Flow-tools Tutorial

SANOG 6
Bhutan
Agenda

• Network flows
• Cisco / Juniper implementation – NetFlow
• Cisco / Juniper Configuration
• flow-tools programs overview and examples from Abilene and Ohio-Gigapop
Network Flows

• Packets or frames that have a common attribute.
• Creation and expiration policy – what conditions start and stop a flow.
• Counters – packets, bytes, time.
• Routing information – AS, network mask, interfaces.
Network Flows

• Unidirectional or bidirectional.
• Bidirectional flows can contain other information such as round trip time, TCP behavior.
• Application flows look past the headers to classify packets by their contents.
• Aggregated flows – flows of flows.
Unidirectional Flow with Source/Destination IP Key

% telnet 10.0.0.2

10.0.0.1 -> login: 10.0.0.2

Active Flows

<table>
<thead>
<tr>
<th>Flow</th>
<th>Source IP</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>2</td>
<td>10.0.0.2</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>
Unidirectional Flow with Source/Destination IP Key

% telnet 10.0.0.2
% ping 10.0.0.2

Active Flows

<table>
<thead>
<tr>
<th>Flow</th>
<th>Source IP</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>2</td>
<td>10.0.0.2</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>
Unidirectional Flow with IP, Port, Protocol Key

% telnet 10.0.0.2
% ping 10.0.0.2

Active Flows

<table>
<thead>
<tr>
<th>Flow</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>prot</th>
<th>srcPort</th>
<th>dstPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
<td>TCP</td>
<td>32000</td>
<td>23</td>
</tr>
<tr>
<td>2</td>
<td>10.0.0.2</td>
<td>10.0.0.1</td>
<td>TCP</td>
<td>23</td>
<td>32000</td>
</tr>
<tr>
<td>3</td>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
<td>ICMP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>10.0.0.2</td>
<td>10.0.0.1</td>
<td>ICMP</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Bidirectional Flow with IP, Port, Protocol Key

% telnet 10.0.0.2
% ping 10.0.0.2

Active Flows

<table>
<thead>
<tr>
<th>Flow</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>prot</th>
<th>srcPort</th>
<th>dstPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
<td>TCP</td>
<td>32000</td>
<td>23</td>
</tr>
<tr>
<td>2</td>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
<td>ICMP</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

10.0.0.1 -> login:
ICMP echo reply

10.0.0.2
% netscape http://10.0.0.2/9090

10.0.0.1 10.0.0.2

Web server on Port 9090

Active Flows

<table>
<thead>
<tr>
<th>Flow</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
<td>HTTP</td>
</tr>
</tbody>
</table>
# Aggregated Flow

## Main Active flow table

<table>
<thead>
<tr>
<th>Flow</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>prot</th>
<th>srcPort</th>
<th>dstPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
<td>TCP</td>
<td>32000</td>
<td>23</td>
</tr>
<tr>
<td>2</td>
<td>10.0.0.2</td>
<td>10.0.0.1</td>
<td>TCP</td>
<td>23</td>
<td>32000</td>
</tr>
<tr>
<td>3</td>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
<td>ICMP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>10.0.0.2</td>
<td>10.0.0.1</td>
<td>ICMP</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

## Source/Destination IP Aggregate

<table>
<thead>
<tr>
<th>Flow</th>
<th>Source IP</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>2</td>
<td>10.0.0.2</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>
Flow Descriptors

• A Key with more elements will generate more flows.

• Greater number of flows leads to more post processing time to generate reports, more memory and CPU requirements for device generating flows.

• Depends on application. Traffic engineering vs. intrusion detection.
Flow Accounting

- Accounting information accumulated with flows.
- Packets, Bytes, Start Time, End Time.
- Network routing information – masks and autonomous system number.
Flow Collection

- Passive monitor.
- Router other existing network device.
Passive Monitor Collection

Flow probe connected to switch port in "traffic mirror" mode
Router Collection

Flow collector stores exported flows from router.
Passive Monitor

• Directly connected to a LAN segment via a switch port in “mirror” mode, optical splitter, or repeated segment.
• Generate flows for all local LAN traffic.
• Must have an interface or monitor deployed on each LAN segment.
• Support for more detailed flows – bidirectional and application.
Router Collection

