

Understanding your Network traffic

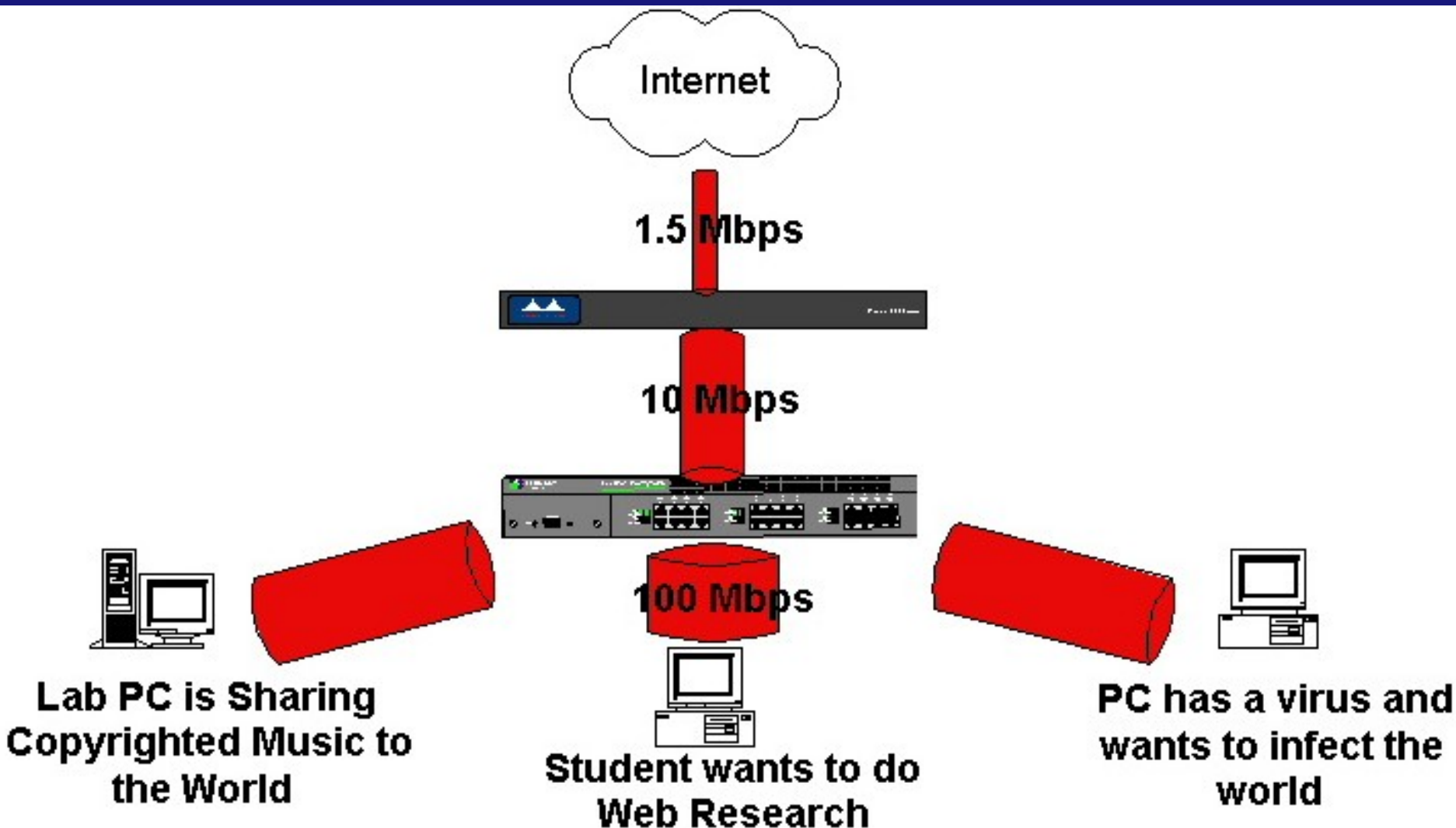
Charles Wright

Network Engineer

Alabama Supercomputer Authority



Internet Bandwidth is Relatively Slow and Expensive



One PC can break your network

You need to be able to quickly

- Locate your heaviest users
- Understand what they are doing
- Review past usage



