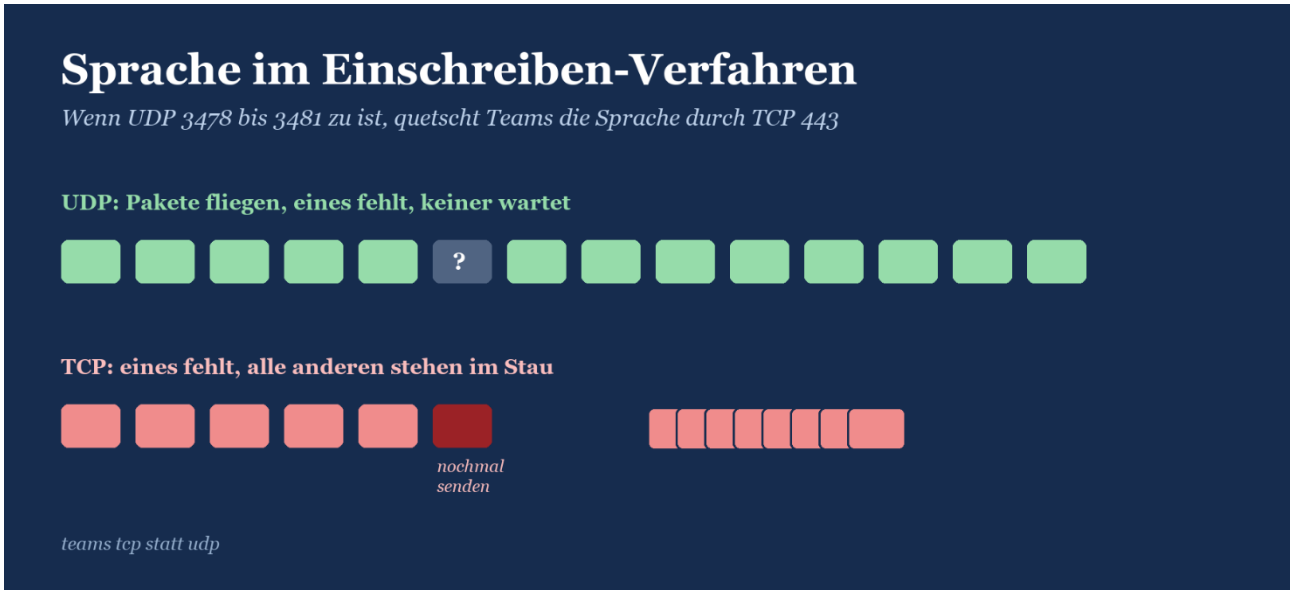
Teams-Telefonie über TCP statt UDP: warum das schlecht klingt



WISSEN

Alles zur Teams-Telefonie: Direct Routing, SBC, Wählpläne, Routing, Notruf und Betrieb an einem Ort.

› **Teams-Telefonie**

BERATUNG

Teams klingt an einem Standort schlecht und keiner weiß, warum? Wir lesen mit dir die Anrufdaten und das Firewall-Regelwerk.

› **Beratung zur Teams-Telefonie**

SCHULUNG

Für Admins, die Medienwege, Ports und Anrufdaten selbst lesen und Fehler im Netz sicher eingrenzen wollen.

› **Schulung Teams-Telefonie**

Teams funktioniert. Das ist das Tückische. Der Anruf baut sich auf, der Ton kommt an, niemand bekommt eine Fehlermeldung. Es klingt nur so, als würde dein Gegenüber aus einem Aquarium anrufen, in dem gerade jemand die Pumpe repariert. Und weil nichts kaputt ist, sucht auch niemand. Das Ticket heißt „Teams klingt mal wieder komisch“, wird mit „WLAN prüfen“ beantwortet und geschlossen.

Eine der häufigsten Ursachen dafür sitzt nicht in Teams, sondern in der Firewall: Die Ports UDP 3478 bis 3481 sind gesperrt. Teams gibt dann nicht auf, sondern weicht aus. Die Sprache läuft per TCP über Port 443, im ungünstigsten Fall durch den Web-Proxy. Microsoft beschreibt diesen Weg selbst als letzten Ausweg und rät wegen der Qualitätsfolgen davon ab. Das Gespräch kommt zustande, es klingt nur schlecht. Und zwar genau dann, wenn das Netz ohnehin schon wackelt.

Dieser Beitrag gehört zur Serie rund um die Teams-Telefonie und ist problemorientiert. Du bekommst das Symptom, die technische Ursache, eine Diagnose mit lesenden Werkzeugen, die Behebung mit Rollback und ein paar Regeln, damit es nicht wiederkommt. Wie QoS, Call Quality Dashboard und Klassifizierung grundsätzlich funktionieren, steht in Sprachqualität in Teams: QoS, CQD und Troubleshooting; hier geht es um den einen Fehler, bei dem Teams zu höflich ist, um sich zu beschweren.

FAKTEN · Das Beispiel in diesem Beitrag

Erfundener Tenant Contoso (contoso.com) mit Standorten in Frankfurt, Köln, Berlin, Hamburg und München. Zentraler Internetausgang mit Web-Proxy in Frankfurt (öffentlich 203.0.113.10), Berlin mit dem Subnetz 10.40.0.0/16 und einem eigenen Router, der nach dem Tausch im Frühjahr nur

noch TCP 80 und 443 nach außen durchlässt. SBCs sbc1.contoso.com (Frankfurt) und sbc2.contoso.com (Hamburg), Rufnummern im Muster +49 30 555 0100 für Berlin. Alle Namen, Adressen und Nummern sind erfunden.

Das Symptom: Es geht, aber es klingt nach Blechdose

So klingt es im Helpdesk

TCP statt UDP meldet sich nie mit Namen. Es meldet sich über Nebenwirkungen, und die Tickets sind erstaunlich treffsicher, wenn man sie übersetzt:

- **„Im Homeoffice klingt Teams besser als im Büro."** Der Klassiker. Zu Hause ist UDP offen, im Büro nicht. Selten war ein Satz so verdächtig.
- **„Am Anfang ist es gut, dann wird es immer schlimmer, und zwischendurch kommt alles auf einmal."** Verzögerung, die sich aufstaut und dann schlagartig abbaut. Typisch für TCP bei Paketverlust.
- **„Wir reden ständig gleichzeitig."** Mehr Laufzeit. Proxy, TLS-Inspektion und Umwege über die Zentrale summieren sich.
- **„Nur wenn das Backup läuft" oder „nur nachmittags".** Sobald die Leitung voll wird, steigen Verluste, und TCP macht aus jedem Verlust eine Wartepause.
- **„Mit dem Handy über Mobilfunk ist alles gut."** Gleiche App, anderes Netz, keine gesperrten Ports. Der Fehler liegt im Firmennetz.
- **„In Berlin ist es schlimm, in Köln nicht."** Ein Standort mit eigener Regel, eigenem Router oder eigenem Proxy-Profil.

