Network Monitoring and Management

NetFlow Overview

Agenda

Netflow

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

Flow-tools

- Architectural issues
- Software, tools etc

Lab

Network Flows

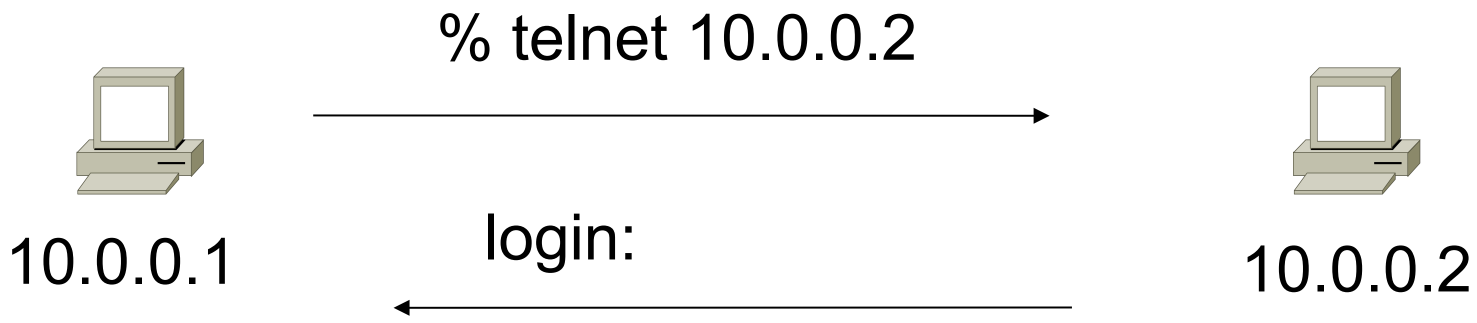
- Packets or frames that have a common attribute
- Creation and expiration policy – what conditions start and stop a flow.
- Counters – packets, bytes, time.
- Routing information – AS, network mask, interfaces.

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

Unidirectional Flow with Source/ Destination IP Key



% telnet 10.0.0.2

login:

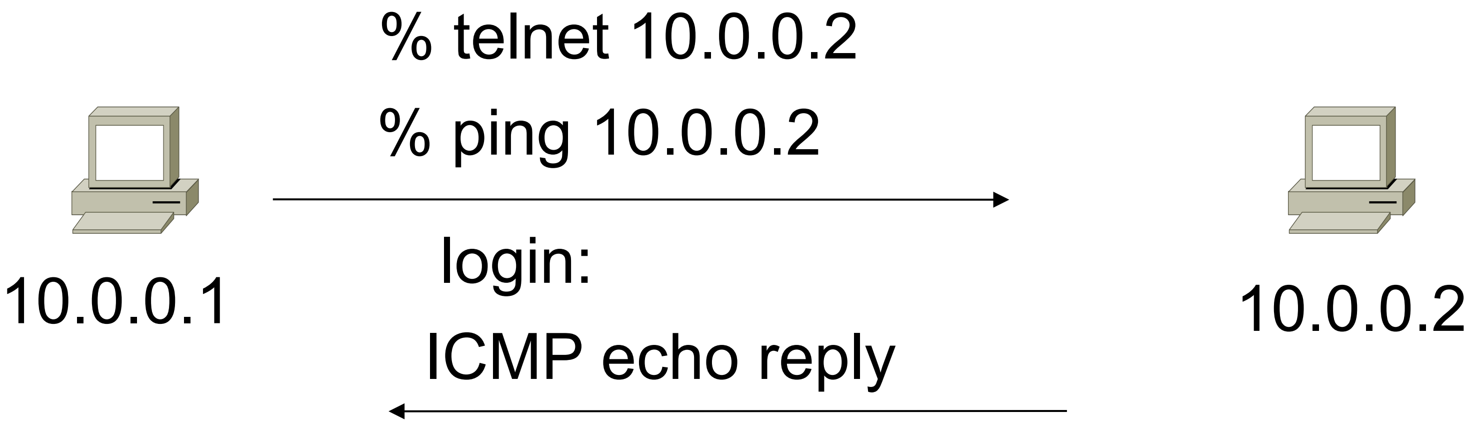
10.0.0.1

10.0.0.2

Active Flows

Flow	Source IP	Destination IP
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

Unidirectional Flow with Source/ Destination IP Key



% telnet 10.0.0.2

% ping 10.0.0.2

10.0.0.1

login:

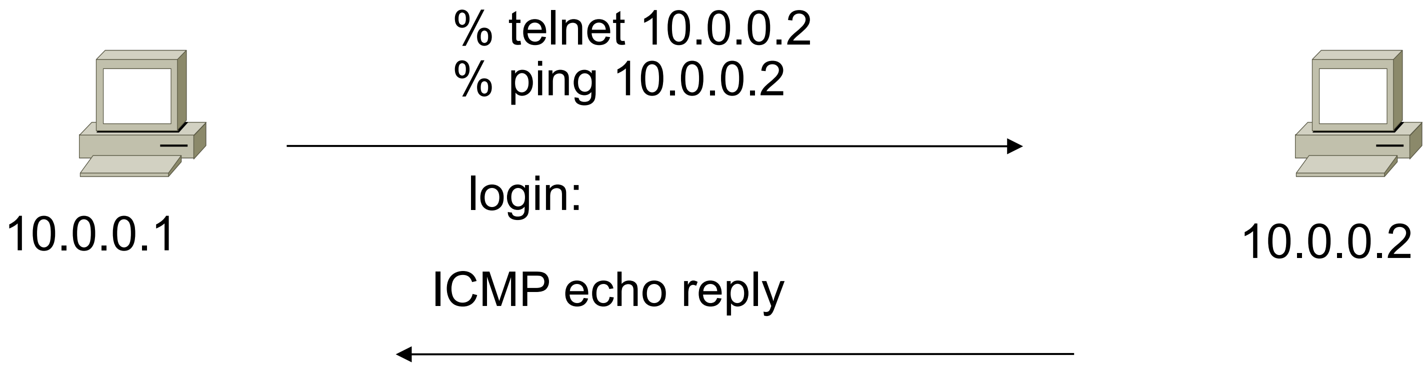
ICMP echo reply

10.0.0.2

Active Flows

Flow	Source IP	Destination IP
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