Basic Strategy

- Understand your network topology
- Establish a baseline for Network Use
- Understand Users Needs
- Plan to ensure these needs are met, while pruning/limiting unwanted traffic



Establish a Baseline

- What should traffic look like on a normal day?
- What applications take up the most traffic?
 - Email? Real audio?
 - Web browsing? Peer 2 Peer?
- Who are my top 3 users?
- How much bandwidth do they use compared to a average user?

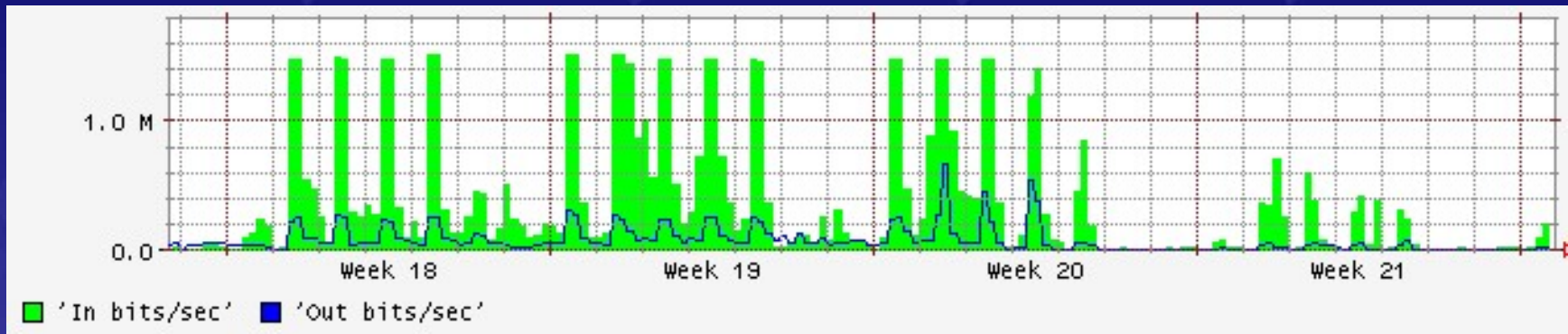


Network Management Tools

- Basic Graphs – History of usage in bits/sec
- Network Sniffer – Captures Everything – Fills up disk quickly but good for real time troubleshooting
- IPAudit – Captures src/dst ip addresses/port numbers and bytes transferred



Graphs – MRTG, (SMNP polled from routers or switches)