Auffällig ist auch, was nicht passiert: Es gibt keinen Fehlercode, keinen Abbruch beim Verbindungsaufbau und keinen roten Hinweis im Client. Die Anrufe tauchen im Call Quality Dashboard auch nicht als Totalausfall auf, sondern als Streams, die öfter als schlecht klassifiziert werden. Microsoft klassifiziert einen Audiostream als schlecht, wenn der durchschnittliche Roundtrip über 500 ms, der Paketverlust über 10 Prozent oder der Jitter über 30 ms liegt. TCP reißt keine dieser Grenzen zwangsläufig. Es macht nur alle drei wahrscheinlicher.

Wer betroffen ist und wer nicht

Situation	Typisches Bild	Wahrscheinlich TCP?
Ganzer Standort oder ganzes Subnetz	Schlechte Qualität an einem Ort, überall sonst gut	Ja, Regel am Standort-Router, an der Firewall oder im Proxy-Profil
Nur Gast-WLAN oder Besprechungsräume	Teams Rooms und Gäste klingen schlecht	Häufig, Gastnetze erlauben oft nur Web-Verkehr
Nur mit VPN	Homeoffice gut, mit VPN schlecht	Oft, wenn der VPN-Tunnel kein UDP trägt oder alles durch den Proxy schickt
Einzelne Personen unterwegs	Hotel, Bahn, Kundennetz	Ja, aber nicht dein Problem. Fremde Netze kannst du nicht reparieren.
Alle, überall, gleichmäßig	Kein Muster nach Ort	Eher nicht. Dann lohnt der Blick auf Endgeräte, Treiber oder die Internetanbindung

Wie der Fehler technisch entsteht

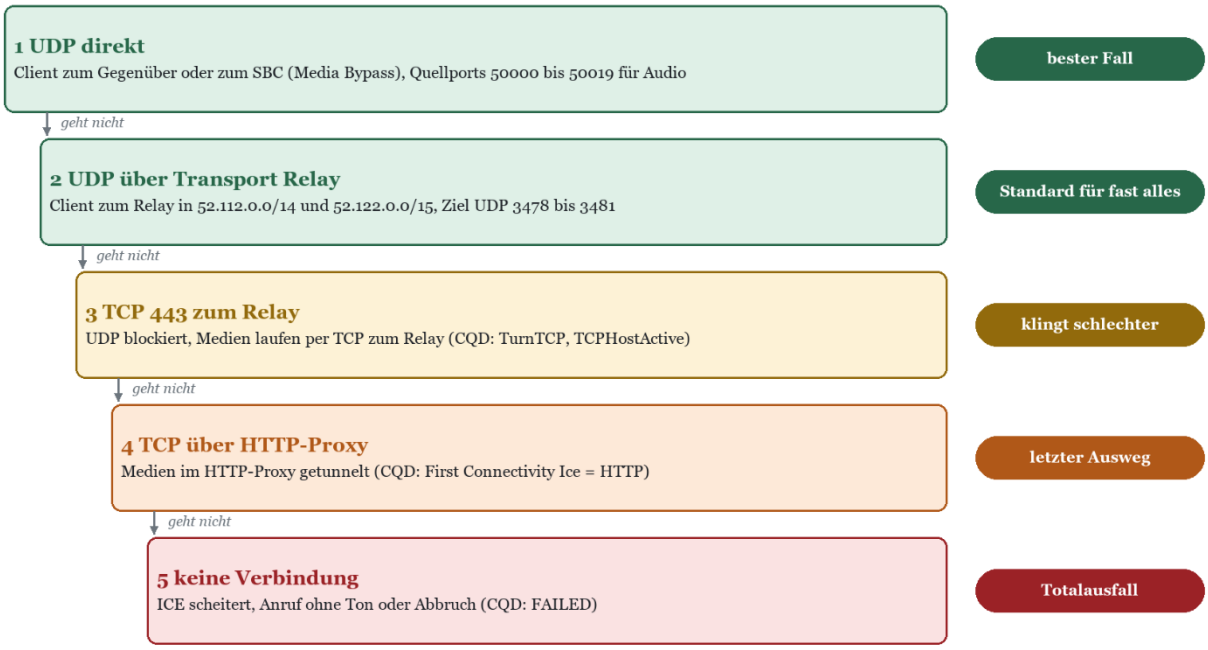
Was Teams eigentlich will

Teams verhandelt den Medienweg für jeden Anruf mit ICE (Interactive Connectivity Establishment). Der Client sammelt Kandidaten: seine lokale Adresse, seine öffentliche Adresse, wie ein Relay sie sieht, und eine Adresse auf einem Microsoft Transport Relay. Dann prüft er, welche Wege tatsächlich funktionieren, und nimmt den besten. Für Sprache ist das UDP. Microsoft formuliert es unmissverständlich: Echtzeitmedien sollen den direktesten Weg nehmen und UDP statt TCP verwenden. Als letzter Ausweg können Medien TCP nutzen und sogar im HTTP-Protokoll getunnelt werden, das wird aber wegen der schlechten Qualität nicht empfohlen. Die Details stehen in Microsoft Teams-Anrufflüsse.

Damit UDP funktioniert, müssen Clients die Microsoft-Netze 52.112.0.0/14 und 52.122.0.0/15 (IPv6 2603:1063::/38) auf UDP 3478 bis 3481 erreichen. In der offiziellen Liste der Microsoft 365-Endpunkte ist das der Eintrag mit der ID 11, Kategorie Optimize, erforderlich. Microsoft nennt die Ports im Dokument zu den Anrufflüssen auch einzeln: 3478 für STUN, 3479 für Audio, 3480 für Video und 3481 für Bildschirmfreigabe. Daneben braucht Teams TCP 443 und 80 sowie UDP 443 (ID 12) für Signalisierung, Chat und als Rückfallweg. Die aktuellen Adressen stehen immer in Microsoft 365-URLs und -IP-Adressbereiche.

Die Rückfallkaskade: Was Teams versucht, wenn UDP nicht durchkommt

ICE prüft die Kandidaten und nimmt den besten Weg, der funktioniert. Von oben nach unten wird es schlechter.



