Netzwerkanforderungen für VoIP

Anforderungen und Empfehlungen zur Realisierung von
Voice over IP und Voice over WLAN

Inhalt

1. Einleitung

Um im Rahmen von Unified Communications Lösungen eine optimale Übertragungsqualität von IP basierenden Diensten (Voice, Video und Realtime-Applikationen) über IP-Netzwerke (LAN, WAN, WLAN) und einen störungsfreien Betrieb gewährleisten zu können, haben wir für Sie in den folgenden Kapiteln die wesentlichen Anforderungen an Ihr zukünftiges oder bereits bestehendes Datennetzwerk zusammengefasst.

Die seitens Unify für OpenScape Applikationen definierten Anforderungen können grundsätzlich von allen Herstellern von Datennetzwerk-Komponenten bereitgestellt werden, da Unify OpenScape bei der Implementierung auf proprietäre Lösungen verzichtet und sich nach allgemein anerkannten Standards im Datennetzwerk bei der Realisierung Ihrer Lösung orientiert.

Falls Sie für die Analyse bzw. Herstellung der Tauglichkeit für Kommunikationsdienste (VoIP/VoWLAN-Readiness) Ihres Netzwerks Unterstützung benötigen, stellt Ihnen Atos im Rahmen der Projektvorbereitungsphase entsprechende Experten, Tools und Dienstleistungen zur Verfügung, damit Sie einen reibungslosen Betrieb der Kommunikations-Lösung in Ihrem Netzwerk sicherstellen können.

Atos ersucht um Ihr Verständnis, dass Fehler oder Nichtfunktionalitäten aufgrund der Nichterfüllung der VoIP/VoWLAN-Readiness gemäß diesem Dokument bzw. auf die darin verwiesene Systemdokumentation bei speziellen Anforderungen nicht anerkannt werden können.

Die in diesem Dokument genannten Parameter gelten, wenn sie nicht im Rahmen der Technical Design Specification Workshops in Abstimmung zwischen dem Kunden und Atos anders definiert werden.

Es ist die Einhaltung der in diesem Dokument definierten Vorgaben durch den Kunden zu gewährleisten.

Werden seitens des Kunden die in diesem Dokument definierten Vorgaben nicht eingehalten, kann daraus eine mangelhafte Funktionsweise der Unify OpenScape Systeme resultieren. Atos darf bei einem begründeten Verdacht den Nachweis der Einhaltung der in diesem Dokument definierten Vorgaben durch den Kunden mittels geeigneter Prüfprotokolle einfordern.

Bei Nichterfüllung der in diesem Dokument genannten Vorgaben werden daraus entstehende Mehraufwendungen seitens Atos gesondert in Rechnung gestellt.

Weitere Leistungen und Unterstützungen können erst nach Erfüllung der Vorgaben durch den Kunden erfolgen.

Atos unterstützt bei gesonderter Beauftragung seine Kunden gerne, die entsprechenden Leistungen und Voraussetzungen bereit- bzw. herzustellen.

2. Übertragung von Sprache

In diesem Kapitel sind die grundlegenden Parameter zur Übertragung von Sprache festgehalten.

2.1. Bandbreite

Die benötigte Bandbreite für Sprache muss im LAN- und WAN-Netzwerk im Bedarfsfall zu jeder Zeit zur Verfügung gestellt werden. Im LAN wird ein 100Mb full duplex Ethernetport für den Anschluss unserer Komponenten empfohlen. Bei Komponenten die 1Gb full duplex Ethernetports zur Verfügung stellen sind diese zu verwenden. Ethernetports für Hauptkomponenten (z.B. Server) sind fix „full duplex“ einzustellen.

Den nachstehenden Tabellen entnehmen sie bitte die Anforderungen an die Bandbreite.

Die angegebenen Werte der nachstehenden Tabellen (Abb. 1 und 2) beziehen sich auf den Layer 3 (IP). Die für den Layer 2 Header benötigte Bandbreite ist je nach verwendeten Layer 2 Protokollen unterschiedlich und in der Darstellung nicht berücksichtigt. Der Layer 2 Overhead ist auf den zu Grunde liegenden Verbindungen entsprechend zu berücksichtigen, sonst kann des zu Bandbreitenengpässen und daraus resultierenden Beeinträchtigungen der Systemfunktionen, z.B. Qualität der Sprachübertragung, kommen.

Die angegebenen Werte entsprechen der Übertragung der Voice-Payload und beinhalten somit den RTP als auch den RTCP Traffic. Signalling ist zusätzlich zu berücksichtigen. Als Richtwert wird hier bis zu 1kbps je Phone angenommen.

Die Komprimierung von Sprache (z.B. G.729) hat einen wesentlichen Einfluss auf deren Qualität. Eine stärkere Komprimierung bedingt eine schlechtere Sprachqualität. Bei bestimmten Gesprächstypen (z.B. für die Vermittlung, ContactCenter Agents oder Music on Hold) wird aus Sprachqualitätsgründen empfohlen keine Komprimierung zu verwenden. Die auf einer Strecke benötigte Mindestbandbreite ergibt sich aus der Anzahl der geforderten gleichzeitigen Gespräche und der jeweiligen Kompressionsrate. Dies kann bei einer Netzwerkanalyse entsprechend simuliert werden. Die Realisierung einer RTP- Verschlüsselung erhöht die erforderliche Bandbreite entsprechend.

Codec	Codec Bit Rate (kbps)	Packetization Intervall (ms)	Required Bandwidth (kbps)	Number of calls possible for a given link speed		
				300 kpps	1Mbps	2Mbps
G.711	64-	10	99,84	3	10	20
		20	83,20	3	12	24
G.722	64-	10	99,84	3	10	20
		20	83,20	3	12	24
G723.1	6,4	30	17,75	16	56	112
		60	12,203	24	81	163
G.729	8	10	41,60	7	24	48
		20	24,96	12	40	80

Tabelle 1: Bandbreitenanforderungen ohne RTP Verschlüsselung für Audio

Codec	Codec Bit Rate (kbps)	Packetization Intervall (ms)	Required Bandwidth (kbps)	Number of calls possible for a given link speed		
				300 kpps	1Mbps	2Mbps
G.711	64	10	108,16	2	9	18
		20	87,36	3	11	22
G.722	64	10	108,16	2	9	18
		20	87,36	3	11	22
G723.1	6,4	30	20,52	14	48	97
		60	13,589	22	73	147
G.729	8	10	49,92	6	20	40
		20	29,12	10	34	68

Tabelle 2: Bandbreitenanforderungen mit RTP Verschlüsselung (SRTP) für Audio

2.2. Verzögerung (Delay)

Nachfolgende Tabelle stellt die Sprachqualität in Abhängigkeit von Delay, Jitter und Paketverlustrate dar. Die Werte beziehen sich auf die End-to-End Sprachverbindung, also inklusive aller Kommunikations- und Übertragungseinrichtungen.

