Application Note

Network Reporting with Exinda Networks

Network traffic optimization reduces the reliance of business upon costly capacity bandwidth upgrades. Exinda Networks delivers the means to effectively deliver traffic optimization through your network through an accessible user interface. The first step to using this interface for optimization is to ascertain how your network is operating to identify any efficiency changes that must be made. Exinda Optimizer allows you to take this step with its extensive network monitoring capabilities. To present an easy to understand overview your network, detailed reports can be generated with your Exinda Optimizer, allowing you to determine how your network is operating.

We now provide an overview of how you can use the reporting feature of your Exinda Optimizer.

About this Document

This document contains the following sections:

Document Definitions

A complete reference of technical terminology used in this application note is provided at the back of the document on page 18.

Question: What kind of reports can my Exinda Optimizer generate?

Your Exinda Optimizer can create Adobe portable document format (pdf) compatible documents containing the following information about your network:

- **Interface Summary:** This section allows you to see how much data your network is carrying at different times of the day. This information allows you to determine the peak traffic periods on your network and verify whether additional network resource capacity is required.
- **Network Summary:** This section allows you to pinpoint the specific sources of the majority of your network traffic at different times in the day.
- **Optimizer Policy Throughput:** This report section displays how your Exinda Optimizer policies are performing over the day. For more information about Optimization policies, refer to "*Application Note: Policy Configuration with Exinda Optimizer*"[1]
- **Remote SLA:** This section displays the availability and reachability of a remote (external) host over different times of the day. Use this report to verify that your ISP is providing with an appropriate level of service, or simply to ensure that your network is meeting your connectivity requirements.
- **Applications:** This section displays the specific applications that are consuming the majority of your network resources over the day. You can use this information to determine whether any unnecessary applications are congesting your network.
- **Hosts:** This section displays the specific hosts (internal and external to your network) that are consuming the most of your network resources over the day. You can use this information to determine which of your network hosts are the most resource intensive.
- **Conversations:** This section identifies the specific conversations (between two hosts using a single application) that are consuming the majority of your network resources over the day.
- **Subnets:** This section provides details about the network traffic into and out of the defined subnets of your network. You can use this feature to identify the network traffic from each department of your business or from groups of external hosts. For further information about defining subnets, refer to section 2.17 of "*Exinda Optimizer: Appliance User Manual*".

As mentioned previously, this application note contains an annotated sample report to demonstrate the power of Exinda Optimizer's monitor reports.

[1] Available at: http://www.exinda.com/pdfs/Exinda_AppNote_Policy_Configuration.pdf.

Question: How can I generate a monitor report?

Monitor Reports are generated from the report generation interface shown below in Figure 1. This interface can be brought up by clicking on the “Reporting” sub menu link as shown:

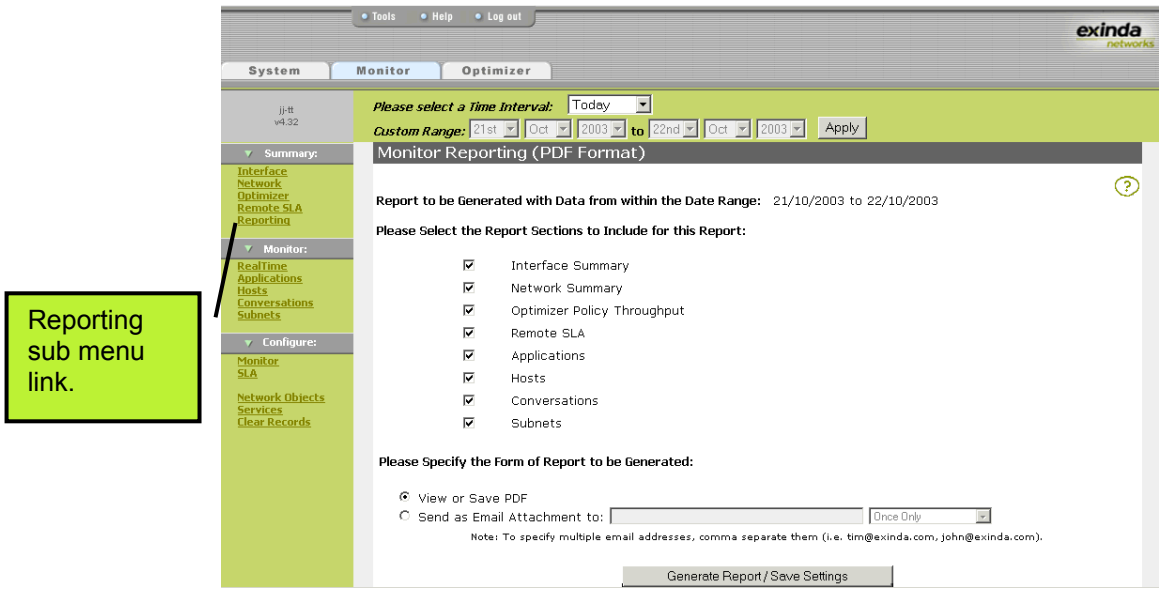


Figure 1. Report Generation Interface.

As you can see in Figure 1, you can select to include report sections (described above) by clicking on the appropriate check boxes. Once this is done, select how you want to view the report from the following settings:

1. Generate the report and download it directly to your computer, allowing you to generate a report on demand.

2. Send the report as an email attachment. This can be done on demand, or automatically configured to send a report to you periodically.

Reports are generated to conform to the Adobe Portable Document Format (pdf) standard. As such, you will need to have Adobe Acrobat reader installed on your computer in order to read your reports. Acrobat can be downloaded free of charge from the internet: ***http://www.adobe.com/products/acrobat/readstep2.html***. Once you have installed this software, you can open Monitor reports as through your Windows Filesystem explorer.

Question: How do I read my monitor report?

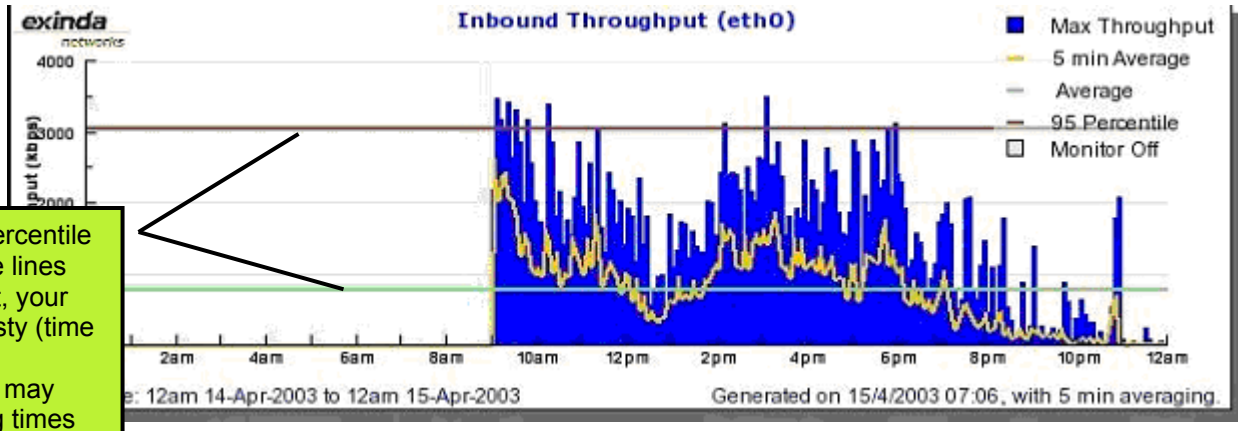
Once you have received your monitor report, you can open the pdf document for reading or printing. The report is structured simply in the order of the report sections you selected in the Report Generation Interface shown in Figure 1. A front cover is provided for the report with report title and report data range information.

