

Note: Some information has been replaced by [REDACTED]
To hide the information of the particular customer, for the purpose of this sample report

Company X Network Audit

Summary

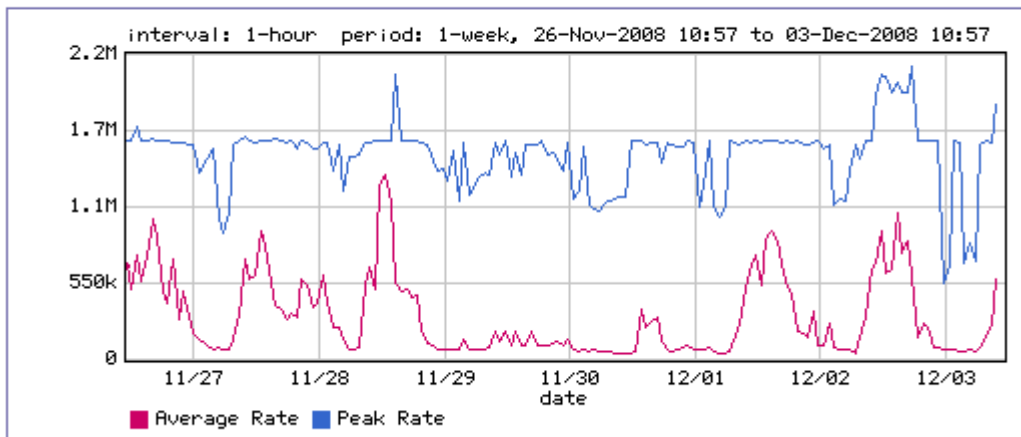
The link as a whole is being utilised within acceptable levels. There is some demand on the outbound link; however this demand falls out of business hours and can be attributed to some form of backup / DR services. Overall the line is capable of handling the volume of traffic that traverses the link with very little degradation to the network efficiency. There are some discovered ports / services running on the link which if unknown to Company X, should be investigated, otherwise the link can be described as non-problematic.

Computrad have also identified and listed within this report, several nodes that are web browsing via by-passing the **lonprox03** web proxy.

Company X Inbound Link Utilisation Summary

Fig 1: Inbound Link Utilisation - 26th November to the 3rd December 2008

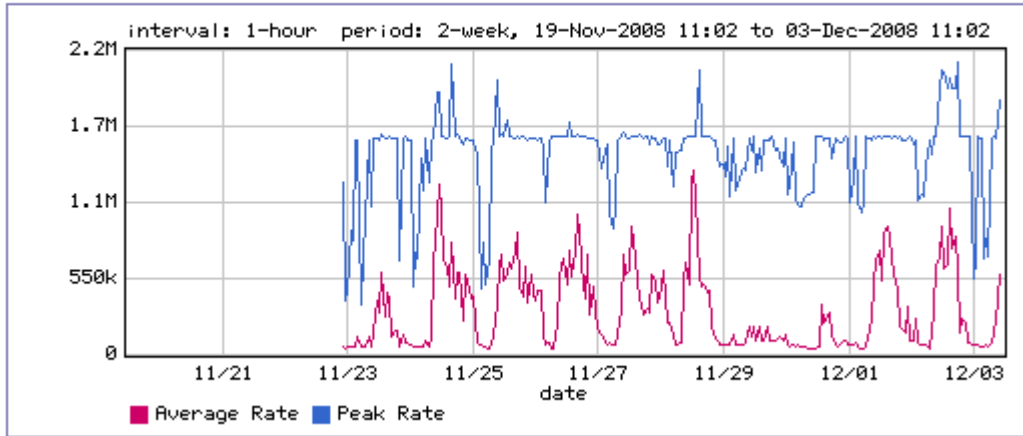
Utilization



The above graph shows the inbound link utilisation between the 26th November and the 3rd of December, a total of 1 week. The graph indicates the link is being utilised within acceptable parameters, this is indicated by the average and peak rates, the greater the distance between the two, the better the link is being utilised. As you can see, the weekend exhibits minimal traffic with the evening traffic exhibiting the same pattern. It should be noted that peak rate in this period is just traffic utilising a virtually unused pipe.

Fig 2: Inbound Link Utilisation - 19th November to 3rd December 2008

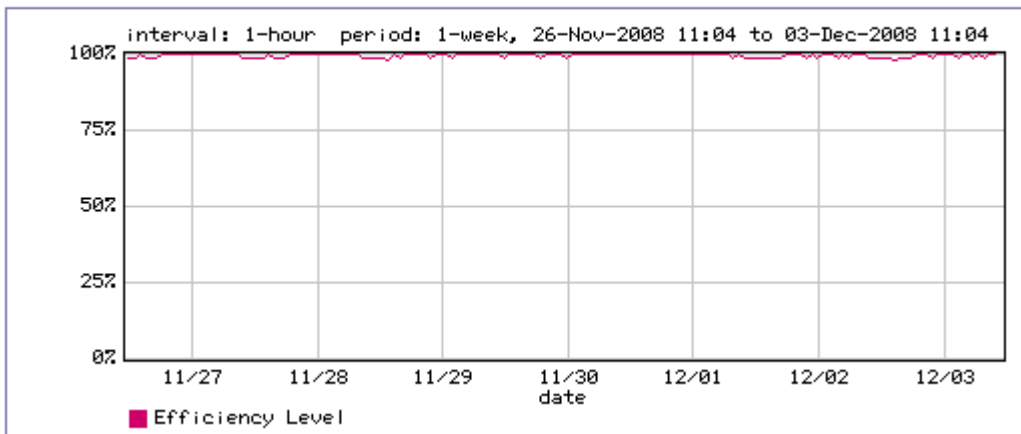
Utilization



The above graph is a reflection of the first graph but at a greater duration (19th November to 3rd December – From the unit inception). – Again, the distance between the average rate and peak rate effectively shows that the pipe is well capable in handling the volume of traffic traversing the link.