Verzögerung (ms)	Paketverlustrate in %						
	< 1%	1%	1,5%	2%	2,5%	3%	> 3%
50	0	4	6	8	10	12	30
100	0	4	6	8	10	12	30
150	0	4	6	8	10	12	30
200	3	7	9	11	13	15	33
250	10	14	16	18	20	22	40
300	15	19	21	23	25	27	45
350	20	24	26	28	30	32	50
400	25	29	31	33	35	37	55

Tabelle 3: Sprachqualität in Abhängigkeit von Delay und Paketverlustrate

- Sehr gute Sprachqualität
- Gute Sprachqualität
- Akzeptable Sprachqualität
- Inakzeptable Sprachqualität

Damit den Gesprächsteilnehmern eine Sprachverbindung natürlich erscheint, soll die Verzögerung (Network-Delay) 50 ms (One-Way-Delay bzw. Network-Delay) nicht überschreiten. Die Verzögerung lässt sich durch Prioritätensteuerung im Netzwerk reduzieren. Bei der Betrachtung End-to-End darf die Verzögerung den Maximalwert von 150 ms nicht überschreiten (Roundtrip-Delay) um gute Sprachqualität gewährleisten zu können.

Das Serialisierungs-Delay auf Verbindungen geringer Bandbreite hat ebenfalls Einfluss auf die Übertragungsqualität. Folgende Tabelle stellt einen Überblick über das Serialisierungs-Delay bei den hauptsächlich von Kunden verwendeten Leitungsgeschwindigkeiten dar.

Referenzwerte für Serialisierungs-Delay					
Link Speed	64 kbps				
Frame (#Byte)	1500	1024	512	256	128
Ms	187,5	128	64	32	16
Link Speed	128 kbps				
Frame (#Byte)	1500	1024	512	256	128
Ms	93,8	64	32	16	8
Link Speed	256kbps				
Frame (#Byte)	1500	1024	512	256	128
Ms	46,9	32	16	8	4
Link Speed	512 kbps				
Frame (#Byte)	1500	1024	512	256	128
Ms	23,4	16	8	4	2
Link Speed	1024 kbps / 1 Mbps				
Frame (#Byte)	1500	1024	512	256	128
Ms	11,7	8	4	2	1
Link Speed	2048 kbps / 2 Mbps				
Frame (#Byte)	1500	1024	512	256	128
Ms	5,9	4	2	1	0,5
Link Speed	10 Mbps				
Frame (#Byte)	1500	1024	512	256	128
Ms	1,2	0,8	0,4	0,2	0,1

Tabelle 4: Referenzwerte für Serialisierungs-Delay

Einen weiteren Einflussfaktor auf die Übertragungsqualität bildet das Queueing Delay in den Übertragungskomponenten (Router, Switches, etc.), vorallem beim Übergang auf Übertragungsstrecken mit geringerer Bandbreite. Da das Queueing Delay von den eingesetzten Komponenten und verwendeten Mechanismen abhängt, wird an dieser Stelle auf die Herstellerdokumentation der eingesetzten Komponenten verwiesen.

2.3. Maximale Paketverluste

Die Paketverluste dürfen max. 1% unter der Annahme der statistischen Verteilung betragen. Dabei ist zu beachten, dass bei einem Verlust von mehr als zwei aufeinander folgenden Sprachpaketen (consecutive packet lost), die Sprachqualität merklich beeinträchtigt wird. Die mit Paketverlusten verbundenen Sprachqualitätseinbußen sind bei stark komprimierenden Codecs (z.B. G.729) größer als bei G.711. Die Anforderungen bei Fax- und Modem-Übertragung sind im Kapitel „Übertragung von Fax und Modem“ beschrieben.

2.4. Jitter

Einer der kritischsten Parameter in der Beschreibung der Netzwerkgüte ist die Verzögerungsvarianz (Jitter). Jitter beschreibt die unregelmäßigen Abweichungen der Übertragungszeit. Diese Verzögerungsvarianz wird durch einen Jitter Buffer im VoIP-Endgerät bis zu einem gewissen Grad ausgeglichen. Es ist zu vermeiden, dass der Jitterbuffer die max. Verzögerung von 50 ms (Networkdelay) bzw. 150 ms (End-to-End) überschreitet.

3. Übertragung von Fax und Modem

Bei der Übertragung von Fax und Modem mit G.711 sollten die Werte für Delay, Packet Loss und Jitter Null sein um eine einwandfreie Übermittlung aufgrund der Sensibilität der Endsysteme zu gewährleisten.

Basierend auf Erfahrungswerten werden bei einem Delay von 50ms, Jitter von 20ms, einem PacketLoss von 0,5% bei einem non-consecutive PacketLoss von maximal 2, wobei eine mindestens consecutive Packet Transfer Rate von 8 benötigt wird, gute Übertragungsergebnisse erzielt werden.

Ab einem concecutive PacketLoss von 3 wird die Fax-Übertragung abgebrochen.

Für Fax-Übertragung ist maximal 9.600 bps zu verwenden.

T.38 zur Übertragung von Fax steht alternativ zu G.711 zur Verfügung. Bei der Übertragung mit T.38 gelten die gleichen Qualitätsparameter für Delay, Jitter und Packet Loss wie bei der Übertragung mit G.711.

4. Übertragung von Video

Auch hier gelten erstmal die Angaben der Beschreibung für Sprachübertragung. Jedoch werden für die Übermittlung der Videodaten andere Codecs (z.B. H.264) verwendet. Desweiteren spielen bei der Berechnung der Bandbreite weitere Faktoren wie zum Beispiel die Bildwiederholrate (FRPS) sowie die Auflösung eine große Rolle.

Die angebotenen Systeme handeln die verwendeten Daten beim Verbindungsaufbau aus. Somit ergibt sich für eine Peer-to-Peer Videokonferenz eine Bandbreite von ca. 1Mbps bei HD Qualität, oder zwischen 384 kbit/s und 1,5 Mbps je nach Abstimmung der obig genannten Faktoren.

Folgende Parameter können zur die Bandbreiten Kalkulation für Video Streams in OpenScape konfiguriert werden:

- H.263 Bandbreite je Video Stream:
  - Mögliche Werte: 32 – 960,000 kbps
  - Default: 160 kbps

- H.264 Bandbreite je Video Stream:
  - Mögliche Werte: 32 – 960,000 kbps
  - Default: 64 kbps

- Bandbreite bei unbekannten Codecs je Video Stream:
  - Mögliche Werte: 32 – 960,000 kbps
  - Default: 128 kbps

5. Bereitstellung von QoS in Datennetzen

Um, wie in gewohnter Weise auf unseren Systemen sehr gute Übertragungsqualität liefern zu können, werden folgende Anforderungen an die Quality of Service (QoS) Implementation vorgegeben:

- Eigene VLAN´s für Realtime Applikationen (Voice, Fax und Video), in Folge „Voice-VLAN“ genannt.
- Alle an der Übertragung beteiligen Komponenten müssen IEEE 802.1pq und DiffServ unterstützen.
- Für den Fall, dass hinter den IP-Endpoints (an das IP-Phone) angesteckte Devices (PCs, Notebooks, etc) benutzt werden, gibt es folgende Realisierungsmöglichkeiten:
    - auf dem Switchport ist 802.1pq mit den nur 2 benötigten VLANs konfiguriert, wobei das Daten-VLAN untagged und das Voice-VLAN tagged ausgegeben wird oder
    - es ist eine herstellerspezifische Konfiguration möglich. Als Beispiel anhand Cisco: das Switchport wird als Accessport dem Daten-VLAN zugewiesen und zusätzlich wird am Interface ein Voice-VLAN mit der entsprechenden VLAN-ID konfiguriert.
    - An dieser Stelle wird zusätzlich auf die Kapitel „Anschaltung OpenStage“ und „Anschaltung analog-/IP Adapter“ verwiesen.
- Die zentralen Komponenten (Server, Gateways, etc.) werden an Ports angeschaltet, die direkt im entsprechenden VLAN konfiguriert sind und die Daten werden untagged übertragen. Gleiches steht auch für IP-Phones zur Verfügung, hinter welchen kein Device angeschlossen ist.
- Zusätzlich müssen in den beteiligten Netzwerkkomponenten Priorisierung auf Layer 3 mit Diffserv nach RFC 2474 oder ToS nach RFC 791 und auf Layer 2 nach IEEE 802.1p durchgängig unterstützen. Seitens Atos werden folgende Werte referenzierend auf RFC 4594 empfohlen und verwendet:
    - Voice-, Fax-Payload und OSUC Video:
        - Layer 3 - DiffServ EF
        - Layer 2 - CoS 5
    - Voice-, Fax-Signaling:
        - Layer 3 - DiffServ CS5
        - Layer 2 - CoS 5
    - Video-Payload ausgenommen. OSUC Video:
        - Layer 3 - DiffServ CS4
        - Layer 2 - CoS 4
    - Video-Signaling mit SIP:
        - Layer 3 - DiffServ CS5
        - Layer 2 - CoS 5
    - Video-Payload und Signaling mit H.323:
        - Layer 3 - DiffServ AF41
        - Layer 2 - CoS 4
- Unify OpenScape setzt per default nur Layer 3 Priorisierung ein. Auf Kundenwunsch kann Layer 2 Priorisierung zusätzlich aktiviert werden.
- Die Priorisierung der Applikationen wird im Kapitel „Applikationen“ behandelt.

6. Netzwerkdienst Anforderungen

In diesem Kapitel werden die Anforderungen die allgemeinen Netzwerkdienste beschrieben.

6.1. Allgemeine Services

Zur Integration der Applikationen in die Kundenumgebungen müssen alle dafür benötigten Services (beispielsweise: Windows Domain Controller, etc.) kundenseits bereitgestellt werden.

6.2. Anforderungen an die DHCP/DNS/FTP Infrastruktur

Es muss beachtet werden, dass für das OpenScape Deployment Service (Tool zum Massen-Rollout und zur zentralen Client-Konfiguration) bestimmte Anforderungen an den DHCP Service im Kundennetzwerk gestellt werden. Die entsprechenden Maßnahmen bzw. Konfigurationsänderungen sind vorab vom Kunden durchzuführen.

Für die Unterstützung von Mobilitätsfunktion, vollständigem Plug&Play und andere Voice Merkmale (z.B.: Verschlüsselung, Display-Uhrzeit) muss der DHCP Dienst des Kunden neben den standardmäßigen Parametern folgendes unterstützen:

- Zeitzonenverschiebung (Option 2)
- Router (Option 3)
- IP-Adressen des primären und sekundären DNS-Servers (Option 6)
- Vendor ID (Option 12)
- DNS Domain Name des Telefones (Option 15)
- IP-Adresse des SNTP-Servers (Option 42)
- Vendor-spezifische Information (Option 43: Tag2 Vlan-ID, Tag3 DLS Server IP-Adresse)
- Leased Time (Option 51)
- Vendor Class Identifier (Option 60)
- DHCP Relay Option for local Information (Option 82)
- IP-Adressen von SIP-Server und SIP-Register (Option 120)

Es dürfen keine „Superscopes“ für Voicescopes am DHCP Server eingerichtet sein.

Ein vollständiges Plug&Play mit dem OpenScape Depoyment Service kann nur dann genutzt werden, wenn im Netzwerk eine DHCP/DNS/FTP-Infrastruktur existiert und diese für die Zusammenarbeit mit dem DLS konfiguriert ist.

Für den Produktivbetrieb von VoIP muss ein konfigurierter DNS Dienst in der Kunden Netzwerkinfrastruktur vorhanden sein. Bei der geographischen Trennung der OpenScape Voice Nodes in zwei verschiedene IP-Subnetze müssen in der DNS Infrastruktur auch DNS-SRV Einträge konfiguriert werden. Für die geographische Trennung über Layer-2 zwischen zwei Standorte im gemeinsamen Subnet sind DNS-SRV Einträge nicht erforderlich. Konfiguration des DNS-Dienstes ist vom Kunden zu erbringen. Der DNS bzw. DNS-SRV Dienst muss an allen Standorten, auch bei Netzwerkausfällen, verfügbar sein.

Zur Versorgung der Endgeräte mit neuer Software wird mindestens ein FTP Server benötigt. Dabei ist es vom Lizenzsystem des FTP-Herstellers abhängig wie viele Endgeräte gleichzeitig versorgt werden können (Concurrent FTP-Sessions). Empfohlen wird, dass jeder FTP Server mind. 10% der ihm zugeordneten Endgeräte gleichzeitig versorgen kann und die Verteilung auf diese 30 Minuten nicht überschreitet. Die FTP Serverfunktion muss in mindestens empfohlener Ausführung vom Kunden bereitgestellt werden.

6.3. Authentifizierung (802.1X)

Authentifizierung mit 802.1X steht bei OpenStage-Endgeräten zur Verfügung.

Bei Verwendung von 802.1X sind die dafür benötigten Zertifikate vom Kunden zu liefern. Ist dies dem Kunden nicht möglich, so kann Atos mit der Zertifikatserstellung inklusive dem damit verbundenen Aufbau der benötigten Infrastruktur optional beauftragt werden.

Um eine automatische Verteilung der Zertifikate mit dem OpenScape Deployment Service durchführen zu können, muss der Zertifikatsname aus der E.164-Nummer oder der Device-ID (MAC-Adresse) des betreffenden OpenStage bestehen.

Ab Version 6 des OpenScape Depoyment Service steht auch eine automtisierte Import-Schnittstelle zur CA von Microsoft zur Verfügung. Bitte entnehmen sie die detaillierten Informationen der jeweils gültigen OpenScape Deployment Service Dokumentation.

Wenn Datenendgeräte an das Telefon angeschlossen werden sollen, welche ebenfalls mit 802.1X authentifiziert werden sollen, muss der eingesetzte Netzwerk-Switch mindestens „Dual-Authentication“ unterstützen und mit Hilfe der dahinterliegenden Infrastruktur in der Lage sein, dem Datenendgerät ein eigenes VLAN zuzuweisen.

Wenn Datenendgeräte an das Telefon angeschlossen werden sollen, welche nicht mit 802.1X authentifiziert werden sollen, sondern nur das IP-Phone mit 802.1X authentifiziert werden soll, muss der eingesetzte Netzwerk-Switch mit Hilfe der dahinterliegenden Infrastruktur in der Lage sein dies zu unterstützen und dem Datenendgerät ein eigenes VLAN zuzuweisen.

Wenn individuelle Zertifikate für jedes IP Phone durch den Kunden erstellt werden, müssen diese Zertifikate bereits wie folgt vorliegen:

Alle Dateinamen der Zertifikate basieren entweder auf

- den Device IDs (MAC-Adressen) der Telefone oder
- den E.164-Rufnummern der Telefone.

Phone-Zertifikate werden im Format PKCS#12 und RADIUS-Zertifikate im Format .pem erwartet.

Die Zertifikatserstellung durch Atos muss, wenn im Vertrag mit dem Kunden nicht anders geregelt, zusätzlich beauftragt werden.