- Router will generate flows for traffic that is directed to the router.
- Flows are not generated for local LAN traffic.
- Limited to “simple” flow criteria (packet headers).
- Generally easier to deploy – no new equipment.
Cisco NetFlow

- Unidirectional flows.
- IPv4 unicast and multicast.
- Aggregated and unaggregated.
- Flows exported via UDP.
- Supported on IOS and CatIOS platforms.
- Catalyst NetFlow is different implementation.
Cisco NetFlow Versions

- 4 Unaggregated types (1,5,6,7).
- 14 Aggregated types (8.x).
- Each version has its own packet format.
- Version 1 does not have sequence numbers – no way to detect lost flows.
- The “version” defines what type of data is in the flow.
- Some versions specific to Catalyst platform.
NetFlow v1

• Accounting: Packets, Octets, Start/End time, Output interface
• Other: Bitwise OR of TCP flags.
NetFlow v5

• Accounting: Packets, Octets, Start/End time, Output interface.
• Other: Bitwise OR of TCP flags, Source/Destination AS and IP Mask.
• Packet format adds sequence numbers for detecting lost exports.
NetFlow v8

• Aggregated v5 flows.
• 3 Catalyst 65xx specific that correspond to the configurable flow mask.
• Much less data to post process, but lose fine granularity of v5 – no IP addresses.
NetFlow v8

- AS
- Protocol/Port
- Source Prefix
- Destination Prefix
- Prefix
- Destination (Catalyst 65xx)
- Source/Destination (Catalyst 65xx)
- Full Flow (Catalyst 65xx)
NetFlow v8

- ToS/AS
- ToS/Protocol/Port
- ToS/Source Prefix
- ToS/Destination Prefix
- Tos/Source/Destination Prefix
- ToS/Prefix/Port
NetFlow Packet Format

- Common header among export versions.
- All but v1 have a sequence number.
- Version specific data field where N records of data type are exported.
- N is determined by the size of the flow definition. Packet size is kept under ~1480 bytes. No fragmentation on Ethernet.
NetFlow v5 Packet Example

IP/UDP packet

NetFlow v5 header

v5 record

...

...

...

v5 record
NetFlow v5 Packet (Header)

```c
struct ftpdu_v5 {
    /* 24 byte header */
    u_int16 version;       /* 5 */
    u_int16 count;         /* The number of records in the PDU */
    u_int32 sysUpTime;     /* Current time in millisecs since router booted */
    u_int32 unix_secs;     /* Current seconds since 0000 UTC 1970 */
    u_int32 unix_nsecs;    /* Residual nanoseconds since 0000 UTC 1970 */
    u_int32 flow_sequence; /* Seq counter of total flows seen */
    u_int8  engine_type;   /* Type of flow switching engine (RP, VIP, etc.) */
    u_int8  engine_id;     /* Slot number of the flow switching engine */
    u_int16 reserved;
};
```
NetFlow v5 Packet (Records)

/* 48 byte payload */
struct ftrec_v5 {
    u_int32 srcaddr;    /* Source IP Address */
    u_int32 dstaddr;    /* Destination IP Address */
    u_int32 nexthop;    /* Next hop router's IP Address */
    u_int16 input;      /* Input interface index */
    u_int16 output;     /* Output interface index */
    u_int32 dPkts;      /* Packets sent in Duration */
    u_int32 dOctets;    /* Octets sent in Duration. */
    u_int32 First;      /* SysUptime at start of flow */
    u_int32 Last;       /* and of last packet of flow */
    u_int16 srcport;    /* TCP/UDP source port number or equivalent */
    u_int16 dstport;    /* TCP/UDP destination port number or equiv */
    u_int8  pad;
    u_int8  tcp_flags;  /* Cumulative OR of tcp flags */
    u_int8  prot;       /* IP protocol, e.g., 6=TCP, 17=UDP, ... */
    u_int8  tos;        /* IP Type-of-Service */
    u_int16 src_as;     /* originating AS of source address */
    u_int16 dst_as;     /* originating AS of destination address */
    u_int8  src_mask;   /* source address prefix mask bits */
    u_int8  dst_mask;   /* destination address prefix mask bits */
    u_int16 drops;
} records[FT_PDU_V5_MAXFLOWS];
};
NetFlow v8 Packet Example (AS Aggregation)

