



# Network Management & Monitoring

## NetFlow Overview



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>)

# Agenda

## Netflow

- What it is and how it works
- Uses and Applications

## Flow-tools

- Architectural issues
- Software, tools etc

## Lab

# 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.

# Cisco's Definition of a Flow

Unidirectional sequence of packets sharing

1. Source IP address
2. Destination IP address
3. Source port for UDP or TCP, 0 for other protocols
4. Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
5. IP protocol
6. Ingress interface (SNMP ifIndex)
7. IP Type of Service

# 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.

# Working with Flows

- Generate the flows from device (usually a router)
- Export flows from the device to collector
  - Configure version of flows
  - Sampling rates
- Collect the flows
  - Tools to Collect Flows - Flow-tools
- Analyze them
  - More tools available, can write your own

# Flow Descriptors

- A Key with more elements will generate more flows.
- Greater number of flows equals:
  - More post processing time to generate reports
  - more memory and CPU requirements for device generating flows
  - More storage needed on the flow processing server
- 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

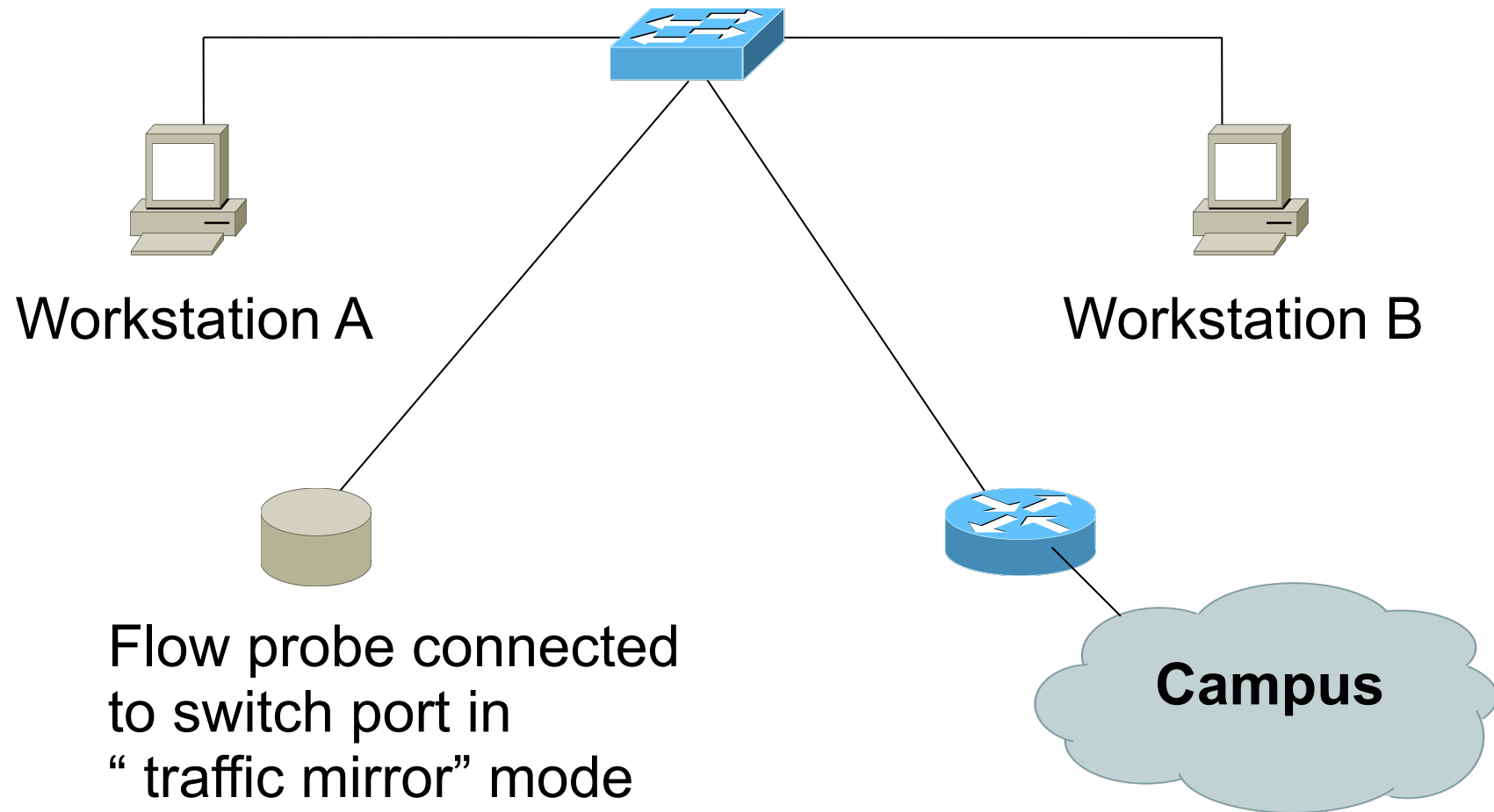
## **Passive monitor**

- A passive monitor (usually a Unix host) receives all data and generates flows.
- Resource intensive

## **Router or other existing network device**

- Router or other existing devices like switch, generate flows.
- Sampling is possible
- Nothing new needed

