Net-flow

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

• Netflow
  – What it is and how it works
  – Uses and Applications
• Vendor Configurations/ Implementation
  – Cisco and Juniper
• Flow-tools
  – Architectural issues
  – Software, tools etc
• More Discussion / Lab Demonstration
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

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

<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>
Application Flow

% firefox http://10.0.0.2/9090

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>
Working with Flows

• Generating and Viewing Flows
• Exporting Flows from devices
  – Types of flows
  – Sampling rates
• Collecting it
  – Tools to Collect Flows - Flow-tools
• Analyzing it
  – More tools available, can write your own
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 Generation/Collection

- Passive monitor
  - A passive monitor (usually a unix host) receives all data and generates flows.
  - Resource intensive, newer investments needed
- Router or other existing network device.
  - Router or other existing devices like switch, generate flows.
  - Sampling is possible
  - Nothing new needed
Passive Monitor Collection

Flow probe connected to switch port in "traffic mirror" mode
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.
Vendor implementations
Cisco NetFlow

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

- 4 Unaggregated types (1, 5, 6, 7).
- 14 Aggregated types (8.x, 9).
- 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.
- Not all flow types available on all equipments
- Much less data to post process, but loses fine granularity of v5 – no IP addresses.
NetFlow v8

- AS
- Protocol/Port
- Source Prefix
- Destination Prefix
- Prefix
- Destination
- Source/Destination
- Full Flow
NetFlow v8

- ToS/AS
- ToS/Protocol/Port
- ToS/Source Prefix
- ToS/Destination Prefix
- Tos/Source/Destination Prefix
- ToS/Prefix/Port
NetFlow v9

- Record formats are defined using templates.
- Template descriptions are communicated from the router to the NetFlow Collection Engine.
- Flow records are sent from the router to the NetFlow Collection Engine with minimal template information so that the NetFlow Collection Engine can relate the records to the appropriate template.
- Version 9 is independent of the underlying transport (UDP, TCP, SCTP, and so on).
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)

```
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)

IP/UDP packet

NetFlow v8 header

v8 record

...

...

...

v8 record
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.
interface FastEthernet0/0
  description Access to backbone
  ip address 169.223.11.194 255.255.252.0
  ip route-cache flow
  duplex auto
  speed auto
!
interface FastEthernet0/1
  description Access to local net
  ip address 169.223.2.1 255.255.255.128
  ip route-cache flow
  duplex auto
  speed auto

ip flow-export version 5
ip flow-export destination 169.223.2.2 5004
Cisco IOS Configuration

• Change in command in newer IOS

