TESSABYTE™

NETZWERKTEST

Hilfedokumentation

Inhalt

Einführung

Tessabyte ist eine Anwendung zum Testen der Leistung eines drahtlosen oder kabelgebundenen Netzwerks. Dieses Dienstprogramm sendet kontinuierlich TCP- und UDP-Datenströme über Ihr Netzwerk, berechnet wichtige Kennzahlen wie Upstream- und Downstream-Durchsatzwerte, Paketverlust, Jitter und Roundtrip-Zeit und zeigt die Ergebnisse sowohl im numerischen als auch im Diagrammformat an. Tessabyte unterstützt sowohl IPv4- als auch IPv6-Verbindungen und ermöglicht dem Benutzer die Bewertung der Netzwerkleistung abhängig von den Quality of Service-Einstellungen (QoS).

Zusätzlich zu dieser Kernfunktionalität kann die Anwendung Berichte im HTML- und Textformat generieren, vorab geplante Tests durchführen und die Anpassung der TCP- und UDP-Nutzlasten ermöglichen.

Tessabyte kann verwendet werden für:

- **Testen der Netzwerkkapazität:** Bewerten Sie die maximale Datenübertragungsrate, die eine Netzwerkverbindung unterstützen kann.
- **Verbindungsqualitätsanalyse:** Bestimmen Sie die Qualität einzelner Netzwerk-Links.
- **Netzwerküberlastung testen:** Simulieren Sie hohe Verkehrslasten und beobachten Sie, wie sich das Netzwerk bei Überlastung verhält.
- **WLAN-Leistungsbewertung:** Testen Sie drahtlose Netzwerke auf Geschwindigkeit und Zuverlässigkeit.
- **Bewertung der Servicequalität (QoS):** Bewerten Sie, wie verschiedene Verkehrstypen im Netzwerk priorisiert werden.
- **Validierung von Firmware- und Hardware-Updates:** Überprüfen Sie die Auswirkungen von Firmware- oder Hardware-Upgrades für Netzwerkgeräte.
- **Netzwerktopologieplanung:** Verstehen Sie, wie sich Netzwerkdesign-Entscheidungen auf die Leistung auswirken.
- **Beheben von Netzwerkproblemen:** Identifizieren Sie die Grundursachen für Leistungseinbußen.
- **Vergleichendes Benchmarking:** Vergleichen Sie die Leistung verschiedener Netzwerkkomponenten.
- **Sicherheitsbewertung:** Bewerten Sie die Auswirkungen von Sicherheitsmaßnahmen auf die Netzwerkleistung.
- **Lastausgleichsüberprüfung:** Testen Sie die Wirksamkeit des Lastausgleichs in einem Netzwerk.
- **SLA-Konformitätsprüfung:** Stellen Sie sicher, dass das Netzwerk seine Service Level Agreements einhält.
- **Hardware-Kompatibilitätstest:** Stellen Sie sicher, dass alle Netzwerkgeräte nahtlos zusammenarbeiten.

Systemanforderungen

Tessabyte kann auf Computern mit den folgenden minimalen Systemanforderungen ausgeführt werden:

- Betriebssysteme:
  Windows 10 und 11. **Windows Server** 2019, 2022 und 2025.
  macOS Monterey, Ventura, Sonoma, Sequoia und Tahoe.
  iOS/iPadOS 17.6 oder höher. Auf **iOS/iPadOS ist nur die Clientkomponente** verfügbar.
  Linux Ubuntu, Debian, Fedora und Red Hat laufen auf x86-64. Andere Linux-Distributionen werden möglicherweise unterstützt, wurden jedoch nicht getestet. Auf **Linux ist nur die Serverkomponente** verfügbar.

  Die Versionen **Windows, macOS, iOS/iPadOS** und **Linux** sind **interoperabel**; beispielsweise können Sie den Server auf macOS und den Client auf einer Windows-Maschine ausführen oder umgekehrt.
- 8 GB RAM.
- 100 MB freier Speicherplatz.

- Docker: Tessabyte Server ist auch als Docker-Container verfügbar, der auf jedem System ausgeführt werden kann, das Docker unterstützt. Das Image ist Multi-Arch und umfasst die Varianten Intel/AMD64 und ARM64. Sie können das neueste Image vom Docker Hub abrufen, indem Sie Folgendes verwenden:
  `docker pull netmantics/tessabyte-server:latest`
  Der Container wird unter https://hub.docker.com/r/netmantics/tessabyte-server gehostet.

Testversion

Tessabyte ist als voll funktionsfähige Testversion verfügbar, sodass Sie das Produkt vor dem Kauf einer Lizenz testen können. Die Testversion unterliegt den folgenden Einschränkungen für Windows und macOS:

- 30-tägiger Testzeitraum – Die Software läuft nach 30 Tagen Nutzung ab.
- Berichte – Einige Werte in Berichten werden zufällig durch "[Trial Ver.]" ersetzt.
- Planer – Es kann nur eine einzige geplante Aufgabe konfiguriert werden.

Die Testversion unterliegt den folgenden Einschränkungen für iOS/iPadOS:

- Tests sind auf 45 Sekunden begrenzt. Nach 45 Sekunden müssen Sie die Verbindung erneut herstellen.

- Berichte – Einige Werte in Berichten werden zufällig durch "[Trial Ver.]" ersetzt.

Um Tessabyte weiterhin ohne diese Einschränkungen nutzen zu können, müssen Sie eine Lizenz erwerben.

Installation und Konfiguration

Um einen Durchsatztest durchzuführen, verwendet die Anwendung zwei Komponenten: einen Server und einen Client. Die Serverkomponente der Anwendung wartet auf Verbindungen von Clients, während der Client eine Verbindung zum Server herstellt. Sobald eine Verbindung hergestellt ist, tauschen Client und Server Daten in beide Richtungen aus und die Clientkomponente berechnet und zeigt die Netzwerkmetriken an. Die Serverkomponente kann Verbindungen von mehreren Clients akzeptieren.

Installation

Wenn Sie die Anwendung installieren, werden sowohl die Server- als auch die Clientkomponente installiert. Anschließend können Sie je nach geplanter Testdurchführung eine der beiden Komponenten ausführen. In einer WLAN-Konfiguration sollte die Serverkomponente auf der kabelgebundenen Seite des Netzwerks und die Clientkomponente auf einem WLAN-Client ausgeführt werden. Bei dieser Konfiguration bezeichnet Downstream den Datenfluss von der kabelgebundenen Seite des Netzwerks über den Access Point zum Client, während Upstream den Datenfluss vom Client über den Access Point zur kabelgebundenen Seite bezeichnet. Bei kabelgebundenen LANs spielt es keine Rolle, welcher der beiden Computer als Server beziehungsweise Client fungiert.

Optionen des Windows-Installationsprogramms

Die Windows-Setup-Datei unterstützt mehrere Befehlszeilenoptionen, die für Systemadministratoren nützlich sein können:

- **/s** – Führt das Installationsprogramm im unbeaufsichtigten Modus ohne Benutzeroberfläche aus.
- **/noclient** – Installiert nur die Serverkomponente.
- **/noserver** – Installiert nur die Clientkomponente.
- **/noshortcuts** – Fügt keine Anwendungsverknüpfungen zum Desktop oder Startmenü hinzu.
- **/env** – Fügt den Anwendungspfad zur Umgebungsvariablen %PATH% hinzu.

Beispiel:

```
"C:\Downloads\tessabyte.exe" /s /noclient
```

Serverkonfiguration unter Windows und macOS

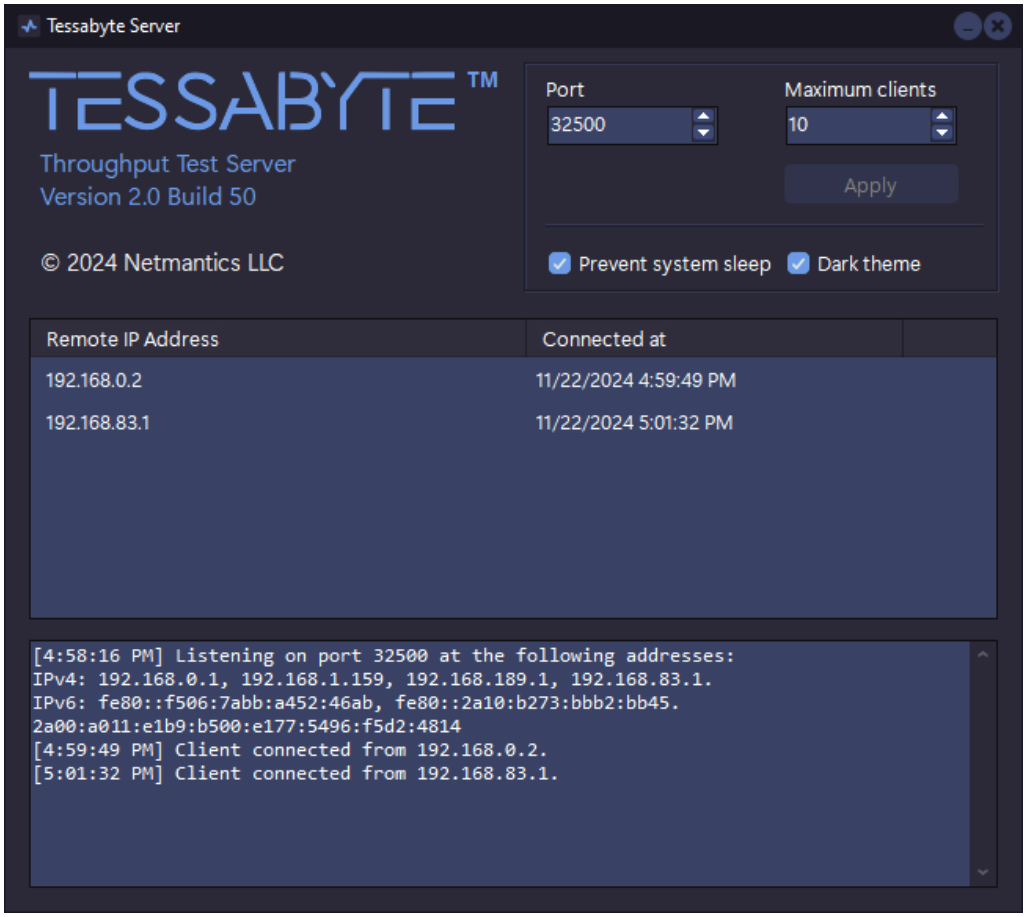
Die Serverkomponente der Anwendung (unten dargestellt) verfügt über zwei wichtige

konfigurierbare Optionen: den **Port**, an dem sie auf eingehende Verbindungen lauscht, und die **maximale Anzahl gleichzeitiger Clientverbindungen**. Standardmäßig lauscht der Server auf Port 32500.

Wenn Sie die Standardparameter ändern möchten, klicken Sie nach dem Ändern unbedingt auf die Schaltfläche **Apply**.

Sie können auch das Kontrollkästchen **Prevent system sleep** aktivieren, um zu verhindern, dass der Computer in den Ruhezustand wechselt, während die Anwendung ausgeführt wird. Verwenden Sie das Feld **Dark Theme**, um zwischen den dunklen und hellen Designs der Benutzeroberfläche zu wechseln (nur Windows; auf macOS verwendet die Anwendung den aktuell aktiven visuellen Stil).

Im mittleren Bereich werden die IP-Adressen und Verbindungszeiten der aktuell verbundenen Clients aufgeführt. Im unteren Bereich werden die IP-Adressen angezeigt, die die Anwendung auf eingehende Verbindungen überwacht (sie überwacht sowohl die Adressen IPv4 als auch IPv6). Im selben Bereich wird ein Protokoll der Client-Verbindungen und -Trennungen angezeigt, sobald diese auftreten.

