IPV6流量分析探讨

北京大学计算中心

周昌令

北京大学

内容

- 流量分析简介
- IPv6下的新问题和挑战
  - 协议格式变更
  - 用户行为特征变更
  - 安全问题演化
  - 流量导出手段变化
- 设备参考配置
- 流量工具
- 总结

流量分析简介

- 流量分析目标
  - who, what, where, when, and how
  - 流量整形、流量工程、网络规划、异常检测、行为分析、以及Qos保证等
- 数据来源
  - SNMP: mibs
  - Raw Data: Tcpdump
  - 流信息：Netflow/IPFIX

流量分析

- What we needs
  - application performance
  - application-based accounting
  - network security
  - Network behavior, application recognition
- ‘debug ip packet’ in router?
- IP Sniffing in shared LAN (or using switch to do so)
- Port Span in switch (how about port span in router?)
- Circuit Sniffing
- Netflow
- What we prefer in backbone:
  - Embeded
  - Fixed length partial packet export
  - Real-time filtered packet export

Netflow的应用范围

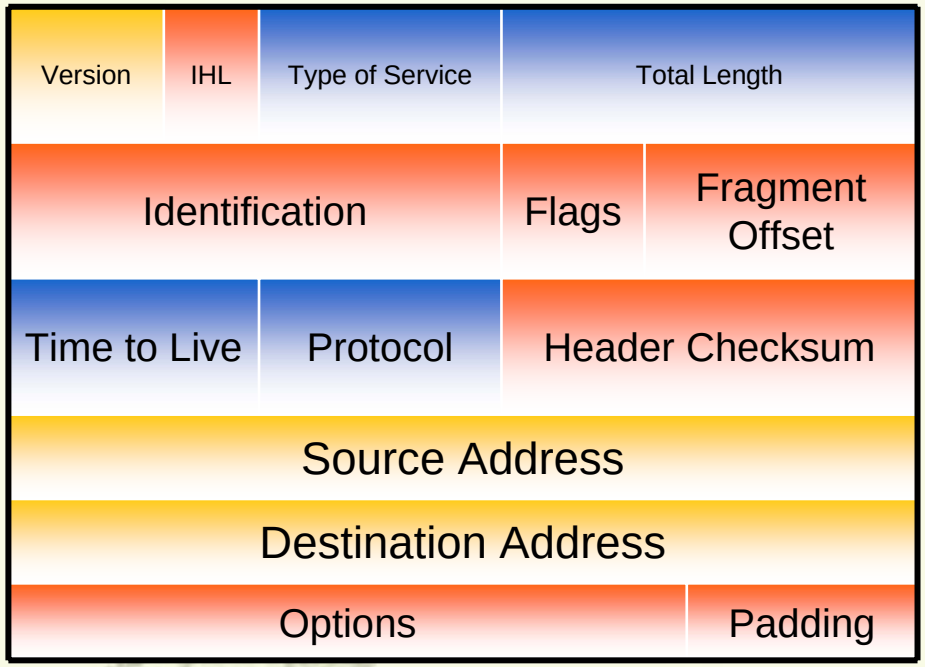
- Network Monitoring
- Network planning
- Security Analysis
- Application Monitoring
- User Monitoring
- Traffic Engineering
- Peering Agreement
- Usage-base Billing
- Destination sensitive billing
- ……

