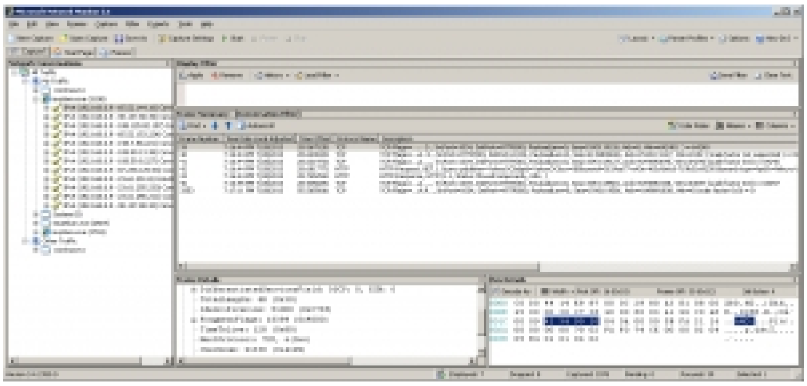
The Top 10 Free Network Monitoring and Analysis Tools for Sys Admins

Andrew Zammit Tabona on July 23, 2013

We know how administrators love free tools that make their life easier and, to supplement the list provided on **101 Free Admin Tools** **,** here are 20 of the best free tools for monitoring devices, services, ports or protocols and analysing traffic on your network. Even if you may have heard of some of these tools before, we’re sure you’ll find a gem or two amongst this list – and if you know of any others, leave us a comment below!

1. Microsoft Network Monitor

Microsoft Network Monitor is a packet analyser that allows you to capture, view and analyse network traffic. This tool is handy for troubleshooting network problems and applications on the network. Main features include support for over 300 public and Microsoft proprietary protocols, simultaneous capture sessions, a Wireless Monitor Mode and sniffing of promiscuous mode traffic, amongst others.



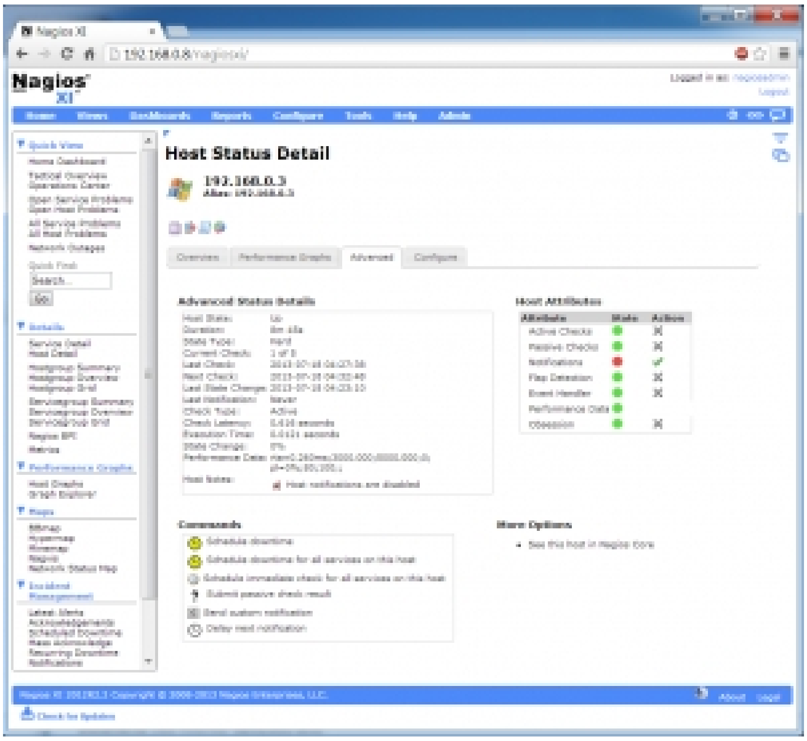
When you launch Microsoft Network Monitor, choose which adapter to bind to from the main window and then click “New Capture” to initiate a new capture tab. Within the Capture tab, click “Capture Settings” to change filter options, adapter options, or global settings accordingly and then hit “Start” to initiate the packet capture process.

2. Nagios

Nagios is a powerful network monitoring tool that helps you to ensure that your critical systems, applications and services are always up and running. It provides features such as alerting, event handling and reporting. The Nagios Core is the heart of the application that contains the core monitoring engine and a basic web UI. On top of the Nagios Core, you are able to implement plugins that will allow you to monitor services, applications, and metrics, a chosen frontend as well as add-ons for data visualisation, graphs, load distribution, and MySQL database support, amongst others.

