

NetFlow Tools and Analysis at Fermilab.

ESCC/Internet2 Joint Techs Workshop

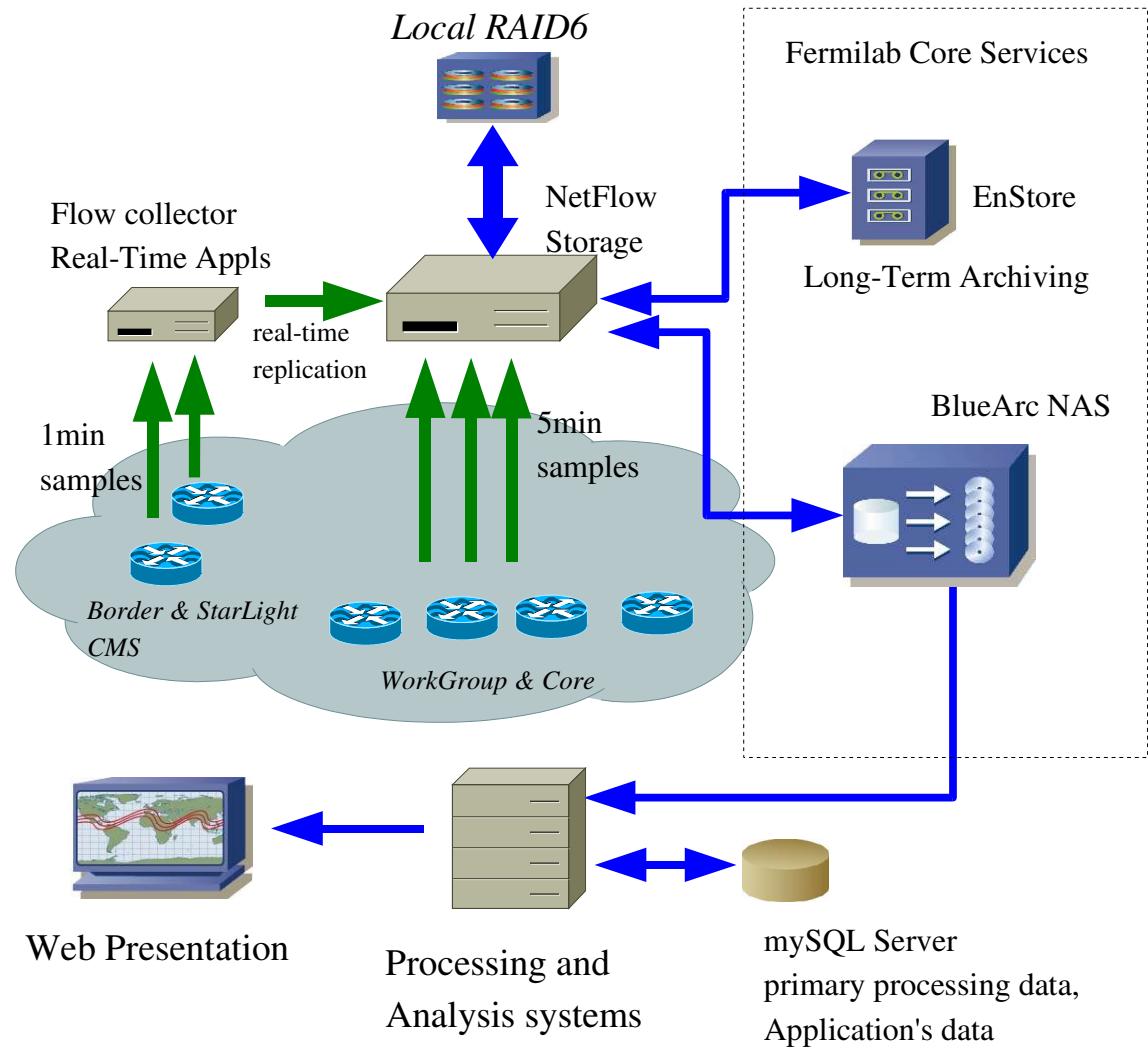
Fermilab, July 15-19, 2007

Outline of the talk:

- Overview of Netflow collection and analysis system at Fermilab
 - Security tools
 - Performance estimation tools
 - Checking of traffic for PBR-ed circuits

Netflow Collection and Analysis system

- Based on: flow-tools OSU package
- Collecting data from Border, StarLight,CMS WG routers in 1min samples, D0 & CDF workgroup routers and from multiple Core routers in 5min samples
- Several applications are running on collector machine in near real-time
- Central storage accumulating data from all routers
- Results of primary processing is stored in multiple SQL tables



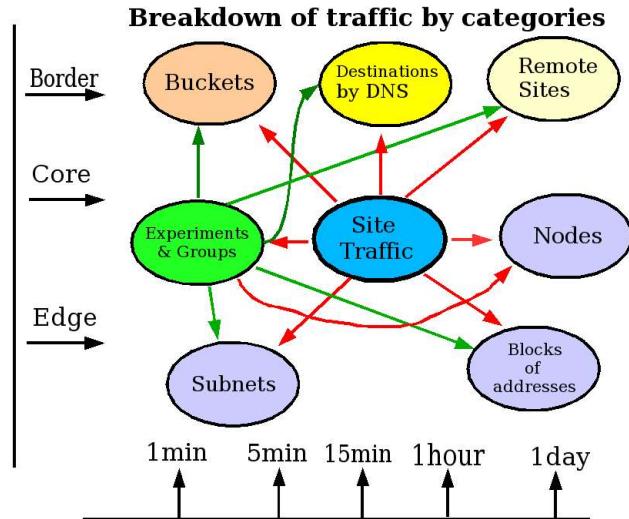
Amount of collected data

	Daily	Monthly
Border	600MB	17GB
StarLight	200MB	5GB
CMS	1.2GB	30GB
CORE	500MB	12GB

Total available ~ 4TB

Older data are archived on EnStore, Fermilab central storage facility

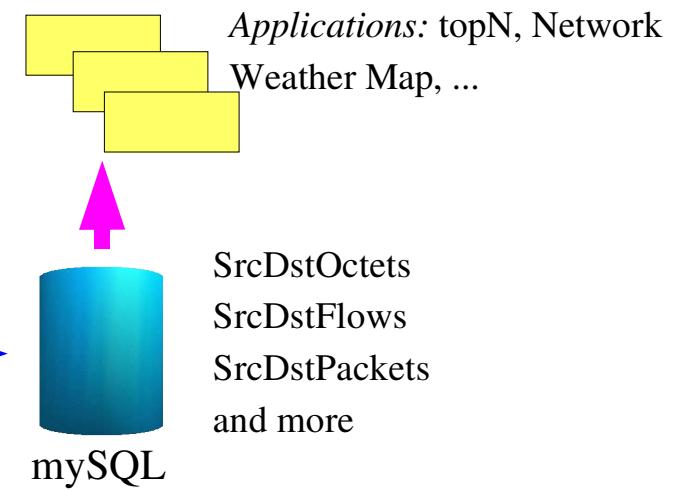
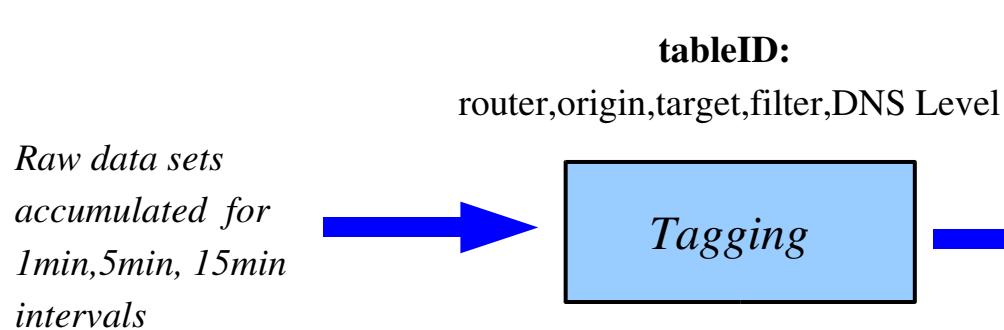
Breakdown of traffic and tagging process



Origin: onsite, offsite, local, transit

Target: CMS, D0, CDF

Filter: particular remote site or group of sites. Ex. Caltech, Tier2, US-Tier2 and etc..



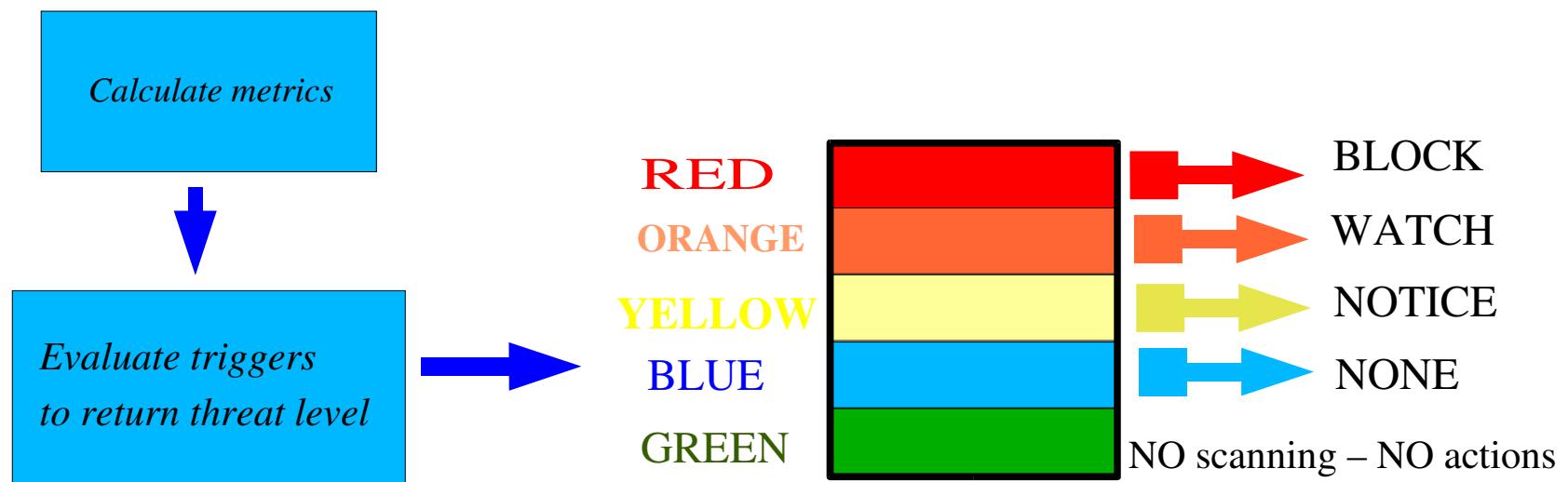
Sources and Destinations are identified by DNS name (host, top level, second level and so on) or statically assigned labels

Security Tools

- AutoBlocker – nearly real-time detection and automatic block/unblocking onsite and offsite scanners
- Top Scanners GUI
- Slow Scanning detection
- Raw Flow reader – packets exchange

AutoBlocker – automatic detection and blocking/unblocking offsite and onsite scanners

The main idea of AB3 is calculating multiple quantified metrics from netflow data to use it for making automated decision on blocking and unblocking of offsite and onsite scanners. In October of this year it will be 5 years since AutoBlocker has been deployed.



