

There's Plenty of Room at the Bottom:

An Invitation to Explore with Network Flows



Benjamin Black

b@fastip.com

What are Flows
&
Why Should You Care?

You Should Care
Because Visibility Makes
Your Life Easier.

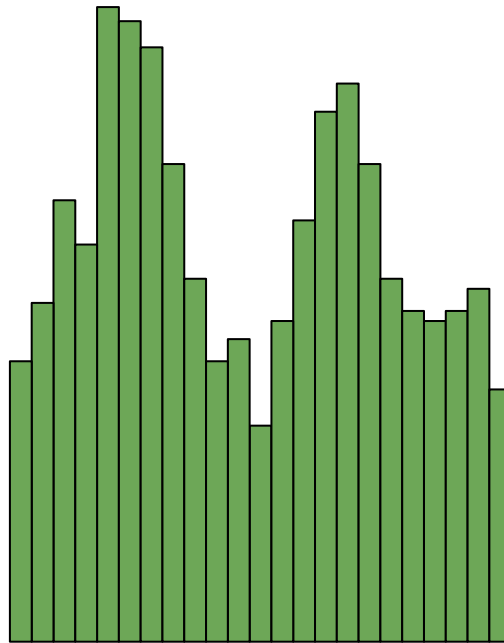
Network Flow Data
Means Great Visibility.

DDoS Detection
Capacity Planning
Traffic Management
Troubleshooting
Correlation

...

The Nature of Flows

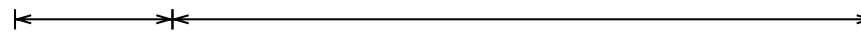
[traffic]



[streams]



[packets]



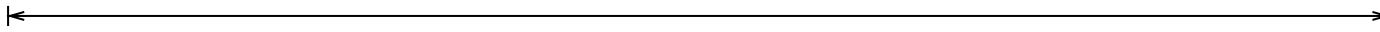
Header

Payload

[headers]

<i>Protocol</i>
<i>Source IP Address</i>
<i>Destination IP Address</i>
<i>Source Port</i>
<i>Destination Port</i>

[latency]



[jitter]



[packet loss]



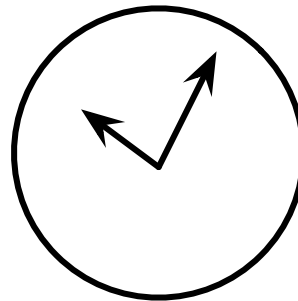
The Structure of Flows

[flow keys]

<i>Protocol</i>
<i>Source IP Address</i>
<i>Destination IP Address</i>
<i>Source Port</i>
<i>Destination Port</i>

=

<i>Protocol</i>
<i>Source IP Address</i>
<i>Destination IP Address</i>
<i>Source Port</i>
<i>Destination Port</i>



[templates]

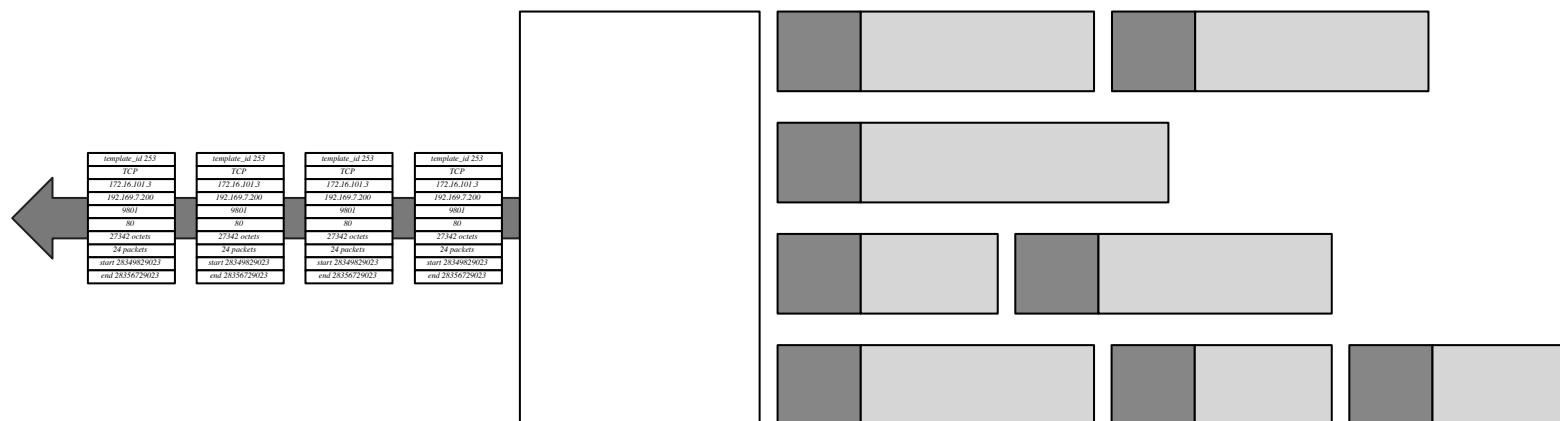
<i>template_id 253</i>
<i>protocol</i>
<i>src IPv4 address</i>
<i>dest IPv4 address</i>
<i>src port</i>
<i>dst port</i>
<i>total octets</i>
<i>total packets</i>
<i>start time</i>
<i>end time</i>