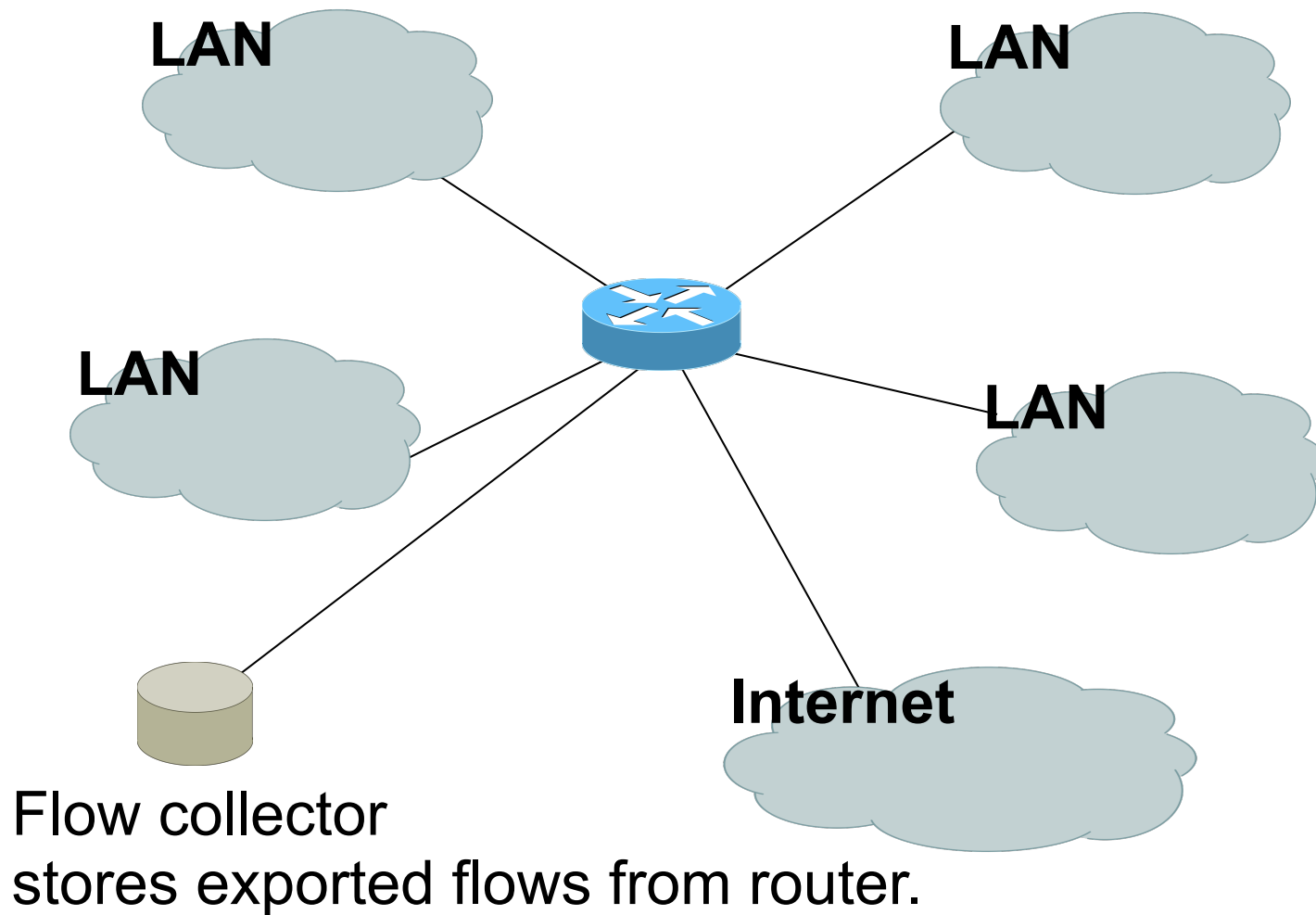
# Passive Monitor Collection



# Passive Collector

- Using passive collection, not all flows in the network will be seen as opposed to collection from the router
- The collector will only see flows from the network point it is connected on
- However this method does relieve the router from processing netflows and exporting them
- Useful on links with only one entry into the network or where only flows from one section of the network are needed

# Router Collection



# Router Collection

- With this method, all flows in the network can be observed
- However, more work for the router in processing and exporting the flows
- Optionally, one can choose on which interfaces netflow collection is needed and not activate it on others
- Also, if there is a router on each LAN, netflow can be activated on those routers to reduce the load on the core router

# 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 Version 1

- 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.
- Obsolete



# NetFlow Versions 2-4

- Cisco internal
- Were never released

# NetFlow v5

- 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.
- IPv4 only

# 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 v9

- IPv6 support
- Additional fields like MPLS labels
- Builds on earlier versions

# 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

```
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. 49 flows processed.
```

# Cisco Command Summary

- Enable CEF (done by default)

- `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>
```

- Origin AS will include the origin AS Number in the flow while Peer AS will only include the AS Number of the peering neighbor
- Exporting aggregated flows