IPv6带来的变化

- 数据报文差别
- 流量模式变化
  - 用户行为
- 安全事件的演进
  - 模式变更
  - 检测方法

IPv6 Header

IPv4 Header 20 bytes



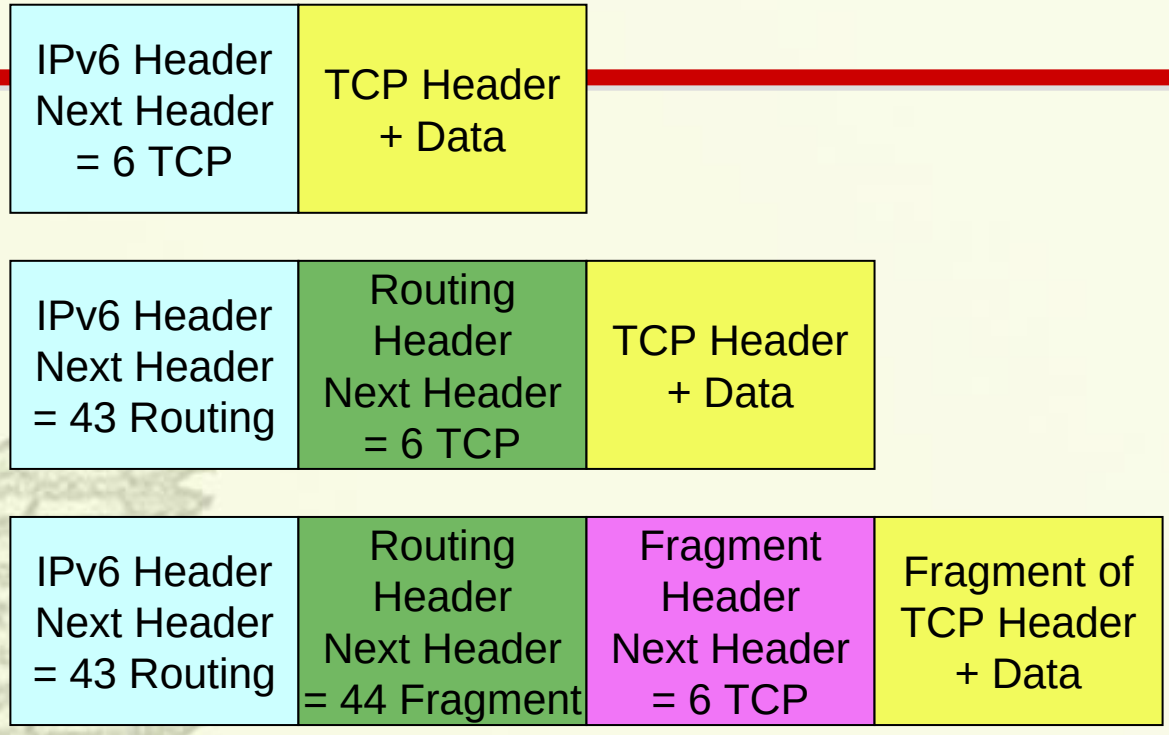
图例

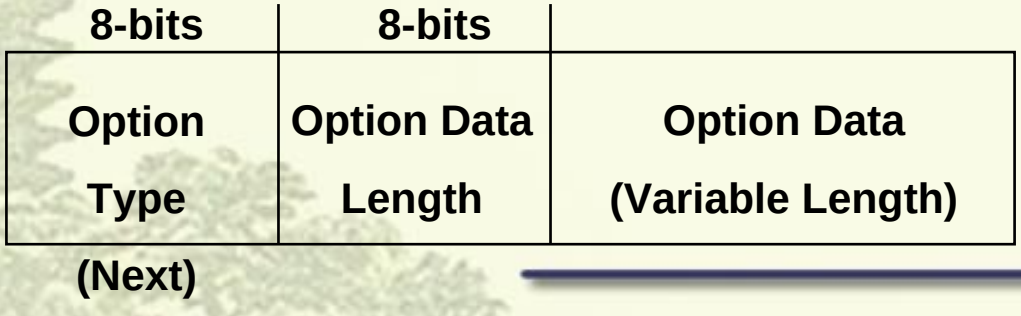
- IPv4 与 IPv6相同的域
- 仅IPv4有的域
- IPv6与IPv4名称不同、功能类似的域
- IPv6新增的域

IPv6 Header, 40 bytes fixed

北京大学

IPv6 Extension Headers





Next Header Field:

0 – Hop-by-Hop Options

60 – Destination Options

(If Routing header is used)

43 – Routing

44 – Fragment

46 – RSVP

51 – AH

50 – ESP

88 – EIGRP

89 – OSPF

6 – TCP

17 – UDP

58 – ICMPv6

135 – Mobility Header

59 – None (no next header)

流量模式(用户行为)变化

- 应用程序的网络行为
  - 流媒体、P2P
- 一个节点多个IPv6地址
  - 不同用途、优先级问题
- 过渡阶段
  - 双栈、隧道、网关…

关注用户行为

- 谁占用了最多的带宽，所占比例？
- 网络的用户数量多少
- 用户使用网络的时间点和长度
- 哪些站点比较热门，站点间有无关联
- 用户使用网络的习惯如何
- 有无明显网络代理行为
- 有无攻击、病毒特征
- 用户体验评估

网络攻击与检测方式变化

- 扫描不再有效？
  - 地址空间扩大
  - 增强的安全特性（IPSec等）
  - 隐藏vs发掘
- LAN攻击
  - 第二层信息

网络攻击

- 总的流量突然上升
- 网络设备负载增加(CPU、Memeory)
- 个别节点或服务突然异常(慢、无法登陆等)
- 大量的ACL冲突记录
- 流数据急速增长，大量到同一节点的单向流
- 由同一节点发出的大量不同目标的流
- 某种类型的流量突然增加，如ICMP
- 突然增加的未知应用类型的流量
- ……

Netflow检测网络攻击

- 命令:

```
Router# sh ip(v6) cache flow | inc xxx.xxx.xxx.xxx

Router# sh mls netflow ip(v6)
```

  - 可确定问题源
  - 及时响应
  - 可配合acl使用
- 分析工具
  - 更全面、高效
  - 历史记录

What Does a DOS Attack Look Like?

Potential DoS Attack on Router
Estimated: 660 pkt/s 0.2112 Mbps

```
Router# show ip cache flow
…
```

SrcIf	SrcIPaddress	SrcP	SrcAS	DstIf	DstIPaddress	DstP	DstAS	Pr	Pkts	B/Pk
29	192.1.6.69	77	aaa	49	194.20.2.2	1308	bbb	6	1	40
29	192.1.6.222	1243	aaa	49	194.20.2.2	1774	bbb	6	1	40
29	192.1.6.108	1076	aaa	49	194.20.2.2	1869	bbb	6	1	40
29	192.1.6.159	903	aaa	49	194.20.2.2	1050	bbb	6	1	40
29	192.1.6.54	730	aaa	49	194.20.2.2	2018	bbb	6	1	40
29	192.1.6.136	559	aaa	49	194.20.2.2	1821	bbb	6	1	40
29	192.1.6.216	383	aaa	49	194.20.2.2	1516	bbb	6	1	40
29	192.1.6.111	45	aaa	49	194.20.2.2	1894	bbb	6	1	40
29	192.1.6.29	1209	aaa	49	194.20.2.2	1600	bbb	6	1	40
…	…	…	…	…	…	…	…	…	…	…

