Olaf Zäncker
VoIP Consulting & Services

CheckList **VoIP-Monitor und TAP**

Version 0.96, deutsch

von

Dipl.-Ing. (TU) Olaf C. Zäncker

29. September 2020

All rights reserved 'Olaf Zäncker VoIP Consulting & Services'

Kommentare oder Bemerkungen bitte per eMail an oz@oz-voip.com

Copyright Olaf C. Zäncker, 2009-2020

1 Vorbemerkung

Diese Checkliste ist als Hilfsmittel zur Vorbereitung von passiven Messungen (VoIP-Troubleshooting, VoIP-Abnahmemessung, VoIP-Statusmessung, Auslastungs- / Protokoll- und Bandbreitenmessung, o.ä.) gedacht und fasst sämtliche relevanten Informationen zusammen.

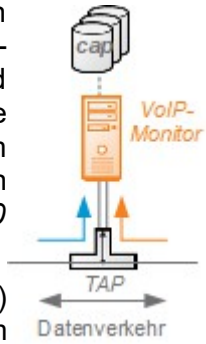
Solche Messungen sollten im Interesse aussagekräftiger, praktisch relevanter Ergebnisse die Dauer von einer Woche (24 / 7) nicht unterschreiten. Damit sind dann alle potentiellen tageszeitlich und / oder wochentäglich bedingten Abhängigkeiten der relevanten Parameter abgedeckt.

Die besonders wichtigen Abschnitte sind rot markiert !

2 Vor Messbeginn benötigte Angaben

Ein Messpunkt besteht immer aus einer Kombination von TAP (Test Access Port; Hersteller: Comcraft) und VoIP-Monitor Server (Hersteller: SuperMicro in individueller Konfiguration).

Die TAPs (Test Access Ports) dienen lediglich der performanten, störungsfreien Ankopplung der VoIP-Monitore durch Einschleifen in die zu messende IP-Verbindung. Darüber hinaus besitzen sie keine weitere Funktion. Sie sind vollkommen transparent und benötigen keine eigene IP-Adresse. Nähere Informationen zur Funktion und zum Umgang mit TAPs können bei Bedarf dem Dokument '*How to … use TAPs.pdf*', sowie den Original-Datenblättern '*Comcraft C1P-1G Datasheet_en.pdf*' (Kupfer) bzw. '*Comcraft F1PL-E-50 Datasheet_en.pdf*' (LWL) entnommen werden.



Bei den VoIP-Monitoren handelt es sich um mit Dual-Port Interface-Karte (NIC) ausgestattete Linux-Server (in nebenstehender Skizze in orange dargestellt) zum richtungsbezogenen Aufzeichnen der Messdaten.

*Achtung ! Die in diesem Hauptabschnitt beschriebenen technischen Sachverhalte (**Übertragungsgeschwindigkeit, physikalisches Medium, Steckertyp und Verschlüsselung**) **müssen** zur Planung der Messung **vorab kundenseitig geklärt werden**.*

2.1 Anzahl der Messpunkte

Im Interesse größtmöglicher Aussagekraft der Ergebnisse gilt grundsätzlich, je mehr Messpunkte (und damit Messdaten), um so besser. Maßgeblich ist jedoch immer deren im Angebot festgelegte Anzahl.

	1 GB		10 GB	Tiefe [mm]	Leistung [W]
	Cu	LWL	Cu		
TAPs	9	2 *SM*			
		3 *MM*			
VoIP-Monitore, Intel Dual-Port NIC	2 *a)*			503	440
	1 *a)*			356	260
	6			249	200

MM = 50µ Multimode (850 nm), SM = 9µm Singlemode (1310 nm)
Split-Ratio LWL-TAPs 50 : 50
Bei LWL-Betrieb: a) = MM oder SM

Insgesamt sind max. 9 Messpunkte (6 + 1 + 2 VoIP-Monitor Server) verfügbar, wobei sechs davon

(gemäß vorstehender Tabelle) über eine feste Konfiguration (1 GB Kupfer) verfügen, während sich drei weitere durch Austausch der Dual-Port Network Interface-Karten (NIC) wahlweise mit Kupfer (Übertragungsgeschwindigkeit beachten !) oder Glasfaser ausstatten lassen.

Die größere Zahl von insgesamt 14 TAPs (9 x Cu, 3 x Multimode, 2 x Singlemode) ermöglicht die flexible Anpassung an die jeweilige projektspezifische Konfiguration der VoIP-Monitor Server.

2.2 Übertragungsgeschwindigkeit (Link Speed)

Pro Messpunkt ist die Übertragungsgeschwindigkeit der zu untersuchenden IP-Verbindung anzugeben. Es sind zwei Arten von Messpunkten verfügbar - 1 GB oder 10 GB, die jeweils abwärtskompatibel sind.

2.2.1 10 GB Kupfer-Verbindungen

Für 10 GB Kupfer-Verbindungen stehen keine TAPs zur Verfügung. In solchen Fällen müssen ausnahmsweise kundenseitig Mirror-Ports konfiguriert werden – um potentielle Bottlenecks zu vermeiden, idealerweise pro Übertragungs*richtung* der zu untersuchenden IP-Verbindung je ein Mirror-Port.

2.3 Physikalisches Übertragungsmedium

Das physikalische Übertragungsmedium der zu untersuchenden IP-Verbindung kann entweder:

- Kupfer
- Glasfaser
  - Multimode-Glasfaser (50 µm), 850 nm Wellenlänge
  - Single- (bzw. Mono-) mode Glasfaser (9 µm), 1310 nm Wellenlänge

sein.

Im Falle von WLAN / DECT over IP werden die Messpunkte üblicherweise an der LAN-Seite der betreffenden Access-Points platziert.

2.4 Steckertypen der IP-Verbindungen

Das Einschleifen von TAPs (Cu, LWL) setzt das Vorhandensein regulärer Patchkabel voraus (kein Direct Attach !).

Bei Kupfer-Verbindungen ist RJ45 der Standard, bei LWL-Verbindungen der LC-Stecker. Weisen die zu messenden IP-Verbindungen im Falle von LWL andere Stecker auf, müssen entsprechende Adapterkabel verwendet werden.

2.5 (Nicht-) Verwendung von Mirror-Ports

Mirror-Ports sind latente Fehlerquellen ! Das ist darauf zurückzuführen, dass der Prozess der Replikation von Messdaten gegenüber der eigentlichen Aufgabe (Switching) mit untergeordneter Priorität ausgeführt wird. In Folge dessen kann es im replizierten Verkehr zu Pseudo-Verlusten (Packet Loss) kommen, die in der Realität jedoch so nicht auftreten. Dieser Sachverhalt wird bei „normalem“ Datenverkehr i.d.R. nicht bemerkt. Im Falle von VoIP-Troubleshooting oder VoIP-Abnahmemessungen wären solche Effekte jedoch fatal.

Ein weiterer entscheidender Nachteil ist der deutlich erhöhte Aufwand bei der Auswertung durch

die Mischung beider Übertragungsrichtungen.