```plaintext
interface FastEthernet0/0
   ip route-cache flow       ! Prior to IOS 12.4
   ip flow [ingress|egress]! From IOS 12.4
```

• If CEF is not configured on the router, this turns off the existing switching path on the router and enables NetFlow switching (basically modified optimum switching).

• If CEF is configured on the router, NetFlow simply becomes a "flow information gatherer" and feature accelerator—CEF remains operational as the underlying switching process.
gw-169-223-2-0#sh ip flow export
Flow export v5 is enabled for main cache
  Export source and destination details :
    VRF ID : Default
    Destination(1)  169.223.2.2 (5004)
Version 5 flow records
55074 flows exported in 3348 udp datagrams
0 flows failed due to lack of export packet
0 export packets were sent up to process level
0 export packets were dropped due to no fib
0 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
Cisco IOS Configuration

gw-169-223-2-0#sh ip cache flow
IP packet size distribution (3689551 total packets):
  1-32  64  96  128  160  192  224  256  288  320  352  384  416  448  480
    .000 .483 .189 .014 .002 .003 .001 .000 .000 .000 .000 .000 .000 .000 .001
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
    .001 .000 .008 .002 .288 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  26 active, 4070 inactive, 55206 added
  1430681 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  26 active, 998 inactive, 55154 added, 55154 added to flow
  0 alloc failures, 0 force free
  1 chunk, 2 chunks added
  last clearing of statistics never
### Cisco IOS Configuration

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Total Flows</th>
<th>Flows /Sec</th>
<th>Flows /Flow</th>
<th>Packets /Pkt</th>
<th>Bytes /Sec</th>
<th>Packets Active(Sec)</th>
<th>Idle(Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-Telnet</td>
<td>3357</td>
<td>0.0</td>
<td>35</td>
<td>92</td>
<td>1.3</td>
<td>0.5</td>
<td>11.5</td>
</tr>
<tr>
<td>TCP-FTP</td>
<td>128</td>
<td>0.0</td>
<td>19</td>
<td>97</td>
<td>0.0</td>
<td>0.6</td>
<td>1.5</td>
</tr>
<tr>
<td>TCP-FTPD</td>
<td>128</td>
<td>0.0</td>
<td>105</td>
<td>771</td>
<td>0.1</td>
<td>0.2</td>
<td>1.5</td>
</tr>
<tr>
<td>TCP-WWW</td>
<td>13462</td>
<td>0.1</td>
<td>125</td>
<td>962</td>
<td>19.3</td>
<td>7.0</td>
<td>5.9</td>
</tr>
<tr>
<td>TCP-X</td>
<td>269</td>
<td>0.0</td>
<td>1</td>
<td>40</td>
<td>0.0</td>
<td>0.0</td>
<td>14.3</td>
</tr>
<tr>
<td>TCP-other</td>
<td>9107</td>
<td>0.1</td>
<td>154</td>
<td>62</td>
<td>16.1</td>
<td>6.9</td>
<td>8.2</td>
</tr>
<tr>
<td>UDP-DNS</td>
<td>2248</td>
<td>0.0</td>
<td>1</td>
<td>73</td>
<td>0.0</td>
<td>0.8</td>
<td>15.4</td>
</tr>
<tr>
<td>UDP-NTP</td>
<td>3132</td>
<td>0.0</td>
<td>1</td>
<td>76</td>
<td>0.0</td>
<td>0.0</td>
<td>15.4</td>
</tr>
<tr>
<td>UDP-TFTP</td>
<td>24</td>
<td>0.0</td>
<td>6</td>
<td>49</td>
<td>0.0</td>
<td>30.0</td>
<td>15.3</td>
</tr>
<tr>
<td>UDP-Frag</td>
<td>6</td>
<td>0.0</td>
<td>1</td>
<td>32</td>
<td>0.0</td>
<td>0.0</td>
<td>15.5</td>
</tr>
<tr>
<td>UDP-other</td>
<td>6700</td>
<td>0.0</td>
<td>9</td>
<td>104</td>
<td>0.7</td>
<td>2.2</td>
<td>15.5</td>
</tr>
<tr>
<td>ICMP</td>
<td>16661</td>
<td>0.1</td>
<td>23</td>
<td>87</td>
<td>4.5</td>
<td>18.5</td>
<td>15.4</td>
</tr>
<tr>
<td>Total:</td>
<td>55222</td>
<td>0.6</td>
<td>66</td>
<td>480</td>
<td>42.3</td>
<td>8.8</td>
<td>11.6</td>
</tr>
</tbody>
</table>

<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>Fa0/1</td>
<td>169.223.2.195</td>
<td>Fa0/0</td>
<td>202.128.0.7</td>
<td>01</td>
<td>0000</td>
<td>0800</td>
<td>4</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.195</td>
<td>Fa0/0</td>
<td>218.185.127.204</td>
<td>01</td>
<td>0000</td>
<td>0800</td>
<td>4</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>Fa0/0</td>
<td>169.223.15.102</td>
<td>06</td>
<td>0016</td>
<td>C917</td>
<td>89</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>Local</td>
<td>169.223.2.1</td>
<td>06</td>
<td>DB27</td>
<td>0016</td>
<td>120</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.195</td>
<td>Fa0/0</td>
<td>202.128.31.179</td>
<td>01</td>
<td>0000</td>
<td>0800</td>
<td>4</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>208.81.191.133</td>