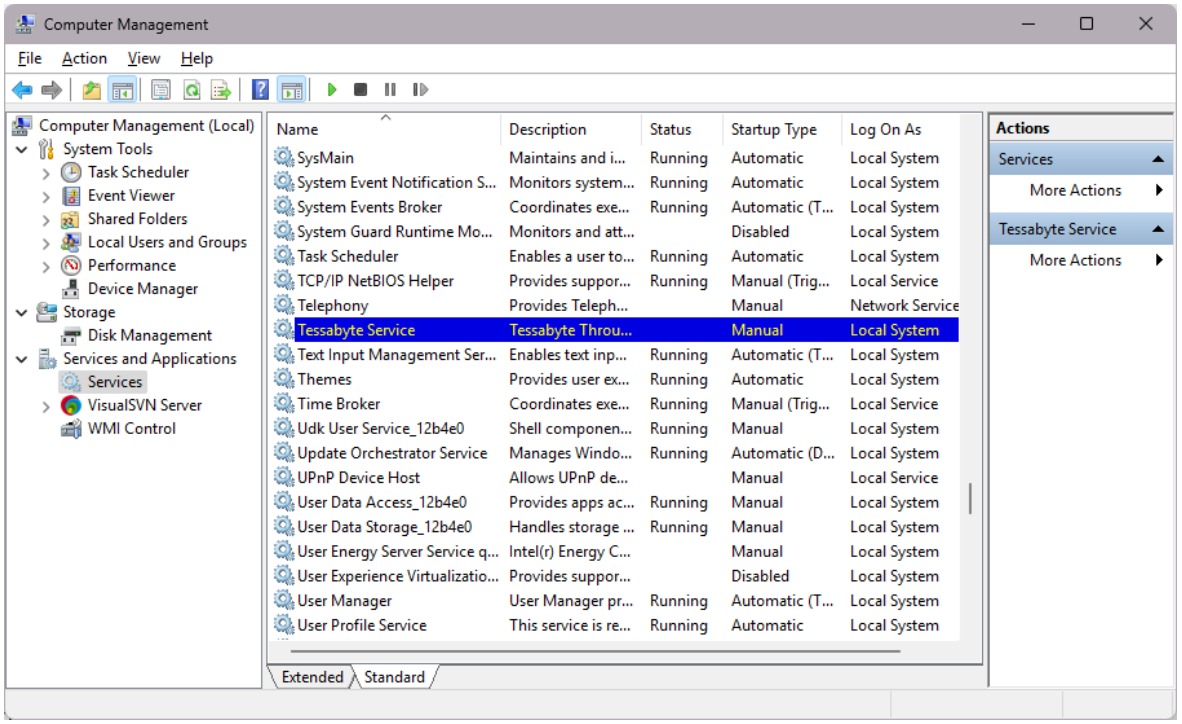


Server als Windows-Systemdienst ausführen

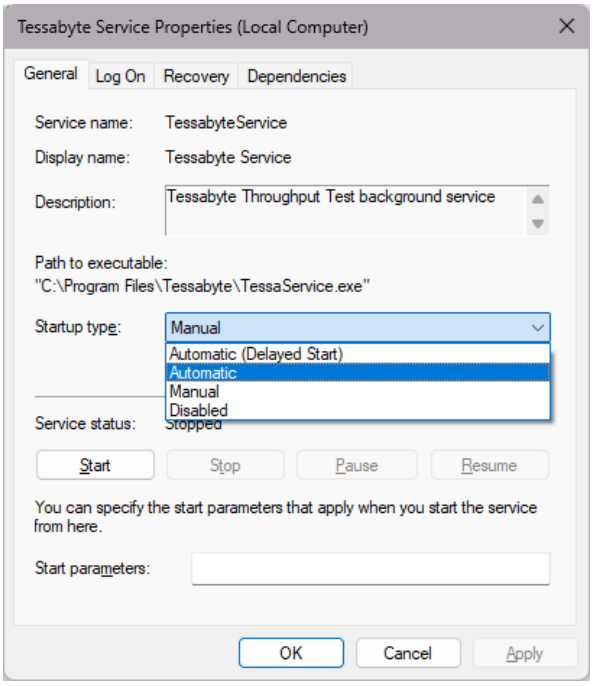
Die Serverkomponente ist sowohl als Standardanwendung mit Benutzeroberfläche, wie oben gezeigt,

als auch als nicht interaktiver Windows-Systemdienst verfügbar. Dieses Kapitel richtet sich an **fortgeschrittene Benutzer**, die mit dem Konzept der Systemdienste vertraut sind. Ist dies nicht der Fall, können Sie einfach die standardmäßige Tessabyte-Serveranwendung ausführen, wann immer Sie einen Test durchführen müssen.

Wenn Sie den Tessabyte-Server jedoch lieber in einem nicht interaktiven, unbeaufsichtigten Modus unter dem Systemkonto ausführen und ihn sofort nach dem Systemstart starten möchten, können Sie dies problemlos tun. Während der Installation erstellt Tessabyte einen neuen Systemdienst mit dem Namen **Tessabyte Service**. Der Dienst wird mit dem Starttyp **Manual** installiert, was bedeutet, dass er nicht automatisch startet, es sei denn, Sie konfigurieren ihn entsprechend. Wie alle anderen Windows-Dienste ist der **Tessabyte-Dienst** im Abschnitt **Dienste** des Bereichs **Computerverwaltung** in Windows zugänglich, wie unten dargestellt.



Sie können auf den Dienst doppelklicken, um den Starttyp in **Automatic** zu ändern, wenn Sie möchten, dass er nach dem Systemstart automatisch gestartet wird. Klicken Sie dann auf **Start**, um den Dienst sofort zu starten:



Ein paar zusätzliche Tipps zur Nutzung dieses Systemdienstes:

- Sie sollten die Standardanwendung von Tessabyte Server natürlich nicht ausführen, während der Dienst ausgeführt wird, da die Überwachungsports bereits vom Dienstprozess verwendet werden.
- Sie können die Standard-Portnummer (32500) und die maximale Anzahl von Clients (5) ändern, indem Sie den folgenden Registrierungsschlüssel ändern: HKEY_LOCAL_MACHINE\SOFTWARE\TessabyteService. Stoppen Sie den Dienst, bearbeiten Sie die Registrierungswerte und starten Sie ihn dann erneut.

Serverkonfiguration unter Linux

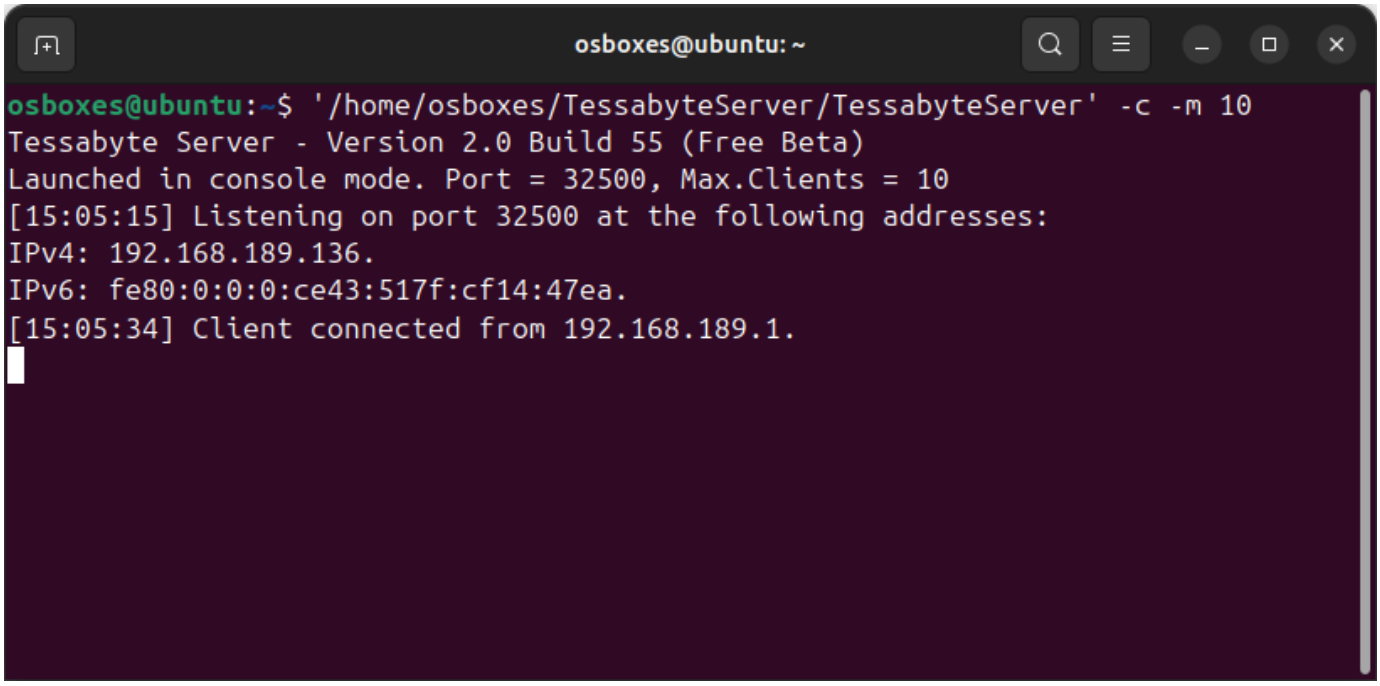
Die Linux-Version enthält nur die Serverkomponente. Der Server kann als Standardsystem-Daemon oder als Konsolendienstprogramm ausgeführt werden. Die folgenden Befehlszeilenargumente werden unterstützt:

- **-c** – Erzwingt die Ausführung der Anwendung im Konsolenmodus und nicht als Daemon.
- **-p** – Gibt den Überwachungsport an (zwischen 1024 und 65535). Wenn nicht angegeben, ist der Standardwert 32500.
- **-m** – Legt die maximale Anzahl gleichzeitiger Clientverbindungen fest (zwischen 1 und 100). Wenn nicht angegeben, ist der Standardwert 5.

Beispiel:

```
./TessabyteServer -c -p 41200 -m 20
```

Bei der Ausführung im Konsolenmodus druckt Tessabyte Protokolle im Terminalfenster:



Ohne das Argument **"-c"** läuft Tessabyte stillschweigend als Daemon. Wenn Sie möchten, dass es nach der Abmeldung des Benutzers weiter ausgeführt wird, ziehen Sie die folgenden zwei Optionen in Betracht.

Option A: Das Beenden von Prozessen durch systemd deaktivieren

Standardmäßig beendet **systemd** alle Prozesse, die als Teil einer Benutzersitzung gestartet wurden, wenn sich der Benutzer abmeldet – selbst wenn sie ordnungsgemäß vom Terminal getrennt wurden. Um dieses Verhalten zu ändern, führen Sie den folgenden Befehl aus:

```
loginctl enable-linger $USER
```

Wenn Sie diese Einstellung später rückgängig machen möchten:

```
loginctl disable-linger $USER
```

Option B: Systemweiter systemd-Dienst, der als Root ausgeführt wird

Schritt 1: Erstellen und bearbeiten Sie die Servicedatei:

```
sudo nano /etc/systemd/system/tessadaemon.service
```

Schritt 2: Fügen Sie der Servicedatei den folgenden Inhalt hinzu:

```
[Unit]
Description=TessaDaemon system-wide service
After=network.target

[Service]
ExecStart=/path/to/TessabyteServer
Restart=always
RestartSec=5
Type=forking
StandardOutput=journal
```

```
StandardError=journal

[Install]
WantedBy=multi-user.target
```

Schritt 3: Laden Sie **systemd** neu, aktivieren und starten Sie den Daemon:

```
sudo systemctl daemon-reload
sudo systemctl enable tessadaemon
sudo systemctl start tessadaemon
```

Serverkonfiguration mit Docker

Um Tessabyte Server in Docker mit der Standardkonfiguration auszuführen, verwenden Sie den folgenden Befehl:

```
docker run --name tessabyte-server \
  -p 32500:32500/tcp \
  -p 32500:32500/udp \
  netmantics/tessabyte-server:latest
```

Sie können auch dieselben Befehlszeilenargumente übergeben, die oben für Linux beschrieben wurden. Um beispielsweise den Server auf Port 41200 auszuführen und die Anzahl gleichzeitiger Clients auf 20 zu begrenzen, verwenden Sie:

```
docker run --name tessabyte-server \
  -p 41200:41200/tcp \
  -p 41200:41200/udp \
  netmantics/tessabyte-server:latest -p 41200 -m 20
```

Firewalls und NAT

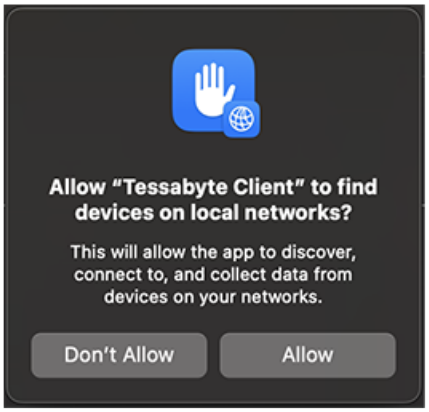
Auf Windows erstellt das Anwendungsinstallationsprogramm automatisch eine Windows-Firewallregel, die es ihm ermöglicht, Verbindungen zu akzeptieren. Wenn Sie eine Firewall eines Drittanbieters oder eine Firewall auf macOS oder Linux verwenden, stellen Sie sicher, dass diese so konfiguriert ist, dass eingehende Verbindungen für diese Anwendung zugelassen werden. Sowohl TCP- als auch UDP-Verbindungen müssen zulässig sein. Da die Anwendung zufällige Ports zum Streamen von Daten zurück zum Client verwendet, besteht die beste Strategie im Allgemeinen darin, die Firewall so zu konfigurieren, dass alle Verbindungen zum und vom Server unabhängig vom Port und Protokoll zugelassen werden.