Aus diesem Grund sollten Mirror-Ports nur in gut begründeten Ausnahmefällen (z.B. 10 GB Kupfer) Verwendung finden.

2.6 Verschlüsselung

Die für VoIP relevanten Protokolle (bzw. Datenströme)

- *Media-Verkehr*: RTP (Realtime Transport Protocol, RFC 3550 / 3551)
- *Signalisierung*: SIP (Session Initiation Protocol, RFC 3261) oder alternativ H.323 (ITU-T H.323)

werden in den meisten Fällen unverschlüsselt übertragen. Es gibt jedoch VoIP-Systeme, bei welchen die Datenströme teilweise oder vollständig verschlüsselt sind.

Die Auswertung (Analyse, Diagnose, Korrelation, Verifikation, etc.) der VoIP-Datenströme erfolgt zunächst immer auf Paket-Ebene, in einigen Fällen jedoch zusätzlich auch auf inhaltlicher Ebene (Payload). Dementsprechend ist die genaue Differenzierung der jeweils verwendeten Verschlüsselung wichtig, um eventuelle Einschränkungen der Auswertung beurteilen, und / oder alternative Messpunkte auswählen zu können. Nachfolgend werden die gängigsten Formen der Verschlüsselung kurz erläutert.

2.6.1 Secure RTP (RF 3711)

Der RFC 3711 definiert die Verschlüsselung der RTP-Payload (Sprache, Video), lässt den RTP-Header jedoch außen vor, so dass die RTP-Pakete weiterhin als solche identifiziert werden können. Damit lassen sich nach wie vor sämtliche Auswertungen auf Paket-Ebene (Erkennung von Packet Loss, Sequenzfehlern, Jitter, Store & Forward, etc.) in vollem Umfang durchführen, was für die meisten Anwendungsfälle (Analyse qualitativer Störungen) absolut ausreichend ist.

2.6.2 Verschlüsselung der Signalisierung

Bei dieser Variante ist die Signalisierung (also SIP, oder das ältere H.323) komplett (z.B. TLS) verschlüsselt, wobei im Falle von SIP sogar eine andere Portnummer als 5060 verwendet wird. Da eine sinnvolle Auswertung der Signalisierung immer auf deren Inhalte fokussiert, ist diese nun nicht mehr möglich.

Die eventuelle Verschlüsselung des RTP-Verkehrs, d.h. also Secure RTP (siehe vorhergehender Unterabschnitt) was dessen Auswertung auf Paket-Ebene immer noch möglich macht, ist davon völlig unabhängig.

2.6.3 Verschlüsselung des Gesamtverkehrs

Schließlich ist es noch möglich, den gesamten Datenverkehr (also nicht notwendigerweise begrenzt auf VoIP) zu verschlüsseln. Diese Methode findet z.B. auf WAN-Links zwischen Rechenzentren und Kundenstandorten Anwendung. Dabei werden alle Datenströme in verschlüsselte Container verpackt, so dass die VoIP-Pakete (RTP, SIP oder H.323) nicht einmal mehr auf Paket-Ebene erkannt werden können.

3 Technische Informationen zu den Messpunkten

*Achtung ! Die in diesem Hauptabschnitt beschriebenen technischen Sachverhalte (**insbesondere Einschleifen (und Entfernen) der TAPs**) **müssen** zur Planung der Messung **vorab kundenseitig geklärt werden**.*

3.1 Einbaugröße, Belüftung

Die VoIP-Monitor Server sind in 19“ Bauweise (1 HE) ausgeführt. Je nach Leistungsklasse besitzen diese eine Einbautiefe von 503 mm (keine Montageschienen verfügbar !), 356 mm bzw. 249 mm. Üblicherweise werden die VoIP-Monitor Server (insbesondere die mit 503 mm Einbautiefe) nicht fest installiert (eingeschraubt), sondern lediglich unter Benutzung freier Einbauplätze horizontal (!) auf vorhandene Geräte gelegt (siehe Tabelle im Abschnitt '*Anzahl der Messpunkte*').

Die Belüftung der VoIP-Monitor Server erfolgt jeweils über Front- und Rückseite, so dass keine zusätzlichen HE zur Belüftung freigelassen werden müssen.

Die Cu-TAPs besitzen eine Größe (BxTxH) von 11,3 x 13,3 x 3 cm (ältere Bauform) bzw. 11,3 x 12,3 x 3 cm (neuere Bauform) – die LWL-TAPs sind 11,3 x 9 x 3 cm (ältere Bauform) bzw. 11,3 x 8,5 x 3 cm (neuere Bauform) groß. Auf Grund ihres geringen, vernachlässigbaren Gewichts können speziell die Cu-TAPs sogar problemlos an den Anschlusskabeln hängen und erfordern daher keinen expliziten Einbauplatz. Belüftung ist für die TAPs nicht relevant.

3.2 Stromversorgung

3.2.1 Netzanschluss

Für die VoIP-Monitore sind wahlweise Anschluss-Schnüre mit Schuko-Stecker, oder Kaltgerätekupplung (IEC 60320) verfügbar. Bei Einsätzen im Ausland können auf Anfrage auch Anschluss-Schnüre für USA, UK bzw. Schweiz zur Verfügung gestellt werden.

Die Steckernetzteile der Cu-TAPs besitzen einen Eurostecker (EN 50075). Bei Einsätzen im Ausland ist ggf. ein Steckeradapter erforderlich.

LWL-TAPs bestehen hingegen nur aus Glasfasern – sie sind also rein passiv und benötigen folglich keine eigene Stromversorgung.

3.2.2 Adapter, Mehrfachsteckdosen

Um die Cu-TAPs auch bei Nicht-Vorhandensein von Schukosteckdosen betreiben zu können, stehen in begrenztem Umfang entsprechende Adapter (Schuko-Kupplung / Kaltgerätestecker) zur Verfügung.

Zusätzlich können 3-fach bzw. 6-fach Mehrfachsteckdosen (Profi-Equipment mit Metallgehäuse und ohne Ein- / Ausschalter, wie es auch zum Festeinbau in Datenschränken verwendet wird) eingesetzt werden.

3.2.3 Stromaufnahme

Bei den leistungsstärkeren VoIP-Monitoren ist von einer Stromaufnahme von ca. 350 .. 440 W

auszugehen, während die kleineren VoIP-Monitore lediglich eine Stromaufnahme von ca. 200 .. 260 W aufweisen (siehe Tabelle im Abschnitt '*Anzahl der Messpunkte*').

Die Leistungsaufnahme der Steckernetzteile der Cu-TAPs ist mit 12 W quasi vernachlässigbar.

3.3 Netzwerkzugang

Die VoIP-Monitor Server sind ausschließlich mittels ihrer Dual-Port NIC über die TAPs (jeweils entweder Cu oder LWL) mit dem Kundennetzwerk verbunden (siehe Skizze im Abschnitt '*Vor Messbeginn benötigte Angaben*'). Da die Dual-Port NIC im Promiscuous Mode arbeitet, zeichnet der VoIP-Monitor Server also nur Daten auf, sendet aber nicht in das Netzwerk.