Tip: If you want to try out Nagios without needing to install and configure it from scratch, download Nagios XI from here and enable the free version. Nagios XI is the pre-configured enterprise class version built upon Nagios Core and is backed by a commercial company that offers support and additional features such as more plugins and advanced reporting.

Note: The free version of Nagios XI is ideal for smaller environments and will monitor up to seven nodes.



Host Status Detail

192.168.0.3
Alias: 192.168.0.3

Advanced Status Details

Host State: Up
Duration: [illegible]
State Type: Hard
Current Check: 1 of 5
Last Check: [illegible]
Next Check: [illegible]
Last State Change: [illegible]
Last Notification: Never
Check Type: Active
Check Latency: [illegible] seconds
Execution Time: [illegible] seconds
State Change: 0%
Performance Data: [illegible]
Host Status: Host notifications are disabled

Host Attributes

Attribute	State	Action
Active Checks	●	☒
Passive Checks	●	☒
Notifications	●	✓
Flap Detection	●	☒
Event Handler	●	☒
Performance Data	●	
Obsession	●	☒

Commands

- Schedule downtime
- Schedule downtime for all services on this host
- Schedule immediate check for all services on this host
- Submit passive check result
- Send custom notification
- Delay next notification

More Options

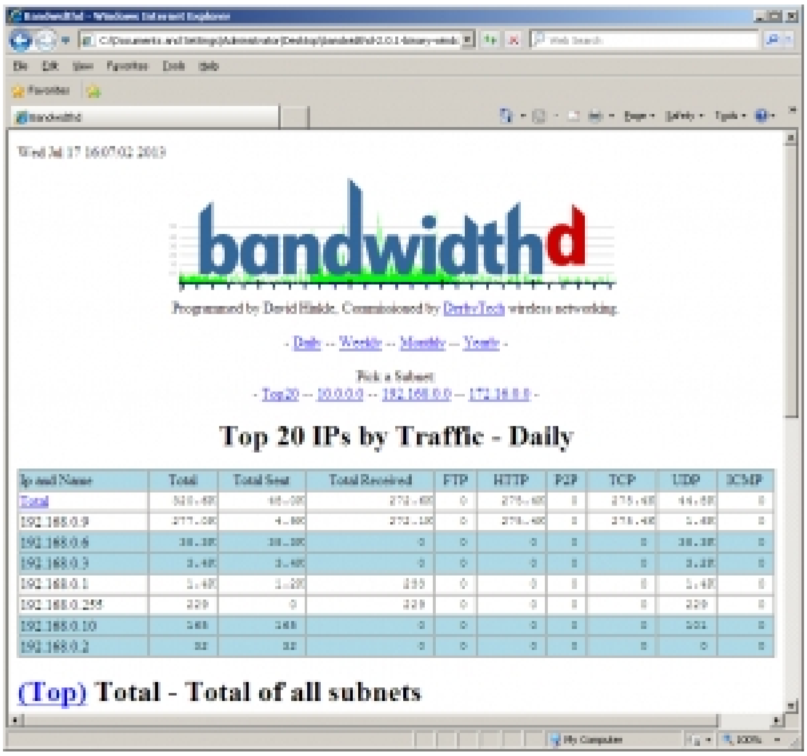
- See this host in Nagios Core

Nagios XI [illegible] Copyright © 2008-2013 Nagios Enterprises, LLC.

Once you’ve installed and configured Nagios, launch the Web UI and begin to configure host groups and service groups. Once Nagios has had some time to monitor the status of the specified hosts and services, it can start to paint a picture of what the health of your systems look like.

3. BandwidthD

BandwidthD monitors TCP/IP network usage and displays the data it has gathered in the form of graphs and tables over different time periods. Each protocol (HTTP, UDP, ICMP, etc) is color-coded for easier reading. BandwidthD runs discretely as a background service.



Wed Jul 17 16:07:02 2013

Programmed by David Hinkle. Commissioned by DerbyTech wireless networking.