Typical DoS Attacks Have the Same (or Similar) Flow Entries:

- Input Interface (SrcIf)
- Destination IP (DstIf)
- 1 Packet per flow (Pkts)
- Bytes per packet (B/Pk)

一些IPv6的攻击

- 由IPv4演进的攻击
  - 蠕虫、僵尸网络
- IPv6隐信道(covert channels)攻击
  - Covert Channels in IPv6， N.B Lucena, G. Lewandowski etc, Lecture Notes in Computer Science, Volume 3856, 2006, 147-166
  - http://www.securityfocus.com/news/11406
- 来自IPv4的攻击
  - Tunnel，双栈
- 协议发展不完善的地方
  - DAD（类似IPv4的ARP）

IPv6与流信息采集

- IPv4环境常用Netflow v5
  - 扩展性问题
  - 不能处理IPv6数据
- Netflow v9 / IPFIX
  - IETF 推荐的标准
  - 使用模板来适应不同的要求
    - IPv6、MPLS、Multicast
  - 设备支持：cisco, huawei, juniper

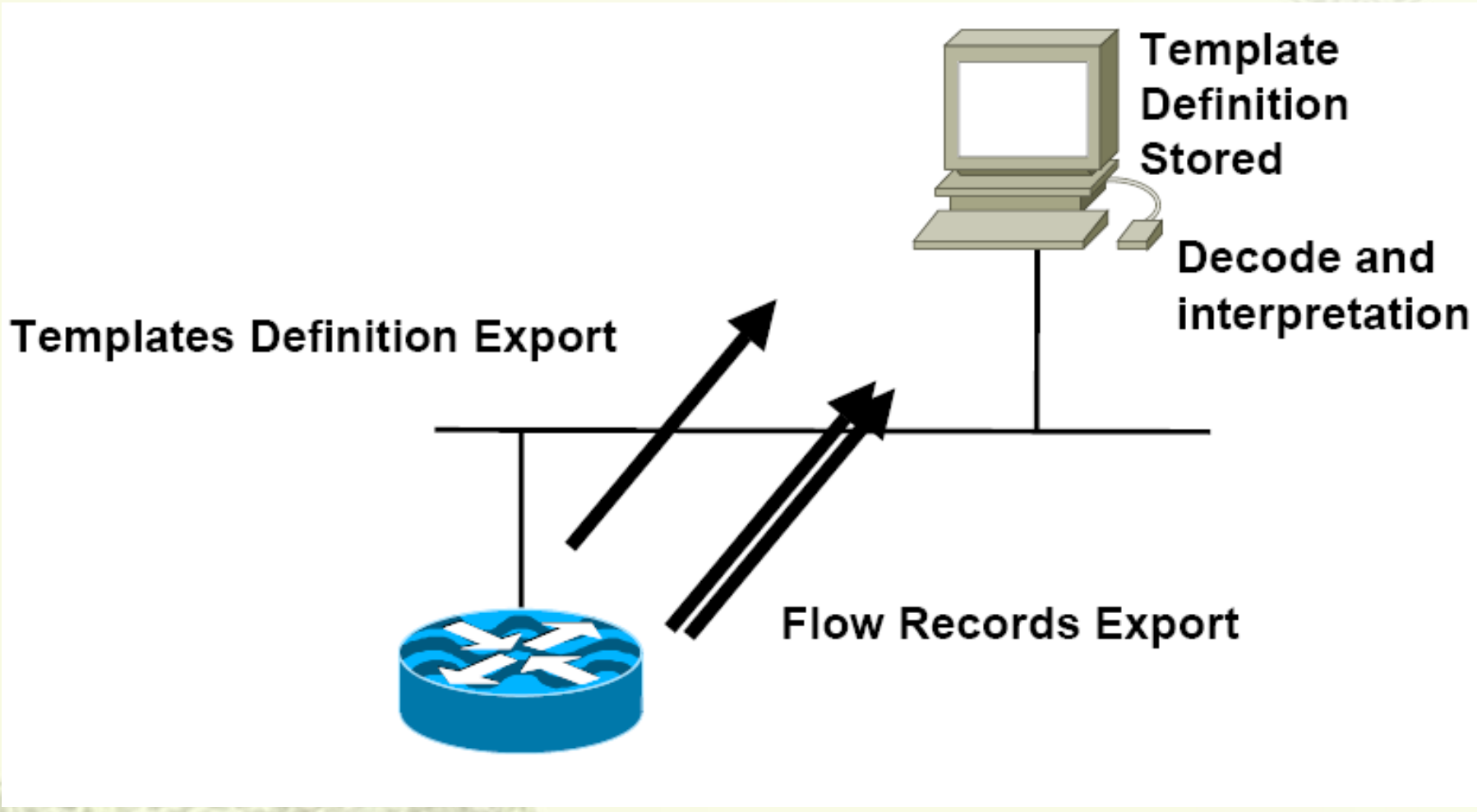
设备支持情况

- Cisco
  - Netflow v9
    - IPv6 packets captured (needs IPv6 CEF)
    - Still uses *IPv4 transport*
    - 12.2(33)SRB of Cisco 7600 began to support IPv6 export
    - May need to update your own Netflow collector
- Huawei
  - Netstream
- Juniper:
  - Jflow

