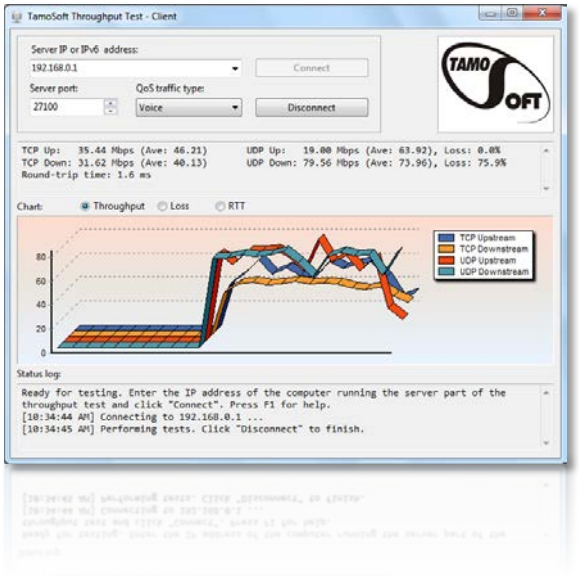
TamoSoft®
Throughput Test

Help Documentation
Version 1.0



Contents

Introduction

Overview

TamoSoft Throughput Test is a utility for testing the performance of a wireless or wired network. This utility continuously sends TCP and UDP data streams across your network and computes important metrics, such as upstream and downstream throughput values, packet loss, and round-trip time, and displays the results in both numeric and chart formats. TamoSoft Throughput Test supports both IPv4 and IPv6 connections and allows the user to evaluate network performance depending on the Quality of Service (QoS) settings.

TamoSoft Throughput Test is free software. It is brought to you by TamoSoft, a software company that develops cutting-edge network monitoring and analysis software for the Internet, LANs, and WLANs, providing clients with the ability and confidence to meet the challenges of tomorrow's technology.

System Requirements

TamoSoft Throughput Test can run on computers with the following minimal system requirements:

- Microsoft Windows: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2. Mac OS X: Mavericks (10.9), Yosemite (10.10), El Capitan (10.11), Sierra (10.12). Android (client only): Android 4.1 and newer.
- 1 GB of RAM.
- 5 MB of free disk space.

Installation and Configuration

To perform a throughput test, the application uses two components: a server and a client. The **server** part of the application listens for connections from the client, and the **client** connects to the server. Once the connection has been established, the client and server send data in both directions, and the client part of the application computes and displays the network metrics.

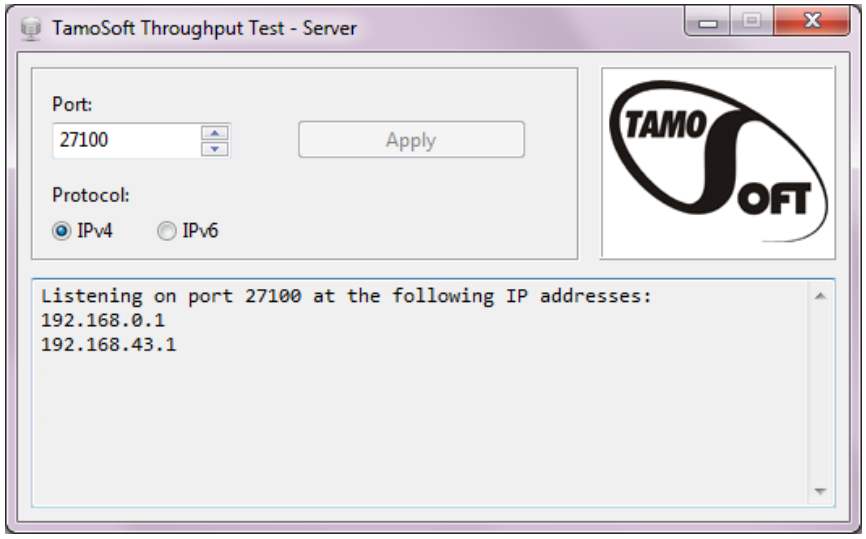
Installation

When you install the application, both the **server** and **client** components are installed. You can then run either one, depending on how you plan to perform the tests. In a WLAN, the server part should be run on the wired side of the network, while the client part should be run on a WLAN client. In this type of a setup, "**downstream**" would be the data flow from the wired side of the network through the access point to the client, and "**upstream**" would be the data flow from the client through the access point to the wired side.