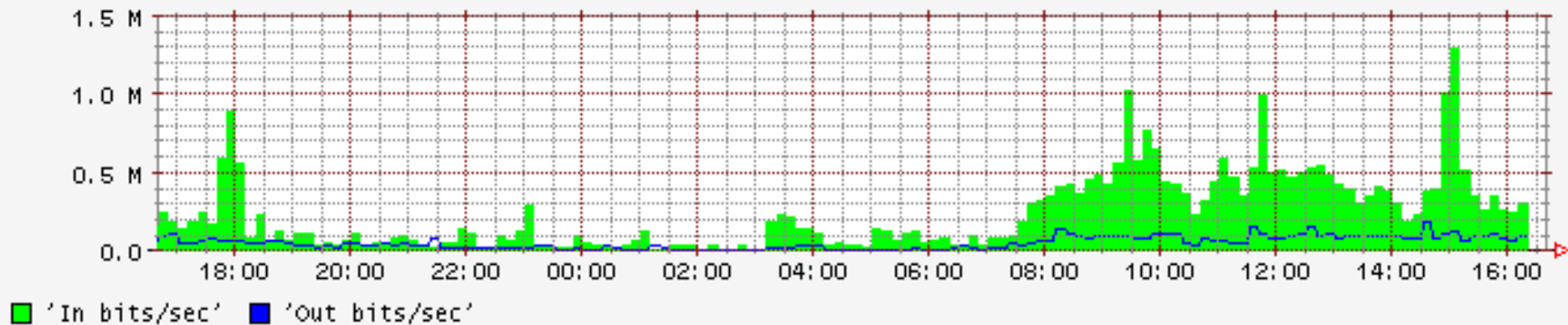


- Good for estimating when to buy bigger pipes (if you are watching for bad stuff)
- Help determine major change in traffic patterns
- Doesn't identify what traffic is or who is using it



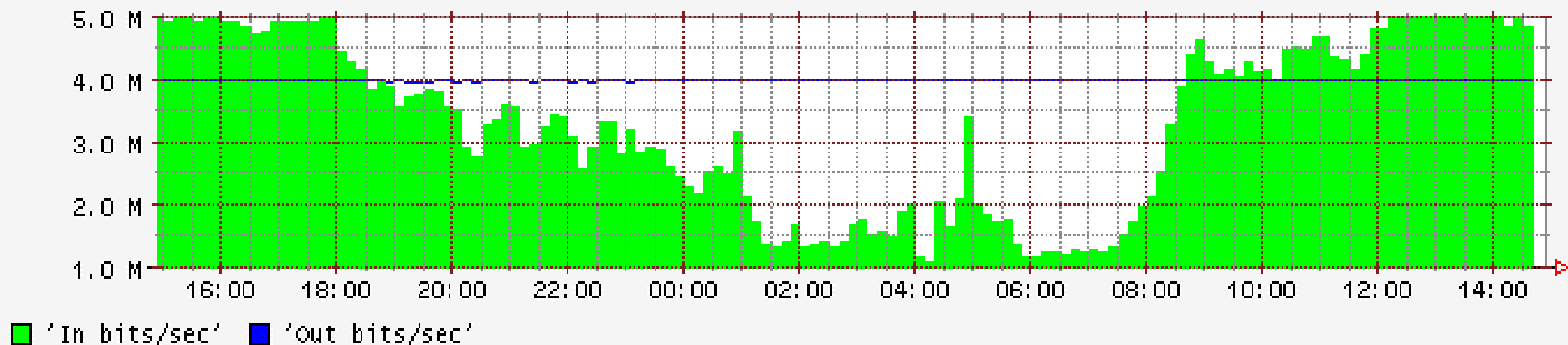
Normal Web Browsing

SUCC Serial0 Traffic : "SUCC -> Mtgmy T1 (AT&T)"

