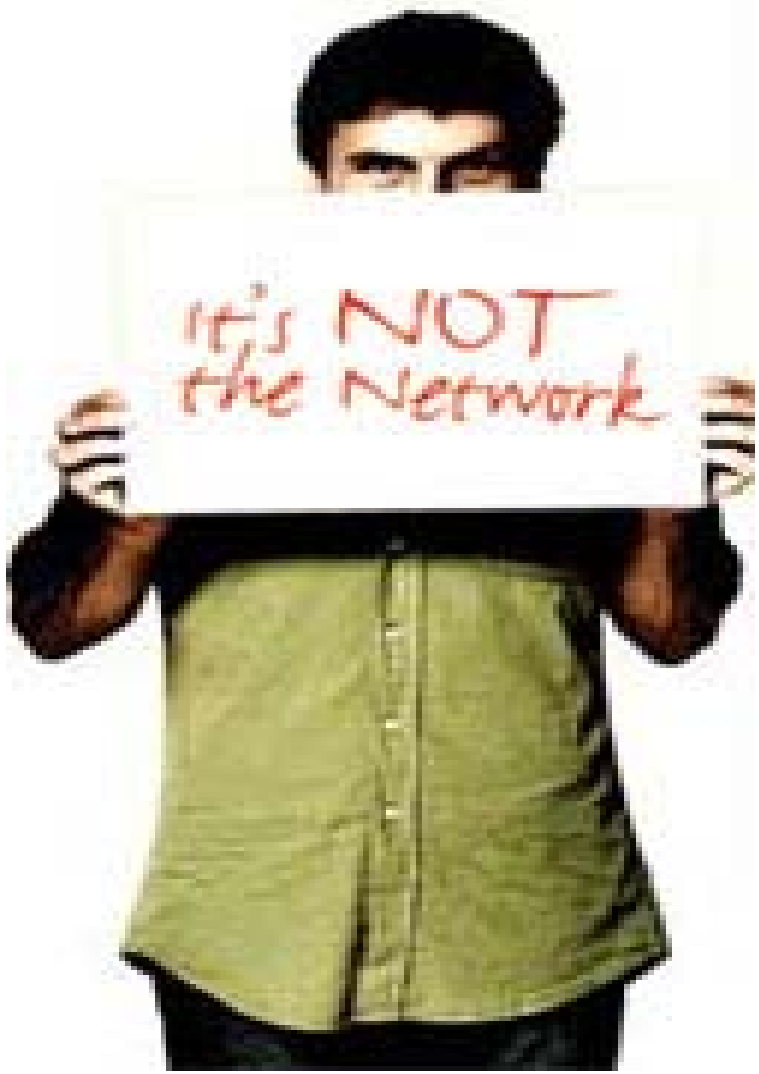
CRANNOGSOFTWARE

NetFlow Tracker Overview

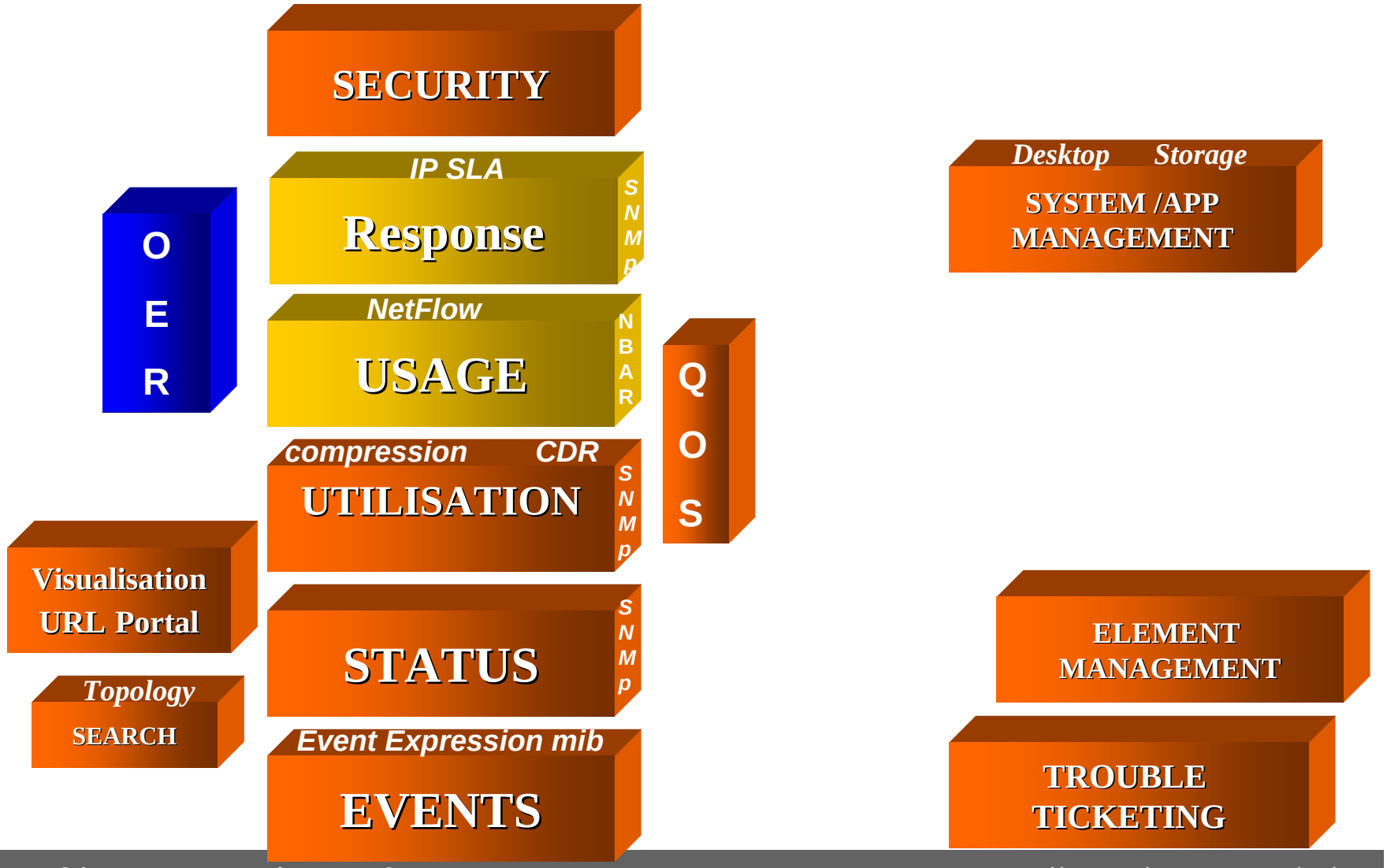
Mike McGrath x ccie
CTO
mike@crannog-software.com

2006


It's NOT
the Network

CRANNOGSOFTWARE

LEVELS OF NETWORK MANAGEMENT



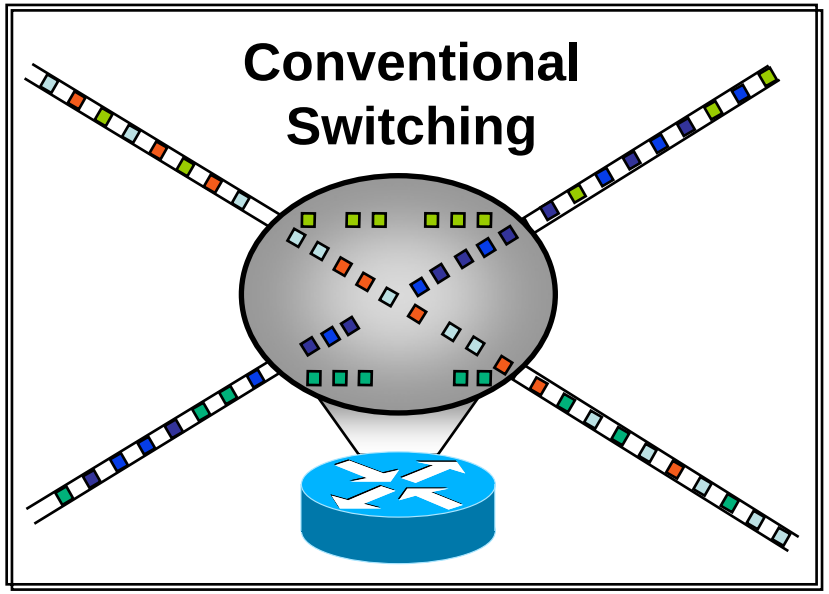
NetFlow As A Technology

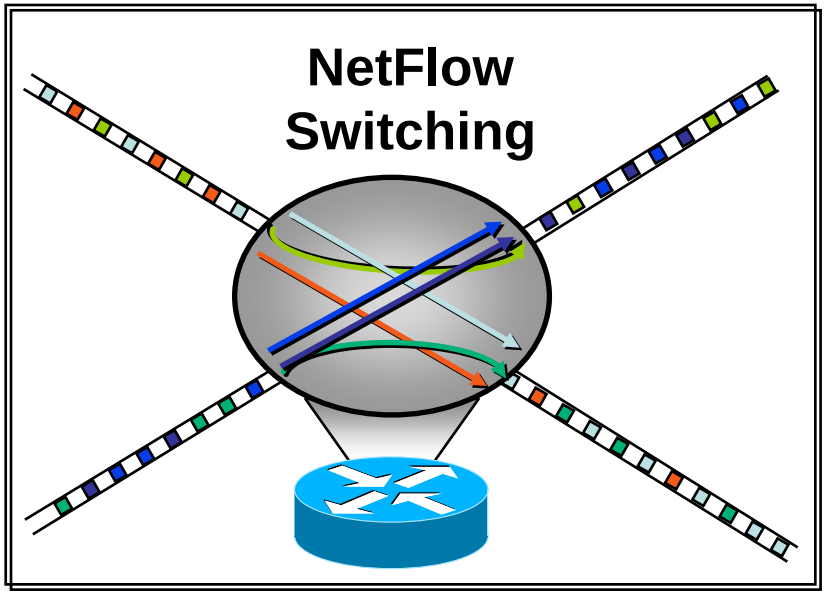
NetFlow – Past, Present, Future…

- Past (1996)
  - Overhead on devices/network
  - Treacherous to turn “data” into information (collection/presentation)
- Present
  - Improved memory management
  - Availability of NetFlow Analysis Tools
  - V5, V7(Catalyst), V9 (“templates”), Almost all Routers and Catalyst switches 45XX, 55XX, 6XXX.
  - Emerging Industry Adoption – Peribit, Juniper (J-flow, Cflow), Huawei Enterasys, Alcatel
- Future (Near)
  - IPFIX (IP Flow Information Export) V9 Chosen as basis for IPFIX by IETF (Internet Engineering Task Force)
  - Increased vendor adoption
  - Continued improvement in tools

NetFlow Switching

•Cisco **NetFlow**: originally designed as switching speedup.
The value of information in the cache was a later discovery

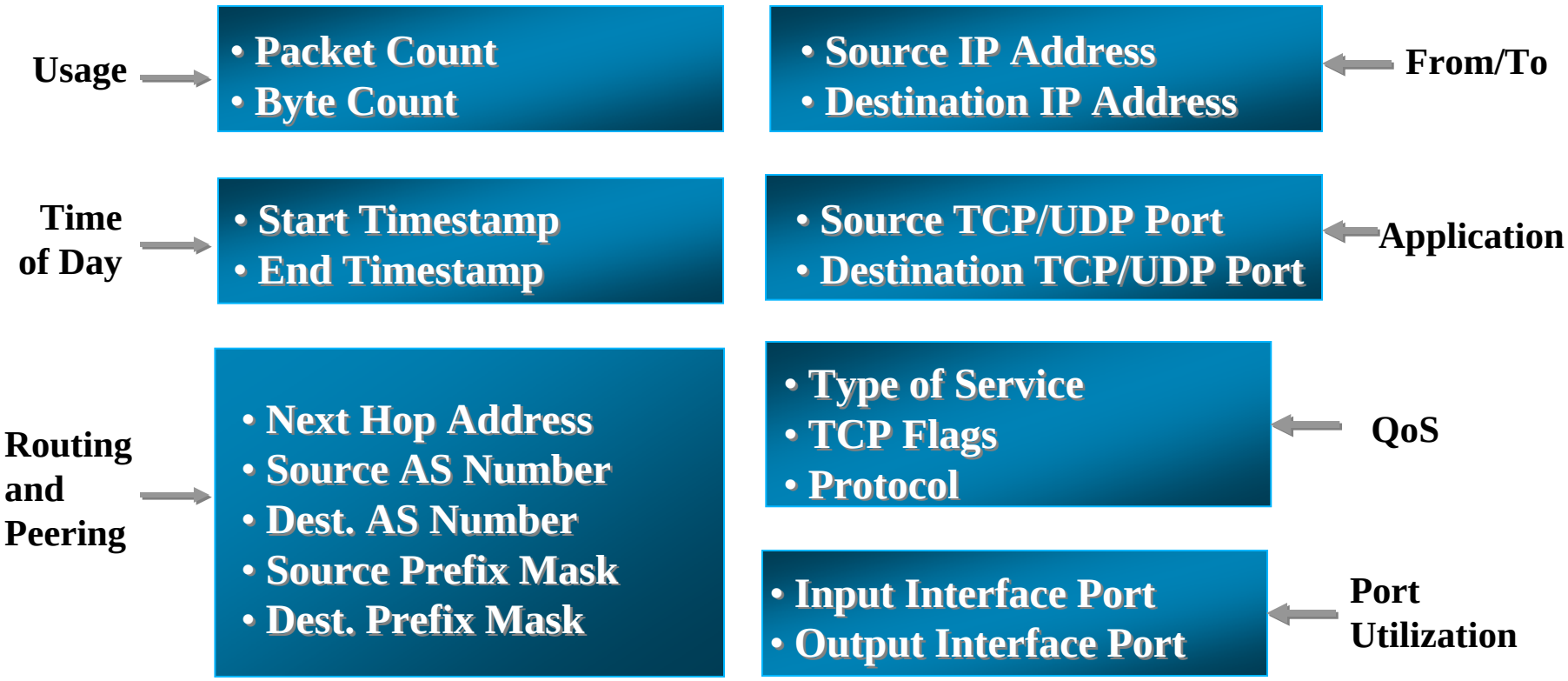




- **Each packet handled individually**
- **Each service applied sequentially by multiple tasks for each packet**
- **No ‘state’ information**

- **Packets handled as identified network flows**
- **Services applied by single task on per flow basis**
- **Flow ‘state’ information maintained**

What does NetFlow "look like" (v5 Export Format)



Version 5 used extensively today

How is the NetFlow Information Used

Statistics

- Packet Count
- Byte Count

- Start Timestamp
- End Timestamp

Routing

- Next Hop Address
- Source AS Number
- Dest. AS Number
- Source Prefix Mask
- Dest. Prefix Mask

Flow Identification

- Source IP Address
- Destination IP Address

- Source TCP/UDP Port
- Destination TCP/UDP Port

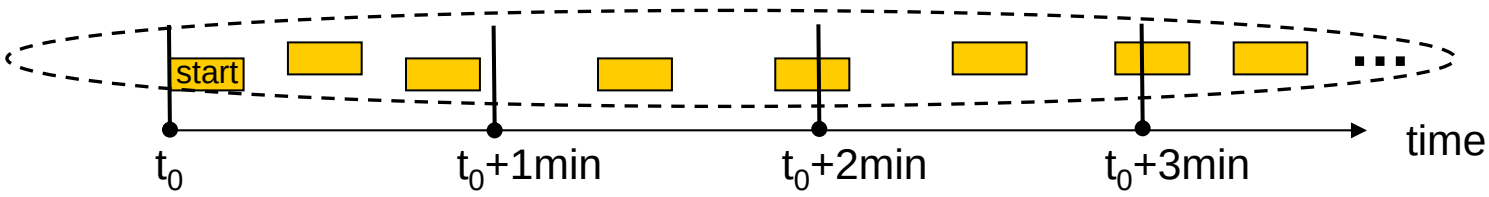
- Type of Service
- TCP Flags
- Protocol

- Input Interface Port
- Output Interface Port

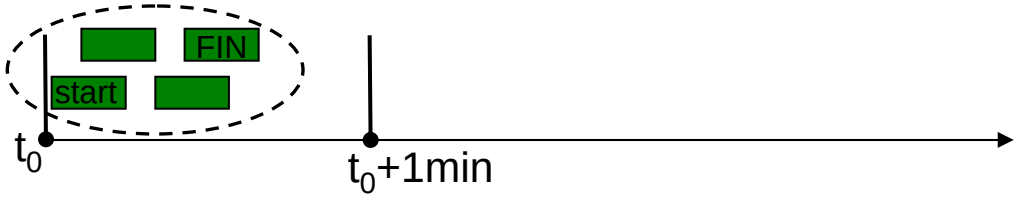
IP Flows and their monitoring

- **IP Flows are groups of IP packets sharing a common characteristic**

Flows can be long lasting...



… or have a limited lifetime...



Export flow information-when?

At flow end ?

Periodically ?

NetFlow Tracker Overview

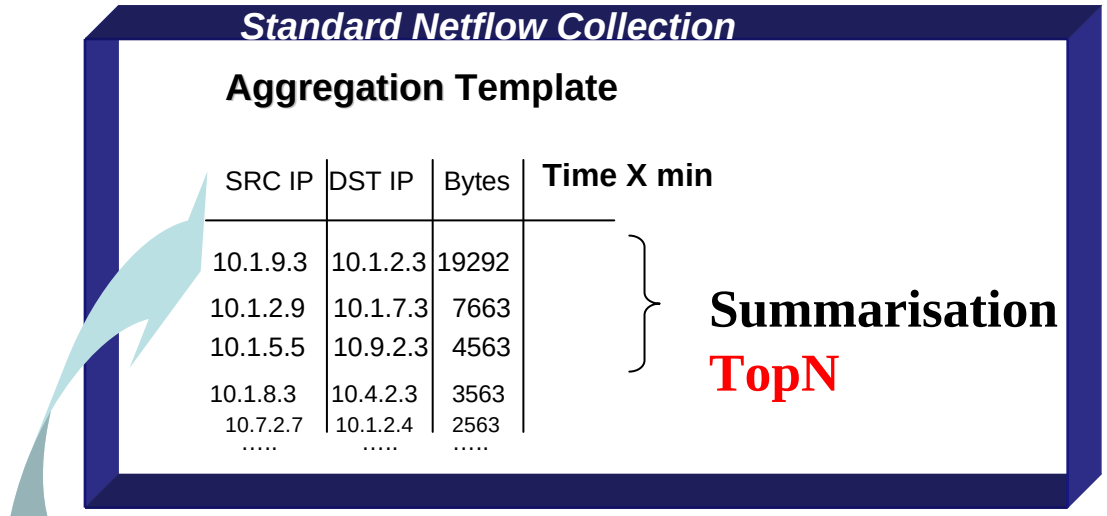
Why destroy relationship and drop netflow data ??

Netflow Record Contains

Src/Dst Interface
Src/Dst IP Address
Src/Dst Application Port
Src/Dst AS
Src/Dst Network Mask
TOS
Protocol
Next Hop Address
Next BGP Hop address

Class Id
Service Id

Byte/Packet counts



SRC IP	DST IP	Bytes
10.1.9.3	10.1.2.3	1563
10.1.9.3	10.1.2.3	7663
10.1.9.3	10.1.2.3	4002
10.1.9.3	10.1.2.3	3563
10.1.9.3	10.1.2.3	2501

Aggregation of fields in records creates totals against objects destroying relationship in record

Summarization takes TopN of aggregation and drops the rest

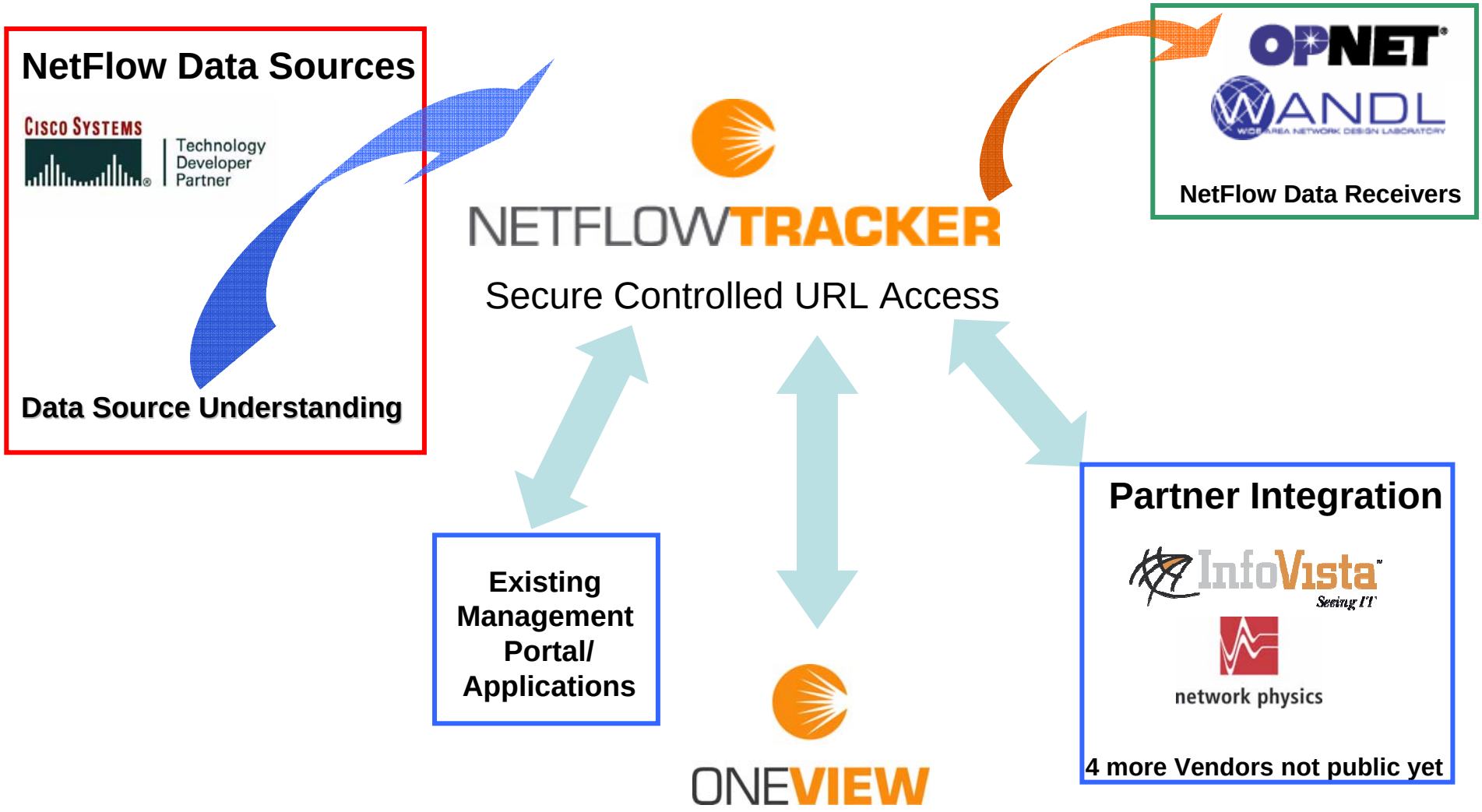
NetFlow Tracker - What does it do

- **Provides reports on network traffic usage**
- **Uses NetFlow records as its source of traffic information**
- **Provides a 100% web based solution**
- **Single server acts as the collector and the reporting engine**
- **Provides authorised access to reports via any web based portal.**
- **Enables differentiated levels of access.**

NetFlow Tracker – Why is it different?