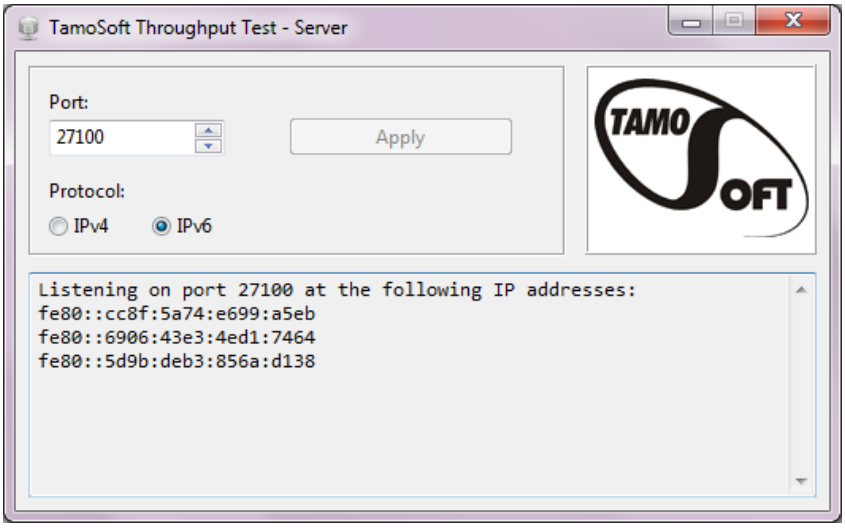
While this application is intended primarily for testing Wi-Fi network throughput, you can also use it to test wired networks. If you test wired LANs, it's not important which of the two computers acts as a server and which one acts as a client.

Configuring the Server

The server part of the application has only two configurable options: the port on which it listens for incoming connections and the network protocol to be used (IP, also known as IPv4, or IPv6). By default, the server listens on port 27100 and uses IPv4, as shown below:



If you want to change the port number or the protocol type, simply make the corresponding changes and click **Apply**:



The picture above illustrates the use of the IPv6 protocol. The log window displays the IPv4 or IPv6 addresses used for listening by the application.

IMPORTANT: This application automatically creates a Windows firewall rule that allows it to accept connections. If you use a third party firewall, be sure to configure it to allow incoming connections for this application. Both UDP and TCP connections must be allowed.

