

Free report about networking tools

[Experience](#), [Anger](#)



Introduction4

1. Traceroute with Pingplotter4

Functional Description4

Testing and screenshots of Traceroute4

Conclusion on Network Tool5

2. Angry IP Scanner used find that is using my network6

Functional Description6

Testing and screenshots of Angry IP Scanner7

Conclusion on Network Tool7

3. Wireshark8

Functional Description8

Testing and screenshots of Wireshark9

Conclusion on Network Tool10

4. Online Speed Test (Bandwidth Test)10

Functional Description (Expectations, Reason Chosen)10

Testing and screenshots of Bandwidth Test11

Conclusion on Network Tool12

Conclusion13

Introduction

This paper investigates and analyzes a variety of Network Protocol Tools. For this purpose, the paper will present investigation and test of freely available tools for network protocol. In today world budget cuts is common because

now there is less money to invest in staff and new tools. This paper has compiled a list of several free network tools that slightly simplify daily work.

1. Traceroute with Pingplotter

Functional Description

Pingplotter combines basic commands Ping and Traceroute (trace route) in an easy to use graphical interface. There are many benefits of using Pingplotter. It performs a few traces in any location of your choice, then combines and creates a graphical report of the results. The diagram includes the midline with minimum, maximum and final value (Hall, 2000). Recently tracked routes are stored in the history of the left, which saves you the time to enter an address that you check often. Export the results as text or as an image of the chart.

Testing and screenshots of Traceroute

Figure 1: Free product PingPlotter

Conclusion on Network Tool

2. Angry IP Scanner used find that is using my network

Functional Description

Angry IP scanner is a very fast and small IP-scanner. It pings each IP-address to check if it `alive, then maybe this decision and the host tries to connect to the specified in the Options dialog box TCP port

This is an open source produc for Windows, Mac and Linux. Angry IP Scanner is another fast and lightweight tool. It requires no installation and is easy to use. Enter the range of IP addresses that you want to scan, and then click

Start. After a few seconds, you will get a list of all network devices, including the host names and ports are open. Here are some possible uses:

- Scan your network to see if there are unauthorized connections - such as WiFi access point
- If you have a plan for electrical building services, instruct your users to disable the car when they go home, and then scan the network to see if the machine were not accidentally left on
- Use a port scan for basic checks for possible vulnerabilities, or to check whether someone has not set mail or Web servers, of which you know nothing
- Look at how many free IP addresses you have in your subnet, then optimize the border DHCP (Hall, 2000).

Tip: Most personal firewalls block ICMP (ping). If you have a network of windows, you can use Group Policy to allow ICMP from specific sources, such as cars administrators.

Testing and screenshots of Angry IP Scanner

Figure 2: AngryIP Scanner

Conclusion on Network Tool

Serdity IP Scanner works quickly, though, as we found out during our testing, in some cases, it may highlight some resources of a computer, if you have been holding Inspections of the whole class IP naprimer. Osobennosti use a special function that will optimize the search and reduce the scan time (Hall, 2000). To do this, it uses a separate thread for each address it skaniruet. Konechno. Angry IP Scanner comes with many options for the scanning

process, so you should be able to control a specific IP, to find out whether he is alive or not. However, look for porty. S open this utility; you can even get access to the 'Windows Shares, FTP, Telnet, or trace route for each of the selected items in the list. Among the available items, you can view the current user, the working group belongs to, the computer name and MAC adresa. Malo that Angry IP scanner comes as a very lightweight package, but due to its ease of use and solid packaging function may well be one of the best scanners there. There is also a portable version available, called X-Angry IP Scanner.

3. Wireshark

Functional Description

Wireshark it is a network sniffer with the source code. Without any special hardware or reconfigure, the program can intercept incoming and outgoing data on any networked computer interface: Ethernet, WiFi, PPP, loopback, and even USB. Wireshark is usually used to detect network problems, such as congestion, too long waiting time or protocol errors. However, in order to learn Wireshark, do not need to wait when there will be any breakage. Let us get down to the review of this program (Hall, 2000).

Wireshark was written in GTK + libraries and a graphical user interface (GUI). However, beyond the GUI, there is a console implementation of the program on behalf of the TShark, Which has the same functionality as the graphical version of it. Since the program is very popular as an administrative tool for the analysis of networks, it is available in the repositories of almost any distro Linux. There is a version for Windows and Mac OS X. If for some reason you cannot find it in their repositories of Linux, you can always download

ready to build a different distributions from the official site. Alternatively, download, compile and install it from source.

It is worth to note that the launch Wireshark is necessary to make the rights of root, so as to intercept the traffic program require root privileges to access the so-called promiscuous mode (" promiscuous mode "). Wireshark is the core of the library libpcap by which the interception is performed (Zheng et al., 2010). The program has built-in support for a very large number of network devices. Verify whether your network card to work under this program, please visit the project wiki Wireshark. However, not almost all modern Ethernet and Wifi card has any compatibility problems in this program.