3.3.1 Remote-Zugang

Für die VoIP-Monitor Server selbst wird kein Remote-Zugang benötigt – weder zum Administrieren, noch zum Download der Messdaten (wegen der üblicherweise großen / sehr großen Datenmengen ohnehin nicht praktikabel). Die Geräte verbleiben i.d.R. für eine Woche vor Ort, um autark Messdaten aufzuzeichnen und werden danach -mit den gespeicherten Messdaten- wieder ausgebaut.

3.3.2 NTP-Service

Auf die Verwendung eines NTP-Service für die VoIP-Monitor Server wird bewusst verzichtet, da hierfür eine explizite Verbindung mit dem Kundennetzwerk erforderlich wäre (siehe Abschnitt '*Netzwerkzugang*'). Statt dessen werden die VoIP-Monitor Server zum Messbeginn automatisch auf die Systemzeit des Admin-Laptops synchronisiert.

3.3.3 Einschleifen (und Entfernen) der TAPs

Das Einschleifen (und das i.d.R. nach einer Woche vorzunehmende Ausschleifen) der TAPs erfordert jeweils eine kurzzeitige Unterbrechung (< 5 Sekunden) der zu untersuchenden IP-Verbindung. Diese Maßnahme ist kundenseitig zu planen (ggf. Wartungsfenster) und kann auf Wunsch auch außerhalb der (Kern-) Arbeitszeit durchgeführt werden. Alternativ ist es möglich, die TAPs rechtzeitig vor Messbeginn bereitzustellen, so dass der Kunde / Auftraggeber das Einschleifen nach ausführlicher (!) schriftlicher Anleitung in Eigenregie vornehmen kann.

Cu-TAPs sind vollkommen transparent und unterbrechen die IP-Verbindung in die sie eingeschleift sind auch bei Ausfall des Steckernetzteils nicht. Lediglich das Replizieren der Messdaten wäre in so einem Fall nicht mehr möglich.

LWL-TAPs hingegen bestehen lediglich aus LWL-Fasern, die zwischen der zu messenden Verbindung und den Monitor-Ports aufgeteilt sind. Man spricht dabei von der sog. Split-Ratio. Die eingesetzten LWL-TAPs besitzen sämtlich eine Split-Ratio von 50 : 50 – reduzieren die Lichtleistung auf der zu messenden IP-Verbindung also auf die Hälfte, was für Verbindungen im Gebäude- bzw. Campusbereich jedoch i.d.R. völlig ausreichend ist.

3.4 Parametrisierung der Datenaufzeichnung

Der Capture-Prozess auf den VoIP-Monitor Servern kann mittels zweier voneinander unabhängiger Kenngrößen (Capture-Limit, Capture-Filter) an die jeweilige Aufgabenstellung / das zu untersuchende Fehlerbild angepasst werden.

3.4.1 Capture-Limit

Mittels des Capture-Limit kann die Länge der aufgezeichneten Messdaten begrenzt werden, um sensible Inhalte (Payload; im Fall von RTP also die Sprache) von vorn herein von der Aufzeichnung auszunehmen. Standardmäßig ist ein Capture-Limit von 60 Byte konfiguriert. Das Capture-Limit wirkt dabei immer auf die gesamte Aufzeichnung. Im Fall der Signalisierung (z.B. SIP) hat das zur Folge, dass die betreffenden Datenpakete an Hand ihrer (UDP oder TCP) Port-Nummern zwar noch als SIP-Pakete erkannt werden, auf Grund des Fehlens der Payload (SIP-Inhalte) jedoch nicht mehr auswertbar sind (Auswertung auf Paket-Ebene).

In Abstimmung mit dem Kunden und nur mit dessen ausdrücklicher schriftlicher Zustimmung (!) kann in Ausnahmefällen auf das Capture-Limit verzichtet werden. Das ist u.a. dann notwendig, wenn die Analyse / Diagnose von funktionalen Störungen (Steuerung der Verbindung, d.h. SIP) oder von Beeinträchtigungen auf inhaltlicher (Sprach-) Ebene (einseitige Verbindungen, Hall, Echo, usw.) gewünscht wird.

Wenn nicht explizit anders vereinbart, wird immer mit 60 Byte Capture-Limit gemessen.

Achtung ! Bei dem Verzicht auf das Capture-Limit ist zu beachten, das bei gleichzeitigem Verzicht auf Capture-Filter (siehe nachfolgender Unterabschnitt) die Menge der Messdaten drastisch ansteigen kann, so dass die Aufzeichnungskapazität der VoIP-Monitor Server (i.d.R. 1 TB Festplatte) bereits vor Ende der geplanten Messdauer erschöpft sein kann.

3.4.2 Capture-Filter

Capture-Filter ermöglichen es, die Aufzeichnung der Messdaten nach unterschiedlichsten Kriterien bzw. einer Kombination daraus (z.B. Protokolle, Adressen, ...) selektiv zu gestalten. Capture-Filter sollten möglichst einfach (performant) gestaltet sein, um die Genauigkeit der Capture-Timestamps (Mess-Zeitstempel) bei der Aufzeichnung der Messdaten nicht negativ zu beeinflussen.

Standardmäßig ist ein Capture-Filter '*udp or (udp and vlan) or port5060 or (port5060 and vlan)*' konfiguriert. UDP sorgt für die Aufzeichnung des RTP- (VoIP Media-) Verkehrs, während Port 5060 auf SIP (unabhängig davon, ob mittels UDP oder TCP übertragen) anspricht.

Insbesondere dann, wenn auf Grund der Aufgabenstellung auf das Capture-Limit verzichtet werden muss, bieten Capture-Filter die Möglichkeit der selektiven Messdatenerfassung (z.B. unter Verwendung von IP-Adresslisten und / oder Angabe von Protokollen / Portnummern).

Der große Vorteil bei der Messung ohne Capture-Filter (idealerweise in Kombination mit Capture-Limit) besteht jedoch darin, den Gesamtverkehr zu erfassen. Das ermöglicht insbesondere bei Störungen des VoIP-Verkehrs, potentielle Zusammenhänge mit dem Niveau des non-VoIP Verkehrs (z.B. Lastspitzen) erkennen zu können. Darüber hinaus lassen sich so auch Sachverhalte wie z.B. Broad- / Multicasts, Fragmentierungen, (gehäufte) TCP-Retransmissions oder ICMP-Meldungen, FlowControl-Meldungen, -um nur einige Effekte exemplarisch zu nennen- auswerten.

Wenn nicht explizit anders vereinbart, wird immer ohne Capture-Filter gemessen.