Metrics/Triggers/Threats/Actions

Metrics:

- ipDestinationAddressCount
- ipDestinationPortCount
- ipSourcePortCount
- blockCount
- activeBlockCount
- detectionCount
- consecutiveDetection
- consecutiveWatch
- watchRate
- flowsIn
- flowsOut
- HitByRemotes
- excessivePrcTime
- tcpSourcePortOut
- tcpSourcePortIn
- tcpDestPortOut
- tcpDestPortIn
- udpSourcePortOut
- udpSourcePortIn
- udpDestPortOut
- udpDestPortIn

Triggers:

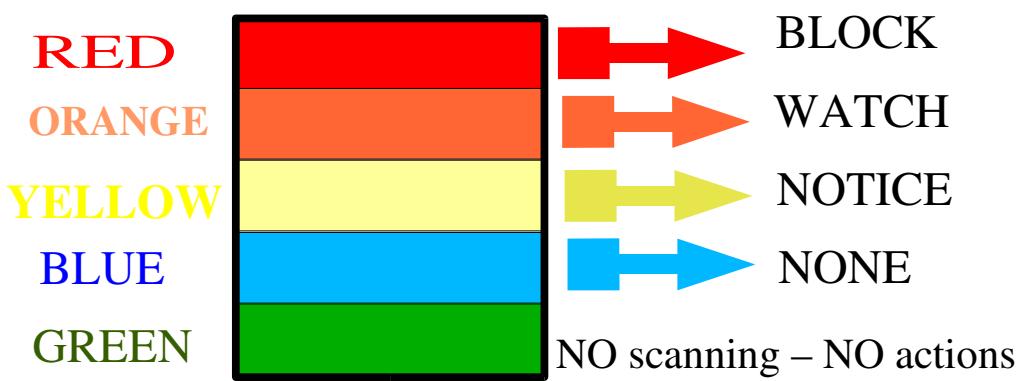
- excessiveHostCount
- excessiveDestinationPort
- flowsResponseInconsistency
- portScanFlowsResponse
- excessiveProcessingRate
- DatectionRate
- consecutiveDetection
- watchRate
- consecutiveWatch

Actions:

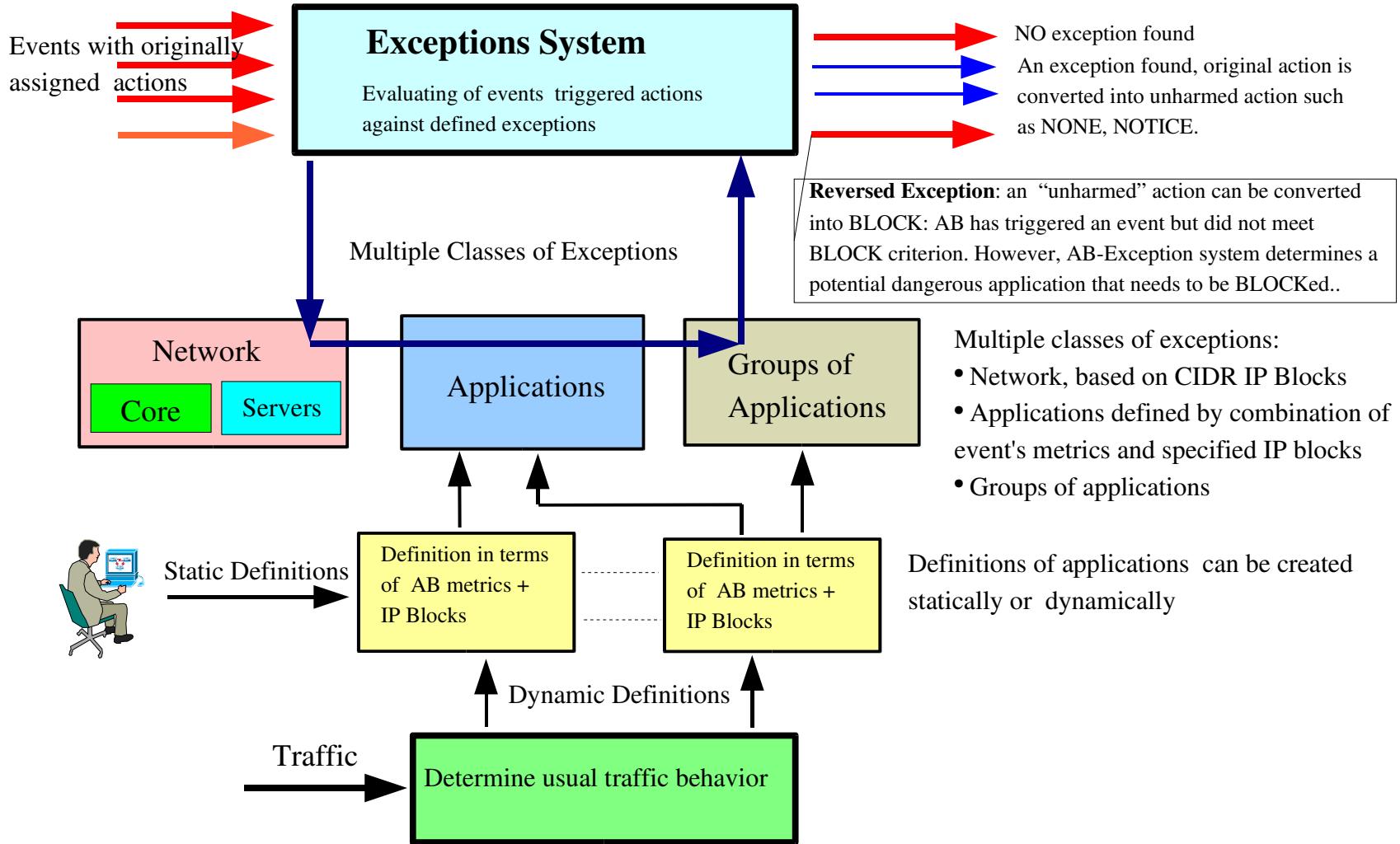
- BLOCK/unBLOCK
- watch/resetWatch
- NONE/flushNONE
- NOTICE

Triggers return the threat identified by a color.

Threats are mapped into actions



AutoBlocker Exceptions System



External AutoBlocker detectors

Several external AutoBlocker detectors:

- DarkNets - analyze traffic to unallocated Fermilab networks and generate alerts to AB3 via SOAP
- SlowScan – detects slow scanning by analyzing flow for a longer periods (1hour, 1 day) and generate alerts to AB3

Raw Flows Reader

WEB- Interface to see raw flow data based on specified criteria, such as time range, port, source/destination addresses

Raw Flows Web Interface – SeaMonkey

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop https://fnndcg3.fnal.gov/secure-bin/rfm.cgi Search Print

Home Bookmarks Scientific Linux Distros http://www.lifetimefit... TopN Daily Host Conv... topnframes CNS: DNS Caching Ser...

Top Up First Previous Next Last Document More

Web Interface to Raw Flows

Query at Router: r-cms-fcc2

Name or IP #1: **Name or IP #2:**

Src or Dest
 Src Only
 As Src OR Dest And Name/Ip#2

Use Port:

Port options:
 Source or Dest (or S/D)
 Source Only
 Destination Only

Search for particular Dates:

Start at: 06/24/07 14:30
End at: 06/25/07 14:45

Router ACL options:

Include blocked flows
 Filter out blocked flows
 Show ONLY blocked flows

Include traffic generated ONLY by:

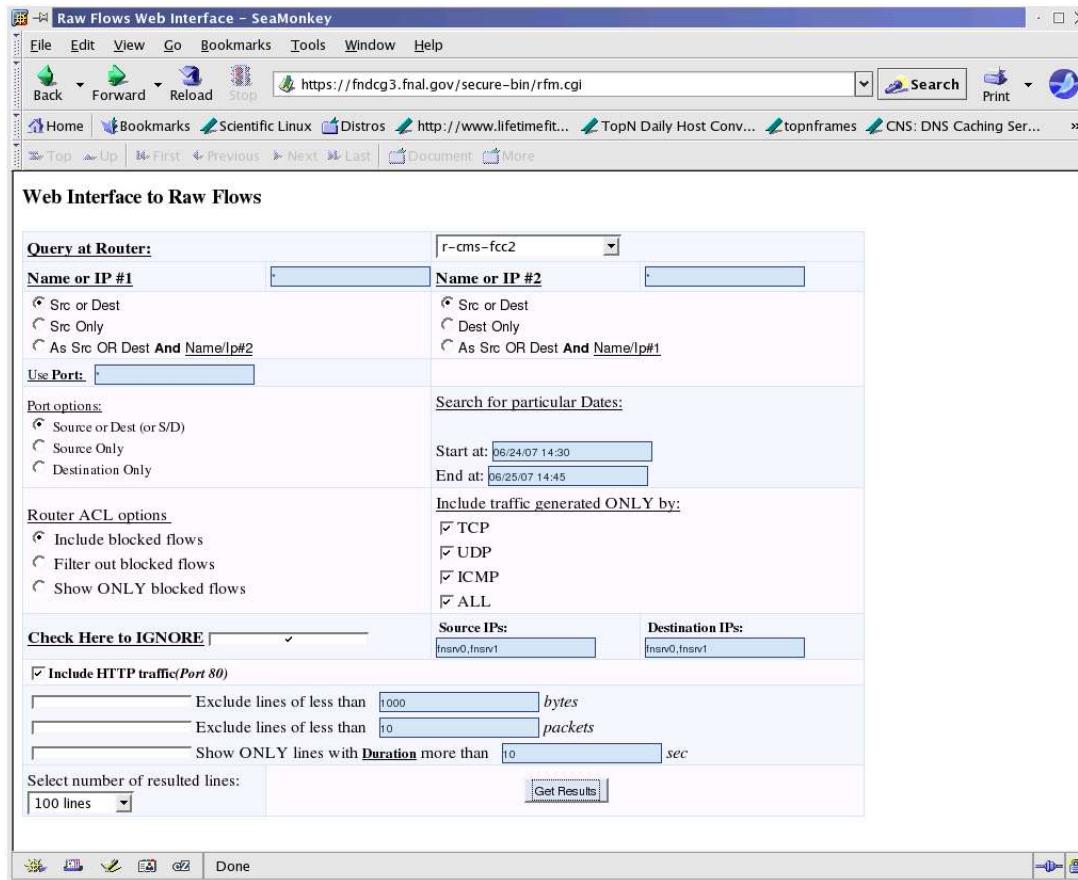
TCP
 UDP
 ICMP
 ALL

Check Here to IGNORE: **Source IPs:** **Destination IPs:**
 Include HTTP traffic(Port 80)