Fig 3: Inbound Link Network Efficiency – 26th November to 3rd December 2008

Network Efficiency

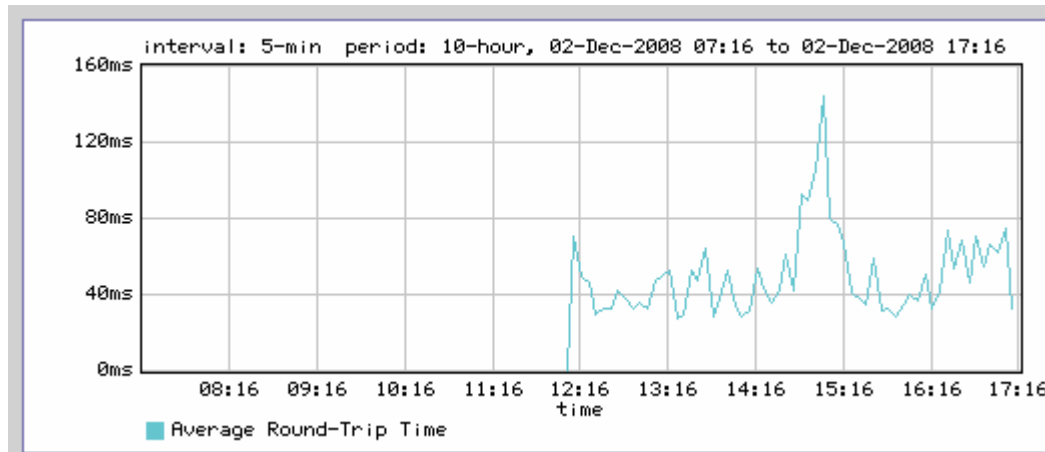


The network efficiency for the same period (1 week) is also indicative of a non problematic link.

(Network efficiency is around 98% peak time and 99-100% off peak time).

Drilling down slightly further, the busiest node on the link would be **lonprox03**. Below we can see the average round trip for a typical packet from this node.

Fig 3a: Inbound Link Round Trip (Latency) – Lonprox03, 2nd December 2008



The latency between Company X and its destination is on average 40ms which is considered to be good.

Below is a snapshot of Citrix ICA traffic in the same 1-week period. We can see that the demand for Citrix is roughly 75k – 300k.

Fig 4: Citrix Inbound Link utilisation – 26th November to 3rd December 2008

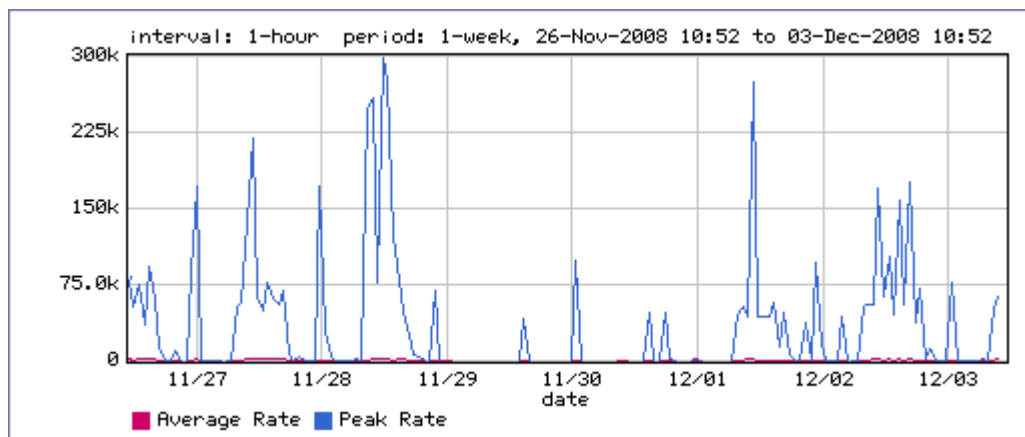
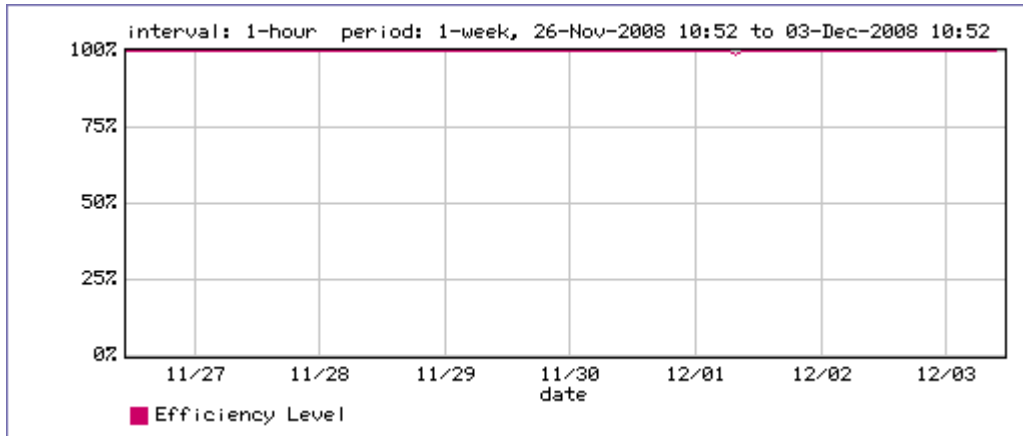


Fig 5: Citrix Inbound Network Efficiency – 26th November to 3rd December 2008

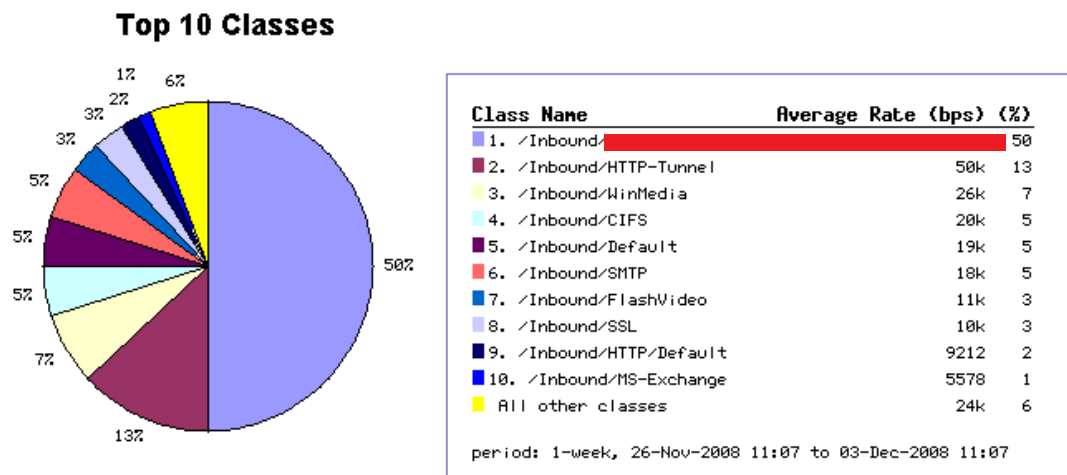


The network efficiency graph shows that for the same 1 week period, Citrix was able to use the pipe at 100% network efficiency!