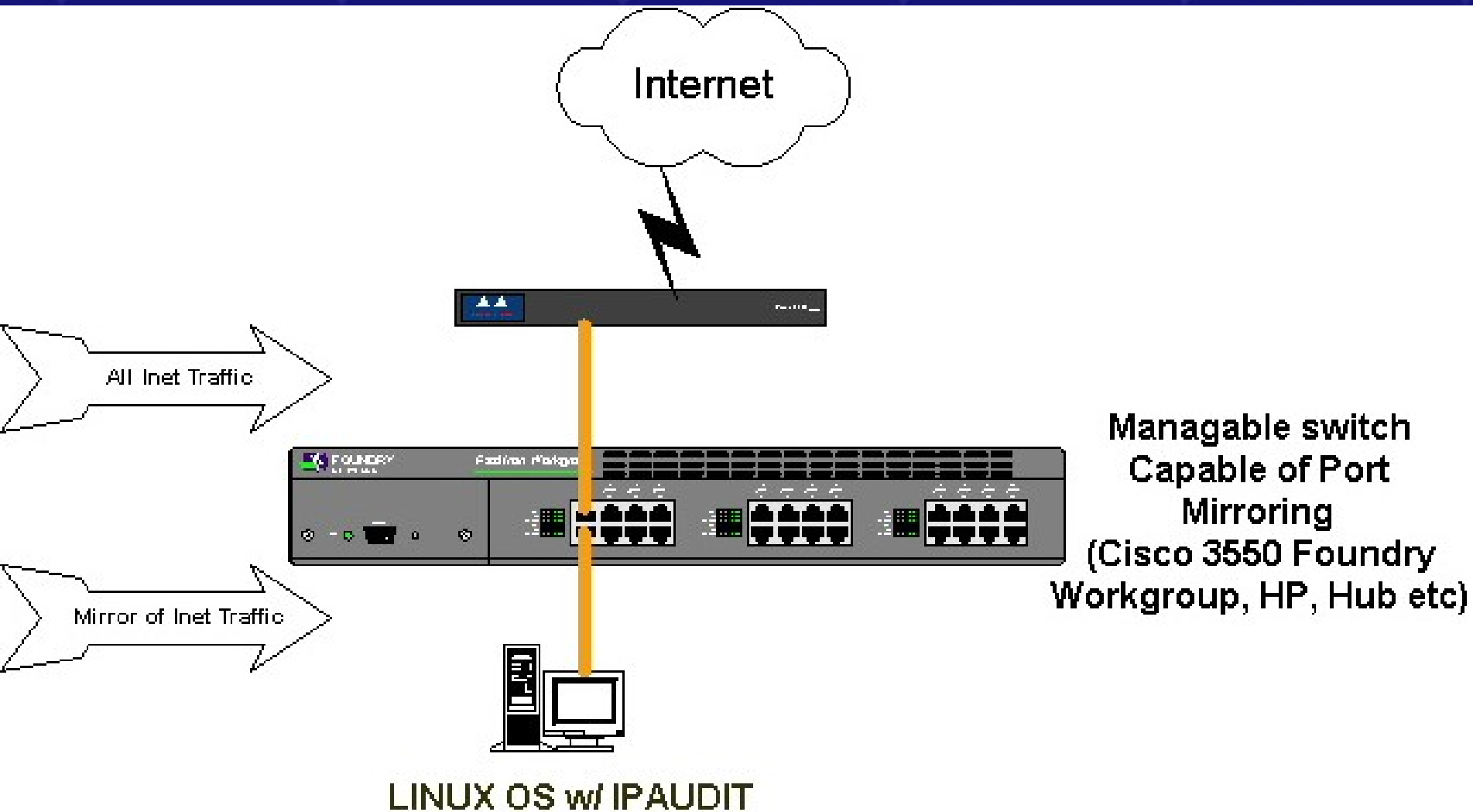


Peer 2 Peer Signature

AAM ATM1/0 Traffic : ""



How IPAudit works



IP Audit – Screenshots

POSSIBLE INCOMING-SCAN HOSTS

IP Address	IP Name	Number of Contacts
195.173.243.208	produktiehuis.demon.nl	261
218.216.053.020	mcn-m1 d53020.miyazaki-catv.ne.jp	109
204.029.088.138	138.domain.tld	31
200.084.123.185	dC8547BB9.dslam-01-18-401-01-01.pdm.dsl.cantv.net	20
212.045.007.060		8
207.157.134.182		6
129.066.020.006	asnsvr2.asc.edu	4
210.082.146.171		3
218.147.143.113		3
172.020.148.050		3
080.117.237.233	host233-237.pool80117.interbusiness.it	3
061.138.010.103		3
065.054.249.126		2
204.031.170.246	dsc02-mpi-ca-2-246.rasserver.net	2
198.095.251.001	ntc-ext101.dns.aol.com	2
199.224.008.037	sopc.telmar.com	2
143.166.083.022	ausoladpds2web.us.dell.com	2
172.020.148.054		2
152.163.207.112	ipt-co09.proxy.aol.com	2