NetFlow Version 9

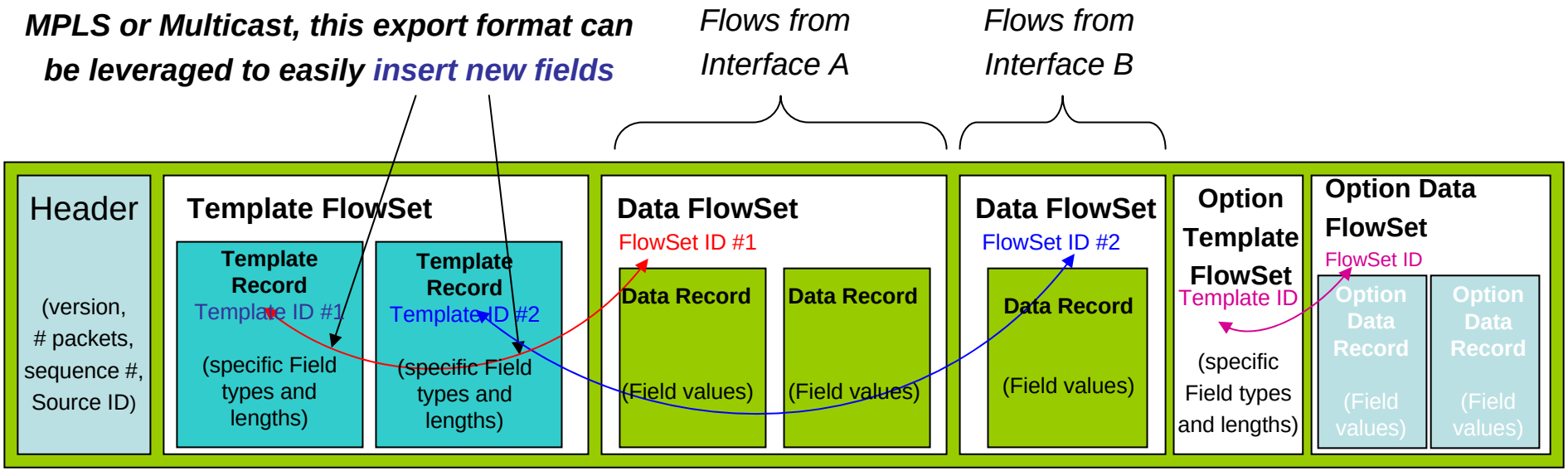
- Version 9 is an export protocol
  - No changes to the metering process
- Version 9 based on templates and separate flow records
  - Templates composed of type and length
  - Flow records composed of template ID and value
  - Sent the template regularly (configurable), because of UDP
- Support: 800, 1700, 1800, 2600, 2800, 3200, 3600, 3700, 6500/7600, 7200, 7300, 7500, cat6000, 7600, 10000, 12000, CRS-1, ASR 1000
- RFC3954 “Cisco Systems® NetFlow Services Export Version 9”
  - NetFlow patent: intellectual property right statement on the IETF website