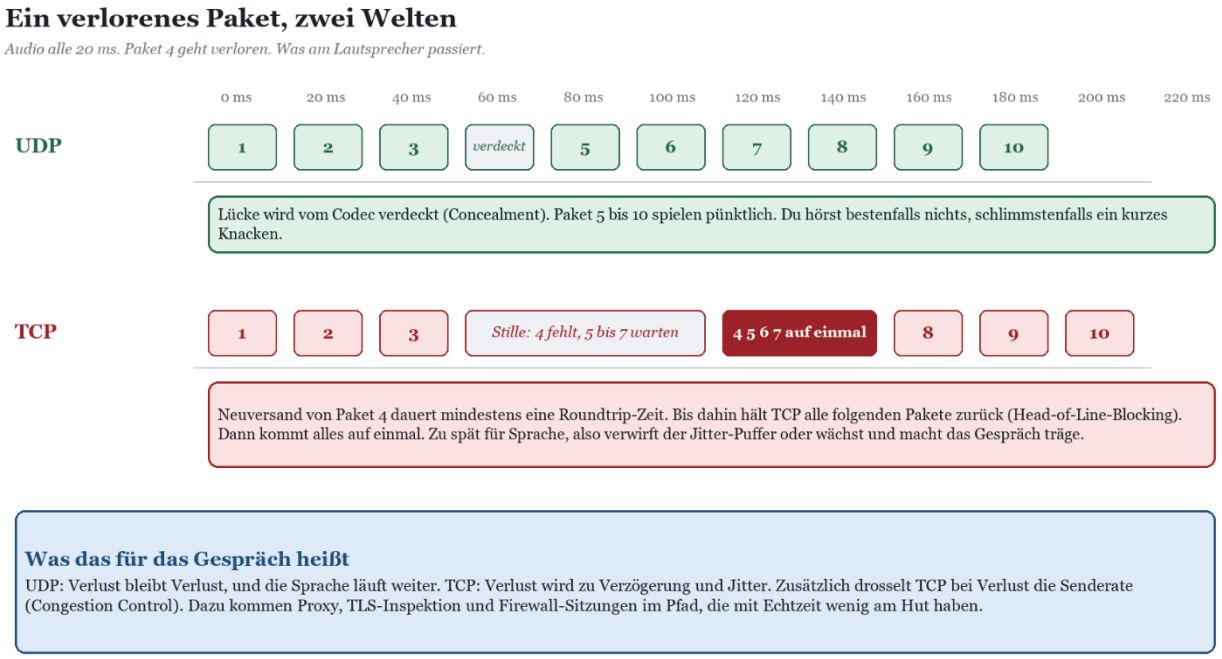
Contoso Berlin landete auf Stufe 3: UDP am Standort-Router gesperrt, TCP 443 offen.

Was passiert, wenn UDP gesperrt ist

Ist UDP zum Relay blockiert, scheitern die UDP-Kandidaten in der ICE-Prüfung. Teams fällt auf TCP zurück: direkt per TCP 443 zum Relay, und wenn auch das nicht geht, durch den konfigurierten HTTP-Proxy. Im Call Quality Dashboard heißen diese Wege zum Beispiel TurnTCP (eine TCP-Zuweisung am Relay, die den Proxy nutzt, wenn einer konfiguriert ist), TCPHostActive oder CompoundTCP. Und das Gemeine daran: Der Anruf funktioniert. Niemand bekommt eine Fehlermeldung, und genau deshalb bleibt der Fehler oft monatelang unentdeckt.

Warum TCP für Sprache schlecht ist

TCP ist für Dateien gebaut. Es garantiert, dass jedes Byte ankommt, und zwar in der richtigen Reihenfolge. Für eine PDF ist das großartig. Für Sprache ist es Gift, denn ein Wort, das 400 ms zu spät kommt, ist kein Wort mehr, sondern ein Störgeräusch. UDP liefert ohne Garantie: Ein verlorenes Paket ist weg, der Audio-Codec überbrückt die Lücke, und das Gespräch läuft weiter. TCP dagegen hält alles an, bis das verlorene Paket erneut gesendet wurde. Die Fachleute nennen das Head-of-Line-Blocking, die Anwender nennen es „Teams hängt“.



Eigenschaft	UDP 3478 bis 3481	TCP 443 (direkt oder über Proxy)
Paketverlust	Verlust bleibt Verlust, der Codec verdeckt die Lücke	Verlust wird zu Wartezeit, danach kommen mehrere Pakete auf einmal
Laufzeit	Kurz, kein Neuversand	Mindestens eine zusätzliche Roundtrip-Zeit je Neuversand
Jitter	Hängt vom Netz ab	Steigt, weil Pakete gestaut und gebündelt ankommen
Bandbreite bei Störung	Teams regelt selbst nach	TCP drosselt zusätzlich, zwei Regelkreise arbeiten gegeneinander
Geräte im Pfad	Firewall, NAT	Zusätzlich Proxy, Authentifizierung, oft TLS-Inspektion
QoS	DSCP-Markierung über Quellports greift	Markierung ist möglich, aber Proxy und Inspektion im Pfad bremsen trotzdem
Microsofts Einschätzung	Empfohlen	Unterstützt, aber nicht empfohlen

WICHTIG · Der Proxy ist kein Echtzeitgerät

Ein Web-Proxy ist dafür gebaut, Webseiten zu prüfen, zwischenzuspeichern und zu protokollieren. Er ist nicht dafür gebaut, Audiopakete im 20-Millisekunden-Takt mit gleichmäßigem Abstand durchzureichen. Microsoft empfiehlt in der QoS-Dokumentation, Hindernisse wie Proxys aus dem Weg zu nehmen, und rät in der Dokumentation zu den Anrufflüssen von Paketinspektion und Paket-

Shapern für Teams-Medien ab. Endpunkte der Kategorie Optimize sollen am Proxy vorbei direkt ins Internet.

Und Direct Routing?

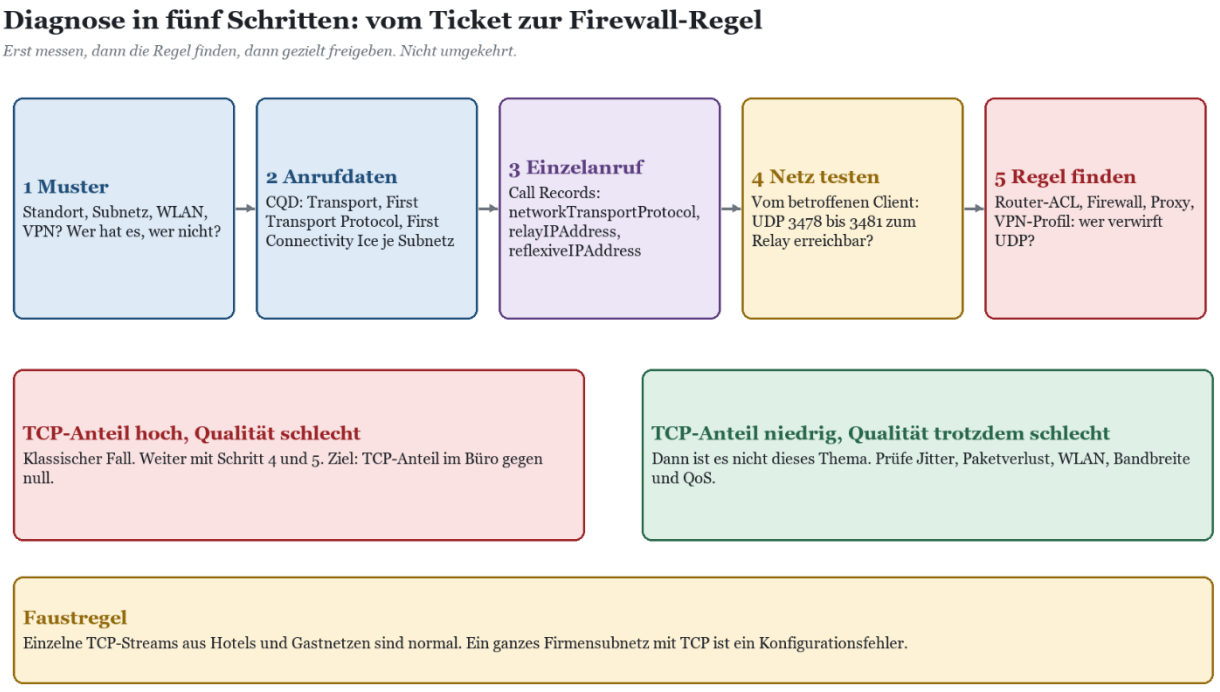
Bei Direct Routing gibt es zwei Medienstrecken, und nur eine davon hat einen TCP-Rettungsring. Die Strecke vom Teams-Client zum Media Processor oder Relay kann, wie oben beschrieben, auf TCP ausweichen. Die Strecke zwischen deinem SBC und Microsoft dokumentiert Microsoft dagegen ausschließlich als UDP/SRTP: zu den Media Processors auf 3478 bis 3481 und 49152 bis 53247, zu den Transport Relays auf 50000 bis 59999 und 3478 bis 3481. Mit Media Bypass laufen die Medien zwischen Client und SBC ebenfalls per UDP, auf der Clientseite mit den Quellports 50000 bis 50019. Ist dort UDP zu, gibt es keinen eleganten Rückfall, sondern einseitiges Audio oder Stille. Das behandelt Einseitiges Audio oder kein Ton bei Teams Direct Routing. Wie Media Bypass grundsätzlich arbeitet, steht in Teams Media Bypass und Local Media Optimization.