Unidirectional Flow with IP, Port,Protocol Key



% telnet 10.0.0.2
% ping 10.0.0.2

login:

ICMP echo reply

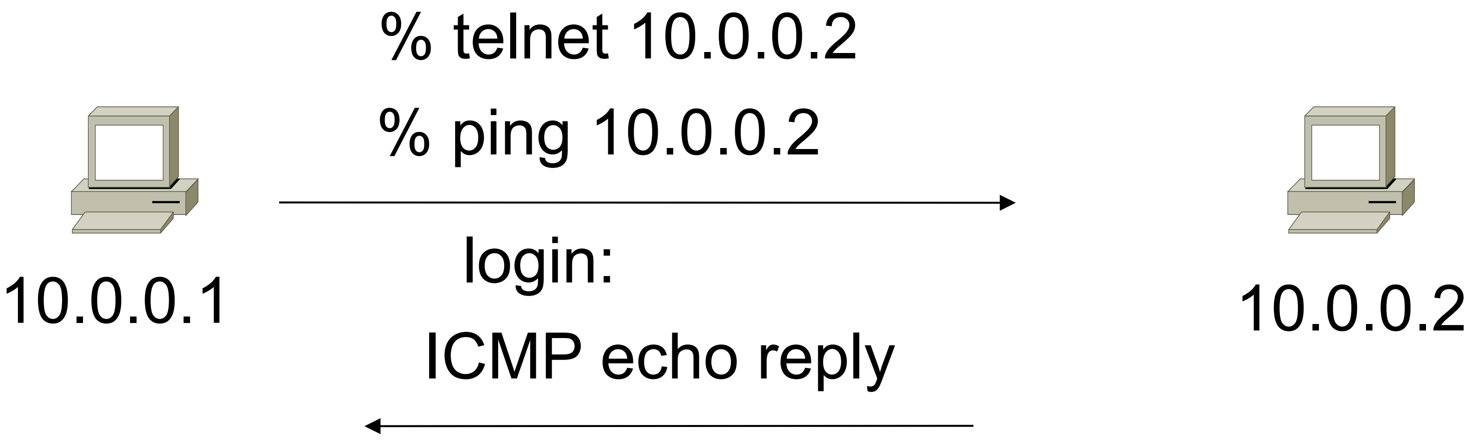
10.0.0.1

10.0.0.2

Active Flows

Flow	Source IP	Destination IP	prot	srcPort	dstPort
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.2	10.0.0.1	TCP	23	32000
3	10.0.0.1	10.0.0.2	ICMP	0	0
4	10.0.0.2	10.0.0.1	ICMP	0	0

Bidirectional Flow with IP, Port,Protocol Key



% telnet 10.0.0.2

% ping 10.0.0.2

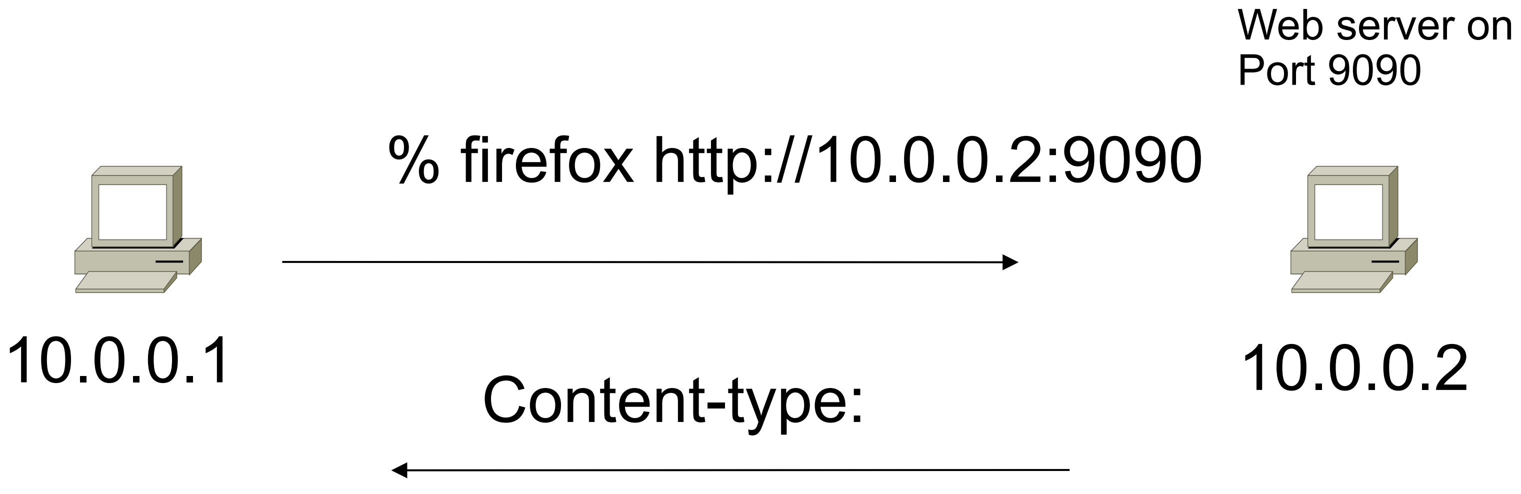
login:

ICMP echo reply

Active Flows

Flow	Source IP	Destination IP	prot	srcPort	dstPort
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.1	10.0.0.2	ICMP	0	0

Application Flow



Web server on
Port 9090

% firefox http://10.0.0.2:9090

10.0.0.1

10.0.0.2

Content-type:

Active Flows

Flow	Source IP	Destination IP	Application
1	10.0.0.1	10.0.0.2	HTTP

Aggregated Flow

Main Active flow table

Flow	Source IP	Destination IP	prot	srcPort	dstPort
1	10.0.0.1	10.0.0.2	TCP	32000	23
2	10.0.0.2	10.0.0.1	TCP	23	32000
3	10.0.0.1	10.0.0.2	ICMP	0	0
4	10.0.0.2	10.0.0.1	ICMP	0	0

Source/Destination IP Aggregate

Flow	Source IP	Destination IP
1	10.0.0.1	10.0.0.2
2	10.0.0.2	10.0.0.1

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

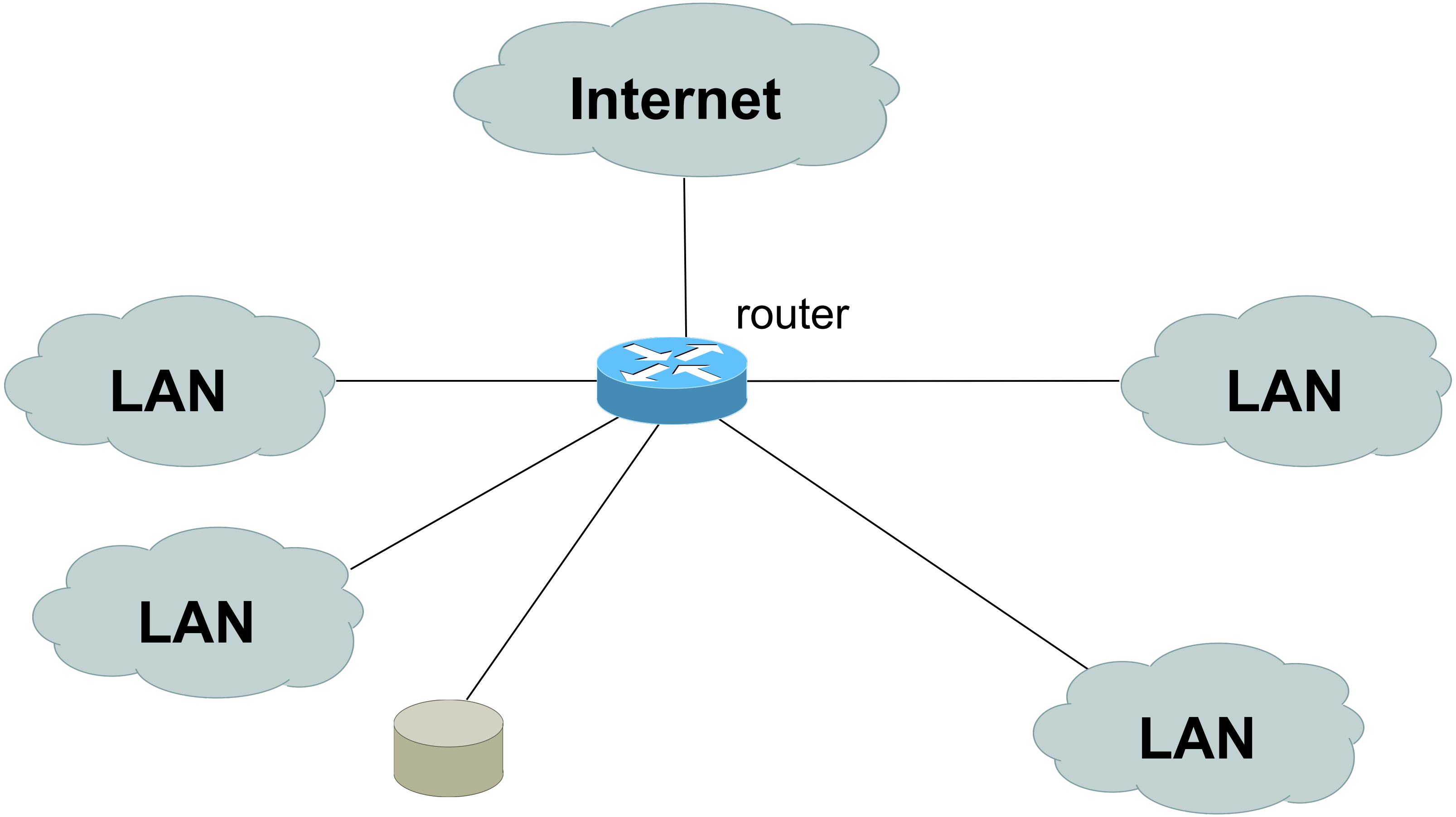
Router or other existing network device

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

Passive monitor

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

Router Collection

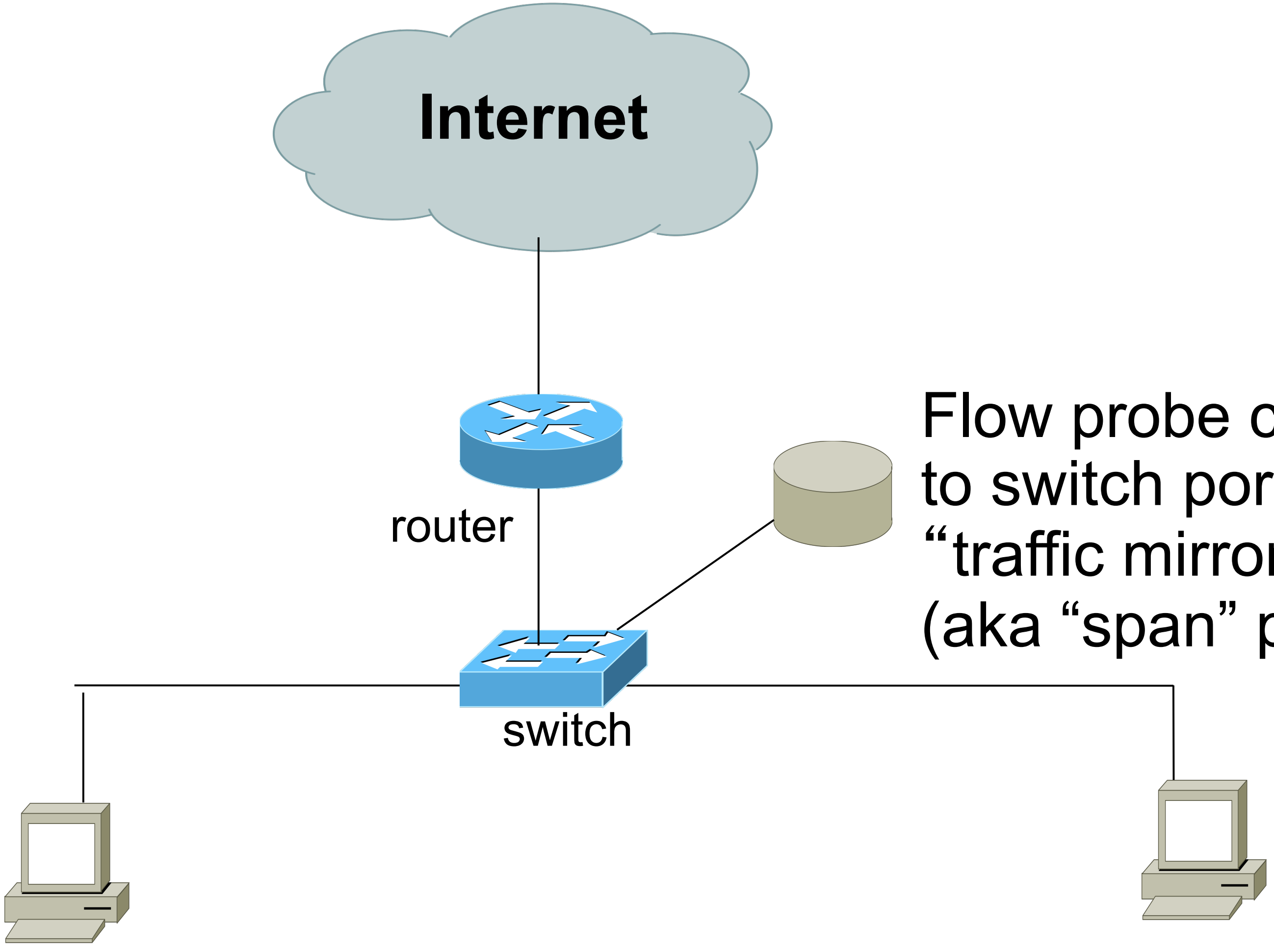


Flow collector
stores exported flows from **router**.

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

Passive Monitor Collection



Flow probe connected to switch port in "traffic mirror" mode (aka "span" port)

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

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

- Major versions: 1, 5 and 9
- 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.

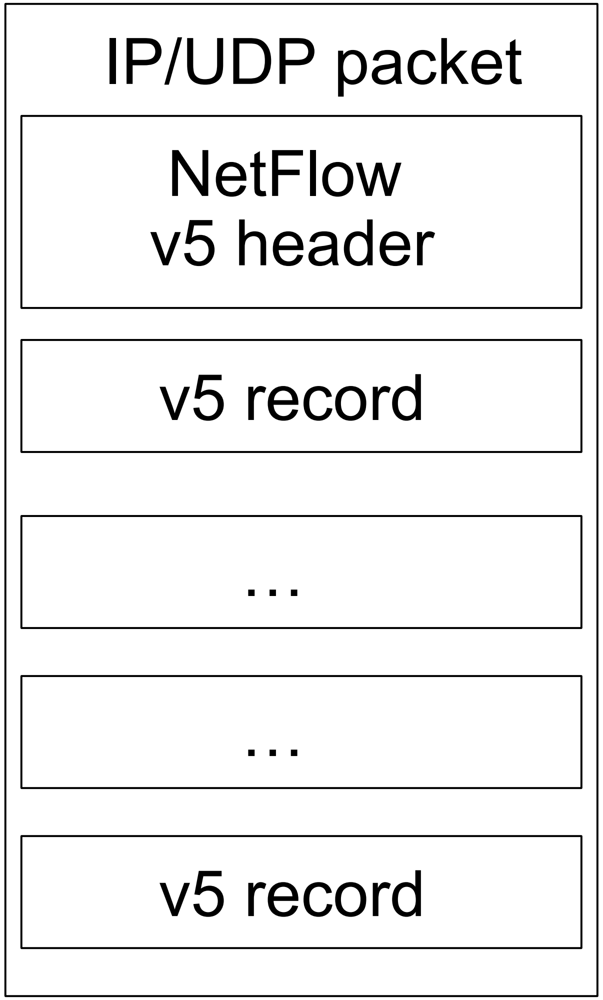
NetFlow Version 1

- 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 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 v5 Packet Example



IP/UDP packet

NetFlow
v5 header

v5 record

…

…

v5 record

NetFlow v9

- IPv6 support
- Additional fields like MPLS labels
- Template support – the NetFlow device exporting the flows can tell the receiver what the format is
- Builds on earlier versions

Enabling NetFlow on IOS

- Configured on each input interface
- Define the version (v5 or v9)
- 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 Command Summary

- Enable flow on each interface:

```
ip flow ingress
ip flow egress
```

- View flow statistics from within IOS
  - `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>
```

Cisco IOS Configuration example

```
interface FastEthernet0/0
 description Access to backbone
 ip address 169.223.132.10 255.255.255.0
 ip flow egress
 ip flow ingress
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description Access to local net
 ip address 169.223.142.1 255.255.255.224
 duplex auto
 speed auto


ip flow-export version 5
ip flow-export destination 169.223.142.3 2002
ip flow-top-talkers
  top 10
  sort-by bytes
```

Cisco IOS Configuration

