## How to Monitor and Analyze Real-time Network Traffic

Real-time network traffic monitoring and analysis are two core works to most enterprise network administrators. However, most administrators soon give up on network monitoring. This is because they find collecting network traffic complicated. Even if they manage to capture network conversations they find it challenging to analyze the raw data in a meaningful way. In this article, you will read how to monitor and analyze real-time network traffic by the great network monitoring software– AthTek NetWalk. If you have no idea about this software, please download and install the <u>free personal edition</u> for a quick view.

When you open <u>AthTek NetWalk</u> for the first time, you will be asked to choose an internet adapter of your network. You can also switch to another one in program's toolbar. After then the real-time network traffic will be displayed in some dynamic diagrams in AthTek NetWalk. Acquiescently you will see some raw data in real-time such as top hosts and bandwidth utilization. You can customize these real-time dynamic diagrams as you need. If you don't need to do further troubleshooting, these dynamic diagrams could be a network analytic report for real-time network monitoring.



For more network analysis details, please click to access the second tab– Layered View. In this tab you can see the detailed network monitoring data in Application, Net&Transport and Physical layers. All the internet requests will be disclosed completely and displayed in groups.

Application      Scott - BOOTP (6)      Content - Attende - NS Einal      Quadation      Content - State      The Annon- NS Einal      Content - State      The Attende - NS Einal      The Attende - State      State	Description 3.90/43 1.90/43 3.90/43 3.90/43 3.90/43 3.90/43 8.134/44 8.134/44 8.134/44 8.139/44 8.139/44 8.155/44 1.95/44 1.95/45 3.90/45 3.	<-> 192.168.1.2/5910 <>> 192.168.1.2/5910 <>> 192.168.1.2/5910 <>> 192.168.1.2/5911 <>> 192.168.1.2/5914 <>> 192.168.1.2/5914 <>> 192.168.1.2/5914 <>> 192.168.1.2/5914 <>>  <>>  <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>> <>>>>>> <>>>>> <>>>>> <>>>>>> <>>>>>>>>>>	7 8 9 00 09 99 22 22 72 71 43		Clent 3.90 1.90 3.90 2.90 3.90 .134 .134 .197	Server 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2	Total Bytes 4,624 5,141 5,199 4,624 5,124 4,624 6,063 97,218	Events 0 2 2 0 1 0 1 0 1 0	Duration 00:00:02 00:00:03 00:00:02 00:00:02 00:00:02 00:00:02 00:00:02	Update Time 2015-01-21 11:49:09 2015-01-21 11:49:10 2015-01-21 11:49:10 2015-01-21 11:49:09 2015-01-21 11:49:10 2015-01-21 11:49:10	
HE BOOTP - BOOTP (6)     Techange - N5 Emal     Quicktime     SP     Ximdons     Trano Nessenge     Trano Nessenge     Trano Nessenge     Sos     Sover - Database     Sos     Sys     Sever - Database     H323     FIP - File Transfer     Kraberos     Mingle - Database     The Nesson's me Protocol     Mingle - Nesson's (12)     Nession's (12)     Nession's (12)	3.90/443 3.90/443 3.90/443 3.90/443 3.90/443 3.90/443 8.134/44 8.134/44 8.135/44 8.155/44 8.155/44 8.155/44 8.155/44 8.157/44	$\begin{array}{l} < > 192.168, 1.2/5910 \\ < > 192.168, 1.2/5910 \\ < > 192.168, 1.2/5910 \\ < > 192.168, 1.2/5911 \\ < > 192.168, 1.2/5911 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\ < > 192.168, 1.2/5913 \\$	7 8 9 0 0 9 20 22 22 72 71 4 3		3.90 1.90 3.90 2.90 3.90 .134 .134 .197	192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2	4,624 5,141 5,199 4,624 5,124 4,624 6,063 97,218	0 2 0 1 0 1 0	00:00:02 00:00:03 00:00:03 00:00:02 00:00:02 00:00:02 00:00:02	2015-01-21 11:49:09 2015-01-21 11:49:10 2015-01-21 11:49:10 2015-01-21 11:49:10 2015-01-21 11:49:09 2015-01-21 11:49:10 2015-01-21 11:49:10	
