Net-flow

Network Security June 2009 Papeete, French Polynesia



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

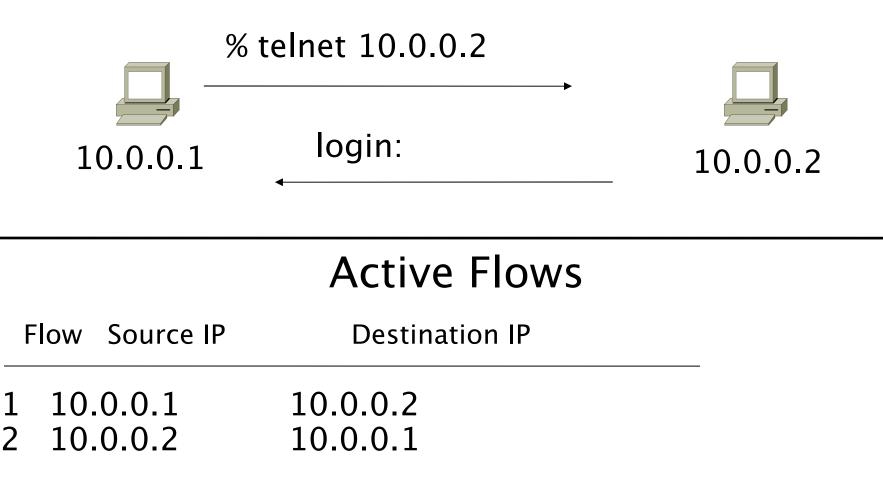
Network Flows

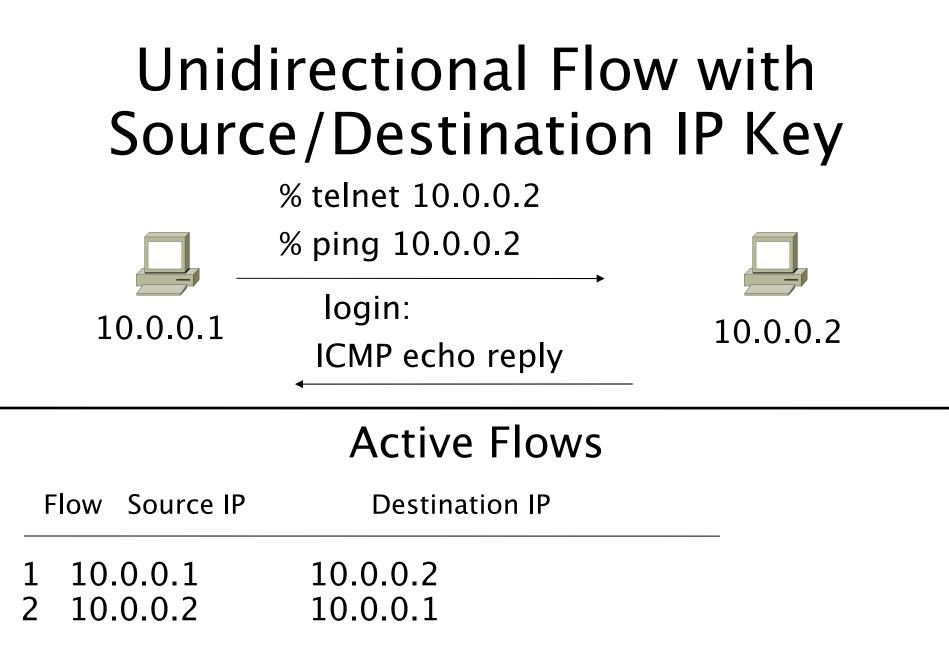
- Packets or frames that have a common attribute.
- Creation and expiration policy what conditions start and stop a flow.
- Counters packets, bytes, time.
- Routing information AS, network mask, interfaces.

