-NAT Port öffnet am Router, weil symmetrisches NAT

   VoIP-Intelligenz (SIP->RTP), S-NAT z.B. Full-Cone, bestimmte ALG Features (NICHT SIP-Header Transformation), STUN-Handler im Router (von SIP auf RTP), ICE -> STUN und TURN, STUN auf Client
   Provider setzt Media Gateway/Proxy ein mit symmetric response routing

5. **Codec**
   - Provider verwenden oft teil-gehostete US-VoIP-Server, welche USA-Codec verwenden. => Transcoding im SIP Pfad, verursachen Fehler und Latenzen und Jitter.

   Early Media deaktivieren, Codec Einschränken, beim Provider RTP-Proxy verlangen.

3. Herausforderungen VoIP

swizzconnexx

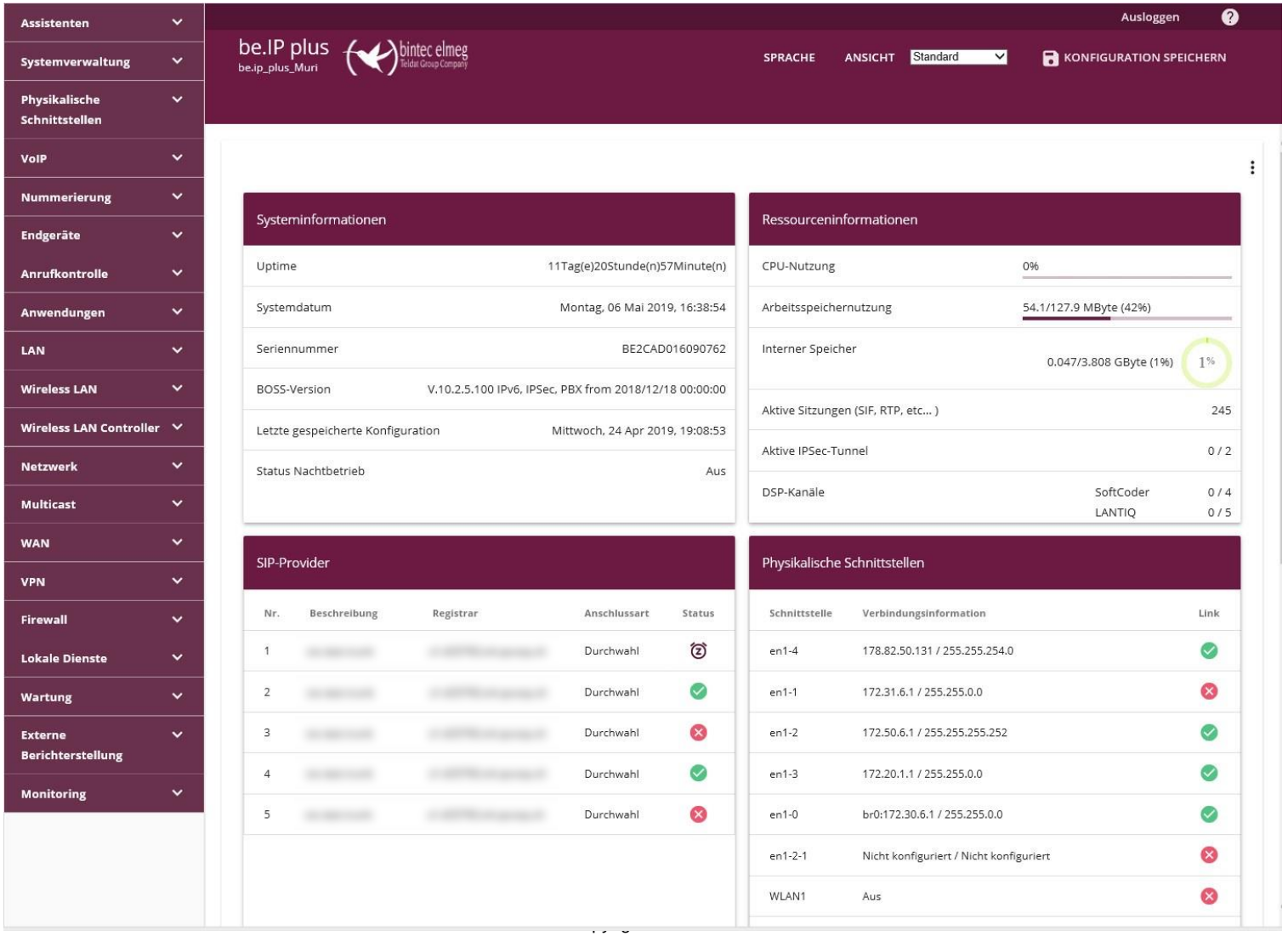
Fazit

- Bei UDP (SIP, RTP) = Telefonie, Multimedia, Streaming etc. in einem gerouteten Netzwerk hilft es sehr zu wissen was man tut.
- Bei TVA mit SIP- und RTP-Verbindungen über z.B. die be.IP plus als NAT-Router/Firewall werden die Probleme gelöst durch die **VoIP-Intelligenz des Routers** (be.IP plus).
- Bei «üblichen» TVA mit SIP- und RTP-Verbindungen über einen **separaten NAT-Router** zu einer VoIP-Plattform eines VoIP-Providers, löst der Provider zu 99% diese Probleme mit seiner SIP-intelligenten Infrastruktur von SIP-Proxies, RTP-Proxies, Media-Gateway mit symmetric RTP, B2BUA (SBC) etc. - ausser Codec Probleme
  => Der Internet Provider (ISP) jedoch nicht immer.
- Beim Einsatz von B2BUA (SBC) in bestimmten Netzstrukturen müssen evtl. Massnahmen ergriffen werden => z.B. für ReInvite
- Bei TVA mit SIP- und RTP-Verbindungen zu externen Clients (z.B. App auf Mobiltelefon) über Layer 3, also nicht VPN, müssen gezielte Massnahmen umgesetzt werden. (-> VoIP-Intelligenz generieren)

