Whitepaper

Netzwerkoptimierung für Microsoft Teams

Jan Böckelt

IN2SUCCESS

Der Ton macht die Musik: Welche Rolle die Medienqualität für Teams spielt

Management Summary

Im Vorfeld für eine Einführung von Microsoft Teams muss das Netzwerk vorbereitet werden, sodass Risiken bezüglich der Diensterreichbarkeit und -qualität minimiert werden können. Dieses Dokument beschreibt die Verbindungsprinzipien nach denen Teams und die Microsoft 365 Cloud arbeiten. Zusätzlich werden in diesem Dokument Handlungsempfehlungen zur Verbesserung der Gesprächsqualität dargestellt, deren Umsetzung durch Microsoft dringend empfohlen wird. Die Umsetzung sollte spätestens zu Beginn eines möglichen Proof of Concept (PoC) Aufbaus abgeschlossen sein. Primäres Ziel der Maßnahmen ist die Sicherstellung der Serviceerreichbarkeit sowie eine möglichst latenzfreie und ungehinderte Übertragung zwischen den Clients im Organisationsnetzwerk zur Microsoft 365 Cloud. Für Außenstandorte wird ein lokaler Internetanschluss dringend empfohlen.

1. Von On-Premise in die Cloud

Die Einführung von Microsoft 365 mit Teams als moderne Unified Communication & Collaboration Lösung führt zu einer starken Verschiebung von Workloads in Richtung Internet. Dienste, die bisher auf internen, zentralisierten Systemen betrieben wurden, werden nun als Software-as-a-Service (SaaS) Lösung innerhalb der Microsoft 365 Cloud bereitgestellt. Ins besondere die Videokommunikation in HD-Qualität hat einen massiven Einfluss auf die Last im internen Netz als auch in Richtung Internet.
Eine voreilige Einführung von Microsoft Teams ohne Optimierung der Netzwerkinfrastruktur in Richtung Microsoft 365 Cloud kann erhebliche Probleme bezüglich der Erreichbarkeit der Dienste, sowie schlechte Medienqualität, zur Folge haben. Daraus resultiert eine schlechte Nutzungserfahrung bei den Anwendern, die zu einer erheblich reduzierten Akzeptanz der Lösung führt.
Dieses Whitepaper beschreibt einige Prinzipien, die von Microsoft für die Bereitstellung der M365 Services verfolgt werden. Einige Optimierungsansätze geben Ansatzpunkte zur schnellen Verbesserung der Diensterreichbarkeit und Qualität.

2. Medienqualität

Wenn Bild- und Tonstörungen den Arbeitsprozess stören

Wenn sich die Telefonie durch die Implementierung von Microsoft Teams in Richtung Internet verlegt, erwarten sich Nutzer eine gute Medienqualität und zuverlässige Anrufverarbeitung. Denn der Abbruch eines Anrufs mitten im Gespräch bzw. Bild- und Tonstörungen beeinträchtigen den Arbeitsprozess und sorgen für Frust. Wer im Vorfeld nicht in die Optimierung der Netzwerkinfrastruktur investiert, riskiert erhebliche Probleme in Bezug auf die Erreichbarkeit der Dienste. Das Ergebnis ist eine schlechte Medienqualität, die

sich wiederum negativ auf die Akzeptanz der User auswirkt. Eine gute Rufaufbau-, Audio-, Video- sowie Präsentationsqualität sind Kernaspekte einer professionellen Unternehmenskommunikation.

Subjektive Qualität

Folgende Grafik gibt einen Überblick über die positiven bzw. negativen Erlebnisse, die während einem Telefonat via Teams auftreten können. Die Benutzererfahrung ergibt sich aus der Summe der Einflüsse und bestimmt, inwieweit Benutzer durch die Technologie abgelenkt werden oder sich voll und ganz auf ihr Meeting konzentrieren können.
Die Grafik zeigt vier Kernaspekte, die sich entweder positiv oder negativ auf das Gesamterlebnis auswirken: Rufaufbau-, Audio-, Video- und Präsentationsqualität.

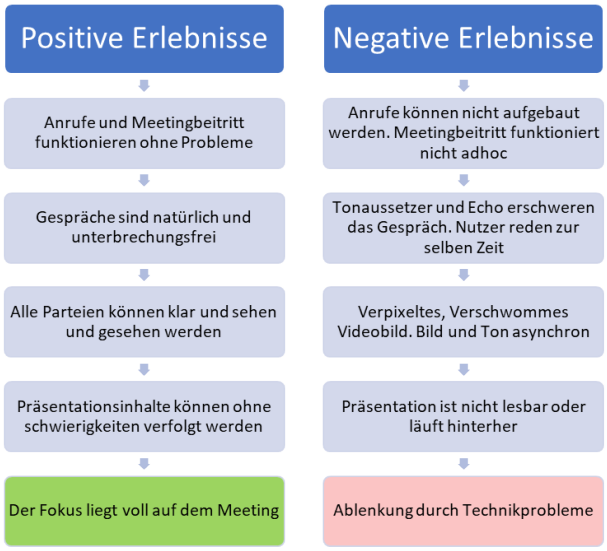

Abbildung 1: Nutzererlebnisse

Anrufe müssen ohne Verzögerungen aufgebaut werden. Der Beitritt zu Meetings muss ebenfalls reibungslos erfolgen. Tonstörungen erschweren das gegenseitige Verstehen, sodass Gesprächsinhalte ggf. mehrfach wiederholt werden müssen. Bei starken Verzögerungen kann es passieren, dass beide Seiten gleichzeitig anfangen zu sprechen. Das stört wiederum den natürlichen Gesprächsfluss. Video- und Präsentationsinhalte sollten möglichst klar und synchron übermittelt werden. Die Benutzererfahrung ergibt sich aus der Summe der Einflüsse und bestimmt, inwieweit Benutzer durch die Technologie abgelenkt werden oder sich voll und ganz auf ihr Meeting konzentrieren können.

Technische Medienqualität

Moderne UC Systeme, wie Microsoft Teams etwa, beruhen auf IP-basierter Echtzeitkommunikation mittels UDP/RTP-Protokoll. Die Übertragungsqualität von Medienströmen lässt sich dank moderner Berechnungsmodelle und Algorithmen in verschiedene Kenngrößen gliedern. So fallen bei Echtzeitübertragungen in der Regel folgende Störgrößen ins Gewicht:

Latenz

Latenzen entstehen durch lange Übertragungsstecken und Stauungen aufgrund von Überlastungen des Netzes. Verzögerungen stören den natürlichen Gesprächsfluss massiv, vor allem wenn ein oder mehrere Gesprächsteilnehmer gleichzeitig anfangen zu sprechen. Als Kenngröße werden in der Regel Oneway (Strecke Sender › Empfänger) und Round Trip Time (Strecke Sender › Empfänger › Sender) bewertet.