[flow records]

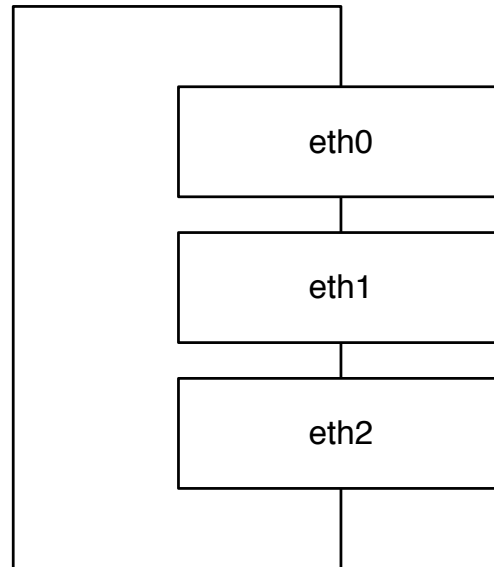
<i>template_id 253</i>
<i>TCP</i>
<i>172.16.101.3</i>
<i>192.169.7.200</i>
<i>9801</i>
<i>80</i>
<i>27342 octets</i>
<i>24 packets</i>
<i>start 28349829023</i>
<i>end 28356729023</i>

The Ecosystem of Flows

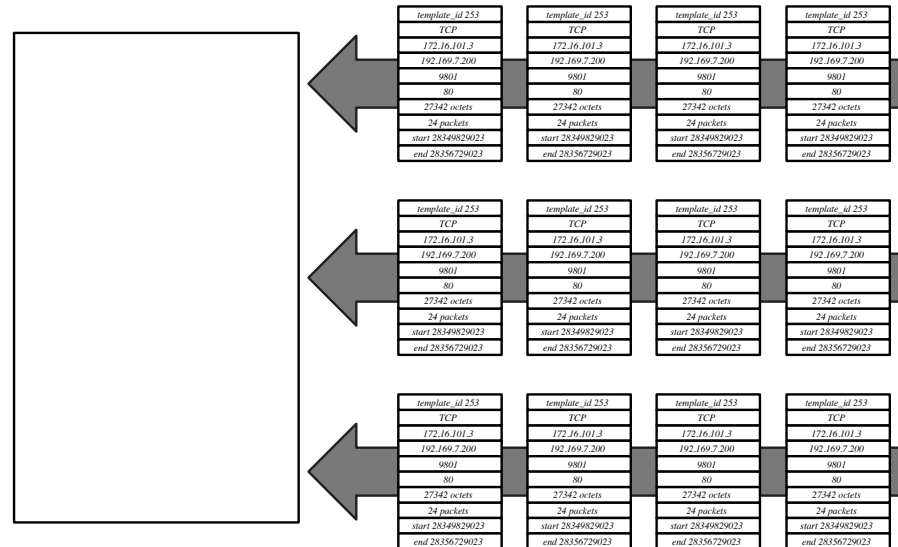
[metering process]