Case Study: How can I use a typical monitor report?

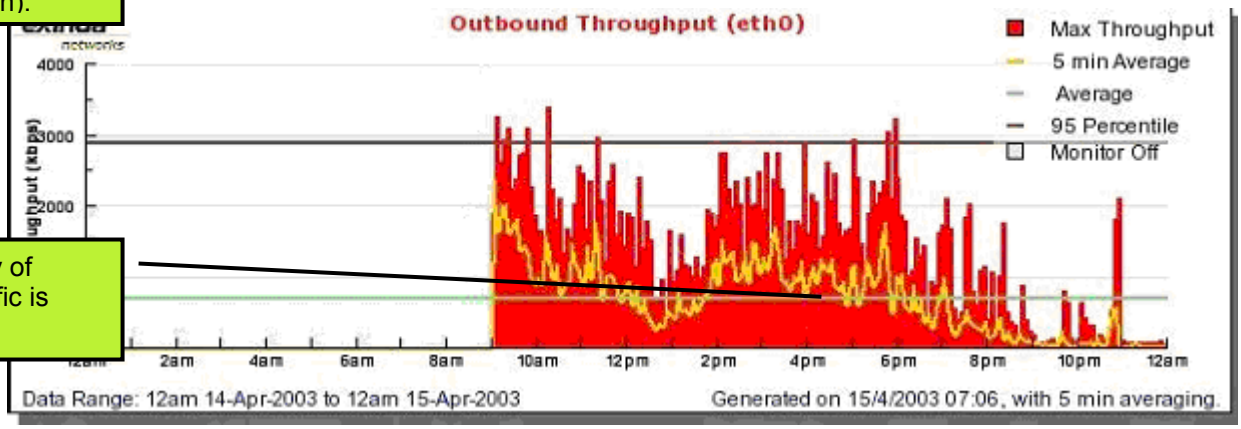
This section details a sample monitor report to demonstrate the many ways in which monitor reports can improve in the performance of you business communications network. This section will provide an actual monitor report, noting the various important sections.

Interface Summary

Data Range: 12am 14/4/2003 to 12am 15/4/2003



As the 95 percentile and average lines are far apart, your traffic is bursty (time sensitive applications may suffer during times of congestion).



The Majority of network traffic is before 6pm

Link Interface Summary (eth0)

Link Status	Data Direction	Total Data (MB)	Throughput (kbps)		
			Min	Avg	Max
Monitored	Inbound	5308.459	0.000	805.313	3495.000
	Outbound	4685.163	0.000	710.757	3380.000

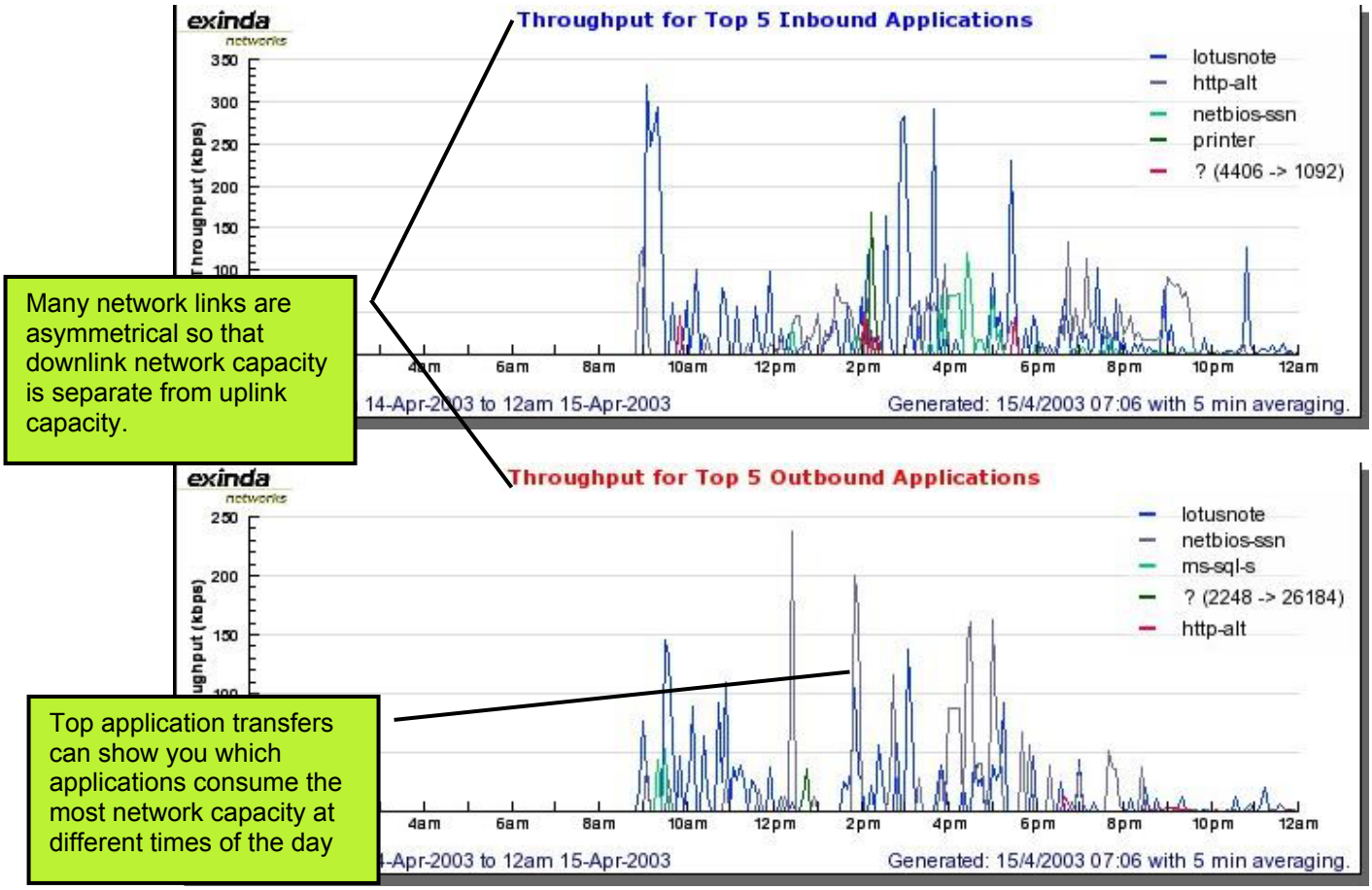
Data transfer statistics can show how much data you have transmitted over you network

Differences between average and max throughput show how bursty your traffic is.

In this section of the monitor report, you can see the times of the day that your network is busy – pinpointing times of congestion when traffic prioritization may be needed. Differences between average and maximum measurements also indicate the burstiness of your traffic. Bursty traffic often is the cause of performance problems with time sensitive applications.

Traffic Throughput By Most Utilised Application

Data Range: 14/4/2003 to 15/4/2003



Many network links are asymmetrical so that downlink network capacity is separate from uplink capacity.