POSSIBLE OUTGOING-SCAN HOSTS

IP Address	IP Name	Number of Contacts
198.180.132.025		98
198.180.132.026	asnaam.aamu.edu	94
204.029.127.061	61.domain.tld	73
198.180.132.075		17
198.180.132.164	antivirus.aamu.edu	16
198.180.132.076		13
207.157.032.249	249.domain.tld	10
198.180.132.022	socrates.aamu.edu	7
198.180.132.100	interscan.aamu.edu	7
198.180.132.237		7
207.157.032.178	178.domain.tld	7
204.029.127.127	127.domain.tld	6
198.180.132.001		6
204.027.217.252		5
198.180.133.020	mycroft.caos.aamu.edu	5
198.180.132.178		4
207.157.032.251	251.domain.tld	4
199.020.028.057	57.domain.tld	3
198.180.132.085		3
198.180.132.090	www2.aamu.edu	3

Column Key:

1-Local IP 2-Remote IP

3-Protocol

4-Local Port (or Outgoing ICMP code) 5-Remote Port (or Incoming ICMP code)

6-Incoming (bytes) 7-Outgoing (bytes)

8-Incoming (packets) 9-Outgoing (packets)

10-First Packet time 11-Last Packet time

12-First Packet source 13-Last Packet source (L Local,R Remote,- OneWay)

192.168.1.56	165.254.12.102	tcp	1062	<u>80</u>	415	1014	4	6	09:12:22.2148	09:12:25.3797	L R
192.168.1.56	216.109.50.69	udp	1029	53	2.4k	531	7	7	09:12:22.2183	09:12:25.7376	L R
192.168.1.56	207.46.249.190	tcp	1063	<u>80</u>	559	628	2	5	09:12:22.3043	09:13:25.4055	L L
192.168.1.56	207.68.172.246	tcp	1064	<u>80</u>	572	589	5	5	09:12:22.6634	09:12:22.9455	L R
192.168.1.56	207.68.171.245	tcp	1065	<u>80</u>	27.8k	1.4k	24	19	09:12:22.9052	09:12:23.7961	L R
192.168.1.56	207.68.177.126	tcp	1066	<u>80</u>	672	760	4	5	09:12:24.9101	09:12:25.1987	L R
192.168.1.56	63.150.188.158	tcp	1067	<u>80</u>	977	1.1k	5	8	09:12:25.0324	09:12:35.3147	L L
192.168.1.56	65.54.131.192	tcp	<u>1068</u>	<u>80</u>	465	647	5	5	09:12:25.5549	09:12:25.9441	L R
192.168.1.56	216.109.50.69	udp	1069	53	8.3k	2.2k	29	30	09:12:25.7170	09:28:42.5081	L R
192.168.1.56	207.68.178.237	tcp	1070	<u>80</u>	638	824	5	5	09:12:25.7301	09:12:26.0462	L R
192.168.1.56	207.68.172.236	tcp	1071	<u>80</u>	10.1k	2.3k	14	17	09:12:25.8794	09:13:30.4336	L L
192.168.1.56	207.68.172.236	tcp	1072	<u>80</u>	4.2k	1.5k	7	11	09:12:25.9404	09:13:30.4191	L L
192.168.1.56	38.117.132.201	tcp	1073	<u>80</u>	1.9k	781	6	7	09:12:26.3390	09:12:26.5082	L R
192.168.1.56	216.34.88.210	tcp	1074	<u>80</u>	647	783	3	5	09:12:26.6912	09:12:26.9118	L L
192.168.1.56	64.156.240.36	tcp	1075	<u>80</u>	2.7k	900	6	7	09:12:27.9563	09:12:40.3309	L L
192.168.1.56	38.117.132.231	tcp	1076	<u>80</u>	1.2k	914	6	7	09:12:30.1961	09:12:30.6552	L R
192.168.1.56	38.117.132.202	tcp	1077	<u>80</u>	256	714	2	5	09:12:57.5888	09:14:19.1907	L L
192.168.1.56	165.254.12.103	tcp	1078	<u>80</u>	255.3k	11.9k	190	140	09:12:57.8510	09:13:53.3207	L R
192.168.1.56	207.68.172.249	tcp	1079	<u>80</u>	819	868	5	5	09:13:49.8591	09:13:50.4148	L R
192.168.1.56	207.68.176.190	tcp	1080	<u>80</u>	14.8k	1.3k	13	12	09:13:50.4295	09:14:52.9151	L L
192.168.1.56	207.68.178.237	tcp	<u>1081</u>	<u>80</u>	638	871	5	5	09:13:51.9090	09:13:52.1915	L R
192.168.1.56	65.54.192.248	tcp	<u>1083</u>	<u>80</u>	586	799	5	5	09:13:51.9585	09:13:52.3293	L R
192.168.1.56	216.34.88.210	tcp	<u>1082</u>	<u>80</u>	660	818	3	5	09:13:51.9619	09:13:52.3789	L L
192.168.1.56	38.117.132.201	tcp	<u>1084</u>	<u>80</u>	741	747	5	5	09:13:52.2891	09:13:53.8350	L R
192.168.1.56	64.156.240.36	tcp	1085	<u>80</u>	11.3k	975	12	10	09:13:52.4474	09:14:00.7688	L L
192.168.1.56	157.149.4.10	tcp	1086	<u>80</u>	132.7k	10.4k	104	77	09:13:55.7172	09:14:33.9122	L L
192.168.1.56	157.149.4.10	tcp	1087	<u>80</u>	99.7k	9.6k	80	64	09:13:57.2226	09:14:33.7999	L L
192.168.1.56	38.117.132.201	tcp	1088	<u>80</u>	401	695	4	5	09:13:57.6070	09:13:57.7966	L R
192.168.1.56	157.149.4.12	tcp	1089	<u>80</u>	4.4k	10.5k	24	33	09:13:57.6896	09:15:18.7064	L L

