



# Beyond NetFlow...

The Need for Centralized Network Monitoring

## "Go With the Flow"

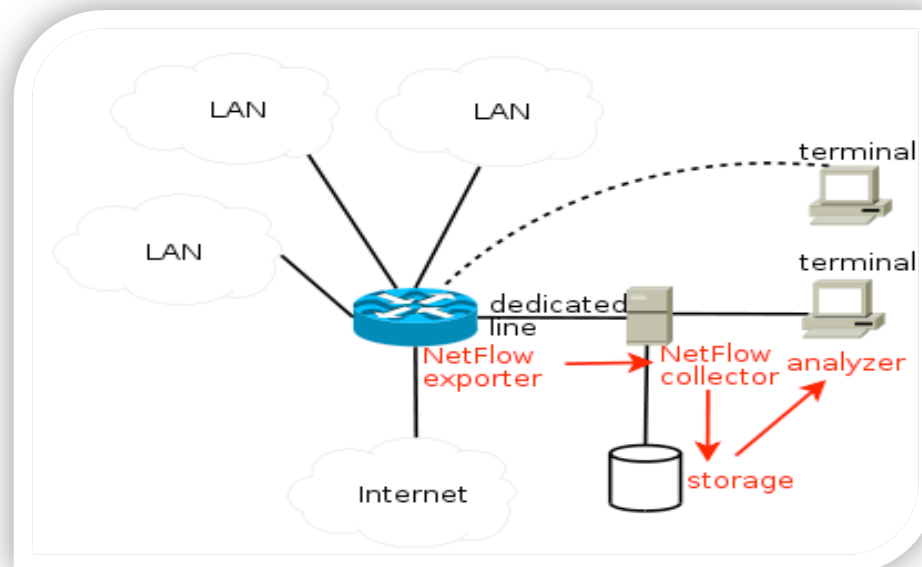
- **Flows, or Flow Records, have become the default element used in centralized network monitoring**
- **A “Flow” is IP data with the following 7 identical characteristics:**
  - Source IP address
  - Destination IP address
  - Source port
  - Destination port
  - Layer 3 protocol type
  - TOS byte
  - Input logical interface
- **By implication, a Flow is unidirectional**

# Flows vs. Flow Records

- **Flows are a defined element**
- **Flow Records are analytical results that vary by overall standard, vendor and configuration**
- **The most common standards for flow records include:**
  - NetFlow
  - IPFIX
  - sFlow
  - JFlow
  - OmniFlow

# Basic Flow Analysis

- Packets enter the switch or router
- Packets sampled and flows determined
- Flow records compiled and exported to flow collector
- Flow records stored and subsequently analyzed by flow analysis software



Source: Wikipedia

# Not All Flows Are Created Equal

Netflow	IPFIX	sFlow	Jflow	OmniFlow
<ul style="list-style-type: none"> <li>• Developed by Cisco</li> <li>• Proprietary</li> <li>• Transit traffic &amp; terminated traffic</li> <li>• Detailed info for each flow</li> <li>• NO payloads</li> <li>• Sampled NetFlow – not 100% accurate</li> </ul>	<ul style="list-style-type: none"> <li>• Internet Protocol Flow Information eXchange</li> <li>• Emerging IETF standard</li> <li>• Based on NetFlow</li> <li>• Detailed info for each flow</li> <li>• NO payloads</li> </ul>	<ul style="list-style-type: none"> <li>• RFC 3176</li> <li>• Statistical sampling</li> <li>• Time-based sampling of interface counters</li> <li>• Higher speed networks</li> <li>• sFlow agents</li> <li>• NO payloads</li> <li>• Sampled – not 100% accurate</li> </ul>	<ul style="list-style-type: none"> <li>• Developed by Juniper</li> <li>• Proprietary</li> <li>• Similar to NetFlow</li> <li>• Detailed info for each flow</li> <li>• NO payloads</li> <li>• Sampled per global rate – not 100% accurate</li> </ul>	<ul style="list-style-type: none"> <li>• Developed by WildPackets</li> <li>• Proprietary</li> <li>• Analysis of every packet AND payload</li> <li>• Unrivaled info for each flow</li> <li>• Layer 3 - 7</li> <li>• 100% accurate</li> <li>• Monitor AND troubleshoot</li> </ul>