Top application transfers can show you which applications consume the most network capacity at different times of the day

---

Here, top applications in your network over the day are presented. Two different graphs (inbound and outbound) as most network links are asynchronous so that network traffic on the downlink (inbound) does not affect uplink (outbound) applications. Using these graphs, you can easily determine which applications are consuming the most network capacity and diagnose problems such as:

a) Starvation of resources for critical applications,

b) Over utilization of network capacity by non-essential or wasteful applications (eg. Kazaa file sharing), and

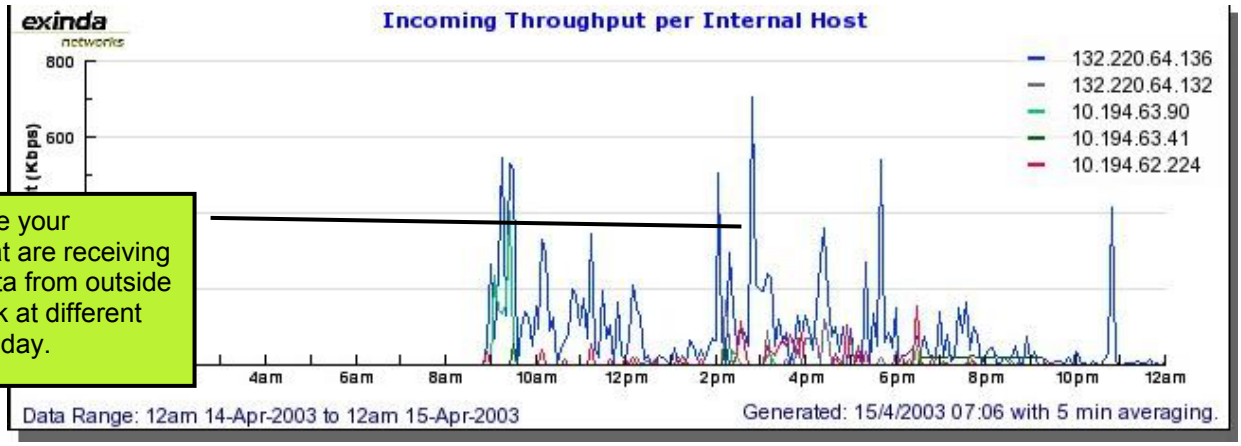
c) Security risks caused by malicious applications operating over your network.

Once these problems have been diagnosed you can take action with your Exinda Optimizer to improve network reliability.

Traffic Throughput By Most Utilised Host

Data Range: 14/4/2003 to 15/4/2003

Hosts (inside your network) that are receiving the most data from outside your network at different times of the day.

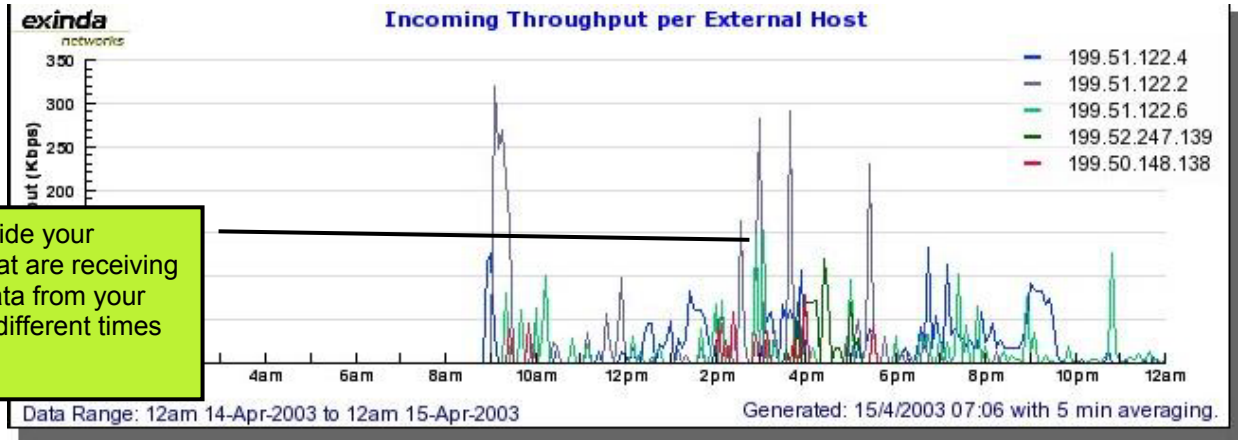


Hosts (inside your network) that are sending the most data from your network at different times of the day.

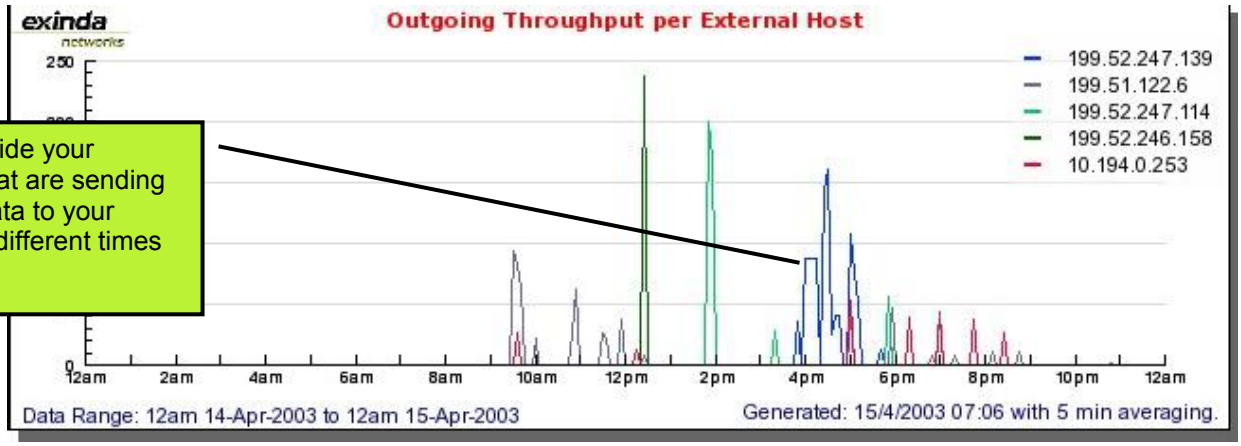
Top Internal Hosts shows each host inside your network that is sending and receiving the most data over the day. With this display you may determine hosts that are accessing the network unnecessarily. This process is made simple using the top applications network display in addition to this display.

Traffic Throughput By Most Utilised Host

Data Range: 14/4/2003 to 15/4/2003



Hosts (outside your network) that are receiving the most data from your network at different times of the day.



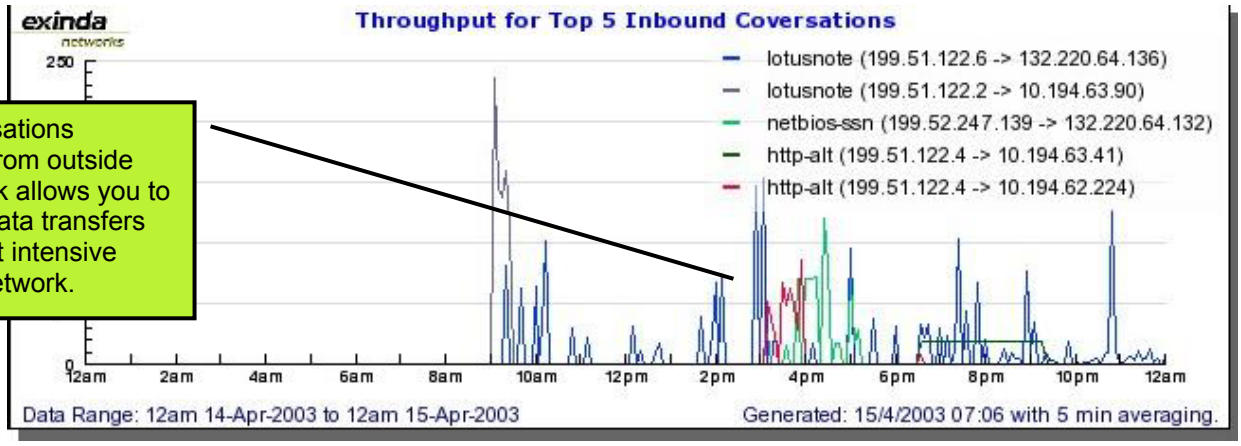
Hosts (outside your network) that are sending the most data to your network at different times of the day.