AUS DER PRAXIS · Ulis anynode-SBC und die Firewall, die es gut meinte

In meinem eigenen Aufbau mit einem anynode-SBC hat ein Update der Firewall die Regel für ausgehendes UDP auf ein „aufgeräumtes“ Adressobjekt umgestellt, in dem ein Teil der Microsoft-Netze fehlte. Ergebnis: Einzelne Anrufe waren still, andere liefen. Der SBC hat keinen TCP-Plan B, also fiel es sofort auf. Die Teams-Clients am selben Anschluss dagegen hatten einen Plan B, sind brav auf TCP umgestiegen und haben wochenlang niemanden gestört, außer den Ohren. Lehre: Der SBC beschwert sich laut, der Client leidet leise.

Diagnose Schritt für Schritt

Die Diagnose ist rein lesend, bis du die Regel gefunden hast. Du brauchst Leserechte im Teams Admin Center und im Call Quality Dashboard, das PowerShell-Modul MicrosoftTeams und jemanden aus dem Netzwerkteam, der Firewall-Protokolle lesen darf. Plan dir keine Änderung am Tenant ein: Die Ursache liegt fast nie in Teams.



Die Schritte 1 bis 4 sind rein lesend. Erst nach Schritt 5 ändert etwas, und zwar am Netz, nicht an Teams.

Schritt 1: Muster finden

Sammle zu jedem Ticket Ort, Netz und Gerät: Standort, kabelgebunden oder WLAN, VPN ja oder nein, Teams-Desktop oder Browser. Wenn sich die Beschwerden auf einen Standort, ein Gebäude oder ein Netz verdichten, bist du richtig. Wenn sie gleichmäßig über alle Orte verteilt sind, eher nicht.

Schritt 2: Anrufdaten im Call Quality Dashboard

Im Call Quality Dashboard (CQD) baust du einen eigenen Bericht für Audiostreams der letzten Wochen. Die entscheidenden Dimensionen sind:

Dimension	Was sie zeigt	Worauf du achtest
Transport	Transportprotokoll des Streams: UDP, TCP oder Unrecognized	Anteil TCP je Gebäude oder Subnetz
First Transport Protocol, Second Transport Protocol	Wie der jeweilige Endpunkt Medien sendet, zum Beispiel UDP, TurnTCP, TCPHostActive, CompoundTCP	Alles außer UDP ist ein TCP-Weg
First Connectivity Ice, Second Connectivity Ice	DIRECT, RELAY, HTTP (über HTTP-Proxy) oder FAILED	HTTP heißt: Medien durch den Proxy. FAILED heißt: gar keine Verbindung
First Subnet, Second Subnet, Gebäudename	Woher der Stream kommt	Gebäudenamen gibt es nur, wenn du Gebäudedaten in CQD hochgeladen hast
Audio Poor Due To Jitter, RoundTrip, PacketLoss	Warum ein Stream als schlecht gilt	Bei TCP stehen oft Jitter und Roundtrip vorn

Filtere auf Audio und lass dir Streamanzahl und Anteil schlechter Streams je Subnetz und Transport ausgeben. Bei Contoso sah das Ergebnis so aus: Berlin mit knapp 39 Prozent TCP und 18 Prozent schlechten Audiostreams, alle anderen Standorte bei rund zwei Prozent TCP. Zwei Prozent sind normal, das sind Leute im Hotel, im Zug oder im Netz eines Kunden. 39 Prozent sind ein Firmennetz, das UDP verbietet.

> **TIPP · Ohne Gebäudedaten ist CQD nur halb so gesprächig**
>
> CQD ordnet Streams nur dann Standorten zu, wenn du eine Gebäudedatei mit deinen Subnetzen hochgeladen hast. Ohne diese Datei siehst du nur Subnetze und musst im Kopf übersetzen, dass 10.40.0.0/16 Berlin ist. Bei einem Maschinenbauer mit zwölf Standorten haben wir so drei Wochen lang das falsche Werk verdächtigt, weil ein Subnetz nach einem Umzug noch dem alten Gebäude zugeordnet war.
>
> Wie du Subnetze, Standorte und Gebäudedaten konsistent hältst, steht in Netzwerkstandorte und Subnetze in Teams richtig pflegen.

Schritt 3: Einzelne Anrufe prüfen

Für einen konkreten Anruf öffnest du im Teams Admin Center unter Benutzer › Benutzer verwalten den betroffenen Benutzer und dort den Anrufverlauf. In den erweiterten Details eines Anrufs findest du je Stream Angaben zum Netzwerk, darunter den Transport, die Relay-Adresse sowie lokale und öffentliche Adresse. Steht dort für einen Anruf aus dem Büro TCP, hast du einen Treffer.

Wer lieber skriptet, liest die Call Records über Microsoft Graph. Das Objekt networkInfo eines Medienstreams enthält die Eigenschaft networkTransportProtocol mit den Werten udp, tcp oder

unknown, dazu relayIPAddress, reflexiveIPAddress und subnet. Damit kannst du den TCP-Anteil je Subnetz selbst zählen. Wie du Call Records abholst und auswertest, beschreibt Teams-Anrufprotokolle auswerten: Call Records statt Bauchgefühl.