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

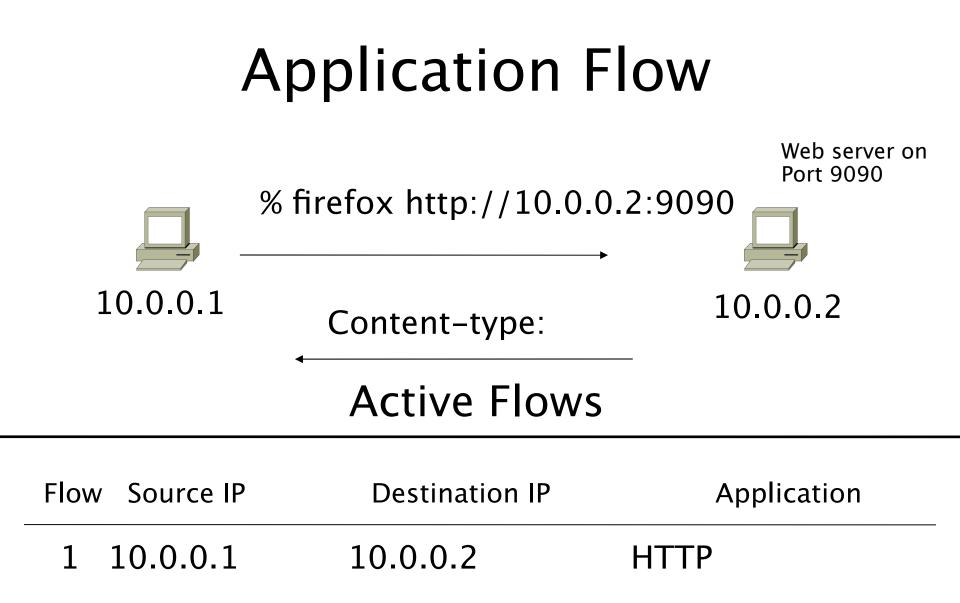




Unidirectional Flow with IP, Port,Protocol Key

10.0.0.1	% telnet 10.0.0.2 % ping 10.0.0.2 login: ICMP echo reply	→ ☐ 10.0.0.2
	Active Flows	
Flow Source IP	Destination IP prot	srcPort dstPort
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	10.0.0.2TCP10.0.0.1TCP10.0.0.2ICMP10.0.0.1ICMP	32000 23 23 32000 0 0 0 0

Bidirectional Flow with IP, Port,Protocol Key							
	% telnet 10.0.0.2						
	% ping 10.0.0.2]			
10.0.0.1	login: ICMP echo repl	У 	10.0	0.0.2			
Active Flows							
Flow Source IP	Destination IP	prot	srcPort o	dstPort			
1 10.0.0.1 2 10.0.0.1	10.0.0.2 10.0.0.2	TCP ICMP	32000 0	23 0			



Aggregated Flow Main Active flow table

Fle	ow Source IP	Destination IP	prot	srcPort	dstPort		
1	10.0.0.1	10.0.0.2	ТСР	32000	23		
3	10.0.0.2 10.0.0.1 10.0.0.2	10.0.0.1 10.0.0.2 10.0.0.1	TCP ICMP ICMP	0	32000 0 0		
Source/Destination IP Aggregate							

Flow Source IP Destination IP Aggregate

110.0.0.110.0.0.2210.0.0.210.0.0.1

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.

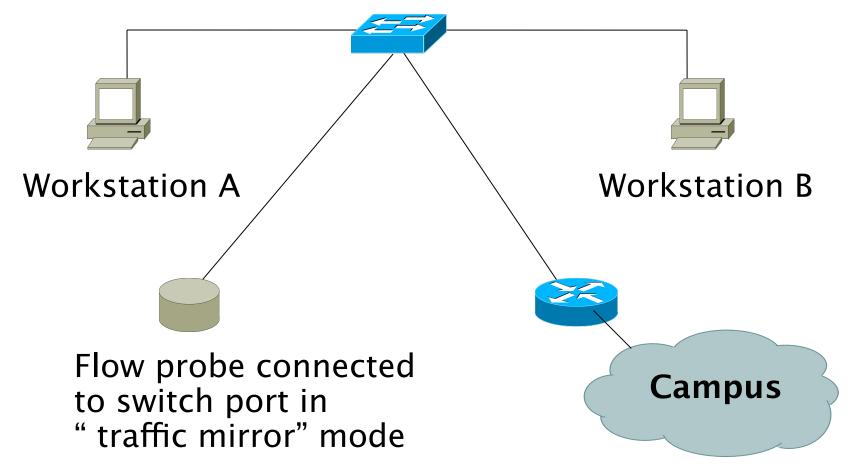
Flow Accounting

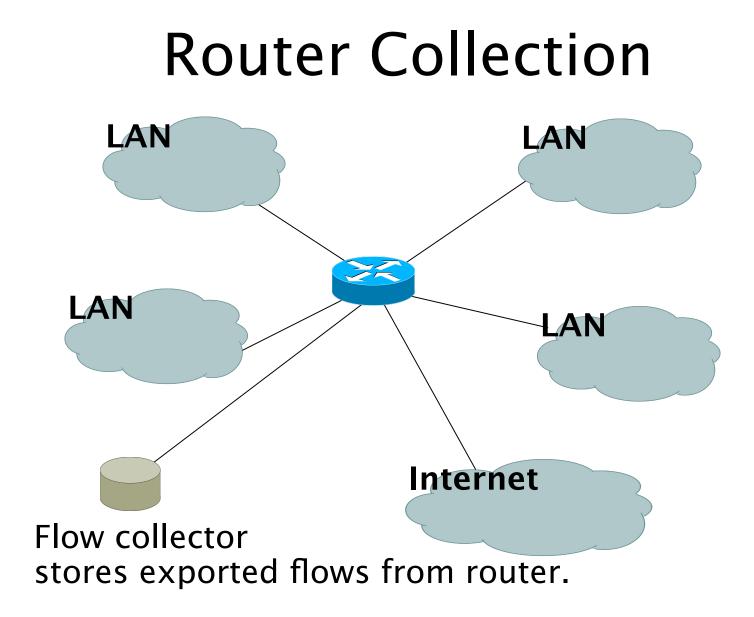
- Accounting information accumulated with flows.
- Packets, Bytes, Start Time, End Time.
- Network routing information masks and autonomous system number.

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

- 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.

- Key fields: Source/Destination IP, Source/Destination Port, IP Protocol, ToS, Input interface.
- Accounting: Packets, Octets, Start/End time, Output interface
- Other: Bitwise OR of TCP flags.

- Key fields: Source/Destination IP, Source/Destination Port, IP Protocol, ToS, Input interface.
- 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.

- 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.