	1,90/443 3,90/443 1,90/443 2,90/443 3,90/443 8,134/44 8,134/44 8,15/14 8,15/14 8,15/14 8,15/14 8,15/14 8,15/14 8,15/14 8,15/14 8,15/14 8,15/14 8,15/14 8,15/14 1,90/443	$\begin{array}{l} < \rightarrow 192, 168, 1, 2/59 100 \\ < \rightarrow 192, 168, 1, 2/59 110 \\ < \rightarrow 192, 168, 1, 2/59 115 \\ < \rightarrow 192, 168, 1, 2/59 13 \\ < \rightarrow 192, 168, 1, 2/59 14 \\ < \rightarrow 102, 10$	8 9 00 19 19 22 22 72 71 43		1.90 3.90 2.90 3.90 .134 .134 .134 .197	192, 168, 1, 2 192, 168, 1, 2	5,141 5,199 4,624 5,124 4,624 6,063 97,218	2 2 0 1 0 1 0	00:00:03 00:00:03 00:00:02 00:00:02 00:00:02 00:00:02	2015-01-21 11:49:10 2015-01-21 11:49:10 2015-01-21 11:49:09 2015-01-21 11:49:09 2015-01-21 11:49:10 2015-01-21 11:49:10	
Qucktime     Qucktime     Variable	3.90/443 2.90/443 3.90/443 3.90/443 8.134/44 8.137/44 8.157/44 8.157/44 8.157/44 8.157/44 8.1597/44 8.1597/44 8.1597/44	<> 192.168.1.2/5911 <> 192.168.1.2/5915 <> 192.168.1.2/5913 <> 192.168.1.2/5913 <> 192.168.1.2/5913 <> 192.168.1.2/592 3 <> 192.168.1.2/592 3 <> 192.168.1.2/590 3 <> 192.168.1.2/591 <> 192.168.1.2/591	9 0 0 9 40 22 72 71 43		3.90 1.90 2.90 3.90 .134 .134 .134 .197	192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2	5,199 4,624 5,124 4,624 6,063 97,218	2 0 1 0 1 0	00:00:03 00:00:02 00:00:02 00:00:02 00:00:02	2015-01-21 11:49:10 2015-01-21 11:49:09 2015-01-21 11:49:10 2015-01-21 11:49:10	
- StP - Y XWindows - Y Tahoo Messenger - Y Trib- Trivial File Transfer - Y 596 - Y 505 server - Database - Y 505 server - Database - Y Hy - Joatabase - Y Hy - Net Database - Y Hy - Net Transfer - Y Kurberos - Y Hy - Network Time Protocol - Y Hy - Network Time Protocol	1,90/443 2,90/443 3,90/443 8,134/44 8,134/44 8,137/44 8,157/44 3,90/443 3,90/443 8,137/44	<> 192.168.1.2/5915 <> 192.168.1.2/5913 <> 192.168.1.2/5914 <> 192.168.1.2/5914 <> 192.168.1.2/5914 <> 192.168.1.2/5913 <> 192.168.1.2/591 <> 192.168.1.2/591 <> 192.168.1.2/591 <> 192.168.1.2/591	0 0 99 440 22 72 71 413		1.90 2.90 3.90 .134 .134 .197	192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2	4,624 5,124 4,624 6,063 97,218	0 1 0 1	00:00:02 00:00:02 00:00:02 00:00:02	2015-01-21 11:49:09 2015-01-21 11:49:10 2015-01-21 11:49:10	
	2,90/443 3,90/443 8,134/44 8,134/44 8,165/44 8,165/44 3,90/443 8,197/44	<> 192.168.1.2/5913 <> 192.168.1.2/5914 3 <> 192.168.1.2/5914 3 <> 192.168.1.2/591 3 <> 192.168.1.2/591 3 <> 192.168.1.2/591 3 <> 192.168.1.2/591 <> 192.168.1.2/5902	0 99 440 422 72 71 443		2.90 3.90 .134 .134 .197	192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2	5,124 4,624 6,063 97,218	1 0 1 0	00:00:02 00:00:02 00:00:02	2015-01-21 11:49:10 2015-01-21 11:49:10	
	3,90/443 8,134/44 8,134/44 8,155/44 8,165/44 8,165/44 3,90/443 8,197/44	<> 192.168.1.2/5914 3 <> 192.168.1.2/5914 3 <> 192.168.1.2/592 3 <> 192.168.1.2/590 3 <> 192.168.1.2/591 3 <> 192.168.1.2/591 <> 173.194/30.134/4 <> 192.168.1.2/5902	9 40 22 72 71 43		3.90 .134 .134 .197	192.168.1.2 192.168.1.2 192.168.1.2 192.168.1.2	4,624 6,063 97,218	0	00:00:02	2015-01-21 11:49:10	