Während Tessabyte in erster Linie zum Testen des LAN- und WLAN-Durchsatzes zwischen lokalen Knoten konzipiert ist, kann es auch zum Testen des WAN-Durchsatzes verwendet werden. Sie sollten jedoch bedenken, dass Probleme mit NAT auftreten können. Im Allgemeinen kann ein Computer, der sich hinter einem NAT befindet, ohne zusätzliche Konfigurations- oder Protokollunterstützung keine eingehenden TCP-Verbindungen und/oder UDP-Streams auf einem beliebigen, unaufgeforderten Port empfangen. Das bedeutet, dass der Server auf einem Computer mit einer öffentlichen IP-

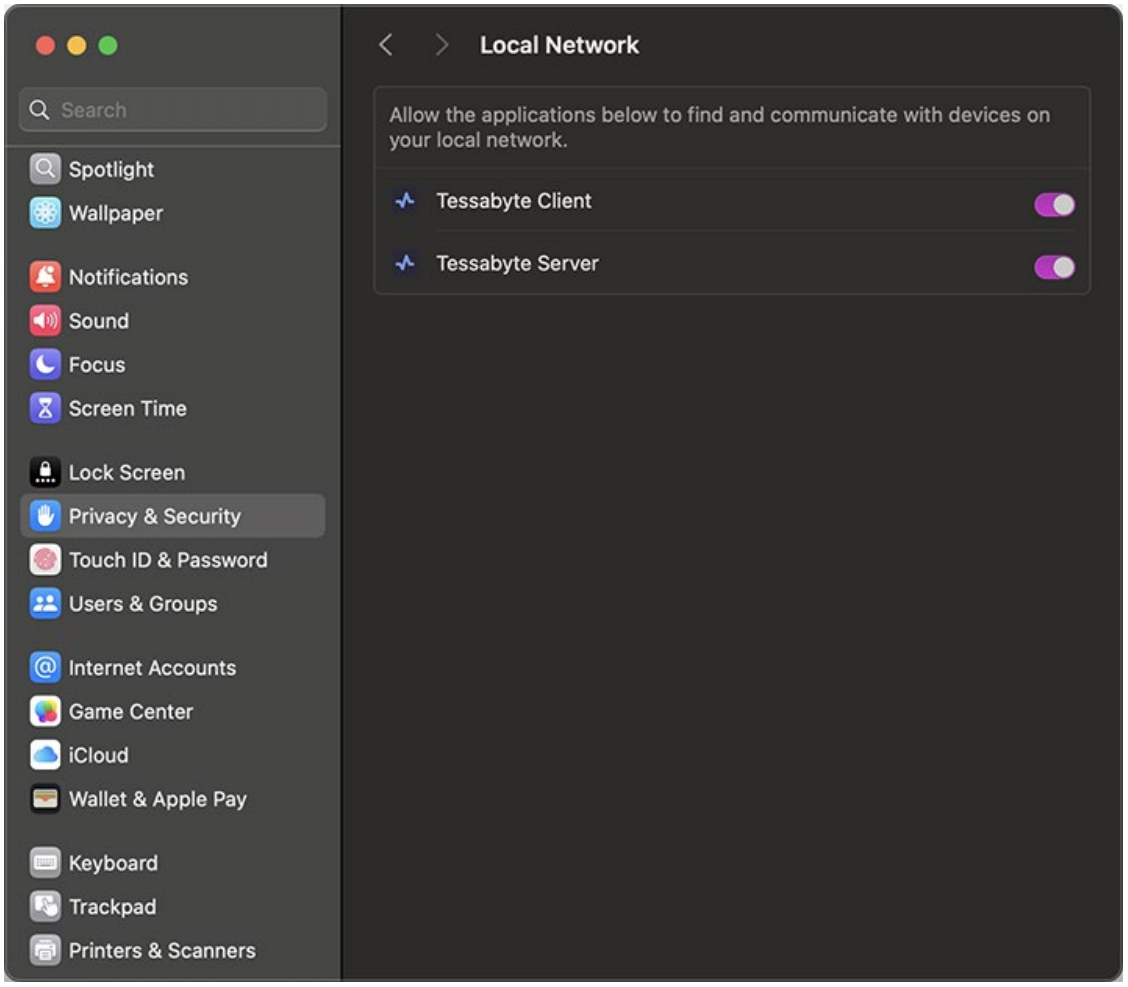
Adresse installiert werden muss und dass die Clients, wenn sie sich hinter einem NAT befinden, möglicherweise nur auf TCP-Tests beschränkt sind. Eine bevorzugte Lösung ist die Verwendung von IPv6, da NAT im Allgemeinen nicht erforderlich ist.

macOS-Systemberechtigungen

Wenn Sie die Anwendung installieren und zum ersten Mal auf macOS Sequoia verwenden, werden Sie vom Betriebssystem um eine Bestätigung gebeten, die für den Client bzw. den Server wie folgt aussieht:



Diese Dialogfelder werden normalerweise angezeigt, nachdem Sie in der Clientanwendung zum ersten Mal auf "Connect" geklickt haben und/oder wenn die Serveranwendung zum ersten Mal eine Clientverbindung akzeptiert. Sie **müssen** diese Berechtigung sowohl den Client- als auch den Serveranwendungen erteilen; andernfalls funktionieren sie nicht richtig. Möglicherweise müssen Sie die Anwendungen nach Erteilung der Genehmigung erneut starten. Um zu überprüfen, ob die Berechtigungen erteilt wurden, öffnen Sie macOS **Systemeinstellungen ➔ Datenschutz & Sicherheit ➔ Lokales Netzwerk**, wie unten gezeigt.


Search
Spotlight
Wallpaper
Notifications
Sound
Focus
Screen Time
Lock Screen
Privacy & Security
Touch ID & Password
Users & Groups
Internet Accounts
Game Center
iCloud
Wallet & Apple Pay
Keyboard
Trackpad
Printers & Scanners
Local Network
Allow the applications below to find and communicate with devices on your local network.
Tessabyte Client
Tessabyte Server

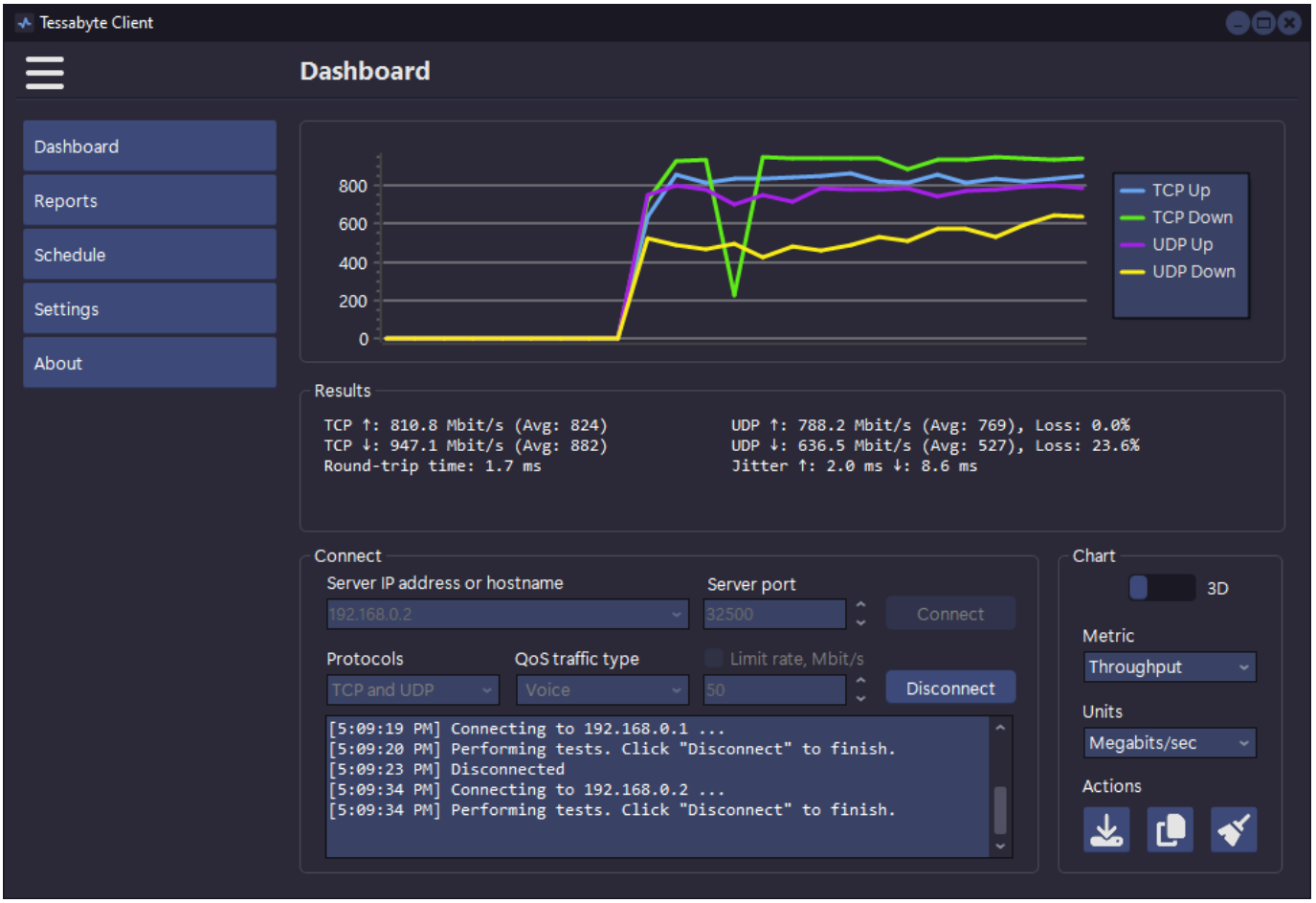
Tests im Dashboard durchführen

Um mit dem Durchsatztest zu beginnen, müssen Sie sowohl den Client als auch den Server auf verschiedenen Computern starten, wie im vorherigen Kapitel beschrieben. Geben Sie im Client-Fenster den Hostnamen, die IPv4-Adresse oder die IPv6-Adresse des Servers ein.

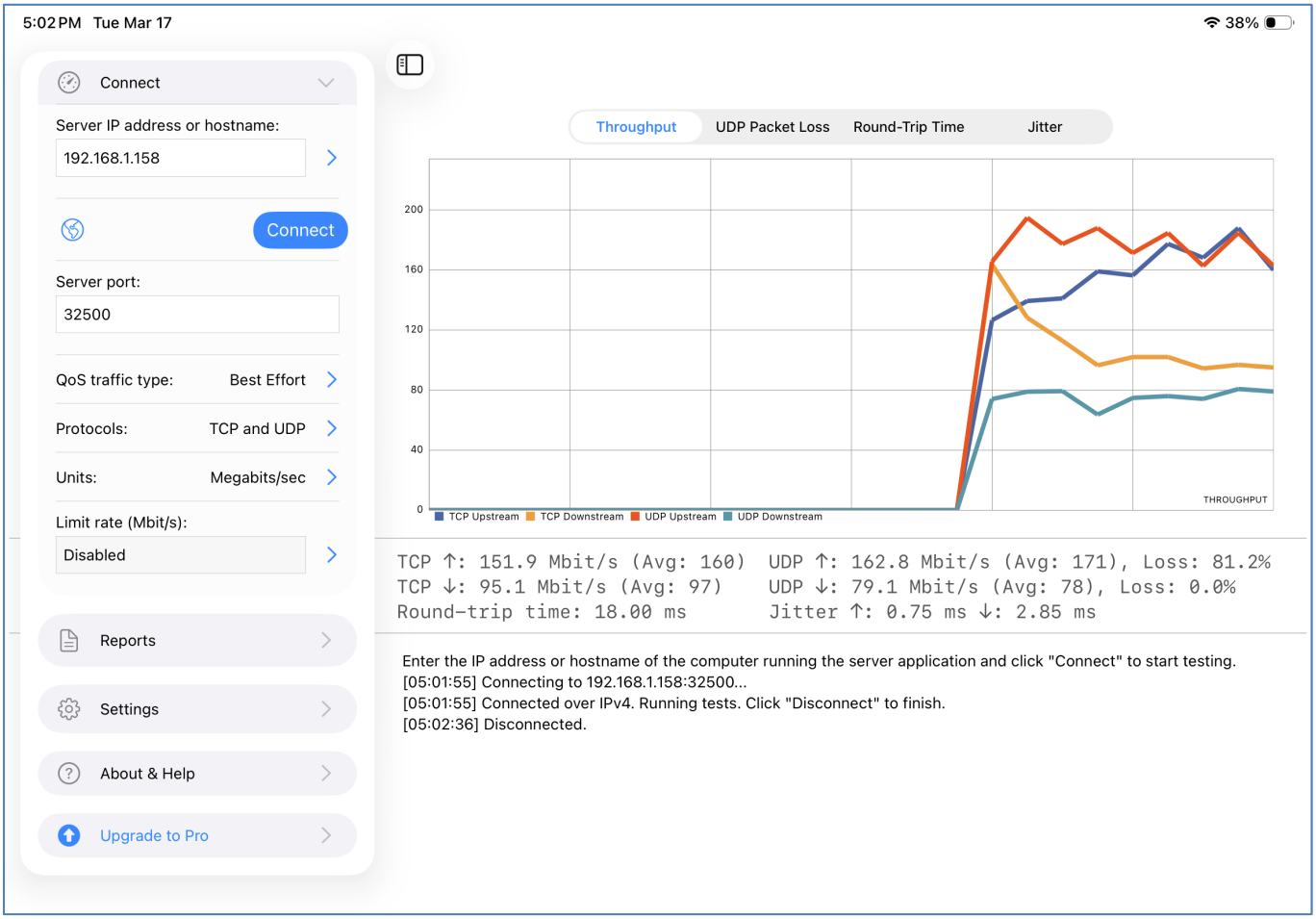
Hinweis: Auf macOS erfordern verbindungslokale IPv6-Adressen möglicherweise einen Zonenindex. Wenn der Fehler "No route to host" auftritt, müssen Sie möglicherweise einen Zonenindex in die Adresse einfügen. Verwenden Sie beispielsweise anstelle von fe80::6a5b:35ff:fed1:4633 (das keinen Zonenindex enthält) fe80::6a5b:35ff:fed1:4633%en0.