- **All the Network, all the Flows, all the Fields. all of the Time**
- **Filter on any/all fields during reporting**
- **Both real-time and historical reporting “on-board”**
- **3rd party support extended fields (traffic class and service id)**
- **Fully URL controllable (Integration, automation)**
- **Licensing (not server or interface based!!)**

NetFlow Tracker – **Collector of Choice**

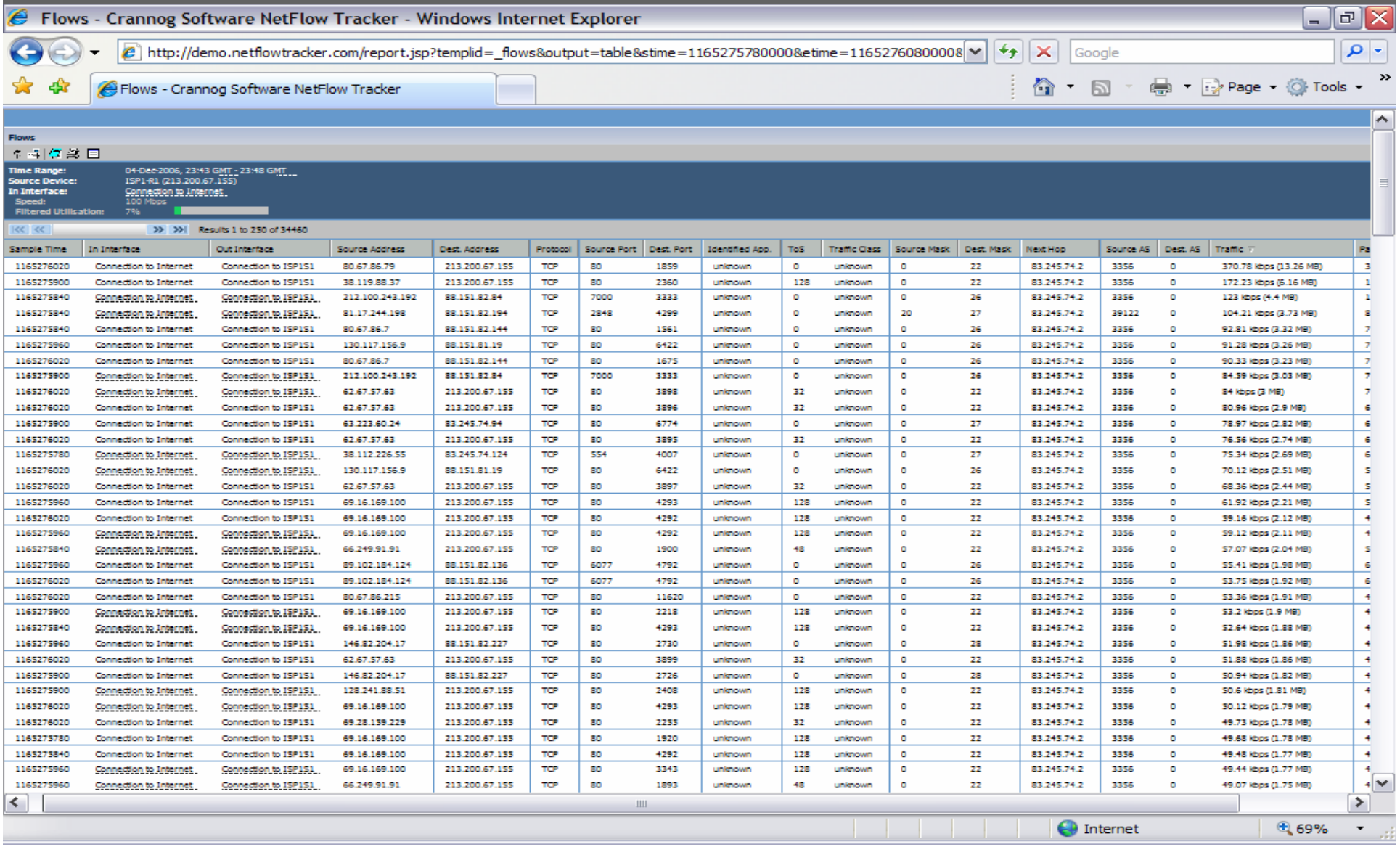


To be Collector of Choice requirements

- **Data Source**
  - **Understand data source environment to allow completeness of records**
  - **Minimise/remove replication**
  - **Use SNMP to complete fields and definitions**
- **Collection**
  - **Collect store present ALL records per minute real time**
  - **Retain field relationship to deliver “drill thru”**
- **Integration**
  - **Provide simple direct access from other Vendor applications plus private portals**
  - **Allow for controlled secure integration**

CRANNOGSOFTWARE

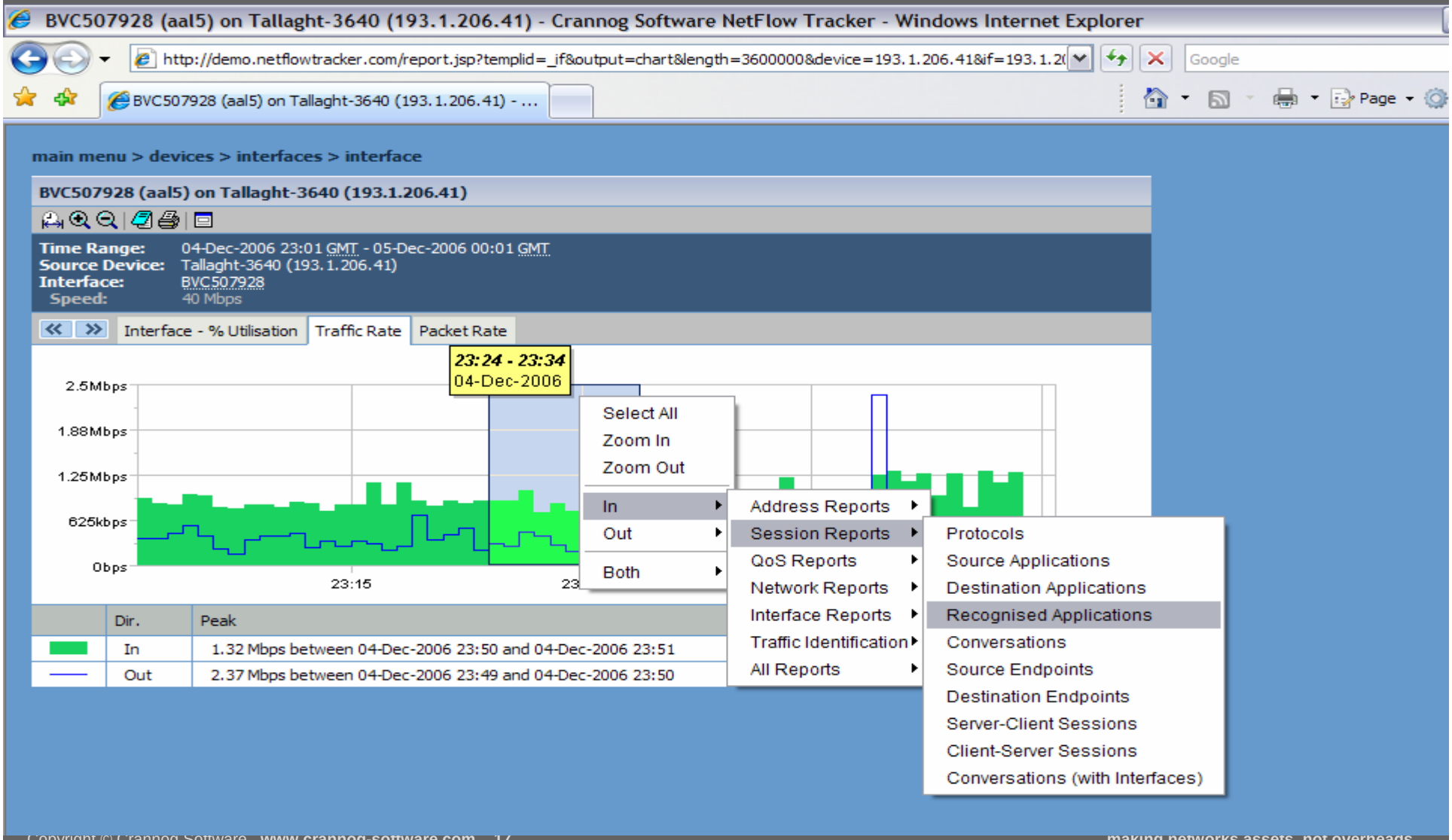
Full Flow Fields no aggregation



Sample Time	In Interface	Out Interface	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	Identified App.	ToS	Traffic Class	Source Mask	Dest. Mask	Next Hop	Source AS	Dest. AS	Traffic
1165276020	Connection to Internet	Connection to ISP1S1	80.67.86.79	213.200.67.155	TCP	80	1859	unknown	0	unknown	0	22	83.245.74.2	3356	0	370.78 kbps (13.26 MB)
1165275900	Connection to Internet	Connection to ISP1S1	38.119.88.37	213.200.67.155	TCP	80	2360	unknown	128	unknown	0	22	83.245.74.2	3356	0	172.23 kbps (6.16 MB)
1165275840	Connection to Internet	Connection to ISP1S1	212.100.243.192	88.151.82.84	TCP	7000	3333	unknown	0	unknown	0	26	83.245.74.2	3356	0	123 kbps (4.4 MB)
1165275840	Connection to Internet	Connection to ISP1S1	81.17.244.198	88.151.82.194	TCP	2848	4299	unknown	0	unknown	20	27	83.245.74.2	39122	0	104.21 kbps (3.73 MB)
1165275840	Connection to Internet	Connection to ISP1S1	80.67.86.7	88.151.82.144	TCP	80	1561	unknown	0	unknown	0	26	83.245.74.2	3356	0	92.81 kbps (3.32 MB)
1165275960	Connection to Internet	Connection to ISP1S1	130.117.156.9	88.151.81.19	TCP	80	6422	unknown	0	unknown	0	26	83.245.74.2	3356	0	91.28 kbps (3.26 MB)
1165276020	Connection to Internet	Connection to ISP1S1	80.67.86.7	88.151.82.144	TCP	80	1675	unknown	0	unknown	0	26	83.245.74.2	3356	0	90.33 kbps (3.23 MB)
1165275900	Connection to Internet	Connection to ISP1S1	212.100.243.192	88.151.82.84	TCP	7000	3333	unknown	0	unknown	0	26	83.245.74.2	3356	0	84.59 kbps (3.03 MB)
1165276020	Connection to Internet	Connection to ISP1S1	62.67.57.63	213.200.67.155	TCP	80	3898	unknown	32	unknown	0	22	83.245.74.2	3356	0	84 kbps (3 MB)
1165276020	Connection to Internet	Connection to ISP1S1	62.67.57.63	213.200.67.155	TCP	80	3896	unknown	32	unknown	0	22	83.245.74.2	3356	0	80.96 kbps (2.9 MB)
1165275900	Connection to Internet	Connection to ISP1S1	63.223.60.24	83.245.74.94	TCP	80	6774	unknown	0	unknown	0	27	83.245.74.2	3356	0	78.97 kbps (2.82 MB)
1165276020	Connection to Internet	Connection to ISP1S1	62.67.57.63	213.200.67.155	TCP	80	3895	unknown	32	unknown	0	22	83.245.74.2	3356	0	76.56 kbps (2.74 MB)
1165275780	Connection to Internet	Connection to ISP1S1	38.112.226.55	83.245.74.124	TCP	554	4007	unknown	0	unknown	0	27	83.245.74.2	3356	0	75.34 kbps (2.69 MB)
1165276020	Connection to Internet	Connection to ISP1S1	130.117.156.9	88.151.81.19	TCP	80	6422	unknown	0	unknown	0	26	83.245.74.2	3356	0	70.12 kbps (2.51 MB)
1165276020	Connection to Internet	Connection to ISP1S1	62.67.57.63	213.200.67.155	TCP	80	3897	unknown	32	unknown	0	22	83.245.74.2	3356	0	68.36 kbps (2.44 MB)
1165275960	Connection to Internet	Connection to ISP1S1	69.16.169.100	213.200.67.155	TCP	80	4293	unknown	128	unknown	0	22	83.245.74.2	3356	0	61.92 kbps (2.21 MB)
1165276020	Connection to Internet	Connection to ISP1S1	69.16.169.100	213.200.67.155	TCP	80	4292	unknown	128	unknown	0	22	83.245.74.2	3356	0	59.16 kbps (2.12 MB)
1165275960	Connection to Internet	Connection to ISP1S1	69.16.169.100	213.200.67.155	TCP	80	4292	unknown	128	unknown	0	22	83.245.74.2	3356	0	59.12 kbps (2.11 MB)
1165275840	Connection to Internet	Connection to ISP1S1	66.249.91.91	213.200.67.155	TCP	80	1900	unknown	48	unknown	0	22	83.245.74.2	3356	0	57.07 kbps (2.04 MB)
1165275960	Connection to Internet	Connection to ISP1S1	89.102.184.124	88.151.82.136	TCP	6077	4792	unknown	0	unknown	0	26	83.245.74.2	3356	0	55.41 kbps (1.98 MB)
1165276020	Connection to Internet	Connection to ISP1S1	89.102.184.124	88.151.82.136	TCP	6077	4792	unknown	0	unknown	0	26	83.245.74.2	3356	0	53.75 kbps (1.92 MB)
1165276020	Connection to Internet	Connection to ISP1S1	80.67.86.215	213.200.67.155	TCP	80	11620	unknown	0	unknown	0	22	83.245.74.2	3356	0	53.36 kbps (1.91 MB)
1165275900	Connection to Internet	Connection to ISP1S1	69.16.169.100	213.200.67.155	TCP	80	2218	unknown	128	unknown	0	22	83.245.74.2	3356	0	53.2 kbps (1.9 MB)
1165275840	Connection to Internet	Connection to ISP1S1	69.16.169.100	213.200.67.155	TCP	80	4293	unknown	128	unknown	0	22	83.245.74.2	3356	0	52.64 kbps (1.88 MB)
1165275960	Connection to Internet	Connection to ISP1S1	146.82.204.17	88.151.82.227	TCP	80	2730	unknown	0	unknown	0	28	83.245.74.2	3356	0	51.98 kbps (1.86 MB)
1165276020	Connection to Internet	Connection to ISP1S1	62.67.57.63	213.200.67.155	TCP	80	3899	unknown	32	unknown	0	22	83.245.74.2	3356	0	51.88 kbps (1.86 MB)
1165275900	Connection to Internet	Connection to ISP1S1	146.82.204.17	88.151.82.227	TCP	80	2726	unknown	0	unknown	0	28	83.245.74.2	3356	0	50.94 kbps (1.82 MB)
1165275900	Connection to Internet	Connection to ISP1S1	128.241.88.51	213.200.67.155	TCP	80	2408	unknown	128	unknown	0	22	83.245.74.2	3356	0	50.6 kbps (1.81 MB)
1165276020	Connection to Internet	Connection to ISP1S1	69.16.169.100	213.200.67.155	TCP	80	4293	unknown	128	unknown	0	22	83.245.74.2	3356	0	50.12 kbps (1.79 MB)
1165276020	Connection to Internet	Connection to ISP1S1	69.28.159.229	213.200.67.155	TCP	80	2255	unknown	32	unknown	0	22	83.245.74.2	3356	0	49.73 kbps (1.78 MB)
1165275780	Connection to Internet	Connection to ISP1S1	69.16.169.100	213.200.67.155	TCP	80	1920	unknown	128	unknown	0	22	83.245.74.2	3356	0	49.68 kbps (1.78 MB)
1165275840	Connection to Internet	Connection to ISP1S1	69.16.169.100	213.200.67.155	TCP	80	4292	unknown	128	unknown	0	22	83.245.74.2	3356	0	49.48 kbps (1.77 MB)
1165275960	Connection to Internet	Connection to ISP1S1	69.16.169.100	213.200.67.155	TCP	80	3343	unknown	128	unknown	0	22	83.245.74.2	3356	0	49.44 kbps (1.77 MB)
1165275960	Connection to Internet	Connection to ISP1S1	66.249.91.91	213.200.67.155	TCP	80	1893	unknown	48	unknown	0	22	83.245.74.2	3356	0	49.07 kbps (1.75 MB)

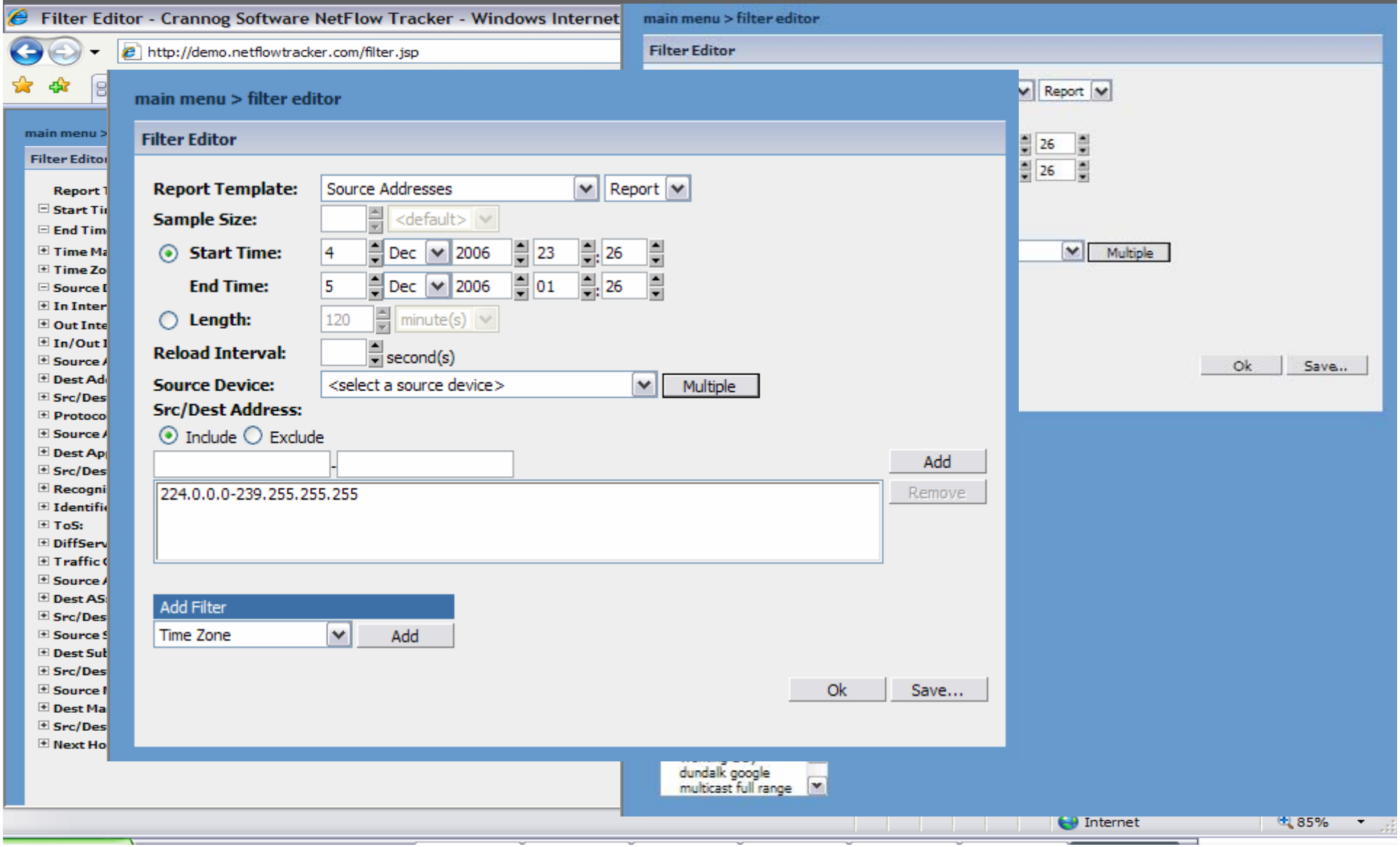
CRANNOGSOFTWARE

Click to Drill thru solution to field combinations

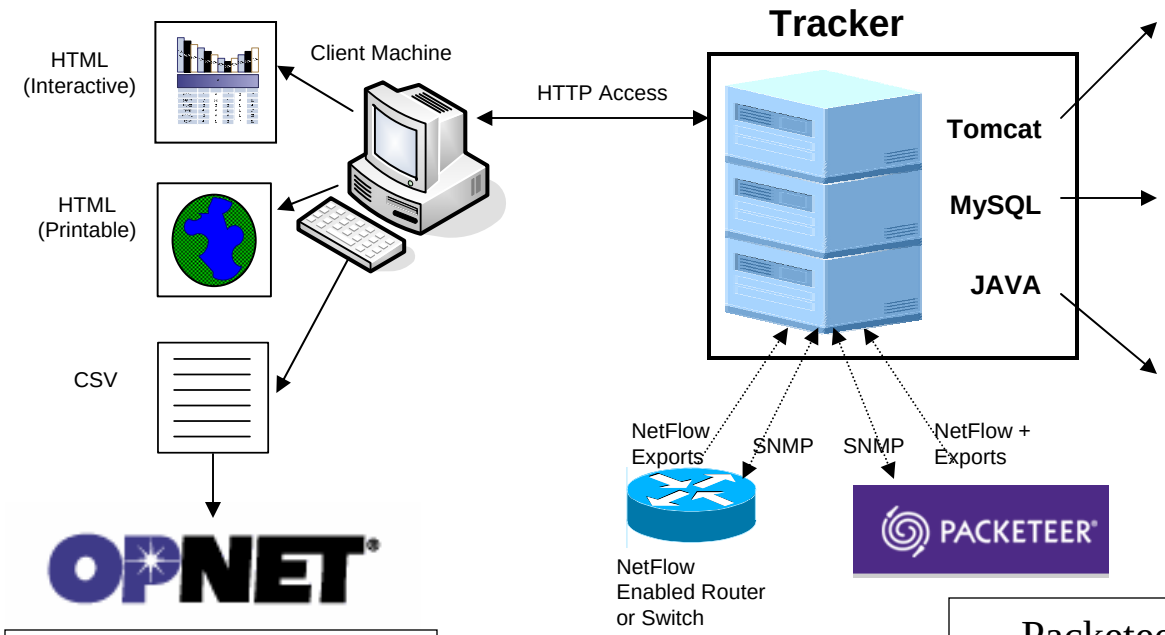


CRANNOGSOFTWARE

The ability to filter on any combination of fields



NetFlow Tracker – Overview



Presentation layer provides web access to all reports

Database used to store information on every flow

Data collection and processing layer

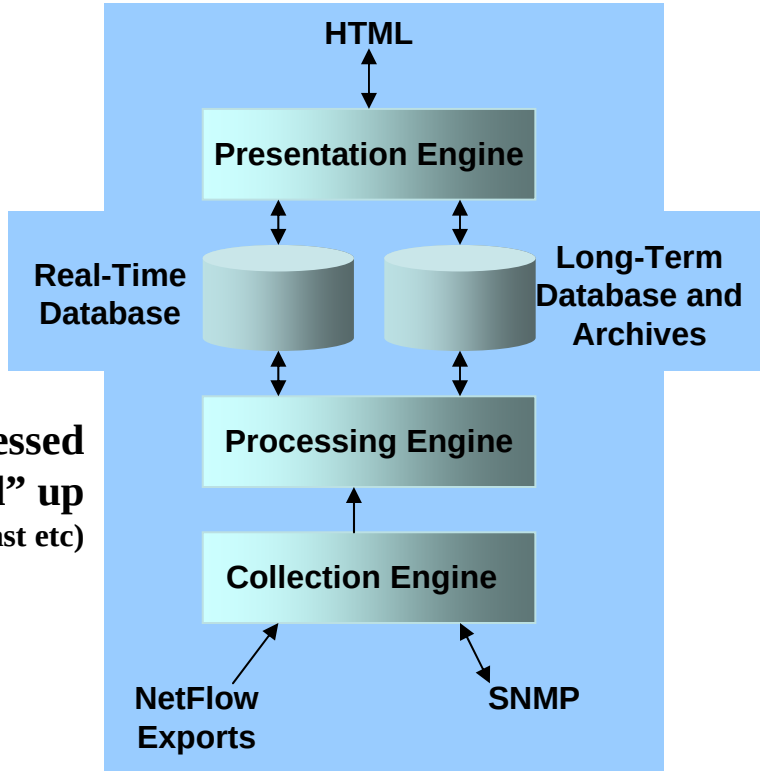
CSV output can be used as a "feeder" into 3rd part applications

Packeteer can provide true application recognition and marking. Reported on within the NetFlow export.