Sniffing

Starting a new session interception is made in the program from the menu " Capture". To see a list of network interfaces that are able to detect Wireshark, navigate to the menu " Capture> Interfaces". A dialog box appears in which, in addition to physical devices will be present pseudo-device " any", which captures data from all of the other devices in this list (Zheng et al., 2010).

Before you start, you can specify some options, which will be launched to intercept. Clicking on the " Capture> Options", just select:

- Filters for selective analysis of the traffic (eg, a specific protocol or address range);
- Automatically stop interception on attaining the times set;
- Sort the data according to the specified size, or date.

Testing and screenshots of Wireshark

Conclusion on Network Tool

Wireshark includes many on the analysis of your network, when you explore it in search of the source of problems. For example, you can run a statistical comparison between the two files has been stored sniffing, and it allows you to capture this when you are just learning the problem, and then compare them again. In other words, you can collect and compare the files grips with the different units, for example, in different network segments or with different configurations (Hall, 2000). This is especially useful, as there are build Wireshark for proprietary operating systems: when asking for performance issues you may need to collect information from various sources.

4. Online Speed Test (Bandwidth Test)

Functional Description (Expectations, Reason Chosen)

Internet speed test allows you to test the quality of the connection. If you are having difficulty working in a network, if you have to wait too long, do not get to watch movies and listen to music, it is necessary to determine the actual speed of your network connection. Not always difficulties in work sites associated with low speed internet, there may be other factors that slow page refreshes. If you have multiple computers and home modem is overloaded if there is an overload on the provider level, it really reduces the speed of the Internet, but it is possible influence of external factors (Zheng et al., 2010).

Testing and screenshots of Bandwidth Test

Remember that the speed test result does not show 100% of the connection speed because the results are influenced by different factors such as the status of your line noise / signal attenuation, electromagnetic radio interference etc Furthermore, it should be noted that these types of connections using various protocols (PPP, TCP / IP) which occupy bandwidth, which reduces the bandwidth useful for downloading data (Hall, 2000).

Figure 4: Bandwith speed Test

Conclusion on Network Tool

The speed meter is a tool that allows users to-consumer Internet access through bandwidth real time testing the speed of your broadband connection by transferring a small temporary file and return measure results. While the Speed Test will give consumers information on the relative velocity, IFT cannot verify the accuracy of the test methods. This is intended to give consumer's access to the Internet via bandwidth information about the speed of their broadband connections and raise awareness about the importance of broadband quality in accessing content and services Internet (Zheng et al., 2010).

The tool is based on the transfer of a small amount of generic data back and forth between the user's computer - consumer and the test server. The test measures the bandwidth in terms of the speed at which data can be transmitted between the computer and test servers Your " speed" determines the time it takes to receive or send data, the download speed concerns rate test server for you, and the upload speed is that the test server. In the IFT speed test, broadband speed is measured in megabits per

secon (Hall, 2000).

At the time of testing should be considered that this is not a completely accurate representation of the connection speed provided by your broadband provider. The results may be affected by a number of factors - for example, the test may vary according to the geographical distance of the users the test server, the end user hardware, network congestion, and the time of day. However, this application can be a useful indicator to compare the relative speed consumer broadband connection and understanding of the performance metrics of broadband connections.

Conclusion

A network management system (NetworkManagementSystems) - centralized software systems that collect data on the status of nodes and communication devices on the network, as well as traffic data circulating in the network (Zheng et al., 2010). These systems not only monitor and analyze the network, but also perform in an automatic or semi-automatic mode of action of network management - on and off the device ports, changing the address tables of bridges, switches and routers, etc. Examples of control systems can serve as a popular system HPOpenView, SunNetManager, IBMNetView. Protocol analyzers (Protocolanalyzers). Are software or hardware and software systems that are limited in contrast to the control system only functions for monitoring and analysis of the traffic in the networks (Zheng et al., 2010). A good protocol analyzer can capture and decode packets large number of protocols used in networks - usually a few dozen. Protocol analyzers allow you to set some logical conditions to capture the individual packets and perform a complete decoding of the captured

packets that is shown in a convenient form for the specialist nesting protocol packets at different levels in each other with details of the content of individual fields of each packet. During the design of a new network or upgrading old often require quantitative measurement of certain characteristics of such a network, such as intensity data flows in network communication lines, delays encountered at various stages of processing packets, reaction times to the requests of any kind, the frequency of occurrence certain events, and other characteristics.

References

Hall. E. (2000). Internet Core Protocols: The Definitive Guide: Help for Network Administrators. O'Reilly Media

Zheng, J. Z. J., Jin, G. J. G., Jiang, X. J. X., Qian, J. Q. J., & Xie, Z. X. Z. (2010). Visualization Design Mode for Networking Construction and Management. Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, 8. doi: 10. 1109/ICCSIT. 2010. 5564947