Given the statistics, we can conclusively state that the inbound link utilisation is within acceptable levels.

Below is a brief overview of the type of traffic that has traversed the link within the same 1 week period.

Fig 6: Inbound Top 10 Traffic Classes – 26th November to 3rd December 2008



It can be noted that 50% of the inbound traffic is generated by lonprox03, web proxy. It should also be noted that a small number of nodes were observed by-passing the web proxy, generating http traffic.

A list of nodes has been identified below:-

Tuesday 2nd December 2008

Fig 7: List of nodes by-passing the Web Proxy and generating HTTP traffic – 2/12/08

Top receiving IP hosts in class /Inbound/HTTP

© Top Listeners Time analyzed: 00:01:55

	DNS Name	IP Address	Usage	
1	[REDACTED]	10.77.3.64	58%	classify ...
2	[REDACTED]	10.77.2.75	37%	classify ...
3	[REDACTED]	10.77.2.43	2%	classify ...
4	[REDACTED]	10.77.3.65	2%	classify ...
5	[REDACTED]	10.77.32.51	<1%	classify ...
6	[REDACTED]	10.77.32.68	<1%	classify ...
7	[REDACTED]	10.77.32.79	<1%	classify ...

Wednesday 3rd December 2008

Fig 8: List of nodes by-passing the Web Proxy and generating HTTP traffic – 3/12/08

© Top Listeners Time analyzed: 15:56:44

	DNS Name	IP Address	Usage	
1	[REDACTED]	10.77.2.75	15%	classify ...
2	[REDACTED]	10.77.3.69	11%	classify ...
3	[REDACTED]	10.77.2.31	10%	classify ...
4	[REDACTED]	10.77.3.45	10%	classify ...
5	[REDACTED]	10.77.3.65	10%	classify ...
6	[REDACTED]	10.77.3.78	10%	classify ...
7	[REDACTED]	10.77.2.38	4%	classify ...
8	[REDACTED]	10.77.3.51	3%	classify ...
9	[REDACTED]	10.77.2.58	2%	classify ...
10	[REDACTED]	10.77.2.61	2%	classify ...

The following node was observed as the top talker for some the http traffic identified.

Fig 9: List of nodes by-passing the Web Proxy and generating HTTP traffic – Top Talkers.

Top sending IP hosts in class /Inbound/HTTP

 **Top Talkers**


Time analyzed: 00:00:55

	DNS Name	IP Address	Usage	
1	[REDACTED]	10.8.20.45	97%	classify ...
2	[REDACTED]	10.4.30.77	2%	classify ...

lonsms101 was being utilised solely by the following node;

Fig 10: Top listener for lonsms01, identified as generating http traffic.

Top receiving IP hosts in class /Inbound/HTTP/lonsms01.corp.nortonro

 **Top Listeners** Time analyzed: 00:06:21

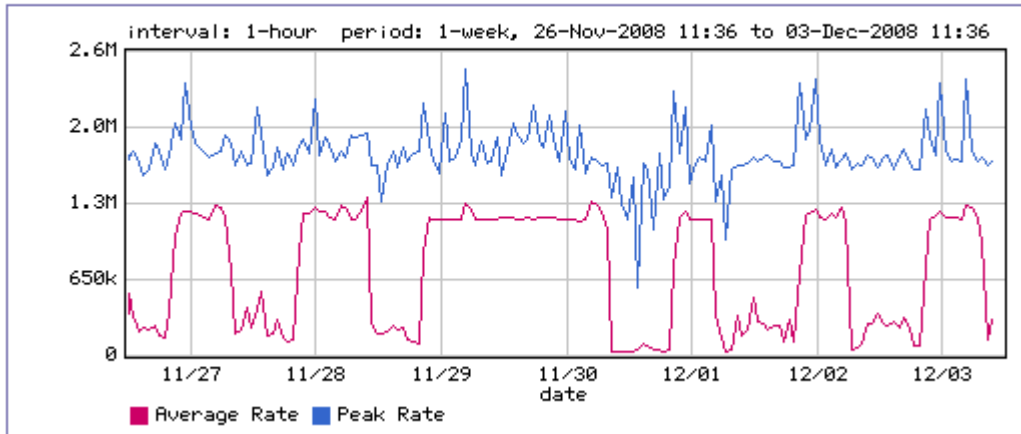
	DNS Name	IP Address	Usage	
1	[REDACTED]	10.77.2.55	100%	classify ...

Company X may want to investigate the legitimacy of these nodes and whether these nodes should indeed be going via **lonprox03** or indeed by-passing the proxy altogether.

Company X Outbound Link Utilisation Summary

Fig 11: Outbound Link Utilisation - 26th November to the 3rd December 2008

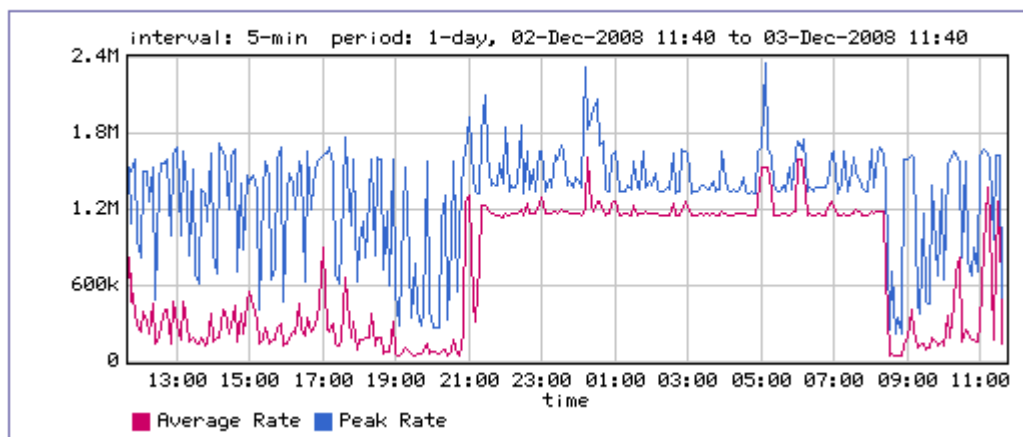
Utilization



The outbound link utilisation appears to be in more demand than the inbound utilisation. The link on average is at a flat rate of 1.3M, this equates to more than half the pipe. However this only appears to be the case out of business hours, more specifically, evenings and weekends. The high volume of traffic observed does not bleed over into production hours and therefore is not affecting the behaviour of business hour traffic and business critical applications whatsoever.