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

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

- 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;
 u int16 count;
 u int32 sysUpTime;
 u int32 unix secs;
 u int32 unix nsecs;
 u int8 engine type;
 u int8 engine id;
 u int16 reserved;
```

/* 5 */ /* The number of records in the PDU */ /* Current time in millisecs since router booted */ /* Current seconds since 0000 UTC 1970 */ /* Residual nanoseconds since 0000 UTC 1970 */ u int32 flow sequence; /* Seq counter of total flows seen */ /* Type of flow switching engine (RP,VIP,etc.) */

/* Slot number of the flow switching engine */

NetFlow v5 Packet (Records)

```
/* 48 byte payload */
 struct ftrec v5 {
   u int32 srcaddr;
                     /* Source IP Address */
                      /* Destination IP Address */
   u int32 dstaddr;
   u int32 nexthop;
                      /* Next hop router's IP Address */
   u int16 input;
                       /* Input interface index */
   u int16 output;
                       /* Output interface index */
                       /* Packets sent in Duration */
   u int32 dPkts;
                     /* Octets sent in Duration. */
   u int32 dOctets;
   u int32 First;
                       /* SysUptime at start of flow */
                      /* and of last packet of flow */
   u int32 Last;
   u int16 srcport; /* TCP/UDP source port number or equivalent */
                       /* TCP/UDP destination port number or equiv */
   u int16 dstport;
   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

NetFlow v8 AS agg. Packet

```
struct ftpdu v8 1 {
 /* 28 byte header */
                        /* 8 */
 u int16 version;
 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.) */
                        /* Slot number of the flow switching engine */
 u_int8 engine_id;
 u_int8 aggregation;
u_int8 agg_version;
                        /* Aggregation method being used */
                        /* Version of the aggregation export */
 u int32 reserved;
 /\overline{*} 28 byte payload */
 struct ftrec v8 1 {
                    /* Number of flows */
   u int32 dFlows;
                     /* Packets sent in duration */
   u_int32 dPkts;
   u int32 dOctets;
                     /* Octets sent in duration */
                     /* SysUpTime at start of flow */
   u int32 First;
   u int32 Last;
                     /* and of last packet of flow */
   u int16 src as; /* originating AS of source address */
                    /* originating AS of destination address */
   u int16 dst as;
                   /* input interface index */
   u int16 input;
   } 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
description Access to backbone
ip address 10.x.y.z 255.255.252.0
ip route-cache flow
duplex auto
speed auto
1
interface FastEthernet0/1
description Access to local net
 ip address 192.168.1.x 255.255.255.192
ip route-cache flow
duplex auto
speed auto
ip flow-export version 5
ip flow-export destination 192.168.1.x 5004
ip flow-top-talkers
  top 10
  sort-by bytes
```

Cisco IOS Configuration

• Change in command in newer IOS

- If CEF is not conf gured on the router, this turns off the existing switching path on the router and enables NetFlow switching (basically modif ed optimum switching).
- If CEF is conf gured on the router, NetFlow simply becomes a "f ow 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) 192.168.1.x (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 fragmentation failures

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 .001

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

Protocol	Total	Flows	Packets	Bytes	Packets	Active (Sec)	Idle	(Sec)
	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/F	'low
TCP-Telnet	3357	0.0	35	92	1.3	0.5	1	1.5
TCP-FTP	128	0.0	19	97	0.0	0.6		1.5
TCP-FTPD	128	0.0	105	771	0.1	0.2		1.5
TCP-WWW	13462	0.1	125	962	19.3	7.0		5.9
TCP-X	269	0.0	1	40	0.0	0.0	1	4.3
TCP-other	9107	0.1	154	62	16.1	6.9		8.2
UDP-DNS	2248	0.0	1	73	0.0	0.8	1	5.4
UDP-NTP	3132	0.0	1	76	0.0	0.0	1	5.4
UDP-TFTP	24	0.0	6	49	0.0	30.0	1	5.3
UDP-Frag	6	0.0	1	32	0.0	0.0	1	5.5
UDP-other	6700	0.0	9	104	0.7	2.2	1	5.5
ICMP	16661	0.1	23	87	4.5	18.5	1	5.4
Total:	55222	0.6	66	480	42.3	8.8	1	1.6
SrcIf	SrcIPaddress	Dst	Tf	DetI	Paddress	Pr SrcP	DetP	Pkts
Fa0/1	169.223.2.19				128.0.7	01 0000		4
Fa0/1	169.223.2.19				185.127.2			4
Fa0/1	169.223.2.2	Fa0			223.15.10			89
Fa0/1	169.223.2.2	Loc			223.2.1	06 DB27		120
Fa0/1	169.223.2.19				128.31.17			4
Fa0/0	208.81.191.1				223.2.194			3

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

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

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Bytes
Fa0/1	169.223.2.2	Fa0/0	169.223.11.33	06	0050	0B64	3444K
Fa0/1	169.223.2.2	Fa0/0	169.223.11.33	06	0050	0B12	3181K
Fa0/0	169.223.11.33	Fa0/1	169.223.2.2	06	0B12	0050	56K
Fa0/0	169.223.11.33	Fa0/1	169.223.2.2	06	0B64	0050	55K
Fa0/1	169.223.2.2	Local	169.223.2.1	01	0000	0303	18K
Fa0/1	169.223.2.130	Fa0/0	64.18.197.134	06	9C45	0050	15K
Fa0/1	169.223.2.130	Fa0/0	64.18.197.134	06	9C44	0050	12K
Fa0/0	213.144.138.195	Fa0/1	169.223.2.130	06	01BB	DC31	7167
Fa0/0	169.223.15.102	Fa0/1	169.223.2.2	06	C917	0016	2736
Fa0/1	169.223.2.2	Local	169.223.2.1	06	DB27	0016	2304
10 of 10 top	talkers shown. 4	9 flows proces	ssed.				