Paketverluste

Paketverluste werden in UDP/RTP-Echtzeitverbindungen nicht durch das Übertragungsprotokoll kompensiert. Die in den Paketen enthaltene Sprach- oder Videoinformationen gehen daher verloren. Geringe Paketverlustraten (Packet Loss) können vom verwendeten Codec kompensiert werden oder werden vom Gehör des Anwenders überhört. Größere Paketverluste, vor allem wenn sie innerhalb von kurzer Zeit auftreten (Burst Packetloss) können nicht mehr kompensiert werden. Im Gespräch kommt es zu Tonaussetzern oder Frequenzverschiebungen, sodass der Sprecher stark metallisch klingt.

Jitter

Jitter bezeichnet Interwallunterschiede zwischen den Datenpaketen. Moderne Netzwerkkarten verfügen über Pufferspeicher (Jitterbuffer) die zur Wiederherstellung der Taktung und Paketreihenfolge dienen. Zu hoher Jitter kann dafür sorgen, dass der Pufferspeicher überläuft und ggf. Pakete verworfen werden. Es kann vorkommen, dass Pakete aufgrund der Übertragungsstrecke in falscher Reihenfolge an der Gegenstelle ankommen. Diese müssen entweder aufwendig einsortiert werden oder werden ggf. verworfen.

Microsoft Vorgaben für Teams

Der Kunde sollte für eine störungsfreie Übertragung von lokalem Traffic sowie bis zum Übergabepunkt an Microsoft sorgen, wobei die Übertragung zwischen Edgerouter und Microsoft unter der Kontrolle des Providers liegt.

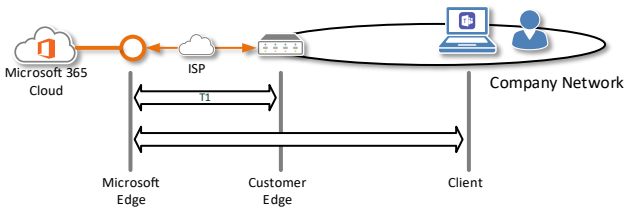

Abbildung 2: Messstrecken

Microsoft gibt Messwerte für zwei Strecken vor. T1 gibt die Strecke zwischen Edge-Netzwerk des Kunden und dem Edge-Netzwerk von Microsoft vor. Die Strecke T2 bezieht sich auf die Strecke von den einzelnen Clients zum Edge-Netzwerk von Microsoft.

	T1 MS Edge ←→ Customer Edge	T2 MS Edge ← → Client
Latency (one way)	30 ms	50 ms
Latency (Round Trip RTT)	60 ms	100 ms
Burst Packetloss (any 200ms interval)	1%	10%
Packetloss (any 15s interval)	0.1%	1%
Packet inter-arrival Jitter	15 ms	30 ms
Packet Reorder (out-of-order packets)	<0.01%	<0.05%

Tabelle 1: QOS Messgrößen für Teams

Die Tabelle zeigt die Vorgaben von Microsoft für ein optimales Nutzungserlebnis. Die Einhaltung der Werte lässt sich im Call Quality Dashboard im Teams Admin Center überwachen.

3. Verbindungsprinzipien / Ziele

Für die optimale Servicequalität werden mehrere Prinzipien verfolgt, auf denen die Optimierungsmaßnahmen basieren. Es wird dringend empfohlen, die Maßnahmen vor einem Flächenrollout abzuschließen.

Direkte UDP Verbindungen

Bei der Echtzeitübertragung von Medienströmen bietet das UDP (User Data Protocol) im Vergleich zum TCP die beste Medienqualität und geringste Latenz. Daher sollte ein Fallback auf TCP und HTTPS jedenfalls vermieden werden. Die Kommunikation zwischen den Clients bzw. mit der Cloud erfolgt idealerweise direkt.

Niedrige Latenzen

Die Bereitstellung der Dienste in der Microsoft Cloud ist auf niedrige Latenz ausgelegt. Netzwerkverbindungen im Netz der Organisation sollten daraufhin optimiert werden, die Daten mit möglichst geringer Latenz in die Microsoft Cloud zu übertragen. Zusätzliche Hops und Umwege durch Routing sollten vermieden werden. Es wird empfohlen für den Microsoft 365 Datenverkehr lokale Internet Ausstiegspunkte bereitzustellen

Hohe Vertrauensstellung

Die Datenübertagung in Microsoft 365 ist prinzipiell verschlüsselt. Ports und Zielnetze sind bekannt und möglichst eng gehalten. Der Datenverkehr sollte daher eine hohe Vertrauensstellung erhalten. Proxyserver und Intursion Prevention Devices müssen daher umgangen werden.

Teams Datenverkehr
Microsoft Teams nutzt für die Verbindungen primär die Ports 3478 bis 3481 UDP. Über diese werden sowohl die Signalisierung als auch die Übertragung der Medienströme abgewickelt.

Signalisierung
Steuerinformationen zwischen den Teams Clients und der Cloud werden über das Signalisierungsprotokoll ausgetauscht. Dies können sowohl Chat-Nachrichten als auch Steuerungsbefehle zum Rufaufbau sein. In Microsoft Teams erfolgt die Signalisierung über eine HTTPS-basierte REST-Schnittstelle, die gegenüber Netzwerkstörungen unempfindlich ist. Allerdings können extreme Latenzen zu entsprechenden Timeouts führen. Die Verschlüsselung ist aufgrund des HTTPS Protokolls nativ.

Das überwiegend in Voice-over-IP-Lösungen (VoIP) eingesetzte SIP Protokoll wird nur noch in Direct Routing Szenarien eingesetzt, in denen Session Border Controller zur Anbindung an das öffentliche Telefonnetz lokal in der Infrastruktur vorgehalten werden.

Echtzeit-Medienverkehr
Moderne IP-Kommunikationslösungen verwenden das SRTP-Protokoll (Secure Real-Time Transport Protocol) zur Übertragung von Sprach- und Videodaten, da der RTP-Medienverkehr gegenüber Netzwerkstörungen empfindlicher ist.