NetFlow Tracker – How does it do it.

When a report is requested, the relevant data is pulled from the database and presented in the required format

Every minute, flows are flushed to the real-time database



Every 6 hours, long-term databases & archives are updated

Flows are processed and "cleaned" up
(fix multicast etc)

Flow records are sent to the server

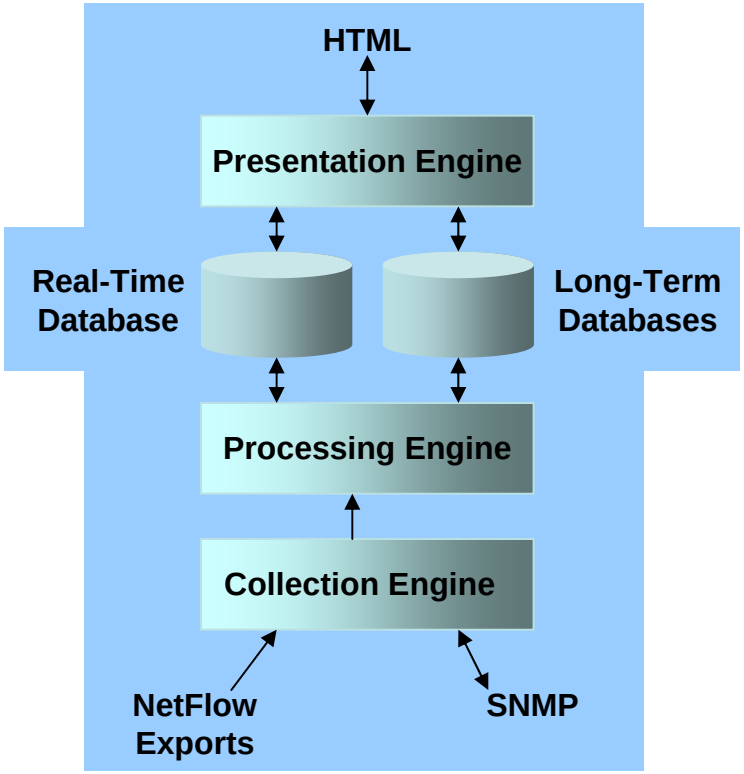
If the originator of NetFlow traffic is new, Tracker will do an SNMP query to pull back relevant information

NetFlow Tracker – Databases - Real Time

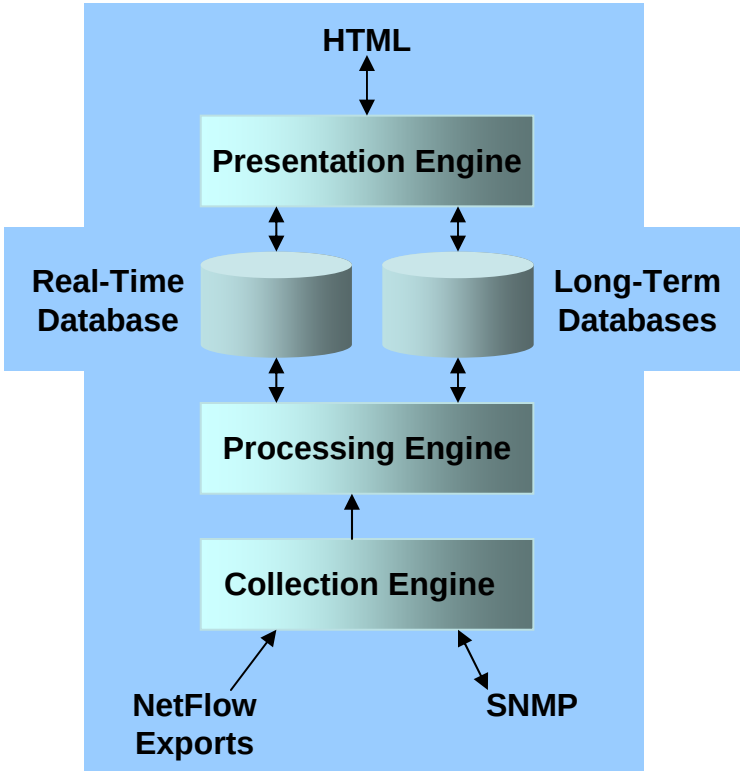
Real-Time database stores flow records

Available Fields

- Source Addresses
- Destination Addresses
- Protocols
- Source Ports
- Destination Ports
- Type of Service TOS
- Differentiated Service
- AS Source
- AS Destination
- Source Network
- Destination Network
- In Interfaces
- Out Interfaces
- Next Hop
- Traffic Classes
- Identified Applications
- Traffic Count
- Packet Count



NetFlow Tracker – Databases – Long Term



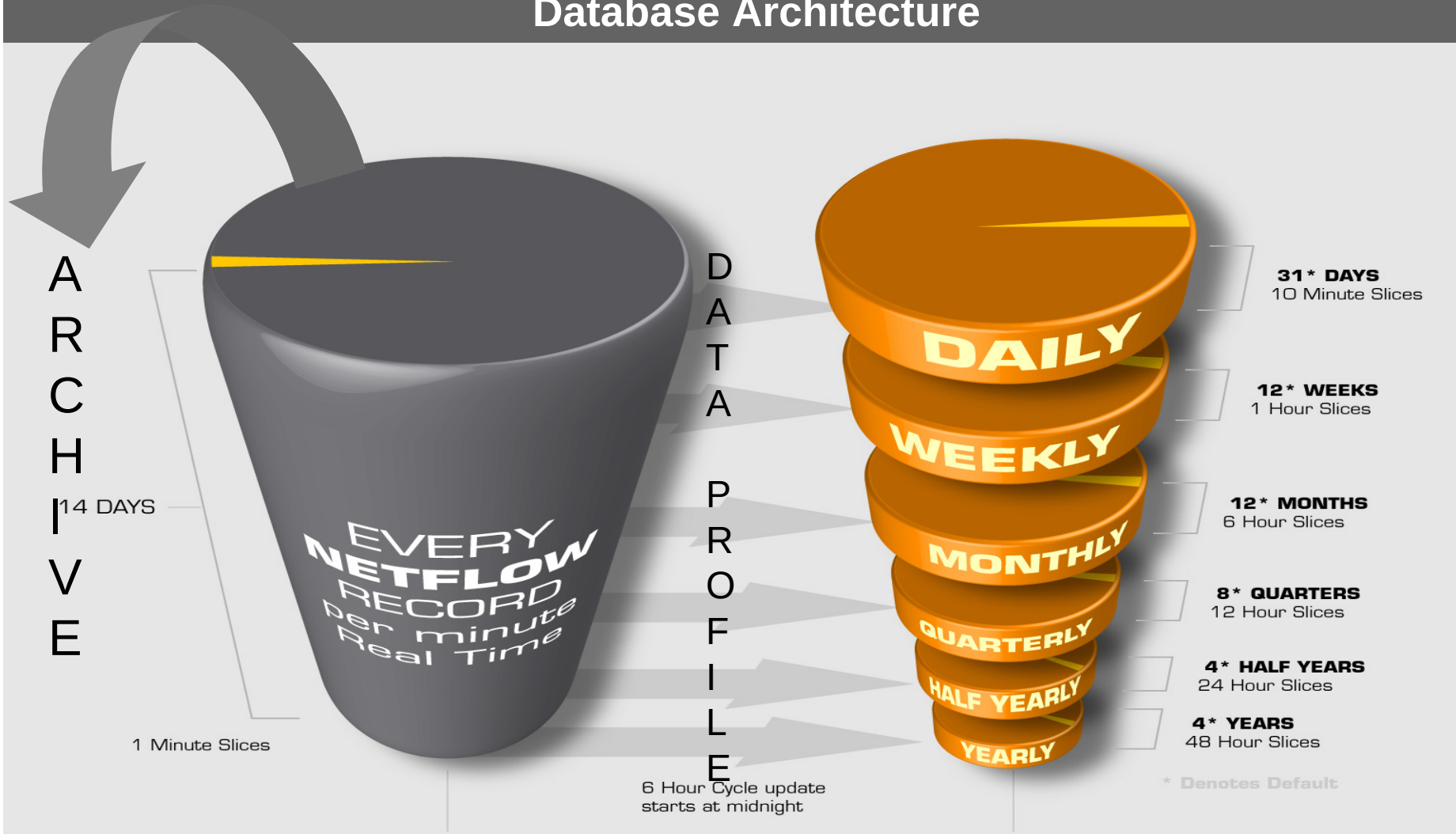
Long-term database stores report data

Available Reports

- Source Addresses
- Destination Addresses
- Address Pairs
- Protocols
- Source Ports
- Destination Ports
- Source Applications
- Destination Applications
- Recognized Applications
- Source Endpoints
- Destination Endpoints
- Server-Client Sessions
- Client-Server Sessions
- Conversations
- Type of Service TOS
- Differentiated Services
- AS Pairs
- Source Networks
- Destination Networks
- Network Pairs
- In Interfaces
- Out Interfaces
- Next Hops
- Source Address Dissemination
- Destination Address Popularity
- Traffic Classes
- Identified Applications

CRANNOGSOFTWARE

Database Architecture



NETFLOWTRACKER

NetFlow Tracker – Storage Periods

Real-Time (all flows)

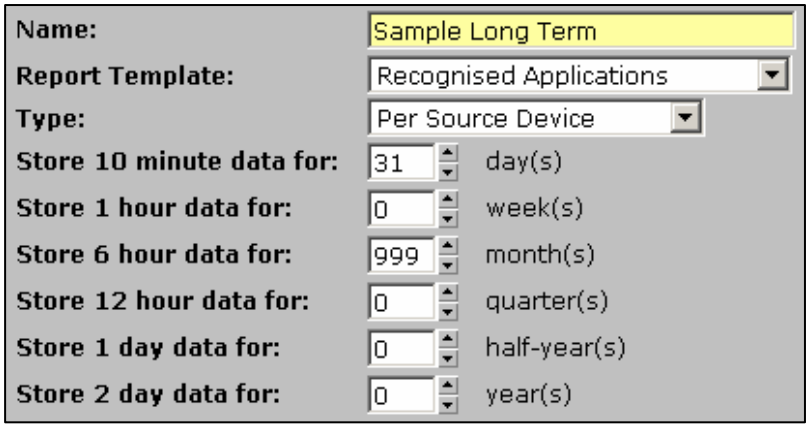
- **1 minute resolution for upto 14 days.**

Archived (all flows)

- **1 minute resolution, forever (depending on disk space)**

Long Term (Top N)

- **Daily – 10 minute resolution for upto 999 days (2.7 years).**
- **Weekly –1 hour resolution for upto 999 (19 years).**
- **Monthly –6 hour resolution for upto 999 Months (83 years).**
- **Quarterly –12 hour resolution for upto 999 quarters (249 years).**
- **½ Yearly –24 hour resolution for upto 999 ½ yeas (450 years).**
- **Yearly –48 hour resolution for upto 999 years.**



Typical settings

NetFlow Tracker – Lets have a look

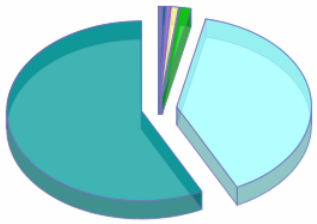
- **Flexible Reporting (including Packeteer integration)**
- **Report Presentation Formats**
- **Scenario of use (Identifying Security Threats)**
- **Scenario of use (Identifying Abnormal behaviour)**
- **Scenario of use - QoS troubleshooting, trending analysis**
- **Scenario of use - Internet Traffic Profiling BGP**

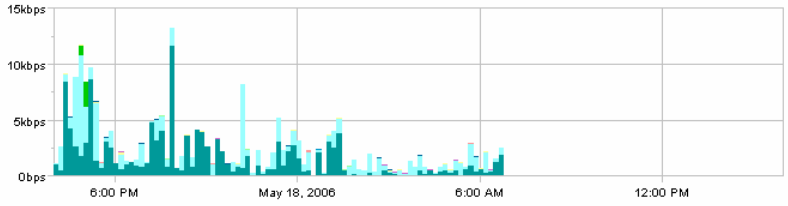
main menu > executive reports > packeteer report pie time range

Packeteer Report Pie Time Range

Time Range: May 17, 2006 4:00 PM BST - May 18, 2006 4:00 PM BST
Source Device: Packeteer SJ (81.6.198.14)

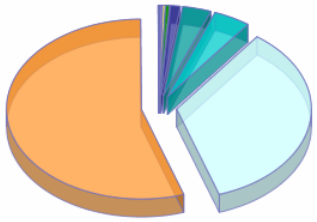
Identified Applications results from the export of services ids from the packetshaper in the form of Netflow private field extensions

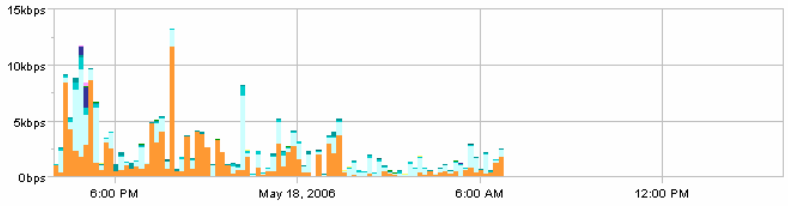




	Identified App.	Peak	Average	% of Total
	unknown	11.63 kbps between May 17, 2006 7:50 PM and May 17, 2006 8:00 PM	917.16 bps (9.45 MB)	57%
	HTTP	8.98 kbps between May 17, 2006 4:50 PM and May 17, 2006 5:00 PM	626.28 bps (6.45 MB)	39%
	SSL	2.15 kbps between May 17, 2006 5:00 PM and May 17, 2006 5:10 PM	21.68 bps (228.69 kB)	1%
	MSN-Messenger	257.84 bps between May 17, 2006 6:10 PM and May 17, 2006 6:20 PM	13.82 bps (145.8 kB)	<1%
	DNS	80.27 bps between May 18, 2006 5:10 AM and May 18, 2006 5:20 AM	7.19 bps (75.87 kB)	<1%
	YahooMsg	53.73 bps between May 17, 2006 5:20 PM and May 17, 2006 5:30 PM	6.5 bps (68.58 kB)	<1%
	ICMP	137.68 bps between May 18, 2006 12:20 AM and May 18, 2006 12:30 AM	2.54 bps (26.74 kB)	<1%
	NTP	21.28 bps between May 18, 2006 1:40 AM and May 18, 2006 1:50 AM	2.28 bps (24.05 kB)	<1%
	DHCP-S	9.07 bps between May 17, 2006 6:10 PM and May 17, 2006 6:20 PM	0.76 bps (7.97 kB)	<1%
	SMTP-Clear	60.19 bps between May 17, 2006 5:40 PM and May 17, 2006 5:50 PM	0.42 bps (4.41 kB)	<1%
	Others	15.55 bps between May 18, 2006 3:50 AM and May 18, 2006 4:00 AM	0.52 bps (5.44 kB)	<1%
		13.24 kbps between May 17, 2006 7:50 PM and May 17, 2006 8:00 PM	**1.6 kbps (16.47 MB)**	

Traffic Classes results from the export of class ids from the packetshaper in the form of Netflow private field extensions



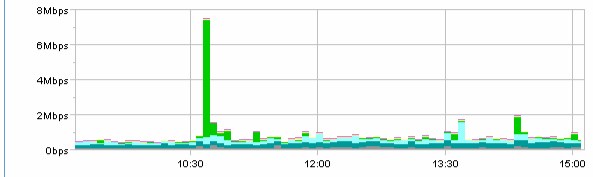


	Traffic Class	Peak	Average	% of Total
	Inbound/Default	11.61 kbps between May 17, 2006 7:50 PM and May 17, 2006 8:00 PM	880.15 bps (9.07 MB)	55%
	Inbound/HTTP	7.83 kbps between May 17, 2006 4:50 PM and May 17, 2006 5:00 PM	555.3 bps (5.72 MB)	35%
	Outbound/HTTP	1.15 kbps between May 17, 2006 4:50 PM and May 17, 2006 5:00 PM	70.98 bps (748.57 kB)	4%
	unknown	581.25 bps between May 17, 2006 6:30 PM and May 17, 2006 6:40 PM	54.73 bps (577.22 kB)	3%
	Inbound/SSL	1.81 kbps between May 17, 2006 5:00 PM and May 17, 2006 5:10 PM	18.61 bps (196.31 kB)	1%
	Outbound/Default	42.73 bps between May 18, 2006 1:30 AM and May 18, 2006 1:40 AM	7.39 bps (77.94 kB)	<1%
	Inbound/DNS	55.13 bps between May 18, 2006 5:10 AM and May 18, 2006 5:20 AM	4.84 bps (51.09 kB)	<1%
	Outbound/SSL	341.45 bps between May 17, 2006 5:00 PM and May 17, 2006 5:10 PM	3.19 bps (33.62 kB)	<1%
	Outbound/DNS	25.13 bps between May 18, 2006 5:10 AM and May 18, 2006 5:20 AM	2.35 bps (24.78 kB)	<1%
	Outbound/DHCP	4.69 bps between May 17, 2006 6:10 PM and May 17, 2006 6:20 PM	0.39 bps (4.12 kB)	<1%
	Others	60.19 bps between May 17, 2006 5:40 PM and May 17, 2006 5:50 PM	1.2 bps (12.7 kB)	<1%

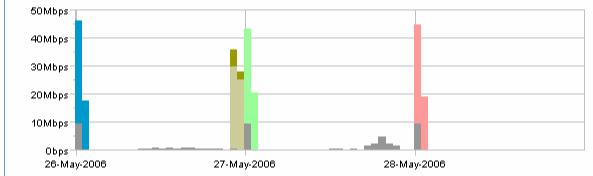
.110)

over time.

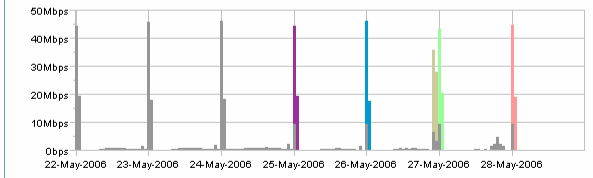
stination of most traffic or packets over various time frames



	Average	% of Total
74 kbps between 14:20 and 14:25	252.16 kbps (649.29 MB)	30%
bps between 13:40 and 13:45	200.8 kbps (517.04 MB)	24%
bps between 10:40 and 10:45	177.37 kbps (456.71 MB)	21%
54 kbps between 11:45 and 11:50	45.17 kbps (116.32 MB)	5%
6 kbps between 09:09 and 09:10	42.09 kbps (108.39 MB)	5%
48 kbps between 11:30 and 11:35	109.62 kbps (282.26 MB)	13%
Mbps between 10:40 and 10:45	**827.21 kbps (2.08 GB)**	



	Average	% of Total
May-2006 00:00 and 28-May-2006 01:00	753.06 kbps (22.72 GB)	19%
7-May-2006 00:00 and 27-May-2006 01:00	753.05 kbps (22.72 GB)	19%
5-May-2006 00:00 and 26-May-2006 01:00	752.7 kbps (22.71 GB)	19%
5-May-2006 22:00 and 26-May-2006 23:00	752.68 kbps (22.71 GB)	19%
May-2006 22:00 and 26-May-2006 23:00	127.91 kbps (3.86 GB)	3%
May-2006 00:00 and 26-May-2006 01:00	877.35 kbps (26.47 GB)	22%
26-May-2006 00:00 and 26-May-2006 01:00	**4.02 Mbps (121.2 GB)**	



	Average	% of Total
May-2006 00:00 and 28-May-2006 01:00	322.74 kbps (22.72 GB)	9%
7-May-2006 00:00 and 27-May-2006 01:00	322.74 kbps (22.72 GB)	9%
ay-2006 00:00 and 25-May-2006 01:00	322.61 kbps (22.71 GB)	9%
5-May-2006 00:00 and 26-May-2006 01:00	322.59 kbps (22.71 GB)	9%
5-May-2006 22:00 and 26-May-2006 23:00	322.58 kbps (22.71 GB)	9%
4-May-2006 00:00 and 24-May-2006 01:00	1.98 Mbps (139.33 GB)	55%
26-May-2006 00:00 and 26-May-2006 01:00	**3.59 Mbps (252.91 GB)**	

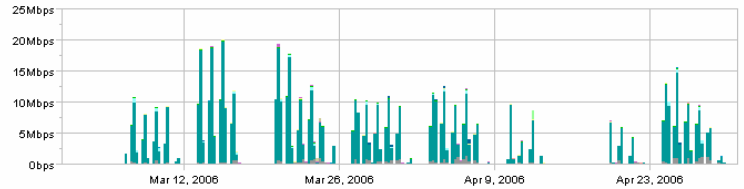
CRANNOGSOFTWARE

Dynamic as well as Static Printable Reports with several format

Recognised Applications

Time Range: Mar 1, 2006 12:00 AM GMT - May 1, 2006 12:00 AM BST
Source Device: DKIT_3640 (193.1.207.54)

Traffic Rate



App.	Peak	Average	% of Total
80/TCP (http)	19.56 Mbps between Mar 15, 2006 12:00 PM and Mar 15, 2006 6:00 PM	2.52 Mbps (1.51 TB)	89%
49156/UDP	672.37 kbps between Mar 7, 2006 12:00 PM and Mar 7, 2006 6:00 PM	38.36 kbps (23.52 GB)	1%
443/TCP (https)	237.25 kbps between Apr 25, 2006 12:00 PM and Apr 25, 2006 6:00 PM	35.26 kbps (21.62 GB)	1%
25/TCP (smtp)	139.37 kbps between Mar 8, 2006 12:00 PM and Mar 8, 2006 6:00 PM	22.84 kbps (14 GB)	<1%
6881/TCP	505.86 kbps between Mar 20, 2006 12:00 PM and Mar 20, 2006 6:00 PM	17.96 kbps (11.01 GB)	<1%
49164/UDP	754.95 kbps between Apr 6, 2006 6:00 PM and Apr 7, 2006 12:00 AM	11.25 kbps (6.9 GB)	<1%
1026/UDP	9.97 kbps between Mar 19, 2006 6:00 AM and Mar 19, 2006 12:00 PM	6.91 kbps (4.24 GB)	<1%
5641/TCP	1.41 Mbps between Apr 12, 2006 12:00 PM and Apr 12, 2006 6:00 PM	5.8 kbps (3.56 GB)	<1%
4500/UDP	17.43 kbps between Mar 17, 2006 6:00 AM and Mar 17, 2006 12:00 PM	5.25 kbps (3.22 GB)	<1%
60127/TCP	521.23 kbps between Mar 24, 2006 6:00 AM and Mar 24, 2006 12:00 PM	4.15 kbps (2.55 GB)	<1%
Others	1.41 Mbps between Apr 6, 2006 12:00 PM and Apr 6, 2006 6:00 PM	172.43 kbps (105.72 GB)	6%
	20.1 Mbps between Mar 15, 2006 12:00 PM and Mar 15, 2006 6:00 PM	**2.84 Mbps (1.7 TB)**	