```
ip flow-aggregation cache as|prefix|dest|source|proto  
enabled  
export destination x.x.x.x <udp-port>
```



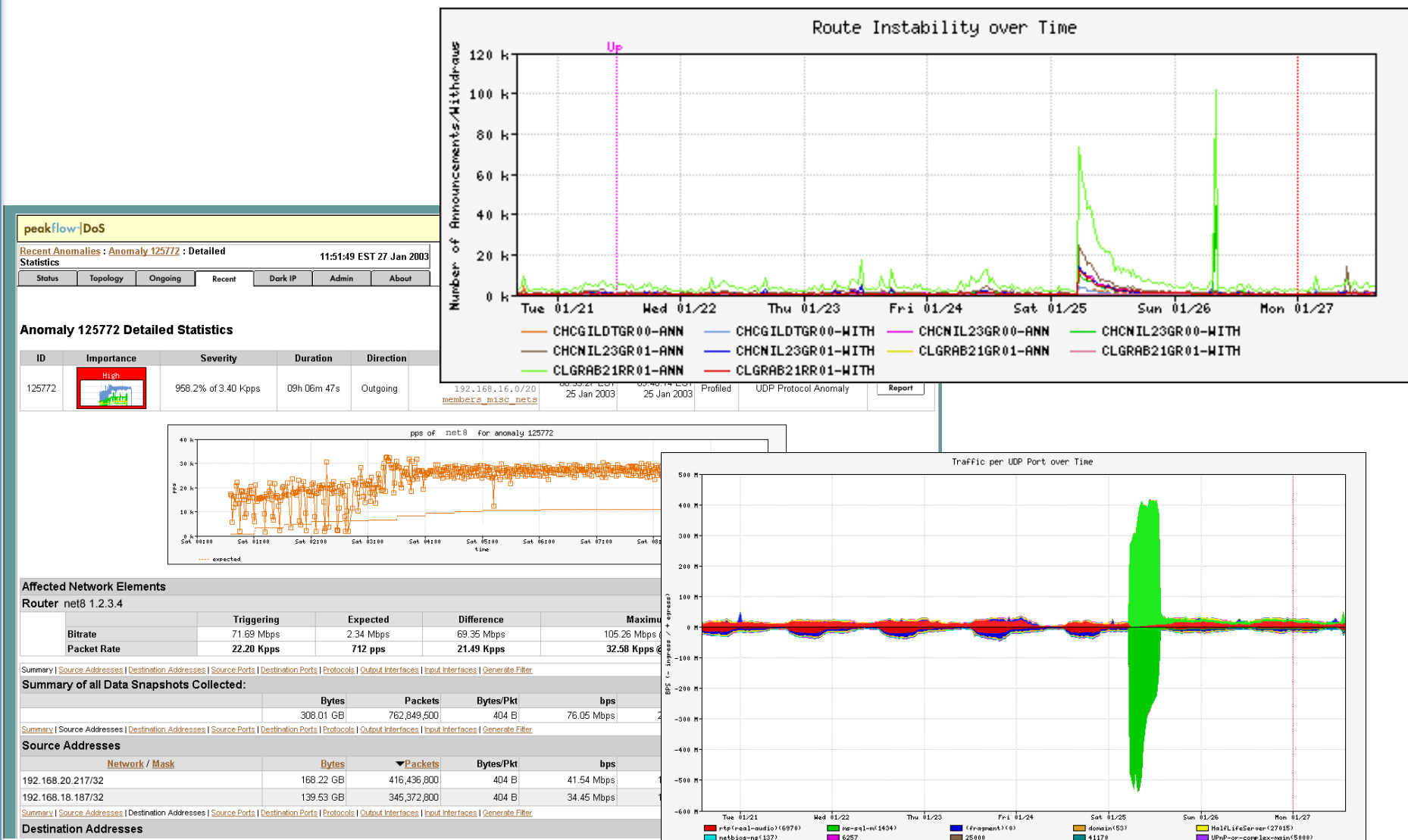


# Flows and Applications

# Uses for NetFlow

- Problem identification / solving
  - Traffic classification
  - DoS Traceback (some slides by Danny McPherson)
- Traffic Analysis and Engineering
  - Inter-AS traffic analysis
  - Reporting on application proxies