Achtung ! Bei dem Verzicht auf Capture-Filter ist zu beachten, das bei gleichzeitigem Verzicht auf das Capture-Limit (siehe vorhergehender Unterabschnitt) die Menge der Messdaten drastisch ansteigen kann, so dass die Aufzeichnungskapazität der VoIP-Monitor Server (i.d.R. 1 TB Festplatte) bereits vor Ende der geplanten Messdauer erschöpft sein kann.

4 Auswahl geeigneter Messpunkte

Messpunkte können grundsätzlich überall dort in IP-Umgebungen installiert werden, wo ein regulärer Ethernet-Protokollstack benutzt wird (z.B. MAC, VLAN, IP, TCP/UDP, ... oder MAC, PPPoE, IP, TCP/UDP, ...).

Dabei gilt bei VoIP-Messungen die Prämisse, dass all jene IP-Verbindungen interessant sind, auf denen unverschlüsselter RTP-Verkehr oder S-RTP (Secure-RTP) gemäß RFC 3711 (bei letzterem kann lediglich die Payload nicht untersucht werden) übertragen wird, da dieser später Gegenstand detaillierter Auswertungen ist. Das erfordert die Kenntnis des CallFlows der zu untersuchenden VoIP-Umgebung. Reine SIP-Komponenten (z.B. Registrar, Proxies) sind hingegen nur dann von Interesse, wenn funktionale Störungen im Bereich der Signalisierung analysiert werden sollen.

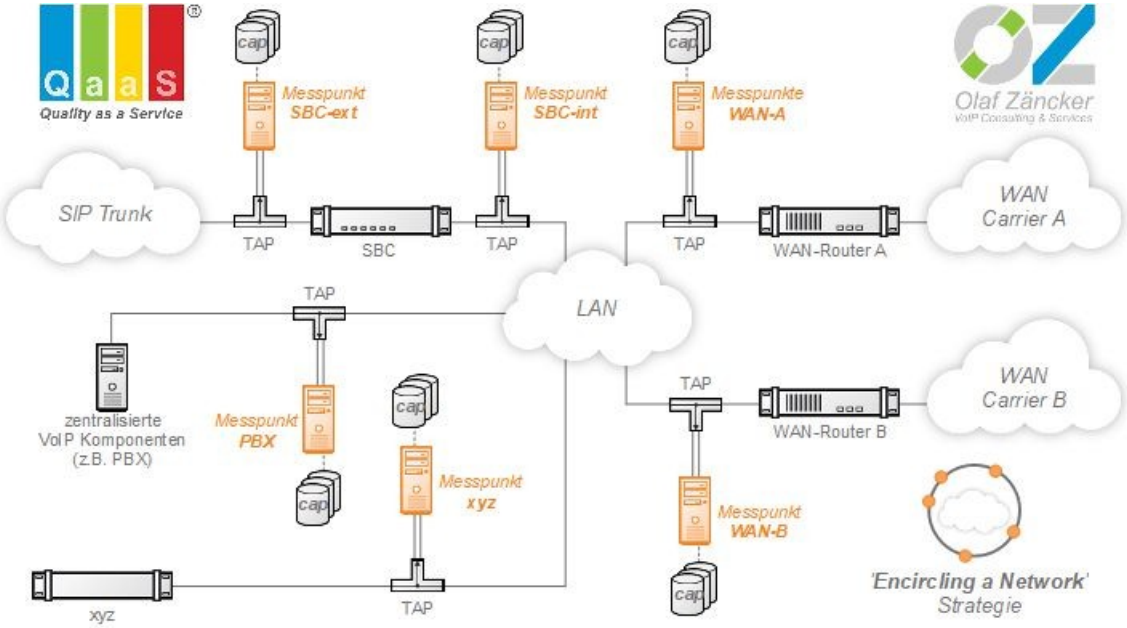
Bandbreiten- und Protokollmessungen fokussieren sich für gewöhnlich auf WAN-Verbindungen (Router).

4.1 Mess-Strategien

Unabhängig von den konkreten Bedingungen an den Messpunkten (Übertragungsgeschwindigkeit, physikalisches Medium, etc.) haben sich in der täglichen VoIP Mess-Praxis hauptsächlich die beiden nachfolgend beschriebenen Mess-Strategien als vorteilhaft herauskristallisiert, wobei es im konkreten Anwendungsfall durchaus zu gemischten Szenarien kommen kann.

4.1.1 '*Encircling a Network*' Strategie

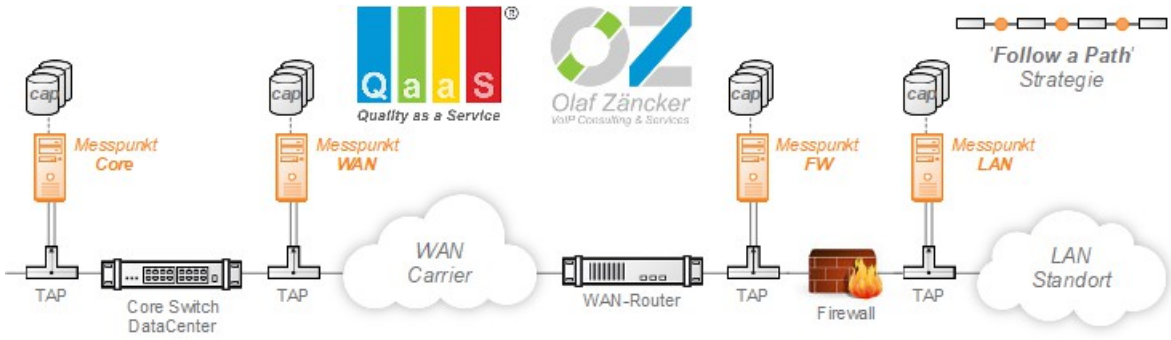
Bei dieser, besonders für LANs konzipierten Strategie '*Encircle a Network*' besteht das Ziel darin, von möglichst vielen unterschiedlichen Messpunkten („Winkeln“) aus einen messtechnischen „Blick“ auf das Netzwerk werfen zu können.



Wegen der richtungsbezogenen Erfassung von Messdaten (TAP) sind dabei zunächst die *aus* Richtung Netzwerk kommenden Datenströme interessant, da sie über dessen Zustand Aufschluss geben. Selbstverständlich werden aber auch die *in* Richtung LAN verlaufenden Datenströme ausgewertet, da sie (zumindest potentiell) auch gestört sein können.

4.1.2 '*Follow a Path*' Strategie

Die Idee hinter der '*Follow a Path*'-Strategie ist, RTP-Streams entlang eines Übertragungsweges an mehreren Messpunkten erfassen (und vergleichen) zu können, wobei der einfachste Fall (2 Messpunkte) in einer „Zangenmessung“ (z.B. beidseitig einer WAN-Verbindung, beidseitig einer Firewall oder beidseitig eines SBCs) besteht.