Fig 12: Outbound Link Utilisation – 2nd December to 3rd December 2008

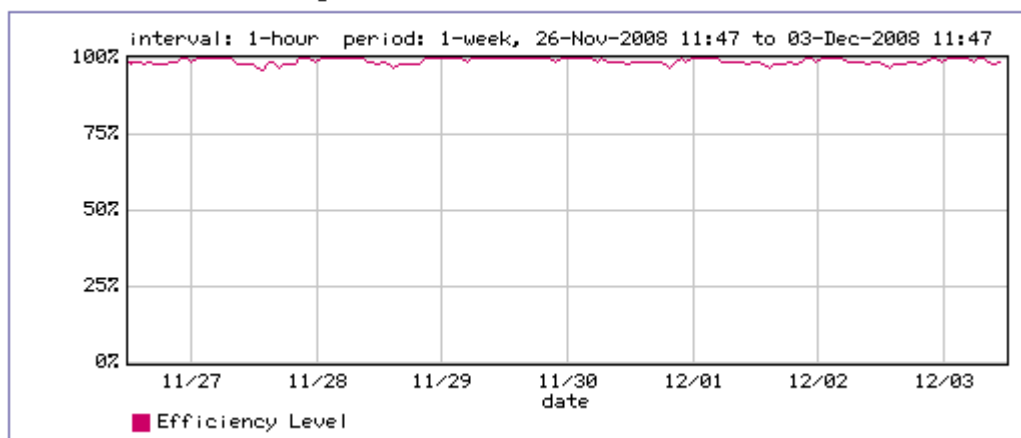
Utilization



An observation can be made that during business hours the line is within acceptable usage levels. The out of hours traffic indicates some form of services / backup / DR being performed across the link, this seem to occur daily between the hours of 9pm and 7am and throughout the weekend. Given the nature and behaviour of the flow of traffic, we can safely assume that the traffic is legitimate.

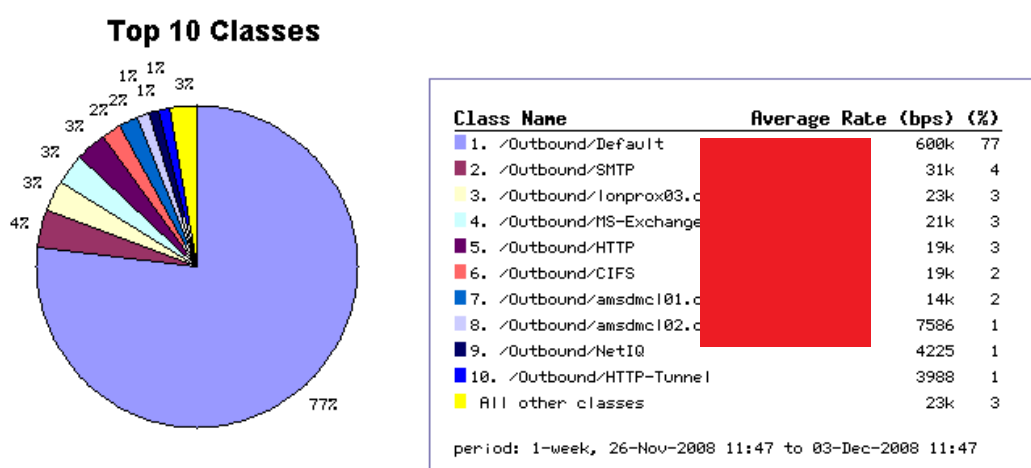
Fig 13: Outbound Link Network Efficiency – 26th November to 3rd December 2008

Network Efficiency



Even with the high level of traffic traversing this link out of hours, we are getting a reasonable level of network efficiency, with the worst case being a slight drop to around 95% efficiency. If we drill down further, we can see that the bulk of business hour traffic is SMTP. SMTP can operate smoothly with low level of network efficiency given it's connectionless vs. connection-orientated nature. The efficiency can be tweaked to an extent should Company X decide to adopt time sensitive application across it link, such as video conferencing or VoIP, but currently the current level of efficiency is above the acceptable level. It should also be noted that no VoIP / Video & Bill Back traffic have been observed traversing the link.

Fig 14: Outbound Top 10 Traffic Classes – 26th November to 3rd December 2008



Top 10 class of traffic in this 1 week period shows 77% being default or 'unclassified' traffic. This would make sense given that majority of the traffic is observed out of hours and it is reasonable to assume they are custom / unclassified traffic unique to Company X.

Unfortunately the unclassified traffic that is traversing the link out of hours can not be classified unless real-time out of hour monitoring is conducted. However, as stated before, given the behaviour of this traffic, it is safe to assume that this is indeed legitimate out of hour traffic.

A break down of the business hour traffic will be documented in the next section of this report

Business hour inbound link utilisation

It has already been identified that the actual total inbound link utilisation is within acceptable levels. The following will look at the various snap shots taken throughout the 2 day live monitoring and summarise (refer to appendix for snapshots for actual traffic-by-traffic analysis). It would appear that **lonprox03** accounts for most of the traffic. This makes sense given that it is the central node for all user web connections.

SMTP and CIFS are also accounted for, though their link utilisation is around 20%.

It should also be noted that a discovered port, 1398, is also utilising the link.

The discovered port is originating from the following source;

🔍 Top Listeners				Time analyzed: 00:11:55
	DNS Name	IP Address	Usage	
1	[REDACTED]	10.4.30.211	100%	classify ...