- Accounting (or billing)
  - Cross verification from other sources
  - Can cross-check with SNMP data

# 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...\*

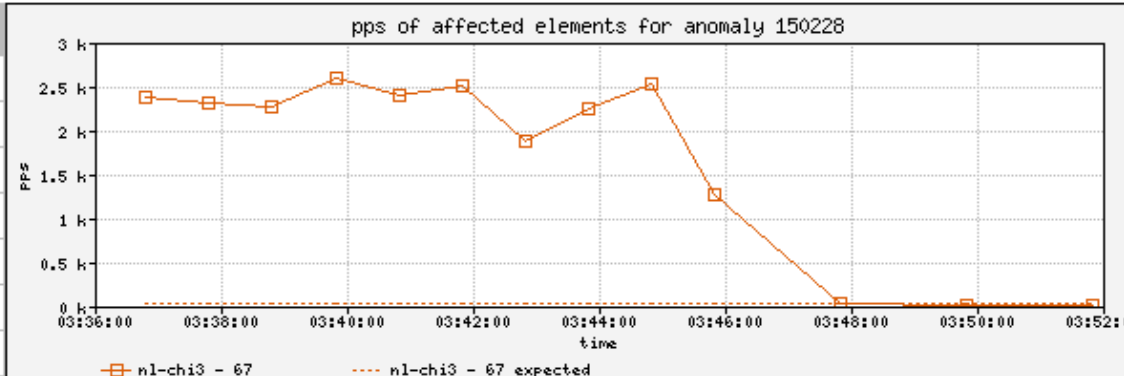
Anomaly 150228

Get Report: [PDF](#) [XML](#)

ID	Importance	Duration	Start Time	Direction	Type	Resource
150228	<b>High</b> 130.0% of 2 Kpps	17 mins	03:34, Aug 16	Incoming	Bandwidth (Profiled)	Microsoft 207.46.0.0/16 <a href="http://windowsupdate.com">windowsupdate.com</a>