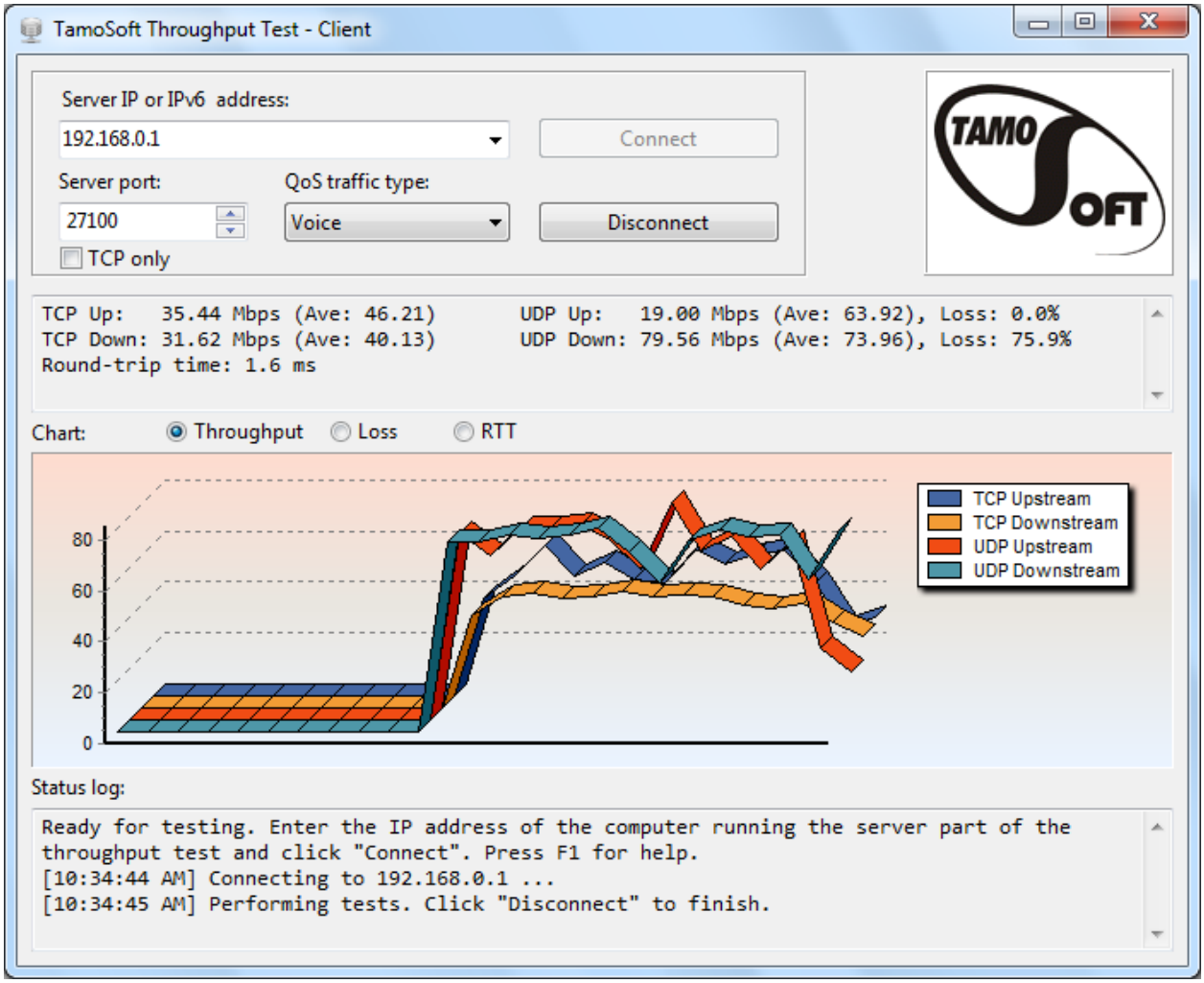
Note that the server part is available for Windows and Mac OS only. It is not available for Android. You can use the Android client with a server running on Windows or Mac OS.

Configuring the Client

In the client component, you only need to specify the port number to be used for connecting to the server (if you changed the default port number 27100 on the server side).