Exclude lines of less than bytes
Exclude lines of less than packets
Show ONLY lines with Duration more than sec

Select number of resulted lines: 100 lines **Get Results**

Done



Sample of RawFlow Output

Raw Flows Web Interface – SeaMonkey

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop https://fndcg3.fnal.gov/secure-bin/rfm.cgi?tr=r-cms-fcc2&srcip=*&desip=*&sdl= Search Print

Home Bookmarks Scientific Linux Distros http://www.lifetimefit... TopN Daily Host Conv... topnframes CNS: DNS Caching Ser...

Top Up First Previous Next Last Document More

Web Interface to Raw Flows

Time	Src IP	Src Port	Dst IP	Dst Port	Protocol	Pkts/Bytes	Duration(sec)
0624.14:28:20.097	131.225.12.194	34620	131.225.204.204	689	TCP	1/46	0
0624.14:28:20.161	131.225.12.194	52345	131.225.204.248	2120	TCP	1/46	0
0624.14:28:20.097	131.225.12.194	34620	131.225.204.204	681	TCP	1/46	0
0624.14:28:20.097	131.225.12.194	34620	131.225.204.204	44	TCP	1/46	0
0624.14:28:18.305	131.225.12.194	47342	131.225.204.30	248	TCP	1/46	0
0624.14:28:20.097	131.225.12.194	34620	131.225.204.204	38037	TCP	1/46	0
0624.14:28:18.305	131.225.12.194	52888	131.225.204.4	8	TCP	1/46	0
0624.14:28:18.817	131.225.204.58	5	131.225.12.193	56818	TCP	1/60	0
0624.14:28:18.305	131.225.12.194	52888	131.225.204.4	888	TCP	1/46	0
0624.14:28:19.329	131.225.12.195	42810	131.225.204.93	15	TCP	1/46	0
0624.14:28:20.161	131.225.12.194	52345	131.225.204.248	659	TCP	1/46	0
0624.14:28:18.304	131.225.12.194	52888	131.225.204.4	8000	TCP	1/46	0
0624.14:28:20.096	131.225.12.194	34620	131.225.204.204	5800	TCP	1/46	0
0624.14:28:20.160	131.225.12.194	52345	131.225.204.248	7009	TCP	1/46	0
0624.14:28:20.160	131.225.12.194	52345	131.225.204.248	644	TCP	1/46	0
0624.14:28:18.304	131.225.12.194	47342	131.225.204.30	274	TCP	1/46	0
0624.14:28:18.304	131.225.12.194	47342	131.225.204.30	183	TCP	1/46	0
0624.14:28:18.304	131.225.12.194	52888	131.225.204.4	501	TCP	1/46	0
0624.14:28:20.160	131.225.12.194	52345	131.225.204.248	371	TCP	1/46	0
0624.14:28:18.304	131.225.12.195	38446	131.225.204.211	1487	TCP	1/46	0
0624.14:28:20.160	131.225.12.194	52345	131.225.204.248	944	TCP	1/46	0
0624.14:28:20.160	131.225.12.194	52345	131.225.204.248	1399	TCP	1/46	0
0624.14:28:20.160	131.225.12.194	52345	131.225.204.248	783	TCP	1/46	0
0624.14:28:20.096	131.225.12.194	34620	131.225.204.204	6558	TCP	1/46	0
0624.14:28:20.160	131.225.12.194	52345	131.225.204.248	1543	TCP	1/46	0
0624.14:28:20.096	131.225.12.194	34620	131.225.204.204	1527	TCP	1/46	0
0624.14:28:18.304	131.225.12.194	47342	131.225.204.30	49	TCP	1/46	0
0624.14:28:19.328	131.225.12.195	42810	131.225.204.93	672	TCP	1/46	0
0624.14:28:19.328	131.225.12.195	42810	131.225.204.93	191	TCP	1/46	0
0624.14:28:20.160	131.225.12.194	52345	131.225.204.248	5400	TCP	1/46	0
0624.14:28:18.304	131.225.204.163	508	131.225.12.194	60800	TCP	1/46	0
0624.14:28:18.304	131.225.204.72	2603	131.225.12.195	46464	TCP	1/46	0
0624.14:28:18.304	131.225.204.218	897	131.225.12.193	62294	TCP	1/46	0

Stopped

TopScan: Generate tables of topN Scanners

TopScan –
on per origin basis
(onsite, offsite, local,
transit) generate tables
of top scanners for
specified time
intervals: 5min, 1hour,
1day.

Information is
available via
interactive GUI and by
E-Mail notifications

The screenshot shows a web browser window titled "Scan Viewer - SeaMonkey". The URL in the address bar is <https://fnadc4.fnal.gov/~netadmin/ft/scan/scanframes.html>. The page displays a "ScanView Menu at Wed Jun 20 16:22:35 2007 (CDT)" from Fermilab Data Communications and Networking. On the left, there is a configuration sidebar with fields for "Start(YYYYMMDDHH):" (set to 06/19/07 00:00:00), "topN" (set to 20), and buttons for "set" and "Defaults". Below these are sections for "Routers:" (r-s-bdr-loop (172.16.1.202)), "Origins:" (onsite, offsite), "Type of scanning:" (host), and "Select traffic for:" (Site show). Under "Searching for period:", there is a dropdown menu showing "1day" selected, with other options like "today", "yesterday", and dates from "06/19/07" to "06/12/07". There is also a "Ihour" option. The main content area is titled "Top 1 day Scanners SAB" and contains a table with the following data:

From	To	router	origin	period	type		
06/19/07 00:00:00	06/20/07 00:00:00	172.16.1.202	offsite	1day	host		
ipaddr	name		hostCount	octets	flows	packets	duration
213.63.185.11	mail.bertrand.pt		40434	4738944	40434	98728	84995
64.246.36.4	download12.contextplus.net		39985	1958888	40154	40688	84995
204.16.208.35	dedicated35.dedicatedservernec.com		39857	62640224	118862	118867	29101
64.27.29.102	ip-64.27.29.102.internetsecure.org		38402	2123552	38406	44463	84995
204.16.209.16			35921	23116886	43863	43872	29101
213.195.77.224	224.77.195.213.ibercom.com		35170	1947628	35175	40779	84995
84.159.105.145	p549F6991.dip.t-dialin.net		34910	2030666	35494	42386	84995
124.155.151.18	host-18.151-155-124.dynamic.totalbb.net.tw		33043	1983192	33043	33055	84995
222.14.140.135	ZR140135.ppp.dion.ne.jp		32697	3070493	33017	50470	84995
87.205.128.63	87-205-128-63.adsl.inetia.pl		32586	3291072	32613	53952	84995
221.142.147.136			32503	3131819	32677	51395	84995
71.200.106.195	c-71-200-106-195.hsd1.md.comcast.net		32491	3098190	32515	50790	84995
222.233.200.238			32451	2961672	32474	48552	84995
89.243.95.220			32450	3107560	32783	51080	84995
12.10.121.167			32416	3213297	32426	52677	29101
220.132.192.57	220-132-192-57.HINET-IP.hinet.net		32305	3346062	32729	55018	84995
124.52.19.166			32255	3069032	32255	50312	84995
201.35.197.91	201-35-197-91.fnsce703.dsl.brasiltelecom.net.br		32123	3620350	32164	59350	84995
64.181.109.126			32046	3746848	32085	61428	84995
200.149.163.13			31952	3214517	31963	52697	84995

The bottom status bar shows the URL <https://fnadc4.fnal.gov/~netadmin/ft/scan/scanview.cgi?topN=20&router=172.16.1.202&origin=offsite&yesterday=1>.