Wenn Sie außerdem die standardmäßige **Portnummer** auf der Serverseite geändert haben, stellen Sie sicher, dass Sie die Portnummer entsprechend anpassen.

Klicken Sie in der Client-Anwendung auf **Connect** und der Client versucht, eine Verbindung zum Server herzustellen. Wenn die Verbindung erfolgreich ist, beginnt der kontinuierliche Durchsatztest und wird fortgesetzt, bis Sie auf **Disconnect** klicken. Die Client-Benutzeroberfläche für Windows und macOS ist unten dargestellt:



Die Client-Benutzeroberfläche auf iOS/iPadOS ist ähnlich, bestimmte Elemente der Benutzeroberfläche sind jedoch anders platziert:



Das Client-Fenster zeigt die Upstream- und Downstream-Durchsatzwerte TCP und UDP (aktuell und durchschnittlich), den Verlustprozentsatz für UDP-Streams, die Umlaufzeit (RTT) und den Jitter an. Dieselben Daten werden durch ein dynamisch aktualisiertes Diagramm veranschaulicht.

Die Dropdown-Liste **Protocols** bietet drei Optionen zum Testen Ihrer Netzwerkverbindung: **TCP and UDP**, **TCP Only** und **UDP Only**, die Sie je nach Ihren Testanforderungen auswählen können. Sie können außerdem **QoS traffic type** und **Limit bitrate** konfigurieren, was weiter unten ausführlich erläutert wird.

Unter Windows und macOS enthält der Bereich **Chart** mehrere Bedienelemente, mit denen die Darstellung der Daten gesteuert wird. Der Schalter **3D** schaltet die **3D-Ansicht** ein oder aus. In der Dropdown-Liste **Metric** können Sie auswählen, welche Daten angezeigt werden sollen: **Throughput**, **UDP Packet Loss**, **RTT,** oder **Jitter** (alternativ können Sie mit der Tastenkombination **Ctrl + 1..4** zwischen den entsprechenden Diagrammen wechseln). Mit der Dropdown-Liste **Units** können Sie schließlich die Maßeinheit ändern: **gigabits per second**, **gigabytes per second, megabits per second**, **megabytes per second**, **kilobits per second** oder **kilobytes per second**. Unter iOS/iPadOS kann die Metrik über die Schaltflächen oberhalb des Diagramms ausgewählt werden.

Bitte beachten Sie einige wichtige Punkte:

- Im Zusammenhang mit Datenraten werden Dezimalpräfixe typischerweise mit ihrer Standard-SI-Interpretation verwendet. Mit anderen Worten: In dieser Anwendung entspricht ein Megabit 1000^2 Bits statt 1024^2 Bits.
- **Jitter** wird nach der allgemein anerkannten Methode gemessen, die in RFC 3550 beschrieben ist.
- Wenn Sie **TCP Only** als Testprotokoll auswählen, sind die UDP-basierten Metriken – **UDP Packet Loss** und **Jitter** – nicht verfügbar.

Die Schaltflächengruppe **Actions** (nur Windows und macOS) bietet schnelle Diagrammaktionen: Sie können das Diagrammbild **speichern**, es in die Zwischenablage kopieren oder das Diagramm löschen.

Das Statusprotokollfenster unten zeigt Meldungen über den Status der aktuellen Anwendung an.

Öffentliche Testserver

Durch Drücken von **F5** im Dashboard (Windows/macOS) oder durch Tippen auf das Globussymbol (iOS/iPadOS) wird ein Fenster geöffnet, in dem Sie einen öffentlichen Testserver auswählen können, mit dem Sie eine Verbindung herstellen möchten. Wir bieten mehrere öffentliche Testserver in verschiedenen Teilen der Welt an. Mit den öffentlichen Tessabyte-Servern können Sie **schnelle WAN-Tests** durchführen, ohne einen eigenen Server einzurichten. Diese Server werden nur zur Vereinfachung bereitgestellt und **sollten nicht für präzise Tests verwendet werden**. Ihre Einschränkungen sind unten aufgeführt:

- Der Durchsatz hängt von der Auslastung des öffentlichen Servers, der Latenz zwischen Client und Server und dem Paketverlust entlang der Route ab, daher können die Ergebnisse niedriger oder inkonsistent sein. Beachten Sie, dass der TCP-Durchsatz eine einzelne TCP-Sitzung darstellt und **nicht mit Bandbreitentests** verglichen werden sollte, die mehrere TCP-Streams und einen nahegelegenen Testserver verwenden.
- Wenn Sie **IPv4** hinter NAT verwenden, müssen Sie mit **100 % UDP-Downlink-Verlust** rechnen, es sei denn, der Client verfügt über eine öffentliche IPv4-Adresse. Verwenden Sie IPv6-Server, wenn Ihr Netzwerk IPv6 unterstützt.
- Verfügbarkeit und Leistung öffentlicher Server können nicht garantiert werden. Wir stellen sie auf "as is"-Basis zur Verfügung, ohne jegliche Garantien oder Support.
- Nach 15 Testzyklen trennt der Tessabyte-Client die Verbindung zum öffentlichen Server. Bei Bedarf können Sie die Verbindung wiederherstellen.
- Für genaue Tests **führen Sie Ihren eigenen lokalen Server aus**.

QoS-Tests

Fortgeschrittene Benutzer möchten möglicherweise das Steuerelement **QoS traffic type** verwenden, um den **QoS-Verkehrstyp** anzugeben, der mit den von der Anwendung gesendeten und empfangenen Datenströmen TCP und UDP verknüpft ist. Eine Beschreibung von QoS und verwandten Standards und Technologien wie WMM, 802.11e, DSCP und 802.11p würde den Rahmen dieses Handbuchs sprengen. Kurz gesagt gibt es jedoch zwei Gründe, warum Sie diese Funktionalität nutzen möchten:

- Um zu überprüfen, wie sich verschiedene QoS-Verkehrstypen auf den Durchsatz auswirken. In einem ordnungsgemäß konzipierten WLAN mit APs der Enterprise-Klasse sollten die Durchsatzwerte für Datenverkehr mit hoher Priorität die für Datenverkehr mit normaler Priorität überschreiten.
- Zur Überprüfung des durchgängigen QoS-Netzwerkdesigns. In einem ordnungsgemäß konzipierten LAN oder WLAN muss der mit QoS markierte Datenverkehr das gesamte Netzwerk von der Quelle zum Ziel sowohl über drahtlose als auch über kabelgebundene Segmente durchlaufen, die möglicherweise unterschiedliche Technologien und Protokollimplementierungen verwenden. Wenn Sie dieses Szenario testen, sollten Sie Tessabyte zum Generieren von mit QoS gekennzeichnetem Datenverkehr verwenden und dann Paketerfassungs- und Analysetools verwenden, um die Pakete zu überprüfen und die QoS- oder DSCP-Werte in den erfassten Paketen zu überprüfen.

Die folgende Tabelle fasst verschiedene QoS-Verkehrstypen zusammen, die Sie verwenden können. Bitte beachten Sie, dass nicht alle in der Anwendung verfügbaren und unten beschriebenen QoS-Typen über entsprechende WMM-Zugriffskategorien verfügen. In der Praxis bedeutet dies, dass, wenn Sie Tessabyte auf einem WLAN-Client ausführen und einen QoS-Typ ohne WMM-Zuordnung auswählen, Ihr Wi-Fi-Adaptertreiber möglicherweise überhaupt nicht mit QoS-Tag-Paketen kompatibel ist.

QoS-Typ	Beschreibung	DSCP-Markierung (Windows)	DSCP-Markierung (macOS, iOS/iPadOS und Linux)
Best Effort	Flussverkehr hat die gleiche Netzwerkpriorität wie regulärer Verkehr, der nicht mit QoS verknüpft ist. Dieser Verkehrstyp ist dasselbe wie das Nichtangeben der Priorität und daher wird die Markierung DSCP nicht zum gesendeten Verkehr hinzugefügt. Entspricht der Zugriffskategorie WMM AC-BE.	0	0

Background	Flow-Traffic hat eine niedrigere Netzwerkpriorität als **Best Effort**. Dieser Datenverkehrstyp könnte für den Datenverkehr einer Anwendung verwendet werden, die eine Datensicherung durchführt. Entspricht der Zugriffskategorie WMM AC-BK.	8	8
Excellent Effort	Flow-Traffic hat eine Netzwerkpriorität, die höher als **Best Effort**, aber niedriger als **AudioVideo** ist. Dieser Verkehrstyp sollte für Datenverkehr verwendet werden, der wichtiger ist als normale Endbenutzerszenarien, wie z. B. E-Mail. Dieser Typ entspricht keiner WMM-Zugriffskategorie.	40	24
AudioVideo	Flussverkehr hat eine höhere Netzwerkpriorität als **Excellent Effort**, jedoch eine niedrigere als **Voice**. Dieser Verkehrstyp sollte für A/V-Streaming-Szenarien wie MPEG2-Streaming verwendet werden. Entspricht der Zugriffskategorie WMM AC-VI.	40	32
Voice	Der Flussverkehr hat eine höhere Netzwerkpriorität als **AudioVideo**, jedoch eine niedrigere als **Control**. Dieser Verkehrstyp sollte für Echtzeit-Sprachstreams wie VOIP verwendet werden. Entspricht der AC-VO-Zugriffskategorie WMM.	56	46
Control	Flussverkehr hat die höchste Netzwerkpriorität. Dieser Verkehrstyp sollte nur für die kritischsten Daten verwendet werden. Es kann beispielsweise für Daten verwendet werden, die Benutzereingaben übertragen. Dieser Typ entspricht keiner WMM-Zugriffskategorie.	56	48

User-defined	Zusätzlich zu den oben beschriebenen vordefinierten QoS-Typen können Sie eine beliebige DSCP-Markierung verwenden, die im Bereich **Settings** konfigurierbar ist. Dies erhöht die Flexibilität Ihrer Testszenarien, da die standardmäßigen QoS-Typen nicht alle möglichen DSCP-Werte abdecken und die Zuordnung des QoS-Typs DSCP je nach Betriebssystem unterschiedlich ist (siehe die Spalten rechts).⇔ Windows-Benutzer: Um das Element User-defined aus der Dropdown-Liste **QoS traffic type** auszuwählen, müssen Sie Tessabyte Client mit **Administratorrechten** starten. Wenn Ihr Tessabyte Server auch auf Windows läuft und nicht als Systemdienst läuft (wie in diesem Handbuch beschrieben), müssen Sie Tessabyte Server ebenfalls mit Administratorrechten starten.	Beliebiger Wert (1..63)	Beliebiger Wert (1..63)

Bitrate begrenzen

Fortgeschrittene Benutzer möchten möglicherweise das Kontrollkästchen **Limit rate** aktivieren und dann die maximale Bitrate angeben, die zum Testen verwendet werden soll (auch als "target bitrate" bezeichnet). Standardmäßig misst Tessabyte den maximal erreichbaren Netzwerkdurchsatz, es gibt jedoch bestimmte Testszenarien, in denen Sie die Bandbreite möglicherweise nicht vollständig auslasten möchten. Beispielsweise verwendet Ihr Netzwerkanbieter möglicherweise eine Committed Information Rate (CIR). Unter einem CIR wird einem Benutzer eine bestimmte Menge an Bandbreite basierend auf einem Service-Level-Agreement (SLA) garantiert, sodass der Benutzer möglicherweise nur beispielsweise 100 Mbit/s in einem 1000-Mbit/s-Netzwerk testen muss. Ein anderes Szenario besteht darin, dass Sie vermeiden möchten, dass die Netzwerkkonnektivität für andere Benutzer, die dieselbe Netzwerkverbindung nutzen, langsamer wird.