The following list a few nodes that the above source is communicating with;

🔍 Top Talkers				Time analyzed: 00:11:22
	DNS Name	IP Address	Usage	
1	[REDACTED]	10.77.2.69	12%	classify ...
2	[REDACTED]	10.77.2.36	10%	classify ...
3	[REDACTED]	10.77.3.44	8%	classify ...
4	[REDACTED]	10.77.3.50	7%	classify ...
5	[REDACTED]	10.77.2.39	7%	classify ...

It is recommended for Company X to identify **loncl08in02** to determine its legitimacy. Though it does not affect the total inbound link utilisation, it is recognised as a port and not as a class of traffic. Generally this type of classification should always be investigated if unknown.

Business hour outbound link utilisation

SMTP and **lonprox03** accounts for most of the traffic within business hours, both of which are legitimate and business critical traffic classes.

A discovered port, 1935, has also been identified as utilising the link.

The following has been identified as the source:

Fig 15: Discovered port 1935 – Top Talkers

	DNS Name	IP Address	Usage	
1	a92-122-210-165.deploy.akamaitechnologies.com	92.122.210.165	100%	classify ...

However the source has been observed changing from time to time

🔍 Top Talkers Time analyzed: 02:00:04

	DNS Name	IP Address	Usage	
1	vmfs1.asg.xpc-mii.net	64.191.209.124	100%	classify ...
2	a92-122-210-165.deploy.akamaitechnologies.com	92.122.210.165	<1%	classify ...

🔍 Top Talkers Time analyzed: 02:58:52

	DNS Name	IP Address	Usage	
1	vmfs1.asg.xpc-mii.net	64.191.209.124	67%	classify ...
2	No such name	81.23.251.90	32%	classify ...
3	a92-122-210-165.deploy.akamaitechnologies.com	92.122.210.165	<1%	classify ...

Some of the top listeners have been identified as:

Fig 16: Discovered port 1935 – Top Listeners

👁 Top Listeners Time analyzed: 03:46:53

	DNS Name	IP Address	Usage	
1		10.77.2.62	55%	classify ...
2		10.77.2.59	44%	classify ...
3		10.77.2.69	<1%	classify ...

It is recommended for Company X to identify some of the source to determine its legitimacy. Though it does not affect the total outbound link utilisation, it is recognised as a port and not as a class of traffic. Generally this type of classification should always be investigated if unknown.





















Appendix - Various Snap shots


Top 10 – Average rate

Tuesday 2nd December 2008, 12pm

Inbound Link Utilization: 30800%

Total Bytes Received: 283.9M























 Average Rate	Average Rate (bps)	% of Total
 lonprox03	475k	75% 
 SMTP	67.7k	11% 
 HTTP	29.2k	5% 
 CIFS	13.8k	2% 
 MS-Exchange	11.2k	2% 
 DiscoveredPorts/TCP_Port_1935	9227	1% 
 Default	7150	1% 
 DCOM	7119	1% 
 DiscoveredPorts/TCP_Port_1398	2660	0%
 DiscoveredPorts/TCP_Port_2418	1679	0%
All other classes	6891	1% 

click on the  icon to see a performance graph for the class

Outbound

Outbound Link Utilization: 14077%

Total Bytes Sent: 129.7M























 Average Rate	Average Rate (bps)	% of Total
 SMTP	92.1k	32% 
 lonprox03.corp.	70.0k	24% 
 MS-Exchange	37.7k	13% 
 Default	31.0k	11% 
 HTTP	16.2k	6% 
 amsdmcl01	10.9k	4% 
 CIFS	10.9k	4% 
 DiscoveredPorts/TCP_Port_1398	3567	1% 
 amsdms01.corp.companyxro	3069	1% 
 Localhost	2606	1% 
All other classes	10.7k	4% 


Top 10 – Peak Rate

Tuesday 2nd December 2008, 12pm

Inbound Link Utilization: 33692%

Total Bytes Received: 310.5M























 Peak Rate	Peak Rate (bps)	% of Total
 SMTP	1.5M	15% 
 Ionprox03.	1.5M	15% 
 DiscoveredPorts/TCP_Port_1935	1.5M	15% 
 Default	1.3M	13% 
 DCOM	1.3M	13% 
 HTTP	1.2M	12% 
 Localhost	614k	6% 
 MS-ActiveDir	434k	4% 
 CIFS	249k	2% 
 MS-Exchange	159k	2% 
All other classes	316k	3% 

click on the  icon to see a performance graph for the class

Outbound

Outbound Link Utilization: 12697%

Total Bytes Sent: 117.0M





















 Peak Rate	Peak Rate (bps)	% of Total
 SMTP	1.6M	18% 
 Default	1.5M	17% 
 amsdmcl01	1.5M	17% 
 MS-Exchange	911k	10% 
 LDAP	910k	10% 
 Ionprox03.corp.	523k	6% 
 Localhost	504k	6% 
 HTTP	355k	4% 
 SOAP-HTTP	312k	4% 
 DCOM	264k	3% 
All other classes	483k	5% 


Top 10 – Total Bytes

Tuesday 2nd December 2008, 12pm

Inbound Link Utilization: 33519%

Total Bytes Received: 308.9M























 Total Bytes	Total Bytes	% of Total
 lonprox03.	193.0M	62% 
 DiscoveredPorts/TCP_Port_1935	50.2M	16% 
 SMTP	29.4M	10% 
 HTTP	13.6M	4% 
 CIFS	6.3M	2% 
 MS-Exchange	4.6M	1% 
 Default	3.5M	1% 
 DCOM	3.2M	1% 
 DiscoveredPorts/TCP_Port_1398	1.2M	0%
 DiscoveredPorts/TCP_Port_2418	738k	0%
All other classes	3.4M	1% 


click on the  icon to see a performance graph for the class

Outbound

Outbound Link Utilization: 12508%

Total Bytes Sent: 115.3M

 Total Bytes	Total Bytes	% of Total
 SMTP	32.5M	28% 
 lonprox03	27.8M	24% 
 MS-Exchange	16.0M	14% 
 Default	10.5M	9% 
 HTTP	6.9M	6% 
 CIFS	4.9M	4% 
 amsdmcl01.	4.9M	4% 
 Localhost	2.5M	2% 
 DiscoveredPorts/TCP_Port_1935	1.7M	1% 
 DiscoveredPorts/TCP_Port_1398	1.6M	1% 
All other classes	6.1M	5% 

click on the  icon to see a performance graph for the class

Outbound Default Traffic – Top Talkers and Top Listeners

Tuesday 2nd December 2008, 12pm

🔍 Top Talkers

Time analyzed: 03:07:31

	DNS Name	IP Address	Usage	
1	[REDACTED]	10.77.32.70	95%	classify ...
2	[REDACTED]	10.77.32.90	2%	classify ...
3	[REDACTED]	10.77.32.53	<1%	classify ...
4	[REDACTED]	10.77.2.39	<1%	classify ...
5	[REDACTED]	10.77.32.66	<1%	classify ...