BUSIEST HOST PAIRS

Local IP	Remote IP	Local Name	Remote Name	Total	Incoming	Outgoing
198.180.132.075	066.230.217.040			97,003,897	94,206,135	2,797,762
207.157.032.172	063.219.179.131	172.domain.tld		57,537,726	55,558,936	1,978,790
199.020.028.042	066.128.101.051	42.domain.tld	oliv01-51.cbnstl.net	33,682,532	802,384	32,880,148
198.180.132.201	064.070.181.076		templeofpraise.net	32,454,051	31,844,167	609,884
199.020.028.042	080.011.046.127	42.domain.tld	ASte-Genev-Bois-103-1-3-127.w80-11.abo.wanadoo.fr	31,762,932	731,948	31,030,984
198.180.132.038	129.066.096.008			20,353,218	19,954,939	398,279
199.020.028.042	081.051.255.053	42.domain.tld	AMarseille-206-1-27-53.w81-51.abo.wanadoo.fr	17,080,224	371,476	16,708,748
198.180.132.129	216.235.080.071			11,701,182	11,398,636	302,546
199.020.027.161	217.227.037.052		pD9E32534.dip.t-dialin.net	11,099,320	239,439	10,859,881
207.157.032.098	129.066.096.007	98.domain.tld		10,860,827	10,629,630	231,197
198.180.132.038	129.066.096.007			10,243,558	10,043,608	199,950
207.157.032.098	129.066.096.008	98.domain.tld		8,957,923	8,768,056	189,867
207.157.032.098	206.024.190.157	98.domain.tld		8,499,440	8,221,709	277,731
198.180.132.102	207.157.057.014		realserverg2.oakwood.edu	8,025,437	7,871,800	153,637
198.180.132.090	067.034.140.065	www2.aamu.edu	adsl-34-140-65.asm.bellsouth.net	7,597,141	442,623	7,154,518
198.180.132.100	198.122.199.007	interscan.aamu.edu	nsstcex2.nsstc.nasa.gov	7,572,450	7,298,390	274,060
198.180.132.075	065.031.116.128		CPE-65-31-116-128.wi.rr.com	7,110,831	6,910,803	200,028
198.180.132.075	066.069.050.053		cs666950-53.satx.rr.com	6,078,757	162,952	5,915,805
198.180.132.113	064.236.240.190	raserver.aamu.edu	atl190.turner.com	5,606,394	483,318	5,123,076
198.180.132.113	068.113.103.078	raserver.aamu.edu	dhcp-138-8.cpe.dectr.al.charter.com	5,543,974	451,404	5,092,570
198.180.132.075	068.062.174.232		pcp02495130pcs.flmc01.al.comcast.net	5,285,153	5,161,213	123,940
198.180.132.172	066.028.222.105			5,283,980	5,274,614	9,366
198.180.132.223	066.250.188.014			5,246,334	4,914,714	331,620
198.180.132.067	066.218.087.254		p1.ymdb.vip.scd.yahoo.com	5,128,152	4,683,116	445,036
198.180.132.114	208.051.070.161			5,060,320	5,019,418	40,902