Anmerkungen:
Microsoft Windows Betriebssysteme haben unter bestimmten Konstellationen Probleme mit der Authentifizierung. Dies kann entweder durch Einspielen der entsprechenden Microsoft Windows Patches oder durch umkonfigurieren der Netzwerkkomponenten gelöst werden. Beides liegt in Kundenverantwortung.

6.4. Minimierung des Broadcast / Multicast Verkehrs

Der Broadcast/Multicast-Verkehr sollte grundsätzlich möglichst geringgehalten werden. Abhilfe kann durch die Strukturierung des Netzes (z.B. VLAN) mit Hilfe von Routern/Layer-3-Switches geschaffen werden. In den für Kommunikationseinrichtungen vorgesehenen Netzsegmenten ist für den Betrieb der Kommunikationslösung nicht benötigter Broadcast/Multicast-Verkehr zu vermeiden.

6.5. Maximum Transmission Unit (MTU)

Atos geht davon aus, dass eine MTU von 1.518 Bytes (wie für Standard Ethernet 802.3 definiert) auf der gesamten Übertragungsstrecke zur Verfügung steht.

Für den Fall, dass nur eine MTU kleiner 1.518 Bytes von der Übertragungsstrecke zur Verfügung gestellt werden kann, wird darauf hingewiesen, dass für die Übertragung der Signalisierung anstelle von UDP, TCP für den Transport eingesetzt werden muss.

7. Applikationen

In diesem Kapitel werden die Anforderungen der Applikationen an das Netzwerk beschrieben.

7.1. Verfügbarkeit von Applikationen

Atos bietet Applikationen, welche eine Carrier Grade Softwarearchitektur besitzen, beispielsweise OpenScape Voice, um bei deren zur Verfügung stehenden Services eine Verfügbarkeit von 99,999% erreichen zu können.

Um beim Einsatz solcher Applikationen eine entsprechende Verfügbarkeit der Gesamtlösung zu erreichen, muss die zugehörige Infrastruktur (Anschlüsse, Netzwerk, Stromversorgung, Virtual Machines, vSwitches, Klimatisierung, etc.) ebenfalls mit entsprechender Verfügbarkeit und Redundanz bereitgestellt werden.

Für Redundanzen werden marktübliche Mechanismen verwendet, bei welchen die MAC- und IP- Adressen eines Interfaces auf ein anderes übernommen werden. Im Netzwerk muss sichergestellt werden, dass das Übernehmen der Adressen möglich ist.

7.2. Übertragung von Applikationsdaten

Der Datentransfer von Unify OpenScape Applikationen (z.B. ContactCenter, Concierge, CTI, etc.) erfolgt grundsätzlich innerhalb des Daten- oder Client-Netzes des Kunden zusammen mit kundeneigenen Applikationsdaten. In gut funktionierenden Datennetzwerken stellt dies für die Applikationen kein Problem dar.

Da Unify OpenScape Applikationsdaten zur Steuerung der Echtzeitkommunikation dienen, bedürfen sie einer guten Übertragungsqualität. Maximales Round Trip Delay 100ms, Retransmissions von < 3% und Non-Consecutive Packet Loss < 1% sind Richtwerte für die Übertragung dieser Applikationsdaten. Die Richtwerte für Delay beziehen sich auf die Datenübertragung in Hochgeschwindigkeitsnetzen (z.B. LAN). Bei WAN Verbindungen kommen die in der „Referenztabelle für Serialisierungs-Delay“ angeführten Werte noch hinzu. Beispielsweise ergibt sich bei Verwendung einer 512kbps Verbindung ein Richtwert von ca. 146,9 ms Round Trip Delay bei der Übertragung von 1.518 Byte Paketen End-to-End, welche nicht den Anforderungen entspricht.

7.3. OpenScape Voice

Wird ein OpenScape Voice Hochverfügbarkeits-Cluster an zwei verschiedenen Rechenzentrumsstandorten (auch „Node-Serperation“ oder „Geo-Seperation“ genannt) installiert, müssen die Installationsvoraussetzungen bezüglich physikalischer und logischer Verbindungen, sowie der benötigten Bandbreiten, der jeweils gültigen OpenScape Voice Dokumentation eingehalten werden.

7.4. OpenScape Contact Center

Im OpenScape Contact Center werden zusätzlich zu den Sprachverbindungen noch für die Applikationen folgende Bandbreiten benötigt:

- Agenten Desktop: 25 kbps
- Manager/Supervisor: 125 kbps

Der hier angegebene Bandbreitenbedarf je Client bezieht sich auf einen in der Praxis evaluierten Wert.

Die tatsächliche Bandbreite hängt stark vom Benutzerverhalten und der Gleichzeitigkeit ab und kann, abhängig von den jeweils benutzen Funktionen, abweichen.

Als Beispiele werden hier die Anzahl von Verzeichnis-Abfragen, Webseiten- und Kalenderzugriffen genannt.

Abhängig vom gewünschten Leistungsumfang muss eine Integration in die Windows Domain und Exchange des Kunden erfolgen.

7.5. OpenScape Unified Messaging Service (UMS)

Wenn das OpenScape UMS via IP angebunden wird, gelten auch hier die für Voice und Fax angegebenen Werte.

Abhängig vom gewünschten Leitungsumfang muss eine Integration in die Windows Domain und Exchange des Kunden erfolgen.

7.6. OpenScape WebCollaboration

OpenScape WebCollaboration unterstützt die Dienste WebCollaboration als Basisservice und überträgt bei Bedarf auch Voice und Video innerhalb der Session.

Der symmetriesche Bandbreitenbedarf zwischen OpenScape WebCollaboration Server und den Clients (sowohl Konferenz-Moderatoren als auch Teilnehmer) für den Dienst WebCollaboration berechnet sich nach folgender Formel:

15 kbps mal Anzahl der gleichzeitig verbundenen Moderatoren und Teilnehmer

Berechnungsbeispiel: 10 parallele Konferenzen mit 10 Moderatoren und 10 Teilnehmern ergibt einen Bandbreitenbedarf von:

15 kbps x (10 Moderatoren + 10 Teilnehmer) = 300 kbps (up/down, symmetrisch)

Wird die Übertragung von Voice und/oder Video innerhalb der Session verwendet, ergibt sich abhängig vom gewählten Codec für die Übertragung ein entsprechend zusätzlicher Bandbreitenbedarf zwischen OpenScape WebCollaboration Server und den Clients.

Auf dem OpenScape WebCollaboration Server darf nur der mitgelieferte Web-Server laufen.

7.7. Integration Kunden-Applikationen

Zur Integration in und von Kundenapplikationen (z.B. Microsoft, IBM, SAP, etc.) muss der Kunde die in den Unify Produktdokumentationen festgehaltenen Anforderungen zur Implementierung des gewünschten Leistungsumfanges bereitstellen. Beispielsweise werden hier Domainintegrationen, Schnittstellen, Versionsvoraussetzungen genannt.