<td>Fa0/1</td>
<td>169.223.2.194</td>
<td>06</td>
<td>0050</td>
<td>8452</td>
<td>3</td>
</tr>
</tbody>
</table>
Cisco IOS Configuration

ip flow-top-talkers
top 10
sort-by bytes

gw-169-223-2-0#sh ip flow top-talkers

<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>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>Fa0/0</td>
<td>169.223.11.33</td>
<td>06</td>
<td>0050</td>
<td>0B64</td>
<td>3444K</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>Fa0/0</td>
<td>169.223.11.33</td>
<td>06</td>
<td>0050</td>
<td>0B12</td>
<td>3181K</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>169.223.11.33</td>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>06</td>
<td>0B12</td>
<td>0050</td>
<td>56K</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>169.223.11.33</td>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>06</td>
<td>0B64</td>
<td>0050</td>
<td>55K</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>Local</td>
<td>169.223.2.1</td>
<td>01</td>
<td>0000</td>
<td>0303</td>
<td>18K</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.130</td>
<td>Fa0/0</td>
<td>64.18.197.134</td>
<td>06</td>
<td>9C45</td>
<td>0050</td>
<td>15K</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.130</td>
<td>Fa0/0</td>
<td>64.18.197.134</td>
<td>06</td>
<td>9C44</td>
<td>0050</td>
<td>12K</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>213.144.138.195</td>
<td>Fa0/1</td>
<td>169.223.2.130</td>
<td>06</td>
<td>01BB</td>
<td>DC31</td>
<td>7167</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>169.223.15.102</td>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>06</td>
<td>C917</td>
<td>0016</td>
<td>2736</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>169.223.2.2</td>
<td>Local</td>
<td>169.223.2.1</td>
<td>06</td>
<td>DB27</td>
<td>0016</td>
<td>2304</td>
</tr>
</tbody>
</table>

10 of 10 top talkers shown. 49 flows processed.
Cisco command summary

• Enable CEF
  - ip cef

• Enable flow on each interface
  ip route cache flow OR
  ip flow ingress
  ip flow egress

• View flows
  - show ip cache flow
  - show ip flow top-talkers
Cisco Command Summary

- Exporting Flows to a collector
  
  ip flow-export version 5 [origin-as|peer-as]
  ip flow-export destination x.x.x.x <udp-port>

- Exporting aggregated flows
  
  ip flow-aggregation cache as|prefix|dest|source|proto enabled
  export destination x.x.x.x <udp-port>
Flows and Applications
Uses for Flow

- Problem identification / solving
  - Traffic classification
  - DoS Traceback (some slides by Danny McPherson)

- Traffic Analysis
  - Inter-AS traffic analysis
  - Reporting on application proxies

- Accounting
  - Cross verification from other sources
  - Can cross-check with SNMP data
Traffic Classification

• Based on Protocol, source and destination ports
  – Protocol identification (TCP, UDP, ICMP)
  – Can define well known ports
  – Can identify well known P2P ports
  – Most common use
    • Proxy measurement - http, ftp
    • Rate limiting P2P traffic
Traceback: Flow-based*

• Trace attack by matching fingerprint/signature at each interface via passive monitoring:
  – Flow data (e.g., NetFlow, cflowd, sFlow, IPFIX)
  – Span Data
  – PSAMP (Packet Sampling, IETF PSAMP WG)
• Number of open source and commercial products evolving in market
• Non-intrusive, widely supported
Flow-based Detection*

- Monitor flows (i.e., Network and Transport Layer transactions) on the network and build baselines for what normal behavior looks like:
  - Per interface
  - Per prefix
  - Per Transport Layer protocol & ports
  - Build time-based buckets (e.g., 5 minutes, 30 minutes, 1 hours, 12 hours, day of week, day of month, day of year)
Detect Anomalous Events: SQL “Slammer” Worm*

Anomaly 125772 Detailed Statistics

<table>
<thead>
<tr>
<th>ID</th>
<th>Importance</th>
<th>Severity</th>
<th>Duration</th>
<th>Direction</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>125772</td>
<td>High</td>
<td>95.82% of 3.40 Kbps</td>
<td>09h 06m 47s</td>
<td>Outgoing</td>
<td>found</td>
</tr>
</tbody>
</table>

Affected Network Elements

Router: net0 1.2.3.4

<table>
<thead>
<tr>
<th>Triggering</th>
<th>Expected</th>