Schritt 4: Tenant-Konfiguration lesen

Im Tenant suchst du nicht nach dem Fehler, sondern nach den Angaben, die das Netzwerkteam braucht: Welche Subnetze gehören zu welchem Standort, welche öffentlichen Adressen kennt Teams, welche Quellports benutzen die Clients, und arbeiten deine SBCs mit Media Bypass? Alle Befehle sind rein lesend.

```
# Verbindung mit dem MicrosoftTeams-Modul
Connect-MicrosoftTeams

# Netzwerkstandorte und Subnetze: Ist 10.40.0.0/16 Berlin zugeordnet?
Get-CsTenantNetworkSite | Select-Object NetworkSiteID, NetworkRegionID, Description
Get-CsTenantNetworkSubnet | Sort-Object NetworkSiteID |
    Select-Object SubnetID, MaskBits, NetworkSiteID

# Öffentliche Adressen, die Teams als Firmennetz kennt
Get-CsTenantTrustedIPAddress | Select-Object IPAddress, MaskBits, Description

# Quellports der Clients (für Firewall-Regeln und QoS)
Get-CsTeamsMeetingConfiguration | Select-Object ClientMediaPortRangeEnabled,
    ClientAudioPort, ClientAudioPortRange, ClientVideoPort, ClientVideoPortRange,
    ClientAppSharingPort, ClientAppSharingPortRange

# SBCs: aktiv und mit Media Bypass?
Get-CsOnlinePSTNGateway | Select-Object Identity, Enabled, MediaBypass
```

Microsoft empfiehlt als Startwerte für die Client-Quellports 50000 bis 50019 für Audio, 50020 bis 50039 für Video und 50040 bis 50059 für Bildschirmfreigabe. Diese Bereiche helfen dir später in Firewall-Protokollen: UDP-Pakete von Quellport 50000 bis 50019 aus Berlin sind Teams-Audio. Wenn du verworfene Pakete mit genau diesen Quellports findest, ist die Diagnose praktisch erledigt.

Schritt 5: Vom Client aus testen und die Regel finden

Jetzt wechselst du die Perspektive und prüfst vom betroffenen Rechner aus, ob UDP zu den Relays durchkommt. Das bekannte Test-NetConnection hilft hier nur halb, denn es prüft ausschließlich TCP. Für UDP nimmst du das Microsoft Teams Network Assessment Tool, das Microsoft zum Download anbietet: Es prüft die Verbindung zu den Teams-Relays und misst Verlust, Jitter und Laufzeit. Ergänzend zeigt der Netzwerkkonnektivitätstest für Microsoft 365 im Browser, über welchen Ausgang ein Standort ins Microsoft-Netz geht und ob ein Proxy im Weg steht.

```
# Gegenprobe: TCP 443 zum Teams-Dienst ist erreichbar (das ist nicht das Problem)
Test-NetConnection -ComputerName teams.microsoft.com -Port 443

# Welcher Proxy ist auf dem Client systemweit gesetzt?
netsh winhttp show proxy
```

Mit dem Ergebnis gehst du zum Netzwerkteam. Die Frage lautet nicht „Habt ihr was an der Firewall geändert?“, denn darauf lautet die Antwort immer „Nein“. Die Frage lautet: „Welche Regel verwirft UDP von 10.40.0.0/16, Quellport 50000 bis 50059, zu 52.112.0.0/14 und 52.122.0.0/15, Zielport 3478 bis 3481?“ Auf so eine Frage gibt es eine Logzeile als Antwort, keine Meinung.

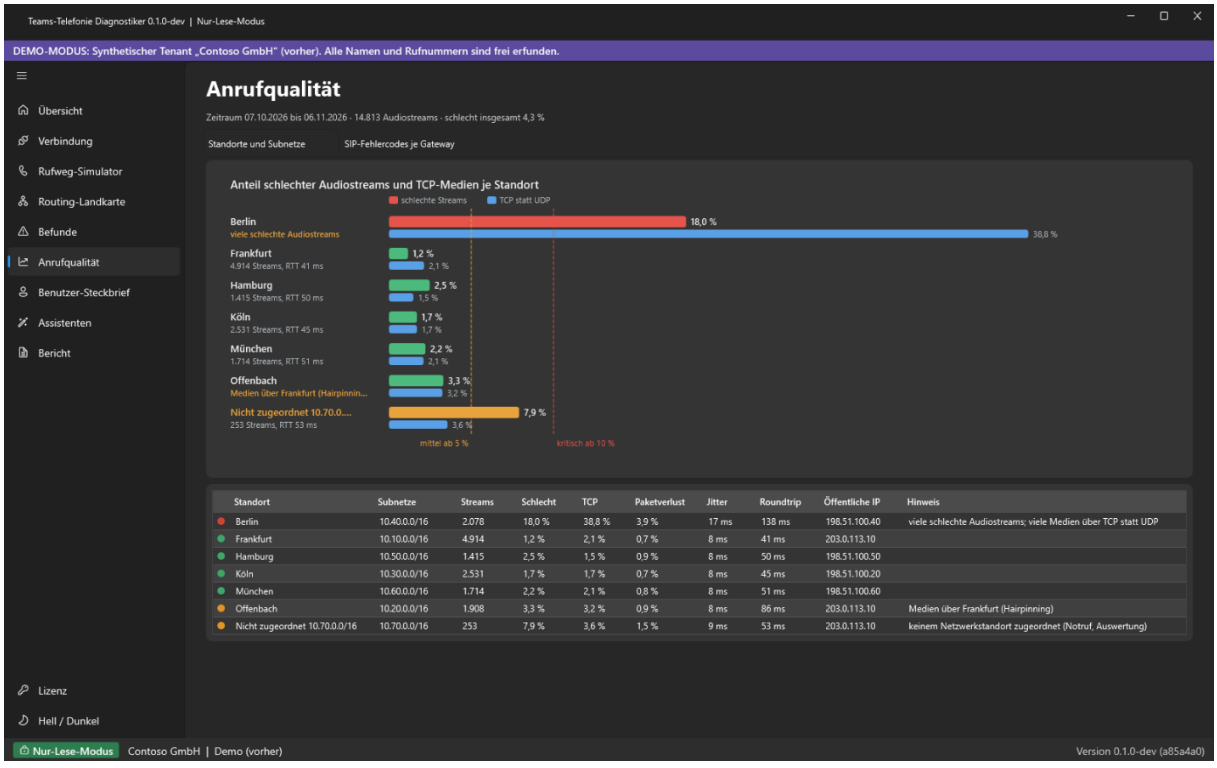
Wo UDP typischerweise stirbt	Woran du es erkennst	Wer es ändern kann
Standort-Router oder	Ein Standort betroffen, CQD zeigt TCP	Netzwerkteam, Standort-IT