4.2 Beispiele typischer Messpunkte

Nachfolgend wird eine exemplarische Auswahl möglicher (situativ bewährter) Messpunkte vorgestellt. IP-Verbindungen mit einem hohen Anteil an RTP-Verkehr ist im Fall von VoIP-Messungen im Vergleich zu einzelnen VoIP-Endgeräten grundsätzlich immer der Vorzug zu geben, jedoch richtet sich die -u.U. sehr individuelle- Mess-Konfiguration eines Projektes immer nach der konkreten, teils sehr speziellen Aufgabenstellung.

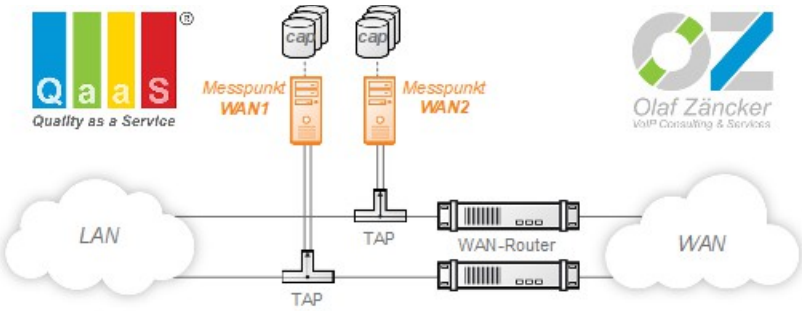
So ist gerade in größeren Projekten wegen der endlichen Verfügbarkeit von Messpunkten abzuwägen, ob z.B. im Fall redundanter Übertragungswege die passive Backup-Verbindung ggf. unberücksichtigt bleibt.

4.2.1 Virtualisierte Komponenten

Sobald Echtzeitverkehr über virtualisierte Komponenten übertragen wird, entstehen potentielle Schwachstellen. Das gilt für reine VoIP-Komponenten (z.B. SBCs) ebenso, wie z.B. für Firewalls. Dabei besteht die Herausforderung oft darin, dass ein virtuelles Cluster auf mehreren physikalischen Maschinen mit performanten Interfaces (10 GB) läuft. Hier ist im Einzelfall abzuwägen, ob die zu untersuchenden Prozesse auf eine physikalische Maschine (und damit ein physikalisches Interface) gebunden werden (Veränderung der Normalkonfiguration), alle physikalischen Interfaces des Clusters überwacht werden (sehr hoher Aufwand für Messung und Auswertung), oder aber auf die unmittelbare Messung der virtuellen Umgebung verzichtet wird.

4.2.2 WAN-Router

WAN-Verbindungen in größeren Netzwerken verfügen ggf. über mehrere WAN-Router, welche wiederum mehr als ein LAN-seitiges physikalischen Port besitzen können. Dabei ist es wichtig, die aktiv Daten übertragenden LAN-Anschlüsse mit Messpunkten zu bestücken.

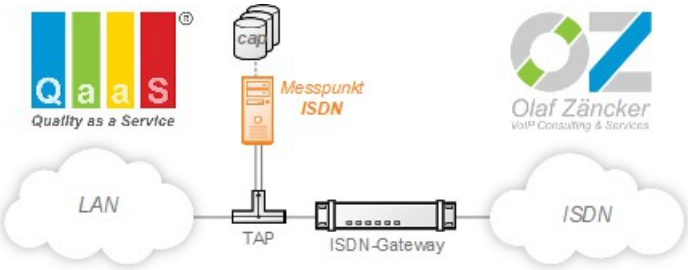


Bei den passiven Backup-Anschlüssen / -Routern kann hingegen -in Abwägung der Gesamtanzahl an Messpunkten- ggf. auf

eine Messung verzichtet werden – insbesondere dann, wenn nach Störungen vom Backup-Anschluss automatisch wieder auf die ursprüngliche (Haupt-) Verbindung zurück geschwenkt wird.

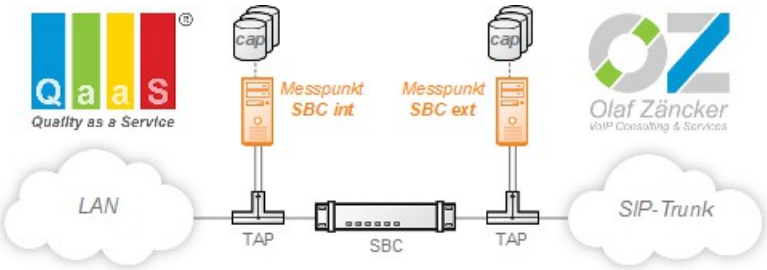
4.2.3 ISDN-Gateways

Bei ISDN-Gateways ist die Platzierung von Messpunkten sehr einfach – der TAP wird auf der LAN-Seite des ISDN-Gateways eingeschleift. Gibt es in einer VoIP-Umgebung mehr als ein ISDN-Gateway, ist jedes mit einem Messpunkt auszustatten.



4.2.4 SBCs (Session Border Controller) und Firewalls

Für Session Border Controller sind unterschiedliche Ausführungen (virtualisiert / dediziert, 1 oder 2 physikalische Ports) und Betriebsarten (transparent / Transcoding) bekannt. Nachfolgend ist die gebräuchlichste Form eines dedizierten Gerätes mit je einem physikalischen Ein- und Ausgang skizziert.

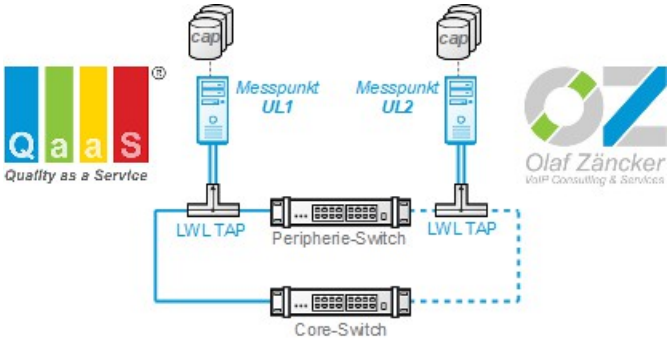


Auf Grund der Tatsache, dass Störungen bereits über den SIP-Trunk eingetragen werden können und SBCs im Zuge des Transcodings solche Störungen teilweise manipulieren, ist bei SBCs die beidseitige („Zangen-“) Messung immer ratsam.

Im Fall von Firewalls liegen die Verhältnisse in Bezug auf Ausführung und Betriebsarten ähnlich, so dass auch hier nach Möglichkeit immer beidseitig gemessen werden sollte.

4.2.5 Uplinks

Uplinks zwischen Core-Switch und Peripherie bestehen i.d.R. aus zwei redundanten LWL-Verbindungen, von denen eine oft passiv bleibt. In solchen Fällen ist es im Interesse der Einsparung von Messpunkten durchaus sinnvoll, in Abstimmung mit den Kunden / Auftraggeber für die Dauer der (zeitlich begrenzten) Messung auf das Backup zu verzichten (gestrichelte Linie).