Wie im ersten Blogbeitrag zum Thema Medienqualität (Link setzen) bereits erwähnt, können Latenzen, Jitter und Paketverluste diese stark reduzieren. Daher ist eine direkte Verbindung zwischen den Teilnehmern wichtig, eine Übertragung mittels UDP Protokoll ist hinsichtlich Latenz optimal.

Microsoft Teams unterstützt jedoch auch die Übertragung der Medienströme per TCP-Protokoll. Als zusätzliche Rückfallebene kann der Medienstrom mittels HTTP-Protokoll getunnelt werden – dies sollte aufgrund der massiven Verschlechterung der Medienqualität jedoch vermieden werden. Bei der Verwendung von SRTP wird der Payload aus Sprach- und Videodaten verschlüsselt.

Microsoft Global Network

Abbildung 3: Microsoft Global Network

Microsoft hat ein globales Netzwerk für die optimale Bereitstellung von Azure und Microsoft 365 Services eingerichtet. Das Netzwerk umfasst den gesamten Globus mittels zehntausender Kilometer dedizierter Dark-Fiber-Leitungen und verfügt über Peering-Punkte zu über 2700 Internetprovidern an 190 Internetknoten. An dieses Netzwerk sind die 50+ Rechenzentren von Microsoft angebunden. Die Anzahl der Peering-Punkte wird durch Microsoft stets weiter erhöht, um den für die Kunden kürzesten Weg in die Cloud bereitzustellen.

Das Netzwerk ist für den Transport von Medien und Echtzeitkommunikation optimiert. Medienströme werden priorisiert, sodass Einflüsse wie Latenzen, Jitter und Paketloss auf ein absolutes Minimum reduziert werden. Die Edgesysteme (Azure Front Door) wurden möglichst dicht an den Peering-Punkten platziert, sodass die Anzahl der Hops reduziert wird. Meetings werden in den Rechenzentren möglichst nahe zu den Teilnehmern gehostet.

Media Services

Innerhalb der Microsoft 365 Cloud werden vielfältige Dienste in Form von Microservices bereitgestellt. Alle Services werden innerhalb der Microsoft Azure Infrastruktur gehostet. Für Teams werden Transport Relays, Media Processors und allgemeine Tenant Services bereitgestellt. Das Routing ist so ausgelegt, dass die Media Serivces netzwerktechnisch immer möglichst nah an den Teilnehmern bereitgestellt werden.

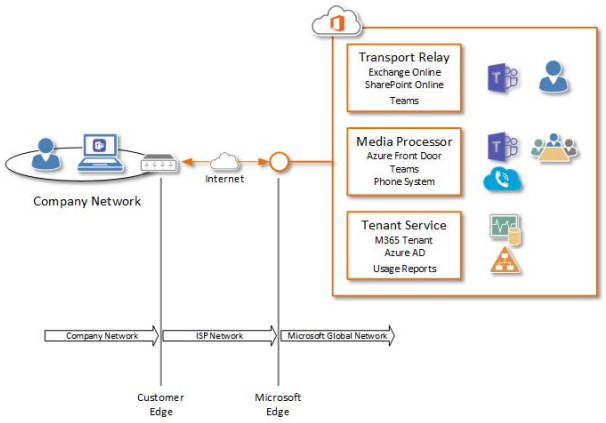

Abbildung 4: Media Services

Transport Relay

Transport Relays sind Knoten zur Datenübertragung und werden als Fallback-Lösung zwischengeschaltet, wenn eine direkte UDP Verbindung zwischen zwei Teams Clients nicht zustande kommen kann. Zusätzlich bieten die Media Relays Möglichkeiten zur Transkodierung von HTTPS und TCP Traffic zu UDP, sodass hier die Verbindungsperformance zwischen den Gesprächsteilnehmern erhöht wird. Die Medienprozessoren sind auf geringe Latenzen optimiert, dennoch ist eine direkte UDP Verbindung zu bevorzugen. Die Aushandlung der Verbindung über ein Transport Relay wird mittels STUN Protokoll durchgeführt.

Media Processor

Medienprozessoren sind Knoten zur Bereitstellung von Telefonie- und Konferenzdiensten. Die Systeme werden netzwerktechnisch möglichst nahe am Kunden bereitgestellt (Azure Front Door), sodass hier möglichst geringe Latenzen auftreten. Konferenzen werden immer in der Cloud gehostet, um eine optimale Erreichbarkeit aller Teilnehmer zu gewährleisten.

Die Medienprozessoren stellen ebenfalls die Systeme für die Anrufverarbeitung der Festnetztelefonie mittels MS Phone System. Teams Anrufe ins Festnetz werden hier lokal ausgeleitet (Calling Plan). Wird die Telefonie lokal beim Kunden über Direct Routing realisiert, so übernehmen die Medienprozessoren die Signalisierung zwischen Session Border Controller und Microsoft 365.

Tenant Services

Die Tenant Services beinhalten sämtliche Backend Dienste der Microsoft 365 Cloud. Hier werden Benutzer, Gruppen und Richtlinien verwaltet. Zusätzlicher Schwerpunkt ist die Vorhaltung von Complience- und Monitoringdaten. Teams erfasst umfassende Daten zur Sprach- und Videoqualität, jedoch keine Gesprächsinhalte. Durch stetiges Monitoring der Qualitätsdaten lassen sich Probleme frühzeitig erkennen und beheben.

4. Optimierungsmaßnahmen

Erreichbarkeit der Microsoft 365 Services

Innerhalb der Microsoft 365 Cloud werden vielfältige Services bereitgestellt. Die meisten Services sind über einen oder mehrere Fully Qualified Domain Name (FQDN) erreichbar. Einzelne Service-Endpunkte liegen in verschiedensten Zielnetzen, die aus dem Firmennetzwerk erreichbar sein müssen.

