Flow tools

APRICOT 2008
Network Management
Taipei, Taiwan
February 20-24, 2008

Flow-tools

- Collection of programs to post process Cisco NetFlow compatible flows.
- Written in C, designed to be fast (scales to large installations).
- Includes library (ftlib) for custom applications.
- Installation with configure;make;make install on most platforms (FreeBSD, Linux, Solaris)...

flow-capture

- Collect NetFlow exports and stores to disk.
- Built in compression.
- Manages disk space by expiring older flow files at configurable limits.
- Detects lost flows by missing sequence numbers and stores with flow metadata.

flow-fanout

- Replicate NetFlow UDP streams from one source to many destinations.
- Destination may be a multicast address.

flow-expire

- Expire (remove) old flow files based on disk usage.
- Same functionality built in to flow-capture.
- Used when managing disk space in a distributed environment.

Collector Placement and configuration

- NetFlow is UDP so the collector should ideally be directly connected to the router to minimize packet loss and IP spoofing risks.
- No flow control. Undersized collector will drop flows. Monitor netstat -s | grep buf and configure syslog so dropped flows will be logged.

flow-print

- Formatted output of flow files.

```
eng1:% flow-print < ft-v05.2002-01-21.093345-0500 | head -15
srcIP            dstIP            prot  srcPort  dstPort  octets packets
131.238.205.199  194.210.13.1     6     6346     40355    221          5
192.5.110.20     128.195.186.5    17    57040    33468    40           1
128.146.1.7      194.85.127.69    17    53       53       64           1
193.170.62.114   132.235.156.242  6     1453     1214     192          4
134.243.5.160    192.129.25.10    6     80       3360     654          7
132.235.156.242  193.170.62.114   6     1214     1453     160          4
130.206.43.51    130.101.99.107   6     3226     80       96           2
206.244.141.3    128.163.62.17    6     35593    80       739          10
206.244.141.3    128.163.62.17    6     35594    80       577          6
212.33.84.160    132.235.152.47   6     1447     1214     192          4
132.235.157.187  164.58.150.166   6     1214     56938    81           2
129.1.246.97     152.94.20.214    6     4541     6346     912          10
132.235.152.47   212.33.84.160    6     1214     1447     160          4
130.237.131.52   130.101.9.20     6     1246     80       902          15
```

flow-cat

- Concat many flow files or directories of files.

```
eng1:% ls
ft-v05.2002-01-21.160001-0500   ft-v05.2002-01-21.170001-0500
ft-v05.2002-01-21.161501-0500   ft-v05.2002-01-21.171501-0500
ft-v05.2002-01-21.163001-0500   ft-v05.2002-01-21.173001-0500
ft-v05.2002-01-21.164501-0500   tmp-v05.2002-01-21.174501-0500

eng1:% flow-cat . | flow-print

srcIP            dstIP            prot  srcPort  dstPort  octets packets
138.26.220.46    192.5.110.20     17    62242    33456    40           1
143.105.55.23    18.123.66.15     17    41794    41794    40           1
129.15.134.66    164.107.69.33    6     1214     2222     4500         3
132.235.170.19   152.30.96.188    6     6346     1475     128          3
```

flow-merge

- Flow-merge is similar to flow-cat except it maintains relative ordering of flows when combining the files.
- Typically used when combining flows from multiple collectors.

flow-filter

- Filter flows based on port, protocol, ASN, IP address, ToS bits, TCP bits, and tags.

```
eng1% flow-cat . | flow-filter -P119 | flow-print | head -10

srcIP            dstIP            prot  srcPort  dstPort  octets      packets
155.52.46.50     164.107.115.4    6     33225    119      114         2
128.223.220.29   129.137.4.135    6     52745    119      1438382     1022
155.52.46.50     164.107.115.4    6     33225    119      374         6
164.107.115.4    192.58.107.160   6     60141    119      5147961     8876
128.223.220.29   129.137.4.135    6     52745    119      1356325     965
128.223.220.29   129.137.4.135    6     52714    119      561016      398
130.207.244.18   129.22.8.64      6     36033    119      30194       121
155.52.46.50     164.107.115.4    6     33225    119      130         2
198.108.1.146    129.137.4.135    6     17800    119      210720652   216072
```

flow-split

- Split flow files into smaller files.
- Typically used with flow-stat and graphing. For example if flow files are 1 hour and want 5 minute data points in graph, flow-split can take the 1 hour flow files and generate 5 minute files.