IFIP - Trivel Fiel Transfer       Image: State Sta	8, 134/44 8, 134/44 8, 197/44 8, 165/44 7/597255 3, 90/443 8, 197/44	3 <> 192.168.1.2/992 3 <> 192.168.1.2/990 3 <> 192.168.1.2/990 3 <> 192.168.1.2/991 <> 192.168.1.2/991 <> 192.168.1.2/9902	40 122 72 71 143		.134 .134 .197	192.168.1.2 192.168.1.2 192.168.1.2	6,063 97,218	1	00:00:02	2015-01-21 11:49:10 2015-01-21 11:49:10 2015-01-21 11:49:10	
Shot = Database     Grade - Database     Grade - Database     WrSQL - Database     WrSQ	8.134/44 8.197/44 8.165/44 3.90/443 8.197/44 8.197/44	3 <> 192.168.1.2/590 3 <> 192.168.1.2/591 3 <> 192.168.1.2/591 <-> 173.194.38.134/4 <-> 192.168.1.2/5902	22 72 71 43		.134 .197	192.168.1.2 192.168.1.2	97,218	0	00:00:02		
Volue - Database     SQLerve - Database     MySQL - Database     MySQL - Database     TH - 33     FTP - File Transfer     WTP- Network Time Protocol     Note: Network Time Protocol     Note: No	8.197/44 8.165/44 2/59255 3.90/443 8.197/44	3 <> 192.168.1.2/591 3 <> 192.168.1.2/591 <-> 173.194.38.134/4 <-> 192.168.1.2/5902	72 71 43		. 197	192, 168, 1, 2		0			
Sq. 35 K = Totalobee     Sq. 35 K = Total	8, 165/44 77/59258 3, 90/443 8, 197/44	3 <> 192.168.1.2/591 <> 173.194.38.134/4 <> 192.168.1.2/5902	71 43				4,861	0	00:00:02	2015-01-21 11:49:10	
H 132     FTP - File Transfer     FTP - File Transfer     TTP - Network Time Protocol     NetBIOS (12)     NetBIOS (12)	3.90/443 8.197/44	<-> 173.194.38.134/4 <> 192.168.1.2/5902	M3		. 165	192.168.1.2	5,419	1	00:00:02	2015-01-21 11:49:10	
FTP - File Transfer Kerberos TTP - Network Time Protocol	<ul> <li>3.90/443</li> <li>8.197/44</li> </ul>	<> 192.168.1.2/5902			1.1.2 1	3.194.38.134	6,302	0	00:00:03	2015-01-21 11:49:11	
Kerberos NTP - Network Time Protocol KetBIOS (12)	8.197/44		5		3.90	192.168.1.2	731	0	00:00:00	2015-01-21 11:49:07	
The NTP - Network Time Protocol	A 100 100 100	3 <> 192.168.1.2/590	124		. 197	192.168.1.2	731	0	00:00:00	2015-01-21 11:49:07	
- 1 NetBIOS (12)	8, 165/44	3 <> 192.168.1.2/591	.86		.165	192, 168, 1, 2	5,141	2	00:00:03	2015-01-21 11:49:11	
TO CARLO Alebund Management	8.134/44	3 <> 192.168.1.2/592	183	6	. 134	192.168.1.2	6,666	0	00:00:03	2015-01-21 11:49:11	
Shame - Network management											
BGP - Border Gateway Protocol	Statistics Events										
IRC - Internet Relay Chat	Clier	t	Se	rver	G	obal	al				
PTEP - Parl Time Strasming	lost Name	192.168.1.2 He	2 Host Name	173.194.38.134	Start Time	2015-01-21 11:49:07					
T IMAP	P Address	192, 168, 1.2 IP	Address	173.194.38.134	Last Update Time	2015-01-	2015-01-21 11:49:11 00:00:03.268				
Remote Desktop	AAC Address	1E:40 M	IAC Address	65:FE	Duration	0					
WHOIS P	Port	59258 Pc	38 Port 6 Packets Sent		Status		Completed 0 1,488 58				
SSH - Secure Shell	Packets Sent	6 Pa			Events						
BitTorrent - P2P B	Bytes Sent	1.23 KB By	ytes Sent	4.92 KB							
- TRTP - VoIP	CP Max Window	32,768 TC	CP Max Window	45,024							
MSN - Windows Live Messenger T	TCP Min Window	0 TC	CP Min Window	42,900 Average Packet Size		370					
- The Others - Unclassified (9444)				Transport Protocol		TCP					
•					TCP Connection Setup Time		N/A				
Application					TCP Retries		0				