Im Zusammenhang mit der Messung von LWL-Verbindungen wird nochmals auf den Sachverhalt der (im Campus-Bereich jedoch im Allgemeinen unkritischen) Split-Ratio (z.B. 50 : 50) von LWL-TAPs hingewiesen.

4.2.6 User

Die Messung an einzelnen Usern ist (wenn es sich nicht gerade um Vermittlungsplätze oder CallCenter-Agenten handelt) im Allgemeinen wegen der durch sie üblicherweise sehr geringen generierten Datenmenge nur bedingt zu empfehlen.

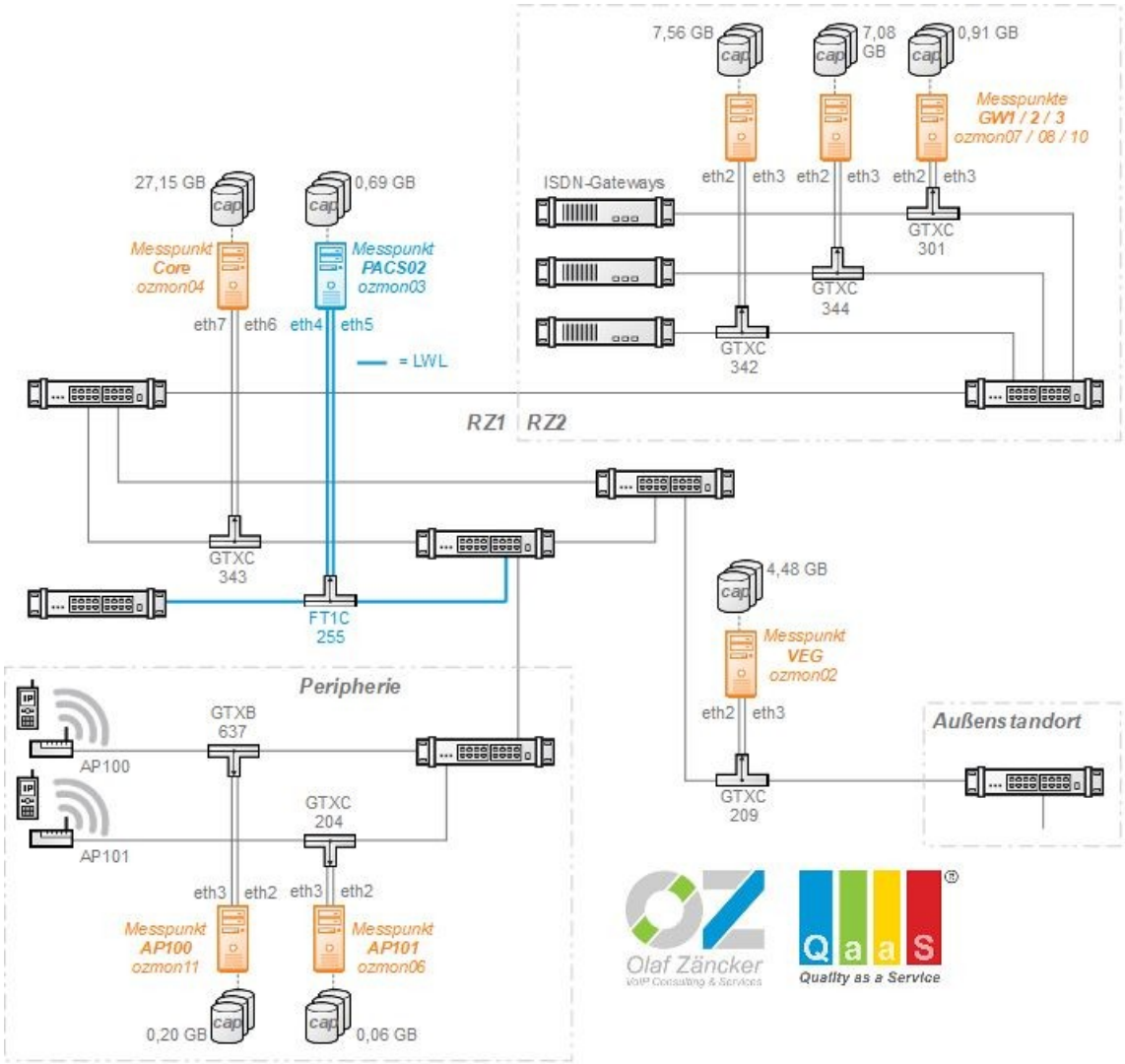
Sofern User jedoch reproduzierbar, oder überproportional häufig von Störungen betroffen sind, sollten sie mit einem Messpunkt ausgestattet werden. Ein weiterer Anwendungsfall ergibt sich bei VoIP-Abnahmemessungen, wo es sehr sinnvoll ist, zum Zwecke der Bestimmung des Broad- / Multicast Levels in der Netzwerk-Peripherie exemplarisch an einem User (IP-Phone oder PC mit SoftClient) einen Messpunkt zu platzieren.

4.2.7 Access-Points

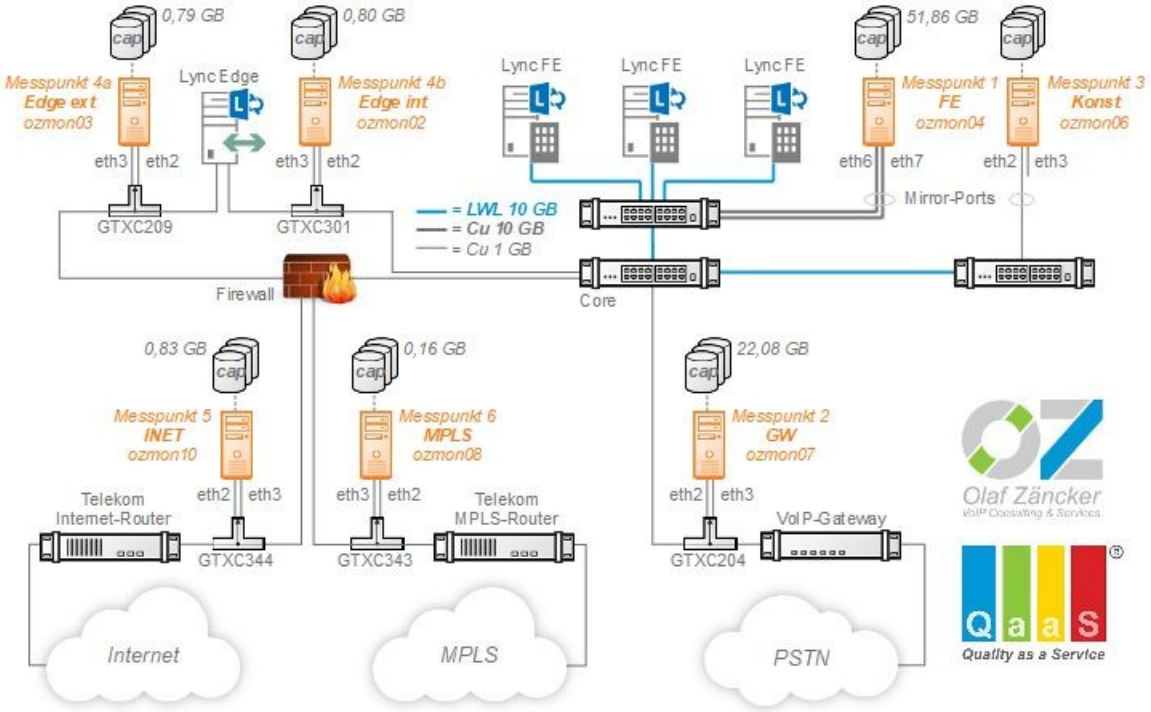
Im Fall von WLAN- oder DECT-Access Points wird der Messpunkt (ähnlich wie beim ISDN-Gateway) jeweils auf der LAN-Seite eingeschleift.