```
bb-gw#sh ip cache flow
IP packet size distribution (1765988 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .538 .113 .049 .027 .006 .002 .006 .002 .001 .001 .001 .017 .002 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .002 .018 .204 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  105 active, 3991 inactive, 127794 added
  2151823 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  105 active, 919 inactive, 127726 added, 127726 added to flow
  0 alloc failures, 0 force free
  1 chunk, 8 chunks added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          62      0.0        60    50      0.0      15.7      14.3
TCP-FTP              1      0.0         3    60      0.0       8.9      15.2
TCP-WWW          54359      0.1        14   658      2.3       5.3       5.1
TCP-SMTP            20      0.0       103    47      0.0       6.3      13.5
...
```

Cisco IOS Configuration

```
TCP-X              1991      0.0        32    40      0.1       0.5      14.3
TCP-other          8069      0.0        61   214      1.5       7.8       8.9
UDP-DNS           24371      0.0         1    69      0.0       0.1      15.4
UDP-NTP            7208      0.0         1    74      0.0       0.0      15.4
UDP-Frag             14      0.0         1   508      0.0       1.2      15.4
UDP-other         27261      0.0        11   105      0.9       0.4      15.4
ICMP               4457      0.0        17    83      0.2      16.9      15.4
IP-other              1      0.0         1    50      0.0       0.0      15.6
Total:           128017      0.3        13   373      5.3       3.5      10.6

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         210.118.80.41   Fa0/1         169.223.142.112 11 0627 059A     1
Fa0/1         169.223.142.3   Fa0/0*        169.223.35.48   06 0050 C166     1
Fa0/0         169.223.35.175  Local         169.223.142.1   06 EFFD 0016   145
Fa0/0         169.223.35.175  Local         169.223.142.1   06 EFFC 0017     1
Fa0/0         169.223.35.175  Fa0/1         169.223.142.3   06 EE61 0016    79
Fa0/1         169.223.142.102 Fa0/0*        216.34.181.71   06 E058 0050     6
Fa0/1         169.223.142.70  Fa0/0*        66.220.146.18   06 CBD3 0050     6
Fa0/0         208.81.191.110  Fa0/1         169.223.142.70  06 0050 DABD    13
…
```

IOS flow commands

```
Rtr# configure terminal
Rtr(config)# ip flow-top-talkers
Rtr(config-flow)# top 10
Rtr(config-flow)# sort-by bytes
```

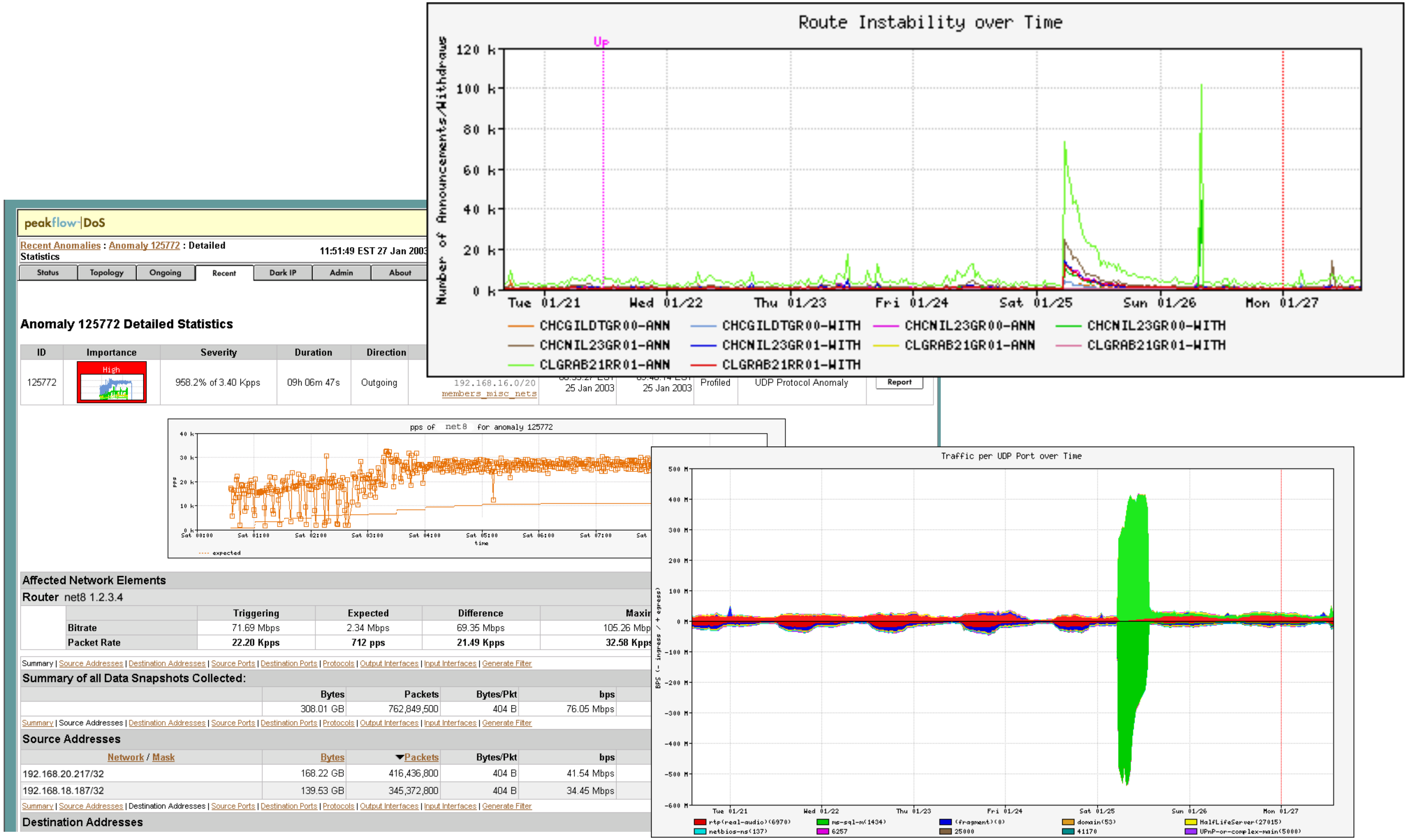
```
Rtr# sh ip flow top-talkers