7.8. Anschaltung OpenStage

OpenStage IP-Phones können auf folgende Weise an das Datennetzwerk logisch angeschlossen werden:

- Native, d.h. das Switchport ist direkt einem VLAN zugewiesen, OpenStage verhalten sich in diesem Fall wie herkömmliche Datenendgeräte (PC, Drucker, etc.) und es ist kein Datenendgerät an OpenStage angeschlossen. Pakete zum und vom OpenStage sind in dieser Variante untagged.
- 802.3q, d.h. hinter dem OpenStage kann ein Datenendgerät angeschlossen werden. OpenStage muss mit der VLAN-ID des Voice-VLANs über LLDP oder DHCP Optionen versorgt werden. Pakete für OpenStage aus dem Voice-VLAN müssen entsprechend tagged ausgegeben werden, Pakete für das an OpenStage angeschlossene Datenendgerät müssen untagged ausgegeben werden. Erfolgt die VLAN-ID Vergabe mit LLDP, werden zusätzlich zur VLAN-ID die Priorisierungsdaten (CoS, QoS oder DiffServ) übergeben und diese müssen vom Netzwerkbetreiber entsprechend den Vereinbarungen gesetzt sein.

7.9. Anschaltung analog-/IP Adapter

Analog-/IP Adapter werden so angeschaltet, dass das Switchport direkt einem VLAN zugewiesen wird. Analog-/IP Adapter verhalten sich wie typische Datenendgeräte (PC, Drucker, etc.). Pakete vom und zum Adapter sind *untagged*.

7.10. HiPath Cordless IP

HiPath Cordless IP (IP-DECT) Basisstationen werden über eine 100 Mbit full-duplex Ethernet-Schnittstelle an das Datennetzwerk angeschaltet. Standardmäßig ist Power over Ethernet (802.3af, Class2) als Stromversorgung vorgesehen.

Zur Priorisierung des Datenstroms müssen mindestens 2 Prioritätsklassen auf Layer2 802.1pq und auf Layer3 ToS oder DiffServ zur Verfügung stehen. Standardmäßig werden die gleichen Einstellungen für Priorisierung wie in der Voice-Lösung verwendet. Desweiteren müssen abhängig von der Ausbaugröße der HiPath Cordless IP Lösung genügend IP-Adressen in den jeweiligen IP-Subnetzen zur Verfügung stehen.

Die Kommunikation zwischen diesen Komponenten muss transparent, also ohne NAT oder ähnliche Dienste, erfolgen.

Um eine einwandfreie Zeit-Synchronisation zwischen den Basisstationen einer Gruppe bei Handover der Mobilteile zu ermöglichen dürfen zwischen der Cordless IP Interworking Unit (IWU) und einer Cordless IP Basisstation maximal 3 unmittelbar aufeinander folgende Layer 2 Hops liegen, welche mit mindestens 1Gbit Links verbunden sind.

Die Layer 2 Switching Leistung muss der eines im „Non-BlockingMode“ betriebenen Enterasys B3G124 oder Cisco Catalyst 3560 entsprechen.

Als Übertragungsprotokoll auf Layer4 wird ausschließlich UDP verwendet.

Die Sprachübertragung erfolgt mit G.711 mit 20ms SampleRate.

Ein NTP-Server (siehe „Netzwerkdienst Anforderugen“) wird benötigt um die korrekte Zeit an den Mobilteilen und in den Ruflisten der Mobilteile darzustellen.

Bitte beachten sie die detaillierten Netzwerkkonzept-Anforderungen in der jeweils gültigen Produkt-Dokumentation.

7.11. Sprachaufzeichnung

Ein aufgezeichnetes Gespräch verhält sich vergleichbar eines Telefongespräches. Der Gesprächsstrom wird zur zentralen Aufzeichnungsressource gesandt.

7.12. Atos Secured Remote Access

Für den Remote-Support durch Atos muss ein Fernwartungszugang gemäß den Anforderungen von SIRA bzw. SSDP durch den Kunden bereitgestellt werden. Mit diesem Zugang ist es Atos möglich auf alle für den Support durch Atos vorgesehenen System zuzugreifen. Ein bidirektionaler Filetransfer muss ebenfalls ermöglicht werden um Updates bzw. Diagnoseinformationen zwischen den Kundensystemen und dem Atos Support transferieren zu können.

SIRA bzw. SSDP ist ein TÜV sicherheits-zertifizierter Fernwartungszugang für Atos Remote Support Abteilungen zu Kundensystemen.

Eine detaillierte Beschreibung inklusive der benötigten Informationen entnehmen sie bitte den Dokumenten „Atos Remote Service Security Concept“ und „Fernwartungszugang Kunden Checkliste VPN“.

Dieser Zugang muß innerhalb der im Servicevertrag definierten Zeiten jederzeit zur Verfügung stehen.

8. Unify Circuit

Allgemeine Unify Circuit Netzwerkanforderungen entnehmen sie bitte folgender WebSite:
https://www.circuit.com/Unifyportalfaqdetail?articleId=48855

Bandbreitenanforerungen von Unify Circuit entnehmen sie bitte folgender WebSite:
https://www.circuit.com/Unifyportalfaqdetail?articleId=36901

Anforderungen bezüglich VDI Anforderungen von Unify Circuit entnehmen sie bitte folgender WebSite:
https://www.circuit.com/Unifyportalfaqdetail?articleId=122185

9. WLAN Anforderungen

Dieses Kapitel fasst die wesentlichen Anforderungen und Empfehlungen zur Umsetzung von Unify Sprachkommunikationslösungen in WLAN-Netzen (VoWLAN) zusammen.

Details und weiterführende Informationen sind der jeweiligen Produktdokumentation und Release Notes von Unify bzw. dem jeweiligen Hersteller der WLAN-/LAN-Infrastruktur zu entnehmen.

9.1. WLAN Planungsgrundlagen

Grundsätzlich muss bei der Planung von WLAN-Netzen berücksichtigt werden, dass für die Echtzeitkommunikation (Sprache, Video, etc.) höhere Anforderungen an die Infrastruktur gestellt werden, als für reine Datenkommunikation.

Daten-Endgeräte, wie ein Laptop, der zum Surfen im Internet oder anderen Anwendungen verwendet werden soll, versucht mit maximaler Paketgröße (1500 Byte), die relativ große Menge an Daten von und zu Web-Seiten bzw. Server zu transportieren. Es nutzt dabei typischerweise TCP als Transportprotokoll und kann somit die Verbindung zum Server mit großen Verzögerungen und Paketverlusten korrigieren, da das Protokoll Mechanismen definiert hat, derartige Störungen bei der Übertragung von Daten zu handhaben.

Sprach-Endgeräte hingegegen verwenden relative kleine Paketgrößen (64 Byte) und bedürfen einem regelmäßigen Zugang zu den Funk-Kanälen, da die Pakete in einem stetigen und gleichmäßigen Datenstrom gesendet und empfangen werden müssen.

Da die Datenpakete bei Sprachübertragung klein sind, ist es wichtig, dass der von den Protokollen verwendete Signalisierungsaufwand (Overhead) so klein wie möglich ist. Mit UDP statt TCP wird der Overhead deutlich reduziert. Die Quittungsmeldungen, die beim TCP-Protokoll für jedes Paket gesendet werden, entfallen beim UDP-Protokoll. Um die richtige Reihenfolge bei der Übertragung von Sprachpaketen sicherzustellen, wird das RTP-Protokoll verwendet. Damit wird eine verständliche Sprache für den Empfänger gewährleistet.