Netflow Version 9 Scenario

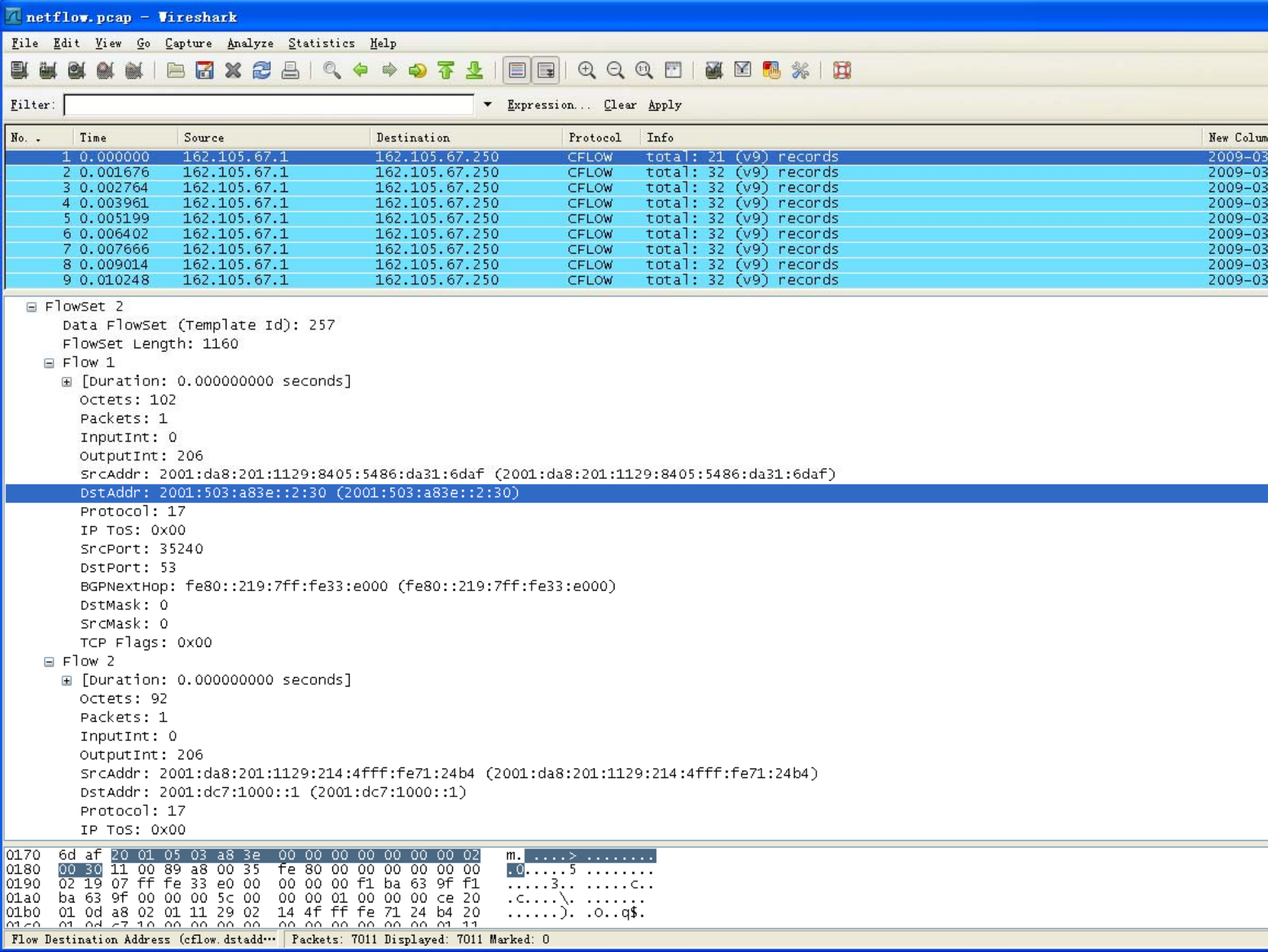


NetFlow v9 Export Packet

To support technologies such as MPLS or Multicast, this export format can be leveraged to easily insert new fields



- **Matching ID #s is the way to associate Template to the Data Records**
- **The Header follows the same format as prior NetFlow versions so Collectors will be backward compatible**
- **Each Data Record represents one flow**
- **If exported flows have the same fields then they can be contained in the same Template Record e.g. unicast traffic can be combined with multicast records**
- **If exported flows have different fields then they can't be contained in the same Template Record e.g. BGP next-hop can't be combined with MPLS Aware NetFlow records**