# OmniFlow Data

OmniEngines Start Page protomatter.pkt

Flows analyzed: 2,317 Flows recycled: 0  
 Events detected: 78 Packets dropped: 0

Name	Flows	Events	Apdex	Packets	Bytes	Duration	Best Response Time	Avg Response Time	Worst Response Time
Web	382	16	0.92	19852	13639742	0:03:30...			
Mail	277	39	0.78	10059	2362677	0:03:29...			
FTP	5	0		59	4448	0:01:07...			
IM	71	0		623	70113	0:03:29...			
Voice & Video	1	0		2150	1830872	0:03:28...			
82.149.226.226	1	0		2150	1830872	0:03:28...			
10.4.3.129	1	0		2150	1830872	0:03:28...			
1200<->rtsp	0	0		2150	1830872	0:03:28...	0.166746	0.168094	0.171444
IP Fragment	3	0		8	882	0:02:06...			
TELNET	1	0		8	5466	0.214225			
10.4.58.8	1	0		8	5466	0.214225			
10.4.3.220	1	0		8	5466	0.214225			
52112<->telnet	0	0		8	5466	0.214225			
DNS	480	0		9991	1316836	0:03:29...			
BOOTP	2	0		40	15967	0:03:06...			
DHCP	9	0		36	13393	0:03:18...			
NetBIOS	32	1	0.92	1486	392948	0:03:25...			
NB Name Svc	48	0		2625	256289	0:03:28...			
MB DC	6	0		68	15247	0:03:04...			

Client	Server	Response Time	C->S bps	S->C bps
10.4.3.129	82.149.226.226	Best 0.166746	4878.000	78212.000
10.4.3.129	82.149.226.226	Worst 0.171444	910.000	57356.000
		Average 0.168094	1628.000	68779.000
		Turns 4	643	1507

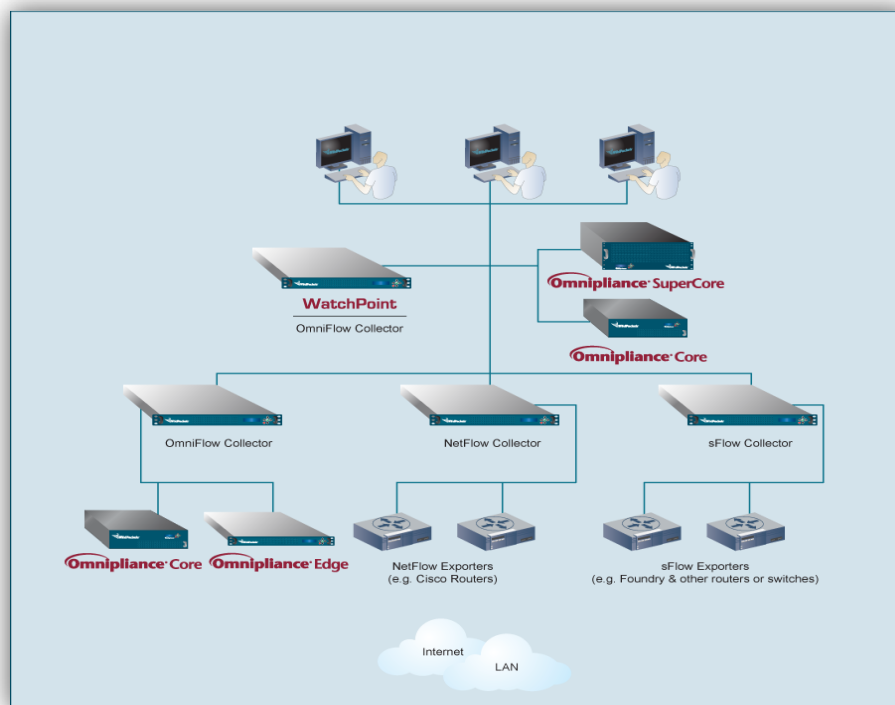
  

Layer	Event	Count

There are no items to show in this view.