Die folgende Tabelle zeigt die Unterschiede von Daten und Sprache in Netzwerken:

	Datentransport	Sprachtransport
Protokolle/Anwendungen	Datei-Transfer (FTP), Webseiten (HTTP)	Sprachkommunikation (RTP over UDP)
Paketgröße	Variert von klein bis sehr groß abhängig von der Applikation	Klein (< 300 bytes)
Sensibilität für verlorene Pakete	Nein. Einsatz von Wiederherstel-lungsmechanismen in TCP.	Ja. Schlechte Sprachqualität
Sensibilität für Verzögerungen im Netzwerk	Nein. Verträgt längere Verzögerungen	Ja. Schlechte Sprachqualität
Sensibilität für Unterbrechungen	Nicht immer. Sitzungen können teilweise wiederhergestellt werden.	Ja. Gespräche werden unterbrochen

Tabelle 5: Unterschiede von Daten und Sprache in Netzwerken

Für die Übertragung von Sprache müssen WLAN-Signale stärker und konsistenter sein, die mögliche Gesprächsdichte (gleichzeitige Gespräche) bei den jeweiligen Access Points (AP) ist dabei ebenso zu berücksichtigen. Hier gibt es Unterschiede bei der Implementierung im 2,4 GHz und 5 GHz Frequenzband, da eine unterschiedliche Zahl von Kanälen zur Übertragung zur Verfügung steht.

Ein WLAN-Telefon arbeitet in der Regel auf „Augenhöhe“ gegenüber einem Laptop, der hauptsächlich stationär von einer Person verwendet wird. Es kann auch festgestellt werden, dass Personen zum Telefonieren oftmals ruhige Gebäudebereiche aufsuchen und sich dort entsprechend bewegen. Dies sind oft Bereiche, in denen WLAN-Abdeckung eine Herausforderung sind bzw. bei der Funkplanung oftmals unberücksichtigt bleiben.

Ein gutes Beispiel ist das Treppenhaus - in der Regel ein schöner, ruhiger Ort für ein Gespräch. Zusätzlich kann die Dämpfung des menschlichen Schädels sowie Weichgewebe bis zu 10 bis 12 dB betragen. Dies und vieles mehr zeigt die Bedeutung eines starken WLAN-Signals ganz klar.

9.2. Wireless-Infrastruktur und Funknetzplanung

9.2.1. Automatische Anpassung der Frequenz-Parametern

Bei der Implementierung von VoWLAN ist darauf zu achten, dass automatische Mechanismen zur Funknetz-, Signalstärken-Steuerung für die sprachrelevanten Frequenzen/Kanäle und APs deaktiviert werden und manuelle Einstellungen auf den APs bzw. den Controller durchgeführt werden.

Eine Automatisierung bzw. Dynamisierung führt u.U. dazu, dass in bestimmten Situationen das Roaming zwischen verschiedenen APs nicht in dem gewünschten Maße und der Qualität erfolgt.

9.2.2. Einsatz mehrerer Wireless Controller

Beim Einsatz mehrerer Wireless Controller ist es vorteilhaft, wenn APs im gleichen Versorgungsbereich (Standort, Gebäude, Stockwerk, etc.) von demselben Wireless Controller gesteuert werden. Somit kann vermieden werden, dass im Falle des Roamings von einem zu nächsten APs zusätzliche Netzwerk-Hops und damit potentielle Verzögerungen hinzukommen.

9.2.3. Einsatz von Loadbalancing

Beim Einsatz von Loadbalancing im WLAN kommt es typischerweise zu dynamischen „Bewegungen“ der WLAN-Endgeräte zwischen den APs, um eine Überlastung zu vermeiden und die Last auf mehrere APs zu verteilen. Dabei werden WLAN-Endgeräte gezwungen sich auf einen anderen AP zu verbinden.

Der Standard 802.11 unterstützt dabei keinen reibungslosen Übergang („Smooth Transistion“) von einem AP zum nächsten, sondern es erfolgt eine De-Authentifizierung und anschließende Re-Authentifizierung des Endgeräts. Speziell ist darauf Rücksicht zu nehmen, wenn sich die Endgeräte über 802.1X am Netzwerk durch Kontaktaufnahme auf einen zentralen RADIUS-Server neu anmelden müssen.

Wird zudem kein OKC (Opportunistic Key Caching) von der WLAN-Infrastruktur unterstützt, kann dieser Vorgang sehr lange dauern. Eine Unterbrechung der Sprachverbindung ist vorprogrammiert, zumindest jedoch der Verlust von vielen Sprachpaketen. (Siehe Kapitel 9.3)

9.2.4. Signalstärke/Sendeleistung

Standardmäßig passt das WLAN-Endgerät (z.B. OpenStage WL3) seine Leistung an die der APs an, jedoch kann die Leistung ebenso manuell in fünf Stufen (zwischen 0-20 dBm) konfiguriert werden. Stellen Sie sicher, dass die APs und Clients so konfiguriert werden, dass die gleiche Sendeleistung verwendet wird, um asymmetrische Kommunikationsverbindungen zu vermeiden.

Das WLAN-Endgerät OpenStage WL3 kann im a- bzw. b/g-Band bis zu 20 dBm konfiguriert (beachten Sie, dass zwischen 14-20 dBm keine festen Schritte wegen des Signalverstärkers eingestellt werden können.)

Für unterversorgte Bereiche empfiehlt sich der Einsatz weiterer APs, die von den Endgeräten erkannt und verwendet werden können (Roaming).

Bewegt sich ein WLAN-Endgerät von einem AP weg, so wird die Übertragungsrate reduziert, um die Reichweite zu erhöhen. Dies hat eine Auswirkung auf die Kapazität (Durchsatz) der Zelle. Da sich alle Endgeräte die Kapazität einer Funkzelle teilen, führt die Reduktion der Übertragungsrate für ein Endgerät zu einer Gesamtreduktion der Kapazität der Funkzelle für alle Endgeräte.

Um eine hohe Übertragungskapazität in jeder Funkzelle zu gewährleisten, muss die Signalstärke in jeder Zelle, in der viele Endgeräte erwartet werden, entsprechend hoch sein.

9.2.5. IEEE 802.11 a/b/g/n

Beim IEEE 802.11-Betrieb im 2,4 GHz-Band stehen nur die drei nicht-überlappende Kanäle, Kanal 1, 6 und 11 zur Verfügung.

Im 5-GHz-Band gibt es viele nicht-überlappende Kanäle zur Auswahl. Die spezifische Nutzung und Anzahl der Kanäle, die verwendet werden können, variiert je nach regulatorischen Vorschriften im betroffenen Land. Die Unterstützung von 802.11d in den APs und WLAN-Endgerät ermöglicht die automatische Anpassung der regulatorischen Vorgaben.