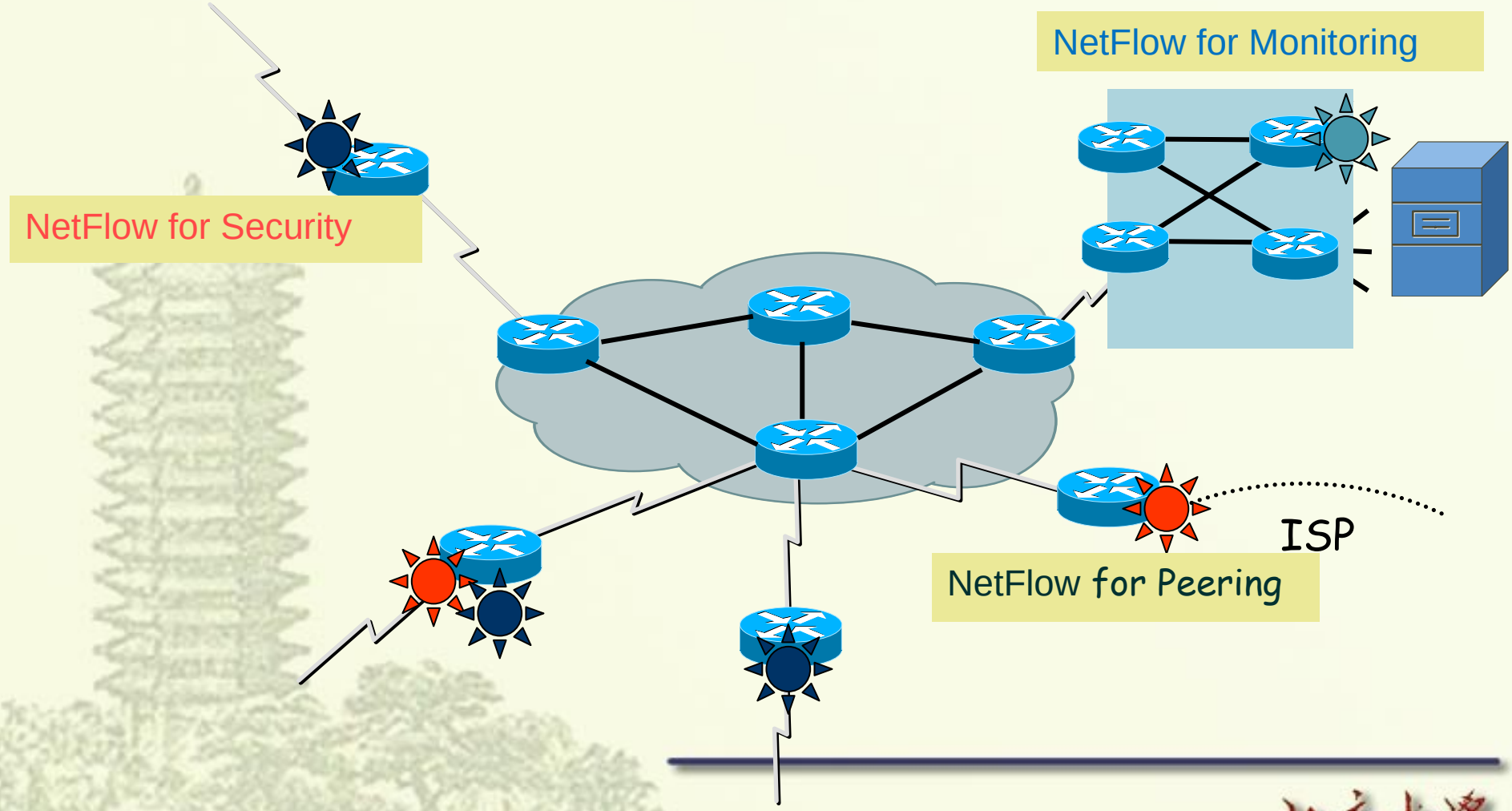

netflow.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info New Colum
1 0.000000 162.105.67.1 162.105.67.250 CFLOW total: 21 (v9) records 2009-03
2 0.001676 162.105.67.1 162.105.67.250 CFLOW total: 32 (v9) records 2009-03
3 0.002764 162.105.67.1 162.105.67.250 CFLOW total: 32 (v9) records 2009-03
4 0.003961 162.105.67.1 162.105.67.250 CFLOW total: 32 (v9) records 2009-03
5 0.005199 162.105.67.1 162.105.67.250 CFLOW total: 32 (v9) records 2009-03
6 0.006402 162.105.67.1 162.105.67.250 CFLOW total: 32 (v9) records 2009-03
7 0.007666 162.105.67.1 162.105.67.250 CFLOW total: 32 (v9) records 2009-03
8 0.009014 162.105.67.1 162.105.67.250 CFLOW total: 32 (v9) records 2009-03
9 0.010248 162.105.67.1 162.105.67.250 CFLOW total: 32 (v9) records 2009-03
FlowSet 2
Data FlowSet (Template Id): 257
FlowSet Length: 1160
Flow 1
[Duration: 0.000000000 seconds]
Octets: 102
Packets: 1
InputInt: 0
OutputInt: 206
SrcAddr: 2001:da8:201:1129:8405:5486:da31:6daf (2001:da8:201:1129:8405:5486:da31:6daf)
DstAddr: 2001:503:a83e::2:30 (2001:503:a83e::2:30)
Protocol: 17
IP ToS: 0x00
SrcPort: 35240
DstPort: 53
BGPNextHop: fe80::219:7ff:fe33:e000 (fe80::219:7ff:fe33:e000)
DstMask: 0
SrcMask: 0
TCP Flags: 0x00
Flow 2
[Duration: 0.000000000 seconds]
Octets: 92
Packets: 1
InputInt: 0
OutputInt: 206
SrcAddr: 2001:da8:201:1129:214:4fff:fe71:24b4 (2001:da8:201:1129:214:4fff:fe71:24b4)
DstAddr: 2001:dc7:1000::1 (2001:dc7:1000::1)
Protocol: 17
IP ToS: 0x00
0170 6d af 20 01 05 03 a8 3e 00 00 00 00 00 00 00 02 m. ....> ....
0180 00 30 11 00 89 a8 00 35 fe 80 00 00 00 00 00 00 .0.....5 ....
0190 02 19 07 ff fe 33 e0 00 00 00 00 f1 ba 63 9f f1 .....3.. .....c..
01a0 ba 63 9f 00 00 00 5c 00 00 00 01 00 00 00 ce 20 .c....\. ....
01b0 01 0d a8 02 01 11 29 02 14 4f ff fe 71 24 b4 20 ......). .O..q$.
Flow Destination Address (cflow.dstadd···
Packets: 7011 Displayed: 7011 Marked: 0

问题

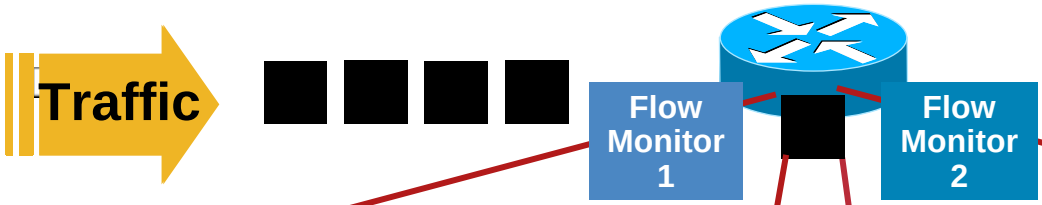
- Netflow v9信息足够？
  - Experiences with IPFIX-based Traffic Measurement for IPv6 Networks，N Choi, H Son, Y Lee, Y Choi，Proc. of ACM IPv6’07
- Flexible Netflow(FNF)*
  - Cisco IOS Release 12.4(20)T
  - 可自定义字段，灵活
  - 目标：不同的目标采用不同的模板

http://www.cisco.com/web/go/fnf/

Netflow不同的部署目的



Flexible NetFlow
Multiple Monitors with Unique Key Fields



Key Fields	Packet 1
Source IP	3.3.3.3
Destination IP	2.2.2.2
Source Port	23
Destination Oort	22078
Layer 3 Protocol	TCP - 6
TOS Byte	0
Input Interface	Ethernet 0