- Daily -- Weekly -- Monthly -- Yearly -

Pick a Subnet:
- Top20 -- 10.0.0.0 -- 192.168.0.0 -- 172.16.0.0 -

Top 20 IPs by Traffic - Daily

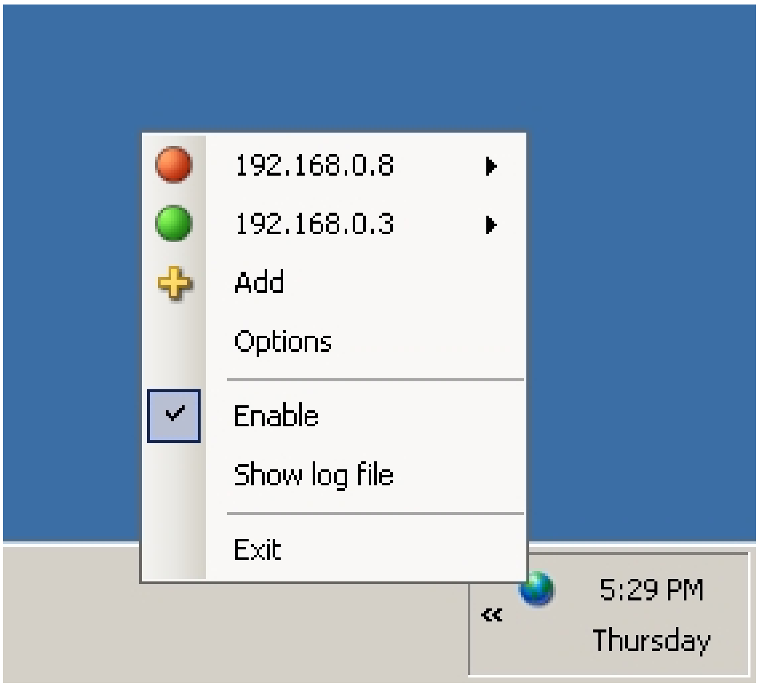
Ip and Name	Total	Total Sent	Total Received	FTP	HTTP	P2P	TCP	UDP	ICMP
Total	310.4K	46.0K	272.6K	0	275.4K	0	275.4K	44.6K	0
192.168.0.9	277.0K	4.8K	272.1K	0	275.4K	0	275.4K	1.4K	0
192.168.0.6	38.3K	38.3K	0	0	0	0	0	38.3K	0
192.168.0.3	3.4K	3.4K	0	0	0	0	0	3.2K	0
192.168.0.1	1.4K	1.2K	255	0	0	0	0	1.4K	0
192.168.0.255	229	0	229	0	0	0	0	229	0
192.168.0.10	168	168	0	0	0	0	0	101	0
192.168.0.2	32	32	0	0	0	0	0	0	0

(Top) Total - Total of all subnets

Installation is easy. Download and install Winpcap version 3.0 or above (you'll already have this installed if you have Wireshark on the same box), unzip BandwidthD to a specified folder, edit the ../etc/bandwidthd.conf file accordingly, double click on the “Install Service” batch file and then start the BandwidthD services from the services.msc console. Once the service is running, give it some time to monitor network traffic and load the index.html page to start viewing bandwidth statistics.

4. EasyNetMonitor

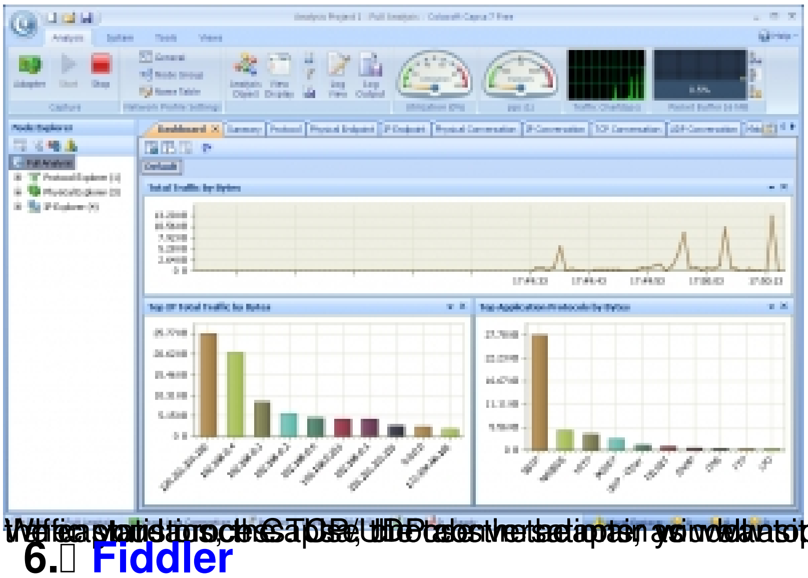
EasyNetMonitor is a super lightweight tool for monitoring local and remote hosts to determine if they are alive or not. It is useful for monitoring critical servers from your desktop, allowing you to get immediate notification (via a balloon popup and/or log file) if a host does not respond to a periodic ping.