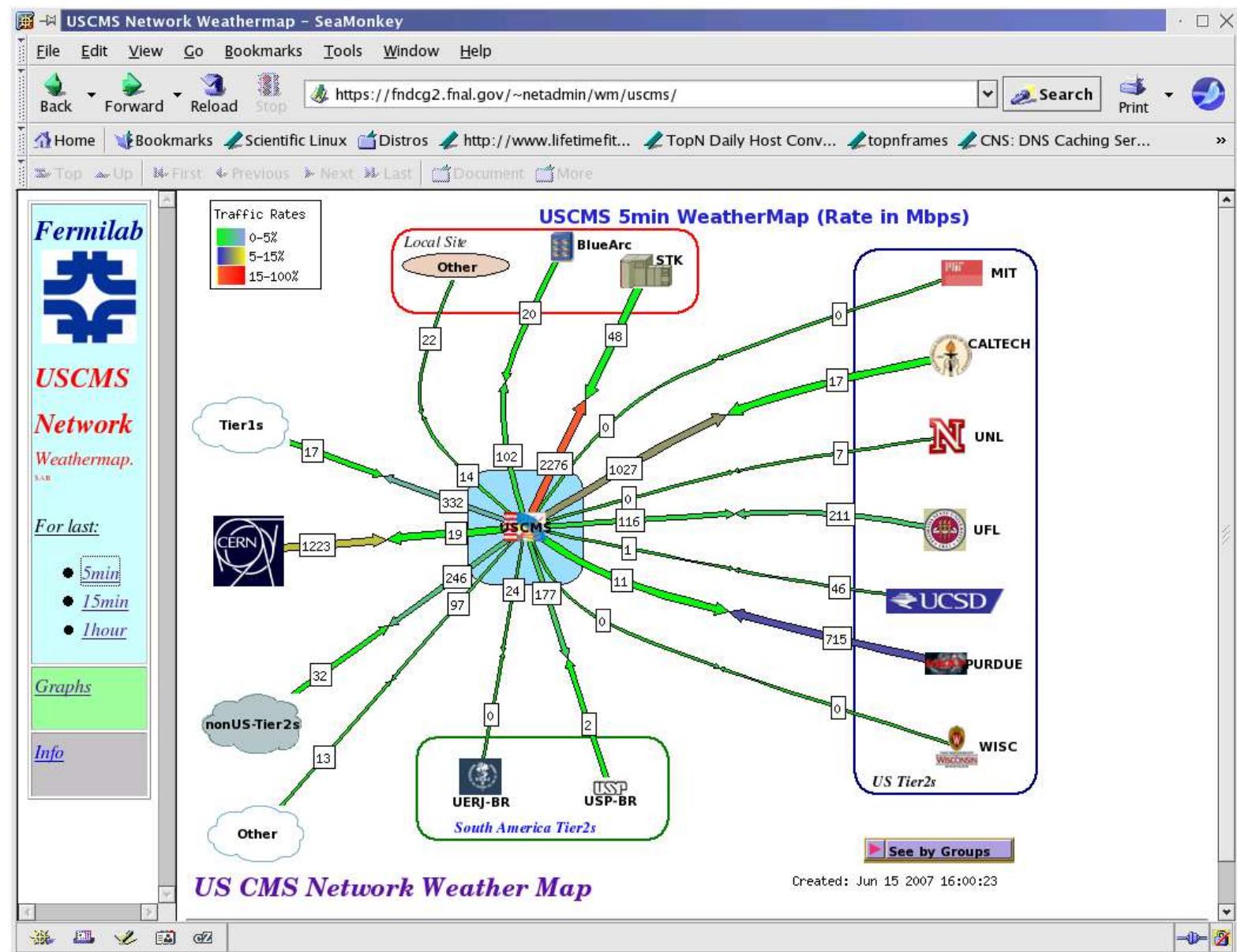
Performance Monitoring and Estimation tools

- USCMS Network Weather Map
- topN
- dotDisplay
- Traffic Summary (ftsumTraffic)
- Traffic asymmetry (bfpsum)
- multistreams

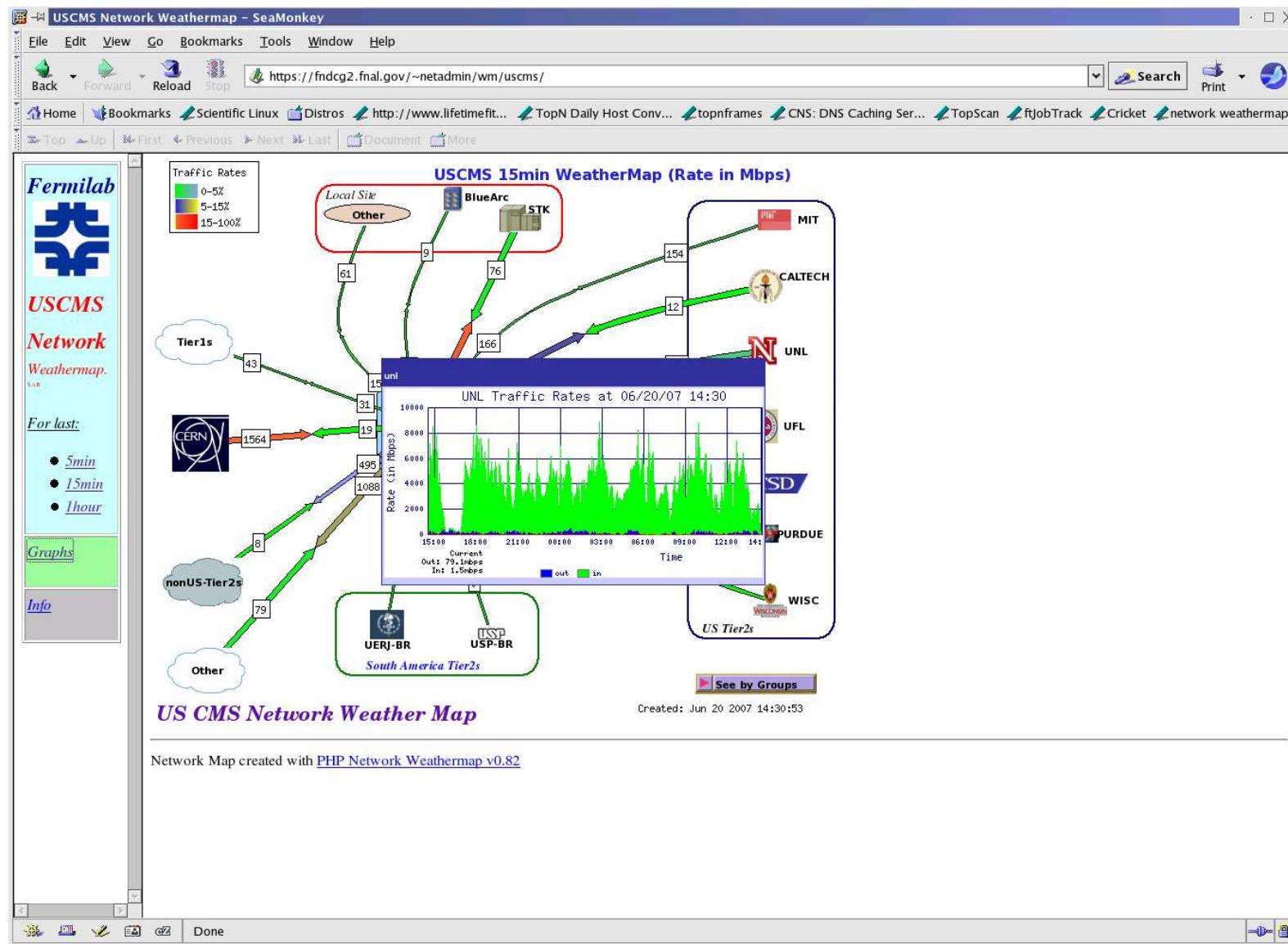
USCMS Network Weather Map

Show estimated rates to various sites: Tier0, other Tier1, USCMS Tier2.
Features:

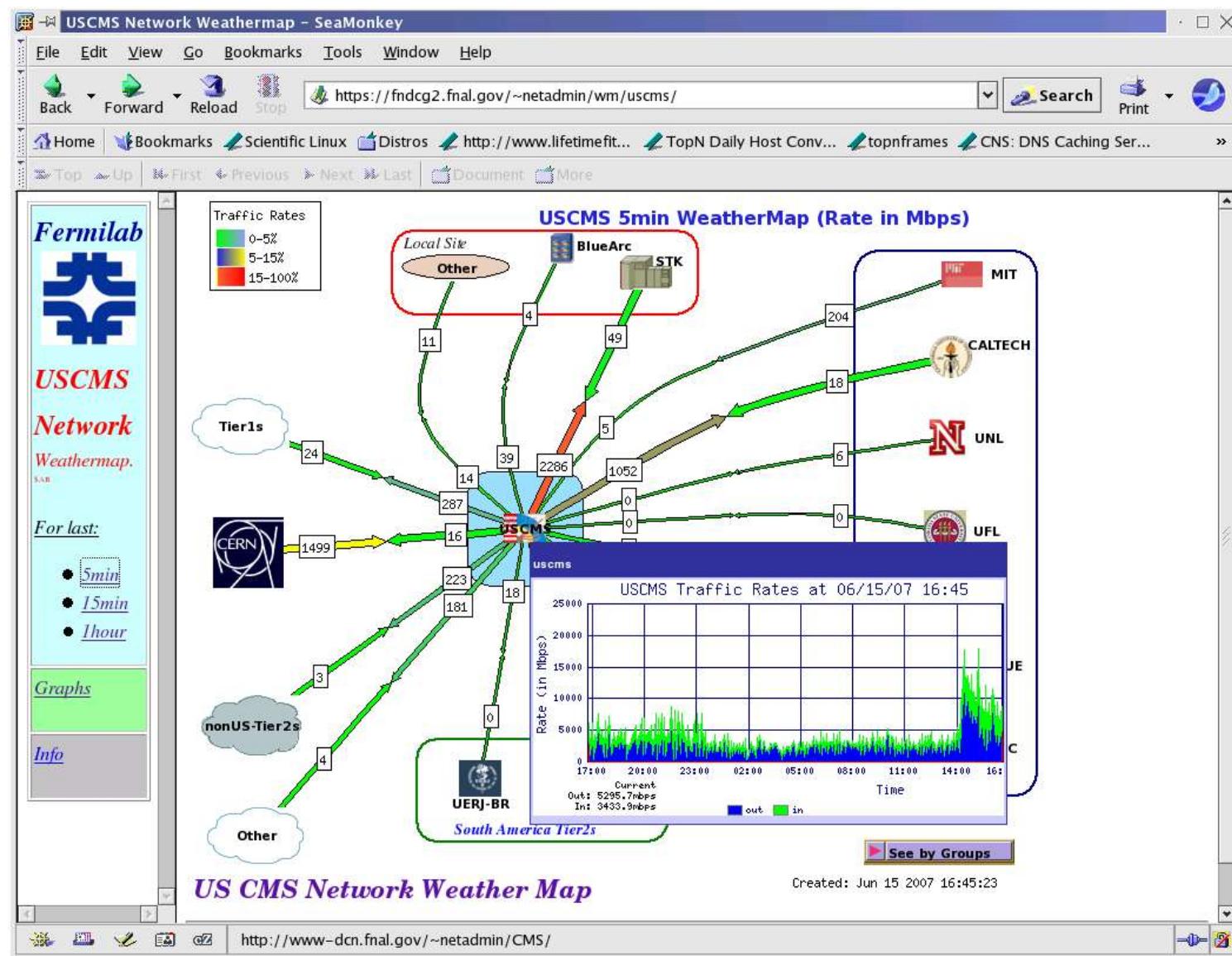
- popup graphs
- clickable icons to direct to other informational sources