Non-Key Fields
Packets
Bytes
Timestamps
Next Hop Address

Key Fields	Packet 1
Source IP	3.3.3.3
Dest IP	2.2.2.2
Input Interface	Ethernet 0
SYN Flag	0

Non-Key Fields
Packets
Timestamps

Traffic Analysis Cache

Source IP	Dest. IP	Source Port	Dest. Port	Protocol	TOS	Input I/F	…	Pkts
3.3.3.3	2.2.2.2	23	22078	6	0	E0	…	1100

Security Analysis Cache

Source IP	Dest. IP	Input I/F	Flag	…	Pkts
3.3.3.3	2.2.2.2	E0	0	…	11000

Flexible Flow Record: Key Fields

Flow
Sampler ID
Direction
Interface
Input
Output
Layer 2
Source VLAN
Destination VLAN
Source MAC address
Destination MAC address

IPv4	
IP (Source or Destination)	Payload Size
Prefix (Source or Destination)	Packet Section (Header)
Mask (Source or Destination)	Packet Section (Payload)
Minimum-Mask (Source or Destination)	TTL
Protocol	Options bitmap
Fragmentation Flags	Version
Fragmentation Offset	Precedence
Identification	DSCP
Header Length	TOS
Total Length	

IPv6	
IP (Source or Destination)	Payload Size
Prefix (Source or Destination)	Packet Section (Header)
Mask (Source or Destination)	Packet Section (Payload)
Minimum-Mask (Source or Destination)	DSCP
Protocol	Extension Headers
Traffic Class	Hop-Limit
Flow Label	Length
Option Header	Next-header
Header Length	Version
Payload Length	

设备配置*

- 以Cisco设备为例
  - Netflow v9
  - Flexible Netflow

http://www.cisco.com/go/netflow

Netflow v9 for IPv6

Configure on Cisco IOS release 12.2(33)SRB or later

```
Router(config)# ipv6 unicast-routing
Router(config)# mls flow ipv6 interface-full
Router(config)# mls nde sender
Router(config)# ip flow-export version 9
Router(config)# ip flow-export destination 172.16.10.2 88
Router(config)# interface FastEthernet1/1
Router(config)# ipv6 address 2001:0DB8::1/64
```

Flexible Netflow*

Configure the Exporter

```
Router(config)# flow exporter my-exporter

Router(config-flow-exporter)# destination 1.1.1.1
```

Configure the Flow Record

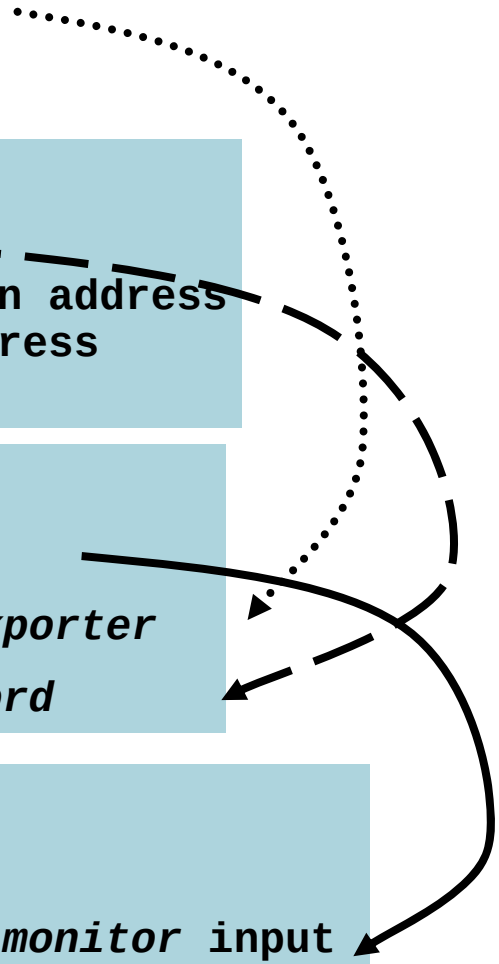
```
Router(config)# flow record my-record
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# collect counter bytes
```

Configure the Flow Monitor

```
Router(config)# flow monitor my-monitor

Router(config-flow-monitor)# exporter my-exporter

Router(config-flow-monitor)# record my-record
```

Configure the Interface

```
Router(config)# interface s3/0

Router(config-if)# ip flow monitor my-monitor input
```



http://www.cisco.com/go/fnf

流量工具介绍

- 按功能分
  - 采集工具和分析工具
- 按目的分
  - 行为分析、安全分析、计费
- 按是否收费分
  - 商业、免费(含开源)
- 按支持数据源分
  - 单一、混合

Cisco Netflow商业合作伙伴

流量分析

OPNET
AdventNet Excellence Matters
Cisco Systems Empowering the Internet Generation NetFlow Collector
IBM
hp invent
InfoVista
isarNet Professional Networking
NetQoS Performance Experts
wiredcity a division of OSIsoft, Inc.
Valencia Systems
PAESSLER
concord
ca
SOLARWINDS
Caligare
ARBOR NETWORKS
net monitor
plixer International
COMPUWARE
IdeaData Group