flow-tag

- Adds a tag field to flows based on IP exporter, IP prefix, Autonomous System, or next hop.
- Like flow-filter used with other tools.
- Used to manage groups of prefixes or ASN's.

flow-header

- Display meta information in flow file.

```
eng1:% flow-header < ft-v05.2002-01-21.093345-0500
#
# mode:                 normal
# capture hostname:     eng1.oar.net
# exporter IP address:  0.0.0.0
# capture start:        Mon Jan 21 09:33:45 2002
# capture end:          Mon Jan 21 09:45:01 2002
# capture period:       676 seconds
# compress:             on
# byte order:           little
# stream version:       3
# export version:       5
# lost flows:           0
# corrupt packets:      0
# sequencer resets:     0
# capture flows:        341370
#
```

flow-stat

- Generates reports from flow files.
- Output is readable and easily imported into graphing programs (gnuplot, etc).
- IP Address, IP address pairs, ports, packets, bytes, interfaces, next hop, Autonomous System, ToS bits, exporter, and tags.

flow-stat - summary

```
Total Flows                          : 24236730
Total Octets                         : 71266806610
Total Packets                        : 109298006
Total Time (1/1000 secs) (flows)     : 289031186084
Duration of data  (realtime)         : 86400
Duration of data (1/1000 secs)       : 88352112
Average flow time (1/1000 secs)      : 11925.0000
Average packet size (octets)         : 652.0000
Average flow size (octets)           : 2940.0000
Average packets per flow             : 4.0000
Average flows / second (flow)        : 274.3201
Average flows / second (real)        : 280.5177
Average Kbits / second (flow)        : 6452.9880
Average Kbits / second (real)        : 6598.7781
```

flow-stat - Source AS % Total

# src AS	flows	octets	packets	duration
NSFNETTEST14-AS	6.430	6.582	7.019	5.693
ONENET-AS-1	2.914	4.417	3.529	3.566
UONET	0.600	4.052	2.484	1.979
UPITT-AS	1.847	3.816	2.697	2.552
CONCERT	1.786	2.931	2.391	1.955
OHIOU	3.961	2.601	2.140	1.655
CMU-ROUTER	1.962	2.577	2.349	2.075
BOSTONU-AS	1.503	2.126	1.665	1.914
PURDUE	2.185	1.994	2.157	2.507
STANFORD	2.124	1.950	2.270	2.636
UR	1.809	1.919	1.652	1.532
UMN-AGS-NET-AS	1.612	1.895	1.788	1.938
RISQ-AS	1.086	1.849	1.378	1.367
PENN-STATE	2.845	1.641	2.666	2.190
RIT-ASN	0.796	1.601	1.414	0.830

flow-stat - Dest AS % Total

# dst AS	flows	octets	packets	duration
NSFNETTEST14-AS	6.202	9.564	8.005	6.762
PENN-STATE	2.037	3.774	2.712	2.153
CONCERT	2.628	3.133	2.888	2.326
ONENET-AS-1	2.818	2.434	2.906	3.000
STANFORD	1.915	2.360	2.122	2.195
JANET	2.508	2.319	2.150	2.485
0	0.831	2.187	2.431	2.910
DFN-WIN-AS	2.349	2.099	1.938	2.359
CMU-ROUTER	1.383	2.090	1.972	1.960
UONET	0.537	2.067	1.699	1.397
PURDUE	2.029	1.934	1.983	2.177
UMN-AGS-NET-AS	1.608	1.784	1.664	1.681
UPITT-AS	1.507	1.707	2.067	2.288
MIT-GATEWAYS	0.677	1.425	1.175	0.806
RIT-ASN	0.644	1.313	1.243	0.868
INDIANA-AS	0.899	1.285	0.996	0.781