Cisco command summary

• Enable CEF

- ip cef - this is the default nowadays

- 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 f ows
- 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

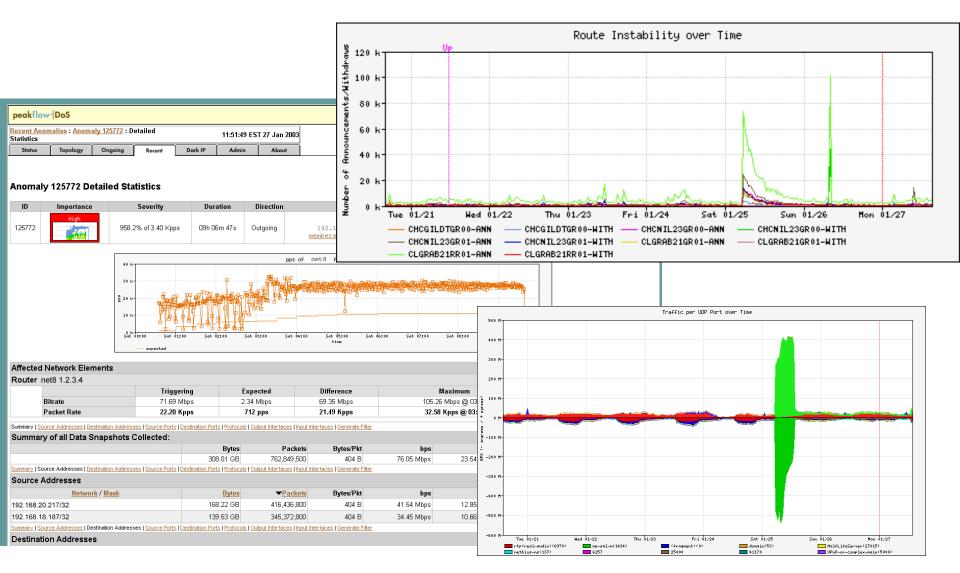
Traceback: Flow-based*

- 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*



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

Get Report: PDF XML

ID	Importance	Duration	Start Time	Direction	Туре	Resource
150228	High 130.0% of 2 Kpps	17 mins	03:34, Aug 16	Incoming	Bandwidth (Profiled)	Microsoft 207.46.0.0/16 windowsupdate.com

Traffic C	haracterization	3 k	-			pps of	affecte	ed eleme	nts for	anomaly 1	.50228		
Sources	204.38.130.0/24	2.5 k			E	3							
	204.38.130.192/26	2 16			-8-			A B	٣\	<u></u>			
	1024 - 1791	å 1.5 k	-					_		<u> </u>			
Destination	207.46.248.234/32	1 к								<u> </u>			
	80 (http)	0.5 k	-								<u> </u>		
Protocols	tcp (6)	0 k 03:	36:00	03:38:00	03:	40:00	03:42:0	0 03:4	4:00	03:46:00	03:48:00	03:50:00	03:52:00
TCP Flags	S (0x02)			-chi3 - 67					ime				

Affected Network Elements		Expected	Obser	ved bps	Observ	red pps
	Importance	pps	Max	Mean	Max	Mean
Router nl-chi3 198.110.131.125	High					
Interface 67 at-1/1/0.14 pvc to WMU		26	832 K	563.1 K	2.6 K	1.7 K Details