[observation domain]



[collecting process]



Storage and Analysis are
Left as an Exercise
for the Reader

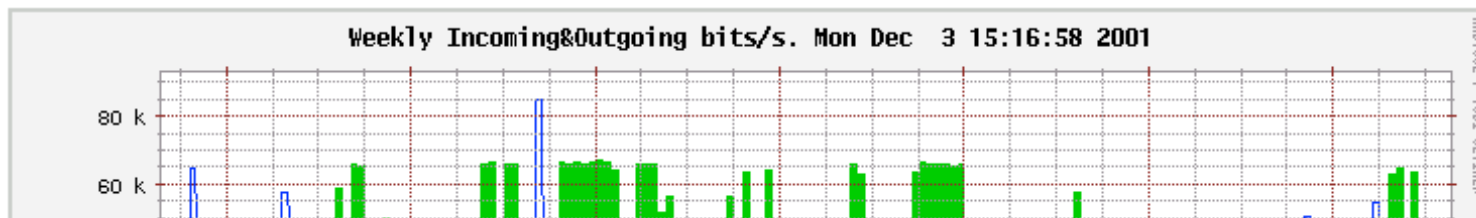
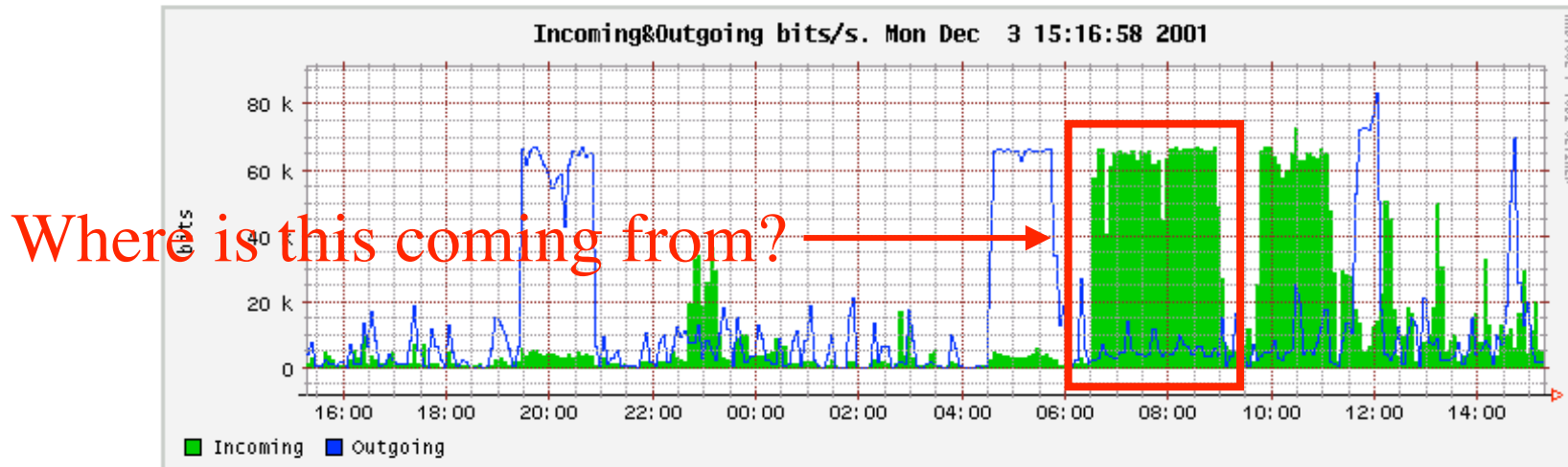
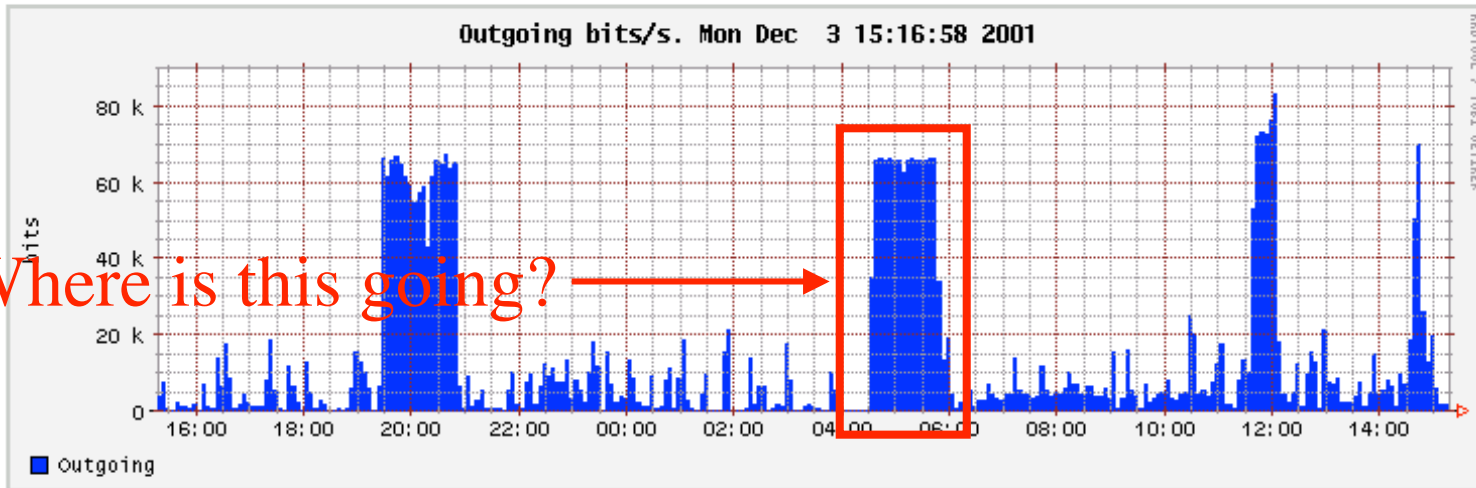
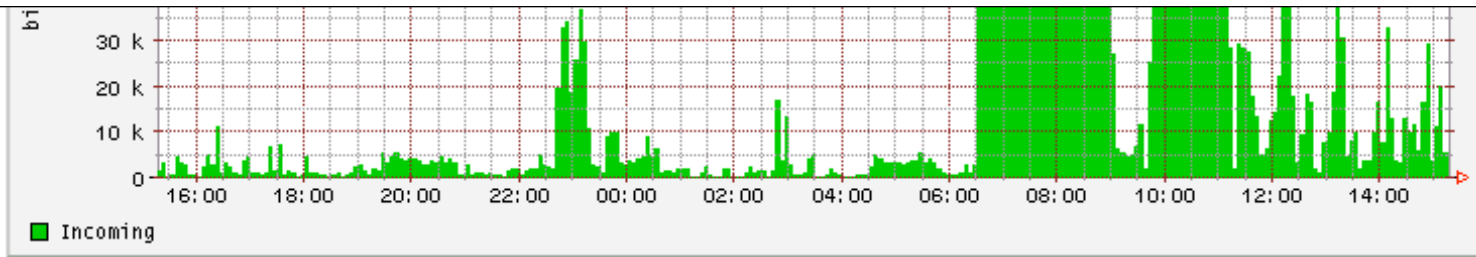
Where Do Meters Run?