The previous report page showed the hosts inside your network that are transmitting and receiving data. In contrast, this page shows the hosts outside your network that are being accessed. Malicious and unwanted hosts may appear here highlighting a security or efficiency problem in your network.

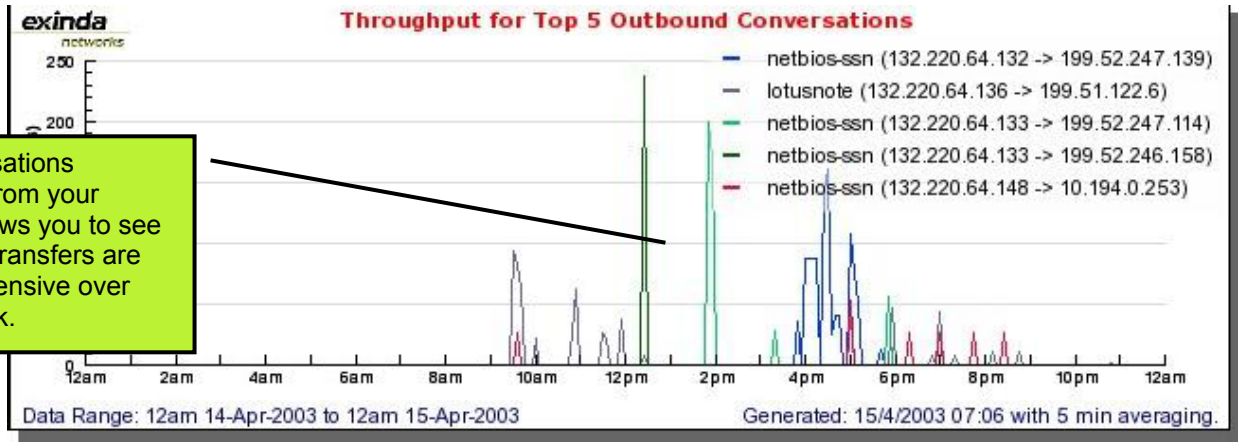
Traffic Throughput By Most Utilised Conversation

Data Range: 14/4/2003 to 15/4/2003

Top conversations originating from outside your network allows you to see which data transfers are the most intensive over your network.



Top conversations originating from your network allows you to see which data transfers are the most intensive over your network.

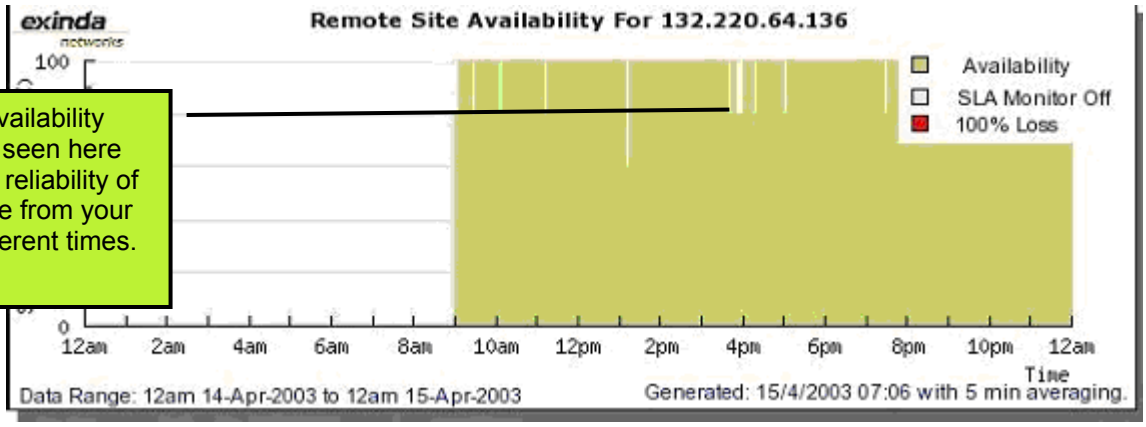


Here the top network conversations are presented according to whether or not they were initiated from your network. Conversations can be used to determine problems with large and extended data transfers between two hosts with the same application.

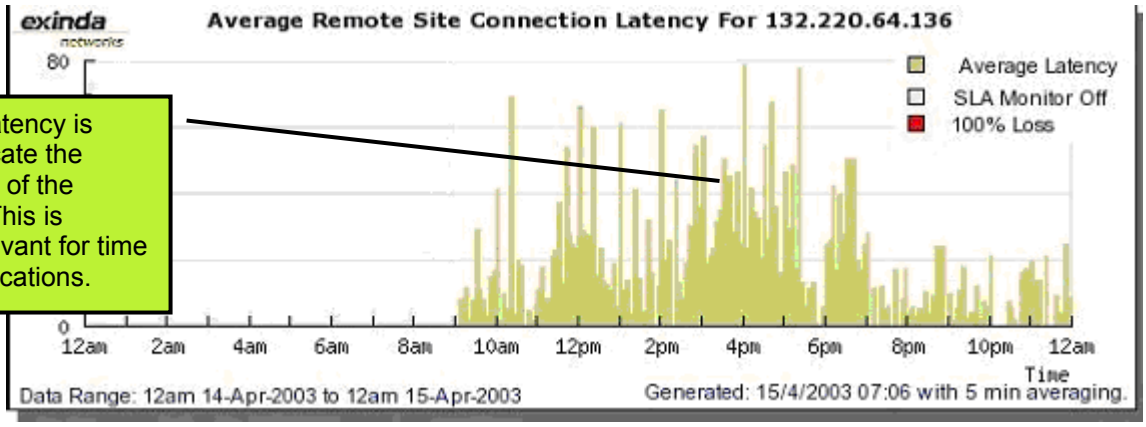
Remote SLA Measurements For 132.220.64.136

Data Range: 12am 14/4/2003 to 12am 15/4/2003

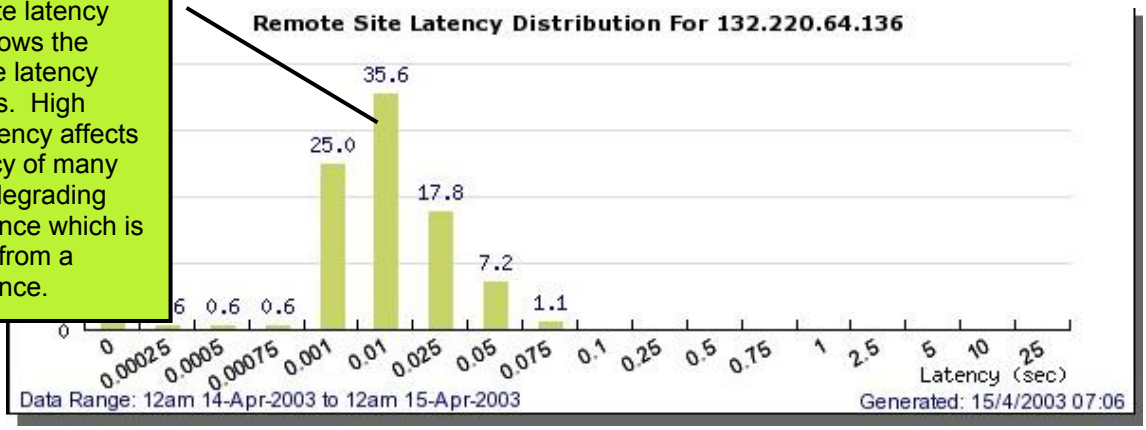
Remote site availability losses can be seen here to indicate the reliability of this remote site from your network at different times.