## Traffic Characterization

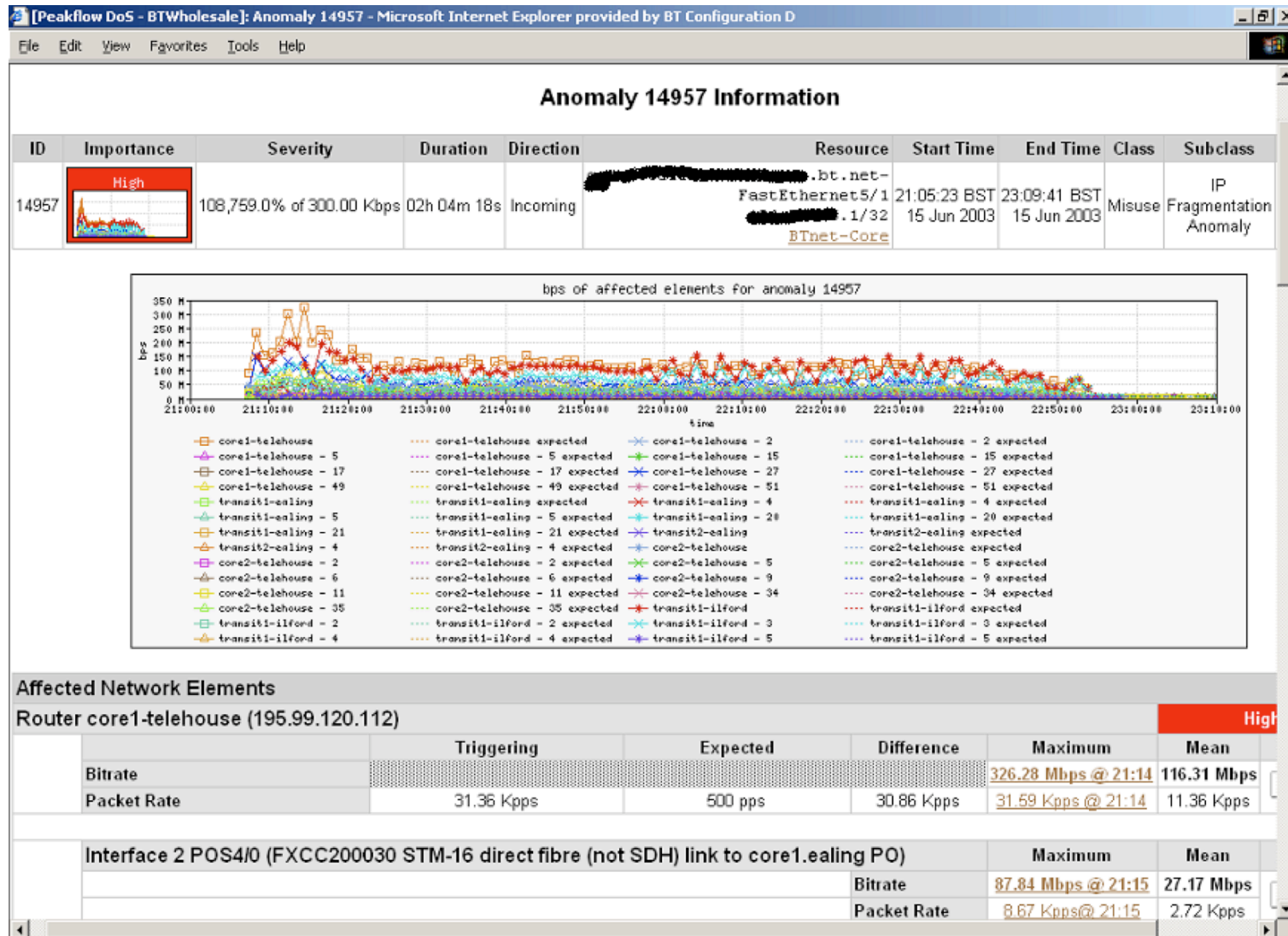
Sources	204.38.130.0/24
	204.38.130.192/26
	1024 - 1791
Destination	207.46.248.234/32
	80 (http)
Protocols	tcp (6)
TCP Flags	S (0x02)



Affected Network Elements		Expected	Observed bps		Observed pps	
	Importance	pps	Max	Mean	Max	Mean
Router nl-chi3 198.110.131.125	<b>High</b>					