Recognised Applications

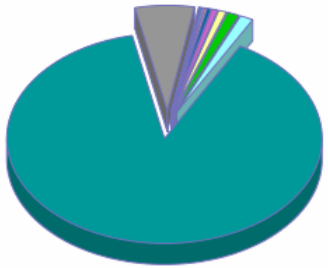
Time Range: Mar 1, 2006 12:00 AM GMT - May 1, 2006 12:00 AM BST
Source Device: DKIT_3640 (193.1.207.54)

App.	Traffic	% of Total Traffic	Packets	% of Total Packets
80/TCP (http)	2.52 Mbps (1.51 TB)	89%	262.88 /s (1.38 G)	76%
49156/UDP	38.36 kbps (23.52 GB)	1%	4.76 /s (25.08 M)	1%
443/TCP (https)	35.26 kbps (21.62 GB)	1%	12.72 /s (67 M)	4%
25/TCP (smtp)	22.84 kbps (14 GB)	<1%	3.73 /s (19.63 M)	1%
6881/TCP	17.97 kbps (11.02 GB)	<1%	5.9 /s (31.06 M)	2%
49164/UDP	11.25 kbps (6.9 GB)	<1%	1.2 /s (6.31 M)	<1%
1026/UDP	6.91 kbps (4.24 GB)	<1%	1.03 /s (5.45 M)	<1%
5641/TCP	5.8 kbps (3.56 GB)	<1%	0.48 /s (2.55 M)	<1%
4500/UDP	5.27 kbps (3.23 GB)	<1%	1.84 /s (9.67 M)	<1%
60127/TCP	4.15 kbps (2.55 GB)	<1%	0.43 /s (2.24 M)	<1%
Others	172.41 kbps (105.71 GB)	6%	50.52 /s (266.08 M)	15%
	2.84 Mbps (1.7 TB)		**345.49 /s (1.82 G)**	

Recognised Applications

Time Range: Mar 1, 2006 12:00 AM GMT - May 1, 2006 12:00 AM BST
Source Device: DKIT_3640 (193.1.207.54)

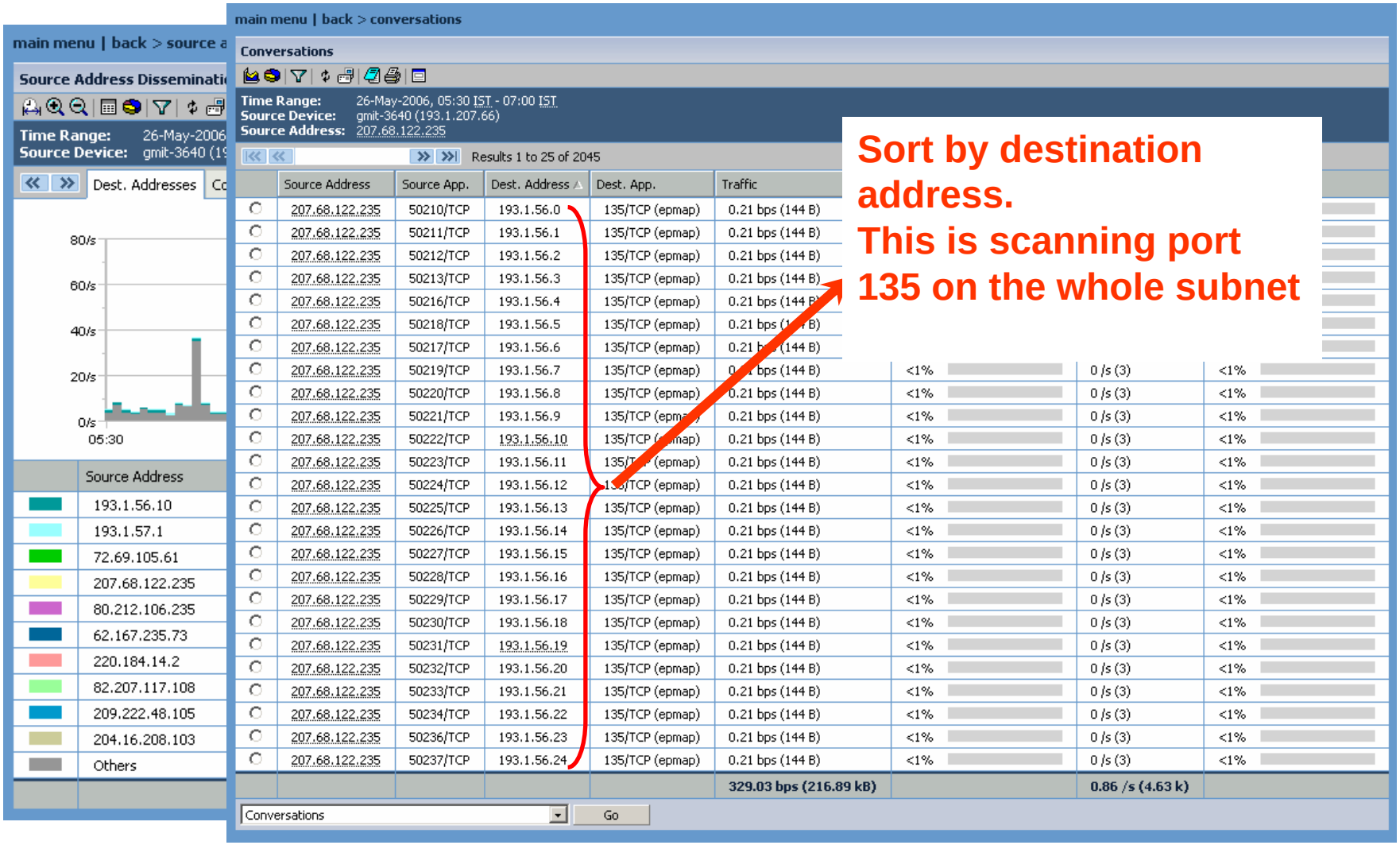
Traffic Rate



App.	Traffic Rate	% of Total
80/TCP (http)	2.52 Mbps (1.51 TB)	89%
49156/UDP	38.36 kbps (23.52 GB)	1%
443/TCP (https)	35.26 kbps (21.62 GB)	1%
25/TCP (smtp)	22.84 kbps (14 GB)	<1%
6881/TCP	17.97 kbps (11.02 GB)	<1%
49164/UDP	11.25 kbps (6.9 GB)	<1%
1026/UDP	6.91 kbps (4.24 GB)	<1%
5641/TCP	5.8 kbps (3.56 GB)	<1%
4500/UDP	5.27 kbps (3.23 GB)	<1%
60127/TCP	4.15 kbps (2.55 GB)	<1%
Others	172.41 kbps (105.71 GB)	6%
	2.84 Mbps (1.7 TB)	

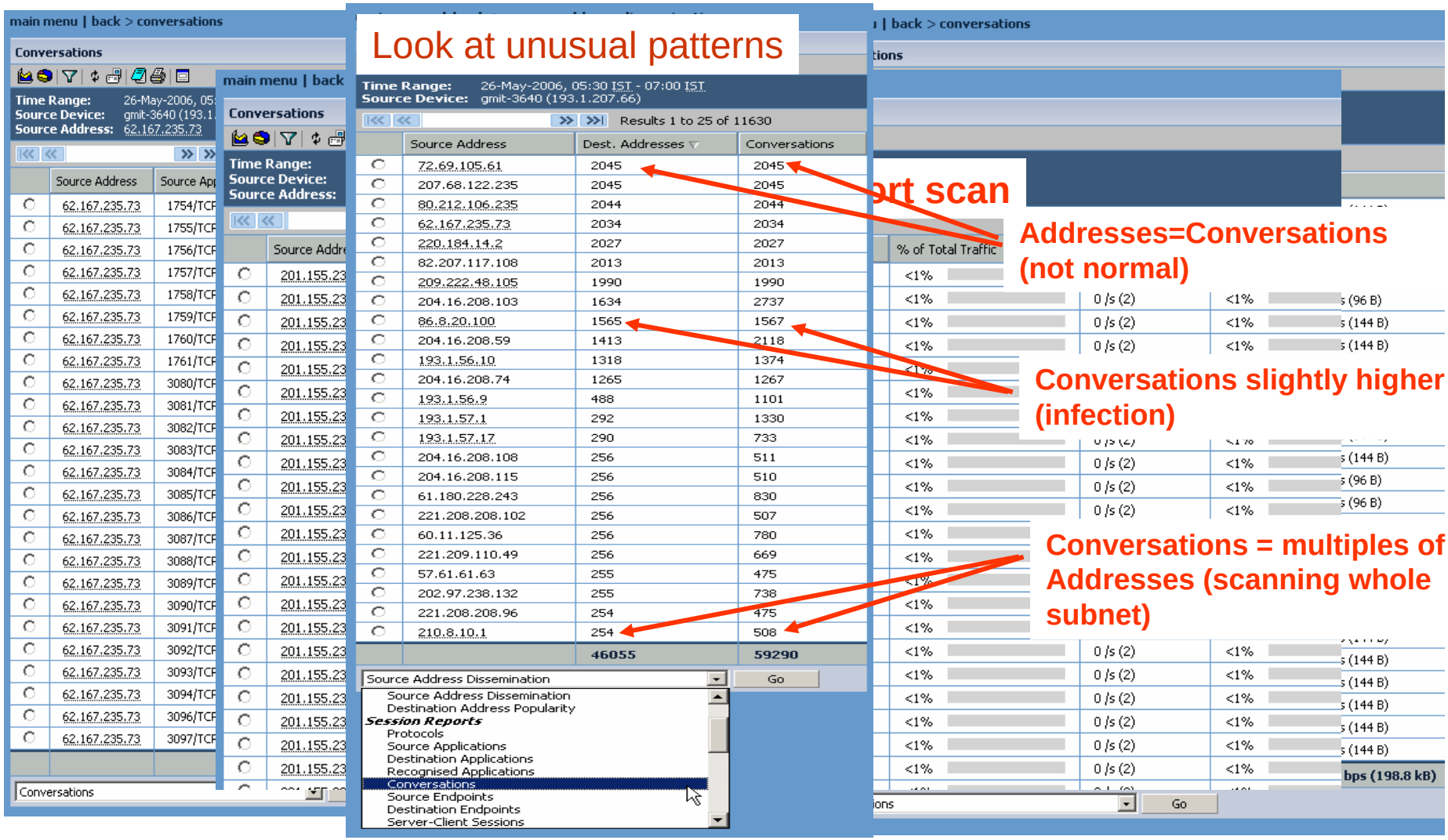
CRANNOGSOFTWARE

Scenario of use - Identifying Security Threats, P2P, Worms

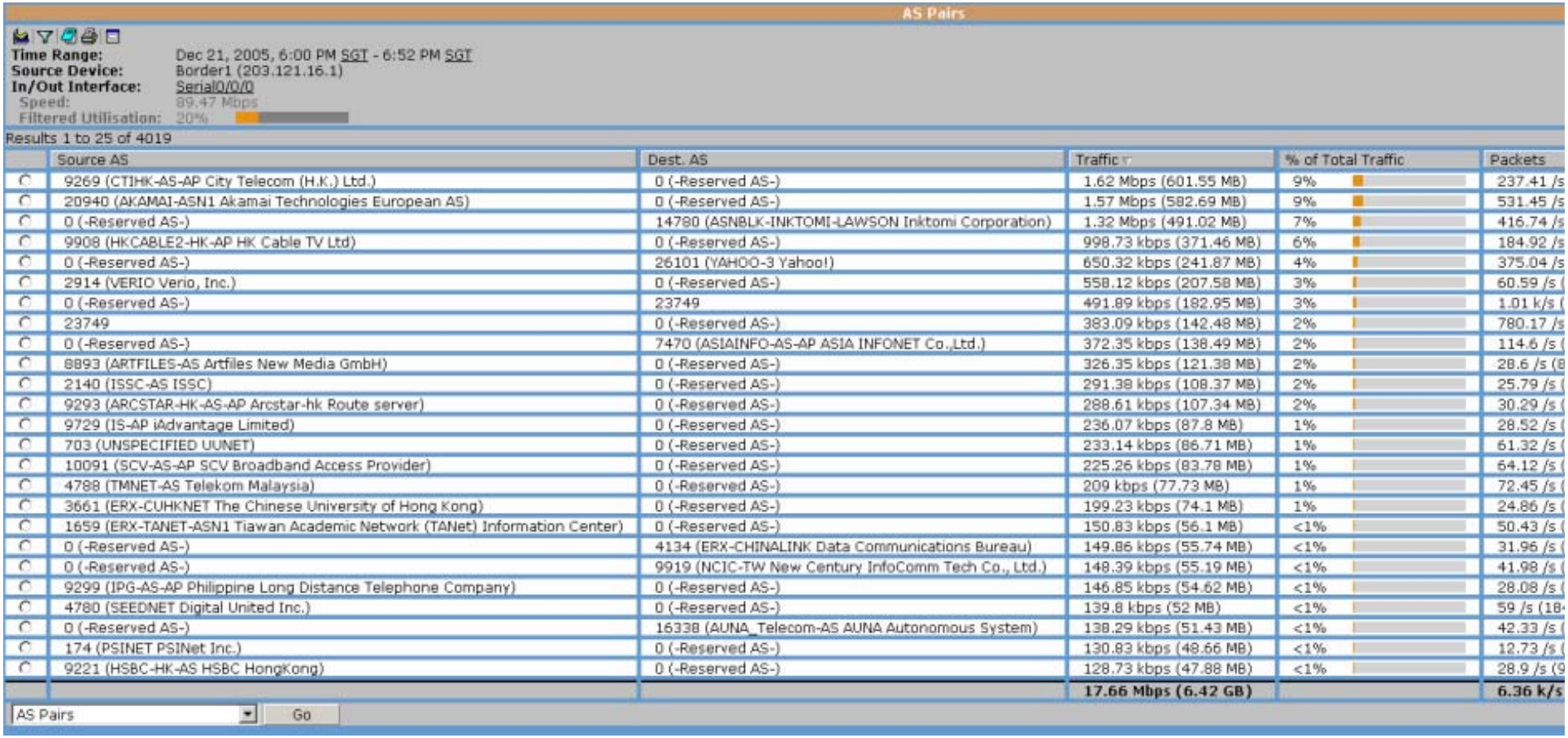


CRANNOGSOFTWARE

Scenario of use - Identifying Suspicious and abnormal activity



Scenario of use ISP - Internet Traffic Profiling BGP



AS Pairs

Time Range: Dec 21, 2005, 6:00 PM SGT - 6:52 PM SGT
Source Device: Border1 (203.121.16.1)
In/Out Interface: Serial0/0/0
Speed: 89.47 Mbps
Filtered Utilisation: 20%

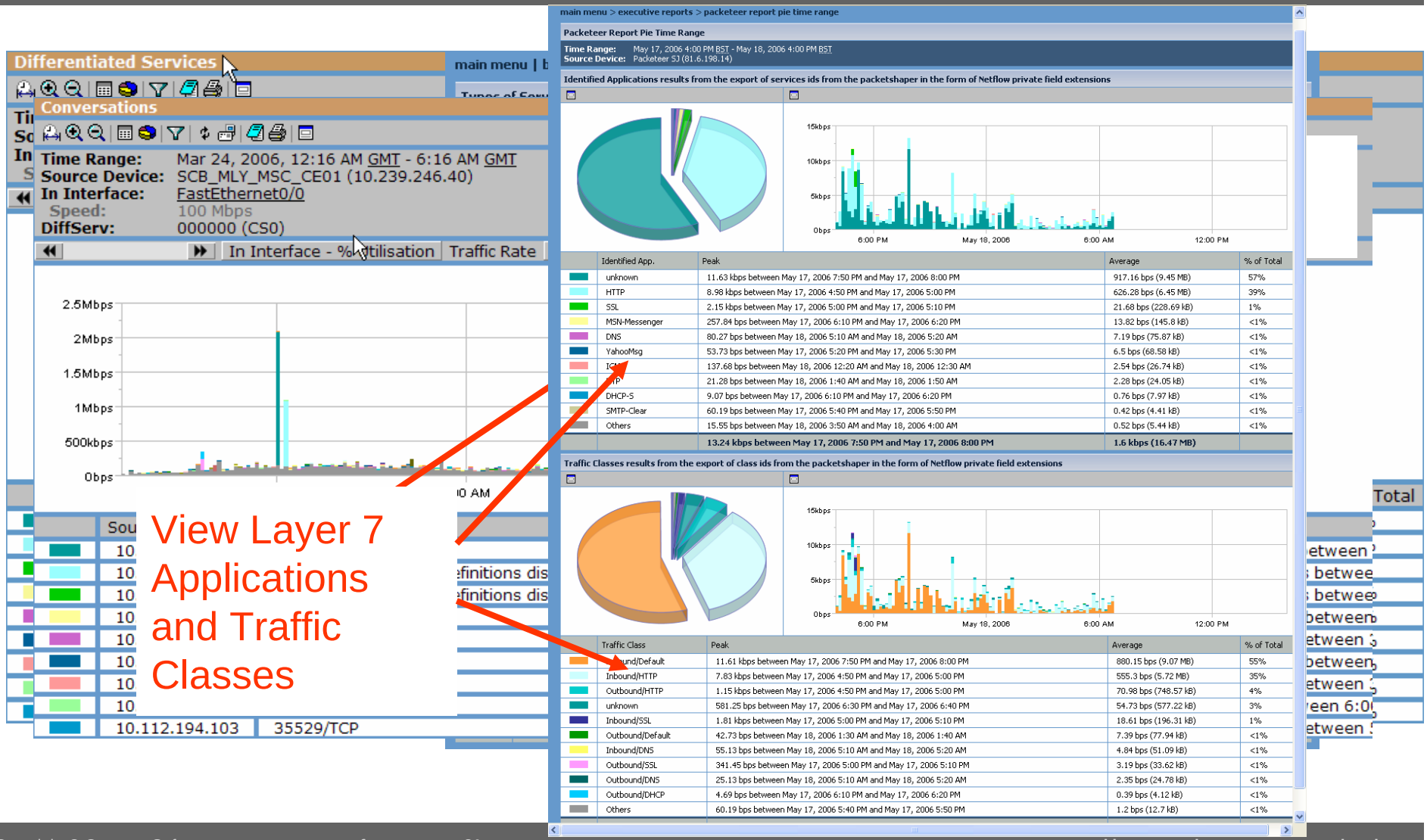
Results 1 to 25 of 4019

Source AS	Dest. AS	Traffic	% of Total Traffic	Packets
9269 (CTIHK-AS-AP City Telecom (H.K.) Ltd.)	0 (-Reserved AS-)	1.62 Mbps (601.55 MB)	9%	237.41 /s
20940 (AKAMAI-ASN1 Akamai Technologies European AS)	0 (-Reserved AS-)	1.57 Mbps (582.69 MB)	9%	531.45 /s
0 (-Reserved AS-)	14780 (ASNBLK-INKTOMI-LAWSON Inktomi Corporation)	1.32 Mbps (491.02 MB)	7%	416.74 /s
9908 (HKCABLE2-HK-AP HK Cable TV Ltd)	0 (-Reserved AS-)	998.73 kbps (371.46 MB)	6%	184.92 /s
0 (-Reserved AS-)	26101 (YAHOO-3 Yahoo!)	650.32 kbps (241.87 MB)	4%	375.04 /s
2914 (VERIO Verio, Inc.)	0 (-Reserved AS-)	558.12 kbps (207.58 MB)	3%	60.59 /s
0 (-Reserved AS-)	23749	491.89 kbps (182.95 MB)	3%	1.01 k/s
23749	0 (-Reserved AS-)	383.09 kbps (142.48 MB)	2%	780.17 /s
0 (-Reserved AS-)	7470 (ASIAINFO-AS-AP ASIA INFONET Co.,Ltd.)	372.35 kbps (138.49 MB)	2%	114.6 /s
8893 (ARTFILES-AS Artfiles New Media GmbH)	0 (-Reserved AS-)	326.35 kbps (121.38 MB)	2%	28.6 /s
2140 (ISSC-AS ISSC)	0 (-Reserved AS-)	291.38 kbps (108.37 MB)	2%	25.79 /s
9293 (ARCSTAR-HK-AS-AP Arcstar-hk Route server)	0 (-Reserved AS-)	288.61 kbps (107.34 MB)	2%	30.29 /s
9729 (IS-AP iAdvantage Limited)	0 (-Reserved AS-)	236.07 kbps (87.8 MB)	1%	28.52 /s
703 (UNSPECIFIED UUNET)	0 (-Reserved AS-)	233.14 kbps (86.71 MB)	1%	61.32 /s
10091 (SCV-AS-AP SCV Broadband Access Provider)	0 (-Reserved AS-)	225.26 kbps (83.78 MB)	1%	64.12 /s
4788 (TMNET-AS Telekom Malaysia)	0 (-Reserved AS-)	209 kbps (77.73 MB)	1%	72.45 /s
3661 (ERX-CUHKNET The Chinese University of Hong Kong)	0 (-Reserved AS-)	199.23 kbps (74.1 MB)	1%	24.86 /s
1659 (ERX-TANET-ASN1 Tiawan Academic Network (TANet) Information Center)	0 (-Reserved AS-)	150.83 kbps (56.1 MB)	<1%	50.43 /s
0 (-Reserved AS-)	4134 (ERX-CHINALINK Data Communications Bureau)	149.86 kbps (55.74 MB)	<1%	31.96 /s
0 (-Reserved AS-)	9919 (NCIC-TW New Century InfoComm Tech Co., Ltd.)	148.39 kbps (55.19 MB)	<1%	41.98 /s
9299 (IPG-AS-AP Philippine Long Distance Telephone Company)	0 (-Reserved AS-)	146.85 kbps (54.62 MB)	<1%	28.08 /s
4780 (SEEDNET Digital United Inc.)	0 (-Reserved AS-)	139.8 kbps (52 MB)	<1%	59 /s (18
0 (-Reserved AS-)	16338 (AUNA_Telecom-AS AUNA Autonomous System)	138.29 kbps (51.43 MB)	<1%	42.33 /s
174 (PSINET PSINet Inc.)	0 (-Reserved AS-)	130.83 kbps (48.66 MB)	<1%	12.73 /s
9221 (HSBC-HK-AS HSBC HongKong)	0 (-Reserved AS-)	128.73 kbps (47.88 MB)	<1%	28.9 /s (9
		17.66 Mbps (6.42 GB)		**6.36 k/s**

AS Pairs Go

CRANNOGSOFTWARE

Scenario of use - QoS troubleshooting, trending analysis



NetFlow Tracker And Multicast

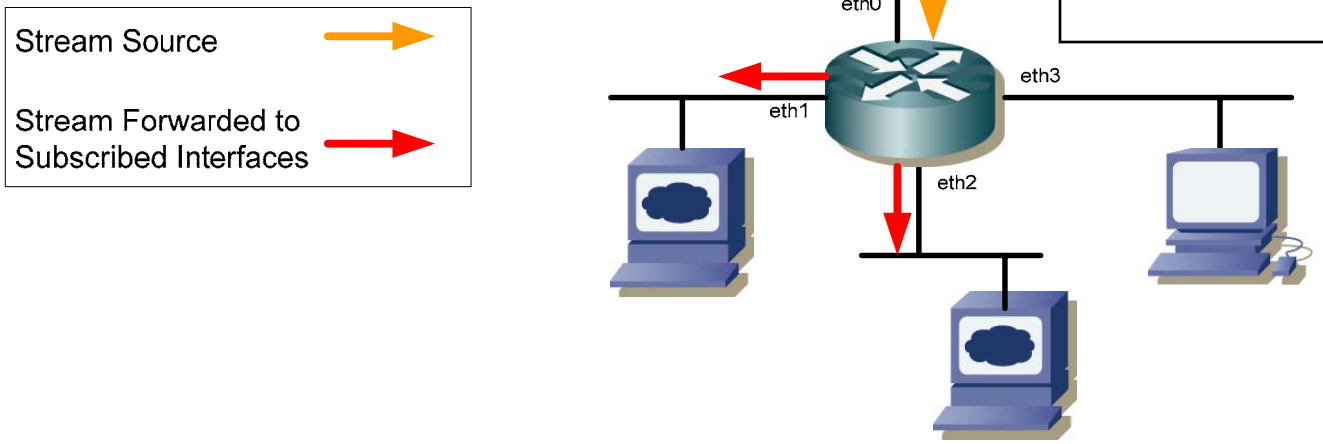
Multicast , The Traffic Reporting Problems

- **Identifying Multicast usage from the network traffic**
  - **What Multicast groups were/are in use (at a specific time) ?**
- **Identifying the volume of Multicast traffic**
  - **How much multicast is there, in total or on a per group basis ?**
  - **Over a defined time period ?**
- **Identifying which links are carrying Multicast traffic**
  - **Which interfaces were carrying traffic ?**
  - **For what groups and when ?**

Multicast NetFlow

- **NetFlow multicast allows you to capture multicast-specific data for multicast flows**
- **You can use NetFlow multicast to identify and count multicast packets on the ingress side and/or the egress side of a router**

```
interface eth0
    ip route-cache flow
interface eth1
    ip multicast netflow egress
interface eth2
    ip multicast netflow egress
interface eth3
    ip multicast netflow egress
```



NetFlow Tracker - Recommendations

- **Due to the interface information provided by Multicast NetFlow, we recommend that both NetFlow Ingress and Multicast Egress be configured.**

  –Ingress, multicast flows are stamped with an inbound interface and NO outbound interface ID.