Remote site latency is shown to indicate the response time of the remote site. This is especially relevant for time sensitive applications.



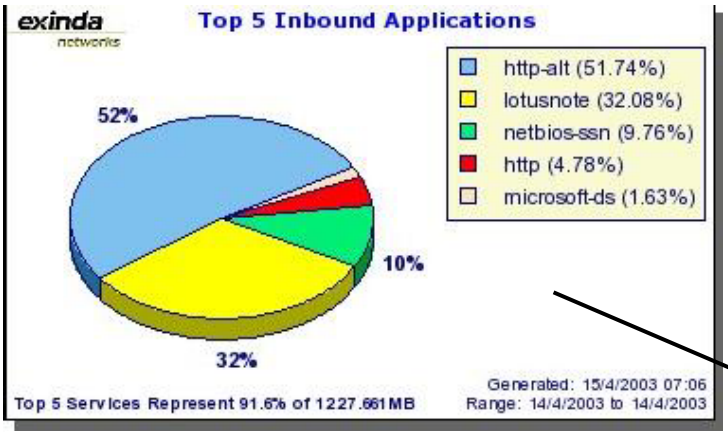
The remote site latency distribution shows the variation of the latency measurements. High variation in latency affects the consistency of many applications, degrading their performance which is unacceptable from a users' experience.

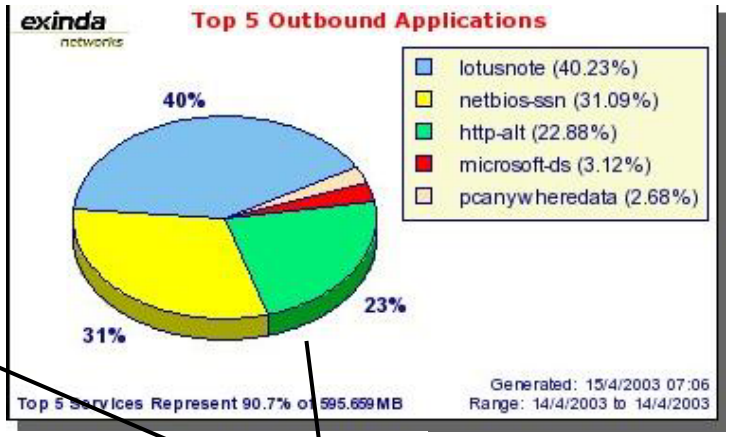


Remote site SLA verification is an essential part of the Exinda Monitor, allowing you to evaluate the accessibility, response and consistency of response of a host outside your network over time. This information enables you to see whether your communications link is allowing your network applications to function sufficiently outside your network.

Traffic Analysis - Top Applications/Services Summary

Data Range: 14/4/2003 to 14/4/2003





Top 30 Inbound Services

LAN ⟵ WAN

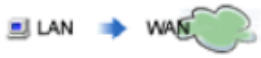
Service Name	Packets	Data (MB)	Throughput (Kbps)		
			Min	Avg	Max
http-alt (8080)	809003	581.847	0.03	**7.40**	425.66
lotusnote (1352)	455167	360.763	0.03	**11.04**	1775.50
netbios-ssn (139)	318798	109.780	0.03	**3.16**	805.95
http (80)	62063	53.732	0.03	**8.54**	486.71
microsoft-ds (445)	119224	18.352	0.03	**1.91**	30.66
printer (515)	8486	11.812	0.10	**72.86**	574.80
ft-role (2429)	41763	11.757	0.03	**1.31**	79.25
domain (53)	46377	10.818	0.03	**1.16**	118.96
unknown (4406 -> 1092)	6496	8.997	0.06	**48.71**	246.00
pcanywheredata (5631)	147507	7.073	0.04	**4.48**	44.86
https (443)	9068	4.740	0.03	**8.64**	174.62
unknown (1475 -> 2307)	5789	3.823	0.03	**5.12**	127.11
unknown (4406 -> 1088)	2475	3.401	0.03	**40.22**	218.40
unknown (4406 -> 1156)	2388	3.339	0.09	**49.96**	237.60
unknown (4406 -> 1964)	1850	2.363	0.04	**36.52**	187.20
virtual-places (1533)	17711	2.321	0.03	**1.03**	132.83
netbios-ns (137)	24161	1.915	0.06	**0.08**	3.12
unknown (4406 -> 1488)	1508	1.902	0.09	**33.03**	201.60
unknown (4406 -> 1996)	1289	1.773	0.03	**40.40**	219.60
unknown (4406 -> 1118)	1203	1.619	0.31	**66.33**	146.67
imgames (1077)	1725	1.352	0.03	**4.84**	74.03
ms-sql-s (1433)	12464	1.317	0.03	**1.87**	73.94
rmiregistry (1099)	1460	1.147	0.03	**5.67**	85.86
snmp (161)	8652	0.893	0.05	**0.09**	0.34

This view of the top applications allows you to see how the majority of your capacity is being used.

Statistics of how much data the top inbound applications have consumed help you pinpoint problems with capacity, security and productivity in your network. For example, this display will show if any unnecessary applications are consuming most of your network capacity.

exinda networks

Top 30 Outbound Services



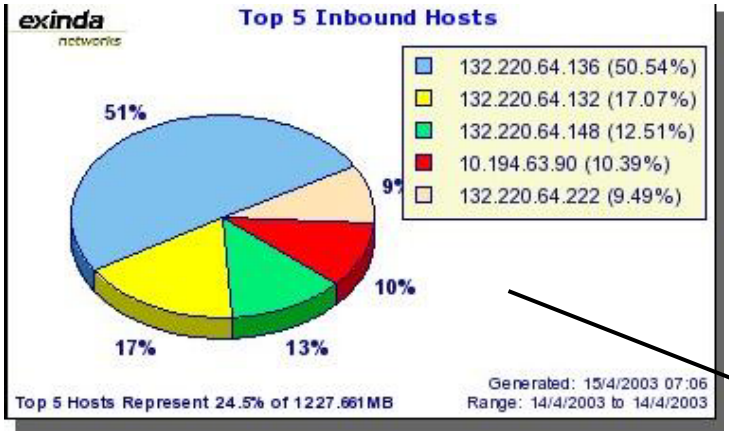
Service Name	Packets	Data (MB)	Throughput (Kbps)		
			Min	Avg	Max
lotusnote (1352)	436619	217.223	0.03	**4.90**	2289.39
netbios-ssn (139)	481698	167.859	0.03	**9.47**	1155.62
http-alt (8080)	687558	123.532	0.03	**1.25**	387.66
microsoft-ds (445)	106686	16.860	0.03	**1.79**	24.93
pcanywheredata (5631)	171280	14.493	0.03	**10.50**	148.83
http (80)	56234	9.186	0.03	**1.15**	17.96
ms-sql-s (1433)	13109	7.779	0.03	**1.69**	95.41
ft-role (2429)	42606	5.555	0.03	**0.63**	30.44
https (443)	8678	3.682	0.03	**5.14**	697.11
domain (53)	45321	2.951	0.03	**0.11**	2.03
netbios-ns (137)	25379	2.889	0.06	**0.12**	4.42
unknown (2248 -> 26184)	4027	1.947	0.23	**56.97**	118.88
unknown (36980 -> 1675)	1238	1.570	0.03	**28.11**	272.86
unknown (2251 -> 26184)	3213	1.564	0.12	**51.24**	141.87
unknown (2284 -> 26184)	2361	1.095	0.12	**27.18**	63.23
unknown (2287 -> 26184)	2443	1.068	0.23	**27.33**	116.55
virtual-places (1533)	17370	0.880	0.03	**0.33**	7.33
snmp (161)	8199	0.870	0.09	**0.09**	0.35
bootps (67)	2449	0.813	0.22	**0.41**	1.92
unknown (36730 -> 1040)	587	0.649	0.51	**24.30**	226.84
unknown (36960 -> 1127)	400	0.438	0.11	**27.61**	216.39
nerv (1222)	974	0.391	0.03	**1.51**	145.52