Branch-Firewall mit „nur Web“-Regel	für dessen Subnetz	
Zentrale Firewall ohne UDP-Regel für die Teams-Netze	Alle Standorte hinter diesem Ausgang betroffen	Firewall-Team
Erzwungener Proxy, auch für Optimize-Endpunkte	Connectivity Ice HTTP, Proxy-Protokolle voller Teams-Verbindungen	Proxy-Team, PAC-Datei oder Proxy-Richtlinie
VPN-Tunnel ohne Split Tunneling	Nur mit VPN schlecht, Transport TCP	VPN-Team
Gast-WLAN oder Raumnetz	Teams Rooms und Gäste betroffen	WLAN-Team
Veraltetes Adressobjekt	Nur einige Relay-Netze betroffen, oft nach Firewall-Update	Firewall-Team, Abgleich mit der Microsoft-Liste

WERKZEUG · So findet es der Teams-Telefonie Diagnostiker

Der Teams-Telefonie Diagnostiker wertet in der Ansicht Anrufqualität die Audiostreams des gewählten Zeitraums je Standort und Subnetz aus. Ein Balkendiagramm stellt für jeden Standort den Anteil schlechter Audiostreams und den Anteil der Medien über TCP statt UDP nebeneinander, mit Schwellen für mittlere und kritische Werte. Die Tabelle darunter zeigt Subnetze, Streams, Paketverlust, Jitter, Roundtrip und die öffentliche Adresse je Standort. Ein Standort, an dem beide Balken gleichzeitig hoch sind, ist der typische Fall aus diesem Beitrag. Auffällige Standorte erscheinen außerdem als Befund im Bereich Netz der Ampel.

Mehr dazu auf der Seite Teams-Telefonie Diagnostiker. Du kannst ihn 15 Tage kostenlos testen.

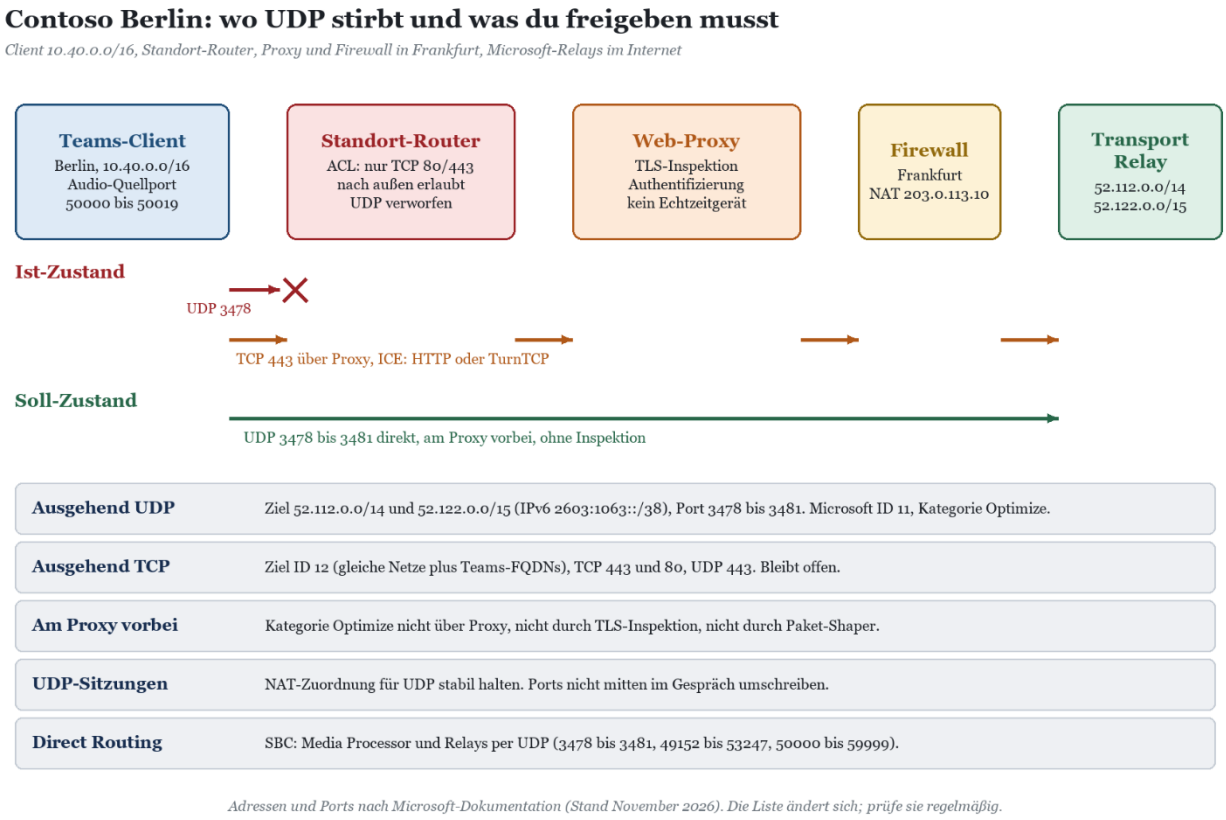


So siehst du in der Anrufqualität, dass Berlin mit 38,8 Prozent TCP-Medien und 18 Prozent schlechten Audiostreams aus der Reihe fällt (Demo-Daten)

Behebung: UDP freigeben, Proxy umgehen

Die Behebung findet im Netz statt, nicht in Teams. In Teams gibt es keinen Schalter „bitte UDP benutzen“, denn Teams will ja UDP. Es darf nur nicht. Deine Aufgabe ist, ihm den Weg

freizumachen, und zwar gezielt: nicht „UDP any any“, sondern genau die Netze und Ports aus der Microsoft-Liste.



Die Firewall-Regeln

Regel	Quelle	Ziel	Protokoll und Port	Hinweis
Teams-Medien	Client-Netze, z. B. 10.40.0.0/16	52.112.0.0/14, 52.122.0.0/15, 2603:1063::/38	UDP 3478 bis 3481	ID 11, Optimize. Am Proxy vorbei, ohne Inspektion
Teams-Dienst	Client-Netze	ID 12: Teams-FQDNs und Netze	TCP 443, 80, UDP 443	Bleibt als Rückfall und für Signalisierung nötig
Media Bypass	Client-Netze, Quellport 50000 bis 50019	Öffentliche Adresse des SBC, z. B. sbc1.contoso.com	UDP, Zielports laut SBC	Nur bei aktivem Media Bypass
SBC-Medien	SBC	52.112.0.0/14, 52.120.0.0/14	UDP 3478 bis 3481, 49152 bis 53247, 50000 bis 59999	Direct Routing, aktuelle Liste in der Microsoft-Dokumentation prüfen

Die Adressbereiche ändern sich gelegentlich. Microsoft veröffentlicht neue Adressen laut Dokumentation 30 Tage vor ihrer Nutzung und bietet die Liste auch als Webdienst an. Viele Firewalls können diese Liste automatisch übernehmen. Wenn deine das kann, nutze es. Handgepflegte Adressobjekte veralten zuverlässig.