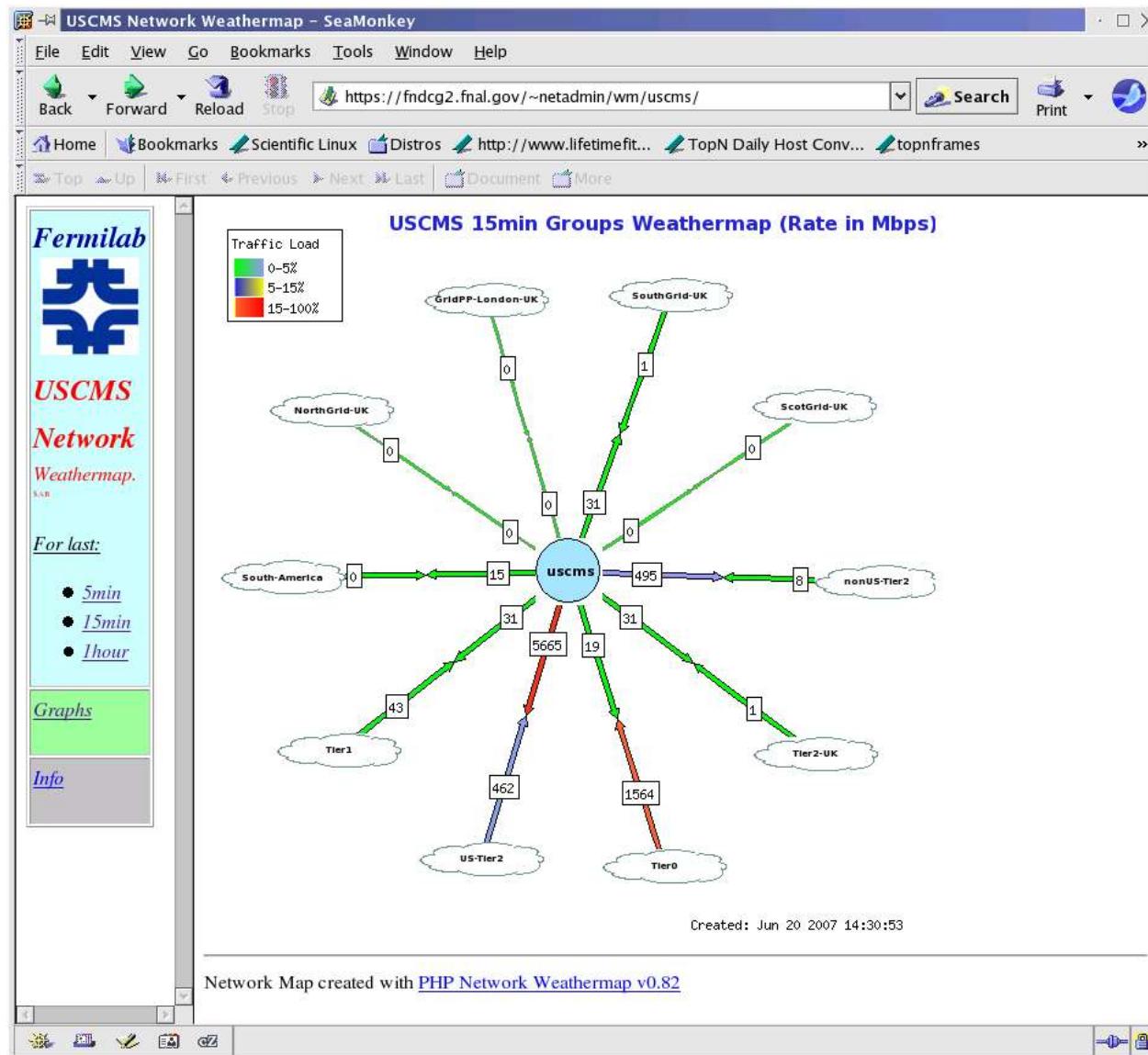
USCMS WM : popup graphs



USCMS WM: Popup graphs, 16Gbps



USCMS WM: Group's rates



USCMS WM: Clickable icons

Click on
BlueArc Icon:
hourly summary
tables for TopN
pairs, senders
and receivers

USCMS Network Weathermap – SeaMonkey

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop https://fndcg2.fnal.gov/~netadmin/wm/uscms/ Search Print

Home Bookmarks Scientific Linux Distros http://www.lifetimefit... TopN Daily Host Conv... topnframes

Top Up First Previous Next Last Document More

HOURLY Summary Table of Conversations at Wed Jun 20 14:34:08 2007 (CDT) SAB

router	origin	layout	knownSitesDef		dns level		
172.16.12.1	local	bluearc	NONE		Host		
ts	octets	Mbps	packets	Pps	flows	Fps	duration
2007-06-20 14:00:00	2054575325 <small>pair sender receiver</small>	27.39	2287527 <small>pair sender receiver</small>	3812.55	27769 <small>pair sender receiver</small>	46.28	600
2007-06-20 13:00:00	20398707894 <small>pair sender receiver</small>	49.45	21590000 <small>pair sender receiver</small>	6542.42	130753 <small>pair sender receiver</small>	39.62	3300
2007-06-20 12:00:00	53855832070 <small>pair sender receiver</small>	130.56	55354675 <small>pair sender receiver</small>	16774.14	151581 <small>pair sender receiver</small>	45.93	3300
2007-06-20 11:00:00	51921283776 <small>pair sender receiver</small>	125.87	53624404 <small>pair sender receiver</small>	16249.82	137584 <small>pair sender receiver</small>	41.69	3300
2007-06-20 10:00:00	54718584941 <small>pair sender receiver</small>	132.65	57672040 <small>pair sender receiver</small>	17476.38	130929 <small>pair sender receiver</small>	39.68	3300
2007-06-20 09:00:00	47432116084 <small>pair sender receiver</small>	114.99	48708983 <small>pair sender receiver</small>	14760.30	133762 <small>pair sender receiver</small>	40.53	3300
2007-06-20 08:00:00	14813365882 <small>pair sender receiver</small>	35.91	15952890 <small>pair sender receiver</small>	4834.21	159037 <small>pair sender receiver</small>	48.19	3300
2007-06-20 07:00:00	24368230950 <small>pair sender receiver</small>	59.07	26054278 <small>pair sender receiver</small>	7895.24	152158 <small>pair sender receiver</small>	46.11	3300
2007-06-20 06:00:00	34227839405 <small>pair sender receiver</small>	82.98	35427312 <small>pair sender receiver</small>	10735.55	163431 <small>pair sender receiver</small>	49.52	3300
2007-06-20 05:00:00	16205567504 <small>pair sender receiver</small>	39.29	17817555 <small>pair sender receiver</small>	5399.26	187342 <small>pair sender receiver</small>	56.77	3300
2007-06-20 04:00:00	23930973103 <small>pair sender receiver</small>	58.01	29954053 <small>pair sender receiver</small>	9076.99	195838 <small>pair sender receiver</small>	59.34	3300
2007-06-20 03:00:00	18930635555 <small>pair sender receiver</small>	45.89	25524118 <small>pair sender receiver</small>	7734.58	133166 <small>pair sender receiver</small>	40.35	3300
2007-06-20 02:00:00	17574646109	42.61	25790674 <small>pair sender receiver</small>	7815.36	128292 <small>pair sender receiver</small>	38.88	3300

Done

Fermilab
USCMS Network Weathermap
For last:
● 5min
● 15min
● 1hour
Graphs
Info

USCMS WM: TopN conversations

Tables of hourly topN senders, receivers and conversations

USCMS Network Weathermap - SeaMonkey

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop https://fnndcg2.fnal.gov/~netadmin/wm/uscms/ Search Print

Home Bookmarks Scientific Linux Distros http://www.lifetimefit... TopN Daily Host Conv... topnframes

Top Up First Previous Next Last Document More

Fermilab USCMS Network Weathermap. SAB

For last:

- 5min
- 15min
- 1hour

Graphs

Info

Top 20 HOURLY Conversations sorted by octets at Wed Jun 20 14:34:40

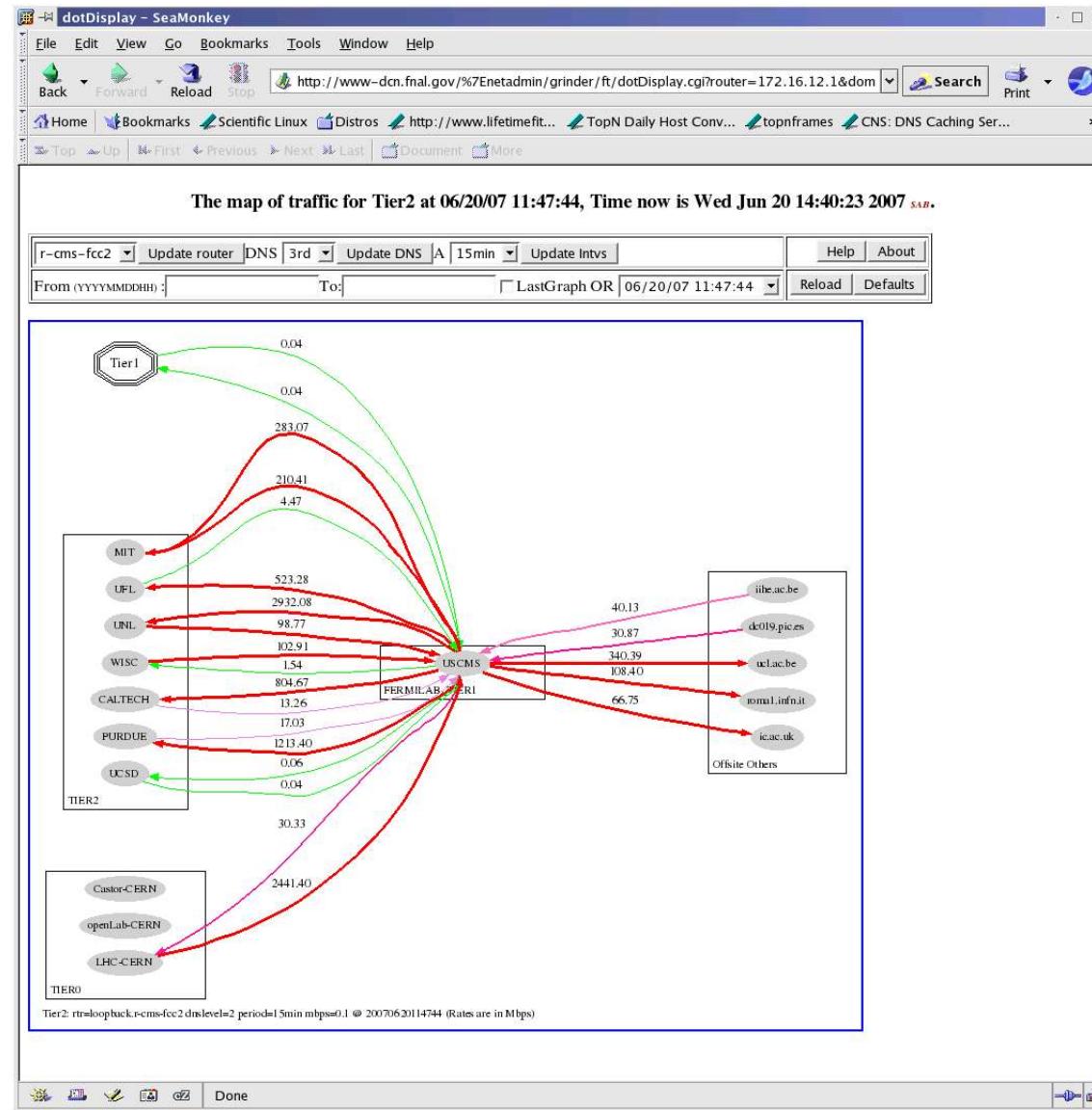
2007 (CDT) SAB

ts	router	origin	layout	knownSitesDef	dns level
06/20/07 14:00:00	172.16.12.1	local	bluearc	NONE	