#	protocol	both	incoming	outgoing
#	-----	----	-----	-----
	TCP	17,731,727,671	13,899,182,173	3,832,545,498
	http	14,398,746,412	10,030,546,290	4,368,200,122
	mail	2,915,386,910	1,395,040,968	1,520,345,942
	Real A/V	1,609,011,217	916,390,680	692,620,537
	UDP	1,251,907,288	573,657,923	678,249,365
	https	443,303,150	357,949,760	85,353,390
	ftp	242,644,315	236,172,925	6,471,390
	napster	131,084,307	78,026,861	53,057,446
	irc	116,350,449	76,447,519	39,902,930
	ICMP	47,550,721	11,654,670	35,896,051
	pop	23,970,473	9,604,002	14,366,471
	icq	14,350,911	10,045,844	4,305,067
	morpheus	7,885,131	5,024,205	2,860,926
	gnutella	4,656,308	2,958,066	1,698,242
	snmp	4,638,413	200,962	4,437,451
	ssh	3,762,735	932,689	2,830,046
	telnet	3,178,498	1,812,986	1,365,512
	imesh	1,337,681	1,046,270	291,411
	socks	922,028	637,326	284,702
	news	895,704	586,186	309,518
	Shoutcast	159,566	117,356	42,210
	ntp	16,562	62	16,500
	imap	13,769	850	12,919
	Hotline	624	170	454
	Half-Life	175	175	0
	scour	54	0	54
	other	111,289,271	94,554,529	16,734,742
	TOTAL	39,064,790,343	27,702,591,447	11,362,198,896

Your Action Plan

- Block Traffic from the router
- Create and Enforce an Acceptable Use Policy
- Track heavy users down and make them aware of their impact on the Network



Another Product – Packetshaper

- Can allocate % of Bandwidth for certain traffic
- Can make one type of traffic higher priority
- Drops in between switch and router
- No Re-addressing required

<http://www.packeteer.com/products/packetshaper.cfm>



Getting a quote for IPAudit

Contact

Kim Carrol 334 242 0155

kcarroll@asc.edu



Generally Includes

- 1 U Server (no monitor)
- Installation of Linux and IPAudit
- Support and maintaince (great if you have little time to spend on learning a new OS)

If you have your own hardware

AREN Can...

- Help you install Linux over the Network on your hardware (you support and maintain!)
- You need a server w/ Floppy drive, Hard drive and Network Card and capable switch

(AREN Customers Only – Others get a quote)

Contact Helpdesk: 800 338 8320



Or Build it yourself, there is no charge for the software!

<http://www.redhat.com>

<http://www.linuxiso.org>

<http://ipaudit.sourceforge.net/ipaudit-web/>

<http://people.ee.ethz.ch/~oetiker/webtools/mrtg>



Questions/Comments