Once you launch EasyNetMonitor, it will appear as an icon in the notification area on your desktop where the IP addresses / host names of the machines you want to monitor can be added. Once you’ve added the machines you wish to monitor, be sure to configure the ping delay time and notification setting.

5. Capsa Free

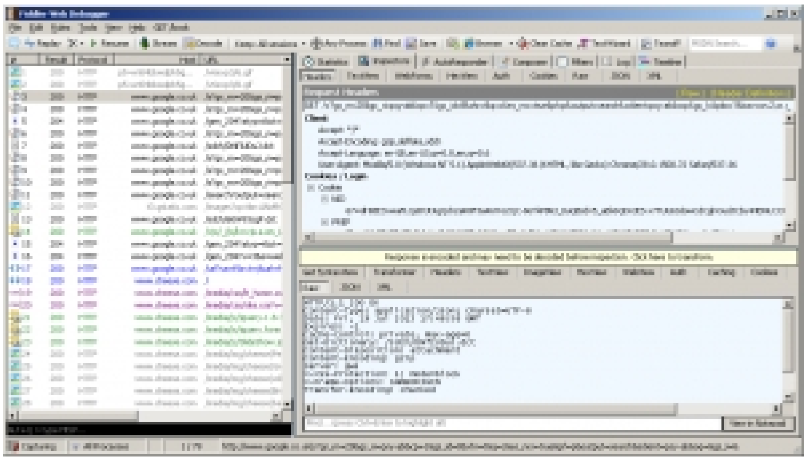
Capsa Free is a network analyzer that allows you to monitor network traffic, troubleshoot network issues and analyze packets. Features include support for over 300 network protocols (including the ability to create and customize protocols), MSN and Yahoo Messenger filters, email monitor and auto-save, and customizable reports and dashboards.



[illegible]

6. [Fiddler]

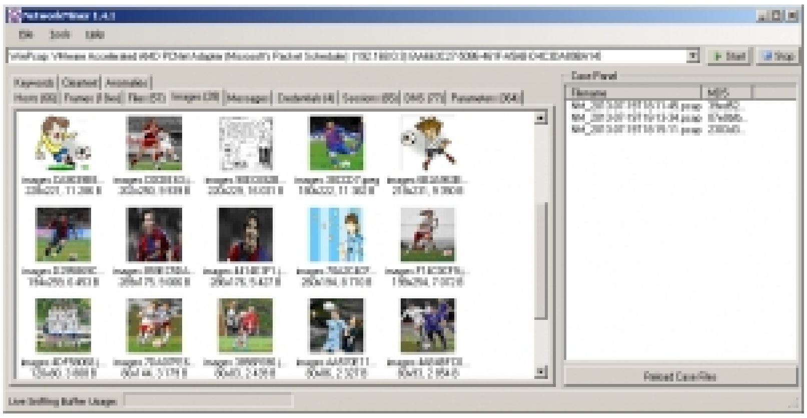
Fiddler is a web debugging tool that captures HTTP traffic between chosen computers and the Internet. It allows you to analyze incoming and outgoing data to monitor and modify requests and responses before they hit the browser. Fiddler gives you extremely detailed information about HTTP traffic and can be used for testing the performance of your websites or security testing of your web applications (e.g. Fiddler can decrypt HTTPS traffic).



When you launch Fiddler, HTTP traffic will start to be captured automatically. To toggle traffic capturing, hit F12. You can choose which processes you wish to capture HTTP traffic for by clicking on “All Processes” in the bottom status bar, or by dragging the “Any Process” icon from the top menu bar onto an open application.

7. [NetworkMiner]

NetworkMiner captures network packets and then parses the data to extract files and images, helping you to reconstruct events that a user has taken on the network – it can also do this by parsing a pre-captured PCAP file. You can enter keywords which will be highlighted as network packets are being captured. NetworkMiner is classed as a Network Forensic Analysis Tool (NFAT) that can obtain information such as hostname, operating system and open ports from hosts.