On Network Switches/Routers [often sampled]

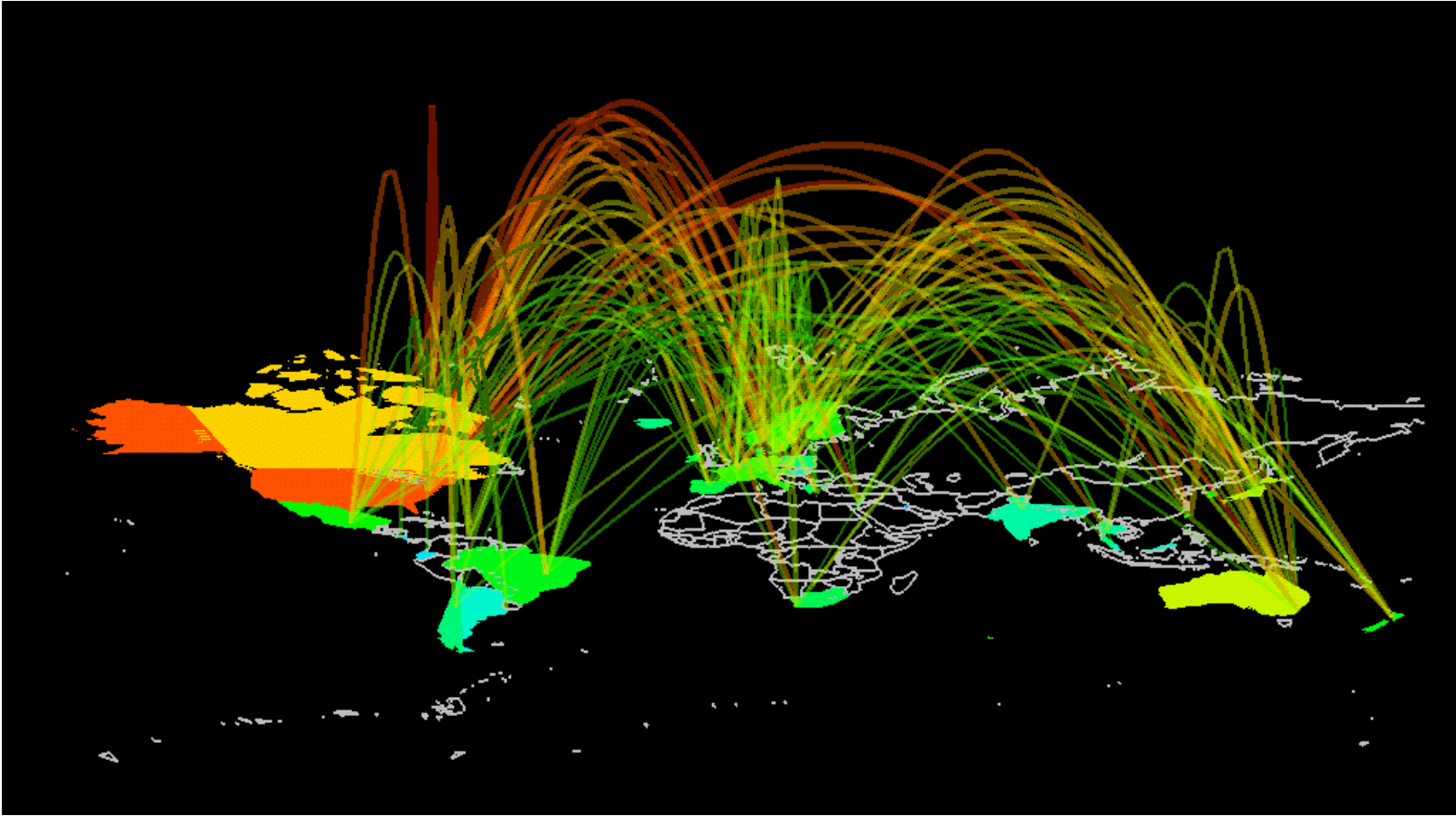
Dedicated Appliances
[expensive/limited storage]

On Hosts
[where does the data go?]

The Classical View



The Flow View



TANSTAAFL

Flow Data Takes Up
LOTS of Space

[often $>1\%$ total traffic]

**LOTS of Space Means Storage
Expense or Loss of Resolution or
Truncation**

LOTS of (Multi-dimensional)
Data is
Hard to Analyze

Inflexible and Limited
or
Expensive and Complicated

REDACTED

[apologies]

[resources]

IPFIX WG

<http://datatracker.ietf.org/wg/ipfix/charter/>

nProbe

<http://www.ntop.org/nProbe.html>

Cisco NetFlow Collection Engine

<http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/index.html>


Arbor Networks

<http://www.arbornetworks.com/>

Dartware

<http://www.intermapper.com/products/intermapper-flows>


[finally...]



fastip is a platform for
flow analytics

Sign up for our beta

<http://fastip.com>



fastip