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.
```

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*



peakflow|DoS

Recent Anomalies : Anomaly 125772 : Detailed Statistics — 11:51:49 EST 27 Jan 2003

Status | Topology | Ongoing | Recent | Dark IP | Admin | About

Anomaly 125772 Detailed Statistics

ID	Importance	Severity	Duration	Direction						
125772	High	958.2% of 3.40 Kpps	09h 06m 47s	Outgoing	192.168.16.0/20 members_misc_nets	25 Jan 2003	25 Jan 2003	Profiled	UDP Protocol Anomaly	Report

Affected Network Elements

Router net8 1.2.3.4

	Triggering	Expected	Difference	Maxi
Bitrate	71.69 Mbps	2.34 Mbps	69.35 Mbps	105.26 Mbp
Packet Rate	22.20 Kpps	712 pps	21.49 Kpps	32.58 Kpps

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

Summary of all Data Snapshots Collected:

	Bytes	Packets	Bytes/Pkt	bps
	308.01 GB	762,849,500	404 B	76.05 Mbps

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

Source Addresses

Network / Mask	Bytes	Packets	Bytes/Pkt	bps
192.168.20.217/32	168.22 GB	416,436,800	404 B	41.54 Mbps
192.168.18.187/32	139.53 GB	345,372,800	404 B	34.45 Mbps