👂 Top Listeners

Time analyzed: 03:07:51

	DNS Name	IP Address	Usage	
1	[REDACTED]	10.8.79.46	50%	classify ...
2	[REDACTED]	10.8.79.157	25%	classify ...
3	[REDACTED]	10.8.79.83	11%	classify ...
4	[REDACTED]	10.8.78.97	9%	classify ...
5	[REDACTED]	10.4.35.23	2%	classify ...

Tuesday 2nd December 2008, 1pm

 **Top Talkers**

Time analyzed: 02:58:43

	DNS Name	IP Address	Usage	
1	[REDACTED]	10.77.32.70	93%	classify ...
2	[REDACTED]	10.77.32.90	2%	classify ...
3	[REDACTED]	10.77.32.53	<1%	classify ...
4	[REDACTED]	10.77.32.66	<1%	classify ...
5	[REDACTED]	10.77.2.39	<1%	classify ...

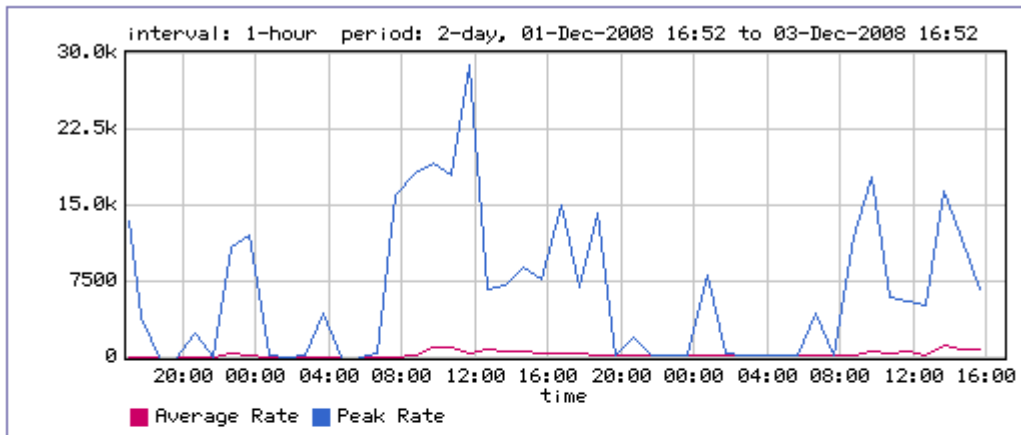
 **Top Listeners**

Time analyzed: 03:00:06

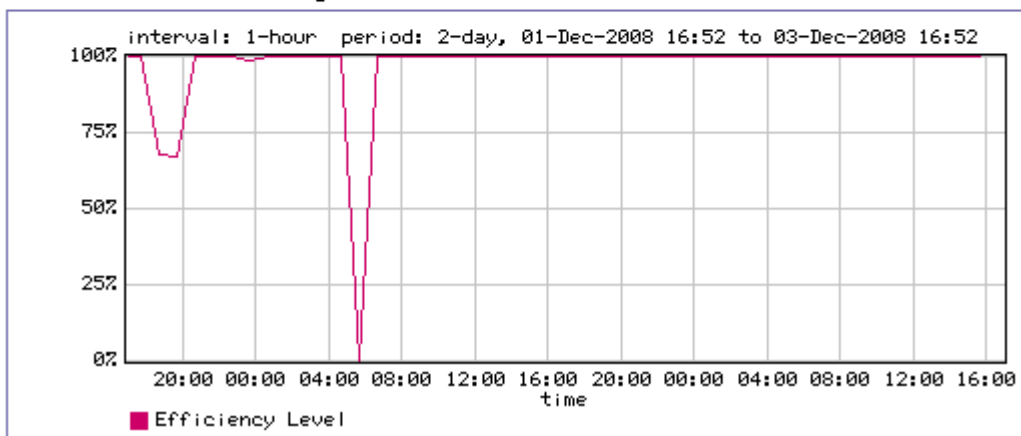
	DNS Name	IP Address	Usage	
1	[REDACTED]	10.8.79.46	56%	classify ...
2	[REDACTED]	10.8.79.157	28%	classify ...
3	[REDACTED]	10.8.78.97	10%	classify ...
4	[REDACTED]	10.4.35.23	2%	classify ...
5	[REDACTED]	10.4.30.139	<1%	classify ...

Citrix stats – outbound, 1st December 2008 to 3rd December 2008

Class Utilization with Peaks



Network Efficiency



The network efficiency drops at the same time the utilisation dropped. This could indicate a reboot or a drop in session.