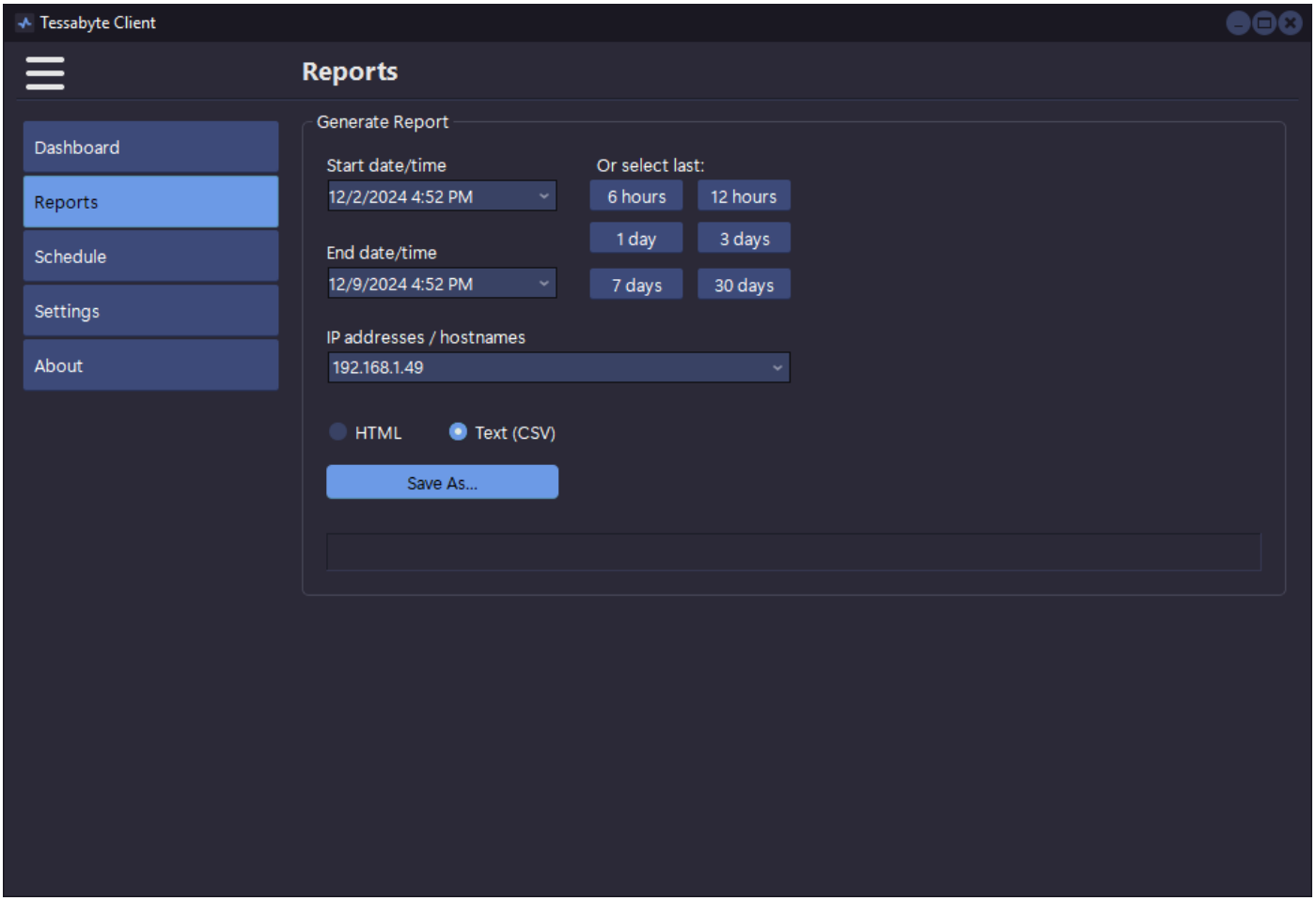
Um die Bitrate zu begrenzen, aktivieren Sie das Kontrollkästchen **Limit rate** und geben Sie die Bitrate an, die Tessabyte erreichen soll, in Megabit pro Sekunde. Wenn Sie beispielsweise "5000" angeben, beträgt die Zielbitrate 5 Gbit/s. Es ist wichtig zu beachten, dass Tessabyte versucht, die Durchsatzrate möglichst nah am angegebenen Grenzwert zu halten. Insbesondere bei UDP kann die vorgegebene Rate jedoch nicht mit hundertprozentiger Genauigkeit erreicht werden. Daher sollten Sie mit gewissen

Schwankungen rechnen, typischerweise innerhalb von 5–7 % der Zielbitrate.

Beachten Sie, dass Sie mit langen TCP-Testzyklen rechnen müssen, wenn Sie ein sehr niedriges Ratenlimit festlegen – z. B. 1 Mbit/s –, es sei denn, Sie geben eine benutzerdefinierte Datenblockgröße an. Beispielsweise dauert die Übertragung von 20 Megabyte Daten über eine auf 1 Mbit/s begrenzte Verbindung über eine Minute. Beachten Sie außerdem, dass das Festlegen eines Limits keine Auswirkungen hat, wenn Ihr Limit über der maximalen Netzwerkverbindungsgeschwindigkeit liegt (z. B. ein Limit von 20.000 Mbit/s (20 Gbit/s) für eine 1-Gbit/s-Verbindung).

Berichte erstellen

Tessabyte speichert die Ergebnisse aller durchgeführten Tests in einer kompakten Datenbank. Mit der Seite **Reports** können Sie einen Bericht erstellen, der alle Messungen für eine bestimmte IP-Adresse oder einen bestimmten Host oder für alle Hosts enthält, die während eines bestimmten Zeitraums getestet wurden.



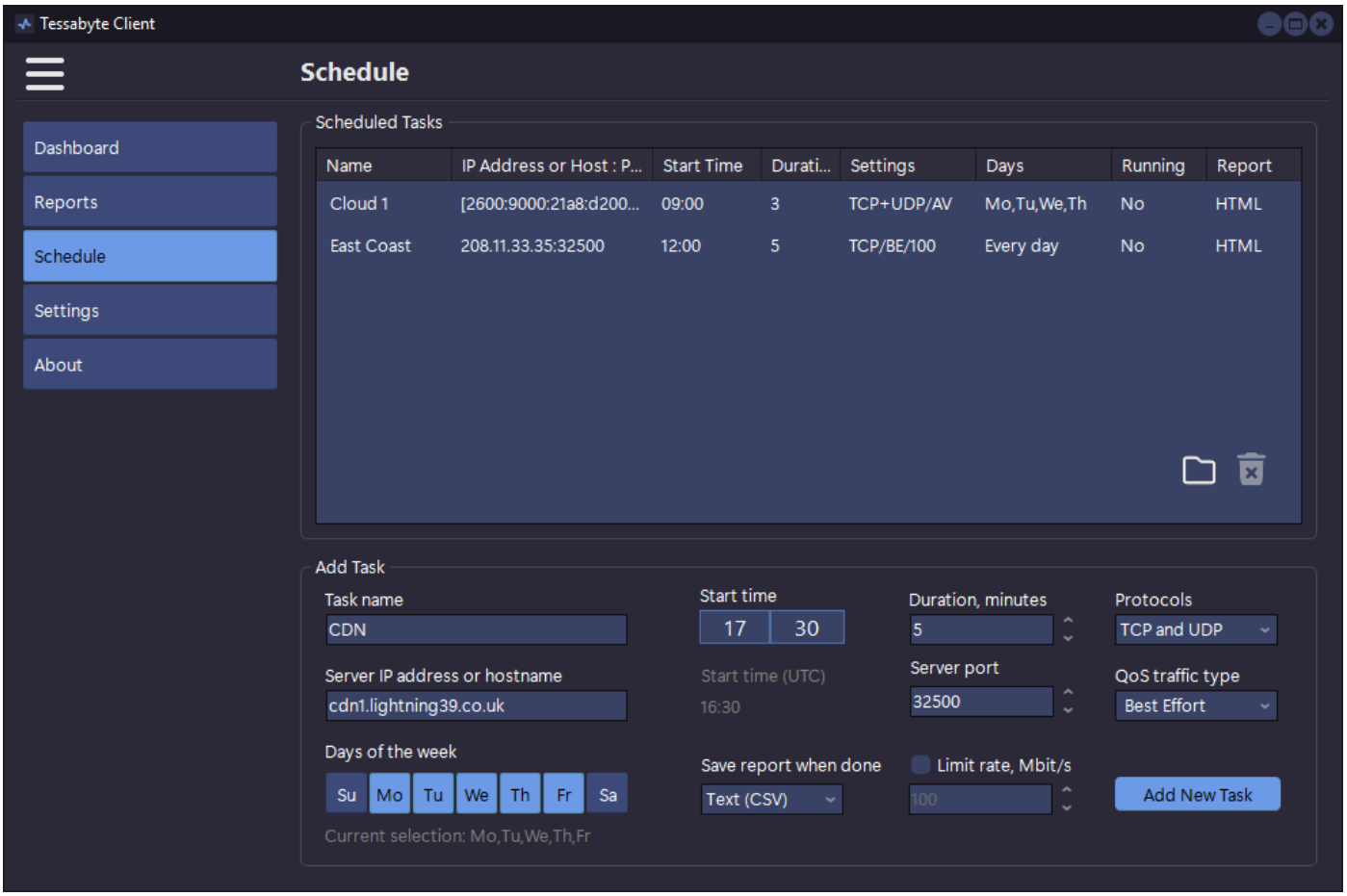
Um einen Bericht zu erstellen, wählen Sie zunächst **Start date/time** und **End date/time** aus oder verwenden Sie die Schnellauswahlschaltflächen auf der rechten Seite, um den Zeitbereich auf eine bestimmte Anzahl von Tagen oder Stunden festzulegen. Wählen Sie dann unter IP address or hostname die IP-Adresse oder den Hostnamen aus, für die bzw. den Sie einen Bericht erstellen möchten. Wählen Sie schließlich das Berichtsformat (**HTML** oder **CSV** bei Windows und macOS, **PDF** oder **CSV** bei iOS/iPadOS) und klicken Sie auf **Save As**, um es zu speichern.

Wenn eine bestimmte Messung in einer bestimmten Zeile nicht verfügbar ist (z. B. wenn Sie einen reinen TCP-Test ausführen, wird in den Spalten UDP und Jitter nichts angezeigt), verwenden wir "-1" in CSV-Dateien und "N/A" in HTML-Dateien.

Einige Berichtseinstellungen sind anpassbar. Weitere Informationen finden Sie im Kapitel **Einstellungen anpassen**.

Aufgaben planen (nur Windows und macOS)

Durchsatztests können als geplante Jobs ausgeführt werden, ohne dass sie manuell gestartet werden müssen. Die Seite **Schedule** bietet eine Schnittstelle zum Erstellen solcher automatischen Aufgaben.



Um eine neue Aufgabe zu erstellen, geben Sie einen eindeutigen Aufgabennamen, die IP-Adresse oder den Hostnamen des Servers ein, wählen Sie die Wochentage durch Umschalten der entsprechenden Schaltflächen aus, wählen Sie die Startzeit und -dauer (um Ihnen die Auswahl der richtigen Zeit zu erleichtern, wird unter dem Startzeitfeld ein Hinweis mit der entsprechenden UTC-Zeit angezeigt) und wählen Sie die zu verwendenden Protokolle sowie den QoS-Typ aus. Ändern Sie bei Bedarf die Standard-Portnummer und/oder begrenzen Sie die Bitrate. Nach Abschluss des Tests kann die Anwendung einen HTML- oder CSV-Bericht generieren und speichern. Wählen Sie also das bevorzugte Format und klicken Sie auf **Add New Task**. Die neue Aufgabe wird zur Aufgabenliste im oberen Teil der Seite hinzugefügt. Die Spalte **Running** zeigt den aktuellen Status an und ändert sich von No zu Yes, wenn eine Aufgabe ausgeführt wird.

Wenn die Ausführung einer Aufgabe geplant ist, während die Anwendung mit der Durchführung eines manuell initiierten Tests beschäftigt ist, wird der manuelle Test zugunsten der geplanten Aufgabe unterbrochen. Um eine Aufgabe zu löschen, wählen Sie sie aus der Liste aus und klicken Sie auf die

Schaltfläche **Papierkorb**. Um den Ordner zu öffnen, in dem Berichte gespeichert werden, klicken Sie auf die Schaltfläche **Ordner**. Berichte werden nach dem Aufgabennamen und der Endzeit benannt, zum Beispiel **"**CDN 26-Dec-2024 15-59-58.htm**"**. Wenn Sie außerdem mit der Maus über eine kürzlich abgeschlossene Aufgabe fahren, werden Sie in einem Tooltip-Fenster aufgefordert, auf die Aufgabe zu doppelklicken, um den neuesten Bericht zu öffnen.

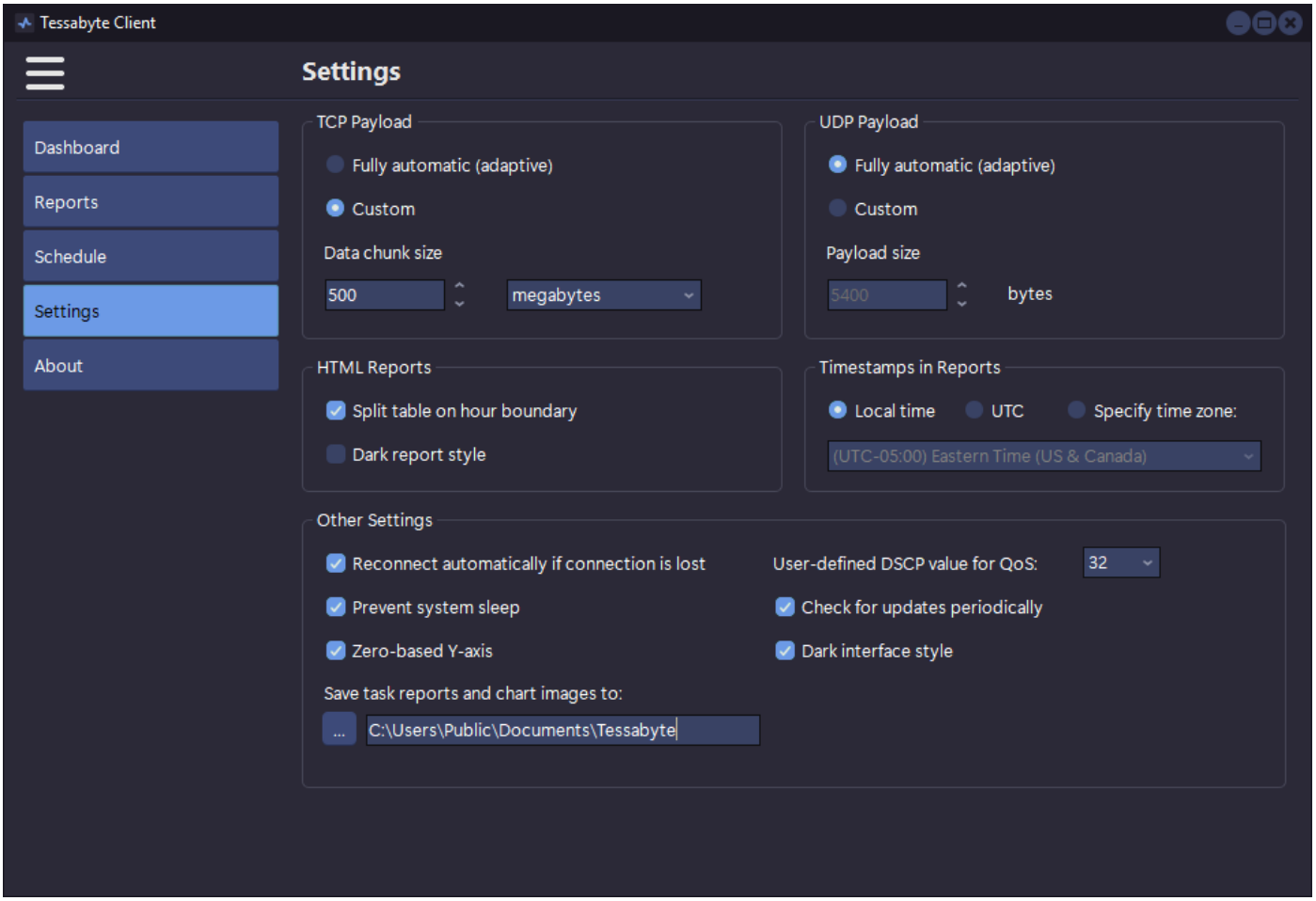
Ein paar weitere wichtige Dinge, die Sie bei der Arbeit mit geplanten Aufgaben beachten sollten:

- Beachten Sie, dass die Anwendung ausgeführt werden muss, wenn die Uhrzeit und der Tag der geplanten Aufgabe erreicht sind. Es gibt keinen Mechanismus zum automatischen Starten der Anwendung zur Durchführung der Tests.
- Die Anwendung verwendet den auf der Seite **Dashboard** konfigurierten Port, um eine Verbindung zum Server herzustellen.
- Vor Version 2.0 Build 58 verwendete Tessabyte die Protokolle (TCP und UDP, nur TCP, nur UDP) und QoS-Einstellungen, die auf der Seite **Dashboard** konfiguriert wurden, um eine Verbindung zum Server herzustellen. In Version 2.0 Build 58 haben wir die Option hinzugefügt, für jeden Test spezifische Einstellungen zu verwenden, die nichts mit den aktuellen Dashboard-Einstellungen zu tun haben. Für die zuvor erstellten Aufgaben wird in der Spalte **Settings** "Default" angezeigt und das alte Verhalten (unter Verwendung der **Dashboard-Einstellungen**) wird angewendet.

Einige Berichtseinstellungen sind anpassbar. Weitere Informationen finden Sie im Kapitel **Einstellungen anpassen**.

Einstellungen anpassen

Auf der Seite Settings sind einige konfigurierbare Optionen aufgeführt, mit denen Sie das Anwendungsverhalten anpassen können.



TCP-Nutzlast

Das Bedienfeld **TCP Payload** bestimmt, wie die Anwendung die Datengröße auswählt, die während jedes TCP-Testzyklus gesendet und empfangen werden soll (Chunk-Größe). Standardmäßig verwendet Tessabyte einen **automatischen, adaptiven** Mechanismus, um die Blockgröße anhand mehrerer Faktoren zu bestimmen, darunter Verbindungstyp (kabelgebunden oder drahtlos), Verbindungsbandbreite und Ergebnisse des vorherigen Testzyklus. Im Allgemeinen besteht das Ziel darin, eine Blockgröße auszuwählen, die innerhalb einer angemessenen Zeitspanne (typischerweise zwischen 0,5 und 1,0 Sekunden) gesendet und empfangen werden kann. Sie können jedoch eine **benutzerdefinierte** Datenblockgröße auswählen, die Ihren spezifischen Testanforderungen am besten entspricht. Beachten Sie, dass die Auswahl einer zu kleinen Blockgröße normalerweise zu ungenauen Ergebnissen mit einer volatilen Diagrammlinie führt, während die Auswahl einer zu großen Blockgröße zu einem langsamen Testzyklus führt, was zu langen Verzögerungen vor der nächsten Diagrammaktualisierung führt.

Stellen Sie sich beispielsweise eine 1-Gbit/s-Verbindung zwischen einem Client und einem Server vor. Eine solche Verbindung bietet unter idealen Bedingungen einen Durchsatz auf Anwendungsebene von etwa 110 Megabyte pro Sekunde. Wenn Sie die Blockgröße auf 1 Megabyte festlegen, wird der Block in nur 9 Millisekunden übertragen. Dies ist aufgrund mehrerer Faktoren, wie z. B. der Pufferung des Netzwerkstapels und der Aufgabenplanung des Betriebssystems, zu schnell, um den tatsächlichen Durchsatz genau zu messen. Wenn Sie die Blockgröße hingegen auf 2.000 Megabyte festlegen, erhalten Sie qualitativ hochwertige Messungen, aber jeder TCP-Testzyklus würde 18 Sekunden × 2 = 36 Sekunden dauern, da die Anwendung sowohl Uplink- als auch Downlink-Geschwindigkeiten messen muss.

UDP-Nutzlast

Das Bedienfeld UDP Payload bestimmt, wie die Anwendung die UDP-Datagrammgröße auswählt, die während jedes UDP-Testzyklus gesendet und empfangen werden soll. Standardmäßig verwendet Tessabyte einen **automatischen, adaptiven** Mechanismus, um die Datagrammgröße anhand mehrerer Faktoren zu bestimmen, darunter Verbindungstyp (kabelgebunden oder drahtlos), Verbindungsbandbreite und Ergebnisse des vorherigen Testzyklus. Das Ziel besteht darin, eine Datagrammgröße auszuwählen, die die maximal mögliche UDP-Datenübertragungsrate gewährleistet und gleichzeitig Paketverluste minimiert und Fragmentierung vermeidet. Normalerweise sollten Sie keine **benutzerdefinierte** UDP-Nutzlastgröße auswählen müssen, aber Sie können diese Option verwenden, wenn dies für Ihre spezifischen Testanforderungen erforderlich ist.

Beachten Sie, dass die maximale theoretische UDP-Datagrammgröße zwar 65.535 Byte beträgt (abzüglich der Größe der IP- und UDP-Header), Anwendungen in der Praxis jedoch selten Datagramme verwenden, die die MTU-Größe (ca. 1.500 Byte) überschreiten. Das Überschreiten der MTU-Größe kann zu einer UDP-Paketfragmentierung und einem Paketverlust führen. Mit anderen Worten: Während Sie eine benutzerdefinierte Größe von beispielsweise 4.000 oder sogar 64.000 Bytes verwenden können, sollten Sie keine zuverlässige Lieferung solcher UDP-Datenströme erwarten. Beachten Sie außerdem, dass auf macOS die maximal unterstützte UDP-Datagrammgröße standardmäßig 9.216 Byte beträgt.

HTML-Berichte (nur Windows und macOS)

Die Optionen im Bereich HTML Reports bestimmen zwei Parameter der von der Anwendung generierten HTML-Berichte. Die Option **Split table on hour boundary** paginiert Tabellen in HTML-Berichten und teilt sie nach Stunden auf. Die Option **Dark report style** schaltet das dunkle visuelle Thema der Berichte ein und aus.

Zeitstempel in Berichten (nur Windows und macOS)

Die Optionen in diesem Bereich bestimmen, welche Art von Zeitstempeln in vom Benutzer generierten

CSV- und HTML-Berichten enthalten sind. Sie können Tessabyte so konfigurieren, dass **Local Time** (die Uhr Ihres Computers), **UTC** (koordinierte Weltzeit) oder eine **spezifische Zeitzone** verwendet wird, indem Sie eine aus der Dropdown-Liste auswählen. Wenn sich Ihr Computer beispielsweise in der mitteleuropäischen Zeitzone befindet, können Ihre Berichte auf Wunsch mit einem Zeitstempel in der US-amerikanischen Bergzeitzone versehen werden. Bitte beachten Sie, dass die Zeitzonen in der Dropdown-Liste aus Konsistenzgründen ihren Standard-UTC-Offset (Winterzeit) angeben. Tessabyte wendet weiterhin den korrekten Offset an, wenn in der entsprechenden Zeitzone derzeit Sommerzeit aktiv ist.

Weitere Einstellungen

Reconnect automatically if connection is lost – Wenn diese Option aktiviert ist, versucht die Anwendung, sich bei jedem Verbindungsverlust erneut mit dem Server zu verbinden.

Die übrigen unten beschriebenen Einstellungen sind **nur in den Clients Windows und macOS** verfügbar:

Prevent system sleep – verhindert, dass der Computer in den Energiespar- oder Ruhezustand wechselt, während die Anwendung ausgeführt wird.
Check for updates periodically – Wenn diese Option aktiviert ist, stellt die Anwendung alle paar Tage eine Verbindung zu unserer Website her, um zu prüfen, ob eine neue Version verfügbar ist.
Dark interface style – wechselt zwischen den dunklen und hellen Benutzeroberflächenthemen (nur Windows; auf macOS verwendet die Anwendung den aktuell aktiven visuellen Stil).
Zero-based Y-axis – schaltet zwischen zwei Modi um: einem, bei dem das Y-Achsen-Minimum des Diagramms immer auf Null gesetzt ist, und einem anderen, bei dem das Y-Achsen-Minimum dynamisch ist und sich an die tatsächlichen Daten anpasst.
Save task reports and chart images to – ermöglicht Ihnen die Auswahl eines Ordners, in dem nach der Ausführung geplanter Aufgaben generierte Berichte automatisch gespeichert werden. Derselbe Ordner wird zum Speichern von Diagrammbildern verwendet, wenn auf der Dashboard-Seite auf die Schaltfläche "quick save" geklickt wird.
User-defined DSCP value for QoS – ermöglicht Ihnen die Auswahl einer beliebigen DSCP-Markierung, die verwendet wird, wenn die Option User-defined aus der Dropdown-Liste **QoS traffic type** ausgewählt wird. Die aufgelisteten DSCP-Werte sind dezimal (von 1 bis 63).

Befehlszeilenparameter von Tessabyte Client

Der Tessabyte-Client auf Windows und macOS kann über die Eingabeaufforderung gestartet werden, wenn Sie möchten, dass er unmittelbar nach dem Start eine Verbindung zu einem bestimmten Hostnamen oder einer bestimmten IP-Adresse herstellt. Darüber hinaus kann er im **Konsolenmodus** (keine grafische Benutzeroberfläche) gestartet werden, wodurch es für Skripterstellung und Ausgabeumleitung geeignet ist.

Standardmodus (Benutzeroberfläche) und Konsolenmodus

- **Auf Windows** werden Standard- (UI) und Konsolenmodi mit **verschiedenen** ausführbaren Dateien gestartet. **`TessabyteClient.exe`** wird zum Starten des Tessabyte-Clients im Standardmodus verwendet, während **`TessabyteConsole.exe`** zum Starten des Tessabyte-Clients im Konsolenmodus verwendet wird. Beide Dateien befinden sich normalerweise in **`C:\Program Files\Tessabyte`**.
- **Auf macOS** sollten Standard- (UI) und Konsolenmodi mit **der gleichen** ausführbaren Datei, **`TessabyteClient`**, gestartet werden. Da der Tessabyte-Client als .app-Bundle verpackt ist, müssen Sie beim Ausführen des Tessabyte-Clients von einem Terminal aus die eigentliche ausführbare Datei im Bundle aufrufen, nicht das Bundle selbst. Die Datei befindet sich normalerweise unter **`/Applications/Tessabyte Client.app/Contents/MacOS/TessabyteClient`**.

Befehlssyntax

Die folgenden Befehlszeilenargumente werden unterstützt:

- **-c** – Gibt die IP-Adresse oder den Hostnamen an, zu dem eine Verbindung hergestellt werden soll.