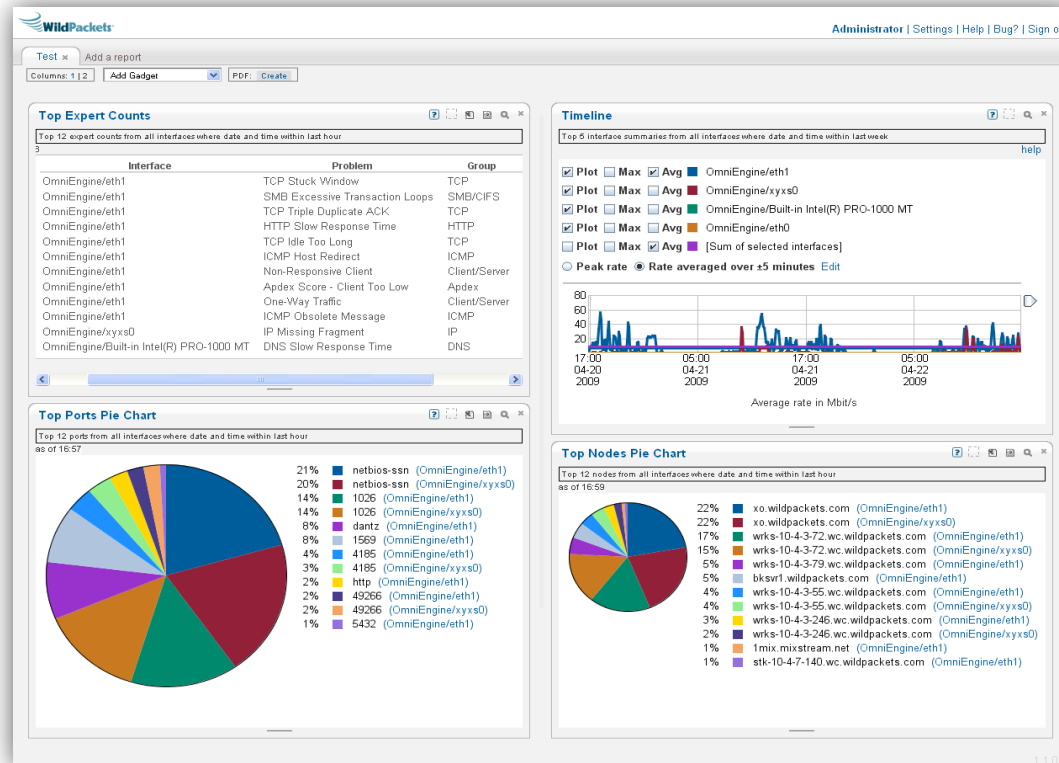
Packets: 137,730 Duration: 0:03:30

# OmniFlow and WatchPoint



- **High-level, aggregated view of all network segments**
  - Monitor per campus, per region, per country
- **Wide range of network data**
  - NetFlow, sFlow, OmniFlow
- **Web-based, customizable network dashboards**
- **Flexible and detailed reports**

# WatchPoint Dashboard



## Summary

- **Flow records are NOT created equal**
- **OmniFlow analyzes packet headers AND payloads**
- **OmniFlow is NOT statistical – 100% accurate**
- **OmniFlow provides analysis for all network layers**
- **WatchPoint aggregates data from multiple OmniFlow streams**
- **When OmniFlow data isn't available, WatchPoint aggregates both NetFlow and sFlow data for complete network visibility**



# Thank You!

WildPackets, Inc.  
1340 Treat Boulevard, Suite 500  
Walnut Creek, CA 94597  
(925) 937-3200

© WildPackets, Inc.

[www.wildpackets.com](http://www.wildpackets.com)