<table>
<thead>
<tr>
<th>IP/UDP packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetFlow v8 header</td>
</tr>
<tr>
<td>v8 record</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>v8 record</td>
</tr>
</tbody>
</table>
struct ftpdu_v8_1 {
    /* 28 byte header */
    u_int16 version;       /* 8 */
    u_int16 count;         /* The number of records in the PDU */
    u_int32 sysUpTime;     /* Current time in millisecs since router booted */
    u_int32 unix_secs;     /* Current seconds since 0000 UTC 1970 */
    u_int32 unix_nsecs;    /* Residual nanoseconds since 0000 UTC 1970 */
    u_int32 flow_sequence; /* Seq counter of total flows seen */
    u_int8  engine_type;   /* Type of flow switching engine (RP,VIP,etc.) */
    u_int8  engine_id;     /* Slot number of the flow switching engine */
    u_int8  aggregation;   /* Aggregation method being used */
    u_int8  agg_version;   /* Version of the aggregation export */
    u_int32 reserved;
    /* 28 byte payload */
    struct ftrec_v8_1 {
        u_int32 dFlows;     /* Number of flows */
        u_int32 dPkts;      /* Packets sent in duration */
        u_int32 dOctets;    /* Octets sent in duration */
        u_int32 First;      /* SysUpTime at start of flow */
        u_int32 Last;       /* and of last packet of flow */
        u_int16 src_as;     /* originating AS of source address */
        u_int16 dst_as;     /* originating AS of destination address */
        u_int16 input;      /* input interface index */
        u_int16 output;     /* output interface index */
    } records[FT_PDU_V8_1_MAXFLOWS];
};
Cisco IOS Configuration

- Configured on each input interface.
- Define the version.
- Define the IP address of the collector (where to send the flows).
- Optionally enable aggregation tables.
- Optionally configure flow timeout and main (v5) flow table size.
- Optionally configure sample rate.
Cisco IOS Configuration

interface FastEthernet0/0/0
   ip address 10.0.0.1 255.255.255.0
   no ip directed-broadcast
   ip route-cache flow

interface ATM1/0/0
   no ip address
   no ip directed-broadcast
   ip route-cache flow

interface Loopback0
   ip address 10.10.10.10 255.255.255.255
   no ip directed-broadcast

   ip flow-export version 5 origin-as
   ip flow-export destination 10.0.0.10 5004
   ip flow-export source loopback 0

   ip flow-aggregation cache prefix
      export destination 10.0.0.10 5555
      enabled
Cisco IOS Configuration