Anomaly Comments

Commercial Detection A Large Scale DOS attack*

∃le <u>E</u> dit	View Favorit	es Iools Help								
				Anom	aly 14957 Inform	ation				
ID	Importance	Severity	Duration	Direction		Resource	Start Time	End Time	Class	Subclass
4957	High	108,759.0% of 300.00 Kbps	02h 04m 18s	Incoming	Fast.	bt.net- Ethernet5/1 .1/32 <u>BTnet-Core</u>		23:09:41 BST 15 Jun 2003	Misuse	IP Fragmentatio Anomaly
				bps of af	fected elements for an	maly 14957				
	350 H 300 H 250 H 200 H 150 H 100 H 50 H	M.	Lander (Ja J		mesichtere	VVTV	- Marter	*** ***		
	0 H+ 21:00	:00 21:10:00 21:20:00	21:30:00 21:4	0:00 21:50:00	22:00:00 22:10:00 time	22:20:00 22:	30:00 22:40:	00 22:50:00	23:00:00	23:10:00
		🖶 conel-telehouse 🕁 conel-telehouse - 5	···· corei-teleb	ouse expected ouse - 5 expected	→ core1-telehouse - 2 → core1-telehouse - 15		1-telehouse - 2 1-telehouse - 15			
		🖶 corel-telehouse - 17	···· core1-teleh	ouse - 17 expecta	ed 🔆 core1-telehouse - 27	core	el-telehouse - 23	/ expected		
		👉 core1-telehouse - 49 ⊕ transit1-ealing	···· corel-teleh ···· transit1-ea	ouse - 49 expects	id → corei-telehouse - 51 → transiti-ealing - 4		e1-telehouse - 5: hsit1-ealing - 4			
		- transit1-ealing - 5		ling - 5 expected			sit1-ealing - 2			
		🕂 transit1-ealing - 21			\rightarrow transit2-ealing		sit2-ealing exp			
		A transit2-caling - 4 □ core2-telehouse - 2		ling - 4 expected ouse - 2 expected			2-telehouse expe 2-telehouse - 5			
		A- core2-telehouse - 6		ouse - 6 expected			2-telehouse - 9			
		🖶 core2-telehouse - 11 🛆 core2-telehouse - 35			ed 🔆 core2-telehouse - 34		2-telehouse - 34			
				ouse - 35 expects ford - 2 expects	ed —★ transit1-ilford →→ transit1-ilford - 3		nsitl—ilford expo nsitl—ilford — 3			
		👍 transit1-ilford - 4	transit1-i)	ford - 4 expected	-*- transiti-ilford - 5	tra	weit1-ilford - 5	expected		
ffecte	d Network E	lements								
louter	core1-teleh	ouse (195.99.120.112)								Hi
		100101	Trigge	ring	Expected	D	ifference	Maximun	n	Mean
	Bitrate							326.28 Mbps @	21:14	16.31 Mbps
	Packet Rate		31.36	<pps< td=""><td>500 pps</td><td>30</td><td>0.86 Kpps</td><td><u>31.59 Kpps @</u></td><td>21:14</td><td>11.36 Kpps</td></pps<>	500 pps	30	0.86 Kpps	<u>31.59 Kpps @</u>	21:14	11.36 Kpps
	Interface 2 F	POS4/0 (FXCC200030	STM-16 dir	ect fibre (n	ot SDH) link to cor	e1.ealing PC	0)	Maximun	n	Mean
						Bitra	te	87.84 Mbps @	21.15	27.17 Mbps
						Ditta			61.1.5	ci.ii muya