4.3 Exemplarische Mess-Szenarien aus der Praxis

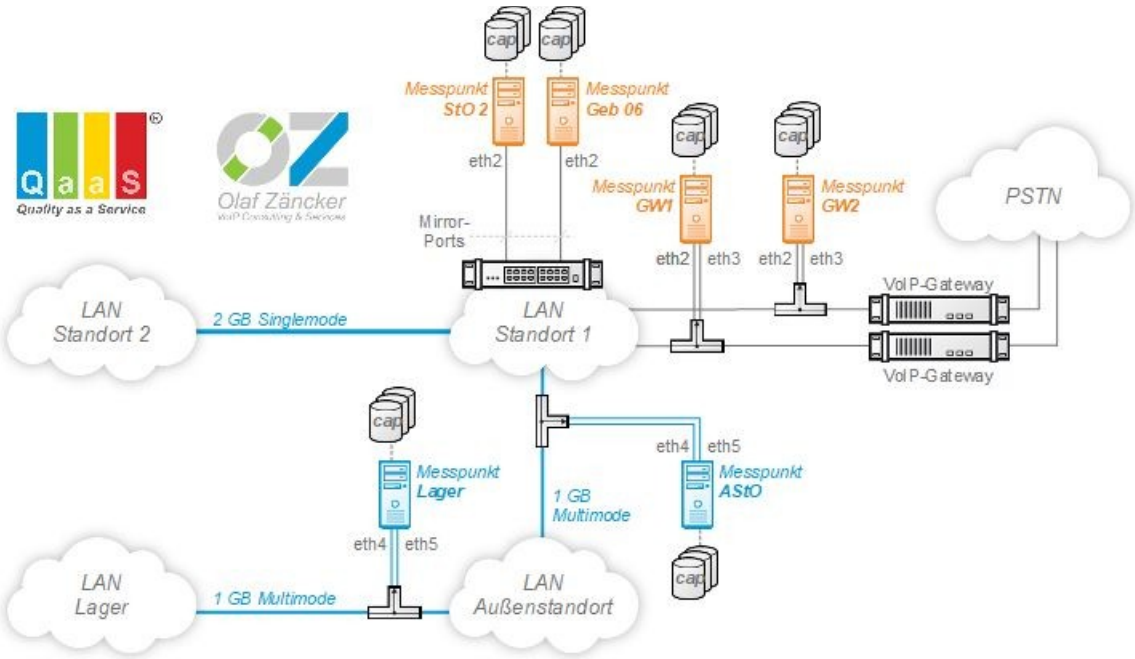
Das erste Beispiel zeigt ein Mess-Szenario mit VoWLAN Access-Points.



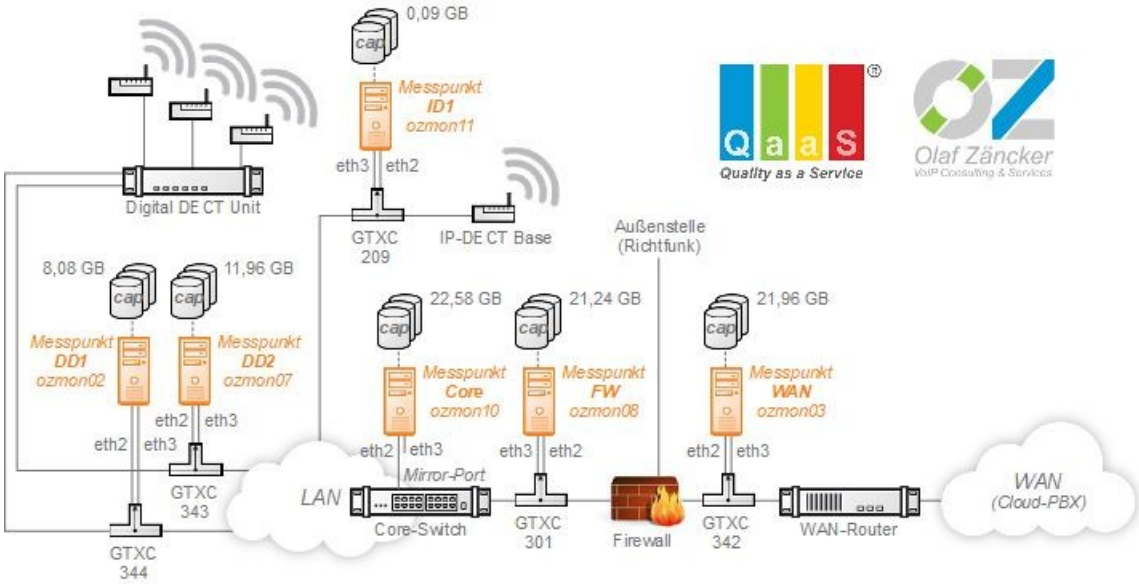
Kennzeichen des zweiten Beispiels ist die Microsoft Lync-Umgebung. Die drei FrontEnds wurden über 10 GB Kupfer Mirror-Ports gemessen, der Edge-Server war direkt zugänglich.