Traffic Class Tree – 2nd December 2008

Class name	Type	Class hits	Policy hits	Cur rate	1 Min avg	Peak rate
/Inbound	+		n/a	1.6M	1.6M	2.1M
localhost	PE	38693	38693	51k	8014	931k
ActiveX		1	n/a	0	0	598k
BITS		28	n/a	0	0	1.3M
Citrix			n/a	0	26	331k
Citrix-CARPE_DIEM_TRACKER		21	n/a	0	0	173k
Citrix-CMS_LIVE		142	n/a	0	26	297k
Default		116	n/a	0	0	330k
CitrixCGP		58	n/a	0	0	34k
CitrixIMA		144	n/a	37	22	26k
eDonkey		4	n/a	0	0	100
FlashVideo		520	n/a	0	644	1.6M
FTP		279	n/a	0	0	1.3M
GoogleVideo		138	n/a	0	112k	1.5M
HTTP		2471063	n/a	677k	378k	1.6M
HTTP-Tunnel		146279	n/a	245k	485k	1.5M
Kali		5	n/a	416	416	416
lockd		2403	n/a	396	109	1419
LotusNotes		6	n/a	0	0	54k
MGCP		6	n/a	0	0	0
MPEG-Audio		39	n/a	0	0	1.5M
MS-ActiveDir		1366	n/a	0	0	705k
MS-Exchange		1278	n/a	18k	12k	1.5M
MSN-Messenger		97	n/a	0	0	30k
NetIQ		264813	n/a	779	905	553k
RADIUS		8	n/a	0	0	113
RDP		85	n/a	0	0	100k
Real		8	n/a	0	0	1.3M
RemotelyAnywhere		26	n/a	0	0	1.3M
SMTP		20907	n/a	0	3928	1.6M
SOAP-HTTP		3837	n/a	0	0	1.5M
SSH		988	n/a	0	0	6314
SSL		10970	n/a	73	73	1.5M
Telnet		25	n/a	0	0	13k
VNC		4	n/a	0	0	55k
WebEx		15	n/a	52	28	1.1M
WinMedia		373	n/a	0	0	1.5M
WorldOfWarcraft		0	n/a	0	0	0
YouTube		851	n/a	591k	384k	1.5M
BitTorrent		2	n/a	0	0	1
CIFS		76038	n/a	20k	22k	1.3M
DCOM		28124	n/a	2473	866	1.5M
DNS		64683	n/a	601	615	34k
Gnutella		105	n/a	0	0	1.2M
H.323		5	n/a	0	0	0
Jabber		2	n/a	0	0	363
LDAP		25252	n/a	24k	4084	88k
Megaco		0	n/a	0	0	0
MSSQL		329	n/a	0	0	1.3M
NetBIOS-IP		57382	n/a	288	188	7252
RTSP		6	n/a	0	0	47k
SMS		85	n/a	0	0	23k
StreamWorks		4	n/a	0	0	0
WINS		395	n/a	0	2	52k
EIGRP		198	n/a	60	81	4533
ICMP		156426	n/a	590	185	18k
DiscoveredPorts			n/a	3793	3468	1.5M
TCP_Port_1270		48597	n/a	424	220	11k
TCP_Port_1398		3923	n/a	2612	2605	1.5M
TCP_Port_1935		76	n/a	0	810	1.5M

TCP_Port_2418		7773	n/a	1033	833	131k
Default	P I	505222	3901280	9454	5338	1.5M
/Outbound	+		n/a	284k	213k	2.4M
localhost	PE	40648	40648	43k	6842	872k
ActiveX		6	n/a	0	0	10k
BITS		28	n/a	0	0	29k
Citrix			n/a	0	49	30k
Citrix-CARPE_DIEM_TRACKER		21	n/a	0	0	28k
Citrix-CMS_LIVE		143	n/a	0	49	24k
Default		122	n/a	0	0	21k
CitrixCGP		58	n/a	0	0	1.5M
CitrixIMA		141	n/a	52	28	125k
eDonkey		6	n/a	0	0	0
FlashVideo		520	n/a	0	18	153k
FTP		78	n/a	0	0	612k
GoogleVideo		140	n/a	0	3322	52k
HTTP		1063820	n/a	46k	42k	1.4M
HTTP-Tunnel		146311	n/a	39k	43k	459k
Kali		5	n/a	0	0	418
L2TP		13	n/a	0	0	388
lockd		40	n/a	0	0	79
LotusNotes		6	n/a	0	0	5776
MGCP		2	n/a	0	0	0
MPEG-Audio		38	n/a	0	0	54k
MS-ActiveDir		1367	n/a	0	0	114k
MS-Exchange		1276	n/a	97k	34k	1.5M
MSN-Messenger		100	n/a	0	0	66k
NetIQ		264841	n/a	2742	2298	564k
RADIUS		9	n/a	0	0	378
RDP		85	n/a	0	0	432k
Real		8	n/a	0	0	41k
RemotelyAnywhere		26	n/a	0	0	1.4M
SHARESUDP		4	n/a	0	0	0
SMTP		20911	n/a	0	46k	2.3M
SNMP		202023	n/a	0	134	72k
SOAP-HTTP		3846	n/a	0	0	411k
SSH		73	n/a	0	0	41k
SSL		10364	n/a	263	263	808k
Telnet		25	n/a	0	0	760k
VNC		4	n/a	0	0	194k
WebEx		15	n/a	100	56	240k
WinMedia		375	n/a	0	0	77k
WorldOfWarcraft		0	n/a	0	0	0
YouTube		854	n/a	9691	10k	83k
BitTorrent		2	n/a	0	0	1
CIFS		78370	n/a	47k	25k	1.5M
DCOM		28484	n/a	2209	1206	1.5M
DNS		66201	n/a	123	126	86k
Gnutella		105	n/a	0	0	126k
LDAP		27530	n/a	19k	3487	1.2M
Megaco		1	n/a	0	0	0
MSSQL		345	n/a	0	0	54k
NetBIOS-IP		9259	n/a	407	226	21k
RTSP		6	n/a	0	0	14k
SMS		85	n/a	0	0	1.1M
StreamWorks		7	n/a	0	0	0
EIGRP		222	n/a	452	362	17k
ICMP		114753	n/a	587	147	15k
DiscoveredPorts			n/a	3644	3598	274k
TCP_Port_1270		50614	n/a	2798	1140	129k
TCP_Port_1398		3932	n/a	3101	2479	196k
TCP_Port_1935		103	n/a	0	170	49k
Default	P I	472449	2570007	49k	8275	1.9M