Traceback: Commercial*

Anomaly 150	0291								
ID	Importance	Duration	Start Time	Direction		Туре			Resou
150291	High 124.6% of 40 Mbps	19 mins	09:16, Aug 17	Incoming		tocol TCP Profiled)			1WF 17
Traffic Chara	acterization		bps	of affected ele	ments for	anomaly 15	0291		
Sources	136.165.56.151/32	60 M							
	59.1.194.74 /32	50 M-				8		۹	
	0 - 4095	40 H-			- Area	A P	A-	17.	
Destination		š 30 H-		A BH	A		***		<u>=</u> K
		20 H-				-EL E	b —-a—-	E	À
	1409 (here-lm)	10 H-			¥××	×	<u> </u>	***	*
rotocols	tcp (6)	0 M	09:20:00 09:22:00 09:24	:00 09:26:00 0	9:28:00 09	:30:00 09:3	<u>Å Å</u> 32:00 09:	:34:00 09:	36:00 09:38
CP Flags	AP (0x18) A (0x10)	05.10.00	05.20.00 05.22.00 05.2	.00 05.20.00 0		.30.00 09.0	2.00 09.	.34.00 05.	36.00 05.30
		ac m ac	11 expected 11 - 38 11 - 38 11 - 43	michnet8 expected michnet8 - 145 aa1 - 38 expected aa1 - 39 aa1 - 43 expected michnet8 - 127	n n o o	nichnet8 – 14 nichnet8 – 14 1a1 – 39 expe 1a1 – 63	6 cted		
Affected Net	work Elements	ac m ac	11 expected 11 - 38 ichnet8 - 146 expected → 11 - 43	michnet8 - 145 aa1 - 38 expected aa1 - 39 aa1 - 43 expected michnet8 - 127	p p c p	nichnet8 – 14 nichnet8 – 14 aa1 – 39 expe aa1 – 63 nichnet8 – 12	6 cted 7 expected	d	
Affected Net	work Elements	ac m ac	11 expected 11 - 38 11 - 38 11 - 43	michnet8 – 145 aa1 – 38 expected aa1 – 39 aa1 – 43 expected	→ a n a -+- a	nichnet8 – 14 nichnet8 – 14 aa1 – 39 expe aa1 – 63 nichnet8 – 12	6 cted	d	
	work Elements 8 198.108.90.125	ac m ac	11 expected	michnet8 - 145 aa1 - 38 expected aa1 - 39 aa1 - 43 expected michnet8 - 127 Expected	Observe	nichnet8 - 14 nichnet8 - 14 na1 - 39 expe na1 - 63 nichnet8 - 12 ed bps	of octed ?7 expected Observe	d ed pps	Details
touter michnet	8 198.108.90.125 27 ATM1/0.27-aal5 layer 198.108.22.1	at at at	11 expected	michnet8 - 145 aa1 - 38 expected aa1 - 39 aa1 - 43 expected michnet8 - 127 Expected bps	Observe Max	nichnet8 - 14 nichnet8 - 14 na1 - 39 expe na1 - 63 nichnet8 - 12 ed bps Mean	6 cted ?7 expected Observe Max	d ed pps Mean	Details Details
louter michnett Interface 12 ρκτλα ΝΕ-ΡΟΡ	8 198.108.90.125 27 ATM1/0.27-aal5 layer 198.108.22.1 */ 45 GigabitEthernet5/0.22 - 802.1q vlan 1	81	11 expected	michnet8 - 145 aa1 - 38 expected aa1 - 39 aa1 - 43 expected michnet8 - 127 Expected bps	Observe Max 49.9 M	nichnet8 - 14 nichnet8 - 14 na1 - 39 expe aa1 - 63 nichnet8 - 12 ed bps Mean 38.7 M	0 cted 7 expected 0 bserve Max 5.3 K	a ad pps Mean 4.2 K	
outer michnett Interface 12 איז או אר איז	8 198.108.90.125 27 ATM1/0.27-aal5 layer 198.108.22.1 */ 45 GigabitEthernet5/0.22 - 802.1q vlan 1	81 subinterface 198.108	11 expected	michnet8 - 145 aa1 - 38 expected aa1 - 39 aa1 - 43 expected michnet8 - 127 Expected bps		nichnet8 - 14 nichnet8 - 14 nic1 - 39 expe and - 63 nichnet8 - 12 ed bps Mean 38.7 M 1.2 K	Observe Max 5.3 K	a Ad pps Mean 4.2 K 2.4	Details
outer michnet Interface 12 prc to NL-POR Interface 14 vian to MchBin Interface 14 CHI-ANN_Bin	8 198.108.90.125 27 ATM1/0.27-aal5 layer 198.108.22.1 77 45 GigabitEthernet5/0.22 - 802.1q vlan s 46 GigabitEthernet5/0.24 - 802.1q vlan s	81 subinterface 198.108	11 expected	michnet8 - 145 aa1 - 38 expected aa1 - 39 aa1 - 43 expected michnet8 - 127 Expected bps		nichnet8 - 14 nichnet8 - 14 nichnet8 - 14 nichnet8 - 14 nichnet8 - 12 ed bps Mean 38.7 M 1.2 K 25.8 M	00000000000000000000000000000000000000	a Mean 4.2 K 2.4 2.6 K	Details Details
louter michnett Interface 12 px: Io NLPOR Interface 14 via Io McKBin Interface 14 CHLANN_Bin Iouter aa1 198	8 198.108.90.125 27 ATM1/0.27-aal5 layer 198.108.22.1 77 45 GigabitEthernet5/0.22 - 802.1q vlan s 46 GigabitEthernet5/0.24 - 802.1q vlan s .108.90.21 8 so-0/2/0.1 192.122.183.9	81 subinterface 198.108	11 expected	michnet8 - 145 aal - 38 expected aal - 39 aal - 43 expected michnet8 - 127 Expected bps 7.2 M - -	Observe Max 49.9 M 3.3 K 38.4 M 16.6 M	nichnet8 - 14 nichnet8 - 14 na1 - 39 expe na1 - 39 expe nichnet8 - 12 ed bps Mean 38.7 M 1.2 K 25.8 M 12.8 M	66 17 expected 0bserve Max 5.3 K 5 3.7 K 1.9 K	ed pps // Mean // 4.2 K // 2.4 // 2.4 // 2.6 K // 1.6 K // 1.6 K	Details Details Details
outer michnett Interface 12 px to NL-POR Interface 14 Wa to McABin Interface 14 CHI-AVIN_Bin outer aa1 198 Interface 38 px to Abites 1	8 198.108.90.125 27 ATM1/0.27-aal5 layer 198.108.22.1 7/ 15 GigabitEthernet5/0.22 - 802.1q vlan t 16 GigabitEthernet5/0.24 - 802.1q vlan t .108.90.21 3 so-0/2/0.1 192.122.183.9 //wdanapa/ss	81 subinterface 198.108	11 expected	michnet8 - 145 aal - 38 expected aal - 39 aal - 43 expected michnet8 - 127 Expected bps 7.2 M - -	Wax 49.9 M 3.3 K 38.4 M 16.6 M 44.4 M	nichnet8 - 14 nichnet8 - 14 nichnet8 - 14 nichnet8 - 14 nichnet8 - 12 ed bps Mean 38.7 M 1.2 K 25.8 M 12.8 M 36.6 M	66 7 67 0bserve Max 5.3 K 5 3.7 K 1.9 K 4.5 K	a ded pps Mean 4.2 K 2.6 K 1.6 K 3.8 K	Details Details Details Details Details
outer michnett Interface 12 pr: to MPOP Interface 14 who to McABin Interface 13 Difference 14 CHI-ANN_Bin outer aal 198 interface 38 pr: to Ower C	8 198.108.90.125 27 ATM1/0.27-aal5 layer 198.108.22.1 77 45 GigabitEthernet5/0.22 - 802.1q vlan s 46 GigabitEthernet5/0.24 - 802.1q vlan s .108.90.21 8 so-0/2/0.1 192.122.183.9 /ndianapais 9 so-0/2/0.2 63.149.0.186 3/hcaga 8 so-1/0/0.0 208.172.10.138	81 subinterface 198.108	11 expected	michnet8 - 145 aal - 38 expected aal - 39 aal - 43 expected michnet8 - 127 Expected bps 7.2 M - -	Observe Max 49.9 M 3.3 K 38.4 M 16.6 M 44.4 M 34.0 M	nichnet8 - 14 nichnet8 - 14 nichnet8 - 14 na1 - 39 expense nichnet8 - 12 mod bps Mean 38.7 M 1.2 K 25.8 M 12.8 M 36.6 M 24.0 M	Max 5.3 K 5.7 K 1.9 K 4.5 K 3.0 K	d Mean 4.2 K 2.4 2.6 K 1.6 K 3.8 K 2.2 K	Details Details Details Details Details Details