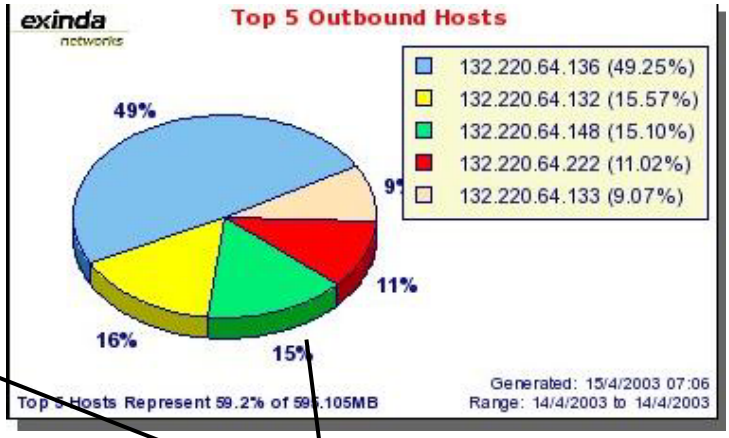
Statistics of how much data the top outbound applications have consumed help you pinpoint problems with capacity, security and productivity in your network.

This shows you which inbound and outbound applications are the most capacity intensive. This allows you to verify that your network capacity is being used in the most efficient manner possible. For example, this display will alert you of any unnecessary applications consuming the majority of your network capacity. Alternatively, you may find that malicious applications are operating on your network, exposing security vulnerabilities and costing you money. Information from this display can be used to formulate an optimization policy with Exinda Optimizer.

Traffic Analysis - Top Internal Hosts Summary

Data Range: 14/4/2003 to 14/4/2003





Top 30 Internal Hosts Receiving Inbound Traffic

LAN

Host Name	Host IP	Packets	Data (MB)	Throughput (Kbps)		
				Min	Avg	M
web03.acme.net	132.220.64.136	205879	151.954	0.03	**4.04**	1775
132.220.64.132	132.220.64.132	134787	51.327	0.02	**3.20**	805.95
payroll .acme.net	132.220.64.148	179352	37.609	0.03	**4.87**	79.62
10.194.63.90	10.194.63.90	23355	31.245	0.03	**29.95**	713.58
132.220.64.222	132.220.64.222	201963	28.546	0.02	**2.75**	78.24
10.194.63.41	10.194.63.41	56651	27.317	0.03	**1.70**	66.97
132.220.64.208	132.220.64.208	33122	27.011	0.03	**1.05**	254.18
132.220.64.210	132.220.64.210	32761	25.075	0.03	**1.27**	246.00
10.194.62.16	10.194.62.16	23491	23.158	0.03	**17.59**	595
10.194.63.33	10.194.63.33	36891	22.881	0.03	**2.94**	136
10.194.62.224	10.194.62.224	21056	22.432	0.03	**5.91**	243
132.220.64.206	132.220.64.206	33709	20.014	0.03	**0.85**	200
132.220.64.205	132.220.64.205	21042	19.106	0.03	**3.21**	639
10.194.62.195	10.194.62.195	16106	18.775	0.03	**43.60**	960
10.194.62.246	10.194.62.246	22710	17.547	0.03	**2.95**	320
10.194.62.23	10.194.62.23	22773	17.536	0.03	**2.84**	77
10.194.63.19	10.194.63.19	21380	17.455	0.03	**6.48**	492.11
web.acme.net	132.220.64.144	140745	16.858	0.02	**0.51**	8.64
132.220.64.203	132.220.64.203	20207	15.800	0.03	**1.83**	345.75
10.194.62.251	10.194.62.251	19586	15.126	0.03	**2.72**	287.89

This view of the top internal allows you to see how the majority of your capacity is being used.

Statistics of the hosts inside your network receiving data can help you determine which hosts are causing the most downlink congestion in your network.

exinda networks

Top 30 Internal Hosts Sending Outbound Traffic

LAN → WAN

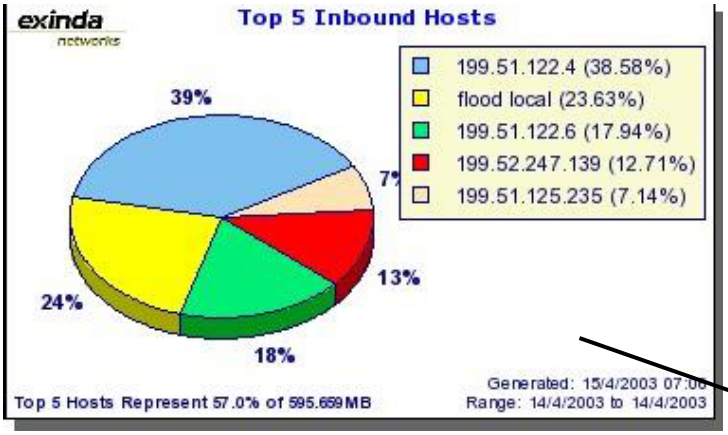
Host Name	Host IP	Packets	Data (MB)	Throughput (Kbps)		
				Min	Avg	Max
asiapac.th.acme.net	132.220.64.136	221044	173.508	0.03	**8.99**	2289.39
132.220.64.132	132.220.64.132	137192	54.833	0.03	**1.91**	977.87
netserver01. th.acme.net	132.220.64.148	163402	53.179	0.03	**33.14**	784.58
132.220.64.222	132.220.64.222	190491	38.810	0.03	**4.93**	141.87
132.220.64.133	132.220.64.133	65566	31.939	0.03	**3.42**	1155.62
sqldb. acme.net	132.220.64.135	21409	21.852	0.03	**24.88**	1147.40
ldap-03. acme.net	132.220.64.144	107009	12.327	0.03	**0.42**	43.45
10.194.60.4	10.194.60.4	82161	8.156	0.03	**1.33**	148.83
132.220.64.138	132.220.64.138	10214	8.113	0.03	**33.19**	361.82
132.220.64.130	132.220.64.130	69339	7.588	0.03	**9.57**	272.86
132.220.64.206	132.220.64.206	32417	5.997	0.03	**0.33**	58.
10.194.63.33	10.194.63.33	32767	5.880	0.03	**1.03**	43.
132.220.64.223	132.220.64.223	8692	5.189	0.03	**6.84**	615.
132.220.64.210	132.220.64.210	27820	5.008	0.03	**0.24**	35.
10.194.63.41	10.194.63.41	57507	4.358	0.03	**0.63**	11.
10.194.62.249	10.194.62.249	9551	4.304	0.03	**1.25**	103
132.220.64.208	132.220.64.208	26358	4.224	0.03	**0.23**	15
10.194.62.74	10.194.62.74	15091	3.812	0.03	**0.81**	27.
zeus-01. acme.net	132.220.64.143	33506	3.790	0.03	**0.17**	19.78
10.194.63.19	10.194.63.19	17247	3.673	0.03	**0.58**	387.66