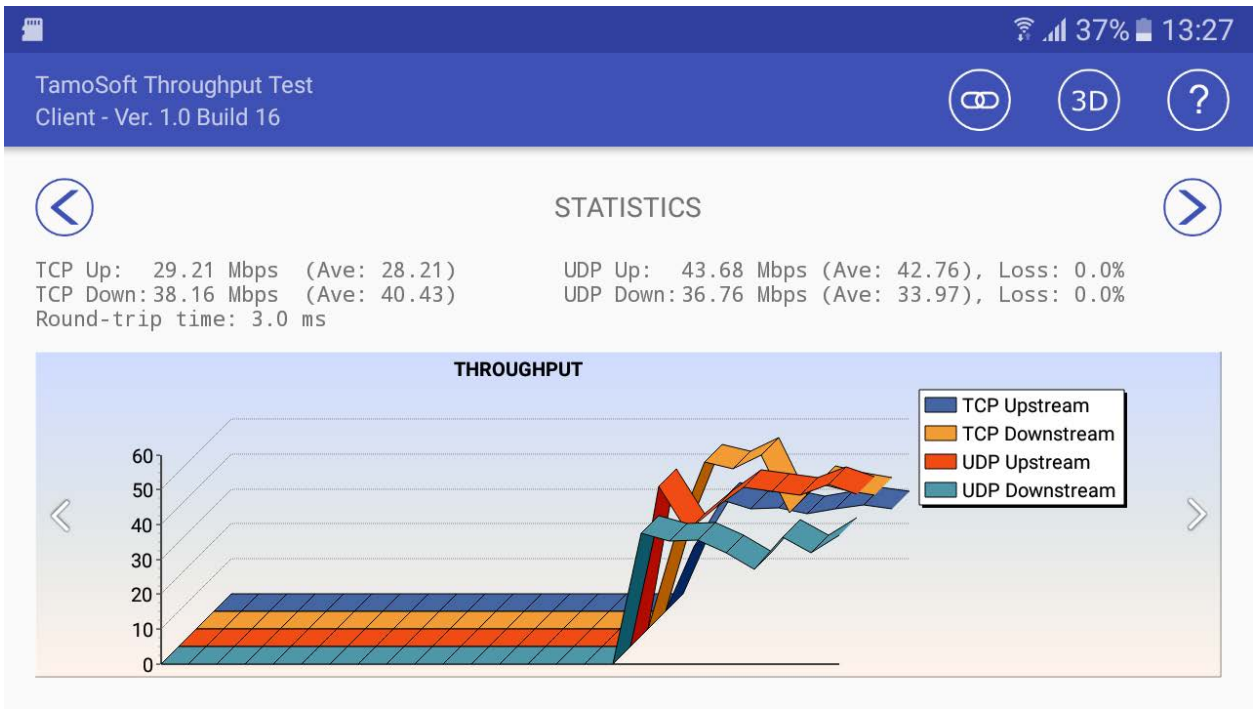
Performing the Tests

To begin throughput testing, you need to launch both the client and server on different computers, as described in the previous chapter. In the client window, enter the IPv4 or IPv6 address of the server and click **Connect**. The client will attempt to connect to the server, and if the connection is successful, continuous throughput testing will commence. This will continue until you click **Disconnect**.



The client window displays TCP and UDP upstream and downstream throughput values (both current and averaged), loss percentage for UDP streams, and the round-trip time. The same data are illustrated by a dynamically updated chart. The chart can display **Throughput**, **Loss**, or **RTT** values, depending on your selection. Note that the application uses Mbps, i.e. **Megabits per second** (not Megabytes!) as the measurement unit. Right-clicking on the chart allows you to clear the chart data, copy the chart, save it as a PNG file, or toggle the 3D view on and off. The status log window at the bottom displays messages about the current application status. If you would like to perform TCP tests only, without UDP, check the **TCP only** box.

On Android devices, the interface is organized slightly differently. The first application screen is used for specifying the server IP address and port, while the second screen displays the charts, as shown below:



Swipe the chart to switch between Throughput, Loss, and RTT views. Click the **3D** button on the tool bar to toggle the 3D view on and off.

QoS Testing

Advanced users might want to use the **QoS traffic type** control to specify the Quality of Service traffic type that will be associated with the TCP and UDP data streams that are sent and received by the application. A description of the use of QoS and related standards and technologies, such as WMM, 802.11e, DSCP, and 802.11p, is beyond the scope of this manual, but in brief, there are two reasons why you may want to use this functionality:

- To check how different QoS traffic types affect throughput. In a properly designed WLAN that uses enterprise-class APs, throughput values for high-priority traffic should exceed those for normal-priority traffic.
- To verify end-to-end QoS network design. In a properly designed WLAN, QoS-tagged traffic must traverse the overall network from the source to the destination through wireless and wired segments with different technology and protocol implementations. When testing this scenario, you should use TamoSoft Throughput Test for generating QoS-tagged traffic, and use packet capture and analysis tools, such as CommView and CommView for WiFi (for wired and wireless LANs, respectively,) to inspect the packets and verify the QoS or DSCP values in the packets.