Zur Priorisierung wurde der Datenverkehr in 3 Verkehrsklassen kategorisiert: „Optimize“, „Allow“ und „Default“:

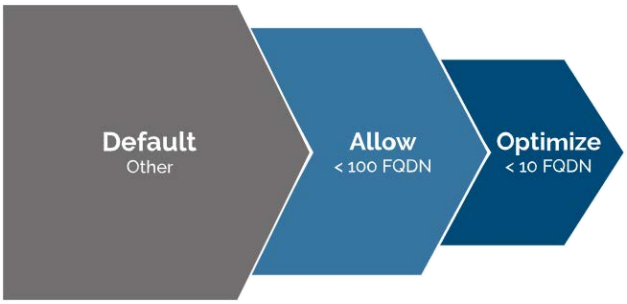

Abbildung 5: Verkehrsklassen

Optimize
Die Verkehrsklasse „Optimize" ist mit weniger als 10 FQDN die kleinste, aber dennoch die wichtigste. In der Klasse befinden sich die kritischen Services von Microsoft 365. Vor allem sind hier die Services für die Echtzeitkommunikation zu finden. Störungen bei Signalisierung und Medienübertragung haben hier den größten Einfluss auf das Nutzererlebnis. Die Optimierung dieser Verbindungen ist daher zwingend erforderlich. Eine Erreichbarkeit muss hierbei stets gewährleistet sein. In puncto IT-Security muss diesen Verbindungen eine sehr hohe Vertrauensstellung eingeräumt werden. Die Datenübertragung findet jederzeit verschlüsselt statt. Die Zielnetze und FQDN sind überschaubar.

Über die Dienste der Verkehrsklasse „Optimize" wird das höchste Datenvolumen umgesetzt, daher sind Änderungen von FQDNs und Zielnetzen sehr selten. Als Optimierungsmaßnahmen werden die folgenden Punkte dringendst empfohlen:
• Umgehung / Deaktivierung von SSL-Inspection
• Proxy Bypass
• Verwendung eines lokalen Internetbreakouts
• Split Tunnel VPN

Allow
In der Verkehrsklasse „Allow" befinden sich ca. 100 FQDN und zugehörige Zielnetze. Als Port kommt hier überwiegend 443 (HTTPS) zum Einsatz. Die Verkehrsklasse hat in der Regel mittleres bis niedriges Datenvolumen. Auch hier muss eine Erreichbarkeit der Dienste sichergestellt werden. Der Datenverkehr ist aufgrund der bekannten Zielnetze und FQDN vertrauenswürdig. Die Datenübertragung findet stets verschlüsselt statt. Microsoft. empfiehlt hier dringend die folgenden Maßnahmen:
• Umgehung / Deaktivierung von SSL-Inspection
• Proxy Bypass

Default
In der Verkehrsklasse „Default" befinden sich unkritische Dienste, die dennoch erreichbar sein sollten. Verbindungen der Klasse Default können wie regulärer Internet-Traffic behandelt werden.

Webservice
Die Liste der FQDN, Zielnetze und Ports ist umfangreich und in stetigem Wandel, da Netze konsolidiert werden oder neue Services hinzukommen. Teils wird die URL- und Endpunktliste monatlich angepasst. Dies stellt insbesondere für das Team der Firewall-Administration vor hohen Wartungsaufwand, um die Erreichbarkeit zu gewährleisten. Zur Vereinfachung können Informationen zu Updates als RSS Feed abgerufen werden. Moderne Firewallsysteme können via Webschnittstelle automatisiert konfiguriert werden. Hierzu stellt Microsoft. eine Web-Schnittstelle bereit, in welcher Regelwerke in verschiedenen Dateiformaten per REST-API Format abgerufen werden können.

Bereitstellung von ausreichender Bandbreite
Das Betreiben eines modernen UC-Systems mit bandbreitenintensiven HD-Videokonferenzen stellt ein Netzwerk vor besondere Herausforderungen. Microsoft gibt Bandbreitenrichtwerte für Anrufe vor (siehe Tabelle) – genaue Bandbreitenberechnungen auf Basis von Netzwerktopologie und Anwender Personas liefert der Netzwerkplaner des Teams Admin Centers.

Wird nicht genügend Bandbreite bereitgestellt, kann Microsoft Teams die Videoauflösung reduzieren, um Qualitätsverlusten entgegenzuwirken. Im schlimmsten Fall kann es dadurch jedoch zu Verbindungsabbrüchen sowie erheblichen Störungen der Medienqualität kommen. Vor allem WAN-Strecken und lokale Internetbreakouts mit unterdimensionierten Bandbreiten können hier Flaschenhälse darstellen.

Bandbreite (up/down)	Modus
30 kbps	1:1 Audioanruf
130 kbps	1:1 Audoanruf mit Screensharing
500 kbps	1:1 Videoanruf mit 360p 30 fps
1,2 Mbps	1:1 HD Videoanruf mit 720p 30 fps
1,5 Mbps	1:1 HD Videoanruf mit 1080p 30 fps
500 kbps / 1Mbps	n:m Videokonferenz
1 Mbps / 2 Mbps	n:m HD Videokonferenz 4x4 540p Videos auf 1080p Bildschirm

Tabelle 2: Bandbreiten für Microsoft Teams

So gewährleisten Sie eine hohe Servicequalität

Quality of Service (Servicequalität) beschreibt die Klassifizierung und Priorisierung von Datenpaketen im Netzwerk. Bei E-Mails, Businessanwendungen oder Dateiübertragungen nimmt der Benutzer in der Regel nicht wahr, wenn Übertragungen länger dauern.

Bei Echtzeit-kommunikationssystemen hingegen führen Störungen des Datenstromes zu Einbrüchen in der Audio- und Videoqualität. Es ist daher dafür zu sorgen, dass Echtzeitdaten möglichst störungsfrei übertragen werden. Durch Markieren der Pakete mit DSCP (Differentiated Services Code Point) Tags und Konfiguration entsprechender Queues auf den Netzwerkkomponenten lassen sich die Daten im Netzwerk priorisieren. Somit werden Stauungen und daraus resultierende Störungen wie Latenzen, Paketverluste und Jitter stark reduzieren. Dies gilt insbesondere, wenn Netzwerkstrecken durch Nebenlasten, wie z.B. Backups stark ausgelastet sind. Prinzipiell sollten entsprechende Bandbreiten im Netz für Voice und ggf. Video reserviert werden.