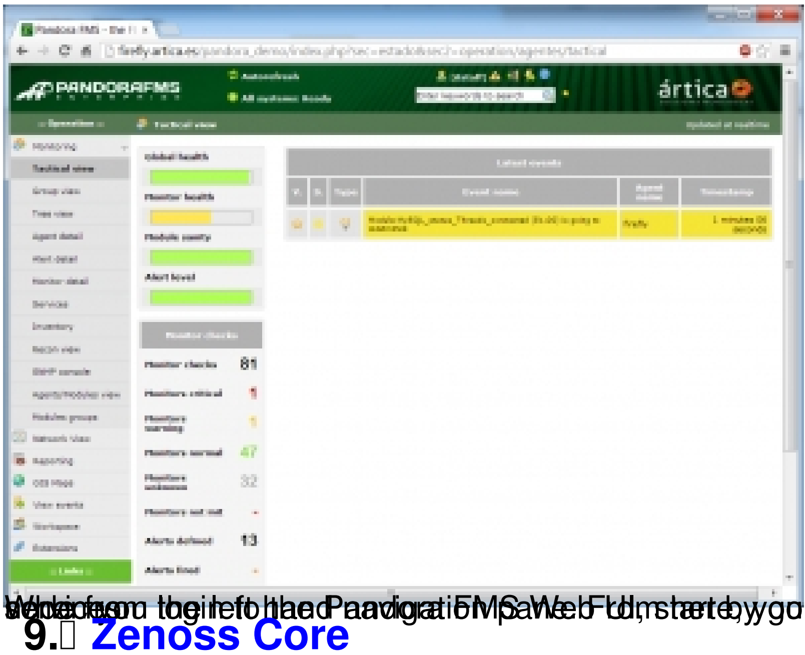


In the example above, I set NetworkMiner to capture packets, opened a web browser and searched for “soccer” as a keyword on Google Images. The images displayed in the Images tab are what I saw during my browser session.

When you load NetworkMiner, choose a network adapter to bind to and hit the “Start” button to initiate the packet capture process.

8. Pandora FMS

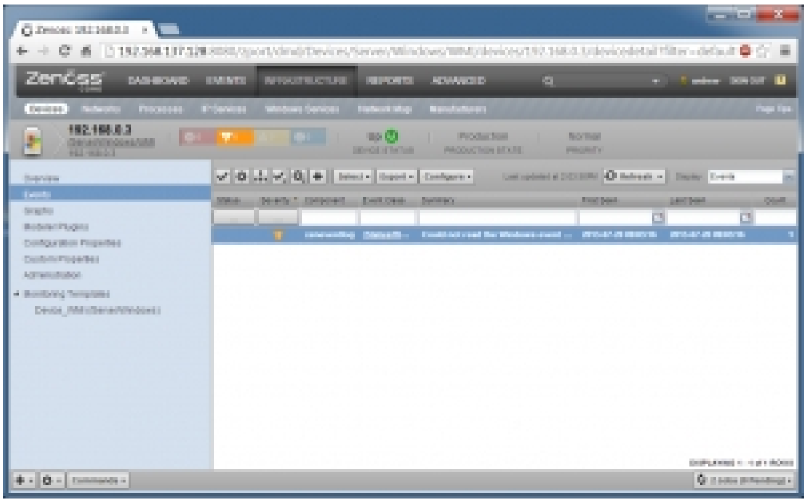
Pandora FMS is a performance monitoring, network monitoring and availability management tool that keeps an eye on servers, applications and communications. It has an advanced event correlation system that allows you to create alerts based on events from different sources and notify administrators before an issue escalates.



When you login to the Pandora FMS Web UI, start by configuring monitoring agents and
section from the left hand navigation panel. Or, start by going to the ‘Agent detail’ and ‘Services’

9. Zenoss Core

Zenoss Core is a powerful open source IT monitoring platform that monitors applications, servers, storage, networking and virtualization to provide availability and performance statistics. It also has a high performance event handling system and an advanced notification system.



Once you login to Zenoss Core Web UI for the first time, you are presented with a two-step wizard that asks you to create user accounts and add your first few devices / hosts to monitor. You are then taken directly to the Dashboard tab. Use the Dashboard, Events, Infrastructure, Reports and Advanced tabs to configure Zenoss Core and review reports and events that need attention.