The table below summarizes different QoS traffic types that you can use. Please pay attention to the fact that not all the QoS types available in the application and described below have corresponding WMM access categories. In practice, this means that when you run a TamoSoft Throughput Test on a WLAN client and select a QoS type that has no WMM mapping, your Wi-Fi adapter driver might fail to QoS-tag packets at all.

QoS Type	Description
Best Effort	Flow traffic has the same network priority as regular traffic not associated with QoS. This traffic type is the same as not specifying priority, and as a result, the DSCP mark and 802.1p tag are not added to sent traffic. Corresponds to the WMM AC-BE access category. On Mac OS X, packets are tagged with Class Selector CS0.
Background	Flow traffic has a network priority lower than that of **Best Effort**. This traffic type could be used for traffic of an application doing data backup. Sent traffic will contain a DSCP mark with a value of 0x08 and an 802.1p tag with a value of 2. Corresponds to the WMM AC-BK access category. On Mac OS X, packets are tagged with Class Selector CS1.
Excellent Effort	Flow traffic has a network priority higher than **Best Effort**, yet lower than **AudioVideo.** This traffic type should be used for data traffic that is more important than normal end-user scenarios, such as e-mail. Sent traffic will contain a DSCP mark with value of 0x28 and 802.1p tag with a value of 5. This doesn't correspond to any WMM access category. On Mac OS X, packets are tagged with Class Selector CS2.
AudioVideo	Flow traffic has a network priority higher than **Excellent Effort**, yet lower than **Voice**. This traffic type should be used for A/V streaming scenarios such as MPEG2 streaming.

	Sent traffic will contain a DSCP mark with a value of 0x28 and an 802.1p tag with a value of 5. Corresponds to the WMM AC-VI access category. On Mac OS X, packets are tagged with Class Selector CS4.
Voice	Flow traffic has a network priority higher than **AudioVideo**, yet lower than **Control**. This traffic type should be used for real time voice streams such as VOIP. Sent traffic will contain a DSCP mark with a value of 0x38 and an 802.1p tag with a value of 7. Corresponds to the WMM AC-VO access category. On Mac OS X, packets are tagged with Class Selector CS5.
Control	Flow traffic has the highest network priority. This traffic type should only be used for the most critical of data. For example, it may be used for data carrying user inputs. Sent traffic will contain a DSCP mark with a value of 0x38 and an 802.1p tag with a value of 7. This does not correspond to any WMM access category. On Mac OS X, packets are tagged with Class Selector CS7.

Understanding Your Results

During each testing cycle, the application performs five tests: sending and receiving TCP data, sending and receiving UDP data, and sending and receiving a time probe packet. Based on these tests, it computes TCP and UDP upstream and downstream throughput values (current, for the latest test, and averaged, for all tests), as well as the round-trip time. When all tasks in a cycle are completed, a new cycle automatically begins.

Throughput

Throughput (also often referred to as "goodput") is the amount of application-layer data delivered from the client to the server (upstream) or from the server to the client (downstream) per second. The protocol overhead is not included, so when we talk, for example, about the TCP throughput rate of 1 Mbps, we mean that 125 Kbytes of actual data payload were sent between two network nodes during one second, not including TCP, IP, and Ethernet or 802.11 headers.

Packet Loss

Packet loss is applicable to UDP tests only, because in TCP, all packets must be acknowledged and no data loss may occur. UDP loss is calculated as the percentage of data that was lost during transmission. For example, let's interpret the following result:

UDP Down: 60.00 Mbps (Ave: 55.00), Loss: 40.0%

This means that during the latest test cycle, the server sent 1 megabit of data in 10 milliseconds (actual data amount and duration may vary; we use this number only as an example,) and the client received 0.6 megabits in 10 milliseconds, while 0.4 megabits were lost en route.