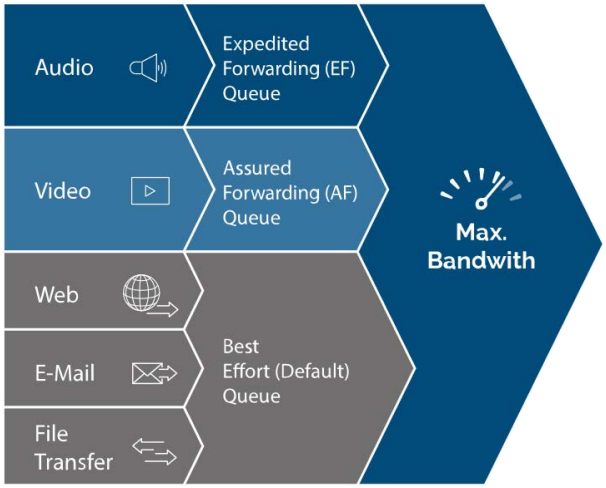

Abbildung 6: QoS Queues

Die Abbildung zeigt die drei QoS Queues die im Netzwerk eingerichtet werden sollten. Für Audio Traffic sollte hier die höchste Priorität (Expedited Forwarding) gesetzt werden, da dieser Traffic am kritischsten in Bezug auf Störeinflüsse ist. Des Weiteren sollten Videoübertragungen mit Priorität gegenüber anderen Nebenlasten behandelt werden. Videoübertragung nutzen erhebliche Bandbreite. Engpässe können sich hier stark auf die Bildqualität und somit das Benutzerempfinden auswirken. Zusätzlich kann eine Queue für Application Sharing eingerichtet werden. Hier sind netzwerkbasierende Störungen allerdings weniger stark wahrnehmbar, sodass viele Organisationen auf eine Einrichtung verzichten.

Microsoft empfiehlt QoS wie folgt zu konfigurieren:

Medientyp	Client source Port	Protokoll	DSCP Wert	DSCP Klasse
Audio	50000-50019	TCP / UDP	46	Expidited Forwarding (EF)
Video	50020-50039	TCP / UDP	34	Assured Forwarding (AF41)
Application Sharing	50040-50059	TCP / UDP	18	Assured Forwarding (AF21)

Tabelle 3: QoS Ports und Queues

Das Setzen der QoS Tags innerhalb der Microsoft 365 Services muss im Teams Admin Center aktiviert werden. Hierbei sind die Portranges durch den Administrator frei wählbar. Die DSCP Werte sind allerdings vorgegeben. Für den Teams Client muss das Tagging per Gruppenrichtlinie (GPO) aktiviert werden. Moderne Netzwerksysteme verfügen über die Möglichkeit, Kommunikationsanwendungen wie Teams anhand von Mustererkennung zu identifizieren und automatisiert zu priorisieren.

Die Umsetzung von QoS im lokalen Netz sollte durch einen Vorabtest verifiziert werden. In der Praxis sollten hier 24/7 Testmessungen über mehrere Wochen mit synthetischen Medienströmen mit Hilfe von im Netz verteilten Messystemen durchgeführt werden. Hierbei ist zu beachten, dass möglichst jede WAN-Strecke geprüft wird.

WLAN

WLANS können aufgrund der zugrundeliegenden Funktechnologien Ursache für starke Qualitätseinbußen sein. Eine Einführung von QoS oder eine Implementation von WiFi Multimedia (WMM) kann hier zu einer Verbesserung der Medienqualität beisteuern. Nach Möglichkeit sollten für die Nutzung von Teams 5 GHz WLANS genutzt werden und 2,4 GHz Netze eher als Fallbacklösung. Für die optimale Platzierung bezüglich Kanalüberlappung und Konfiguration sollten die Best-Practices des jeweiligen Herstellers angewendet werden. Ein Test von Ausleuchtung und Handover wird empfohlen.

Lokaler Internet Breakout

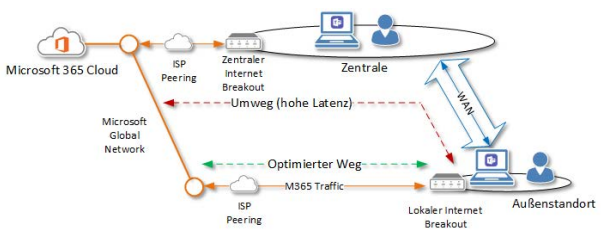

Abbildung 7: Lokaler Internet Breakout

Besonders für Dienste mit der Verkehrsklasse „Optimize“ gilt es, das Microsoft Global Network mit möglichst geringer Latenz zu erreichen. Für Außenstandorte wird daher dringend empfohlen für diese Dienste eine lokale Internetanbindung bereitzustellen. Ein Umweg über WAN Strecken zu einem zentralisierten Internetanschluss würde eine starke Erhöhung der Latenz zur Folge haben. Zusätzlich können Engpässe auf den WAN Strecken zu Störungen der Medienqualität führen.

DNS-Konfiguration

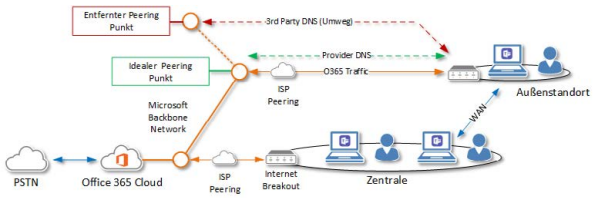

Abbildung 8: DNS-Konfiguration

Bei der Nutzung von 3rd Party DNS-Server z.B. von Google oder Cloudflare kann es dazu kommen, dass nicht optimale Verbindungen aufgebaut werden. Beispielsweise könnte ein Google DNS-Server einen Request mit einer amerikanische IP Adresse für einen Microsoft 365 FQDN beantworten. Somit würde der Teams Client Verbindungen mit der Microsoft Cloud über einen Peering Punkt in Amerika herstellen. Als Resultat können erhebliche Laufzeiterhöhungen auftreten. Prinzipiell sollte daher der DNS des eigenen Internetproviders verwendet werden. Dieser wird in der Regel Requests mit der IP des lokalen oder zumindest nächstmöglichen Peering-Punktes beantworten, sodass ein möglichst schnelles Routing ins Microsoft Netz erfolgen kann.

Proxy Bypass

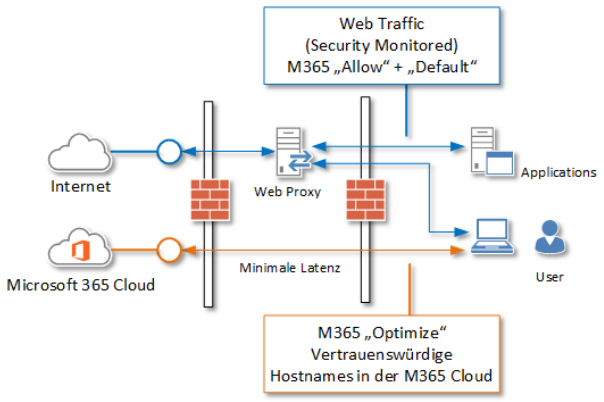

Abbildung 9: Proxy Bypass

Webproxy Server und andere SSL Break & Inspection Systeme können erhebliche Latenzen und Störungen der Datenströme hervorrufen. Besonders schwerwiegend ist der Fall, wenn der Internet-Traffic Cloud-gehostete Inspectionsysteme durchlaufen muss und dann zurück an den Internet-Breakout der Organisation geleitet wird (Network-Hairpinning).