Interface 67 at-1/1/0.14 <i>pvc to WMU</i>		26	832 K	563.1 K	2.6 K	1.7 K
						<a href="#">Details</a>

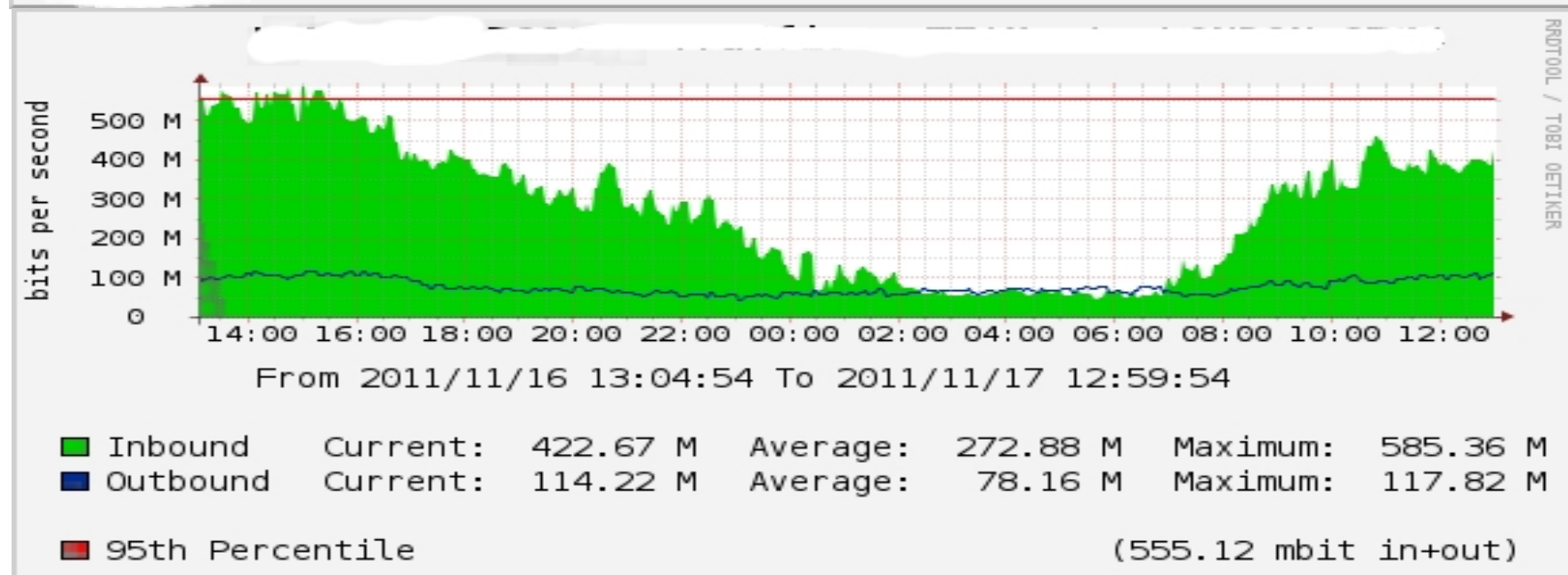
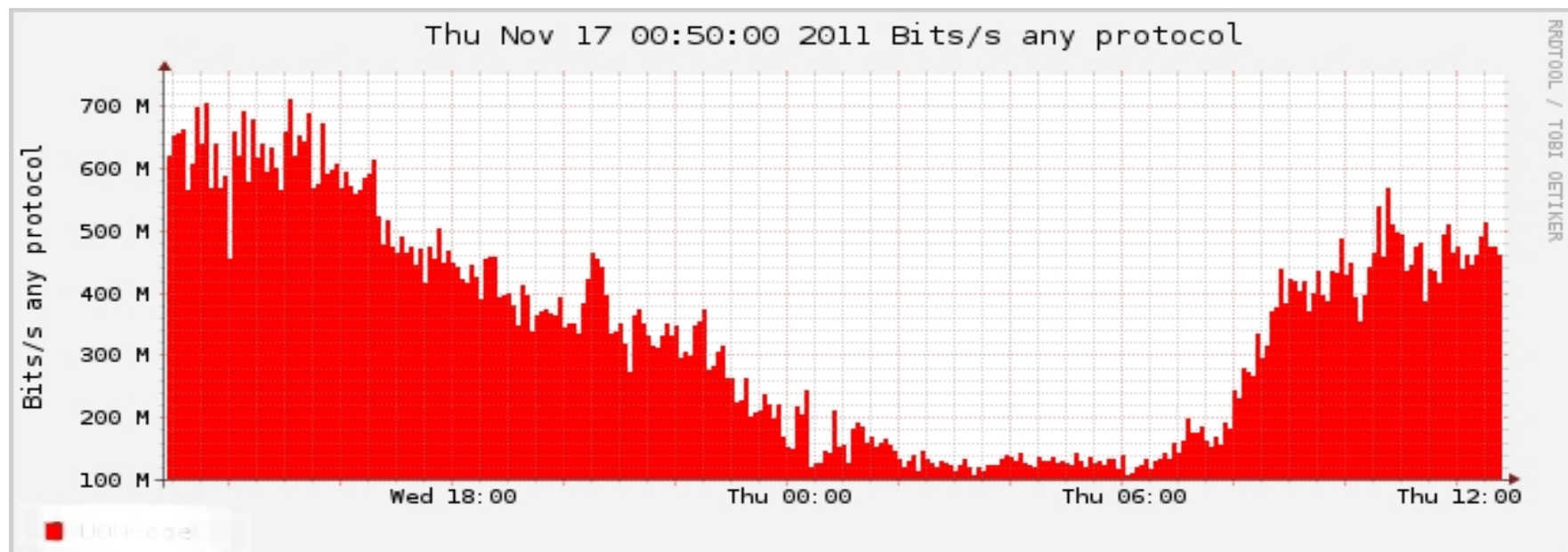
## Anomaly Comments

# Commercial Detection: A Large Scale DOS Attack



# Accounting

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





# References

- flow-tools:  
<http://www.splintered.net/sw/flow-tools>
- Wikipedia:  
<http://en.wikipedia.org/wiki/Netflow>
- 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](mailto:flow-tools@splintered.net)
- Cisco Centric Open Source Community  
<http://cosi-nms.sourceforge.net/related.html>
- Cisco NetFlow Collector User Guide  
[http://www.cisco.com/en/US/docs/net\\_mgmt/netflow\\_collection\\_engine/6.0/tier\\_one/user/guide/user.html](http://www.cisco.com/en/US/docs/net_mgmt/netflow_collection_engine/6.0/tier_one/user/guide/user.html)