<th>Difference</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitlete</td>
<td>71.63 Mbps</td>
<td>2.34 Mbps</td>
<td>69.36 Mbps</td>
</tr>
<tr>
<td>Packet Rate</td>
<td>22.20 Kbps</td>
<td>712 pps</td>
<td>21.49 Kbps</td>
</tr>
</tbody>
</table>

Summary of all Data Snapshots Collected:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Packets</th>
<th>Bytes/Min</th>
<th>bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>309.01 GB</td>
<td>370,040,500</td>
<td>404 B</td>
<td>76.05 Mbps</td>
</tr>
</tbody>
</table>

Summary | [Source Addresses] | [Destination Addresses] | [Source Ports] | [Destination Ports] | [Protocols] | [Output Interfaces] | [Input Interfaces] | [Generate Filter] |

Summary of Source Addresses:

<table>
<thead>
<tr>
<th>Source Addresses</th>
<th>Network / Mask</th>
<th>Bytes</th>
<th>Packets</th>
<th>Bytes/Min</th>
<th>bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.217/32</td>
<td>163.22 GB</td>
<td>416,436,300</td>
<td>404 B</td>
<td>41.54 Mbps</td>
<td>12.85</td>
</tr>
<tr>
<td>192.168.18.187/32</td>
<td>139.53 GB</td>
<td>345,372,300</td>
<td>404 B</td>
<td>34.45 Mbps</td>
<td>10.68</td>
</tr>
</tbody>
</table>

Summary of Destination Addresses:

<table>
<thead>
<tr>
<th>Destination Addresses</th>
<th>Network / Mask</th>
<th>Bytes</th>
<th>Packets</th>
<th>Bytes/Min</th>
<th>bps</th>
</tr>
</thead>
</table>

[Graphs and data visualizations related to network instability over time and traffic per UDP port over time]
Flow-based Detection (cont)*

- Once baselines are built anomalous activity can be detected
  - Pure **rate-based** (pps or bps) anomalies may be legitimate or malicious
  - Many **misuse** attacks can be immediately recognized, even **without** baselines (e.g., TCP SYN or RST floods)
  - **Signatures** can also be defined to identify “interesting” transactional data (e.g., proto udp and port 1434 and 404 octets(376 payload) == slammer!)
  - Temporal compound signatures can be defined to detect with higher precision
Flow-based Commercial Tools...

Anomaly 150228

<table>
<thead>
<tr>
<th>ID</th>
<th>Importance</th>
<th>Duration</th>
<th>Start Time</th>
<th>Direction</th>
<th>Type</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>150228</td>
<td>High 130.0% of 2 Kpps</td>
<td>17 mins</td>
<td>03:34, Aug 16</td>
<td>Incoming</td>
<td>Bandwidth (Profiled)</td>
<td>Microsoft 207.46.0.0/16 windowsupdate.com</td>
</tr>
</tbody>
</table>

Traffic Characterization

**Sources**
- 204.38.130.0/24
- 204.38.130.192/26
- 1024 - 1791

**Destination**
- 207.46.248.234/32
- 80 (http)

**Protocols**
tcp (6)

**TCP Flags**
S (0x02)

Affected Network Elements

<table>
<thead>
<tr>
<th>Router nl-chi3 198.110.131.125</th>
<th>Expected pps</th>
<th>Observed bps</th>
<th>Observed pps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Importance</td>
<td>pps</td>
<td>Max</td>
<td>Mean</td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Interface 67 at-1/1/0.14 pvc to WMU**

|                  | 26 | 832 K | 563.1 K | 2.6 K | 1.7 K |

Anomaly Comments
Commercial Detection
A Large Scale DOS attack*

### Anomaly 14957 Information

<table>
<thead>
<tr>
<th>ID</th>
<th>Importance</th>
<th>Severity</th>
<th>Duration</th>
<th>Direction</th>
<th>Resource</th>
<th>Start Time</th>
<th>End Time</th>
<th>Class</th>
<th>Subclass</th>
</tr>
</thead>
<tbody>
<tr>
<td>14957</td>
<td>High</td>
<td>108.759%</td>
<td>02h 04m 18s</td>
<td>Incoming</td>
<td>.bt.net-10.0.1.2 FastEthernet5/1</td>
<td>21:05:23 BST</td>
<td>23:09:41 BST</td>
<td>Misuse</td>
<td>IP Fragmentation Anomaly</td>
</tr>
</tbody>
</table>

### Affected Network Elements

**Router core1-telehouse (195.99.120.112)**

<table>
<thead>
<tr>
<th></th>
<th>Triggering</th>
<th>Expected</th>
<th>Difference</th>
<th>Maximum</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitrate</td>
<td></td>
<td>31.36 Kbps</td>
<td>500 pps</td>
<td>326.28 Mbps @ 21:14</td>
<td>116.31 Mbps</td>
</tr>
<tr>
<td>Packet Rate</td>
<td></td>
<td>31.59 Kbps @ 21:14</td>
<td>11.36 Kbps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Interface 2 POS4/0 (FXCC200030 STM-16 direct fibre (not SDH) link to core1.ealing PO)**

<table>
<thead>
<tr>