Die Kommunikation zwischen Teams Client und Microsoft 365 Cloud findet ausschließlich verschlüsselt statt. Ein Aufbrechen und Wiederverpacken der Transportverschlüsselung könnte von den Sicherheitsalgorithmen von Microsoft als Man-in-the-Middle-Angriff erkannt werden und zu Störungen führen.

Für die Verkehrsklasse „Optimize“ ist die Anzahl der Zielports und Netze in der Cloud stark limitiert, sodass der Datenverkehr innerhalb dieses Korridors eine besonders hohe Vertrauensstellung attestiert werden kann. In dieser Verkehrsklasse arbeiten die Störanfälligsten Dienste von Microsoft 365 - Insbesondere die Echtzeitkommunikationsdienste von Teams. Microsoft empfiehlt für die Verkehrsklassen „Optimize“ und „Allow“ dringend die Umgehung von Proxyservern und Inspection Devices.

Split Tunnel VPN

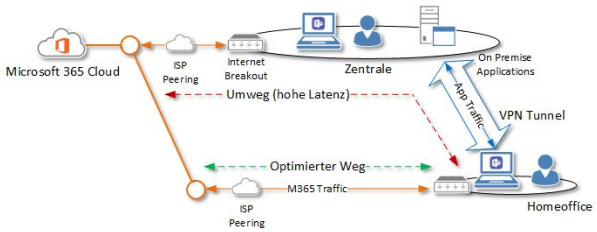

Abbildung 10: Split Tunnel VPN

Immer mehr Organisationen ermöglichen den Arbeitnehmern mobiles Arbeiten bzw. ihre Arbeit im Homeoffice zu verrichten. In der Regel werden die Clients mittels VPN Tunnel mit dem Firmennetzwerk verbunden. Hierbei kann es zu signifikant höheren Latenzen, unter anderem durch mehrfache Verschlüsselung, zu Netzwerkstörungen kommen, wenn Echtzeitmedien über den Umweg des Firmennetzwerks in die Microsoft 365 Cloud geleitet werden. Es wird daher empfohlen, den Microsoft 365 Traffic direkt über den Internet Service Provider des Benutzers abzuwickeln, während der reguläre Anwendungsdatenverkehr durch den VPN Tunnel geleitet wird.

5. Konfiguration für Telefonie

Microsoft Phone System

Bei der Nutzung des Microsoft Phone Systems für die PSTN Telefonie wird die Amtsanbindung direkt innerhalb der Microsoft Cloud realisiert. Die Kommunikationspfade entsprechen hier dem regulären Microsoft 365 Traffic und sind entsprechend der vorangegangenen Maßnahmen zu optimieren. Das Routing kann als Direct Routing, via Media Bypass, mit standortbasiertem Routing oder einem Location Information Service (LIS) für Notrufe erfolgen.

Direct Routing

Mit Direct Routing werden lokale „Session Border

Controller“ (SBC) an die Microsoft 365 Cloud via SIR/RTP angebunden. Der Vorteil daran? Bestehende IP-basierte Amtsanschlüsse können weiterhin betrieben werden. Wenn kein Media Bypass konfiguriert ist, vermittelt der SBC ein- und ausgehenden „Voice over IP“-Traffic (VoIP) an die Microsoft 365 Cloud weiter. Das Gespräch wird dann über die Cloud an den Teams Benutzer weitervermittelt.

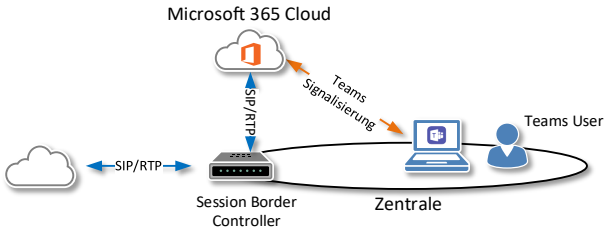

Abbildung 11: Teams Direct Routing

Media Bypass

Die Aktivierung des Media Bypass erlaubt die direkte Übertragung von Medienströmen zwischen SBS und Teams Client. Dadurch vermeidet man Umwege und minimiert das Risiko von Latenzen. Bei der Übertragung sollte die Beeinträchtigung durch Firewalls und andere Inspection Devices vermieden werden. In diesem Szenario empfehlen wir dringend den Einsatz von QoS Queues (Link zu Blogbeitrag Optimierungsmaßnahmen).

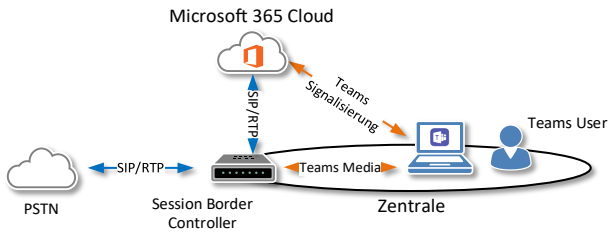

Abbildung 12 Teams Routing via Media Bypass

Standortbasiertes Routing

Um Anrufe anhand eines Standorts zu routen („Location Based Routing“), muss die Netzwerktopologie der Organisation im Teams Admin Center eingepflegt werden. Hierzu können mehrere Regionen mit den jeweils zugehörigen Standorten (Sites) angelegt werden. Jeder Standort verfügt über eine Liste der zugehörigen Subnetze und eine externe IP-Adresse über welche die Kommunikation mit der Microsoft 365 Cloud abgewickelt wird. Anhand des Standortes wird identifiziert, welcher SBS für die Abwicklung der PSTN Telefonie optimal ist. Zusätzlich werden die lokalen Wahlregeln (Dialplan) und Richtlinien angewendet (Policies).