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

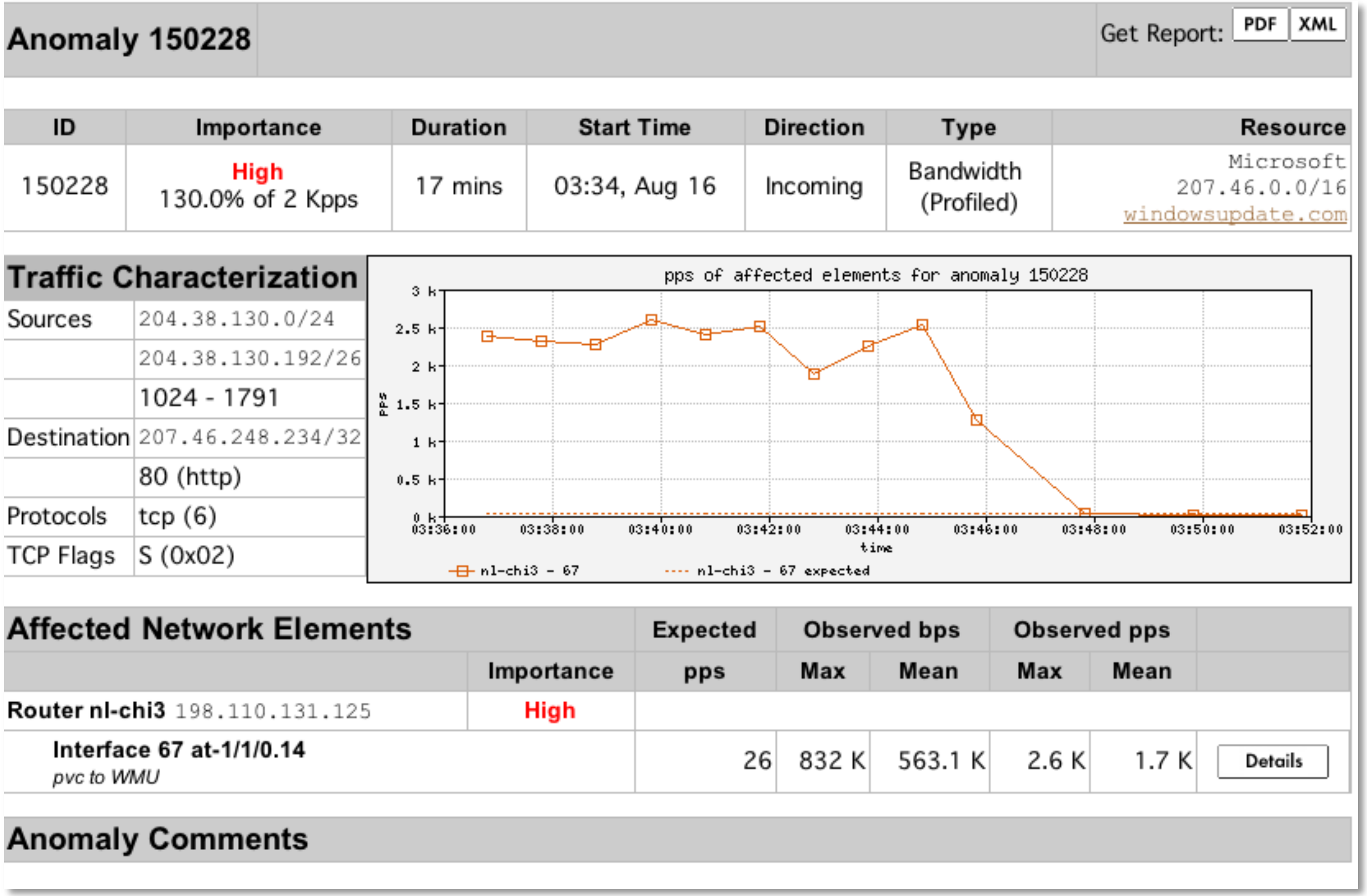
Destination Addresses

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	High 130.0% of 2 Kpps	17 mins	03:34, Aug 16	Incoming	Bandwidth (Profiled)	Microsoft 207.46.0.0/16 windowsupdate.com

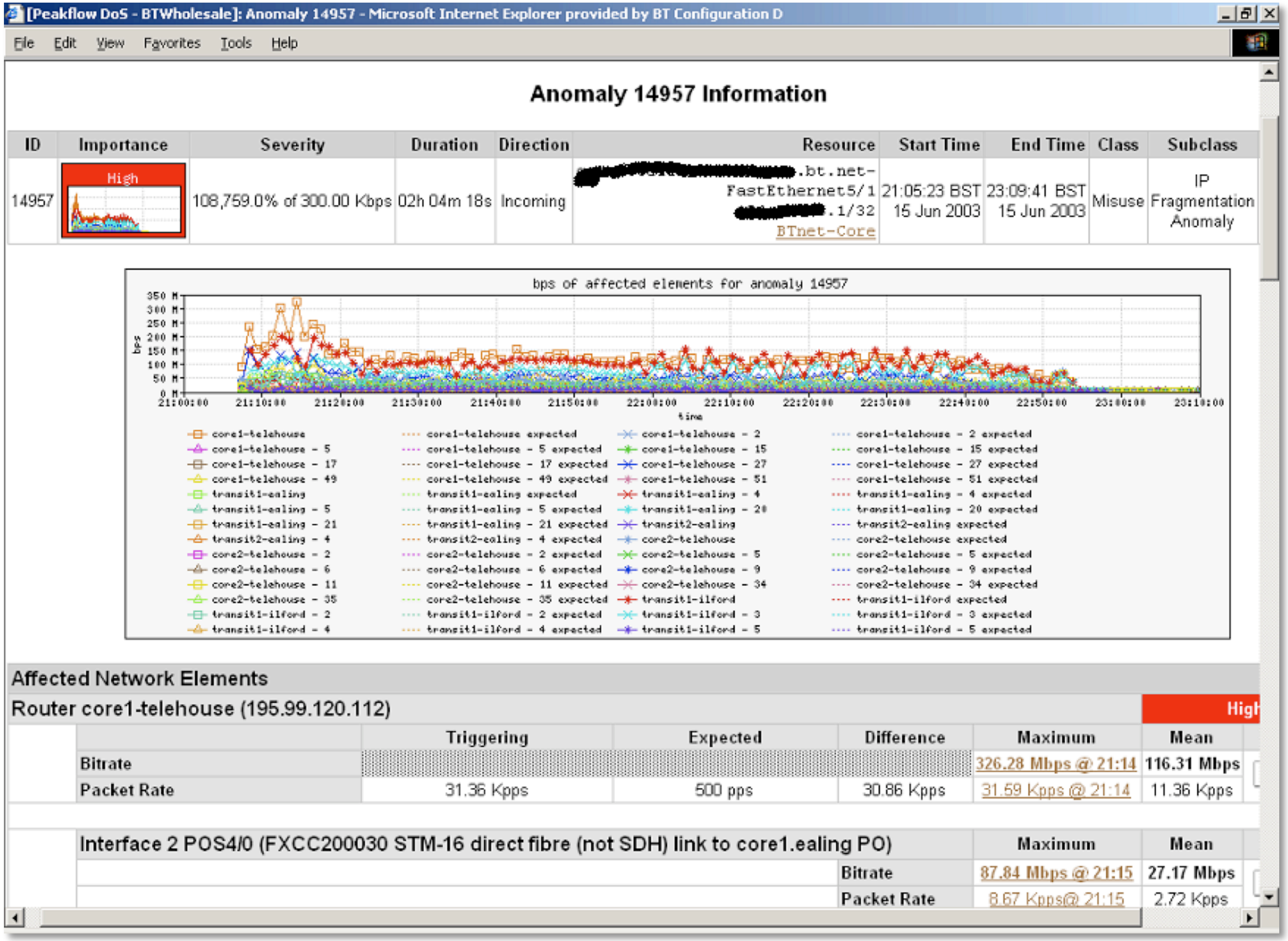
Traffic Characterization

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	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


[Peakflow DoS - BTWholesale]: Anomaly 14957 - Microsoft Internet Explorer provided by BT Configuration D
File
Edit
View
Favorites
Tools
Help

Anomaly 14957 Information

ID	Importance	Severity	Duration	Direction	Resource	Start Time	End Time	Class	Subclass
14957	High	108,759.0% of 300.00 Kbps	02h 04m 18s	Incoming	[redacted].bt.net- FastEthernet5/1 [redacted].1/32 BTnet-Core	21:05:23 BST 15 Jun 2003	23:09:41 BST 15 Jun 2003	Misuse	IP Fragmentation Anomaly

Affected Network Elements

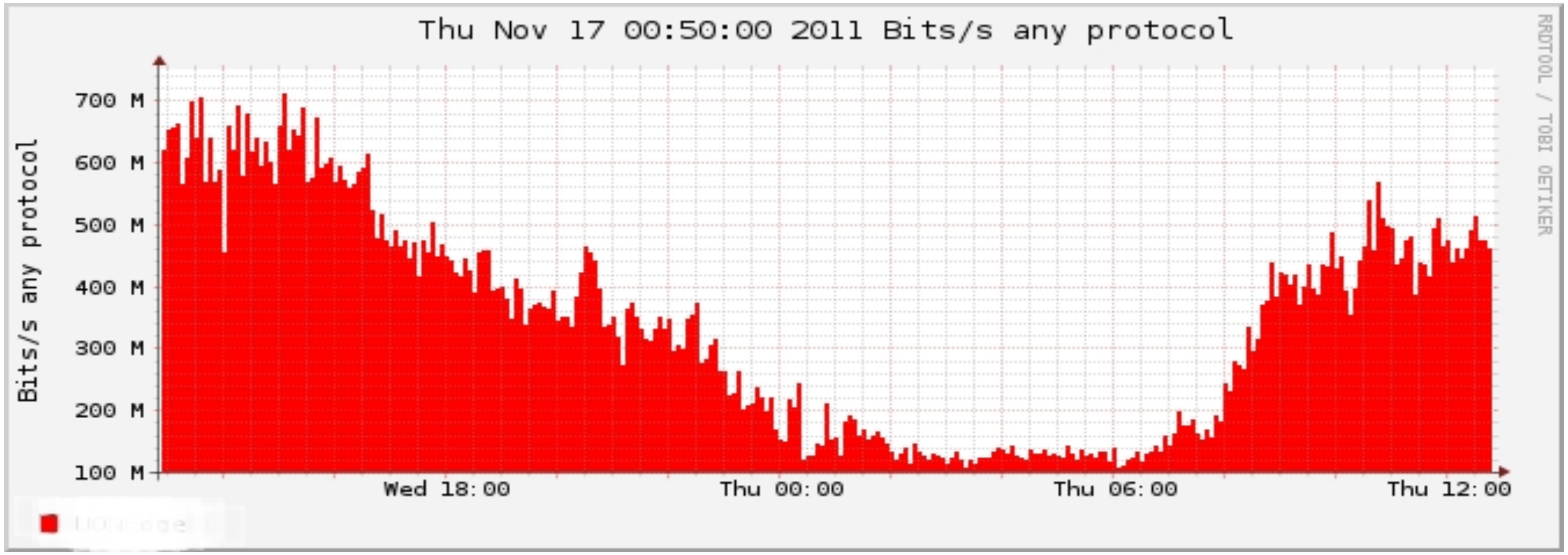
Router core1-telehouse (195.99.120.112) High