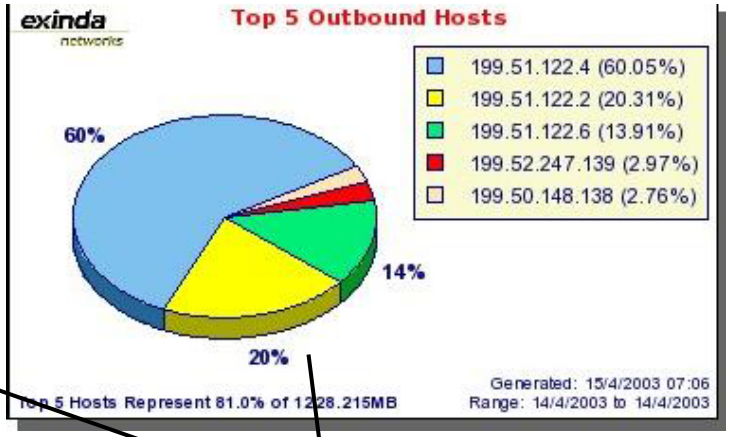
Statistics of the hosts inside your network sending data can help you determine which hosts are causing the most uplink congestion in your network.

This page shows you which hosts inside your network are causing the most uplink and downlink congestion in your network. This information can be used to formulate an optimization policy with your Exinda Optimizer.

Traffic Analysis - Top External Hosts Summary

Data Range: 14/4/2003 to 14/4/2003





Top 30 External Hosts Receiving Inbound Traffic

LAN → WAN

Host Name	Host IP	Packets	Data (MB)	Throughput (Kbps)		
				Min	Avg	M
proxy. acme.net	199.51.122.4	712604	131.026	0.03	**1.24**	400
flooding to local hosts	flood local	40539	80.233	0.06	**13.55**	228
phoeb-01. acme.net	199.51.122.6	140878	60.922	0.03	**2.91**	1233.88
199.52.247.139	199.52.247.139	60194	43.173	0.03	**40.54**	977.87
199.51.125.235	199.51.125.235	186602	24.246	0.03	**2.01**	95.41
mail02 acme.net	199.51.122.2	199011	24.116	0.03	**1.58**	580
199.51.122.58	199.51.122.58	148625	20.870	0.03	**0.32**	117
199.52.247.114	199.52.247.114	27045	20.030	0.03	**53.46**	993
mail04 acme.net	199.51.122.57	44481	17.366	0.03	**1.95**	46.
10.194.0.253	10.194.0.253	11702	13.845	0.03	**63.52**	784
199.51.122.10	199.51.122.10	58283	13.402	0.03	**11.34**	697
199.51.122.38	199.51.122.38	49466	11.344	0.03	**2.21**	141
199.51.125.118	199.51.125.118	81782	9.565	0.03	**0.80**	56
199.52.246.158	199.52.246.158	14779	8.701	0.03	**19.80**	115
199.52.247.112	199.52.247.112	43892	7.776	0.03	**12.22**	211.75
199.52.246.65	199.52.246.65	8094	7.664	0.03	**21.74**	693.19
199.52.246.112	199.52.246.112	10789	7.511	0.03	**29.91**	377.00
199.52.246.179	199.52.246.179	54239	7.221	0.03	**1.03**	35.41
199.51.122.253	199.51.122.253	4600	5.384	0.04	**35.26**	638.04
132.220.67.124	132.220.67.124	4008	4.361	0.04	**15.03**	89.47

This view of the top external hosts shows you where data transmitted from your network is going.

Statistics of the hosts outside your network receiving data shows you the external hosts that are most contacted by your network.

Top 30 External Hosts Sending Outbound Traffic

exinda networks

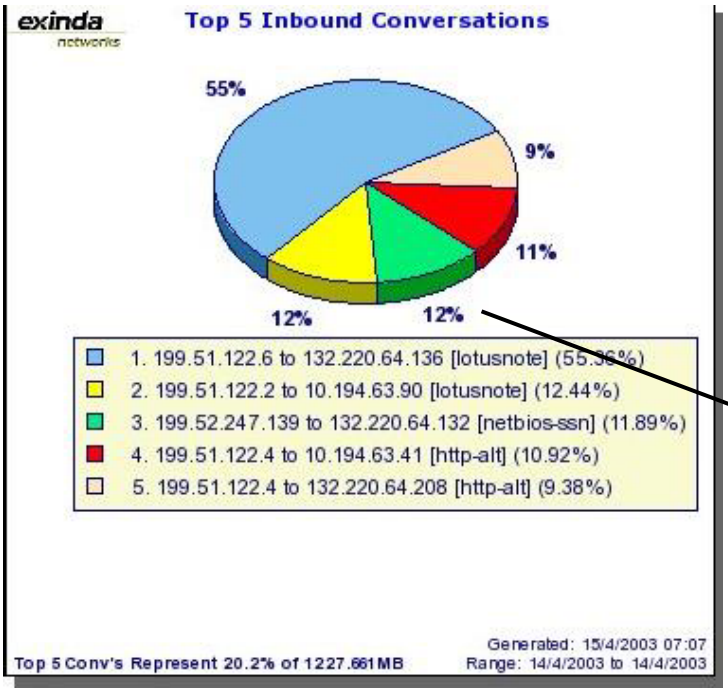
Host Name	Host IP	Packets	Data (MB)	Throughput (Kbps)		
				Min	Avg	Max
proxy.acme.net	199.51.122.4	836485	597.428	0.03	**5.29**	425.66
mail02.acme.net	199.51.122.2	237557	202.050	0.03	**13.74**	1218.13
phoeb-01. acme.net	199.51.122.6	162266	138.395	0.03	**8.36**	1775.50
199.52.247.139	199.52.247.139	55461	29.514	0.03	**20.27**	805.95
199.50.148.138	199.50.148.138	34819	27.448	0.03	**0.77**	246.00
199.51.122.58	199.51.122.58	147997	26.218	0.03	**0.57**	249.43
199.51.122.38	199.51.122.38	50835	19.923	0.03	**8.84**	574.80
199.51.125.235	199.51.125.235	180414	19.844	0.02	**1.49**	
web.acme.net	199.51.122.57	64326	18.658	0.03	**2.03**	
ldap. acme.net	199.51.122.60	14338	18.461	0.03	**30.06**	
199.51.125.118	199.51.125.118	110408	12.924	0.02	**0.49**	
199.50.20.218	199.50.20.218	12608	11.219	0.03	**6.87**	
geosystemb.acme.net	164.57.152.195	12068	9.011	0.03	**5.74**	
199.52.246.179	199.52.246.179	62372	8.457	0.02	**1.03**	
199.50.20.80	199.50.20.80	7743	5.906	0.03	**5.62**	
199.52.134.26	199.52.134.26	8480	5.861	0.03	**3.68**	
doncaster.acme.net	199.51.101.217	3776	4.889	0.04	**17.58**	66.47
199.52.247.132	199.52.247.132	3955	4.212	0.03	**13.87**	1216.74
199.52.247.112	199.52.247.112	40638	3.865	0.02	**3.44**	852.18
199.50.9.70	199.50.9.70	2765	3.214	0.04	**20.47**	174.62