Commercial Traceback: More Detail*

	_	maly 14957 : I	Detailed Statistic	cs - Microsoft Internet	Explorer provided	υγ			_ 8
	ools <u>H</u> elp								
Anomaly 14957 Det	tailed Statistics						Sample 8	@ 21:14	-
ID Importance	Severity	Duration	Direction		Resource	Start Time	End Time	Class	Subclass
High 14957	3,759.0% of 300.00 Kbps	02h 04m 18s	Incoming	Fast	Ethernet5/12 BTnet-Core	21:05:23 BST 23 15 Jun 2003		Misuse F	IP ragmentat Anomaly
	- 2		bps of co	pre1-telehouse for an	omaly 14957				
360 H- <u>\$</u> 260 H- 160 H-		Ŀ₹ _ſ ₽₽ _₽ ₽₽ _₽ ₽₽	₽₽₽₽₽₽	peres being be	₱ _⊌ ኈ₽ _₽ ₽₽₽	La Bash ba	₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽		
•	21:10:00 21:20:00 expected ments	21:50:00	21:40:00 21:5	0:00 22:00:00 22 time	22120100 22120100	22:30:00	22:40:00 :	22:50:00	23:00:00
Affected Network Ele	expected ments	21:30:00	21:40:00 21:5		22120100 22120100	22:30:00	22140100 :	22:50:00	23:00:00 High
Affected Network Ele	expected ments		211:40:00 2115		Max	kimum	22:40:00 :	22:59:00 Mea	High
Affected Network Eler Router core1-telehou Bitrate	expected ments se (195.99.120.112) Triggering	Exj	pected	tine Difference	Ma: 326.28 M	kimum bps @ 21:14	22140100 :	Mea 326.28	High n Mbps
Affected Network Ele Router core1-telehou	expected ments se (195.99.120.112)	Exj		tine	Ma: 326.28 M	kimum	22:40:00	Mea	High n Mbps
Affected Network Eler Router core1-telehou Bitrate Packet Rate	expected ments se (195.99.120.112) Triggering 31.36 Kpps estination Addresses Source	Exj 50 Ports Destinati	Dected Opps on Ports Protocols	Difference 30.86 Kpps	Мал 326.28 М 31.59 Кр	kimum bps @ 21:14 ps @ 21:14	22:40:00	Mea 326.28	High n Mbps
Affected Network Eler Router core1-telehou Bitrate Packet Rate	expected ments se (195.99.120.112) Triggering 31.36 Kpps estination Addresses Source	Exp 50 Ports Destinati ed for 60 s Bytes	oected 0 pps on Ports Protocols econds: Packets	Difference 30.86 Kpps Output Interfaces Input Bytes/Pkt	Ma: 326.28 M 31.59 Kg Interfaces Generaty bps	kimum bps @ 21:14 ps @ 21:14 <u>= Filter</u> Pl	15	Mea 326.28	High n Mbps
Affected Network Eler Router core1-telehou Bitrate Packet Rate	expected ments se (195.99.120.112) Triggering 31.36 Kpps estination Addresses Source uter at 21:14 collected	Exp 50 Ports Destinati ed for 60 s Bytes 2.45 GB	oected 0 pps on Ports Protocols econds: Packets 1,895,200	Difference 30.86 Kpps Output Interfaces Input Bytes/Pkt 1.29 KB	Ma: 326.28 M 31.59 Kş Interfaces Generate bps 326.28 Mbps	kimum bps @ 21:14 ips @ 21:14 sFilter PF 31.59 Kpp 31.59 Kpp	15	Mea 326.28	High n Mbps
Affected Network Eler Router core1-telehou Bitrate Packet Rate Summary Source Addresses Du	expected ments se (195.99.120.112) Triggering 31.36 Kpps estination Addresses Source uter at 21:14 collected	Exp 50 Ports Destinati ed for 60 s Bytes 2.45 GB	oected 0 pps on Ports Protocols econds: Packets 1,895,200	Difference 30.86 Kpps Output Interfaces Input Bytes/Pkt 1.29 KB	Ma: 326.28 M 31.59 Kş Interfaces Generate bps 326.28 Mbps	kimum bps @ 21:14 ips @ 21:14 sFilter PF 31.59 Kpp 31.59 Kpp	15	Mea 326.28	High n Mbps
Affected Network Eler Router core1-telehou Bitrate Packet Rate Summary Source Addresses Dr Snapshot for this Rou	expected ments se (195.99.120.112) Triggering 31.36 Kpps estination Addresses Source uter at 21:14 collector estination Addresses Source	Exj 50 Ports Destinati ed for 60 s Bytes 2.45 GB Ports Destinati	oected 0 pps on Ports Protocols econds: Packets 1,895,200 on Ports Protocols	Difference 30.86 Kpps Outout Interfaces Input Bytes/Pkt 1.29 KB Outout Interfaces Input	Ma: 326.28 M 31.59 Kg Interfaces Generate bps 326.28 Mbps Interfaces Generate	kimum bps @ 21:14 ps @ 21:14 <u>s Filter</u> 91 31.59 Kpp <u>a Filter</u>	95 15	Mea 326.28 31.59	High n Mbps (pps
Affected Network Eler Router core1-telehou Bitrate	expected ments se (195.99.120.112) Triggering 31.36 Kpps estination Addresses Source uter at 21:14 collector estination Addresses Source	Exp 50 Ports Destinati ed for 60 s Bytes 2.45 GB	oected 0 pps on Ports Protocols econds: Packets 1,895,200	Difference 30.86 Kpps Output Interfaces Input Bytes/Pkt 1.29 KB	Ma: 326.28 M 31.59 Kş Interfaces Generate bps 326.28 Mbps	kimum bps @ 21:14 ips @ 21:14 sFilter PF 31.59 Kpp 31.59 Kpp	95 15	Mea 326.28	High n Mbps (pps