SrcIF	SrcIPAddr	DstIF	DstIPAddr	Prot	TOS	Flags	SrcPort	SrcMask	DstPort	DstMask	NextHop	Bytes	Packets
eth0	192.168.1.1	Null	224.0.0.21	11	80	10	00A2	24	00A2	24		12223	23

  –Multicast Egress, flows are stamped with BOTH an inbound and an outbound interface ID.

SrcIF	SrcIPAddr	DstIF	DstIPAddr	Prot	TOS	Flags	SrcPort	SrcMask	DstPort	DstMask	NextHop	Bytes	Packets
eth0	192.168.1.1	eth1	224.0.0.21	11	80	10	00A2	24	00A2	24		12223	23
eth0	192.168.1.1	eth2	224.0.0.21	11	80	10	00A2	24	00A2	24		12223	23

NetFlow Tracker – How does it handle "NetFlow Multicast"

- **NetFlow Tracker nullifies the inbound interface of a multicast flow that has a valid outbound interface**

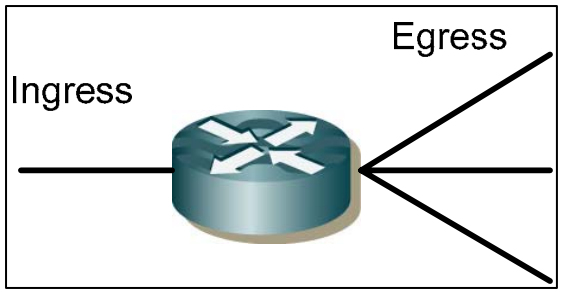
SrcIF	SrcIPAddr	DstIF	DstIPAddr	Prot	TOS	Flags	SrcPort	SrcMask	DstPort	DstMask	NextHop	Bytes	Packets
eth0	192.168.1.1	Null	224.0.0.21	11	80	10	00A2	24	00A2	24		12223	23

SrcIF	SrcIPAddr	DstIF	DstIPAddr	Prot	TOS	Flags	SrcPort	SrcMask	DstPort	DstMask	NextHop	Bytes	Packets
Null	192.168.1.1	eth1	224.0.0.21	11	80	10	00A2	24	00A2	24		12223	23
Null	192.168.1.1	eth2	224.0.0.21	11	80	10	00A2	24	00A2	24		12223	23

  - **It does have an added benefit: a flow is stored for each interface the traffic is routed out of, along with one for the interface it came in.**

  - **This means that all the interface traffic volume charts are correct, one stream in, one stream out!!!**

NetFlow Tracker – Interface Nullification Impact



	# Records for Ingress Interface	# Records For Egress Interface	Issue
Ingress Only	1	0	No record of outgoing Multicast
Egress Only	1 for each exit interface	1 for each exit interface	Dual (or more) for ingress interface
Ingress & Egress	1 for each exit interface + 1 for the ingress flow	1 for each exit interface	Dual (or more) for ingress interface
Ingress & Egress with Nullification	1	1 for each exit interface	

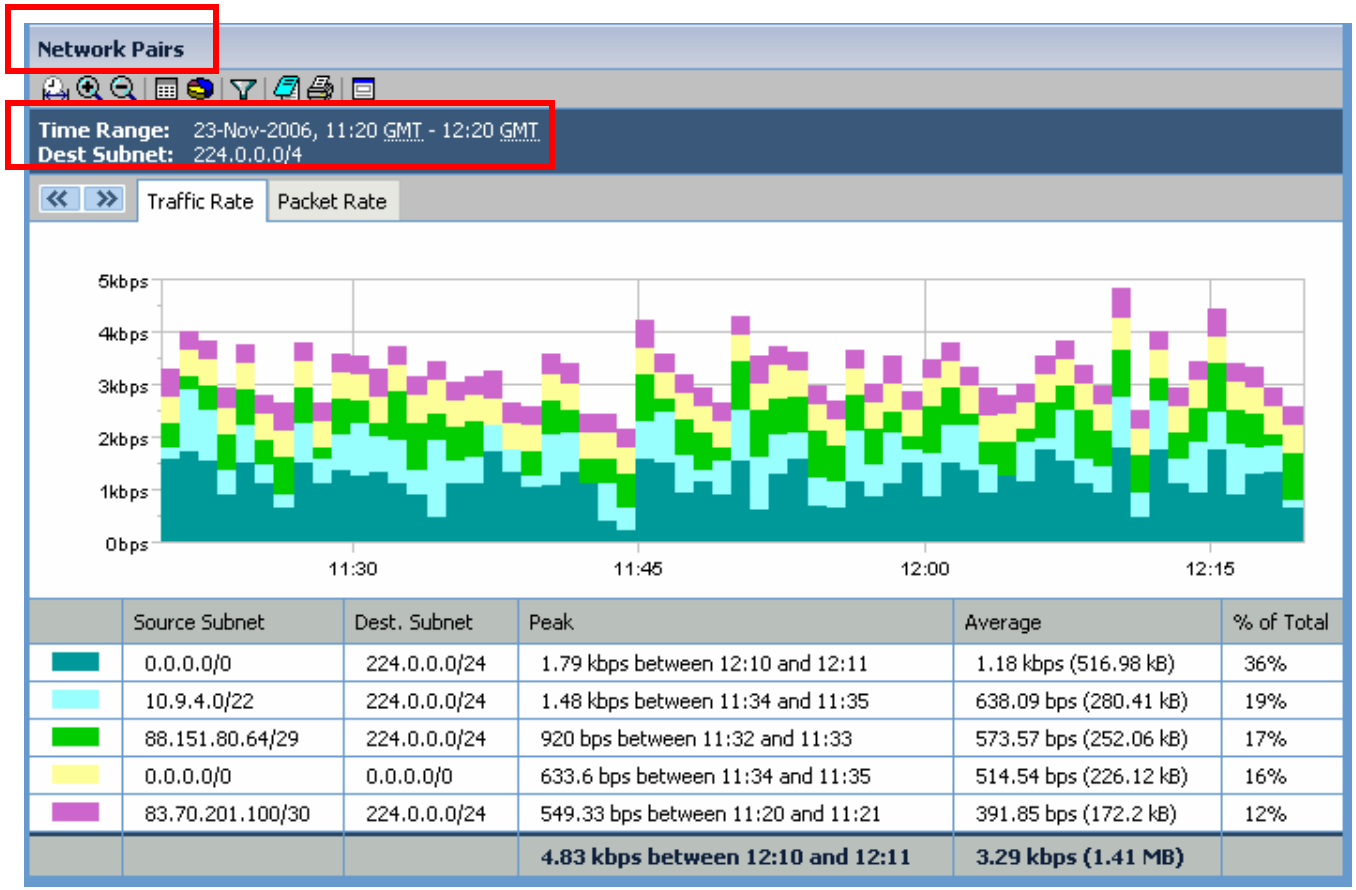
NetFlow Tracker - Multicast

Using NetFlow Tracker to Identify:

Networks Carrying Multicast
End Devices Generating Multicast

NetFlow Tracker – In Action

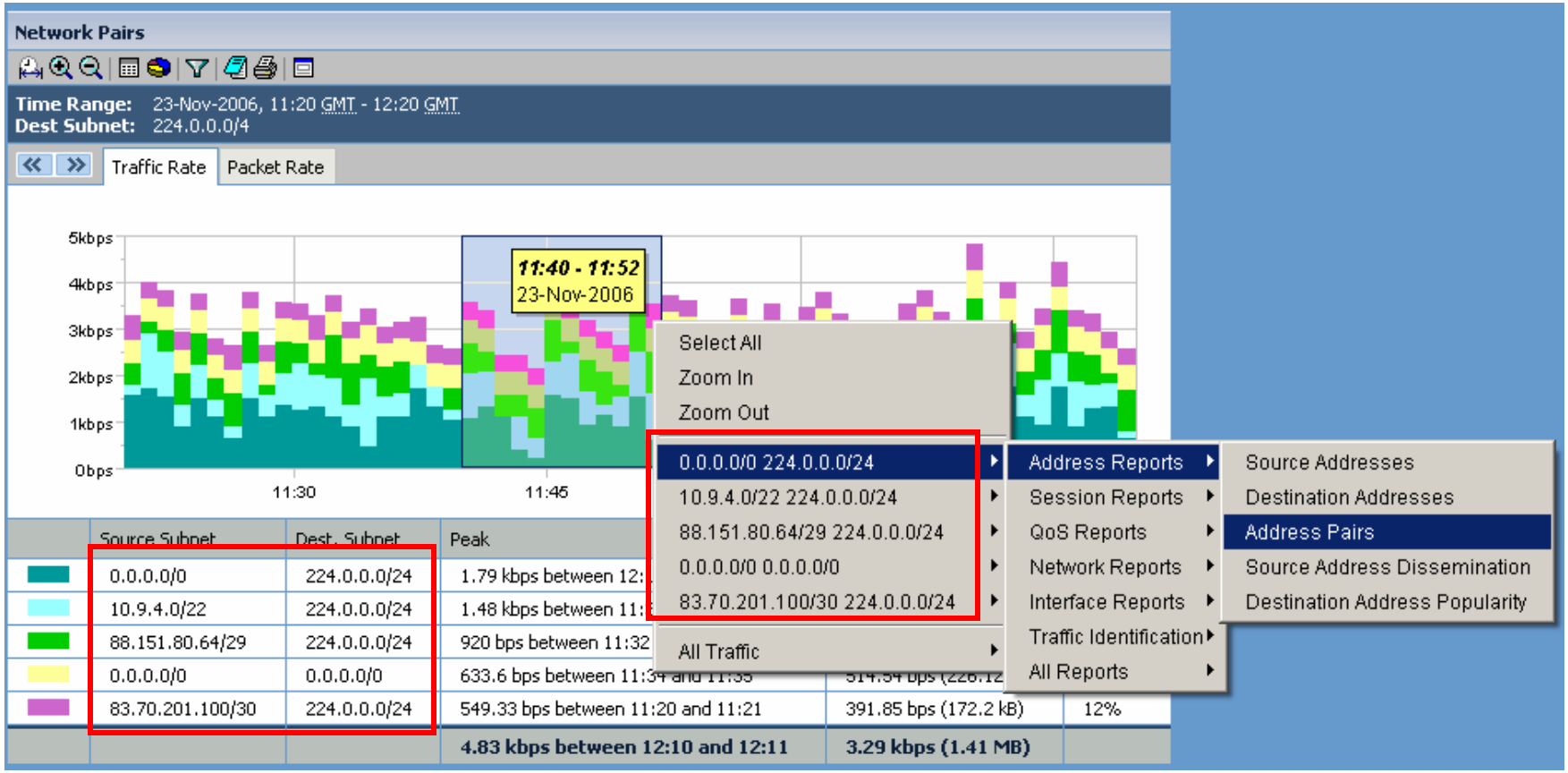
- **Use Tracker to filter for subnets carrying multicast**



	Source Subnet	Dest. Subnet	Peak	Average	% of Total
	0.0.0.0/0	224.0.0.0/24	1.79 kbps between 12:10 and 12:11	1.18 kbps (516.98 kB)	36%
	10.9.4.0/22	224.0.0.0/24	1.48 kbps between 11:34 and 11:35	638.09 bps (280.41 kB)	19%
	88.151.80.64/29	224.0.0.0/24	920 bps between 11:32 and 11:33	573.57 bps (252.06 kB)	17%
	0.0.0.0/0	0.0.0.0/0	633.6 bps between 11:34 and 11:35	514.54 bps (226.12 kB)	16%
	83.70.201.100/30	224.0.0.0/24	549.33 bps between 11:20 and 11:21	391.85 bps (172.2 kB)	12%
			4.83 kbps between 12:10 and 12:11	**3.29 kbps (1.41 MB)**	

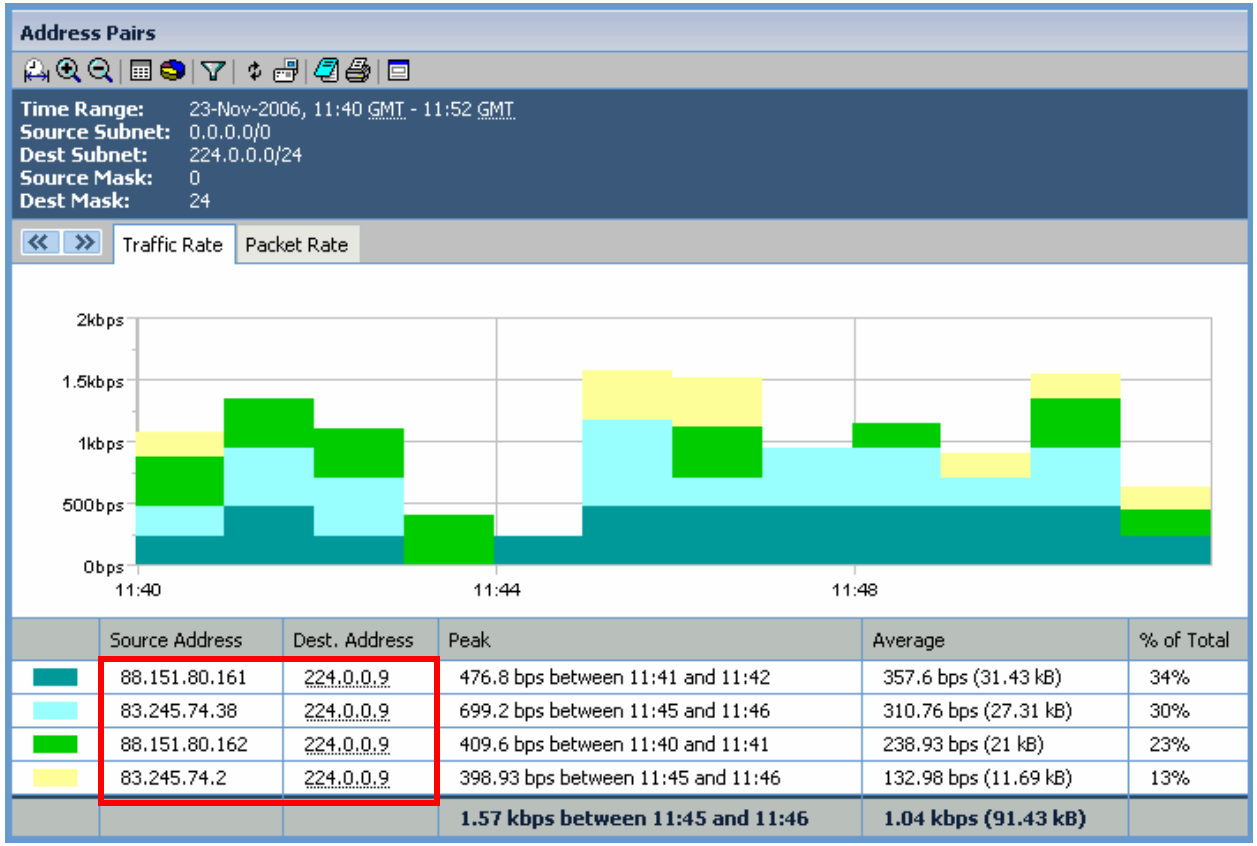
NetFlow Tracker – In Action

- **Focusing on a subnet pair of interest, lets see which addresses are being used**



NetFlow Tracker – In Action

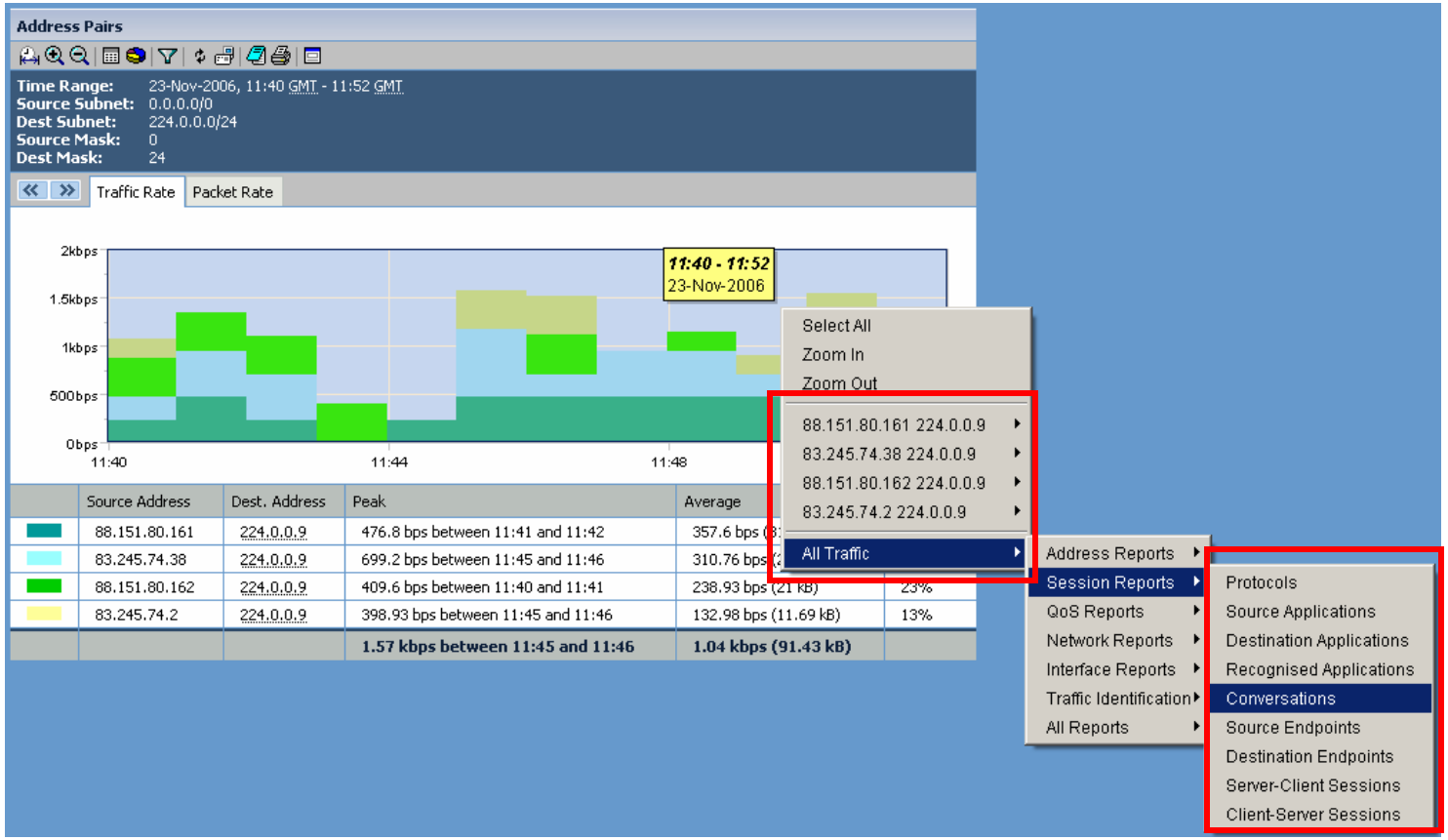
- **Here we can see the end devices which are generating multicast and the multicast group/address being used.**



	Source Address	Dest. Address	Peak	Average	% of Total
	88.151.80.161	224.0.0.9	476.8 bps between 11:41 and 11:42	357.6 bps (31.43 kB)	34%
	83.245.74.38	224.0.0.9	699.2 bps between 11:45 and 11:46	310.76 bps (27.31 kB)	30%
	88.151.80.162	224.0.0.9	409.6 bps between 11:40 and 11:41	238.93 bps (21 kB)	23%
	83.245.74.2	224.0.0.9	398.93 bps between 11:45 and 11:46	132.98 bps (11.69 kB)	13%
			1.57 kbps between 11:45 and 11:46	**1.04 kbps (91.43 kB)**	

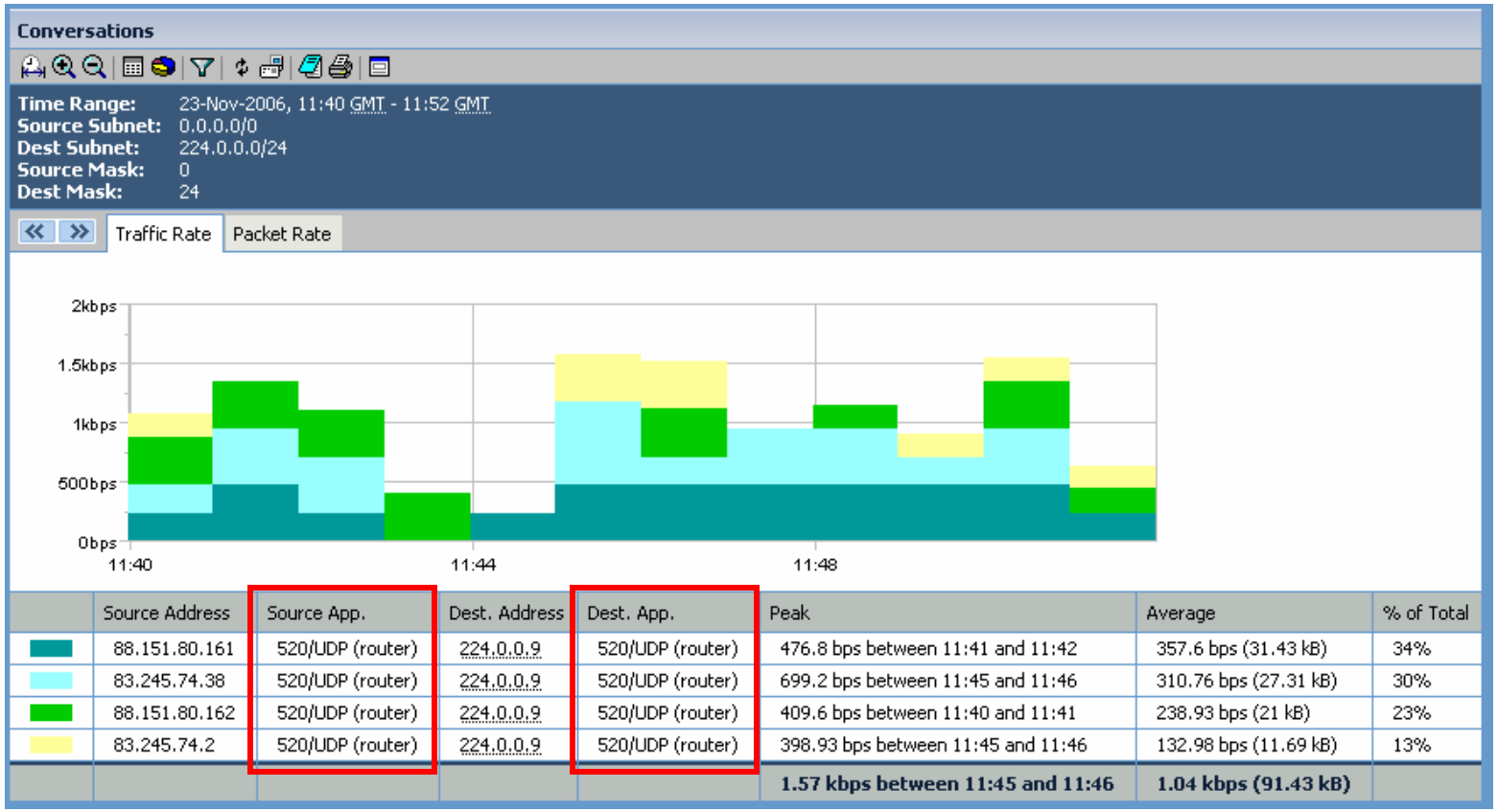
NetFlow Tracker – In Action

- **Selecting these addresses we can no look at the individual flows to see what applications are being carried by the multicast traffic.**