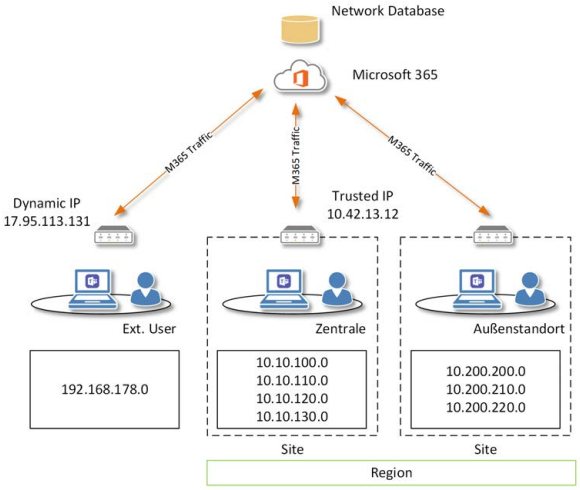

Abbildung 13: Netzwerk Topologie

Local Media Optimization

Local Media Optimization erweitert das vorher beschriebene Direct-Routing-Szenario mit der Einbindung von weiteren Session Border Controllern und Mediagateways, die keine direkte Anbindung an die M365 haben.

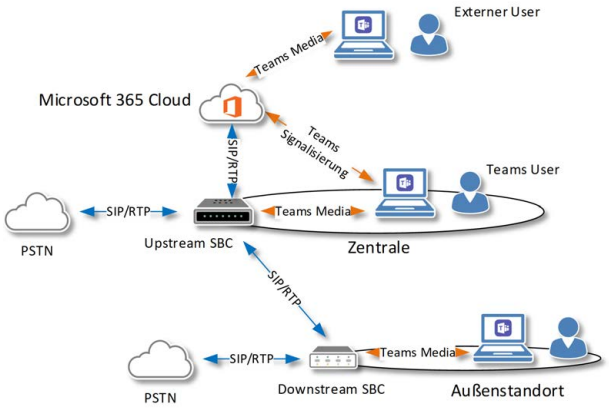

Abbildung 14: Darstellung eines Netzes mit Local Media Optimization

In der obenstehenden Grafik verfügt der Außenstandort über keinen lokalen Internetbreakout. Lediglich ein SIP-Trunk (ggf. auch ISDN Anschluss) ist als PSTN-Anbindung verfügbar. Der Downstream SBC leitet in diesem Szenario die Signalisierung an den Upstream SBC in der Zentrale weiter, welcher wiederum die Signalisierung mit der M365 Cloud übernimmt. Der Medienverkehr in Richtung PSTN erfolgt lokal am Außenstandort zwischen Teams Client und Downstream SBC.

Die Auswahl des zum User gehörenden SBC ist vergleichbar mit dem „Location Based Routing" und erfolgt via Netzwerk, WLAN oder Region. Externe User und User, die an mehreren Standorten tätig sind können entweder dynamisch den nächsten SBC nutzen oder an den SBC ihres Heimatstandortes gebunden werden, sodass die Telefonie immer über den Heimat-SBC erfolgt.

Location Information Service (LIS) für Notrufe

Um Notrufen abzuwickeln, müssen Netzwerkobjekte mit realen Standortadressen verknüpft werden. Im Teams Admin Center können hierfür Subnetze, Chassis IDs von Netzwerkswitchen, Switchports oder WLAN SSIDs hinterlegt werden.

Jedes Netzwerkobjekt wird mit der Adresse des Standortes verknüpft und erhält ein zusätzliches Identifizierungsmerkmal, z.B. eine Stockwerk- oder Raumnummer.

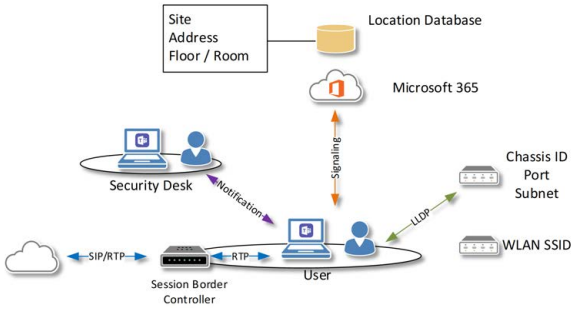

Abbildung 15: Darstellung eines LIS für Notrufe

Beim Start prüft der Client automatisch, ob LIS Informationen vorliegen. Die Bestimmung von Chassis ID und Port erfolgt über eine Link-Layer-Discovery-Protocol (LLDP) Abfrage. Subnetz und WLAN-SSID werden aus dem Betriebssystem ausgelesen. Die gewonnenen LIS Informationen werden mit der Location Database in der Microsoft 365 Cloud abgeglichen. Wird eine Übereinstimmung festgestellt, werden automatisch die entsprechenden Notrufrouting- und Wahlrichtlinien (Policies) gesetzt. Danach wird ein Notruf über den lokalen SBC an die für den Standort zuständige Rettungsleitstelle weitergeleitet. In den Richtlinien kann man ebenfalls konfigurieren, ob die Sicherheitswarte (Security Desk) benachrichtigt werden soll.

6. Assessment und Monitoring

Um den Erfolg der Maßnahmen zu prüfen, sollten vorher und nachher Assessments durchgeführt werden. Hierzu wird eine Reihe von Tools durch Microsoft bereitgestellt:

Network Planner

Der Network Planner ist ein Tool, das im Vorfeld zur Berechnung von Bandbreiten eingesetzt wird. Diese können anhand der Netzwerktopologie und der individuell konfigurierbaren Personas ermittelt werden. Dabei kann für jede Persona die Häufigkeit der Dienstnutzung (Anrufe, Videokonferenzen, Application Sharing) separat konfiguriert werden.

Network Testing Companion

Das Network Testing Companion Tool unterstützt beim Assessment und beim Troubleshooting aus der Clientperspektive. Das Tool benötigt keinen M365 und kann auf beliebigen Windows Clients installiert werden. Die Verbindungstests sollen eine Erreichbarkeit aller bekannten M365 Endpunkte sicherstellen. Die Sprachqualitätstests geben Auskunft über Probleme bei der Medienübertragung. Mit Hilfe des Tools kann sich ein Admin ein schnelles Lagebild bei Clientproblemen verschaffen. Vor allem bei Problemen die bei Clients im Homeoffice im Zusammenhang mit WLAN oder VPN auftreten können.