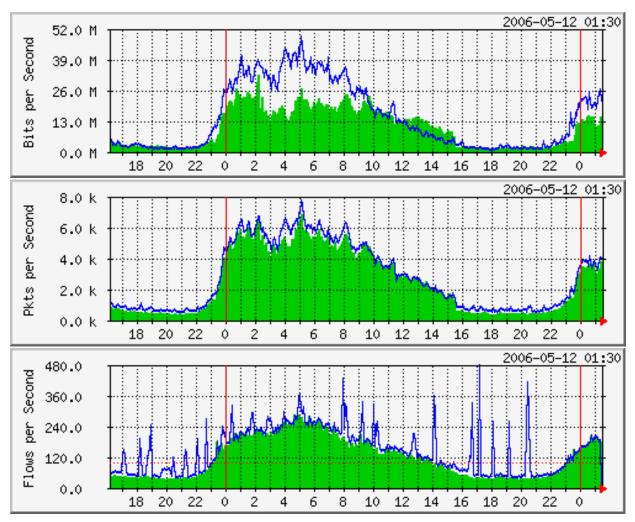
Traffic Analysis

- 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

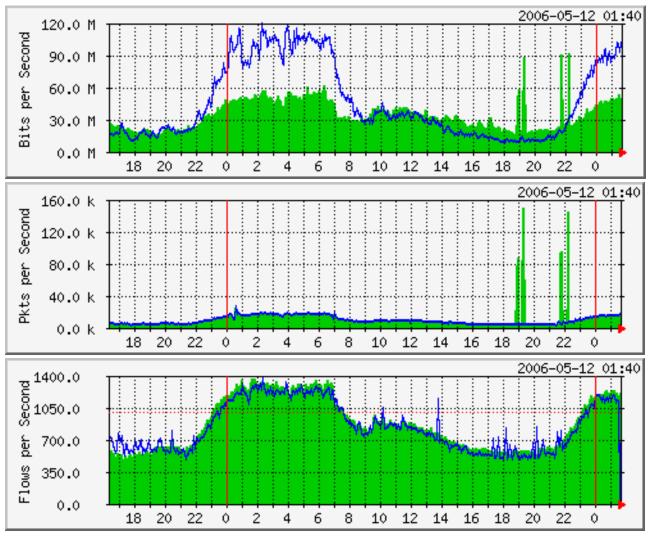
• Flow based accounting can be a good supplement to SNMP based accounting.

SNMP and Flows



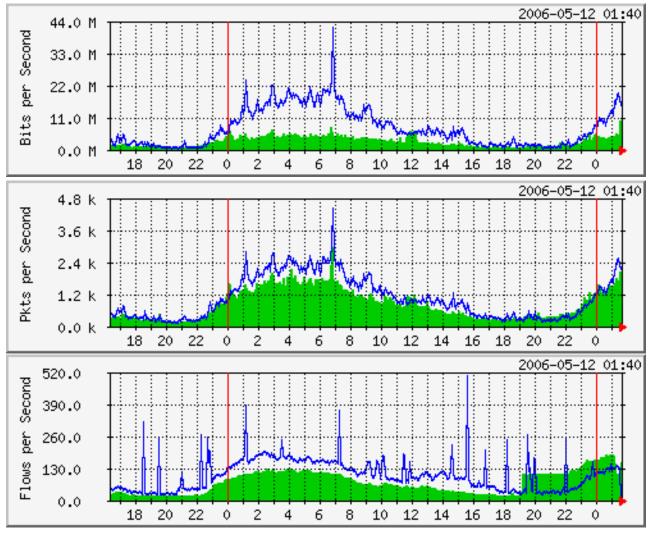
Data Courtesy AARNET, Australia and Bruce Morgan

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
 - http://www1.ietf.org/html.charters/ipfix-charter.html
 - <u>Requirements for IP Flow Information Export (RFC 3917)</u>
 - <u>Evaluation of Candidate Protocols for IP Flow Information</u> <u>Export (IPFIX) (RFC 3955)</u>

References

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

http://www.inmon.com/technology/netflowap

ps.php

- Netflow HOW–TO http://www.linuxgeek.org/netflow–howto.php
- IETF standards effort: http://www.ietf.org/html.charters/ipfixcharter.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

References

- http://ensight.eos.nasa.gov/FlowView er/
- http://nfsen.sourceforge.net/
- http://www.netflowdashboard.com/