NetFlow Tracker – In Action

- **Now we can see the application/port details**



	Source Address	Source App.	Dest. Address	Dest. App.	Peak	Average	% of Total
	88.151.80.161	520/UDP (router)	224.0.0.9	520/UDP (router)	476.8 bps between 11:41 and 11:42	357.6 bps (31.43 kB)	34%
	83.245.74.38	520/UDP (router)	224.0.0.9	520/UDP (router)	699.2 bps between 11:45 and 11:46	310.76 bps (27.31 kB)	30%
	88.151.80.162	520/UDP (router)	224.0.0.9	520/UDP (router)	409.6 bps between 11:40 and 11:41	238.93 bps (21 kB)	23%
	83.245.74.2	520/UDP (router)	224.0.0.9	520/UDP (router)	398.93 bps between 11:45 and 11:46	132.98 bps (11.69 kB)	13%
					1.57 kbps between 11:45 and 11:46	**1.04 kbps (91.43 kB)**	

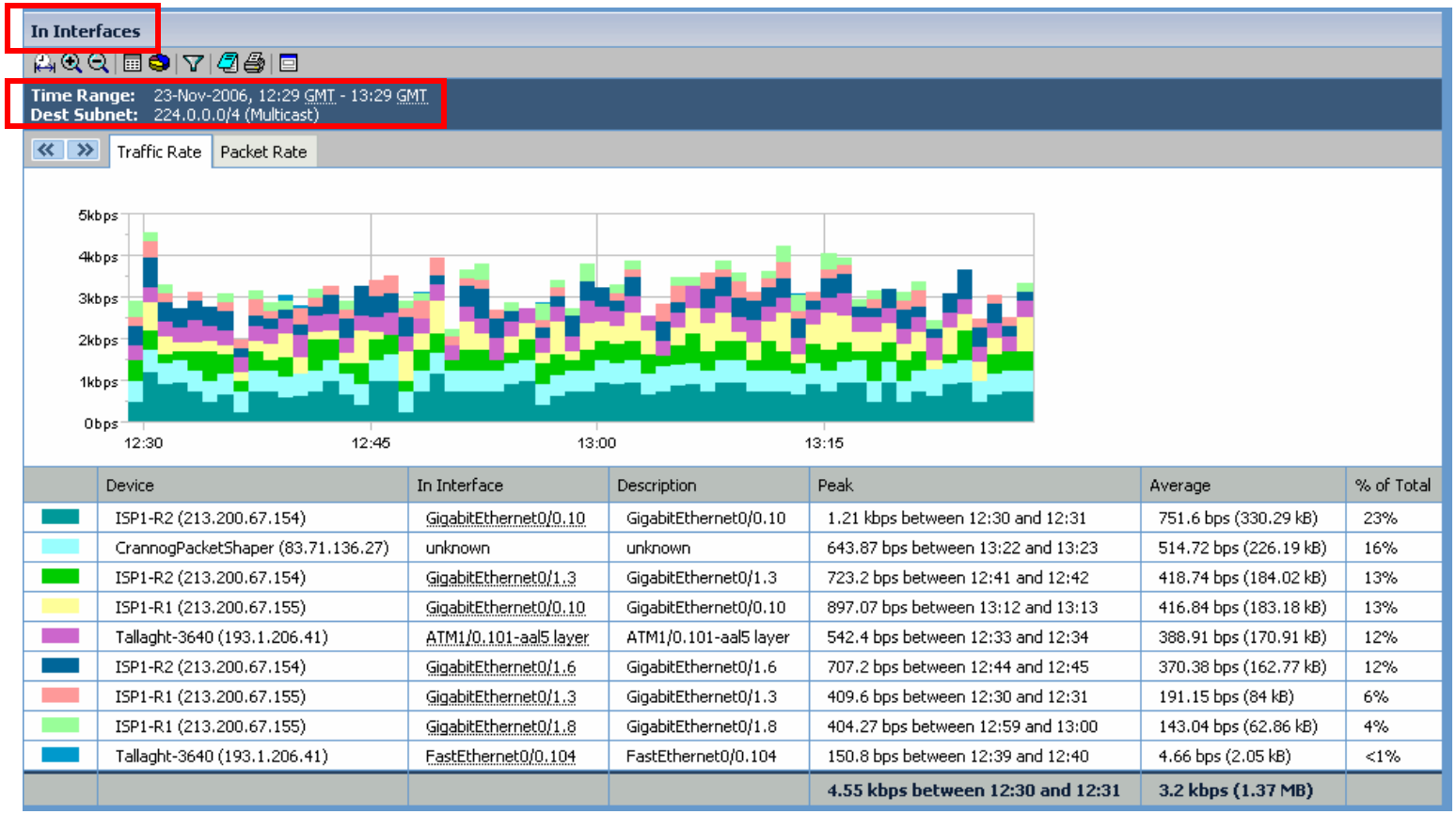
NetFlow Tracker - Multicast

Using NetFlow Tracker to Identify:

Interfaces Carrying Multicast

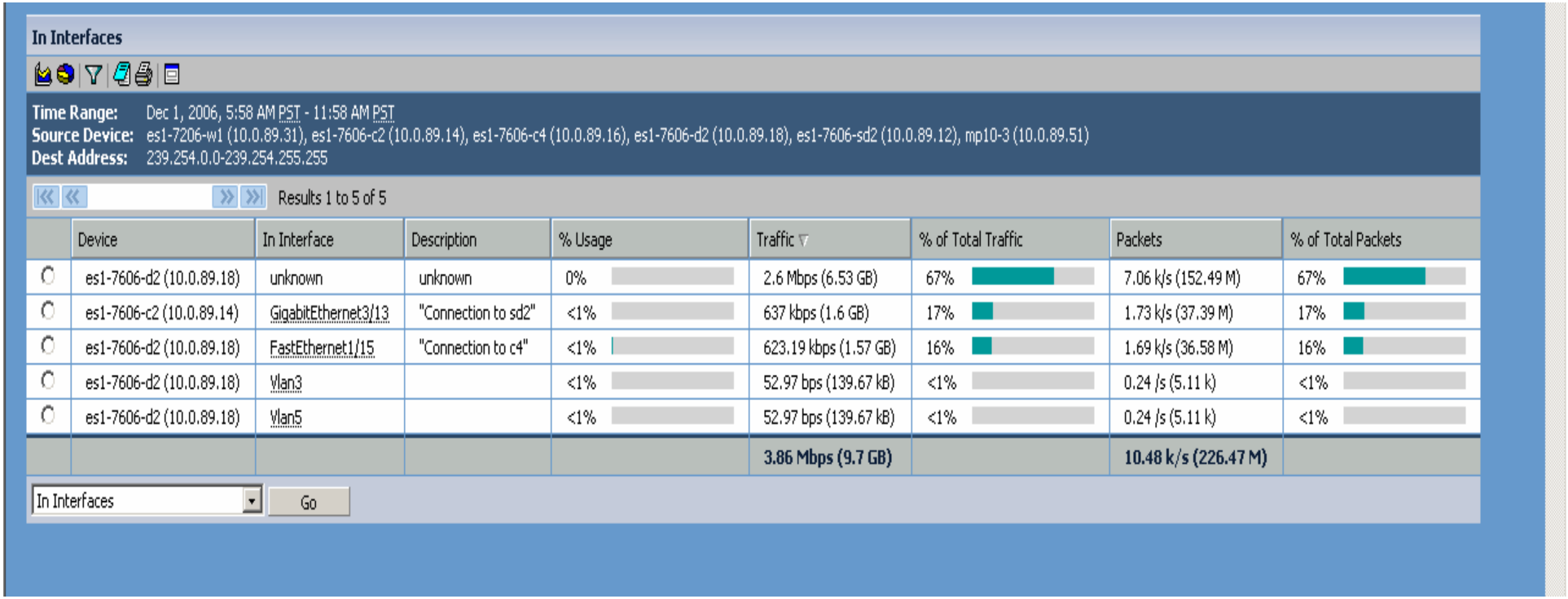
NetFlow Tracker – In Action

- **Selecting an Interface report and applying the multicast subnet filter provides us with the interfaces delivering Multicast around the network**



Device	In Interface	Description	Peak	Average	% of Total
ISP1-R2 (213.200.67.154)	GigabitEthernet0/0.10	GigabitEthernet0/0.10	1.21 kbps between 12:30 and 12:31	751.6 bps (330.29 kB)	23%
CrannogPacketShaper (83.71.136.27)	unknown	unknown	643.87 bps between 13:22 and 13:23	514.72 bps (226.19 kB)	16%
ISP1-R2 (213.200.67.154)	GigabitEthernet0/1.3	GigabitEthernet0/1.3	723.2 bps between 12:41 and 12:42	418.74 bps (184.02 kB)	13%
ISP1-R1 (213.200.67.155)	GigabitEthernet0/0.10	GigabitEthernet0/0.10	897.07 bps between 13:12 and 13:13	416.84 bps (183.18 kB)	13%
Tallaght-3640 (193.1.206.41)	ATM1/0.101-aal5 layer	ATM1/0.101-aal5 layer	542.4 bps between 12:33 and 12:34	388.91 bps (170.91 kB)	12%
ISP1-R2 (213.200.67.154)	GigabitEthernet0/1.6	GigabitEthernet0/1.6	707.2 bps between 12:44 and 12:45	370.38 bps (162.77 kB)	12%
ISP1-R1 (213.200.67.155)	GigabitEthernet0/1.3	GigabitEthernet0/1.3	409.6 bps between 12:30 and 12:31	191.15 bps (84 kB)	6%
ISP1-R1 (213.200.67.155)	GigabitEthernet0/1.8	GigabitEthernet0/1.8	404.27 bps between 12:59 and 13:00	143.04 bps (62.86 kB)	4%
Tallaght-3640 (193.1.206.41)	FastEthernet0/0.104	FastEthernet0/0.104	150.8 bps between 12:39 and 12:40	4.66 bps (2.05 kB)	<1%
			4.55 kbps between 12:30 and 12:31	**3.2 kbps (1.37 MB)**	

Multicast per Device Interface 239.254.0.0-239.254.255.255



In Interfaces

Time Range: Dec 1, 2006, 5:58 AM PST - 11:58 AM PST
Source Device: es1-7206-w1 (10.0.89.31), es1-7606-c2 (10.0.89.14), es1-7606-c4 (10.0.89.16), es1-7606-d2 (10.0.89.18), es1-7606-sd2 (10.0.89.12), mp10-3 (10.0.89.51)
Dest Address: 239.254.0.0-239.254.255.255

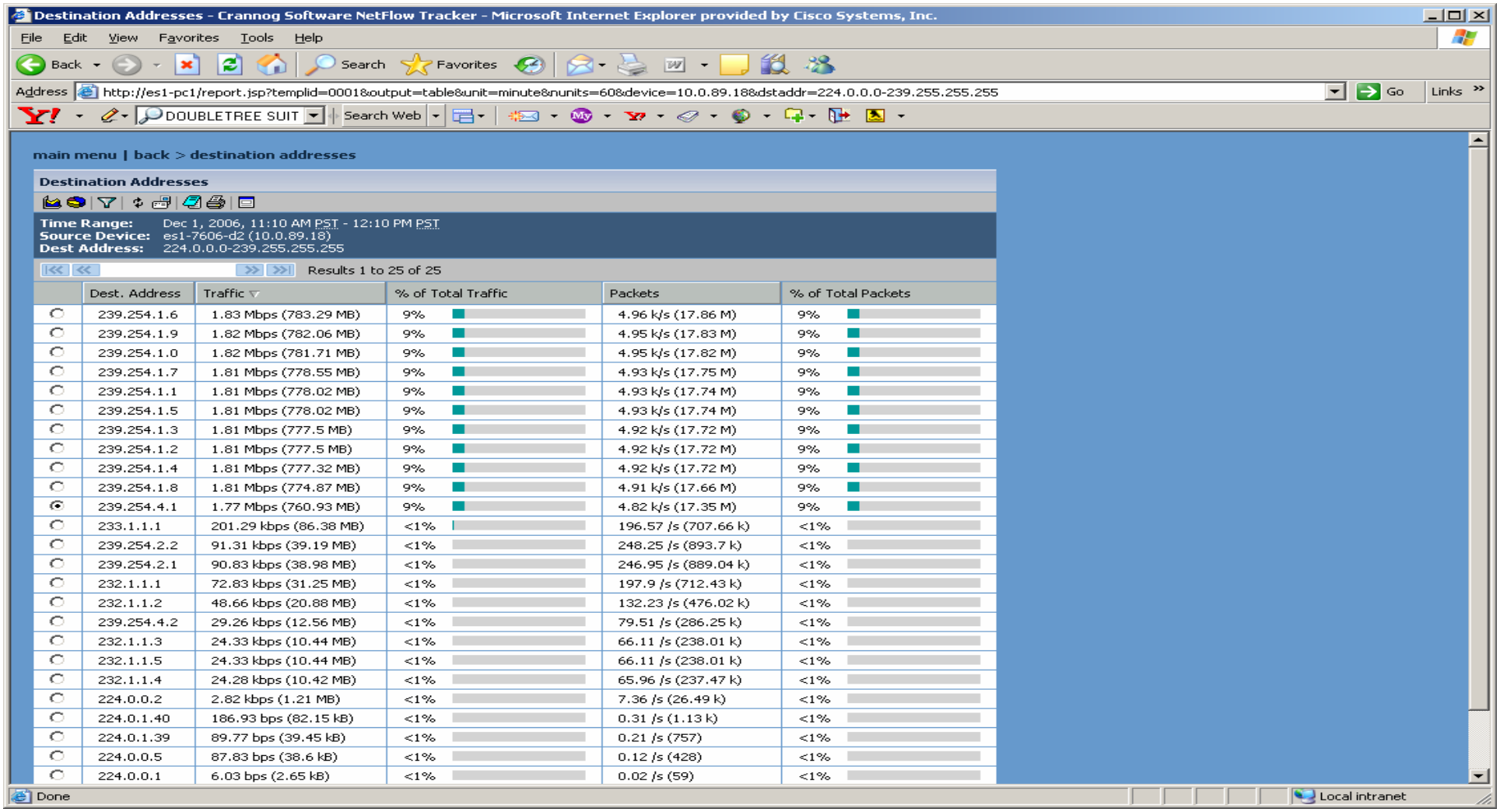
Results 1 to 5 of 5

Device	In Interface	Description	% Usage	Traffic	% of Total Traffic	Packets	% of Total Packets
es1-7606-d2 (10.0.89.18)	unknown	unknown	0%	2.6 Mbps (6.53 GB)	67%	7.06 k/s (152.49 M)	67%
es1-7606-c2 (10.0.89.14)	GigabitEthernet3/13	"Connection to sd2"	<1%	637 kbps (1.6 GB)	17%	1.73 k/s (37.39 M)	17%
es1-7606-d2 (10.0.89.18)	FastEthernet1/15	"Connection to c4"	<1%	623.19 kbps (1.57 GB)	16%	1.69 k/s (36.58 M)	16%
es1-7606-d2 (10.0.89.18)	Vlan3		<1%	52.97 bps (139.67 kB)	<1%	0.24 /s (5.11 k)	<1%
es1-7606-d2 (10.0.89.18)	Vlan5		<1%	52.97 bps (139.67 kB)	<1%	0.24 /s (5.11 k)	<1%
				3.86 Mbps (9.7 GB)		**10.48 k/s (226.47 M)**	

In Interfaces Go

CRANNOGSOFTWARE

Multicast volume per Multicast Group



Dest. Address	Traffic	% of Total Traffic	Packets	% of Total Packets
239.254.1.6	1.83 Mbps (783.29 MB)	9%	4.96 k/s (17.86 M)	9%
239.254.1.9	1.82 Mbps (782.06 MB)	9%	4.95 k/s (17.83 M)	9%
239.254.1.0	1.82 Mbps (781.71 MB)	9%	4.95 k/s (17.82 M)	9%
239.254.1.7	1.81 Mbps (778.55 MB)	9%	4.93 k/s (17.75 M)	9%
239.254.1.1	1.81 Mbps (778.02 MB)	9%	4.93 k/s (17.74 M)	9%
239.254.1.5	1.81 Mbps (778.02 MB)	9%	4.93 k/s (17.74 M)	9%
239.254.1.3	1.81 Mbps (777.5 MB)	9%	4.92 k/s (17.72 M)	9%
239.254.1.2	1.81 Mbps (777.5 MB)	9%	4.92 k/s (17.72 M)	9%
239.254.1.4	1.81 Mbps (777.32 MB)	9%	4.92 k/s (17.72 M)	9%
239.254.1.8	1.81 Mbps (774.87 MB)	9%	4.91 k/s (17.66 M)	9%
239.254.4.1	1.77 Mbps (760.93 MB)	9%	4.82 k/s (17.35 M)	9%
233.1.1.1	201.29 kbps (86.38 MB)	<1%	196.57 /s (707.66 k)	<1%
239.254.2.2	91.31 kbps (39.19 MB)	<1%	248.25 /s (893.7 k)	<1%
239.254.2.1	90.83 kbps (38.98 MB)	<1%	246.95 /s (889.04 k)	<1%
232.1.1.1	72.83 kbps (31.25 MB)	<1%	197.9 /s (712.43 k)	<1%
232.1.1.2	48.66 kbps (20.88 MB)	<1%	132.23 /s (476.02 k)	<1%
239.254.4.2	29.26 kbps (12.56 MB)	<1%	79.51 /s (286.25 k)	<1%
232.1.1.3	24.33 kbps (10.44 MB)	<1%	66.11 /s (238.01 k)	<1%
232.1.1.5	24.33 kbps (10.44 MB)	<1%	66.11 /s (238.01 k)	<1%
232.1.1.4	24.28 kbps (10.42 MB)	<1%	65.96 /s (237.47 k)	<1%
224.0.0.2	2.82 kbps (1.21 MB)	<1%	7.36 /s (26.49 k)	<1%
224.0.1.40	186.93 bps (82.15 kB)	<1%	0.31 /s (1.13 k)	<1%
224.0.1.39	89.77 bps (39.45 kB)	<1%	0.21 /s (757)	<1%
224.0.0.5	87.83 bps (38.6 kB)	<1%	0.12 /s (428)	<1%
224.0.0.1	6.03 bps (2.65 kB)	<1%	0.02 /s (59)	<1%

Source Addresses of Multicast 239.254.4.1

main menu | back > source addresses

Source Addresses

Time Range: Dec 1, 2006, 11:12 AM PST - 12:12 PM PST
Source Device: es1-7606-d2 (10.0.89.18)
Dest Address: 239.254.4.1

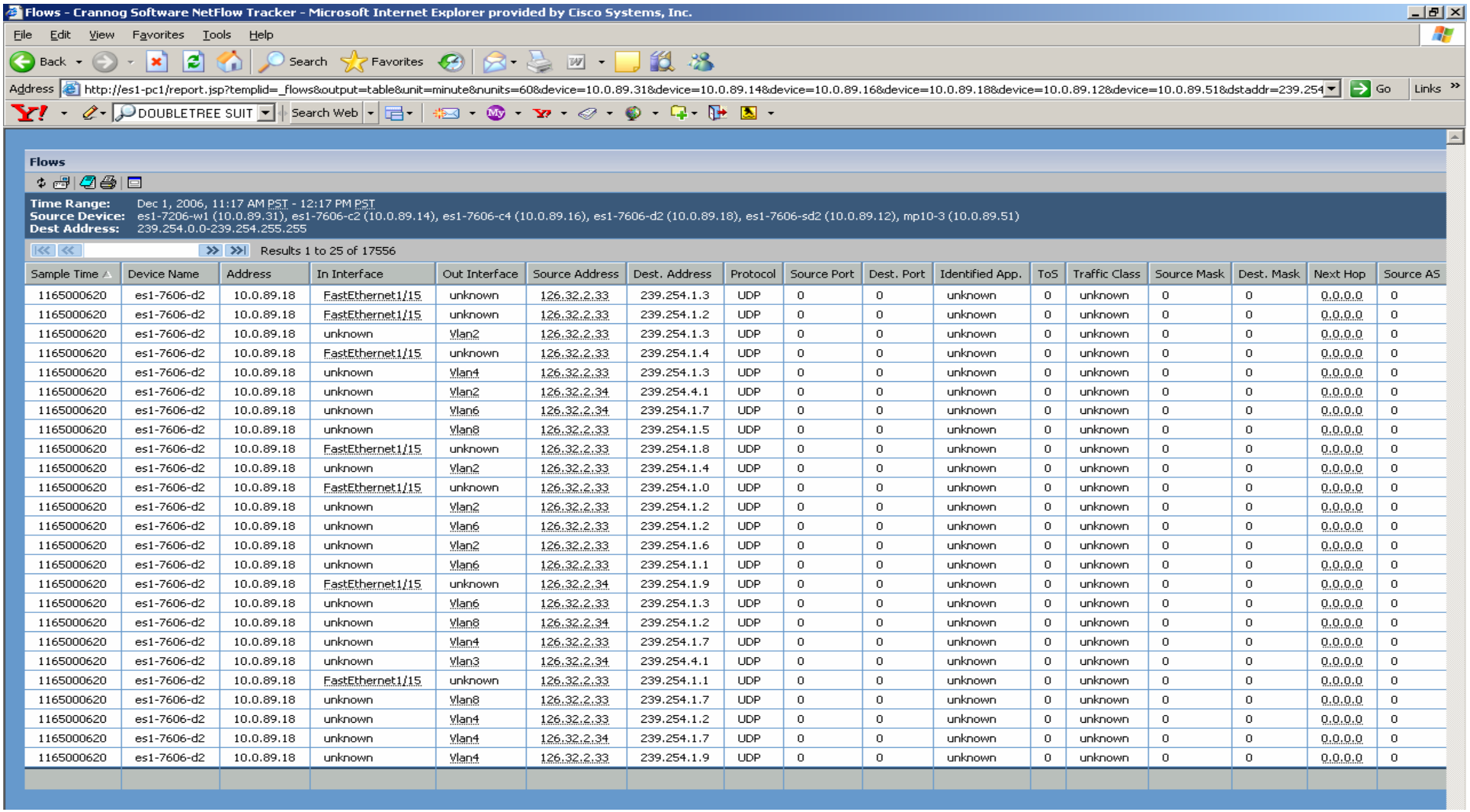
Results 1 to 12 of 12

Source Address	Traffic	% of Total Traffic	Packets	% of Total Packets
126.32.2.34	1.43 Mbps (612.43 MB)	82%	3.88 k/s (13.96 M)	82%
126.32.2.36	28.85 kbps (12.38 MB)	2%	78.4 /s (282.26 k)	2%
126.32.2.40	28.72 kbps (12.32 MB)	2%	78.03 /s (280.92 k)	2%
126.32.2.33	28.67 kbps (12.3 MB)	2%	77.91 /s (280.49 k)	2%
126.32.2.44	28.37 kbps (12.17 MB)	2%	77.09 /s (277.53 k)	2%
126.32.2.39	28.33 kbps (12.16 MB)	2%	76.99 /s (277.15 k)	2%
126.32.2.35	28.31 kbps (12.15 MB)	2%	76.92 /s (276.9 k)	2%
126.32.2.43	28.18 kbps (12.1 MB)	2%	76.59 /s (275.71 k)	2%
126.32.2.37	28.16 kbps (12.09 MB)	2%	76.53 /s (275.51 k)	2%
126.32.2.41	28.1 kbps (12.06 MB)	2%	76.37 /s (274.94 k)	2%
126.32.2.42	28.1 kbps (12.06 MB)	2%	76.36 /s (274.91 k)	2%
126.32.2.38	27.94 kbps (11.99 MB)	2%	75.93 /s (273.35 k)	2%
	1.74 Mbps (746.22 MB)		**4.73 k/s (17.01 M)**	