krc4#sh ip flow export
Flow export is enabled
  Exporting flows to 10.0.0.10 (5004)
  Exporting using source IP address 10.10.10.10
  Version 5 flow records, origin-as
  Cache for prefix aggregation:
    Exporting flows to 10.0.0.10 (5555)
    Exporting using source IP address 10.10.10.10
  3176848179 flows exported in 105898459 udp datagrams
  0 flows failed due to lack of export packet
  45 export packets were sent up to process level
  0 export packets were punted to the RP
  5 export packets were dropped due to no fib
  31 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
  0 export packets were dropped due to output drops
Cisco IOS Configuration

```
krc4#sho ip ca fl
IP packet size distribution (106519M total packets):
  1-32  64  96  128  160  192  224  256  288  320  352  384  416  448  480
     .002 .405 .076 .017 .011 .010 .007 .005 .004 .004 .003 .002 .002
  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
     .002 .006 .024 .032 .368 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  36418 active, 29118 inactive, 3141073565 added
  3132256745 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Total Flows</th>
<th>Flows /Sec</th>
<th>Packets /Flow</th>
<th>Bytes /Pkt</th>
<th>Packets /Sec</th>
<th>Active (Sec)</th>
<th>Idle (Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-Telnet</td>
<td>2951815</td>
<td>0.6</td>
<td>61</td>
<td>216</td>
<td>42.2</td>
<td>26.6</td>
<td>21.4</td>
</tr>
<tr>
<td>TCP-FTP</td>
<td>24128311</td>
<td>5.6</td>
<td>71</td>
<td>748</td>
<td>402.3</td>
<td>15.0</td>
<td>26.3</td>
</tr>
<tr>
<td>TCP-FTPD</td>
<td>2865416</td>
<td>0.6</td>
<td>916</td>
<td>843</td>
<td>611.6</td>
<td>34.7</td>
<td>19.8</td>
</tr>
<tr>
<td>TCP-WWW</td>
<td>467748914</td>
<td>108.9</td>
<td>15</td>
<td>566</td>
<td>1675.8</td>
<td>4.9</td>
<td>21.6</td>
</tr>
<tr>
<td>TCP-SMTP</td>
<td>46697428</td>
<td>10.8</td>
<td>14</td>
<td>370</td>
<td>159.6</td>
<td>4.0</td>
<td>20.1</td>
</tr>
<tr>
<td>TCP-X</td>
<td>521071</td>
<td>0.1</td>
<td>203</td>
<td>608</td>
<td>24.7</td>
<td>24.5</td>
<td>24.2</td>
</tr>
<tr>
<td>TCP-BGP</td>
<td>2835505</td>
<td>0.6</td>
<td>5</td>
<td>94</td>
<td>3.3</td>
<td>16.2</td>
<td>20.7</td>
</tr>
</tbody>
</table>
```
Cisco IOS Configuration

```
krc4#sho ip ca fl

TCP-other     1620253066  377.2    47  631  18001.6   27.3   23.4
UDP-DNS       125622144   29.2     2  78   82.5     4.6   24.7
UDP-NTP       67332976    15.6     1  76   22.0     2.7   23.4
UDP-TFTP      37173       0.0      2  76   0.0      4.1   24.6
UDP-Frag      68421       0.0     474 900   7.5   111.7   21.6
UDP-other     493337764   114.8    17 479 1990.3  111.7   21.6
ICMP          243659509   56.7      3 166  179.7     3.3   23.3
IGMP           18601      0.0     96  35  0.4     941.4    8.1
IPINIP        12246       0.0     69  52  0.1     548.4   15.2
GRE           125763      0.0    235 156   6.9    50.3   21.1
IP-other      75976755     17.6      2  78  45.4     3.9   22.8
Total:        3176854246  739.6    33 619 24797.4  16.2   22.6

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>DstIPaddress</th>
<th>Pr</th>
<th>SrcP</th>
<th>DstP</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT5/0/0.4</td>
<td>206.21.162.150</td>
<td>AT1/0/0.1</td>
<td>141.219.73.45</td>
<td>06</td>
<td>0E4B</td>
<td>A029</td>
<td>507</td>
</tr>
<tr>
<td>AT4/0/0.10</td>
<td>132.235.174.9</td>
<td>AT1/0/0.1</td>
<td>137.99.166.126</td>
<td>06</td>
<td>04BE</td>
<td>074C</td>
<td>3</td>
</tr>
<tr>
<td>AT4/0/0.12</td>
<td>131.123.59.33</td>
<td>AT1/0/0.1</td>
<td>137.229.58.168</td>
<td>06</td>
<td>04BE</td>
<td>09BB</td>
<td>646</td>
</tr>
<tr>
<td>AT1/0/0.1</td>
<td>137.99.166.126</td>
<td>AT4/0/0.10</td>
<td>132.235.174.9</td>
<td>06</td>
<td>074C</td>
<td>04BE</td>
<td>3</td>
</tr>
</tbody>
</table>
```
Juniper Configuration

• Sample packets with firewall filter and forward to routing engine.
• Sampling rate is limited to 7000pps. Fine for traffic engineering, but restrictive for DoS and intrusion detection.
• Juniper calls NetFlow cflowd.
Juniper Configuration