Click to access the third tab and you will see all the events happened during network monitoring. Blue ball stands for TCP Connection Slow Setup. Yellow ball stands for TCP Out of Order. Orange ball stands for TCP Retransmission. Red ball stands for TCP Important Errors. Right click on any of the records, and then network administrator can jump to the Net&Transport layer for troubleshooting.

Ath Tek N	NetWalk - Microsoft									
View	Monitor Capture	Tools Help								
-			-							
2.60	U • 🐨 😤	199 🖏 🕨 💻 😏 🏹	2	💑 🛄 🖑 🧕						
Monito	or									
To	tal Count: 18,7	152 993 917,282		0 🐴 Filte	r: Net&Transport	ayer 🔻				
	Time	Description	_	Sec. Addrace	Sec. Port	Det Ad	franc	Det Port Tuna	Lavar	
	1010 PALE AL AL AL AL AL				448	107.10		Sacron Type	cuye	
	2015-01-21 11:49:08	TCP Retransmission		.134	443	192.16	8.1.2	59,145 Advanced	Netal ransport Layer	
8	2015-01-21 11:49:08	TCP Retransmission		3.90	443	192.16	8.1.2	59,062 Advanced	NetaTransport Layer	
	2015-01-21 11:49:08	TCP Retransmission		.134	443	192.16	8.1.2	59,115 Advanced	Net&Transport Layer	
	2015-01-21 11:49:08	TCP Retransmission		3.90	443	192.16	8.1.2	59,026 Advanced	Net&Transport Layer	
•	2015-01-21 11:49:08	TCP Retransmission		-197	443	192.16	8.1.2	58,979 Advanced	Net&Transport Layer	
	2015-01-21 11:49:08	TCP Retransmission		1.90	443	192.16	8.1.2	59,063 Advanced	Net&Transport Layer	
	2015-01-21 11:49:08	TCP Retransmission		3.90	443	192.16	8.1.2	59,007 Advanced	Net&Transport Layer	
	2015-01-21 11:49:08	TCP Retransmission	-	. 197	443	192.16	8.1.2	59,006 Advanced	Net&Transport Layer	
	2015-01-21 11:49:08	TCP Retransmission	-	64-122-106-12	0.10	192,16	8.1.2	58,993 Advanced	Net&TransportLayer	
•	2015-01-21 11:49:08	TCP Retransmission	13	Сору	Ctri+	-	134	443 Advanced	Net&Transport Layer	
9	2015-01-21 11:49:08	TCP Connection Slow Setup	195	Europet Coloriand			2.90	443 Advanced	Net&Transport Layer	
•	2015-01-21 11:49:08	TCP Retransmission	-	export selecteu		1	,134	443 Advanced	Net&Transport Layer	
•	2015-01-21 11:49:08	TCP Retransmission		Export All		1	.134	443 Advanced	Net&Transport Layer	
•	2015-01-21 11:49:08	TCP Retransmission				-	2.90	443 Advanced	Net&Transport Layer	
	2015-01-21 11:49:08	TCP Retransmission		Jump to Host 64.233	186.17		.165	443 Advanced	Net&Transport Layer	