src	dst	octets	Mbps	packets	Pps	flows	Fps	duration
blue2.fnal.gov	cmswn055.fnal.gov	448676146	11.96	303721	1012.40	16	0.05	300
onsite_other	blue2.fnal.gov	130219824	3.47	140813	469.38	6888	22.96	300
cmswn653.fnal.gov	blue2.fnal.gov	79864372	2.13	53422	178.07	75	0.25	300
cmswn640.fnal.gov	blue2.fnal.gov	76829294	2.05	51381	171.27	73	0.24	300
cmswn084.fnal.gov	blue2.fnal.gov	67416812	1.80	48748	162.49	84	0.28	300
cmswn076.fnal.gov	blue2.fnal.gov	55230850	1.47	40614	135.38	112	0.37	300
cmswn664.fnal.gov	blue2.fnal.gov	50187478	1.34	35845	119.48	71	0.24	300
cmswn067.fnal.gov	blue2.fnal.gov	48992256	1.31	51362	171.21	192	0.64	300
cmswn083.fnal.gov	blue2.fnal.gov	45014284	1.20	34242	114.14	227	0.76	300
cmswn672.fnal.gov	blue2.fnal.gov	36188180	0.97	24714	82.38	65	0.22	300
cmswn685.fnal.gov	blue2.fnal.gov	34209146	0.91	22912	76.37	55	0.18	300
cmswn645.fnal.gov	blue2.fnal.gov	30586324	0.82	20957	69.86	39	0.13	300
cmswn683.fnal.gov	blue2.fnal.gov	30340766	0.81	21238	70.79	78	0.26	300
cmswn681.fnal.gov	blue2.fnal.gov	29561766	0.79	20313	67.71	63	0.21	300
cmswn638.fnal.gov	blue2.fnal.gov	28565294	0.76	20097	66.99	65	0.22	300
cmswn605.fnal.gov	blue2.fnal.gov	26584400	0.71	18342	61.14	74	0.25	300
cmswn667.fnal.gov	blue2.fnal.gov	26134550	0.70	18468	61.56	58	0.19	300

dotDisplay: previous USCMS WM

dotDisplay:
Show traffic
rates for
statically defined
sites. All other
sites are
identified
dynamically by
specified DNS
levels.

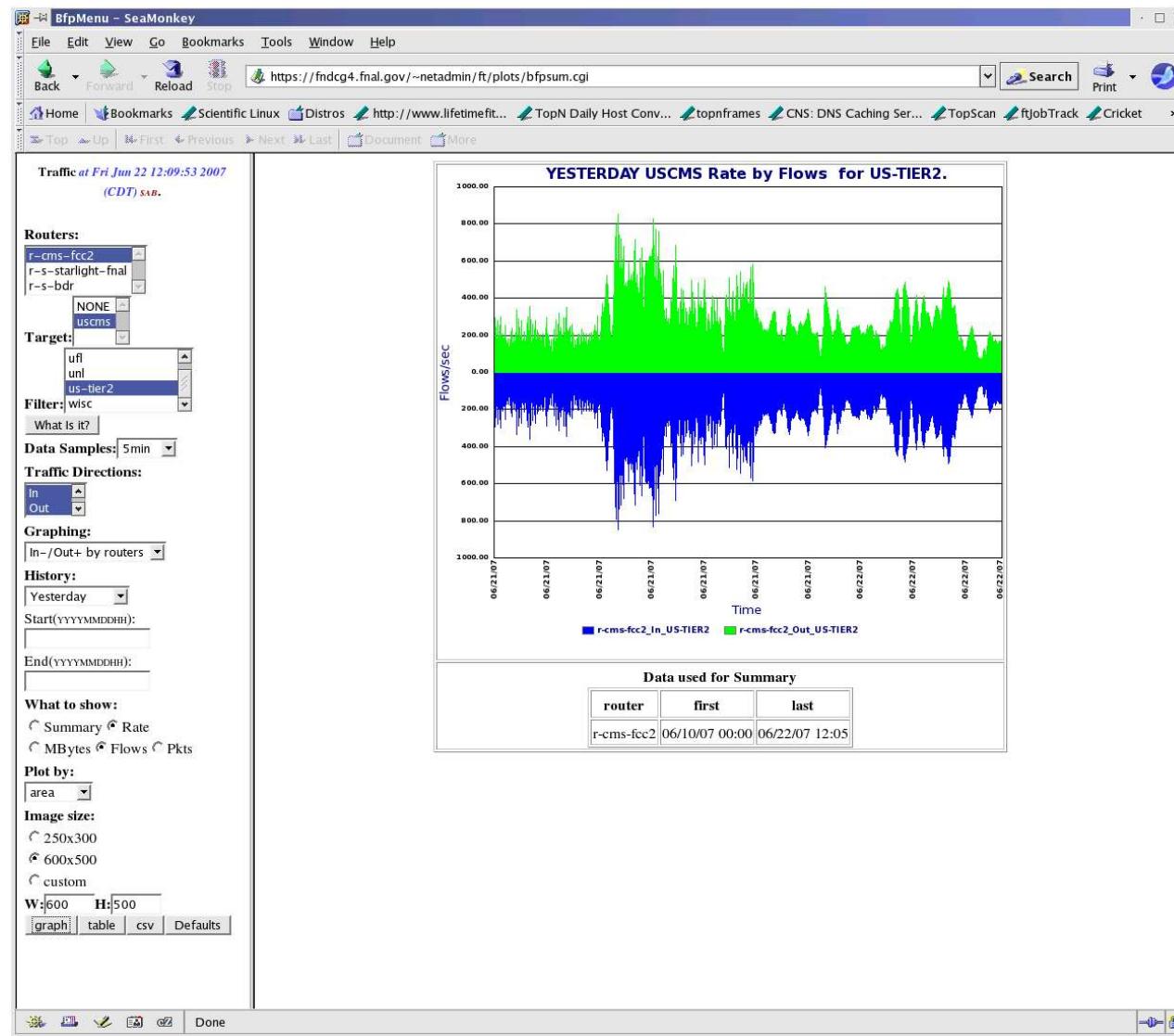


bfpsum: ByteFlowPacket Summary

bfpsum allows to build graphs and tables for traffic of specified targets, such as USCMS to the various remote sites.

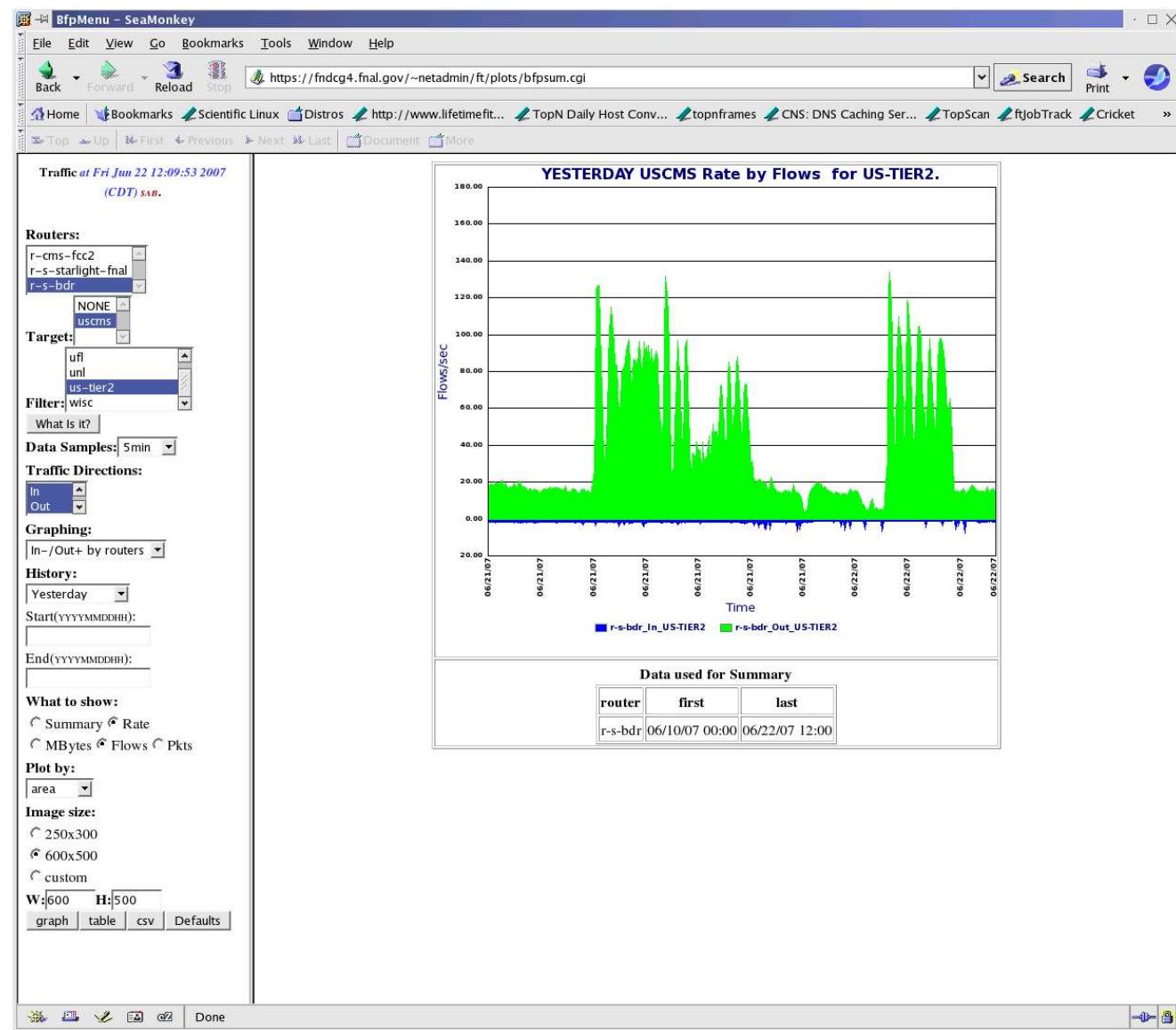
Single or multiple routers can be selected as well as multiple targets and filters.