4. Funktionen / Konfiguration be.IP plus

swizzconnexx

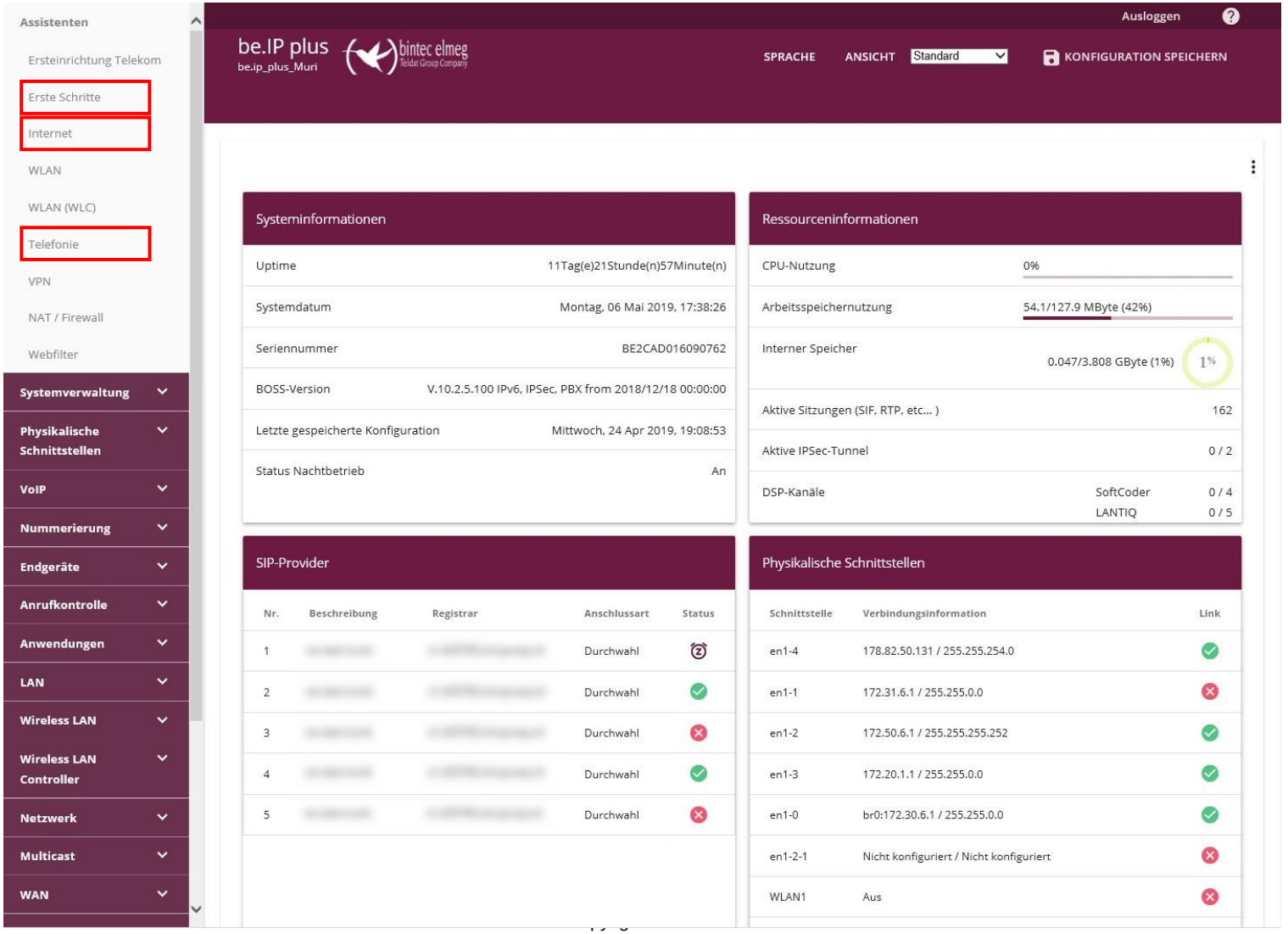
Konfigurationsoberfläche (GUI)



4. Funktionen / Konfiguration be.IP plus

swizzconnexx

Assistenten in der Konfigurationsoberfläche



4. Funktionen / Konfiguration be.IP plus

swizzconnexx

Dokument Inbetriebnahmehilfe

Das Dokument beschreibt für die erste Inbetriebnahme kurz und übersichtlich mit entsprechenden Bildern und Grafiken die folgenden Konfigurationsschritte mittels den Assistenten:

1. Zugriff erstellen auf Konfigurationsoberfläche
2. IP-LAN Konfiguration
3. Internet WAN Zugang, falls be.IP plus auch als Gateway-Router eingesetzt wird.
4. Telefonie Konfiguration