Traffic Class Tree – 3rd December 2008

Class name	Type	Class hits	Policy hits	Cur rate	1 Min avg	Peak rate
/Inbound	+		n/a	124k	281k	2.2M
localhost	PE	10357	10357	75k	86k	1.2M
lonprox03.corp.companyxr		107802	n/a	2428	88k	
1.6M						
ActiveX		0	n/a	0	0	0
BITS		0	n/a	0	0	0
HTTP			n/a	7648	4809	1.5M
lonsms01.corp.companyxro		129	n/a	0	6	
7751						
Default		72256	n/a	7648	4809	1.5M
Citrix			n/a	18k	3674	176k
Citrix-CARPE_DIEM_TRACKER		1	n/a	0	0	77k
Citrix-CMS_LIVE		71	n/a	18k	3674	176k
Default		8	n/a	0	0	39k
CitrixCGP		3	n/a	0	0	15k
CitrixIMA		24	n/a	0	168	10k
eDonkey		0	n/a	0	0	0
FlashVideo		0	n/a	0	0	0
FTP		15	n/a	0	2	38k
GoogleVideo		0	n/a	0	0	0
HTTP-Tunnel		0	n/a	0	0	0
Kali		3	n/a	0	0	3
lockd		555	n/a	100	116	390
LotusNotes		0	n/a	0	0	0
MGCP		0	n/a	0	0	0
MPEG-Audio		0	n/a	0	0	0
MS-ActiveDir		129	n/a	0	104	210k
MS-Exchange		139	n/a	10k	8758	778k
MSN-Messenger		0	n/a	0	0	0
NetIQ		27812	n/a	580	536	8061
RADIUS		0	n/a	0	0	0
RDP		5	n/a	0	0	11k
Real		0	n/a	0	0	0
RemotelyAnywhere		0	n/a	0	0	0
SMTP		2137	n/a	0	1130	1.6M
SOAP-HTTP		304	n/a	0	6	71k
SSH		119	n/a	0	0	2179
SSL		925	n/a	0	31	1.5M
Telnet		0	n/a	0	0	0
VNC		0	n/a	0	0	0
WebEx		0	n/a	0	16	392
WinMedia		1	n/a	0	0	0
WorldOfWarcraft		0	n/a	0	0	0
YouTube		0	n/a	0	0	0
BitTorrent		0	n/a	0	0	0
CIFS		8373	n/a	6248	16k	1.4M
DCOM		3301	n/a	136	225	619k
DNS		5393	n/a	0	25	22k
Gnutella		0	n/a	0	0	0
H.323		0	n/a	0	0	0
Jabber		0	n/a	0	0	0
LDAP		2619	n/a	0	153	78k
Megaco		0	n/a	0	0	0
MSSQL		33	n/a	0	10	160
NetBIOS-IP		5957	n/a	147	145	4596
RTSP		0	n/a	0	0	0
SMS		3	n/a	0	2	3
StreamWorks		2	n/a	0	0	101
WINS		41	n/a	0	26	22k
EIGRP		12	n/a	61	112	2109
ICMP		14834	n/a	7	32	12k

DiscoveredPorts			n/a	3696	19k	1.2M	
TCP_Port_1270	4597		n/a	0	118	3468	
TCP_Port_1398	2412		n/a	701	19k	1.2M	
TCP_Port_1935	9		n/a	0	8	698k	
TCP_Port_2418	1039		n/a	582	1331	104k	
UDP_Port_135	14339		n/a	1785	1060	6042	
UDP_Port_2247	14362		n/a	568	500	2342	
Default	P I	40514	377579	985	1135	1.3M	
/Outbound				n/a	102k	179k	2.3M
Localhost	+				64k	97k	1.2M
amsdmcl01.corp.companyxr	PE	15557	15557	n/a	738	1549	
1.6M		1281					
amsdmcl02.corp.companyxr		141		n/a	0	0	
1.6M							
amsdms01.corp.companyxro		40958		n/a	3292	3793	
266k							
lonprox03.corp.companyxr		79493		n/a	782	13k	
684k							
ActiveX		0		n/a	0	0	0
BITS		0		n/a	0	0	0
Citrix				n/a	4268	2257	17k
Citrix-CARPE_DIEM_TRACKER		1		n/a	0	0	8393
Citrix-CMS_LIVE		70		n/a	4268	2257	17k
Default		6		n/a	0	0	11k
CitrixCGP		3		n/a	0	0	414k
CitrixIMA		24		n/a	0	203	88k
eDonkey		0		n/a	0	0	0
FlashVideo		0		n/a	0	0	0
FTP		2		n/a	0	2	8678
GoogleVideo		0		n/a	0	0	0
HTTP		25012		n/a	11k	4917	1.2M
HTTP-Tunnel		0		n/a	0	0	0
Kali		0		n/a	0	0	0
L2TP		0		n/a	0	0	0
lockd		8		n/a	0	0	1
LotusNotes		0		n/a	0	0	0
MGCP		1		n/a	0	0	0
MPEG-Audio		0		n/a	0	0	0
MS-ActiveDir		128		n/a	0	31	77k
MS-Exchange		125		n/a	11k	18k	901k
MSN-Messenger		0		n/a	0	0	0
NetIQ		22844		n/a	635	1293	213k
RADIUS		2		n/a	0	0	402
RDP		5		n/a	0	8	294k
Real		0		n/a	0	0	0
RemotelyAnywhere		0		n/a	0	0	0
SHARESUDP		0		n/a	0	0	0
SMTP		2137		n/a	0	9662	1.6M
SNMP		24945		n/a	0	305	54k
SOAP-HTTP		265		n/a	0	6	347k
SSH		8		n/a	0	0	2062
SSL		822		n/a	0	180	212k
Telnet		0		n/a	0	0	0
VNC		0		n/a	0	0	0
WebEx		0		n/a	0	30	1004
WinMedia		1		n/a	0	0	0
WorldOfWarcraft		0		n/a	0	0	0
YouTube		0		n/a	0	0	0
BitTorrent		0		n/a	0	0	0
CIFS		8808		n/a	4611	7784	1.4M
DCOM		3275		n/a	93	174	581k
DNS		5688		n/a	0	19	65k
Gnutella		0		n/a	0	0	0
LDAP		2806		n/a	0	210	1.2M
Megaco		0		n/a	0	0	0
MSSQL		32		n/a	0	3	46
NetBIOS-IP		793		n/a	41	102	7706

RTSP	0	n/a	0	0	0
SMS	1	n/a	0	0	0
StreamWorks	0	n/a	0	0	0
EIGRP	12	n/a	361	368	7854
ICMP	11431	n/a	7	32	3383
DiscoveredPorts		n/a	699	4549	1.5M
TCP_Port_1270	4742	n/a	0	671	62k
TCP_Port_1398	2412	n/a	700	3850	1.5M
TCP_Port_1935	10	n/a	0	0	33k
Default	P I 21487	259779	1877	1086	1.8M