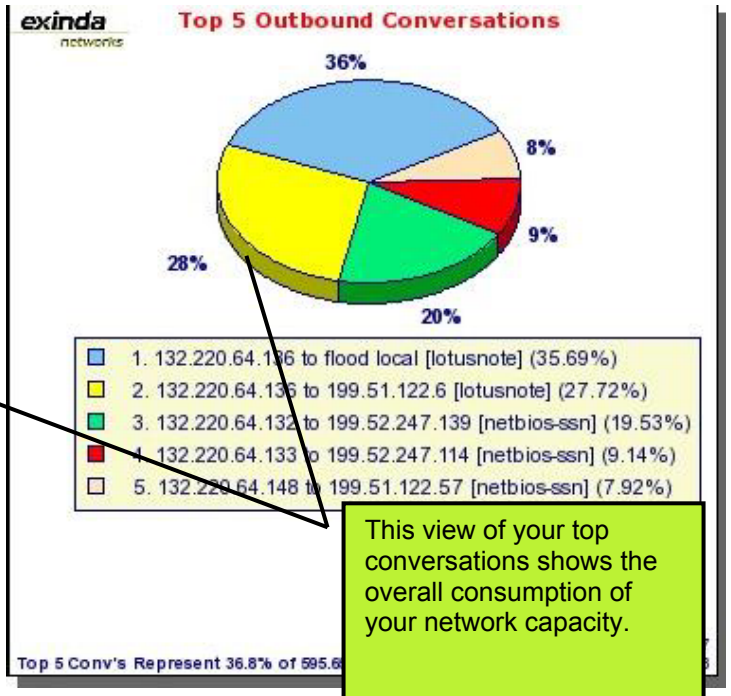
Statistics of the hosts outside your network sending data shows you the external hosts that are contacting your network most frequently.

This page shows the external hosts that are receiving the most data from your network as well as the hosts that are contacting your network most frequently. These external sites are typically the source of most of your unnecessary network congestion and are a major cause of security vulnerabilities.

Traffic Analysis - Top Conversations Summary

Data Range: 14/4/2003 to 14/4/2003





This view of your top conversations shows the overall consumption of your network capacity.

Top 30 Inbound Conversations

LAN ← WAN

Source Host	Destination Host	Service	Sessions	Data Size (MB)	Transfer Rate (Kbps)		
					Min	Avg	Max
199.51.122.6	132.220.64.136	lotusnote (1352)	1724	137.349	0.04	**26.07**	366.73
199.51.122.2	10.194.63.90	lotusnote (1352)	2	30.870	0.06	**74.02**	713.58
199.52.247.139	132.220.64.132	netbios-ssn (139)	0	29.503	0.16	**40.33**	6.65
199.51.122.4	10.194.63.41	http-alt (8080)	1483	27.103	0.10	**4.81**	0.65
199.51.122.4	132.220.64.208	http-alt (8080)	1431	23.286	0.03	**6.14**	22.81
199.51.122.4	10.194.63.33	http-alt (8080)	2932	22.548	0.04	**5.40**	72.68
199.51.122.4	10.194.62.224	http-alt (8080)	291	22.312	0.21	**17.72**	6
199.51.122.57	132.220.64.148	netbios-ssn (139)	0	18.653	0.48	**3.84**	5
199.51.122.4	132.220.64.206	http-alt (8080)	2819	17.965	0.03	**7.57**	7
199.51.122.58	132.220.64.148	netbios-ssn (139)	0	17.453	0.68	**13.67**	7
199.51.122.4	10.194.62.23	http-alt (8080)	100	17.286	0.03	**17.30**	
199.51.122.2	10.194.62.195		1	15.635	197.35	**494.94**	884.64

The top inbound conversations show data traffic that originates from an external host and is coming into your network.

Top 30 Outbound Conversations

LAN → WAN

Source Host	Destination Host	Service	Sessions	Data Size (MB)	Transfer Rate (Kbps)		
					Min	Avg	Max
132.220.64.136	flood local	lotusnote (1352)	71	78.223	1.94	**213.39**	1670.62
132.220.64.136	199.51.122.6	lotusnote (1352)	2830	60.747	0.16	**8.46**	469.08
132.220.64.132	199.52.247.139	netbios-ssn (139)	5	42.811	0.03	**49.09**	6.16
132.220.64.133	199.52.247.114	netbios-ssn (139)	1	20.030	0.18	**62.36**	776.37
132.220.64.148	199.51.122.57	netbios-ssn (139)	2	17.363	0.43	**3.58**	46.24
132.220.64.148	199.51.122.58	netbios-ssn (139)	5	16.376	0.72	**12.41**	
132.220.64.222	199.51.125.235	microsoft-ds (445)	8	11.575	1.56	**5.90**	
132.220.64.133	199.52.246.158	netbios-ssn (139)	1	8.701	0.03	**19.80**	
132.220.64.148	10.194.0.253	netbios-ssn (139)	17	7.760	0.29	**144.37**	
132.220.64.148	199.52.246.112	netbios-ssn (139)	5	7.494	0.19	**103.95**	377.00
132.220.64.136	199.52.246.65	lotusnote (1352)	2	7.292	12.13	**57.98**	405.52
132.220.64.144	199.51.125.118	netbios-ssn (139)	9149	6.716	0.03	**0.48**	0.66
132.220.64.138	10.194.0.253	netbios-ssn (139)	17	6.077	0.29	**114.87**	178.60
10.194.63.33	199.51.122.4	http-alt (8080)	0	5.787	0.03	**1.26**	12.17
132.220.64.206	199.51.122.4	http-alt (8080)	0	5.513	0.03	**1.36**	6.35
132.220.64.223	199.51.122.10	netbios-ssn (139)	1	5.184	0.10	**23.64**	615.81

The top inbound conversations show data traffic that originates from your network and is being sent to an external host.

Top Conversations allow you to see the composition of your network traffic over extended periods in and out of your network. To ensure network efficiency, unnecessary network conversations should be blocked from your network (or de-prioritised) using an appropriate Exinda Optimizer policy.

Definition Reference

Adobe Portable Documents: The Adobe Portable Document Format (pdf) is a type of document that is used extensively due to their small document size. In order to view portable documents, you must install Adobe Acrobat Reader on your computer. This software can be downloaded free of charge from the internet (*http://www.adobe.com/products/acrobat/readstep2.html*)

Application: A network application is a type of data that is sent over a network to support applications such as file sharing and web browsing.

Conversation: A network conversation is a transaction of data that occurs between two hosts using the same application.

Capacity (Network): Network capacity – sometimes called bandwidth – is the raw amount of data that your network can transmit in a specified time period. Simply, network capacity is the speed of your network link.

Host: Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services, such as SMTP (email) and HTTP (web).

Inbound/Outbound Traffic: Inbound traffic is data that is transmitted into your internal network from external hosts, outbound traffic is data that is transmitted from your internal network.

Internal/External Host: Hosts are either internal or external depending on whether or not they are part of your private network (Internal).

ISP (Internet Service Provider): An institution that provides access to the Internet in some form, usually on a commercial basis.

Latency: Latency is the time it takes for a message to travel from your network to a remote host. Latency is an important way of measuring the efficiency of a network link for network applications.

Latency Distribution: Latency distributions are important to determine the consistency of a network link. Many network applications are intolerant of variations in latency, and so require a low distribution of latency.

Network Interface: The point between your Exinda Optimizer and the network. Typically, each Exinda Optimizer is packaged with two network interfaces: one for your internal network, and one for your external network.

SLA (Service Level Agreement): An agreement between a company and an ISP to deliver a particular Internet access service level.

Subnet: A group of hosts in a network that are assigned similar network (IP) addresses.

Throughput: The rate at which data is transmitted over your network.