Source Addresses | Go

CRANNOGSOFTWARE

Full Fields _flows



Flows

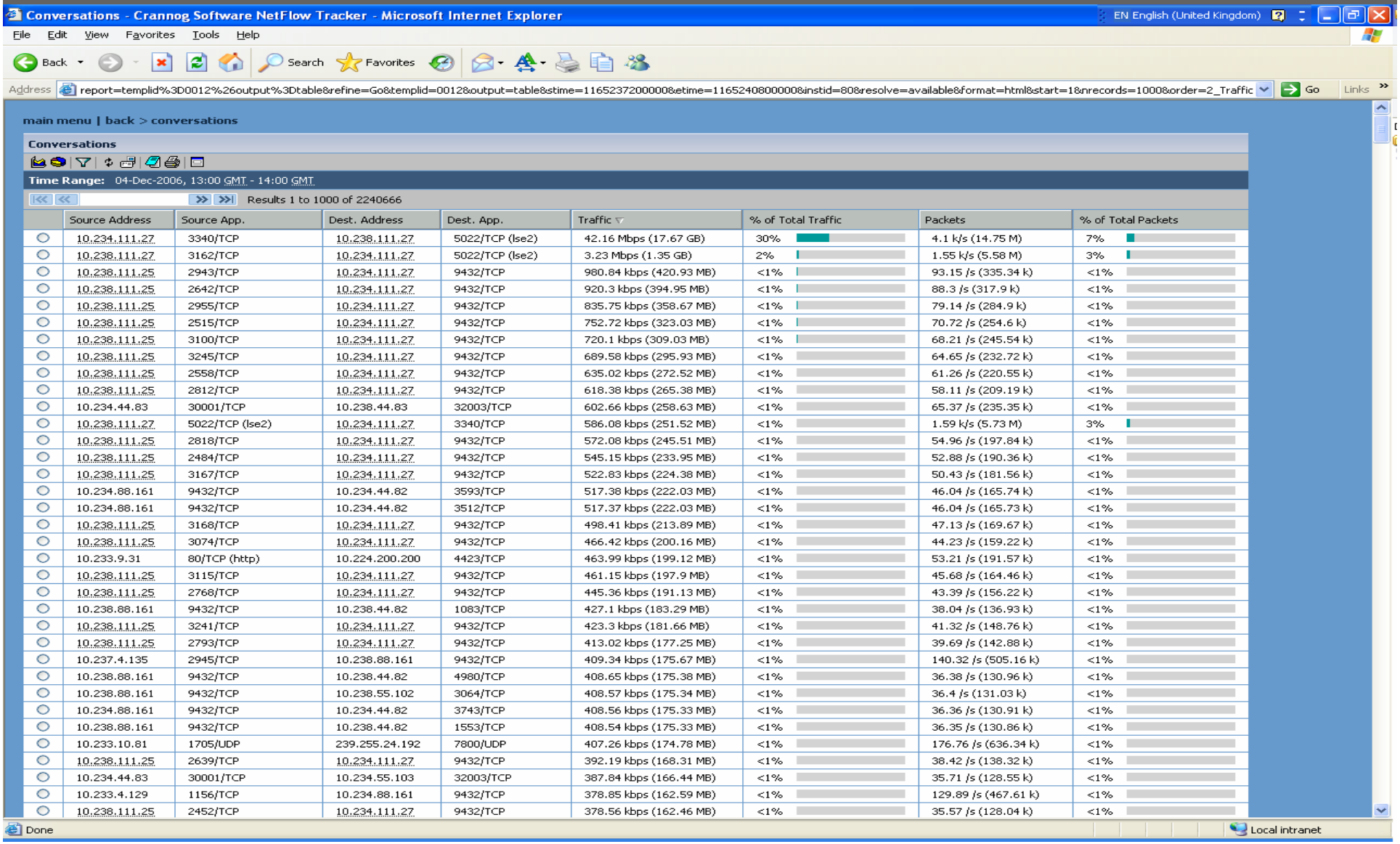
Time Range: Dec 1, 2006, 11:17 AM PST - 12:17 PM PST
Source Device: es1-7206-w1 (10.0.89.31), es1-7606-c2 (10.0.89.14), es1-7606-c4 (10.0.89.16), es1-7606-d2 (10.0.89.18), es1-7606-sd2 (10.0.89.12), mp10-3 (10.0.89.51)
Dest Address: 239.254.0.0-239.254.255.255

Results 1 to 25 of 17556

Sample Time	Device Name	Address	In Interface	Out Interface	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	Identified App.	ToS	Traffic Class	Source Mask	Dest. Mask	Next Hop	Source AS
1165000620	es1-7606-d2	10.0.89.18	FastEthernet1/15	unknown	126.32.2.33	239.254.1.3	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	FastEthernet1/15	unknown	126.32.2.33	239.254.1.2	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan2	126.32.2.33	239.254.1.3	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	FastEthernet1/15	unknown	126.32.2.33	239.254.1.4	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan4	126.32.2.33	239.254.1.3	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan2	126.32.2.34	239.254.4.1	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan6	126.32.2.34	239.254.1.7	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan8	126.32.2.33	239.254.1.5	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	FastEthernet1/15	unknown	126.32.2.33	239.254.1.8	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan2	126.32.2.33	239.254.1.4	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	FastEthernet1/15	unknown	126.32.2.33	239.254.1.0	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan2	126.32.2.33	239.254.1.2	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan6	126.32.2.33	239.254.1.2	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan2	126.32.2.33	239.254.1.6	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan6	126.32.2.33	239.254.1.1	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	FastEthernet1/15	unknown	126.32.2.34	239.254.1.9	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan6	126.32.2.33	239.254.1.3	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan8	126.32.2.34	239.254.1.2	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan4	126.32.2.33	239.254.1.7	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan3	126.32.2.34	239.254.4.1	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	FastEthernet1/15	unknown	126.32.2.33	239.254.1.1	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan8	126.32.2.33	239.254.1.7	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan4	126.32.2.33	239.254.1.2	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan4	126.32.2.34	239.254.1.7	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0
1165000620	es1-7606-d2	10.0.89.18	unknown	Vlan4	126.32.2.33	239.254.1.9	UDP	0	0	unknown	0	unknown	0	0	0.0.0.0	0

CRANNOGSOFTWARE

LSE



Conversations - Crannog Software NetFlow Tracker - Microsoft Internet Explorer

EN English (United Kingdom)

File Edit View Favorites Tools Help

Back Search Favorites

Address report=templid%3D0012%26output%3Dtable&refine=Go&templid=0012&output=table&stime=1165237200000&etime=1165240800000&instid=80&resolve=available&format=html&start=1&nrecords=1000&order=2_Traffic Go Links

main menu | back > conversations

Conversations

Time Range: 04-Dec-2006, 13:00 GMT - 14:00 GMT

Results 1 to 1000 of 2240666

Source Address	Source App.	Dest. Address	Dest. App.	Traffic	% of Total Traffic	Packets	% of Total Packets
10.234.111.27	3340/TCP	10.238.111.27	5022/TCP (lse2)	42.16 Mbps (17.67 GB)	30%	4.1 k/s (14.75 M)	7%
10.238.111.27	3162/TCP	10.234.111.27	5022/TCP (lse2)	3.23 Mbps (1.35 GB)	2%	1.55 k/s (5.58 M)	3%
10.238.111.25	2943/TCP	10.234.111.27	9432/TCP	980.84 kbps (420.93 MB)	<1%	93.15 /s (335.34 k)	<1%
10.238.111.25	2642/TCP	10.234.111.27	9432/TCP	920.3 kbps (394.95 MB)	<1%	88.3 /s (317.9 k)	<1%
10.238.111.25	2955/TCP	10.234.111.27	9432/TCP	835.75 kbps (358.67 MB)	<1%	79.14 /s (284.9 k)	<1%
10.238.111.25	2515/TCP	10.234.111.27	9432/TCP	752.72 kbps (323.03 MB)	<1%	70.72 /s (254.6 k)	<1%
10.238.111.25	3100/TCP	10.234.111.27	9432/TCP	720.1 kbps (309.03 MB)	<1%	68.21 /s (245.54 k)	<1%
10.238.111.25	3245/TCP	10.234.111.27	9432/TCP	689.58 kbps (295.93 MB)	<1%	64.65 /s (232.72 k)	<1%
10.238.111.25	2558/TCP	10.234.111.27	9432/TCP	635.02 kbps (272.52 MB)	<1%	61.26 /s (220.55 k)	<1%
10.238.111.25	2812/TCP	10.234.111.27	9432/TCP	618.38 kbps (265.38 MB)	<1%	58.11 /s (209.19 k)	<1%
10.234.44.83	30001/TCP	10.238.44.83	32003/TCP	602.66 kbps (258.63 MB)	<1%	65.37 /s (235.35 k)	<1%
10.238.111.27	5022/TCP (lse2)	10.234.111.27	3340/TCP	586.08 kbps (251.52 MB)	<1%	1.59 k/s (5.73 M)	3%
10.238.111.25	2818/TCP	10.234.111.27	9432/TCP	572.08 kbps (245.51 MB)	<1%	54.96 /s (197.84 k)	<1%
10.238.111.25	2484/TCP	10.234.111.27	9432/TCP	545.15 kbps (233.95 MB)	<1%	52.88 /s (190.36 k)	<1%
10.238.111.25	3167/TCP	10.234.111.27	9432/TCP	522.83 kbps (224.38 MB)	<1%	50.43 /s (181.56 k)	<1%
10.234.88.161	9432/TCP	10.234.44.82	3593/TCP	517.38 kbps (222.03 MB)	<1%	46.04 /s (165.74 k)	<1%
10.234.88.161	9432/TCP	10.234.44.82	3512/TCP	517.37 kbps (222.03 MB)	<1%	46.04 /s (165.73 k)	<1%
10.238.111.25	3168/TCP	10.234.111.27	9432/TCP	498.41 kbps (213.89 MB)	<1%	47.13 /s (169.67 k)	<1%
10.238.111.25	3074/TCP	10.234.111.27	9432/TCP	466.42 kbps (200.16 MB)	<1%	44.23 /s (159.22 k)	<1%
10.233.9.31	80/TCP (http)	10.224.200.200	4423/TCP	463.99 kbps (199.12 MB)	<1%	53.21 /s (191.57 k)	<1%
10.238.111.25	3115/TCP	10.234.111.27	9432/TCP	461.15 kbps (197.9 MB)	<1%	45.68 /s (164.46 k)	<1%
10.238.111.25	2768/TCP	10.234.111.27	9432/TCP	445.36 kbps (191.13 MB)	<1%	43.39 /s (156.22 k)	<1%
10.238.88.161	9432/TCP	10.238.44.82	1083/TCP	427.1 kbps (183.29 MB)	<1%	38.04 /s (136.93 k)	<1%
10.238.111.25	3241/TCP	10.234.111.27	9432/TCP	423.3 kbps (181.66 MB)	<1%	41.32 /s (148.76 k)	<1%
10.238.111.25	2793/TCP	10.234.111.27	9432/TCP	413.02 kbps (177.25 MB)	<1%	39.69 /s (142.88 k)	<1%
10.237.4.135	2945/TCP	10.238.88.161	9432/TCP	409.34 kbps (175.67 MB)	<1%	140.32 /s (505.16 k)	<1%
10.238.88.161	9432/TCP	10.238.44.82	4980/TCP	408.65 kbps (175.38 MB)	<1%	36.38 /s (130.96 k)	<1%
10.238.88.161	9432/TCP	10.238.55.102	3064/TCP	408.57 kbps (175.34 MB)	<1%	36.4 /s (131.03 k)	<1%
10.234.88.161	9432/TCP	10.234.44.82	3743/TCP	408.56 kbps (175.33 MB)	<1%	36.36 /s (130.91 k)	<1%
10.238.88.161	9432/TCP	10.238.44.82	1553/TCP	408.54 kbps (175.33 MB)	<1%	36.35 /s (130.86 k)	<1%
10.233.10.81	1705/UDP	239.255.24.192	7800/UDP	407.26 kbps (174.78 MB)	<1%	176.76 /s (636.34 k)	<1%
10.238.111.25	2639/TCP	10.234.111.27	9432/TCP	392.19 kbps (168.31 MB)	<1%	38.42 /s (138.32 k)	<1%
10.234.44.83	30001/TCP	10.234.55.103	32003/TCP	387.84 kbps (166.44 MB)	<1%	35.71 /s (128.55 k)	<1%
10.233.4.129	1156/TCP	10.234.88.161	9432/TCP	378.85 kbps (162.59 MB)	<1%	129.89 /s (467.61 k)	<1%
10.238.111.25	2452/TCP	10.234.111.27	9432/TCP	378.56 kbps (162.46 MB)	<1%	35.57 /s (128.04 k)	<1%

Done

Local intranet

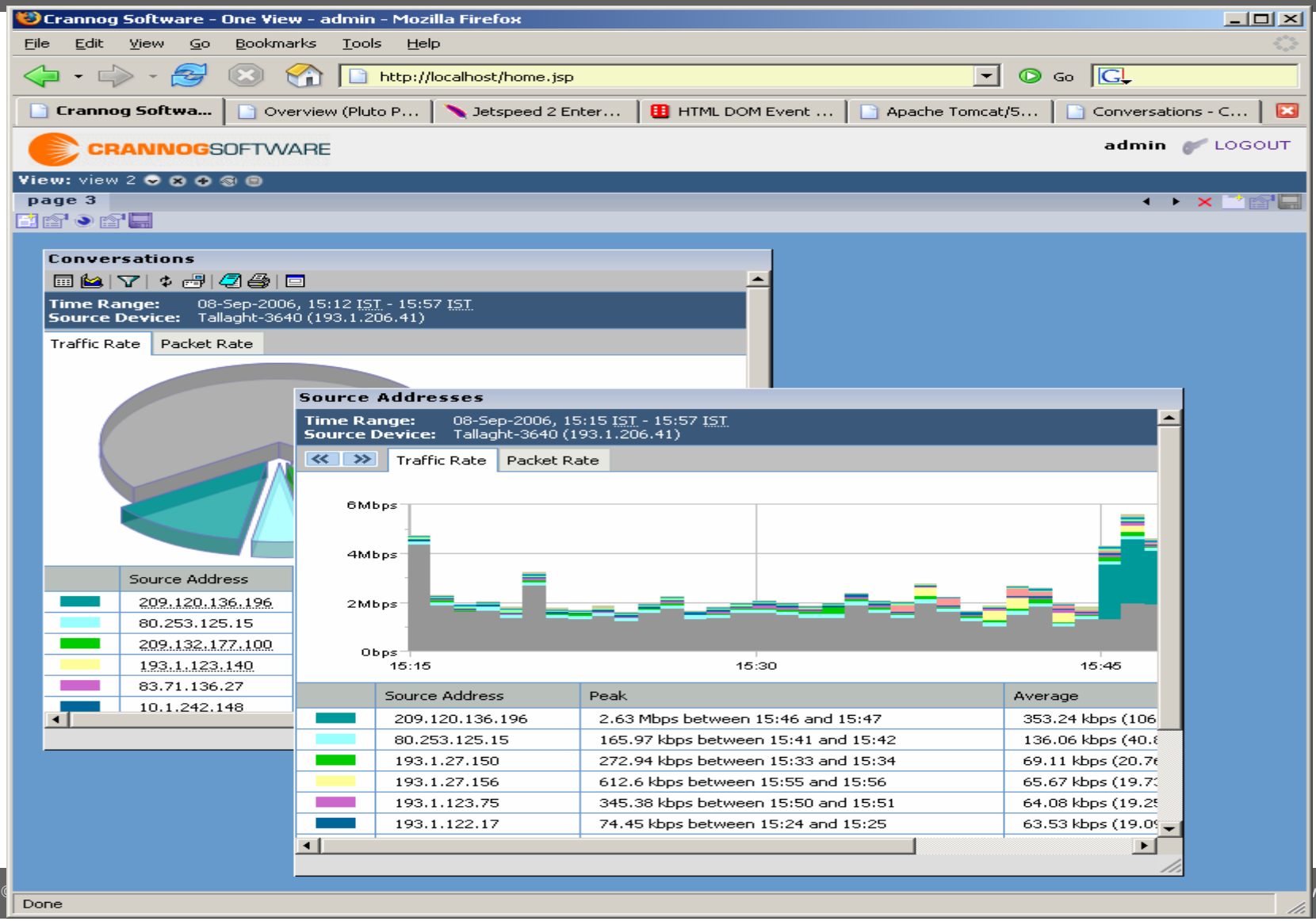
NetFlow Tracker – What does it provide

- **Identifying Multicast groups from network traffic ✓**
- **What Multicast groups were/are in use ✓**
- **Identifying the volume of Multicast traffic ✓**
- **How much in total or on a per address basis ✓**
- **Over a defined time period ✓**
- **Which interfaces are carrying traffic ✓**
- **What addresses on each interface ✓**

OneView and Audience Appreciation

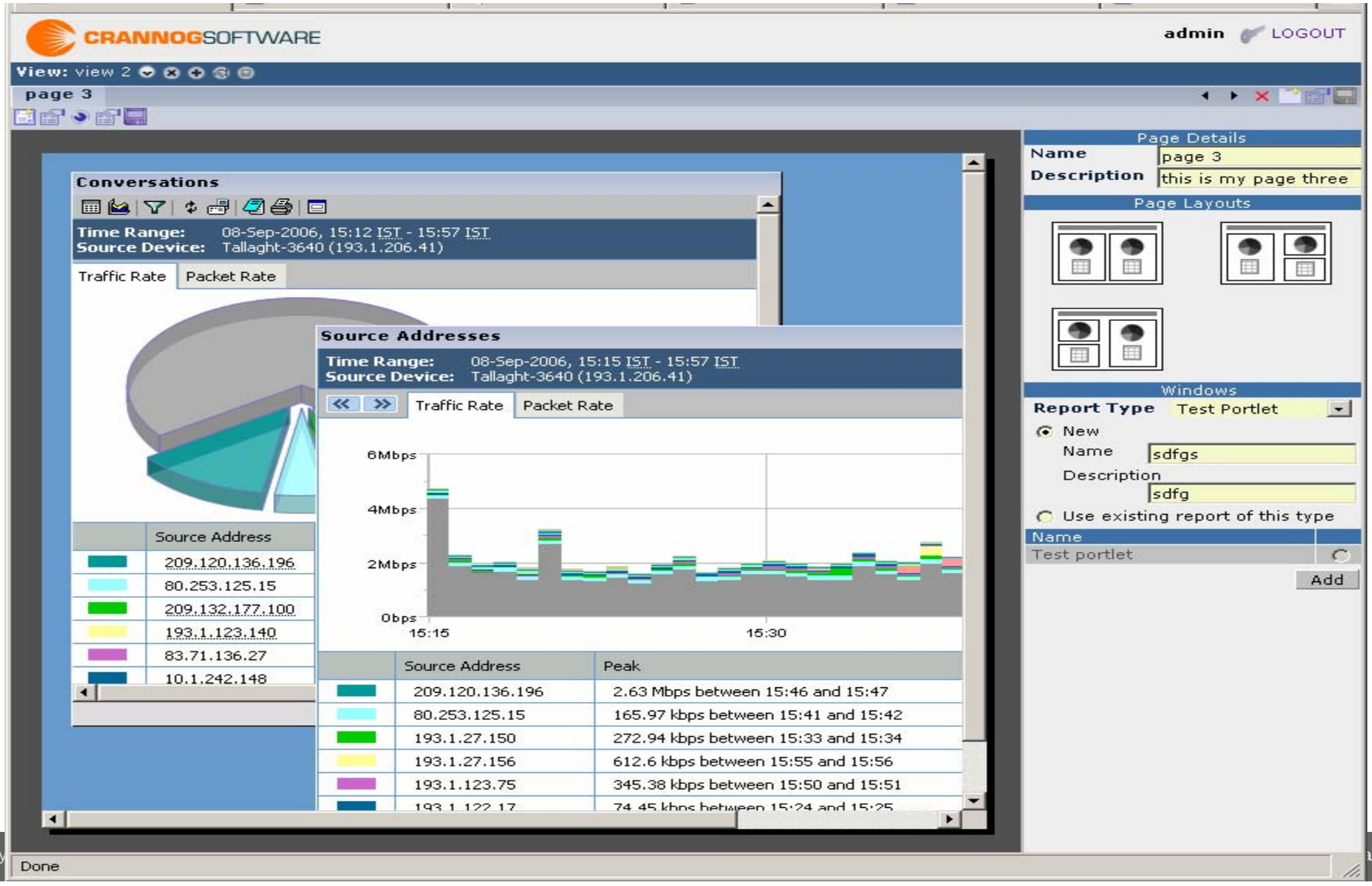
CRANNOGSOFTWARE

OneView New release



CRANNOGSOFTWARE

OneView New Editor



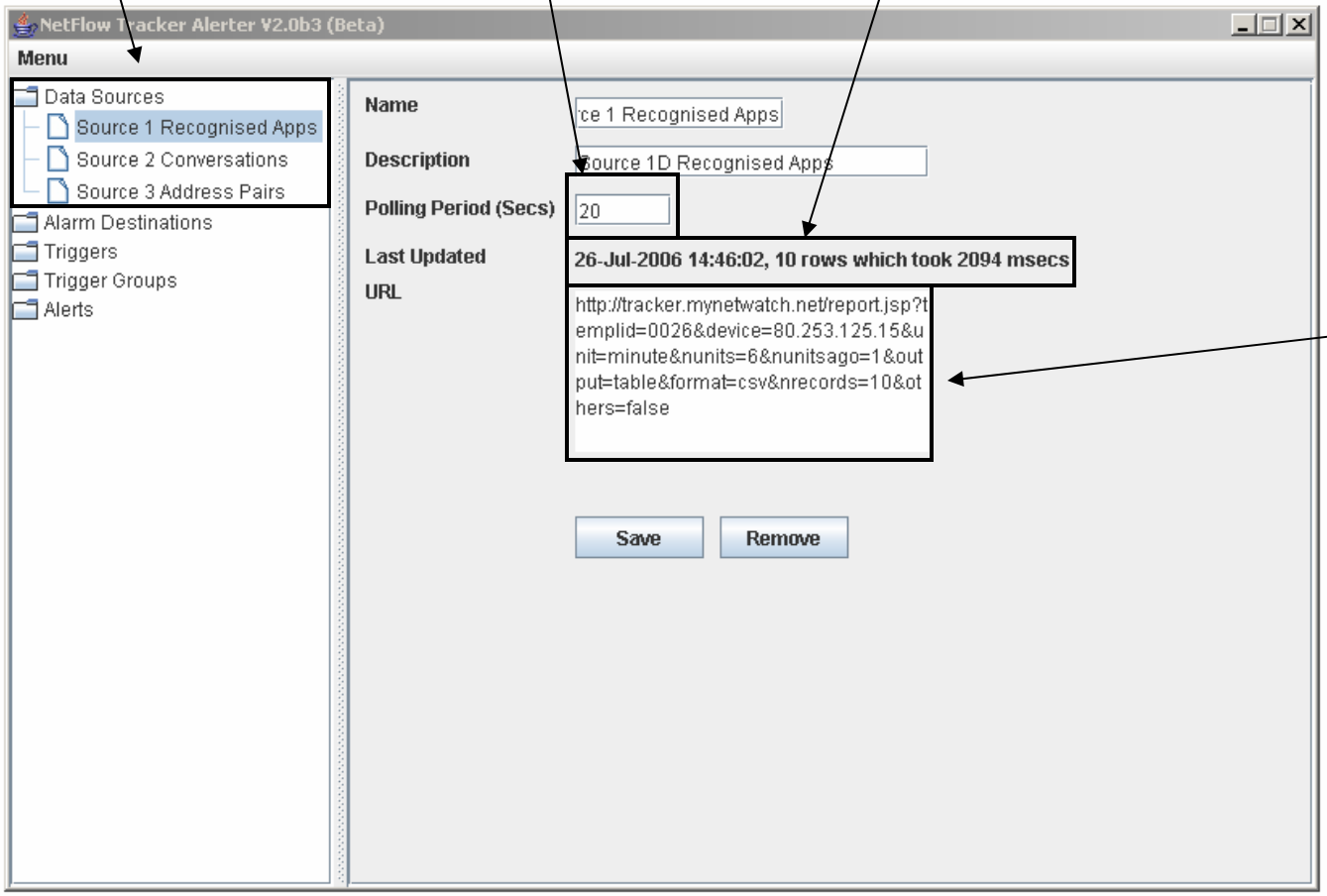
Netflow Alerting

Data Sources - In The Application

Right click to add new data source, left click to edit.