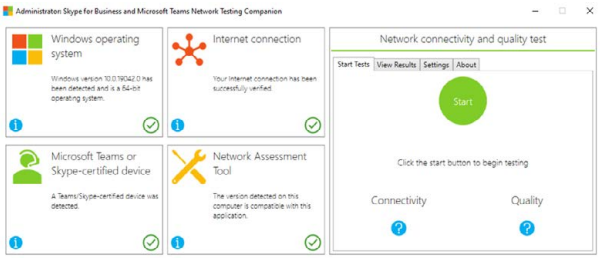

Abbildung 15: Darstellung des Network Testing Companion

Das Tool bietet die folgenden Funktionen:

- **Betriebssystem**: Das Tool führt eine Kompatibilitätsprüfung anhand der Betriebssystemversion durch
- **Internetverbindung:** Das Tool führt eine Kurzprüfung zur generellen Erreichbarkeit des Internets durch.
- **Zertifiziertes Endgerät:** Die Wahl des Endgerätes kann die Sprachqualität massiv beeinflussen. Den Endanwendern sollte in jedem Fall ein für Microsoft Teams zertifiziertes Endgerät zur Verfügung gestellt werden.
- **Connectivity Check:** Hier findet ein Verbindungsaufbau zu allen bekannten O365-Endpunkten in der Cloud über die Ports 3478 UDP, 443 TCP und HTTPS (443) statt. Das Ergebnis wird als Textdatei bereitgestellt.
- **Voice Quality Check:** Dieses Tool baut einen ca. 17 Sekunden langen Sprachanruf zu Teams auf und misst während des Calls gängige QoS Werte, wie Round Trip Time (RTT), Paket Loss und Jitter. Das Ergebnis wird in einer CSV Datei zusammengefasst. Für Langzeittests können bis zu 50 Tests sequenziell durchgeführt werden. Als Intervall zwischen den einzelnen Tests können bis zu 120 Sekunden eingestellt werden.
- **Ergebnisanzeige:** Das Tool wertet die Messergebnisse anhand der Microsoft-Vorgaben aus. Hierbei wird zwischen Client-Computer und Edge-Netzkomponenten differenziert. Für Edge-Komponenten gelten schärfere Vorgaben als für Clientgeräte.

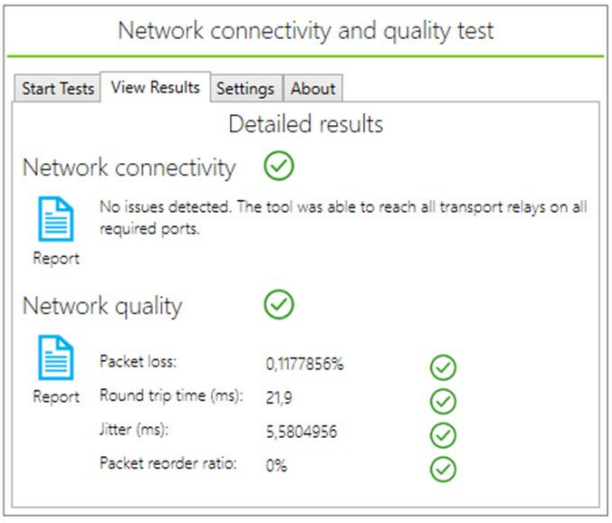

Abbildung 16: Qualitätstest

Call Quality Dashboard

Sowohl für die Pilotphase als auch für den Betrieb ist eine stetige Überwachung der Medienqualität unerlässlich. Das Call Quality Dashboard bietet hierfür umfangreiche Übersichten. Zum Troubleshooting können einzelne Anrufe direkt analysiert werden.

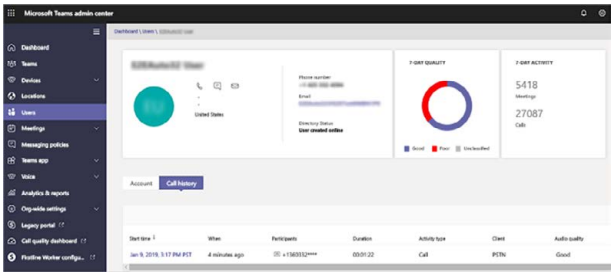

Abbildung 17: Dashboard der Anrufqualität

7. Fazit

Für die optimale Dienstqualität wird dringend empfohlen Maßnahmen im Organisationsnetzwerk umzusetzen. Schlechte Medienqualität führt zu einer erheblichen Reduzierung der Benutzerakzeptanz bei der Einführung von Microsoft Teams.

Teams Medienströme sind empfindlich gegenüber Latenzen und Netzwerkstörungen. Um diese zu vermeiden sollte der Traffic ohne Umwege in Richtung Microsoft 365 Cloud geleitet werden. Arbeiten am Netzwerk sollten nur außerhalb der Geschäftszeiten stattfinden. Für Außenstandorte wird ein lokaler Internet Breakout mit ausreichender Bandbreite empfohlen. Quality of Service Maßnahmen erhöhen die Medienqualität im Netz signifikant.

8. Quellen

Foliensatz Teams Calling & Meeting Bootcamp - Teams Networking – Bryan Nyce, Microsoft

https://docs.Microsoft.com/en-us/Microsoft-teams/prepare-network

http://www.djeek.com/2018/01/Microsoft-teams-and-the-protocols-it-uses-opus-and-mnp24/

https://docs.Microsoft.com/de-de/office365/enterprise/office-365-network-connectivity-principles

https://docs.Microsoft.com/de-de/office365/enterprise/office-365-network-connectivity-principles#BKMK_SecurityComparison

https://docs.Microsoft.com/de-de/Microsoft-teams/cloud-voice-network-settings

https://docs.Microsoft.com/en-us/office365/enterprise/external-domain-name-system-records?redirectSourcePath=%252farticle%252fExternal-Domain-Name-System-records-for-Office-365-c0531a6f-9e25-4f2d-ad0e-a70bfef09ac0

https://docs.Microsoft.com/en-us/office365/enterprise/network-and-migration-planning#BestPractices

https://docs.Microsoft.com/en-us/Microsoft-teams/proxy-servers-for-skype-for-business-online

https://docs.Microsoft.com/de-de/Microsoft-teams/office-365-urls-ip-address-ranges

https://docs.Microsoft.com/de-de/Microsoft-teams/qos-in-teams

https://docs.Microsoft.com/en-us/Microsoft-teams/configure-dynamic-emergency-calling

https://docs.Microsoft.com/en-us/Microsoft-teams/prepare-network

https://blogs.perficient.com/2019/02/13/-plan-your-network-Microsoft-teams-2019-part-4/

https://docs.Microsoft.com/en-us/Microsoft-teams/Microsoft-teams-online-call-flows

in2success GmbH

Am Forstanger 45
82041 Oberhaching

mail: info@in2success.de
tel: +49 89 2620 727 97

www.in2success.de

WEIL ERFOLG MACHBAR IST