Traffic can be seen in the terms of bytes, flows and packets. Both rates or amount can be seen.



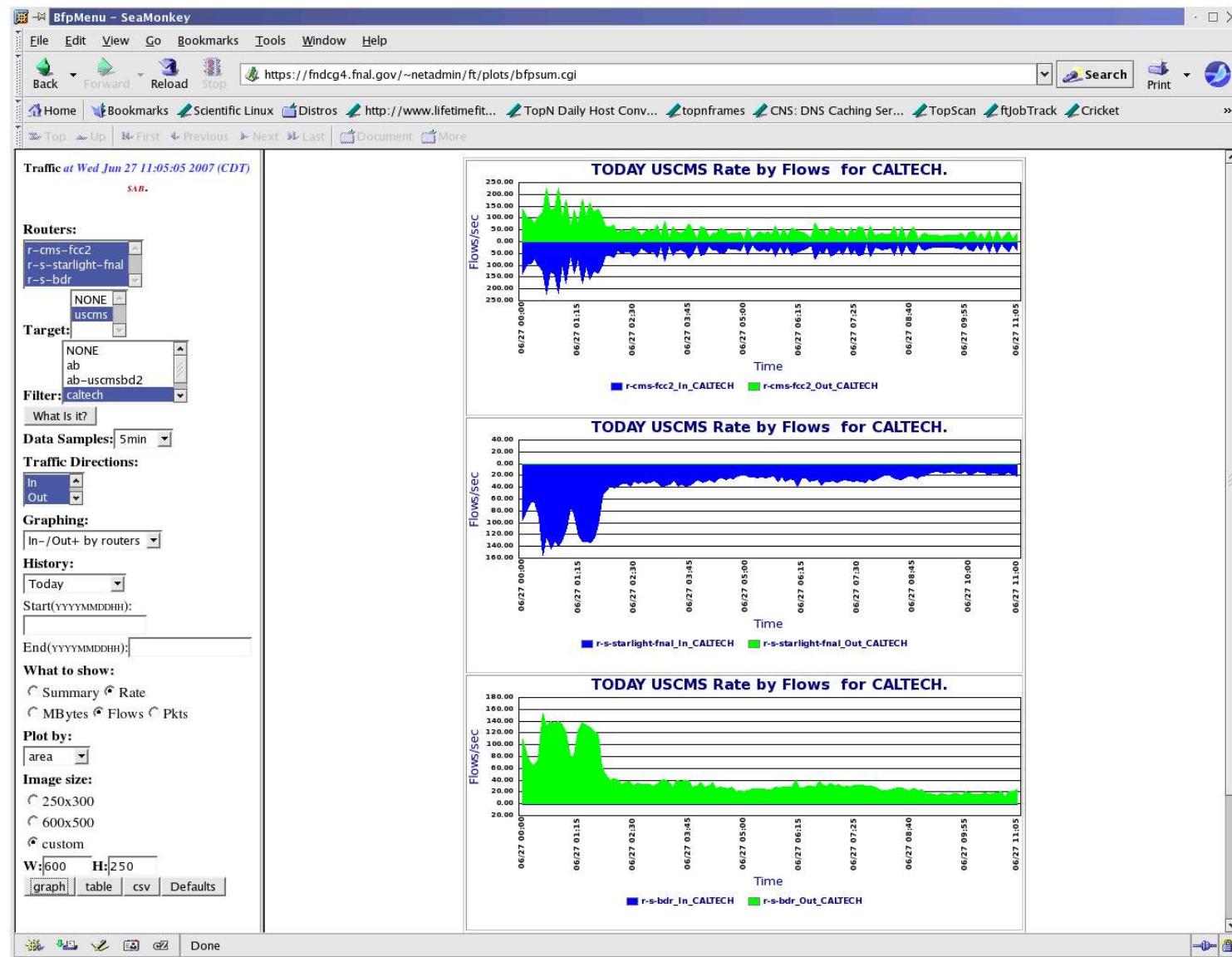
bfpsum: Verifying symmetry of PBR-ed traffic

This tool is used for interactive inspection of USCMS PBR-ed traffic to detect potential asymmetry. When traffic is symmetric flow rates of inbound and outbound traffic is practically the same (see graph on the previous slide). An example of traffic asymmetry is graph on this slide (caused by Caltech when LS was shutdown and outbound traffic was going through the core network).

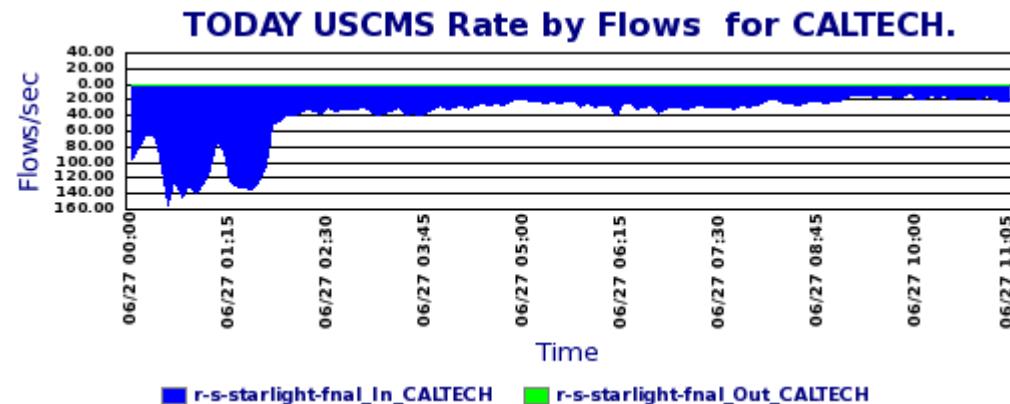
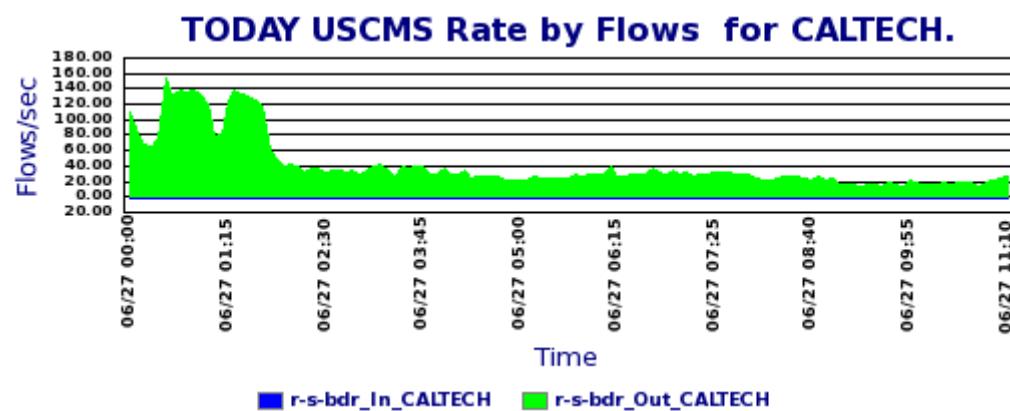
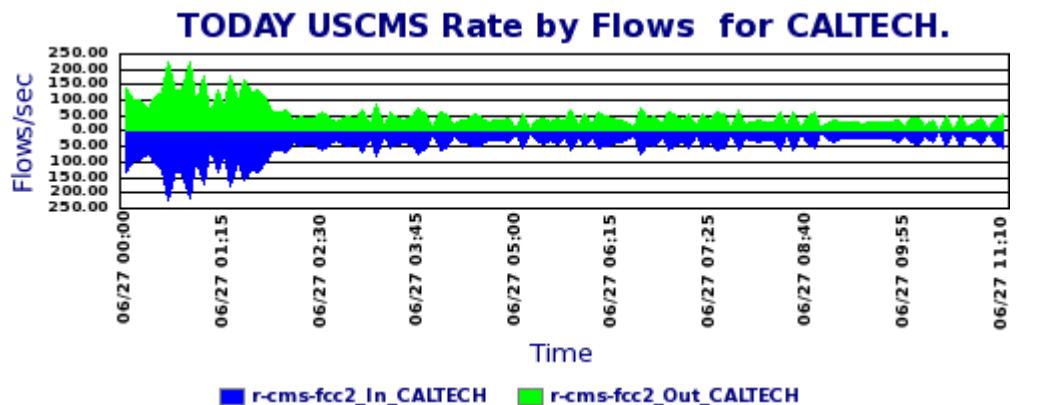
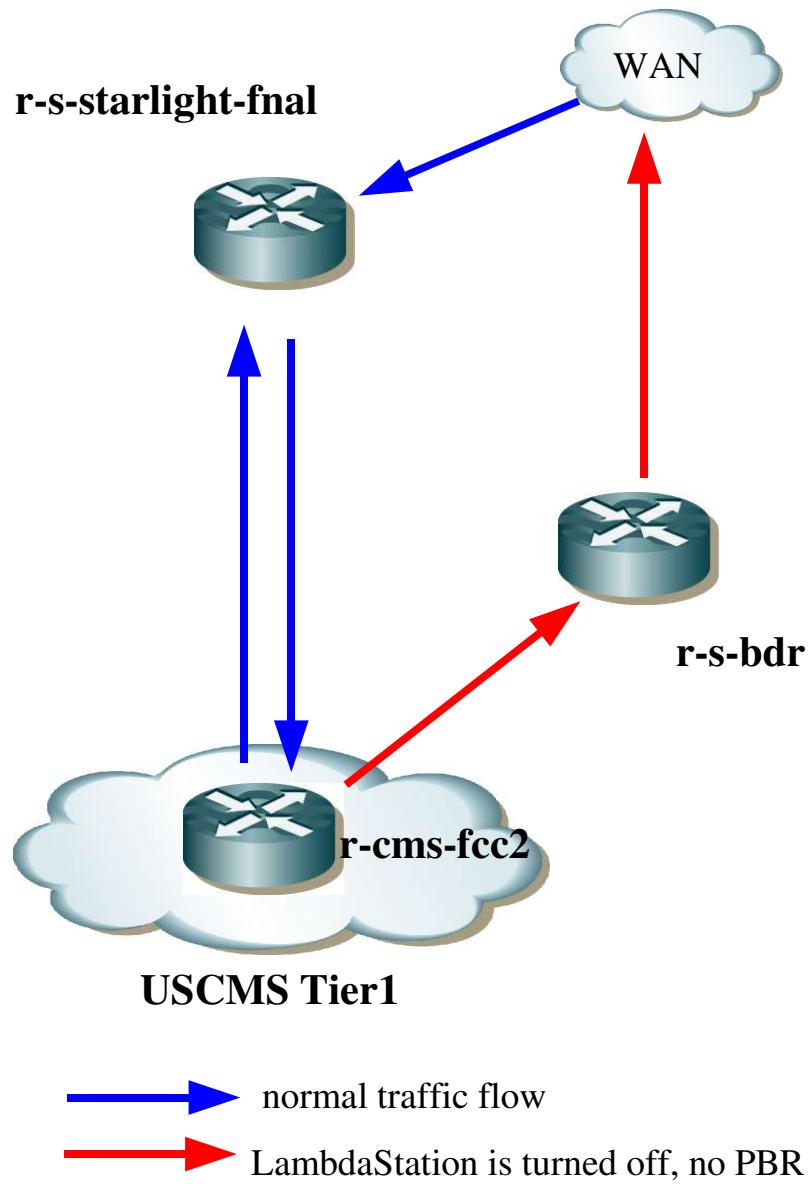