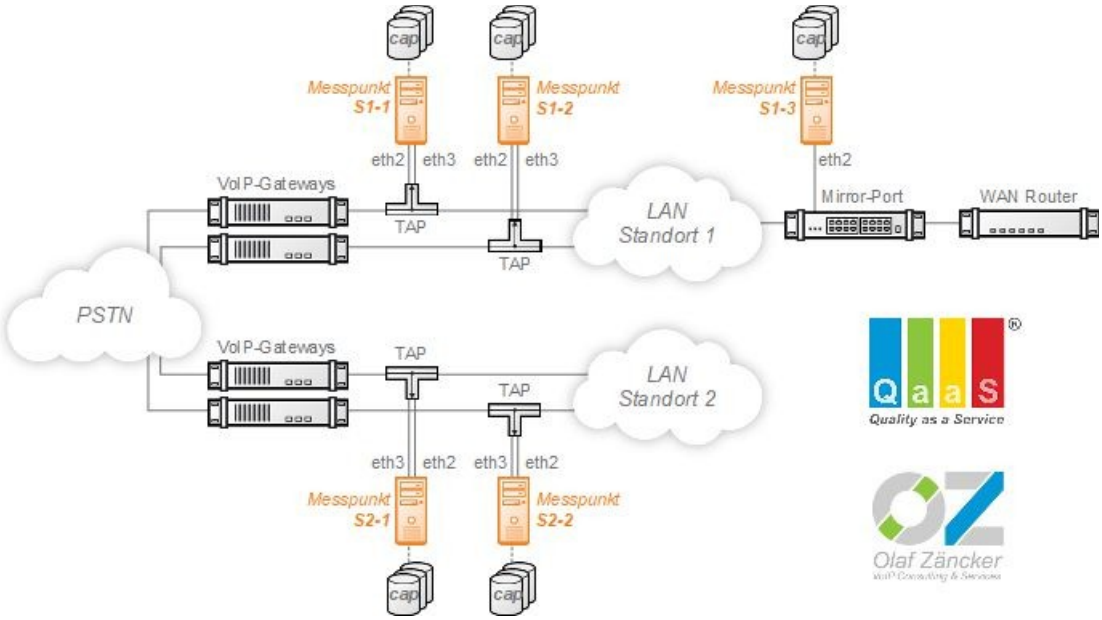
Im dritten Beispiel waren LWL-Messpunkte erforderlich. An zwei Stellen mussten Mirror-Ports verwendet werden.



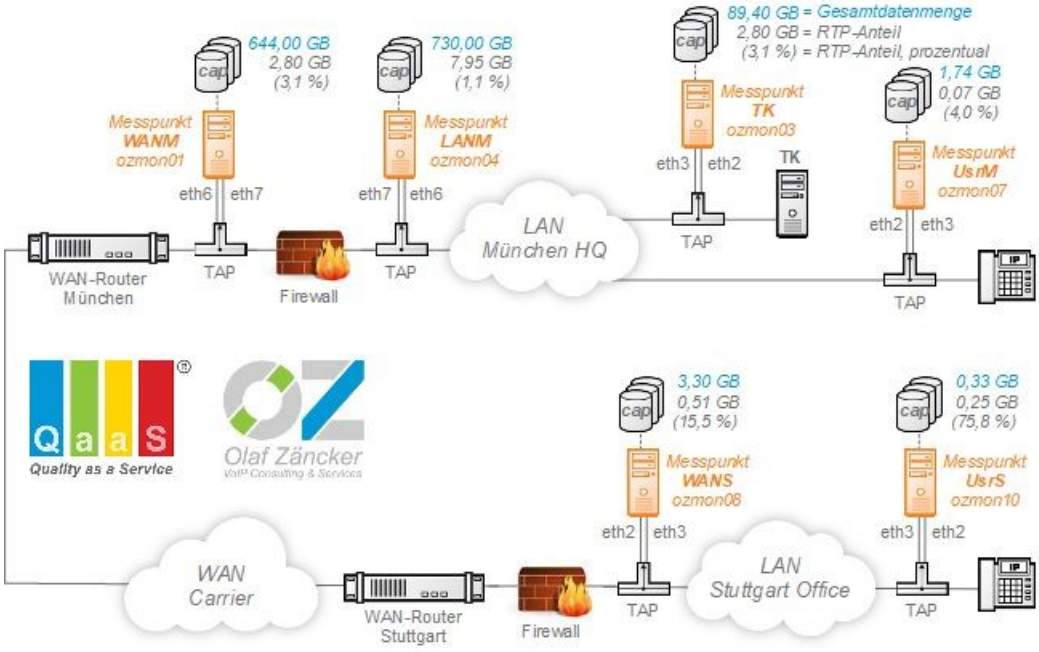
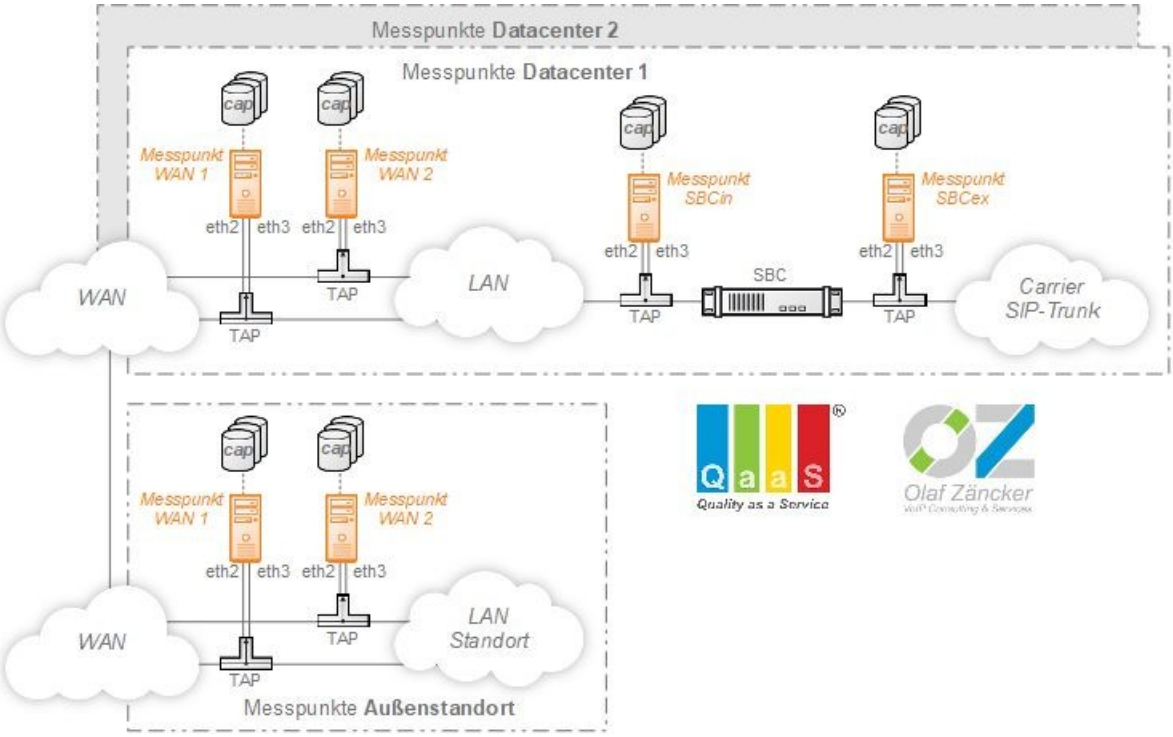
Beispiel vier (BBX Cloud-Service) zeichnet sich durch eine Vielzahl unterschiedlicher DECT Access-Points aus.



In Beispiel fünf waren wegen Störungen der externen Kommunikation mehrere VoIP-Gateways mit Messpunkten auszustatten.



Im Beispiel sechs ging es um die Analyse von Störungen am Außenstandort. Sinnvollerweise wurde der gesamte Übertragungsweg mit Messpunkten versehen.



In Beispiel sieben ging es um einen zentralisierten SBC, sowie zwei DataCenters.