flow-stat – Src/Dest AS % Total

# src AS	dst AS	flows	octets	packets	duration
GEORGIA-TECH	PENN-STATE	0.030	0.965	0.459	0.071
NWU-AS	0	0.008	0.734	0.379	0.170
UONET	CONCERT	0.064	0.698	0.438	0.290
UCLA	NSFNETTEST14-AS	0.037	0.568	0.269	0.111
CONCERT	UONET	0.052	0.543	0.364	0.221
BCNET-AS	MIT-GATEWAYS	0.019	0.538	0.274	0.134
UONET	0	0.015	0.536	0.318	0.200
MIT-GATEWAYS	STANFORD	0.032	0.477	0.245	0.073
ONENET-AS-1	NSFNETTEST14-AS	0.140	0.451	0.263	0.159
UONET	PENN-STATE	0.019	0.439	0.200	0.063
NOAA-AS	NOAA-FSL	0.018	0.438	0.255	0.031
DENET	UONET	0.032	0.410	0.189	0.188
NSFNETTEST14-AS	UC-DOM	0.022	0.365	0.244	0.081
ITALY-AS	UONET	0.016	0.358	0.228	0.117
NSFNETTEST14-AS	CONCERT	0.322	0.349	0.335	0.228
UONET	ITALY-AS	0.022	0.349	0.210	0.130

flow-dscan

- DoS detection / network scanning tool.
- Flag hosts which have flows to many other hosts.
- Flag hosts which are using a large number of TCP/UDP ports.
- Works better on smaller networks or with flow-filter to limit traffic. For example filter TCP port 25 to detect hosts infected with e-mail worm.

flow-gen

- Debugging tool to generate flows.

```
eng1:% flow-gen -V8.1 | flow-print | head -10

srcAS   dstAS   in      out     flows       octets      packets     duration
0       65280   0       65280   2           1           1           4294901760
1       65281   1       65281   4           2           2           4294901760
2       65282   2       65282   6           3           3           4294901760
3       65283   3       65283   8           4           4           4294901760
4       65284   4       65284   10          5           5           4294901760
5       65285   5       65285   12          6           6           4294901760
6       65286   6       65286   14          7           7           4294901760
7       65287   7       65287   16          8           8           4294901760
8       65288   8       65288   18          9           9           4294901760
```

flow-send

- Transmit flow files with NetFlow protocol to another collector.
- Can be used to take flow-tools files and send them to other NetFlow compatible collector.

flow-receive

- Like flow-capture but does not manage disk space. Output is to standard out and can be used directly with other flow-tools programs.
- Typically used for debugging.

```
eng1:% flow-receive 0/0/5555 | flow-print
flow-receive: New exporter: time=1011652474 src_ip=199.18.112.114
 dst_ip=199.18.97.102 d_version=8
srcPrefix           srcAS  dstPrefix           dstAS  input  output flows
143.105/16          600    128.9/16            4      48     25     1
140.141/16          600    150.216/16          81     48     25     4
132.235/16          17135  130.49/17           4130   38     25     25
131.123/16          11050  129.59/16           7212   42     25     1
206.21/16           600    128.239/16          11975  48     25     2
199.218/16          600    128.255/16          3676   48     25     1
```

flow-import

- Import flows from other formats into flow-tools.
- Currently supports ASCII and cflowd formats.

flow-export

- Export flows from flow-tools files to other formats.
- Currently supports ASCII and cflowd formats.
- ASCII output can be used with perl or other scripting languages (with a performance penalty).

flow-xlate

- Translate flows among NetFlow versions.
- Originally intended for use with Catalyst switches since they export some flows in version 7 and others in version 5 format.

Front End applications

- Flow-tools is good at collecting raw flows
- You may need additional tools to generate customized reports
- Perl applications are very popular.
  - flowscan.pm
  - Cflow.pm
  - CuGrapher.pl
- Integration with RRDTool, MRTG etc. makes it more useful

References

- flow-tools:
  http://www.splintered.net/sw/flow-tools
- NetFlow Applications

  http://www.inmon.com/technology/netflowaps.php
- Netflow HOW-TO
  http://www.linuxgeek.org/netflow-howto.php
- IETF standards effort:
  http://www.ietf.org/html.charters/ipfix-charter.html

References

- Abilene NetFlow page
  http://abilene-netflow.itec.oar.net/
- Flow-tools mailing list:
  flow-tools@splintered.net
- Cisco Centric Open Source Community
  http://cosi-nms.sourceforge.net/related.html