Firewall filter

Enable sampling / flows

```conf
firewall {
    filter all {
        term all {
            then {
                sample;
                accept;
            }
        }
    }
}

forwarding-options {
    sampling {
        input {
            family inet {
                rate 100;
            }
        }
        output {
            cflowd 10.0.0.16{
                port 2055;
                version 5;
            }
        }
    }
}
```
Apply firewall filter to each interface.

```conf
interfaces {
    ge-0/3/0 {
        unit 0 {
            family inet {
                filter {
                    input all;
                    output all;
                }
                address 192.148.244.1/24;
            }
        }
    }
}
```
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, BSDi, NetBSD).
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.

```
engl:~% flow-print < ft-v05.2002-01-21.093345-0500 | head -15

<table>
<thead>
<tr>
<th>srcIP</th>
<th>dstIP</th>
<th>prot</th>
<th>srcPort</th>
<th>dstPort</th>
<th>octets</th>
<th>packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>131.238.205.199</td>
<td>194.210.13.1</td>
<td>6</td>
<td>6346</td>
<td>40355</td>
<td>221</td>
<td>5</td>
</tr>
<tr>
<td>192.5.110.20</td>
<td>128.195.186.5</td>
<td>17</td>
<td>57040</td>
<td>33468</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>128.146.1.7</td>
<td>194.85.127.69</td>
<td>17</td>
<td>53</td>
<td>53</td>
<td>64</td>
<td>1</td>
</tr>
<tr>
<td>193.170.62.114</td>
<td>132.235.156.242</td>
<td>6</td>
<td>1453</td>
<td>1214</td>
<td>192</td>
<td>4</td>
</tr>
<tr>
<td>134.243.5.160</td>
<td>192.129.25.10</td>
<td>6</td>
<td>80</td>
<td>3360</td>
<td>654</td>
<td>7</td>
</tr>
<tr>
<td>132.235.156.242</td>
<td>193.170.62.114</td>
<td>6</td>
<td>1214</td>
<td>1453</td>
<td>160</td>
<td>4</td>
</tr>
<tr>
<td>130.206.43.51</td>
<td>130.101.99.107</td>
<td>6</td>
<td>3226</td>
<td>80</td>
<td>96</td>
<td>2</td>
</tr>
<tr>
<td>206.244.141.3</td>
<td>128.163.62.17</td>
<td>6</td>
<td>35593</td>
<td>80</td>
<td>739</td>
<td>10</td>
</tr>
<tr>
<td>206.244.141.3</td>
<td>128.163.62.17</td>
<td>6</td>
<td>35594</td>
<td>80</td>
<td>577</td>
<td>6</td>
</tr>
<tr>
<td>212.33.84.160</td>
<td>132.235.152.47</td>
<td>6</td>
<td>1447</td>
<td>1214</td>
<td>192</td>
<td>4</td>
</tr>
<tr>
<td>132.235.157.187</td>
<td>164.58.150.166</td>
<td>6</td>
<td>1214</td>
<td>56938</td>
<td>81</td>
<td>2</td>
</tr>
<tr>
<td>129.1.246.97</td>
<td>152.94.20.214</td>
<td>6</td>
<td>4541</td>
<td>6346</td>
<td>912</td>
<td>10</td>
</tr>
<tr>
<td>132.235.152.47</td>
<td>212.33.84.160</td>
<td>6</td>
<td>1214</td>
<td>1447</td>
<td>160</td>
<td>4</td>
</tr>
<tr>
<td>130.237.131.52</td>
<td>130.101.9.20</td>
<td>6</td>
<td>1246</td>
<td>80</td>
<td>902</td>
<td>15</td>
</tr>
</tbody>
</table>
```
flow-cat