Den Proxy aus dem Medienweg nehmen

Ist ein Proxy im Spiel, reicht die Firewall-Regel allein manchmal nicht. Die Endpunkte der Kategorie Optimize sollen direkt ins Internet gehen, ohne Proxy, ohne TLS-Inspektion und ohne Paket-Shaper. Je nach Umgebung heißt das: eine Ausnahme in der PAC-Datei, eine Bypass-Liste in der Proxy-Richtlinie oder eine Ausnahme im Agenten des Cloud-Proxys. Für die Teams-FQDNs aus ID 12 gilt mindestens: keine TLS-Inspektion.

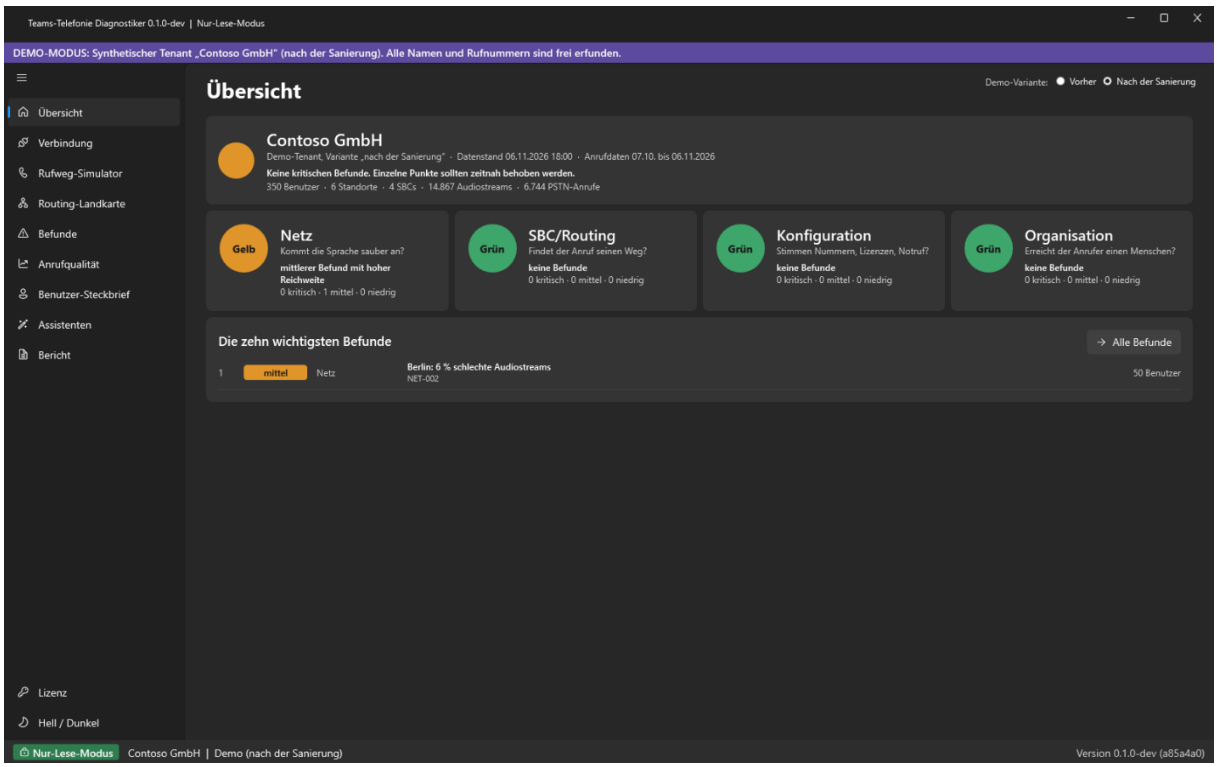
> **WARNUNG · Nicht aus Bequemlichkeit alles öffnen**
>
> „Mach halt UDP raus komplett auf“ ist die schnellste Lösung und die, über die im nächsten Audit jemand stolpert. Gib genau die Ziele und Ports frei, die Microsoft nennt, und dokumentiere die Regel mit Verweis auf die Endpunkt-ID. Dann versteht auch der Kollege in drei Jahren noch, warum sie existiert, und löscht sie nicht beim Aufräumen.

Reihenfolge und Rollback

1. **Ist-Zustand sichern.** Export der betroffenen Firewall- und Proxy-Regeln, Werte aus CQD für den Standort notieren: TCP-Anteil, Anteil schlechter Streams, Roundtrip.
2. **Regel für einen Standort einspielen.** Zuerst Berlin, nicht alle Standorte auf einmal. Regel mit Protokollierung, damit du Treffer siehst.
3. **Testanruf.** Ein Anruf aus Berlin zu einer externen Nummer und ein Teams-zu-Teams-Anruf. Im Anrufverlauf des Testbenutzers muss jetzt UDP stehen, und die Firewall muss Treffer auf der neuen Regel zeigen.
4. **Beobachten.** CQD braucht etwas Zeit, bis neue Daten auftauchen. Prüfe nach einigen Tagen erneut den TCP-Anteil und den Anteil schlechter Streams.
5. **Ausrollen.** Dann die übrigen Standorte und Netze mit derselben Regel versorgen.

Der Rollback ist simpel: die neue Regel deaktivieren, den alten Proxy-Eintrag zurückspielen. Teams fällt dann wieder auf TCP zurück. Das ist unschön, aber kein Ausfall, denn TCP 443 bleibt ja offen. Genau deshalb ist diese Änderung eine der risikoärmeren, die du für die Telefonie vornehmen kannst.

> **WICHTIG · Auch der Notruf läuft über diesen Weg**
>
> Ein Anruf an 110 oder 112 aus Teams nutzt denselben Medienweg wie jeder andere Anruf. Ein Notruf mit abgehackter Sprache, bei dem die Leitstelle die Adresse dreimal erfragen muss, ist das letzte, was du willst. Das ist ein gutes Argument, wenn das Firewall-Team die Änderung erst im nächsten Quartal einplanen möchte.
>
> Wie du den Notruf prüfst, ohne die Leitstelle zu verärgern, steht in Notruf in Teams testen, ohne die Leitstelle zu verärgern; die Grundlagen in Notruf in Microsoft Teams konfigurieren.



So sieht die Übersicht nach der Freigabe aus: Im Netz bleibt für Berlin nur noch ein mittlerer Befund mit 6 Prozent schlechten Audiostreams (Demo-Daten)

Dass Berlin nach der Freigabe nicht sofort auf null fällt, ist übrigens normal. Wenn UDP wieder durchkommt, siehst du endlich die echten Netzwerte des Standorts. Bleibt dann noch ein Rest an Paketverlust oder Jitter, ist das ein neues, ehrlicheres Problem: Bandbreite, WLAN oder QoS. Damit geht es weiter in Abgehackte Sprache in Teams: Jitter, Paketverlust und Roundtrip.

Vorbeugung: damit UDP offen bleibt

UDP wird selten bei der Einführung gesperrt. Es wird danach gesperrt: beim Router-Tausch, beim Firewall-Update, beim neuen Proxy-Dienst, beim Umbau des Gastnetzes. Vorbeugung heißt deshalb, diese Ereignisse mit der Telefonie zu verknüpfen.