	2015-01-21 11:49:08	TCP Retransmission		Jump to Host 192.16	8.1.2		.1.2	58,989 Advanced	Net&Transport Layer	
•	2015-01-21 11:49:08	TCP Retransmission	_	197 168.1.2	59,301	1	.134	443 Advanced	Net&Transport Layer	
	2015-01-21 11:49:09	TCP Retransmission		8.1.2	58,989		4.90	443 Advanced	Net&Transport Layer	
	2015-01-21 11:49:09	TCP Retransmission		8.1.2	59,318	17	134	443 Advanced	Net&Transport Layer	
	2015-01-21 11:49:09	TCP Retransmission		B.134	443		.1.2	59,202 Advanced	Net&Transport Laver	
	2015-01-21 11:49:09	TCP Retransmission		8.1.2	59,344	17	.134	443 Advanced	Net&Transport Layer	
	2015-01-21 11:49:09	TCP Retransmission		8.1.2	59,090	2	.165	443 Advanced	Net&Transport Layer	
	2015-01-21 11:49:09	TCP Retransmission		93.90	443		1.2	59,092 Advanced	Net&Transport Laver	
	2015-01-21 11:49:09	TCP Retransmission		8.1.2	59,204	2	165	443 Advanced	Net&Transport Laver	
	2015-01-21 11:49:09	TCP Retransmission		8,1.2	59,205	2	197	443 Advanced	Net&Transport Layer	
	2015-01-21 11:49:09	TCP Retransmission		92.90	443	Lun	1.1.2	58,964 Advanced	Net&Transport Laver	
	2015-01-21 11:49:09	TCP Retransmission		173, 194, 38, 134	443	192,16	8.1.2	59,089 Advanced	Net&Transport Laver	
	2015-01-21 11:49:09	TCP Retransmission		173, 194, 38, 134	443	192.16	8.1.2	59,170 Advanced	NetSTransport Laver	
	2015-01-21 11:49:09	TCP Retransmission		74,125,193,90	443	192,16	8.1.2	59,106 Advanced	Net&Transport Laver	
	2015-01-21 11:49:09	TCP Retransmission		192, 168, 1, 2	59,173	74, 125, 19	93.90	443 Advanced	Net&Transport Laver	
1	2015-01-21 11-49-09	TCP Retransmission		216 58 218 165	443	192.16	812	59 142 Advanced	NetSTrapsport Laver	
	2015-01-21 11:40-00	TCP Retransmission		192 168 1 2	59 202	173 194 3	8 134	443 Advanced	NetSTransport Laver	

Click on the fourth tab and you can see the real-time matrix map of your network. You can choose to display the Matrix Map on IP/Domain or MAC address basis. Green line stands for real-time activate connection and blue line stands for historical connection. Like in Events tab,

double click on any of the addresses network administrator can jump to the Net&Transport layer for troubleshooting.



Click on the last tab, you will see the real-time traffic in dynamic area chart, curve chart, bar chart or pie chart.