Round-Trip Time

Round-trip time (RTT) is the length of time it takes for a data packet to be sent from the client to the server and back. The application uses TCP packets for RTT measurements.

Frequently Asked Questions

Q. Why is the UDP downstream throughput value always zero?

A. This is a firewall issue. This means that the UDP data being sent from the server cannot reach the client. When performing UDP testing, the client sends upstream UDP traffic to the server from a random UDP port to the server port (27100 by default.) The return downstream traffic goes from port 27101 to the client source port. Use this information to configure your firewall.

Q. Why do I see very high (over 50%) UDP downstream loss?

A. This is normal if you're running the client on a WLAN station. UDP traffic is not acknowledged. This means that the party that sends traffic can send as much traffic as the networking system can handle without "caring" about how much of it will be lost. If you run the server on the wired side of the network, then a typical PC equipped with a gigabit adapter can send hundreds of megabits per second. These data will first reach a switch, which might be the first bottleneck, and then the access point, which is almost always a bottleneck, because a typical 802.11n access point cannot send more than 100 Mbps of data downstream, i.e. to the client. As a result, most of the UDP packets might be lost en route, but this is the only way to figure out the maximum downstream UDP throughput value.

Q. Why does the application require administrative privileges on Windows?

A. The lion's share of problems with throughput tests is related to firewalls. For this reason, we took the liberty of opening the Windows firewall for our EXE file. Our application creates a permissive firewall rule on launch and deletes it on exit. This requires administrative privileges.

Q. I entered a valid IPv6 address, clicked "Connect", and got the "No route to host" error. Why?

A. Link-local IPv6 addresses may require a zone index. For example, instead of fe80:0:0:0:6a5b:35ff:fed1:4633, which does not contain a zone index, you may need to use fe80:0:0:0:6a5b:35ff:fed1:4633%en0.

Q. Are the Windows, Mac, and Android versions interoperable?

A. Yes, you can run the server on a Mac and the client on a Windows machine or vice versa. The Android client can work with either a Mac or a Windows server.

Other Network Analysis Software

In addition to simple test utilities like TamoSoft Throughput Test, we make a number of professional cutting-edge WLAN and LAN analysis and monitoring products:

- TamoGraph Site Survey is a wireless site survey software tool for collecting, visualizing, and analyzing 802.11 a/b/g/n/ac Wi-Fi data. Wireless network deployment and maintenance requires the use of a professional RF site survey tool that facilitates otherwise time-consuming and very complex tasks, such as ongoing analysis and reporting of signal strength, noise and interference, channel allocation, data rates, etc. By using TamoGraph, your business can dramatically reduce the time and costs that are involved in deploying and maintaining Wi-Fi networks and improve network performance and coverage.

- CommView for WiFi is a powerful wireless network monitor and analyzer for 802.11 a/b/g/n/ac networks. Loaded with many user-friendly features, CommView for WiFi combines performance and flexibility with an ease of use unmatched in the industry. CommView for WiFi captures every packet on the air to display important information such as the list of access points and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc. By providing this information, CommView for WiFi can help you to view and examine packets, pinpoint network problems, and troubleshoot your software and hardware.

- NetResident is a network content analysis application designed to monitor, store, and reconstruct a wide range of network events and activities, such as e-mail messages, Web pages, downloaded files, instant messages, and VoIP conversations. NetResident uses advanced monitoring technology to capture the data on the network, save the data to a database, reconstruct it, and display the content in an easy-to-understand format. NetResident helps your organization to protect sensitive information and enforce security policies, as well as to adhere to government and industry information protection regulations, by providing event-based network visibility and data leak detection and by reducing the risks associated with uncontrolled information flow.

We welcome you to visit us at www.tamos.com to learn more about these and our other network-related software products.