Maßnahme	Was du konkret tust	Warum
TCP-Anteil als Kennzahl	Monatlich den Anteil TCP-Audiostreams je Standort aus CQD oder den Call Records ziehen	Ein Standort, der plötzlich auf 30 Prozent springt, hat eine neue Regel
Endpunktliste automatisieren	Firewall-Objekte aus dem Microsoft-Webdienst befüllen statt von Hand	Neue Adressen kommen mit Vorlauf, aber sie kommen
Teams in den Änderungsprozess	Jede Änderung an Router, Firewall, Proxy und VPN bekommt einen Testanruf mit Blick auf den Transport	Der Fehler macht keinen Lärm, also musst du hinsehen
Standardvorlage für Standorte	Neue Standorte bekommen die Teams-Regeln ab Werk	Die nächste Niederlassung soll nicht wieder Berlin werden
Split Tunneling für VPN	Optimize-Endpunkte am Tunnel vorbei	Microsoft empfiehlt es für Teams-Medien
Gebäudedaten pflegen	Subnetze in CQD und in der Teams-Netzwerktopologie aktuell halten	Sonst siehst du den Standort nicht, an dem es klemmt

Wie VPN und Split Tunneling für Teams aussehen sollten, beschreibt Teams-Telefonie über VPN: Split Tunneling richtig einrichten. Wer für Netz, Firewall und Telefonie verantwortlich ist und wer wen bei Änderungen informiert, gehört in ein Betriebskonzept; das Gerüst dafür steht in Microsoft Teams Telefonie-Governance. Dass sich Einstellungen unbemerkt verändern, behandelt Konfigurationsdrift in der Teams-Telefonie erkennen. Wenn du das Thema für viele Standorte strukturiert angehen willst, ist die Beratung zur Teams-Telefonie der passende Einstieg; wenn dein Team Medienwege und Anrufdaten selbst lesen lernen soll, die Schulung Teams-Telefonie.

WEITERLESEN · Passend dazu

› Sprachqualität in Teams: QoS, CQD und Troubleshooting
› Abgehackte Sprache in Teams: Jitter, Paketverlust und Roundtrip
› Teams-Telefonie über VPN: Split Tunneling richtig einrichten
› Netzwerkstandorte und Subnetze in Teams richtig pflegen
› Teams-Anrufprotokolle auswerten: Call Records statt Bauchgefühl
› Einseitiges Audio oder kein Ton bei Teams Direct Routing
› Teams-Anruf bricht nach einigen Minuten ab
› Hairpinning in Teams: wenn Anrufe Umwege über andere Standorte nehmen
› Teams Media Bypass und Local Media Optimization
› Teams-Telefonie Probleme: die zehn häufigsten Ursachen

FAQ

Funktioniert Teams-Telefonie ohne UDP überhaupt?

Ja. Teams fällt auf TCP 443 zurück, notfalls über den HTTP-Proxy. Microsoft bezeichnet TCP für Medien als unterstützt, rät aber wegen der Qualitätsfolgen davon ab. Es funktioniert also, es klingt nur schlechter, vor allem sobald das Netz Pakete verliert.

Welche Ports muss ich für Teams-Audio freigeben?

Ausgehend UDP 3478 bis 3481 zu 52.112.0.0/14 und 52.122.0.0/15, dazu IPv6 2603:1063::/38, laut Microsoft-Endpunktliste ID 11. Zusätzlich TCP 443 und 80 sowie UDP 443 für die Teams-Dienste aus ID 12. Prüfe die aktuelle Liste, sie ändert sich gelegentlich.

Woran erkenne ich in den Anrufdaten, dass TCP benutzt wurde?

Im Call Quality Dashboard an den Dimensionen Transport, First und Second Transport Protocol (zum Beispiel TurnTCP oder TCPHostActive) und Connectivity Ice mit dem Wert HTTP. In den Call Records über Microsoft Graph an der Eigenschaft networkTransportProtocol mit dem Wert tcp.

Ist ein kleiner TCP-Anteil normal?

Ja. Benutzer in Hotels, Zügen, Kundennetzen oder restriktiven Gast-WLANs landen oft auf TCP, und diese Netze kannst du nicht ändern. Auffällig wird es, wenn ein Firmenstandort oder ein ganzes Subnetz einen hohen TCP-Anteil hat.

Hilft QoS, wenn Teams über TCP läuft?

Nur begrenzt. Das eigentliche Problem, das Warten auf neu gesendete Pakete und der Proxy im Pfad, bleibt bestehen. Erst UDP freigeben, dann QoS.

Kann ich TCP für Teams-Medien einfach verbieten?

Eine Einstellung dafür gibt es im Teams Admin Center nicht, der Client wählt den Weg über ICE selbst. Du steuerst ihn, indem du den UDP-Weg freigibst, nicht indem du TCP sperrst. TCP 443 zu sperren würde Teams insgesamt lahmlegen.

Betrifft das auch Direct Routing und den SBC?

Den Client-Teil ja: Der Weg vom Client zum Media Processor oder Relay kann auf TCP ausweichen. Für die Medien zwischen SBC und Microsoft dokumentiert Microsoft nur UDP. Fehlt dort eine Freigabe, gibt es eher Stille oder einseitiges Audio als schlechte Qualität.

Warum klingt es im Homeoffice besser als im Büro?

Weil der Heimrouter UDP in der Regel nicht sperrt und kein Proxy im Weg steht. Wenn das Homeoffice besser klingt als die Zentrale, ist das ein starkes Indiz für eine restriktive Regel im Firmennetz, sofern das VPN Teams nicht durch den Tunnel schickt.

Wie schnell sehe ich nach der Freigabe eine Verbesserung?

Der nächste Anruf nutzt bereits UDP, das siehst du im Anrufverlauf des Testbenutzers. In den aggregierten Auswertungen wie CQD dauert es, bis genug neue Anrufe zusammengekommen sind. Vergleiche deshalb Zeiträume von mindestens einer Woche.

Fazit: Teams ist zu höflich, um sich zu beschweren

TCP statt UDP ist kein Ausfall, sondern ein Dauerzustand mit schlechter Laune. Teams findet immer einen Weg, auch durch den Proxy, und genau deshalb fällt niemandem auf, dass es der falsche ist. Die Diagnose ist dafür erfreulich klar: Transport und Connectivity Ice in den Anrufdaten, aufgeschlüsselt nach Standort, und der Fall ist eingegrenzt. Die Behebung ist eine präzise Firewall-Regel für UDP 3478 bis 3481 zu den Microsoft-Netzen und eine Ausnahme im Proxy.

Und dann gilt die alte Regel aller Netzwerker: Was gestern offen war, ist nach dem nächsten Firmware-Update nur noch eine Erinnerung. Schau monatlich auf den TCP-Anteil je Standort. Er ist die billigste Frühwarnung, die die Teams-Telefonie zu bieten hat.