How long to cache report before re-polling

Lets you know when the report was last run, how many rows were returned and how long it took to "get"

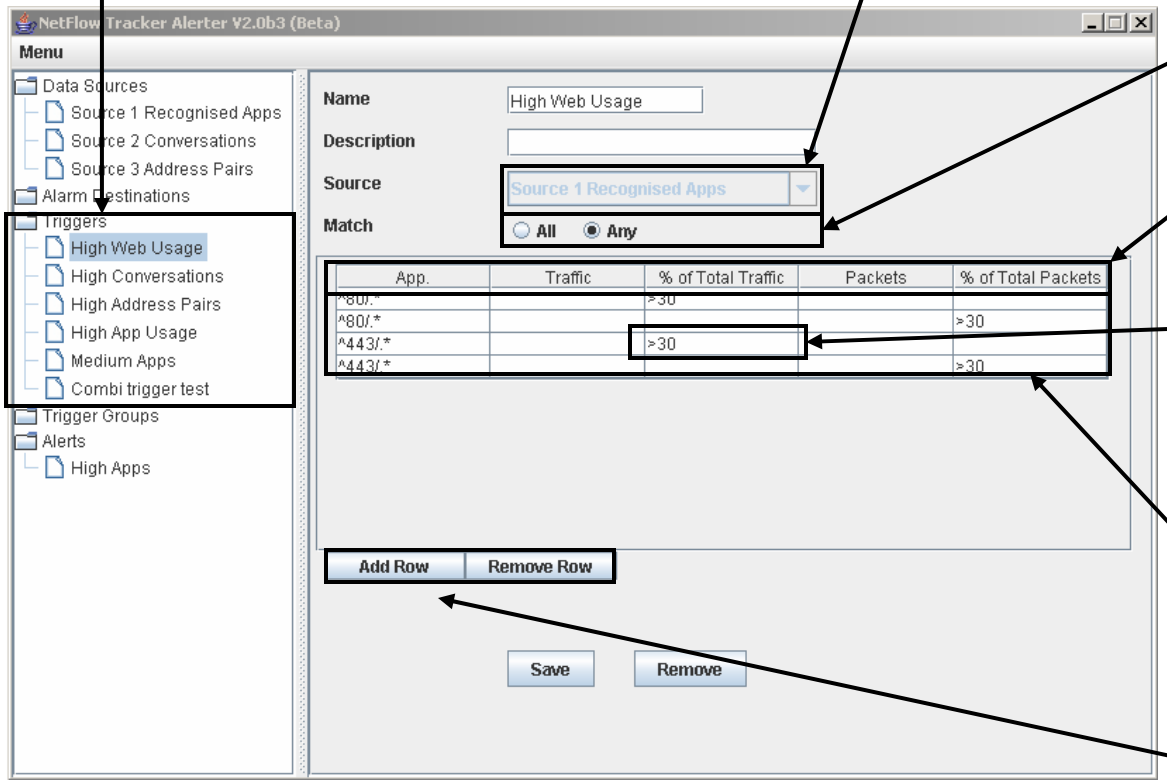


The "Clean" URL used to gather data from a particular tracker server. This is "cleaned" when you press the save button.

Trigger – In The Application

Right click to add new Trigger, left click to edit.

Select from the available data sources and press "Save"



Should this trigger match all rows or any row?

Columns for all reports are automatically presented when a source has been committed to by pressing "Save"

Directly edit each field by double clicking, blank cells are not evaluated. Populated cells are evaluated straight away (even if save isn't pressed)

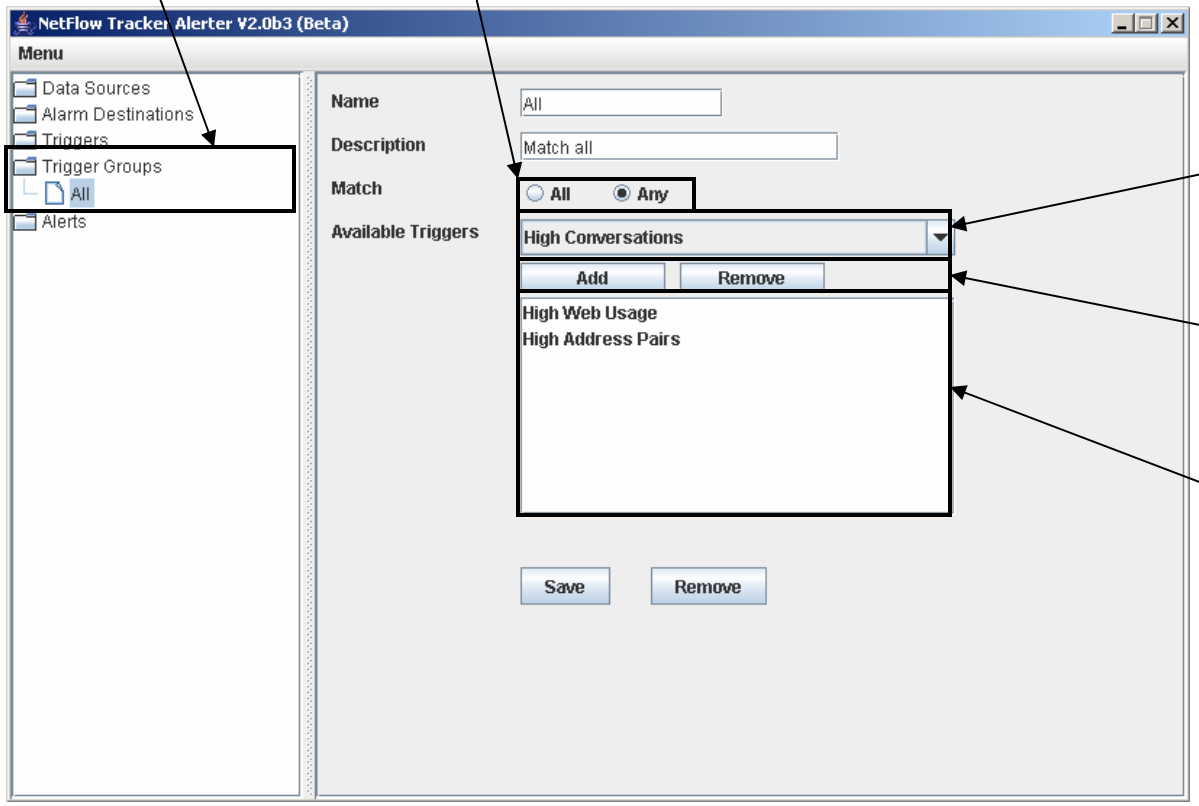
All populated fields in a row are evaluated

Add/Remove rows as requested

Trigger Groups – In The Application

Right click to add new trigger group, left click to edit.

Select to match any/all triggers within this group



Drop down menu lists all available triggers

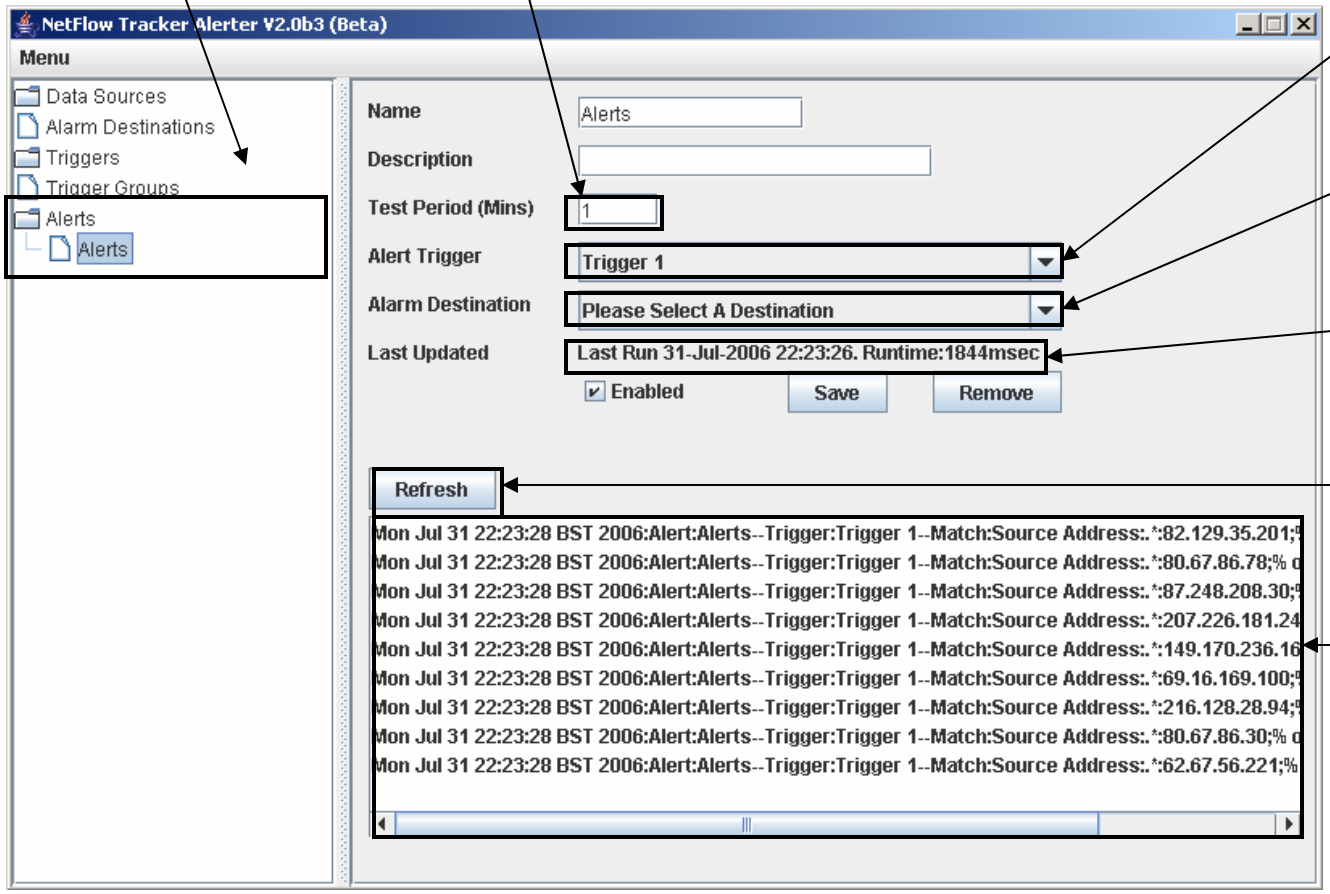
Add/Remove selected trigger from group

Lists what triggers are currently in this group

Alerts – In The Application

Right click to add new trigger group, left click to edit.

How long to cache report before re-polling



Drop down menu lists all available triggers & groups

Drop down menu lists all available destinations

Shows the last time this alert was checked

This will refresh the "Last Updated" item and the alert list

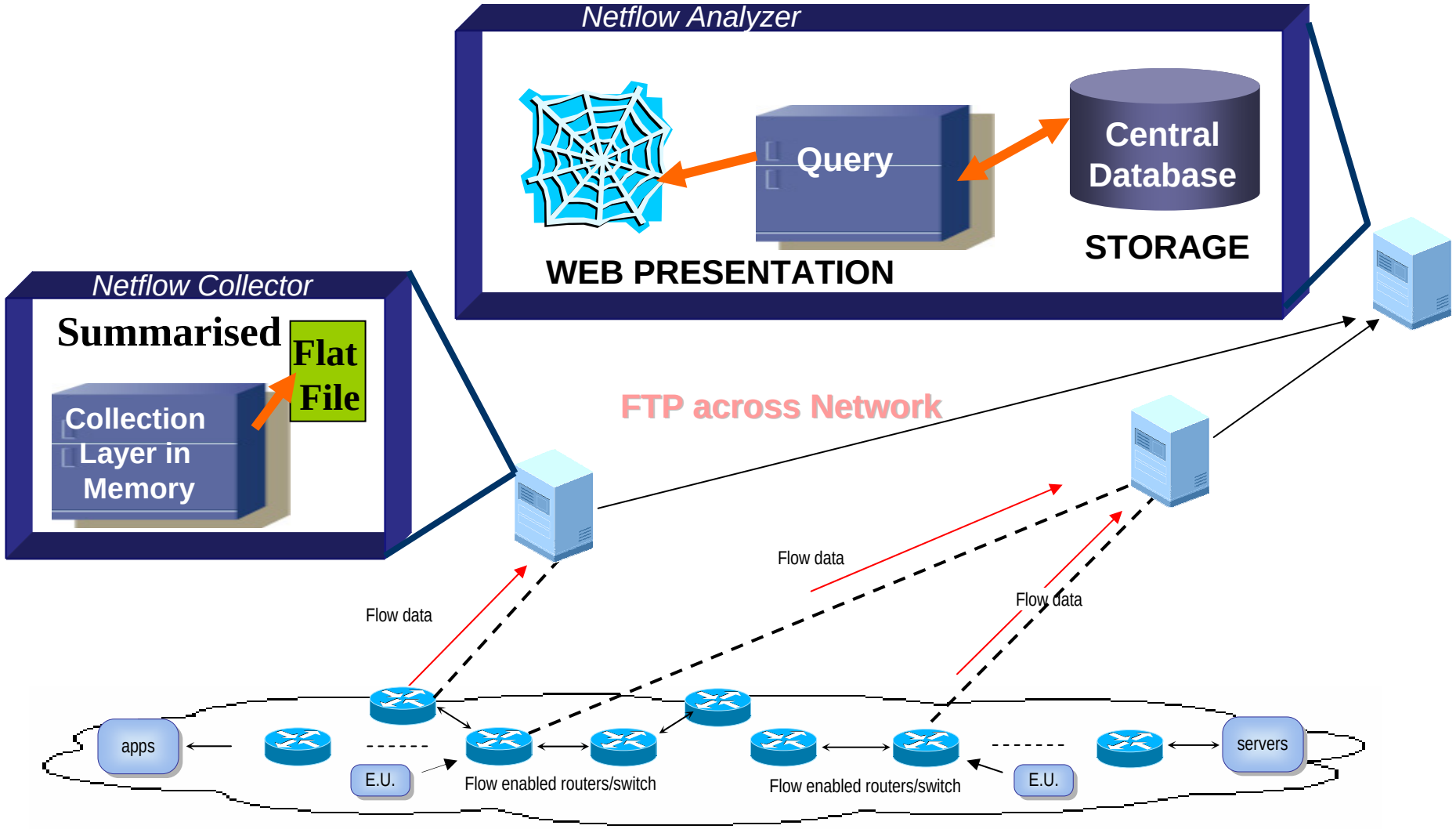
List showing the last 10 alerts.

NetFlow Tracker - Thank you

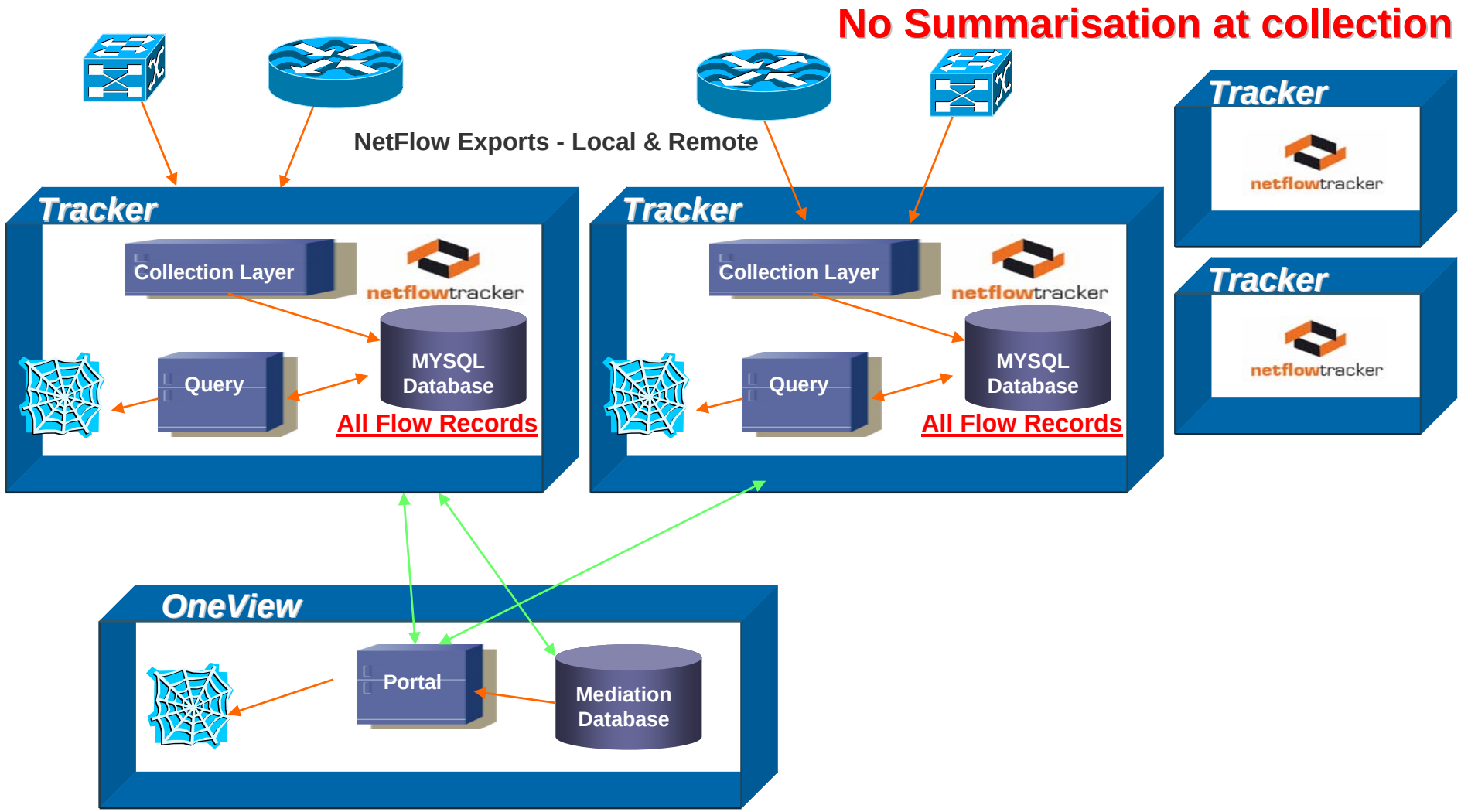
think **outside** the box

Thank you for your time

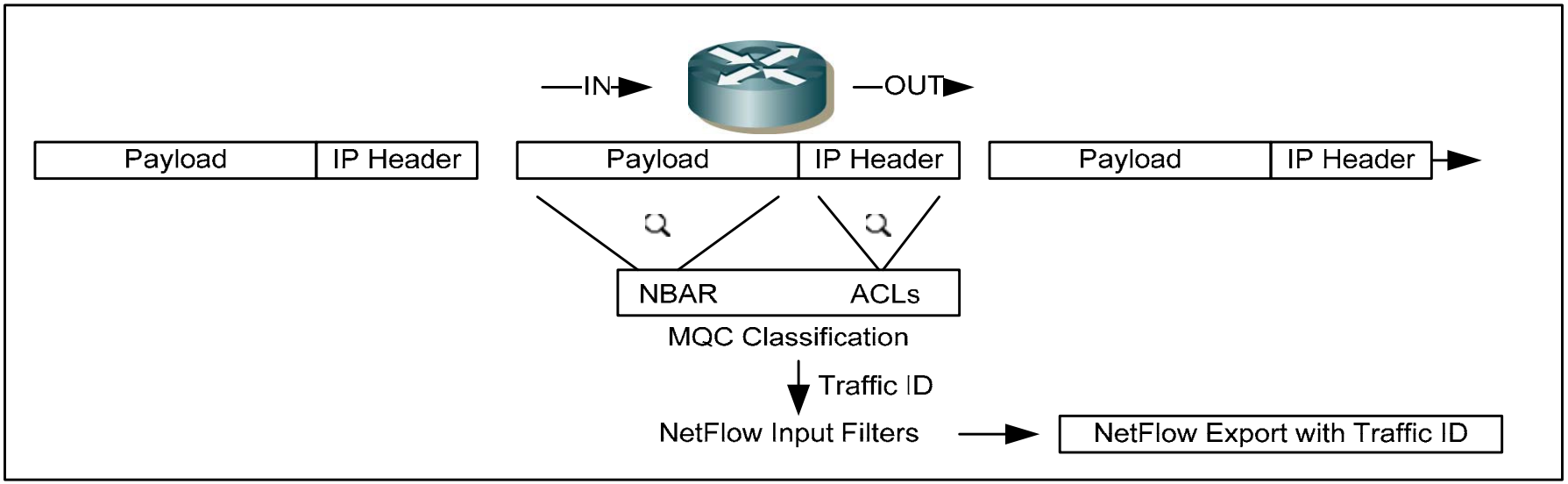
Two Tier Central Architecture



Netflow Tracker collection architecture



Traffic ID Feature



NetFlow Record

Router Address
Source Address
Destination Address
Source Port
Destination Port
ClassID

Tracker ID Mapping

NetFlow Record		Traffic ID
Router Address1	ClassID 1	TrafficID 1
Router Address1	ClassID 12	TrafficID 2
Router Address1	ClassID 22	TrafficID 3
Router Address2	ClassID 98	TrafficID 1
Router Address2	ClassID4	TrafficID 2
Router Address3	ClassID 2	TrafficID 1
Router Address3	ClassID 1	TrafficID 2
Router Address4	ClassID 2	TrafficID 1
Router Address4	ClassID 1	TrafficID 2

Tracker Record

Router Address
Source Address
Destination Address
Source Port
Destination Port
TrafficID