Dies ist das einzige obligatorische Argument. Die folgenden Argumente sind optional. Wenn sie nicht verwendet werden, wendet Tessabyte Client Standardwerte an:

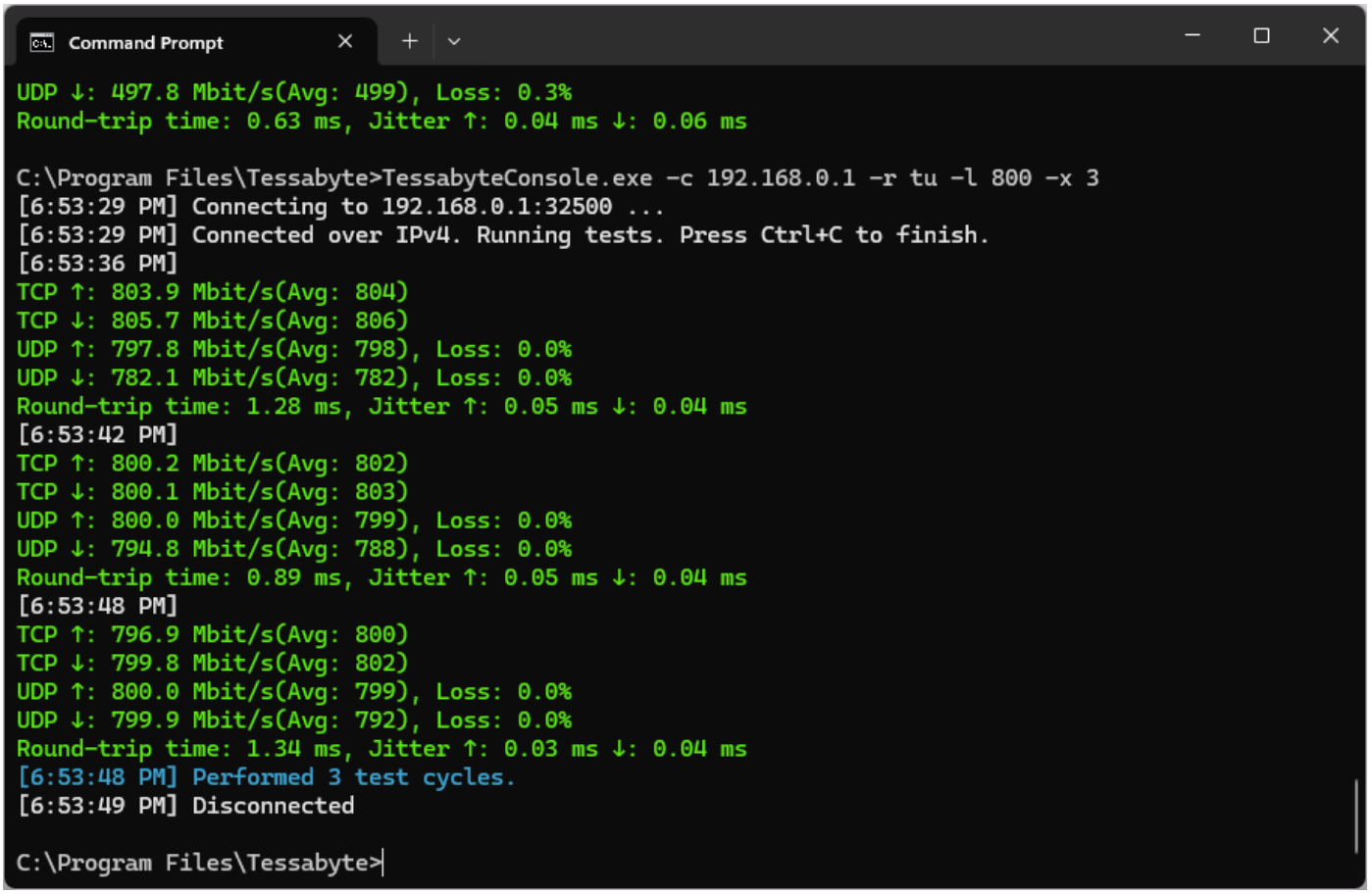
- **-p** – Gibt die Portnummer an, zu der eine Verbindung hergestellt werden soll. Wenn nicht angegeben, ist der Standardwert **32500**.
- **-r** – Gibt die zu testenden Protokolle an. Zulässige Werte sind "**tu**" (TCP und UDP), "**t**" (nur TCP) und "**u**" (nur UDP). Wenn der Parameter nicht angegeben wird, ist der Standardwert "**tu**".
- **-q** – Gibt den QoS-Verkehrstyp an. Akzeptable Werte liegen zwischen 0 (Best Effort) und 6 (User-defined). Diese Nummern entsprechen den Einträgen in der Liste QoS traffic type in der Benutzeroberfläche. Wenn nicht angegeben, ist der Standardwert **0**.
- **-l** – Gibt die Ratenbegrenzung in Mbit/s an. Zulässige Werte liegen zwischen **1** und **20000**. Wenn

nicht angegeben, wird keine Ratenbegrenzung angewendet.

- **-s** – Aktiviert den Stressmodus. Es ist kein zusätzlicher Wert erforderlich. Der Stressmodus kann in bestimmten Testszenarien nützlich sein, in denen Sie häufige TCP-Verbindungen und -Trennungen emulieren müssen. Wenn dieser Modus aktiviert ist, stellt der Tessabyte-Client eine Verbindung zum Server her, führt die Tests aus, trennt die Verbindung nach einer zufälligen Anzahl von Sekunden (zwischen 5 und 60) und stellt dann innerhalb von drei Sekunden wieder eine Verbindung her. Dieser Zyklus wird fortgesetzt, bis die Anwendung geschlossen wird.
- **-w** – Auf macOS wird der Tessabyte-Client im Konsolenmodus ausgeführt (keine grafische Benutzeroberfläche). **Auf Windows wird dieses Argument nicht unterstützt**; Der Konsolenmodus ist verfügbar, indem eine andere ausführbare Datei ausgeführt wird, wie am Anfang dieses Kapitels erläutert.
- **-x** – Gibt bei Ausführung im Konsolenmodus die Anzahl der durchzuführenden Testzyklen an. Zulässige Werte liegen zwischen **1** und **1000000.** Wenn nicht angegeben, ist der Standardwert 10. Nach Abschluss der angegebenen Anzahl von Zyklen wird die Anwendung beendet. **Im Standardmodus (UI) wird diese Option nicht unterstützt**.
- **-f** – Gibt bei der Ausführung im Konsolenmodus **auf Windows** eine Ausgabedatei an, in der die Testergebnisse gespeichert werden sollen. **Verwenden Sie für diesen Zweck nicht die standardmäßige Windows-Konsolenumleitung** (>), da verschiedene Shells möglicherweise inkonsistente Textkodierungen anwenden. Die mit -f erstellte Datei wird explizit in der UTF-8-Kodierung geschrieben. **Im Standardmodus (UI) wird diese Option nicht unterstützt**. **Auf macOS wird diese Option nicht unterstützt**; Verwenden Sie stattdessen die Standard-Shell-Umleitung (>).

Beispiele

Das Bild unten zeigt, wie Sie Tessabyte im Konsolenmodus ausführen können:



Windows-Eingabeaufforderung

```
"C:\Program Files\Tessabyte\TessabyteClient.exe" -c 192.168.12.9 -p 32500 -r u -q 1 -l 500 -s

"C:\Program Files\Tessabyte\TessabyteConsole.exe" -c node5.cloud.com -x 25

"C:\Program Files\Tessabyte\TessabyteConsole.exe" -c 192.168.0.4 -x 25 -f "C:\Logs\test1.txt"
```

Windows PowerShell

```
& "C:\Program Files\Tessabyte\TessabyteConsole.exe" -c 192.168.55.4

& "C:\Program Files\Tessabyte\TessabyteConsole.exe" -c 192.168.55.4 -f "C:\Logs\test1.txt"
```

macOS Terminal

```
"/Applications/Tessabyte Client.app/Contents/MacOS/TessabyteClient" -c 192.168.12.9 -q 3

"/Applications/Tessabyte Client.app/Contents/MacOS/TessabyteClient" -c 192.168.12.9 -w >
/Users/Dan/Desktop/test1.txt
```

Testergebnisse verstehen

Während jedes Testzyklus führt die Anwendung mehrere Tests durch: Senden und Empfangen von TCP-Daten, Senden und Empfangen von UDP-Daten und Senden und Empfangen eines Zeitsondenpakets. Basierend auf diesen Tests werden die Upstream- und Downstream-Durchsatzwerte TCP und UDP (aktuell für den letzten Test und gemittelt für alle Tests) sowie die Umlaufzeit berechnet.

Wenn alle Aufgaben in einem Zyklus abgeschlossen sind, beginnt automatisch ein neuer Zyklus. Wenn die Auswahl unter Protocols auf der Seite Dashboard auf TCP Only oder UDP Only gesetzt ist, wird der UDP- beziehungsweise TCP-Teil übersprungen. Wenn der UDP-Teil übersprungen wird, sind natürlich alle UDP-basierten Metriken – UDP-Durchsatz, UDP-Paketverlust und Jitter – nicht verfügbar.

Durchsatz

Der Durchsatz (oft auch als "goodput" bezeichnet) ist die Menge an Daten auf Anwendungsebene, die pro Sekunde vom Client an den Server (Upstream) oder vom Server an den Client (Downstream) übermittelt werden. Der Protokoll-Overhead ist nicht enthalten. Wenn wir uns beispielsweise auf eine TCP-Durchsatzrate von 1 Mbit/s beziehen, bedeutet dies, dass 125 Kbyte tatsächlicher Datennutzlast innerhalb einer Sekunde zwischen zwei Netzwerkknoten gesendet wurden, ausgenommen TCP-, IP- und Ethernet- oder 802.11-Header.

Paketverlust

Paketverlust gilt nur für UDP-Tests, da in TCP alle Pakete bestätigt werden müssen und kein Datenverlust auftreten kann. Der UDP-Verlust wird als Prozentsatz der während der Übertragung verlorenen Daten berechnet. Lassen Sie uns beispielsweise das folgende Ergebnis interpretieren:

```
UDP Down: 60.00 Mbps (Avg: 55), Loss: 40.0%
```

Das bedeutet, dass der Server während des letzten Testzyklus 10 Megabit Daten in 100 Millisekunden gesendet hat (was 100 Megabit pro Sekunde entspricht; tatsächliche Datenmengen und -dauern können variieren – dies ist nur ein Beispiel) und der Client 6 Megabit in 100 Millisekunden empfangen hat, während unterwegs 4 Megabit verloren gegangen sind.

Einige UDP-Verluste kommen recht häufig vor und weisen nicht unbedingt auf ein Problem mit Ihrem Netzwerk hin. Eine ausführliche Diskussion finden Sie im Kapitel **Umgang mit häufigen Problemen**.

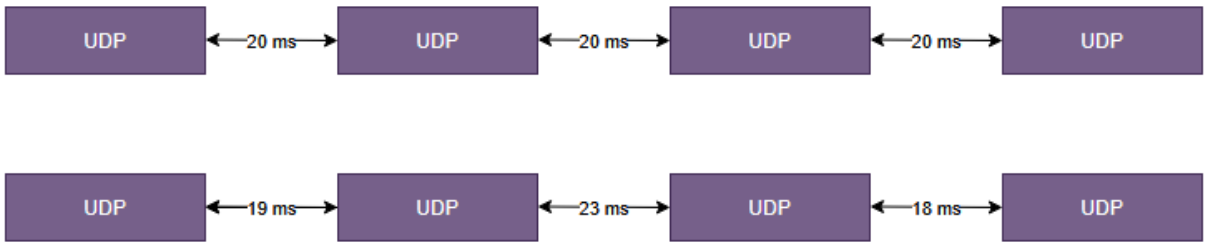
Round-Trip-Zeit

Die Round-Trip-Zeit (RTT) ist die Zeitspanne, die ein Datenpaket benötigt, um vom Client zum Server und zurück zu gelangen. Die Anwendung verwendet TCP-Pakete für RTT-Messungen, die daher

normalerweise etwas langsamer ausfallen als ein standardmäßiger ICMP-Ping.

Jitter

Jitter bezieht sich auf die Schwankung der Paketankunftszeiten, gemessen als Unterschied zwischen der Verzögerung aufeinanderfolgender Pakete. Hoher Jitter kann bei Echtzeitanwendungen wie VoIP und Video-Streaming zu Problemen führen, bei denen ein konsistentes Timing entscheidend ist. Tessabyte berechnet Jitter mithilfe der weithin akzeptierten Methode, die in RFC 3550 beschrieben ist und die ihn als mittlere Abweichung der Paketverzögerungsschwankung definiert. Betrachten Sie zur Veranschaulichung des Konzepts das folgende Diagramm:



Auf der Seite des Absenders überträgt eine Anwendung, beispielsweise ein VoIP-Telefon, alle 20 Millisekunden UDP-Pakete. Auf der Empfängerseite empfängt eine Anwendung diese UDP-Pakete. In einer idealen Welt bleiben die Paketintervalle auf der Empfängerseite gleich bei 20 Millisekunden. In Wirklichkeit weichen diese Intervalle jedoch von den erwarteten 20 Millisekunden ab – einige Pakete kommen schneller an, während andere möglicherweise verzögert ankommen. Diese Variation wird als Jitter bezeichnet. Niedrigere Jitter-Werte deuten auf eine stabilere Netzwerkverbindung hin, während höhere Werte auf eine Überlastung oder Netzwerkinstabilität hinweisen können.

Empfohlene Jitter-Grenzwerte für verschiedene Anwendungen

Anwendung	Akzeptabler Jitter (ms)
VoIP	<30 ms (ideal: <10 ms)
Videokonferenzen (Zoom, Teams usw.)	<40 ms
Online-Gaming	<30 ms (ideal: <10 ms)
Live-Streaming (Twitch, YouTube Live usw.)	<50 ms
Standard-Video-Streaming (Netflix, YouTube usw.)	<100 ms

Häufige Probleme beheben

Bandbreite mit anderen Clients teilen

Da der Tessabyte-Server mehrere Clients gleichzeitig verwalten kann, wird die Bandbreite zwangsläufig zwischen ihnen geteilt, wenn mehr als ein Client mit dem Server verbunden ist. Sofern der Server nicht über eine Verbindung mit sehr großer Bandbreite verfügt, die die Bandbreite der Clients bei weitem übersteigt, sollten Sie damit rechnen, dass sich mehrere gleichzeitige Clientverbindungen auf den Durchsatz pro Client auswirken.