bfpsum: Caltech Traffic Asymmetry Test

Selected filter
“caltech” and
multiple
routers



Test: detection of traffic asymmetry



Detection of multistreams GridFTP sessions

ftGftp: detects and estimates transfer rates for multistreams gridFTP sessions.
Traffic specific remote sites could be selected first before passing it to the detector.

MultiStreams to HTML Table - SeaMonkey												
http://www-dcn.fnal.gov/~netadmin/ft/nph-MultiStreams2table.cgi?dns=1&dir=UNL/r-cms-fcc2/2007-06-26&fi												
Home Bookmarks Scientific Linux Distros http://www.lifetimefit... TopN Daily Host Conv... topnframes CNS: DNS Caching Ser... TopScan ftJobTrack												
Top Up First Previous Next Last Document More												
Fermilab Data Communications and Networking												
167 sessions(61 aggregated) with MultiStreams found since 06/26/07 12:23:01 until 06/26/07 12:29:12												
Source Host	Destination Host	SessionID	Number of Streams	Bytes	Packets	Flows	Mbps	Pps	Start	End	Duration (msecs)	
Stream Index	SrcPort	DstPort	Protocol	Bytes	Packets	Flows	Mbps	Pps	Start	End	Duration (msecs)	
131.225.205.219 (cmsstor97)	129.93.239.138 (dcache03.unl.edu)	1:31	10	2819551717	1918000	20	230.069	20032	12:24:39.893	12:26:15.637	95744	
1	47651	20002	tcp	281912118	191845	2	23.004	2003	12:24:39.894	12:26:15.637	95743	
2	47652	20002	tcp	282209879	191721	2	23.028	2002	12:24:39.894	12:26:15.637	95743	
3	47653	20002	tcp	281884531	191890	2	23.001	2004	12:24:39.893	12:26:15.637	95744	
4	47655	20002	tcp	281865777	191848	2	23.015	2005	12:24:39.957	12:26:15.637	95680	
5	47656	20002	tcp	281952573	191784	2	23.022	2004	12:24:39.957	12:26:15.637	95680	
6	47658	20002	tcp	281782087	191736	2	23.024	2005	12:24:40.23	12:26:15.637	95614	
7	47659	20002	tcp	281955720	191944	2	23.038	2007	12:24:40.23	12:26:15.637	95614	
8	47654	20002	tcp	281957786	191687	2	23.023	2003	12:24:39.957	12:26:15.637	95680	
9	47657	20002	tcp	282075062	191856	2	23.048	2006	12:24:40.23	12:26:15.637	95614	
10	47660	20002	tcp	281956184	191689	2	23.038	2004	12:24:40.23	12:26:15.637	95614	
131.225.205.219 (cmsstor97)	129.93.239.138 (dcache03.unl.edu)	10:21	10	2820344759	1917579	20	229.671	19987	12:24:39.254	12:26:15.191	95937	
1	47646	20001	tcp	281977209	191698	2	22.978	1999	12:24:39.318	12:26:15.190	95872	
2	47647	20001	tcp	282104735	191805	2	23.004	2001	12:24:39.318	12:26:15.125	95807	
3	47649	20001	tcp	282035736	191619	2	23.013	2001	12:24:39.382	12:26:15.126	95744	
4	47643	20001	tcp	281958974	191781	2	22.977	2000	12:24:39.254	12:26:15.126	95872	
5	47650	20001	tcp	281952399	191599	2	22.991	1999	12:24:39.381	12:26:15.191	95810	
6	47648	20001	tcp	282112058	191861	2	23.020	2003	12:24:39.382	12:26:15.125	95743	
7	47641	20001	tcp	282204811	191799	2	22.996	2000	12:24:39.254	12:26:15.127	95873	

Commercial Products

- AdventNet Netflow Analyzer
- NetFlow Tracker from Crannog-Software

Most packages have similar capabilities, many useful features, however does not cover all our needs and not flexible enough to customize it.

Purchased AdventNet , ~\$1K for 20 interfaces, allows to define IP groups based on the list of IP blocks

ManageEngine NetFlow Analyzer 5 - SeaMonkey

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://fnblack:8080/netflow/jspui/index.jsp Search Print

Home Bookmarks Scientific Linux Distros http://www.lifetimefit... TopN Daily Host Conv... topnframes CNS: DNS Caching Ser... TopScan ftJobTrack Cricket network weathermap

Top Up First Previous Last Document More

Global View Listening for NetFlow Packets at Port 9996,9997,9998

All Devices - Dashboard View

Interface View Autonomous System View Custom Report Troubleshoot Quick View NBAR Report

Router List

Router Name	Traffic Details - Last 1 Hour [Show All] [Hide All] [Filter]				
	Interface Name	Status	IN Traffic	OUT Traffic	Alerts
r-cms-fcc2	frontierLAN	✓	<div style="width: 1%;">1%</div> 65.71 Mbps	<div style="width: 0%;">0%</div> 857.76 Kbps	-
Router IP: 172.16.12.1	IfIndex449	-	<div style="width: 0%;">0%</div> 0.00 bps	<div style="width: 0%;">0%</div> 0.00 bps	-
NetFlow Packets Rcvd: 91550090	IfIndex450	✓	<div style="width: 100%;">+100%</div> 1699.04 Mbps	<div style="width: 0%;">0%</div> 644.12 bps	-
NBAR Support: UnKnown	IfIndex453	✓	<div style="width: 8%;">8%</div> 75.58 Kbps	<div style="width: 0%;">0%</div> 4.97 Kbps	-
	r-s-hub-fcc	✓	<div style="width: 2%;">2%</div> 209.63 Mbps	<div style="width: 41%;">41%</div> 4070.41 Mbps	-
	StarLight	-	<div style="width: 0%;">0%</div> 0.00 bps	<div style="width: 0%;">0%</div> 0.00 bps	-
	VI207	✓	<div style="width: 41%;">41%</div> 4071.14 Mbps	<div style="width: 20%;">20%</div> 1973.25 Mbps	-
2 Interface(s)					
r-s-bdr.fnal.gov					
r-s-starlight-fnal.fnal.gov			9 Interface(s)		

IP Group List [View Description]

IP Group Name	IN Traffic (Last 1 Hour)	OUT Traffic (Last 1 Hour)	Quick View
BlueArc [View Description]	<div style="width: 1%;">1%</div> 69.41 Mbps	<div style="width: 1%;">1%</div> 116.94 Mbps	[View]
Caltech [View Description]	<div style="width: 0%;">0%</div> 196.53 Kbps	<div style="width: 0%;">0%</div> 276.61 Kbps	[View]
DESY [View Description]	<div style="width: 0%;">0%</div> 13.97 Kbps	<div style="width: 0%;">0%</div> 12.49 Kbps	[View]
MIT [View Description]	<div style="width: 3%;">3%</div> 338.98 Mbps	<div style="width: 0%;">0%</div> 4.58 Mbps	[View]
PURDUE [View Description]	<div style="width: 1%;">1%</div> 55.4 Mbps	<div style="width: 0%;">0%</div> 715.53 Kbps	[View]
STK [View Description]	<div style="width: 1%;">1%</div> 94.77 Mbps	<div style="width: 0%;">0%</div> 3.45 Mbps	[View]
UCSD [View Description]	<div style="width: 0%;">0%</div> 0.00 bps	<div style="width: 0%;">0%</div> 0.00 bps	[View]
UERJ-BR [View Description]	<div style="width: 0%;">0%</div> 344.65 bps	<div style="width: 0%;">0%</div> 338.84 bps	[View]
UFL [View Description]	<div style="width: 12%;">12%</div> 1249.86 Mbps	<div style="width: 0%;">0%</div> 10.85 Mbps	[View]
UNL [View Description]	<div style="width: 20%;">20%</div> 1994.56 Mbps	<div style="width: 0%;">0%</div> 23.28 Mbps	[View]
USCAMS [View Description]	<div style="width: 1%;">1%</div> 208.75 Mbps	<div style="width: 20%;">20%</div> 4070.82 Mbps	[View]
USCAMS-SL [View Description]	<div style="width: 0%;">0%</div> 0.00 bps	<div style="width: 0%;">0%</div> 0.00 bps	[View]
USP-BR [View Description]	<div style="width: 0%;">0%</div> 0.00 bps	<div style="width: 0%;">0%</div> 0.00 bps	[View]
WISC [View Description]	<div style="width: 0%;">0%</div> 959.0 Kbps	<div style="width: 1%;">1%</div> 63.18 Mbps	[View]

Generated Alerts

- Last Hour 0 0 0
- All Alerts 0 0 0

Admin Operations

- Alert Profile Management
- Schedule Reports
- NBAR Configuration
- Device Group Management
- IP Group Management
- User Management
- Application Mapping
- Settings
- License Management

Copyright © 2004 - 2006 AdventNet Inc.