- Concat many flow files or directories of files.

```
eng1:% ls
ft-v05.2002-01-21.164501-0500  tmp-v05.2002-01-21.174501-0500  

eng1:% flow-cat . | flow-print

<table>
<thead>
<tr>
<th>srcIP</th>
<th>dstIP</th>
<th>prot</th>
<th>srcPort</th>
<th>dstPort</th>
<th>octets</th>
<th>packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>138.26.220.46</td>
<td>192.5.110.20</td>
<td>17</td>
<td>62242</td>
<td>33456</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>143.105.55.23</td>
<td>18.123.66.15</td>
<td>17</td>
<td>41794</td>
<td>41794</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>129.15.134.66</td>
<td>164.107.69.33</td>
<td>6</td>
<td>1214</td>
<td>2222</td>
<td>4500</td>
<td>3</td>
</tr>
<tr>
<td>132.235.170.19</td>
<td>152.30.96.188</td>
<td>6</td>
<td>6346</td>
<td>1475</td>
<td>128</td>
<td>3</td>
</tr>
</tbody>
</table>
```
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
```

<table>
<thead>
<tr>
<th>srcIP</th>
<th>dstIP</th>
<th>prot</th>
<th>srcPort</th>
<th>dstPort</th>
<th>octets</th>
<th>packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>155.52.46.50</td>
<td>164.107.115.4</td>
<td>6</td>
<td>33225</td>
<td>119</td>
<td>114</td>
<td>2</td>
</tr>
<tr>
<td>128.223.220.29</td>
<td>129.137.4.135</td>
<td>6</td>
<td>52745</td>
<td>119</td>
<td>1438382</td>
<td>1022</td>
</tr>
<tr>
<td>155.52.46.50</td>
<td>164.107.115.4</td>
<td>6</td>
<td>33225</td>
<td>119</td>
<td>374</td>
<td>6</td>
</tr>
<tr>
<td>164.107.115.4</td>
<td>192.58.107.160</td>
<td>6</td>
<td>60141</td>
<td>119</td>
<td>5147961</td>
<td>8876</td>
</tr>
<tr>
<td>128.223.220.29</td>
<td>129.137.4.135</td>
<td>6</td>
<td>52745</td>
<td>119</td>
<td>1356325</td>
<td>965</td>
</tr>
<tr>
<td>128.223.220.29</td>
<td>129.137.4.135</td>
<td>6</td>
<td>52714</td>
<td>119</td>
<td>561016</td>
<td>398</td>
</tr>
<tr>
<td>130.207.244.18</td>
<td>129.22.8.64</td>
<td>6</td>
<td>36033</td>
<td>119</td>
<td>30194</td>
<td>121</td>
</tr>
<tr>
<td>155.52.46.50</td>
<td>164.107.115.4</td>
<td>6</td>
<td>33225</td>
<td>119</td>
<td>130</td>
<td>2</td>
</tr>
<tr>
<td>198.108.1.146</td>
<td>129.137.4.135</td>
<td>6</td>
<td>17800</td>
<td>119</td>
<td>210720652</td>
<td>216072</td>
</tr>
</tbody>
</table>
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.

```plaintext
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

<table>
<thead>
<tr>
<th>Metric Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Flows</td>
<td>24236730</td>
</tr>
<tr>
<td>Total Octets</td>
<td>71266806610</td>
</tr>
<tr>
<td>Total Packets</td>
<td>109298006</td>
</tr>
<tr>
<td>Total Time (1/1000 secs) (flows)</td>
<td>289031186084</td>
</tr>
<tr>
<td>Duration of data (realtime)</td>
<td>86400</td>
</tr>
<tr>
<td>Duration of data (1/1000 secs)</td>
<td>88352112</td>
</tr>
<tr>
<td>Average flow time (1/1000 secs)</td>
<td>11925.0000</td>
</tr>
<tr>
<td>Average packet size (octets)</td>
<td>652.0000</td>
</tr>
<tr>
<td>Average flow size (octets)</td>
<td>2940.0000</td>
</tr>
<tr>
<td>Average packets per flow</td>
<td>4.0000</td>
</tr>
<tr>
<td>Average flows / second (flow)</td>
<td>274.3201</td>
</tr>
<tr>
<td>Average flows / second (real)</td>
<td>280.5177</td>
</tr>
<tr>
<td>Average Kbits / second (flow)</td>
<td>6452.9880</td>
</tr>
<tr>
<td>Average Kbits / second (real)</td>
<td>6598.7781</td>
</tr>
<tr>
<td>src AS</td>
<td>flows</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>NSFNETTEST14-AS</td>
<td>6.430</td>
</tr>
<tr>
<td>ONENET-AS-1</td>
<td>2.914</td>
</tr>
<tr>
<td>UONET</td>
<td>0.600</td>
</tr>
<tr>
<td>UPITT-AS</td>
<td>1.847</td>
</tr>
<tr>
<td>CONCERT</td>
<td>1.786</td>
</tr>
<tr>
<td>OHIOU</td>
<td>3.961</td>
</tr>
<tr>
<td>CMU-ROUTER</td>
<td>1.962</td>
</tr>
<tr>
<td>BOSTONU-AS</td>
<td>1.503</td>
</tr>
<tr>
<td>PURDUE</td>
<td>2.185</td>
</tr>
<tr>
<td>STANFORD</td>
<td>2.124</td>
</tr>
<tr>
<td>UR</td>
<td>1.809</td>
</tr>
<tr>
<td>UMN-AGS-NET-AS</td>
<td>1.612</td>
</tr>
<tr>
<td>RISQ-AS</td>
<td>1.086</td>
</tr>
<tr>
<td>PENN-STATE</td>
<td>2.845</td>
</tr>
<tr>
<td>RIT-ASN</td>
<td>0.796</td>
</tr>
</tbody>
</table>
# flow-stat – Dest AS % Total