- **IEEE 802.11 b/g/n (2,4 GHz)**
  Dieser Standard arbeitet im 2,4 GHz Industrial Scientific Medical (ISM) Band. Diese Band ist nicht lizenziert und viele verschiedene Wireless-Gerät verwendet diese Band mit verschiedenen Radio-Techniken. Deshalb gibt es bei diesen Systemen und Produkten verschiedene Beeinflussungen bei der Übertragung. Dies gilt für alle HF-Signale, nicht nur andere Geräte 802.11.
  Wenn Probleme auftreten, kann es Auswirkungen auf die Übertragung zwischen dem AP und dem Endgerät kommen. Wenn der Sende-Uplink (vom Endgerät) unterbrochen wird, liegt das Problem
  meist in der Nähe des Endgeräts. Prüfen Sie in der Nähe Geräte wie drahtlose Überwachungskameras, Bluetooth Geräte, WiDi Geräte, ZigBee/Z-Wave zur HLK-Steuerungen, Lichtsteuerung, Automatisierung usw.
- **IEEE 802.11 a/n (5 GHz)**
  DFS (Dynamic Frequency Selection) Kanäle: Atos empfiehlt für Voice-over-WLAN den Einsatz von Non-DFS Kanälen
- **IEEE 802.11n (2,4 und 5 GHz)**
  Ein voll ausgelasteter/belegter 802.11n AP kann die drahtgebundene LAN-Verbindung zum Ethernet Switch überlasten, da vom AP durchaus mehr als 100 Mbps Übertragungsbandbreite benötigt werden kann.
  Um von den Möglichkeiten und Fähigkeiten des 802.11n-Standard bestmöglich profitieren zu können, sollte die LAN-Verbindung zum Switch auf Gigabit-Ethernet aufgerüstet bzw. eingesetzt werden, da sonst der AP Datenpakete in die Warteschlange einreihen (Verzögerung) oder schließlich Pakete verwerfen muss.

9.2.6. Positionierung von APs für optimale Leistung/Performance

Es besteht ein gewisser Widerspruch zwischen den beiden wesentlichen Anforderungen für eine optimale Platzierung bzw. Positionierung von APs: gute Leistung erfordert eine gute Abdeckung, aber „Überdeckung“ reduziert die Leistung einer WLAN-Infrastruktur.

Die Überlappung von benachbarten Funkzellen/APs sollte einerseits ausreichende Signalstärke gewährleisten und andererseits genug Spielraum beim Roaming eines Endgeräts zwischen diesen Funkzellen bieten.

Benachbarte Funkzellen dürfen dabei nicht mit demselben Kanal/derselben Frequenz arbeiten, da es sonst zur „Co-Channel Interferenz“ kommt. Je weiter die APs mit gleicher Frequenz voneinander entfernt sind, umso geringer ist dieses Problem.

Diese beiden Anforderungen sind bei der optimalen Netzplanung zu berücksichtigen und in jedem möglichen Szenario berücksichtigt werden. Atos bietet zu diesem Zweck entsprechende Funknetzplanungen bzw. –messungen an.

Grundsätzlich ist bei der Platzierung der APs auch auf die „Bewegungsmuster“ der Menschen, die mit WLAN-Endgeräten unterwegs sind zu achten. Dies bedeutet, dass APs so positioniert werden sollten, dass auch Gang-ecken/-kreuzungen, lange Gänge oder z.B. Durchgänge von dicken Türen abgedeckt werden.

9.2.7. Konfigurationsempfehlungen VoWLAN

Die minimale Empfangssignalstärke für den VoWLAN-Einsatz im Zellgrenzbereich liegt bei -70 dB (oder höher). Geringere Signalstärke kann zu einer abgehackten Sprache führen. Das bedeutet natürlich, dass die abgestrahlte/konfigurierte Signalstärke entsprechend höher sein muss, um im gewünschten Abdeckungsbereich die erforderliche minimale Empfangssignalstärke zu erreichen.

- Der Wert von mindestens -70 dBm erlaubt einerseits hohe Datentransferraten und andererseits können kleine Zellbereiche vermieden werden.
- Der Mindestabstand sollte so gewählt werden, dass der minimale Signalabstand zwischen zwei WLAN Zellen mit dem gleichen Kanal -19 dBm nicht unterschreitet.
- Die Überlappung zweier benachbarter Zellen sollte in etwa 20-30% betragen, um ausreichend Spielraum für sicheres Roaming zu haben.
- Die Kanalauslastung im QoS Basic Service Set QBSS sollte unter 45% liegen.
- Die Paketfehlerrate (PER) sollte unter 1% liegen.
- Der Signal-/Rauschabstand (SNR) sollte mindestens 25 dB betragen.
- Die APs verwenden optimalerweise mehrere Antennen („diversity antennas“)

Atos empfiehlt grundsätzlich Wi-Fi zertifizierte Access Points mit folgenden Funktionen:

- IEEE 802.11a, b, g und n
- Wi-Fi Protected Access (WPA2 Enterprise)
- Wi-Fi Multimedia (WMM®)
- Wi-Fi Multimedia Power Save (WMM Power Save®)

9.3. Security Maßnahmen

Unify OpenStage WL3 können verschiedene Verschlüsselungs- und/oder Authentifizierungsmethoden verwenden. Es ist jedoch zu berücksichtigen, dass der Einsatz derartiger Methoden zu Gesprächsabbrüchen während des Roamings aufgrund der länger dauernden Authentifizierung führen können. Während dieser Phase werden keine Sprachpakete gesendet oder empfangen, bis diese erfolgreich abgeschlossen ist.

Atos empfiehlt den Einsatz von WPA2. Wird dies zusammen mit einer 802.1X Authentifizierung verwendet, so ist der Einsatz von „Proactive Key Caching (PKC)“ oder „Opportunistic Key Caching (OKC)“ unumgänglich. Diese Funktionen ermöglichen ein rasches Roaming zwischen APs. Der dabei erforderliche Austausch von Sitzungsschlüssel („4-way handshake“) kann zu geringfügigen Sprach-Paketverlusten führen.

Dies gilt insbesondere beim Roaming zwischen APs, die vom selben Wireless Controller gesteuert werden. Beim Übergang zwischen APs, die von unterschiedlichen Controller gesteuert werden, ist typischerweise eine vollständige Authentifzierung erforderlich, was wiederum zu Gesprächsabbrüchen führen kann/wird.

Opportunistic Key Caching (OKC) muss auch von den WLAN-Endgeräten und Clients unterstützt werden. Die Implementierung in der Infrastruktur alleine genügt nicht. Besonders zu berücksichtigen ist dies bei der Nutzung von z.B. WLAN-Softclients/Mobile Apps auf SmartPhones (siehe OpenScape Mobile).

Auf proprietäre Mechanismen (z.B. Cisco Centralized Key Management CCKM) wird in diesem Dokument nicht eingegangen. Atos kann seine Kunden bei derartigen Implementierungen unterstützen, um bestmögliche Ergebnisse zu erzielen.

Folgende Sicherheitsmechanismen werden seitens Atos grundsätzlich nicht empfohlen:

- WEP – Wired Equivalent Privacy
- Shared Key Authentication
- MAC Address Filtering
- Hidden SSID – dies erschwert das passive Roaming von WLAN-Endgeräten und führt zu Qualitätseinbußen

10. Allgemeine Anforderungen

In diesem Kapitel werden die allgemeinen Anforderungen an die Infrastruktur beschrieben.

10.1. Virtuelle Maschinen und Server-Umgebungen

Wenn Server-Applikationen für den Einsatz auf Virtual Machines (z.B. VMware ESX) von Unify freigegeben sind und auf diesen eingesetzt werden sollen, müssen vom Kunden die von den Applikationen benötigten Ressourcen entsprechend reserviert werden. Die benötigten Ressourcen der betreffenden Applikationen werden von Unify bekannt gegeben.

Bitte beachten sie die detaillierten Anforderungen zur Implementierung in der jeweils gültigen Produkt-Dokumentation bzw. in den der Technical Design Specification zugehörigen Dokumenten.