10. PRTG Network Monitor Freeware

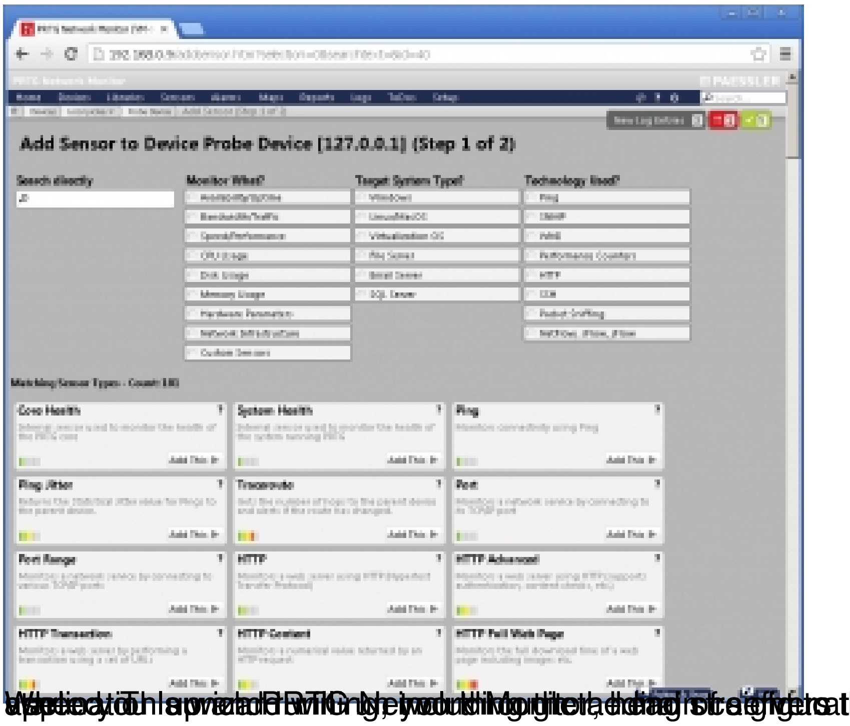
PRTG Network Monitor monitors network availability and network usage using a variety of protocols including SNMP, Netflow and WMI. It is a powerful tool that offers an easy to use web-based interface and apps for iOS and Android. Amongst others, PRTG Network Monitor’s key features include:

(1) Comprehensive Network Monitoring which offers more than 170 sensor types for application monitoring, virtual server monitoring, SLA monitoring, QoS monitoring

(2) Flexible Alerting, including 9 different notification methods, status alerts, limit alerts, threshold alerts, conditional alerts, and alert scheduling

(3) In-Depth Reporting, including the ability to create reports in HTML/PDF format, scheduled reports, as well as pre-defined reports (e.g. Top 100 Ping Times) and report templates.

Note: The Freeware version of PRTG Network Monitor is limited to 10 sensors.



PRTG Network Monitor

Home Devices Libraries Sensors Alarms Maps Reports Logs ToDos Setup

Add Sensor to Device Probe Device [127.0.0.1] (Step 1 of 2)

Search directly	Monitor What?	Target System Type?	Technology Used?
	□ Availability/Uptime	□ Windows	□ Ping
	□ Bandwidth/Traffic	□ Linux/MacOS	□ SNMP
	□ Speed/Performance	□ Virtualization OS	□ WMI
	□ CPU Usage	□ File Server	□ Performance Counters
	□ Disk Usage	□ Email Server	□ HTTP
	□ Memory Usage	□ SQL Server	□ SSH
	□ Hardware Parameters		□ Packet Sniffing
	□ Network Infrastructure		□ NetFlow, IPFIX, jFlow
	□ Custom Sensors		

Matching Sensor Types - Count: 180

Core Health
Internal sensor used to monitor the health of the PRTG core

System Health
Internal sensor used to monitor the health of the system running PRTG

Ping
Monitors connectivity using Ping

Ping Jitter

Traceroute

Port
Monitors a network service by connecting to its TCP/IP port

Port Range
Monitors a network service by connecting to various TCP/IP ports

HTTP
Monitors a web server using HTTP (Hypertext Transfer Protocol)

HTTP Advanced

HTTP Transaction
Monitors a web server by performing a transaction using a set of URLs

HTTP Content
Monitors a numerical value returned by an HTTP request

HTTP Full Web Page
Monitors the full download time of a web page including images etc.

[illegible] PRTG Network Monitor, [illegible] to