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

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

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

<table>
<thead>
<tr>
<th>srcAS</th>
<th>dstAS</th>
<th>in</th>
<th>out</th>
<th>flows</th>
<th>octets</th>
<th>packets</th>
<th>duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>65280</td>
<td>0</td>
<td>65280</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4294901760</td>
</tr>
<tr>
<td>1</td>
<td>65281</td>
<td>1</td>
<td>65281</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>4294901760</td>
</tr>
<tr>
<td>2</td>
<td>65282</td>
<td>2</td>
<td>65282</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>4294901760</td>
</tr>
<tr>
<td>3</td>
<td>65283</td>
<td>3</td>
<td>65283</td>
<td>8</td>
<td>4</td>
<td>4</td>
<td>4294901760</td>
</tr>
<tr>
<td>4</td>
<td>65284</td>
<td>4</td>
<td>65284</td>
<td>10</td>
<td>5</td>
<td>5</td>
<td>4294901760</td>
</tr>
<tr>
<td>5</td>
<td>65285</td>
<td>5</td>
<td>65285</td>
<td>12</td>
<td>6</td>
<td>6</td>
<td>4294901760</td>
</tr>
<tr>
<td>6</td>
<td>65286</td>
<td>6</td>
<td>65286</td>
<td>14</td>
<td>7</td>
<td>7</td>
<td>4294901760</td>
</tr>
<tr>
<td>7</td>
<td>65287</td>
<td>7</td>
<td>65287</td>
<td>16</td>
<td>8</td>
<td>8</td>
<td>4294901760</td>
</tr>
<tr>
<td>8</td>
<td>65288</td>
<td>8</td>
<td>65288</td>
<td>18</td>
<td>9</td>
<td>9</td>
<td>4294901760</td>
</tr>
</tbody>
</table>
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.

```bash
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

<table>
<thead>
<tr>
<th>srcPrefix</th>
<th>srcAS</th>
<th>dstPrefix</th>
<th>dstAS</th>
<th>input</th>
<th>output</th>
<th>flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>143.105/16</td>
<td>600</td>
<td>128.9/16</td>
<td>4</td>
<td>48</td>
<td>25</td>
<td>1</td>
</tr>
<tr>
<td>140.141/16</td>
<td>600</td>
<td>150.216/16</td>
<td>81</td>
<td>48</td>
<td>25</td>
<td>4</td>
</tr>
<tr>
<td>132.235/16</td>
<td>17135</td>
<td>130.49/17</td>
<td>4130</td>
<td>38</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>131.123/16</td>
<td>11050</td>
<td>129.59/16</td>
<td>7212</td>
<td>42</td>
<td>25</td>
<td>1</td>
</tr>
<tr>
<td>206.21/16</td>
<td>600</td>
<td>128.239/16</td>
<td>11975</td>
<td>48</td>
<td>25</td>
<td>2</td>
</tr>
<tr>
<td>199.218/16</td>
<td>600</td>
<td>128.255/16</td>
<td>3676</td>
<td>48</td>
<td>25</td>
<td>1</td>
</tr>
</tbody>
</table>
```
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.
References

- flow-tools: http://www.splintered.net/sw/flow-tools
- Netflow HOW-TO http://www.linuxgeek.org/netflow-howto.php
- IETF standards effort: http://ipfix.doit.wisc.edu
References

• flow-tools:
  http://www.splintered.net/sw/flow-tools

• Abilene NetFlow page
  http://www.itec.oar.net/abilene-netflow

• Flow-tools mailing list:
  flow-tools@splintered.net

• Cisco Centric Open Source Community
  http://cosi-nms.sourceforge.net/related.html
More Info

- e-mail: gaurab @ lahai.com
- On the web: http://lahai.com/netmgmt/