10.2. Infrastruktur

Beim Einsatz von physischen und virtuellen Maschinen ist auf die erforderliche Verfügbarkeit der Gesamtlösung zu achten, daher muss die zugehörige Infrastruktur (Anschlüsse, Netzwerk, Stromversorgung, physische oder virtuelle Maschinen, vSwitches, Klimatisierung, etc.) ebenfalls mit entsprechender Verfügbarkeit und Redundanz bereitgestellt werden.

10.3. Terminalserver / Citrix-basierte Clients

Die benötigten Applikationen müssen für Terminalserverlösungen freigegeben sein. Die darin genannten Rahmenbedingungen (Ressourcen, Funktionen, etc.) müssen entsprechend eingehalten werden.

Die Rahmenbedingungen sind für Terminalserver Desktop Sharing definiert.

Terminalserver Application Sharing unterliegt den Limitierungen von verteilten Applikationsinstallationen.

Bitte beachten sie die detaillierten Anforderungen zur Implementierung in der jeweils gültigen Produkt-Dokumentation.

10.4. Kommunikations-Endgeräte im Datennetzwerk

Wenn Kommunikations-Endgeräte in das Datennetzwerk (Daten-Vlan) eingebunden werden (typischerweise bei Softphones) muss der Kunde für die generellen Routingmöglichkeiten zwischen Daten- und Sprachnetzwerk (Voice-Vlan) sorgen und die entsprechenden Qualitäts- und Security-Aspekte berücksichtigen. Ebenso müssen die Hardwarevorgaben an die Workstations laut der jeweils gültigen Produkt-Dokumentation bzw. in den der Technical Design Specification zugehörigen Dokumenten erfüllt werden. Des Weiteren sind die für die Applikation vorgegebenen Parameter einzuhalten.

10.5. Firewalls

Firewalls müssen gewährleisten, dass sie alle von OpenScape zu einer Kommunikationsbeziehung benötigten Verbindungen bestehen lässt.

Sollte eine dieser Kommunikationsbeziehungen ausgelöst (Reset, Reject, etc.) werden müssen, müssen alle anderen zu dieser Kommunikationsbeziehung gehörenden Verbindungen ebenfalls sowohl Richtung Client als auch Richtung Server ausgelöst werden. Wird dies seitens der Firewall nicht unterstützt, handelt es sich um ein Fehlverhalten der Firewall und kann dies zu undefiniertem Verhalten der Clients, vor allem des Client-Betriebssystems, führen. Eine entsprechende Konfiguration der Firewall liegt in Kundenverantwortung.

Es müssen die in der jeweils gültigen Produkt-Dokumentation bzw. in den der Technical Design Specification zugehörigen Dokumenten definierten Ports für die Applikationen freigeschalten werden.

10.6. Network Address Translation (NAT)

Network Address Translation (NAT) sollte grundsätzlich nicht auf VoIP/VoWLAN-Verkehr angewendet werden.

Sollte NAT trotzdem benötigt werden, wird der Einsatz eines OpenScape Session Border Controllers in SIP Umgebungen empfohlen.

Wenden sie sich bitte in diesem Zusammenhang an ihren Atos Ansprechpartner.

11. Verkabelung

In diesem Kapitel werden die Anforderungen an die Verkabelung beschrieben.

11.1. Datennetzwerk Verkabelung

Die Verkabelung des Datennetzwerkes muss den entsprechenden Normen bzw. Standards gemäß den bei der Übertragung verwendeten Protokollen entsprechen.

Dies inkludiert ebenfalls alle an der Übertragung beteiligten passiven Komponenten (Patchfelder, Anschlussdosen und –stecker, Patchkabel, etc.).

Die Bereitstellung einer den Normen bzw. Standards entsprechenden Verkabelung liegt in Kundenverantwortung.

11.2. Verkabelung für traditionelle Endgeräte

Die Verkabelung für traditionelle (analoge, digitale, etc.) Endgeräte erfolgt über eine so genannte 2-Draht Verkabelung, auch wenn diese physikalisch anders ausgeführt ist.

Der Anschluss traditioneller Endgeräte erfolgt über eine störungsfreie Verkabelung.

Unter störungsfrei wird verstanden, dass die Leitung frei von

- induktiven Einflüssen,
- auf Feuchtigkeit zurückzuführende Fehler,
- mechanischen Fehlern (z.B. Beschädigungen),
- elektrischen Fehlern (z.B. Kontaktprobleme)
- etc.

ist, auch wenn diese nur temporär / sporadisch auftreten.

Die Bereitstellung einer störungsfreien Verkabelung liegt in Kundenverantwortung.

12. Troubleshooting

Bei Problemfällen muss es Atos ermöglicht werden, abhängig vom Problem, Netzwerkmessungen und Protokollanalysen durchzuführen. Die Netzwerkmessungen, sowie die Messpunkte werden seitens Atos im Problemfall individuell definiert.

Für Servicezwecke (Installation, Updates, Upgrades, Troubleshooting, etc.) durch Atos muss entsprechend den Vereinbarungen im Servicevertrag physikalischer und Remote-Zugang zu den Kommunikationskomponenten ermöglicht werden.

Dies betrifft auch den Zugang zu VMware Servern über die VMware Console.

13. Anhang A – Tabellen- und Abbildungsverzeichnis

14. Anhang B – Glossar

Begriff	Beschreibung
ACELP	Algebraic Code-Excited Linear Prediction
AP	Access Point
802.1p	3 bit field within an Ethernet frame header when using IEEE 802.1Q
802.1Q	VLAN Tagging
802.1X	Authentifizierung
AMR	Adaptive MultiRate Compression
AMR-WB	AMR-WideBand
BSS	Basic Service Set
CA	Certificate Authority
CoS	Class of Service (Layer 2)
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DLS	Deployment and Licensing Server
DNS	Domain Name System
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
E.164	ITU-T Standard für Rufnummern-Nomenklatur
FTP	File Transfer Protocol
G.711	ITU-T Codec zur Übertragung von Sprache
G.722	ITU-T Codec zur Übertragung von Sprache
G.723	ITU-T Codec zur Übertragung von Sprache
G.729	ITU-T Codec zur Übertragung von Sprache
Gb	Gigabit
Gbit	Gigabit
H.263	ITU-T Codec zur Übertragung von Video
H.264	ITU-T Codec zur Übertragung von Video
HW	Hardware
IEEE	Institute of Electrical and Electronics Engineers
iLBC	internet Low Bandwidth Codec
IP	Internet Protocol
kb	kilobit
kbps	kilobit per second
LAN	Local Area Network
LLDP	Link Layer Distribution Protocol
MAC	Media Access Control Address
Mb	Megabit
Mbit	Megabit
MOS	Mean Opinion Score
ms	millisecond
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
OKC	Opportunistic Key Caching
PER	Packet Error Rate
PKC	Proactive Key Caching
PKCS	Personal Information Exchange Syntax Standard
QBSS	QoS Basic Service Set

Begriff	Beschreibung
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RTP	Realtime Transport Protocol
RTPC	RTP Control Protocol
SIP	Session Initiation Protocol
SFTP	Secure File Transfer Protocol
SNR	Signal-to-Noise Ratio
SNTP	Secure Network Time Protocol
SRTP	Secure Realtime Transport Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SW	Software
TCP	Transmission Control Protocol
ToS	Type of Service (Layer 3)
UDP	User Datagram Protocol
UMS	Unified Messaging System
VLAN	Virtual LAN
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access

© Copyright 2019, Atos IT Solutions and Services GmbH