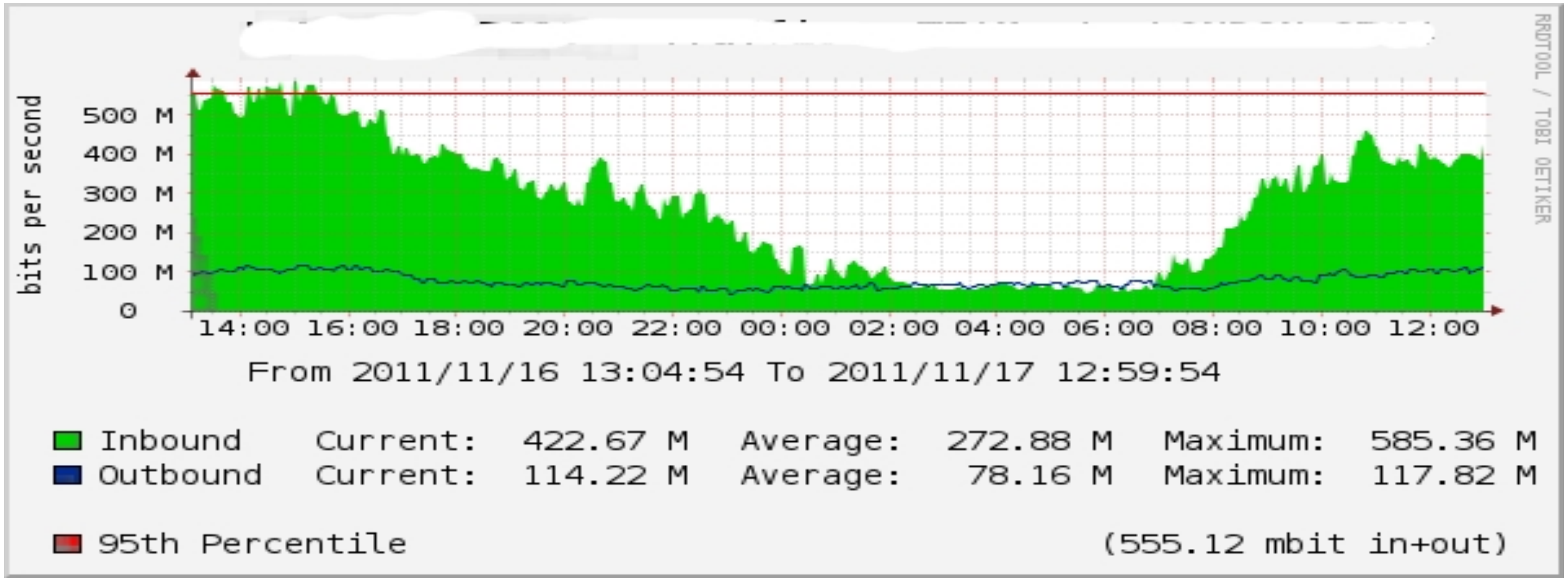
		Triggering	Expected	Difference	Maximum	Mean
	Bitrate				326.28 Mbps @ 21:14	116.31 Mbps
	Packet Rate	31.36 Kpps	500 pps	30.86 Kpps	31.59 Kpps @ 21:14	11.36 Kpps

Interface 2 POS4/0 (FXCC200030 STM-16 direct fibre (not SDH) link to core1.ealing PO)	Maximum	Mean
Bitrate	87.84 Mbps @ 21:15	27.17 Mbps
Packet Rate	8.67 Kpps@ 21:15	2.72 Kpps

Accounting

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


Thu Nov 17 00:50:00 2011 Bits/s any protocol
Bits/s any protocol
700 M
600 M
500 M
400 M
300 M
200 M
100 M
Wed 18:00
Thu 00:00
Thu 06:00
Thu 12:00
RRDTOOL / TOBI OETIKER
🟥 [redacted]


[redacted]
bits per second
500 M
400 M
300 M
200 M
100 M
0
14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00
RRDTOOL / TOBI OETIKER
From 2011/11/16 13:04:54 To 2011/11/17 12:59:54
🟩 Inbound Current: 422.67 M Average: 272.88 M Maximum: 585.36 M
🟦 Outbound Current: 114.22 M Average: 78.16 M Maximum: 117.82 M
🟥 95th Percentile (555.12 mbit in+out)

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
- 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