<th></th>
<th>Maximum</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitrate</td>
<td>87.84 Mbps @ 21:15</td>
<td>27.17 Mbps</td>
</tr>
<tr>
<td>Packet Rate</td>
<td>8.67 Kbps @ 21:15</td>
<td>2.72 Kbps</td>
</tr>
</tbody>
</table>
Traceback: Commercial*

Anomaly 150291

<table>
<thead>
<tr>
<th>ID</th>
<th>Importance</th>
<th>Duration</th>
<th>Start Time</th>
<th>Direction</th>
<th>Type</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>150291</td>
<td>High</td>
<td>19 mins</td>
<td>05:16, Aug 17</td>
<td>Incoming</td>
<td>Protocol TCP (Profiled)</td>
<td></td>
</tr>
</tbody>
</table>

Traffic Characterization

Sources:
- 126.165.86.151/32
- 60.1.104.76/32
- 0 - 4095

Destination:
- 1409 (internal)

Protocols:
- tcp (6)

TCP Flags:
- AP (0x18) A (0x10)

Affected Network Elements

<table>
<thead>
<tr>
<th>Router michael8 190.106.90.125</th>
<th>Importance</th>
<th>Expected</th>
<th>Observed bps</th>
<th>Observed pps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>bps</td>
<td>Max</td>
<td>Mean</td>
</tr>
<tr>
<td>Interface 127 ATM/1/0.27-asl5 layer 190.106.22.181</td>
<td>High</td>
<td>7.2 M</td>
<td>49.9 M</td>
<td>38.7 M</td>
</tr>
<tr>
<td>Interface 145 GigabitEthernet5/62 - 802.1q vlan subinterface 190.103.29.243</td>
<td>-</td>
<td>3.3 K</td>
<td>1.2 K</td>
<td>S</td>
</tr>
<tr>
<td>Interface 146 GigabitEthernet5/64 - 802.1q vlan subinterface 190.103.29.245</td>
<td>-</td>
<td>38.4 M</td>
<td>25.8 M</td>
<td>3.7 K</td>
</tr>
<tr>
<td>Interface 147 GigabitEthernet5/66 - 802.1q vlan subinterface 190.103.29.248</td>
<td>-</td>
<td>16.6 M</td>
<td>12.8 M</td>
<td>1.9 K</td>
</tr>
</tbody>
</table>

| Router asl 190.106.90.21 | High | 5.1 M | 44.4 M | 36.6 M | 4.5 K | 3.8 K | Details |

| Interface 38 se-0/2/0/1 128.132.165.7 | - | 34.0 M | 24.0 M | 3.0 K | 2.2 K | Details |
| Interface 39 se-0/2/0/2 128.132.165 | - | 13.9 M | 11.6 M | 1.3 K | 1.1 K | Details |
| Interface 40 se-0/1/0/0.209.172.10.128 | - | 1.6 M | 939.6 K | 600 | 408.8 | Details |
| Interface 41 se-0/1/0/1 190.186.96.17 | - | 411.5 K | 56.9 K | 83.3 | 41.7 | Details |
Commercial Traceback: More Detail*

### Anomaly 14957 Detailed Statistics

<table>
<thead>
<tr>
<th>ID</th>
<th>Importance</th>
<th>Severity</th>
<th>Duration</th>
<th>Direction</th>
<th>Resource</th>
<th>Start Time</th>
<th>End Time</th>
<th>Class</th>
<th>Subclass</th>
</tr>
</thead>
<tbody>
<tr>
<td>14957</td>
<td>High</td>
<td></td>
<td>02h 04m 18s</td>
<td>Incoming</td>
<td>bt.net-5-FastEthernet5/1</td>
<td>21:05:23 BST</td>
<td>23:09:41 BST</td>
<td>Misuse</td>
<td>IP Fragmentation Anomaly</td>
</tr>
</tbody>
</table>

#### Affected Network Elements

**Router core1-telehouse (195.99.120.112)**

<table>
<thead>
<tr>
<th></th>
<th>Triggering</th>
<th>Expected</th>
<th>Difference</th>
<th>Maximum</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitrate</td>
<td>31.36 Kpps</td>
<td>500 pps</td>
<td>30.86 Kpps</td>
<td>326.28 Mbps @ 21:14</td>
<td>31.59 Kpps</td>
</tr>
<tr>
<td>Packet Rate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Summary

**Snapshot for this Router at 21:14 collected for 60 seconds:**

- **Bytes:** 2.45 GB
- **Packets:** 1,895,200
- **Bytes/Pkt:** 1.29 KB
- **bps:** 326.28 Mbps
- **pps:** 31.59 Kpps
Traffic Analysis

• Can see traffic based on source and destination AS
  - Source and destination AS derived through the routing table on the router
  - Introduces the need to run full mesh BGP at IXPs as well as transit and peering
  - Source and destination prefix based flows can be collected and plotted against external prefix to ASN data
Accounting

• Flow based accounting can be a good supplement to SNMP based accounting.
SNMP and Flows

Data Courtesy  AARNET, Australia and Bruce Morgan
See the fine lines..

Data Courtesy  AARNET, Australia and Bruce Morgan
SNMP and Flows

Data Courtesy  AARNET, Australia and Bruce Morgan
What Next

• IPFIX (IP Flow Information Exchange)
  – To make the flow format uniform and make it easier to write analysis tools
References

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

• NetFlow Applications
  http://www.inmon.com/technology/netflowapps.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