Betrachten Sie beispielsweise ein lokales LAN-Segment mit einer 1-Gbit/s-Verbindung zwischen einem Server und einigen Clientcomputern. Wenn Sie Tessabyte Client nur auf einem dieser Clientcomputer ausführen, können Sie einen maximalen Durchsatz von etwa 0,9 Gbit/s erwarten. Sind drei Clients verbunden, gibt es zwangsläufig Zeiträume, in denen alle drei einen TCP-Datenstrom an den Server senden, da die Testzyklen (TCP Up ➔ TCP Down ➔ UDP Up ➔ UDP Down) nicht synchronisiert sind. In diesen Zeiträumen kann der Durchsatz auf etwa 0,3 Gbit/s pro Client sinken. Sendet zu einem bestimmten Zeitpunkt dagegen nur ein Client Daten, kann der Durchsatz 0,9 Gbit/s erreichen. Daher kann das Diagramm bei mehreren aktiven Clientverbindungen schwankend erscheinen.

Beachten Sie, dass das Protokollfenster des Clients auf der Dashboard-Seite Sie über die Anzahl der derzeit verbundenen Clients informiert, wenn sich diese Zahl ändert. So können Sie jederzeit feststellen, ob die Verbindung ausschließlich Ihnen gehört oder ob andere Clients die Bandbreite mit Ihnen teilen.

Niedriger TCP-Durchsatz

Wenn Sie im Vergleich zu dem, was Sie von der Netzwerkverbindung zwischen dem Server und dem Client erwarten, einen konstant niedrigen Durchsatz feststellen, dann zunächst einmal herzlichen Glückwunsch! Sie haben das richtige Tool verwendet, um das Problem zu entdecken. Lassen Sie uns jedoch nach einer kurzen Feier näher auf das Thema eingehen. Die häufigsten Gründe für einen Durchsatz unterhalb des erwarteten Niveaus sind:

- **Wi-Fi-Netzwerke:** Wenn Sie den Durchsatz über ein Wi-Fi-Netzwerk messen, ist es wichtig zu bedenken, dass die vom drahtlosen AP oder Router angegebene maximale PHY-Rate nur ein theoretisches Maximum ist und in der Praxis nie erreicht wird. In realen Szenarien schränken viele Einschränkungen den WLAN-Durchsatz ein, wie zum Beispiel:
    - Client-Funktionen: Zum Beispiel nur 2 MIMO-Streams im Vergleich zu 4 vom AP unterstützten MIMO-Streams oder eine Kanalbreite von 160 MHz im Vergleich zu 320 MHz, die vom AP unterstützt werden.
    - Protokoll-Overhead: Der durch Protokoll-Header verursachte Overhead.

- Signalstärke: Schwache Signale verringern den Durchsatz.
- RF-Rauschen: Funkfrequenzstörungen können die Leistung beeinträchtigen.
- Medienkonflikt: Wenn mehrere Clients verbunden sind, konkurrieren sie um das gemeinsam genutzte drahtlose Medium, was den Durchsatz weiter verringert.

Das führt uns zum nächsten Punkt.

- **Konkurrierender Datenverkehr (Überlastung):** Der Netzwerkverkehr konkurriert um verfügbare Bandbreite, was zu einer Überlastung führen kann. Dieses Problem ist besonders in Wi-Fi-Netzwerken von Bedeutung, in denen mehrere Clients eine kleine Anzahl von Funkkanälen gemeinsam nutzen und Mechanismen zur Kollisionsvermeidung zur Zugriffsverwaltung einsetzen. Im Gegensatz dazu sind moderne kabelgebundene Netzwerke – beispielsweise solche mit Gigabit-Switches – mit ausreichend interner Kapazität ausgestattet, um die kombinierte Bandbreite aller Ports gleichzeitig zu verarbeiten. Beispielsweise kann ein 4-Port-Gigabit-Switch theoretisch bis zu 4 Gbit/s Gesamtdatenverkehr unterstützen (1 Gbit/s pro Port, in beide Richtungen). Obwohl Verkehrsstaus auf kabelgebundenen lokalen Segmenten seltener vorkommen, kann es in bestimmten Szenarien dennoch zu Staus kommen.
- **CPU- oder Systemengpässe:** Hohe CPU-Auslastung oder schlechte NIC-Offloading-Leistung schränken den Durchsatz ein. Moderne NICs unterstützen das Auslagern von Aufgaben (z. B. Prüfsumme, Segmentierung), und das Fehlen dieser Optimierungen führt zu einer CPU-Überlastung.
- **Zwischennetzwerkgeräte:** Router, Firewalls oder Proxyserver im Pfad können den Datenverkehr drosseln oder verzögern. Fehlkonfigurationen, Traffic Shaping oder richtlinienbasierte Drosselung können den Durchsatz einschränken.
- **Fehlerhafte Verkabelung:** Beschädigte Kabel können zu einer Signalverschlechterung führen, was zu Paketverlusten und häufigen Neuübertragungen führt. Schlecht abgeschirmte Kabel oder Kabel, die nicht den Kategoriespezifikationen entsprechen (z. B. Cat5e, Cat6), können elektromagnetischen Störungen oder Übersprechen ausgesetzt sein. Schließlich verwenden moderne Ethernet-Geräte die automatische Aushandlung, um die bestmögliche Verbindungsgeschwindigkeit (z. B. 1 Gbit/s, 100 Mbit/s) zu bestimmen. Eine fehlerhafte Verkabelung oder Kabel von schlechter Qualität können dazu führen, dass die Verbindung auf eine niedrigere Geschwindigkeit zurückfällt, z. B. 100 Mbit/s statt 1 Gbit/s.
- **Thermische Drosselung**: Wenn eine Netzwerkkarte überhitzt, kann sie drosseln und ihre Verarbeitungsgeschwindigkeit verringern. Dies kann insbesondere bei hohen Datenraten zu einem geringeren Durchsatz und Paketverlusten führen. Eine Überhitzung von Switches oder Routern kann auch dazu führen, dass diese ihre Paketverarbeitungsgeschwindigkeit drosseln, Latenz verursachen oder Pakete vorübergehend verwerfen, um die thermische Stabilität aufrechtzuerhalten.

Beachten Sie, dass dies keineswegs eine umfassende Liste ist; es gibt viele andere mögliche Ursachen für einen geringen Durchsatz, wie z. B. hohe Netzwerklatenz und kleine TCP-Fenstergröße,

Paketfragmentierung usw.

Ungewöhnlich hoher TCP-Durchsatz

Manchmal kann die gemeldete Durchsatzrate das theoretische Maximum überschreiten. Wenn Sie beispielsweise eine 5-Gbit/s-Verbindung zwischen zwei Computern testen, können Sie einen Anstieg des Downlink- oder Uplink-Durchsatzes TCP beobachten, der 5 Gbit/s überschreitet. Dies wird typischerweise durch Pufferung auf Betriebssystemebene verursacht, wo ein relativ großer Datenblock angesammelt wird, bevor er an die empfangende Anwendung weitergeleitet wird.

Wenn Sie solche Spitzen beobachten, ist die beste Lösung die Verwendung einer benutzerdefinierten TCP-Nutzlastgröße. Die Nutzlastgröße sollte groß genug sein, dass die Übertragung über Ihre Netzwerkverbindung mindestens eine halbe Sekunde dauert. Informationen zur Verwendung einer benutzerdefinierten TCP-Nutzlastgröße finden Sie im Kapitel **Anpassen der Einstellungen**.

Netzwerkverbindung fällt nach einigen Testzyklen aus

Dies ist möglicherweise kein gutes Zeichen für Ihre Netzwerkinfrastruktur. Jedes Durchsatztesttool erzeugt eine erhebliche Belastung der Netzwerkhardware, manchmal so weit, dass die Hardware die hohe Last nicht zuverlässig bewältigen kann. Auch wenn der konkrete Grund variieren kann (z. B. könnten die Adapterchips überhitzen und einen Selbstschutzmechanismus wie eine thermische Abschaltung auslösen), ist dies oft ein Hinweis darauf, dass die getestete Infrastruktur den Stresstest nicht bestehen kann.

Hoher UDP-Paketverlust im Upstream und/oder Downstream

Im Allgemeinen ist ein Verlust von UDP-Paketen ungleich Null völlig normal. Im Gegensatz zu TCP ist das UDP-Protokoll verbindungslos und garantiert keine Zustellung. Mehrere Faktoren können zu einem solchen Verlust beitragen:

- **Netzwerküberlastung**: Netzwerkgeräte (Router, Switches) haben begrenzten Pufferspeicher. Wenn das Netzwerk überlastet ist, werden Pakete verworfen.
- **Paketrate übersteigt die Hardwarekapazität**: Wenn der sendende Knoten Pakete schneller überträgt, als der empfangende Knoten oder die zwischengeschaltete Hardware (z. B. Router) verarbeiten kann, werden Pakete verworfen.
- **Pufferüberläufe**: Sowohl der sendende als auch der empfangende Knoten verfügen über Netzwerkpuffer. Wenn diese Puffer aufgrund einer hohen Paketankunftsrate überlaufen, werden Pakete verworfen.
- **Falsch konfigurierte Netzwerkparameter**: Eine Nichtübereinstimmung der maximalen Übertragungseinheit (MTU) kann dazu führen, dass Pakete, die größer als MTU sind,

fragmentiert oder verworfen werden. Stellen Sie sicher, dass Sie keine benutzerdefinierte UDP-Paketgröße verwenden, die die MTU (konfiguriert auf der Seite **Settings**) überschreitet. Einige Hardware verwirft möglicherweise fragmentierte UDP-Pakete. Wenn Ihre benutzerdefinierte Paketgröße beispielsweise 2.000 Byte beträgt, werden Ihre UDP-Pakete wahrscheinlich fragmentiert.

- **QoS-Einstellungen**: Der UDP-Verkehr wird möglicherweise zugunsten anderer Protokolle wie TCP oder UDP mit einem höheren QoS-Tag herabgestuft. Verwenden Sie das QoS-Steuerelement, um zu überprüfen, wie sich ein QoS-Tag mit hoher Priorität auf die Leistung auswirkt.
- **Langsamer/alter Computer**: Versuchen Sie, Tessabyte auf einem anderen Computer auszuführen. Ihr aktueller Computer ist möglicherweise alt oder langsam oder seine CPU ist möglicherweise durch andere Prozesse belastet.

100 % UDP-Paketverlust im Downstream

Ein hundertprozentiger UDP-Verlust im Downlink wird typischerweise durch eine Firewall oder NAT verursacht. Dies bedeutet, dass die vom Server gesendeten UDP-Daten den Client nicht erreichen können. Während des UDP-Tests sendet der Client Upstream-UDP-Datenverkehr an den Server von einem beliebigen UDP-Port an den Server-Port (standardmäßig 32500). Der Downstream-Rückverkehr stammt von einem beliebigen Server-Port und wird an einen Port auf der Client-Seite gesendet, der durch die folgende Regel bestimmt wird: (Server-Port, standardmäßig 32500) + 1. Wenn dieser Port nicht verfügbar ist, wird der nächste verfügbare Port ausgewählt. Während diese Informationen Ihnen bei der Konfiguration einer Firewall- oder Portweiterleitungsregel helfen können, kann **UDP-Verkehr über IPv4 normalerweise keine NATs passieren**. Wenn Tessabyte Server auf einem Computer mit einer öffentlichen IPv4-Adresse außerhalb Ihres LAN ausgeführt wird und Tessabyte Client auf einem Computer ohne öffentliche IPv4-Adresse innerhalb Ihres LAN ausgeführt wird, ist ein Verlust von 100 % UDP unvermeidlich. Wenn Sie UDP testen möchten, sollten Sie die Verwendung von NATs vermeiden und **die Verwendung von IPv6 in Betracht ziehen**, wodurch NAT im Allgemeinen nicht mehr erforderlich ist.

Hoher UDP-Paketverlust im Downstream in WLANs

Ein hoher UDP-Paketverlust im Downstream tritt häufig auf, wenn der Client auf einem Computer mit einer WLAN-Verbindung ausgeführt wird. UDP-Datenverkehr wird nicht bestätigt. Der Absender kann daher so viele Daten übertragen, wie das Netzwerk verarbeiten kann, ohne sich darum zu kümmern, wie viel davon verloren geht. Wenn Sie den Server auf der kabelgebundenen Seite des Netzwerks ausführen, kann ein typischer Computer mit Gigabit-Adapter Hunderte Megabit pro Sekunde senden. Diese Daten erreichen zunächst einen Switch, der den ersten Engpass darstellen kann, und anschließend den Access Point, der ebenfalls häufig einen Engpass darstellt. In einer Umgebung mit mehreren Clients können selbst moderne 802.11be-Access-Points nicht allen Clients gleichzeitig einen Gigabit-Downstream bereitstellen. Daher können viele UDP-Pakete auf dem

Übertragungsweg verloren gehen. Dies ist jedoch die einzige Möglichkeit, den maximalen UDP-Durchsatz im Downstream zu bestimmen. Ein "normaler" UDP-Paketverlust verschwindet in der Regel, sobald Sie in Tessabyte eine Bitratenbegrenzung anwenden. Eine ausführliche Erläuterung finden Sie im Artikel Understanding UDP Metrics in Network Speed Tests. Dieser Artikel ist Teil unseres Blogs Networking Testing Academy.

Info

Tessabyte wird Ihnen von Netmantics LLC zur Verfügung gestellt.

Kommentare? Fragen? Funktionswünsche? Besuchen Sie uns unter **www.netmantics.com**.