安全

Cisco Systems Empowering the Internet Generation CS-Mars
Lancope®
ARBOR NETWORKS

计费

EVIDENT SOFTWARE
PORTAL
NetQoS Performance Experts

More info: http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/commercial/

Some Open Source NetFlow Tools

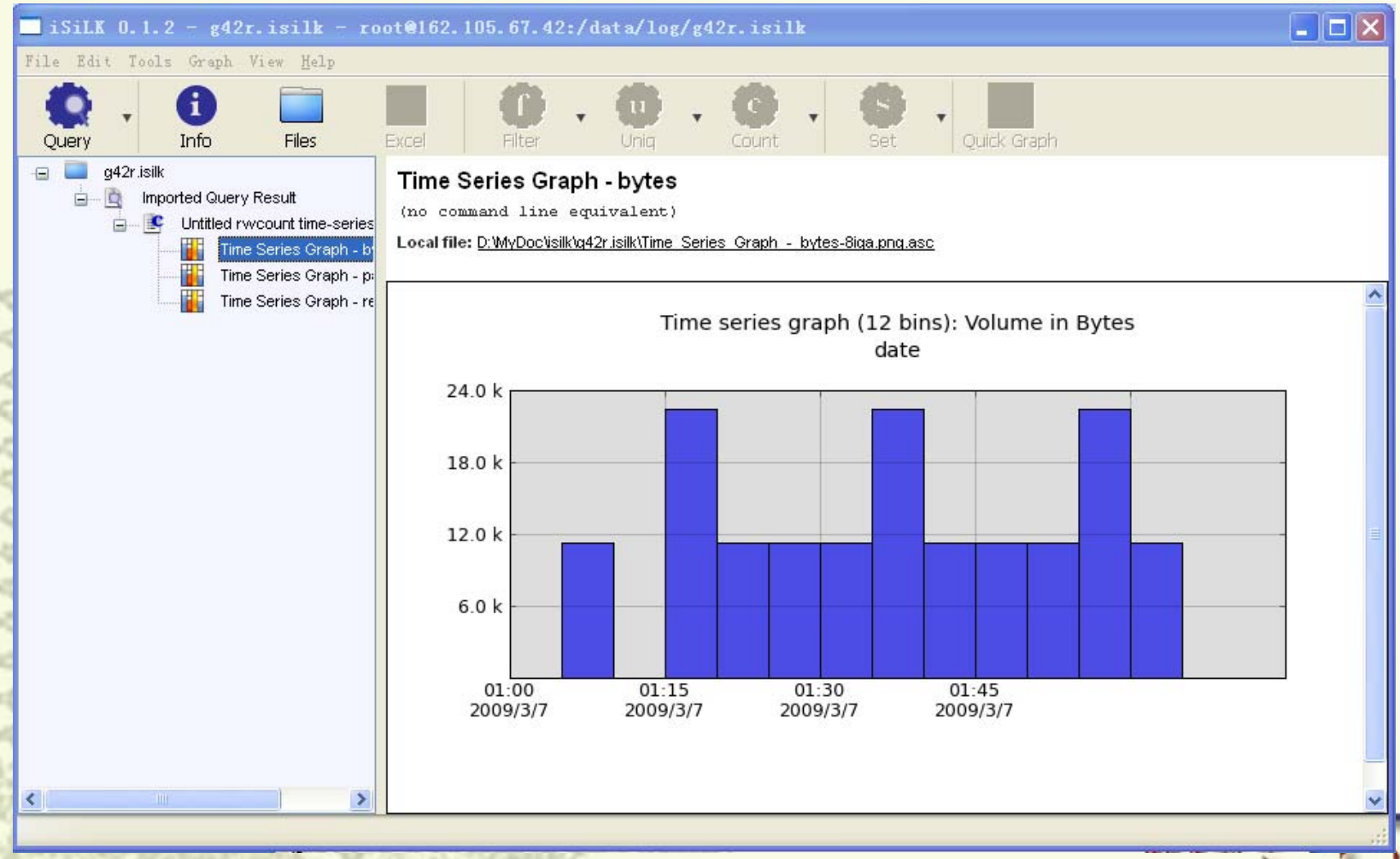
Product Name	Primary Use	Comment	OS
Cflowd	Traffic Analysis	No longer supported	UNIX
Flow-tools	Collector Device	Scalable	UNIX
Flowd	Collector Device	Support V9	BSD, Linux
FlowScan	Reporting for Flow-Tools		UNIX
IPFlow	Traffic Analysis	Support V9, IPv4, IPv6, MPLS, SCTP, etc..	Linux, FreeBSD, Solaris
SilkTools	Security analysis	Support V9/IPFIX, IPv6	BSD, Linux
NetFlow Monitor	Traffic Analysis	Supports V9	UNIX
Ntop/nProbe	Security Monitoring	Support V9, IPv6	UNIX
Panoptis	Security Monitoring		UNIX
NfSen	Collector Device	Support V9, IPv6	Linux
Stager	Reporting for Flow-Tools		UNIX

Different Costs: Implementation and Customization

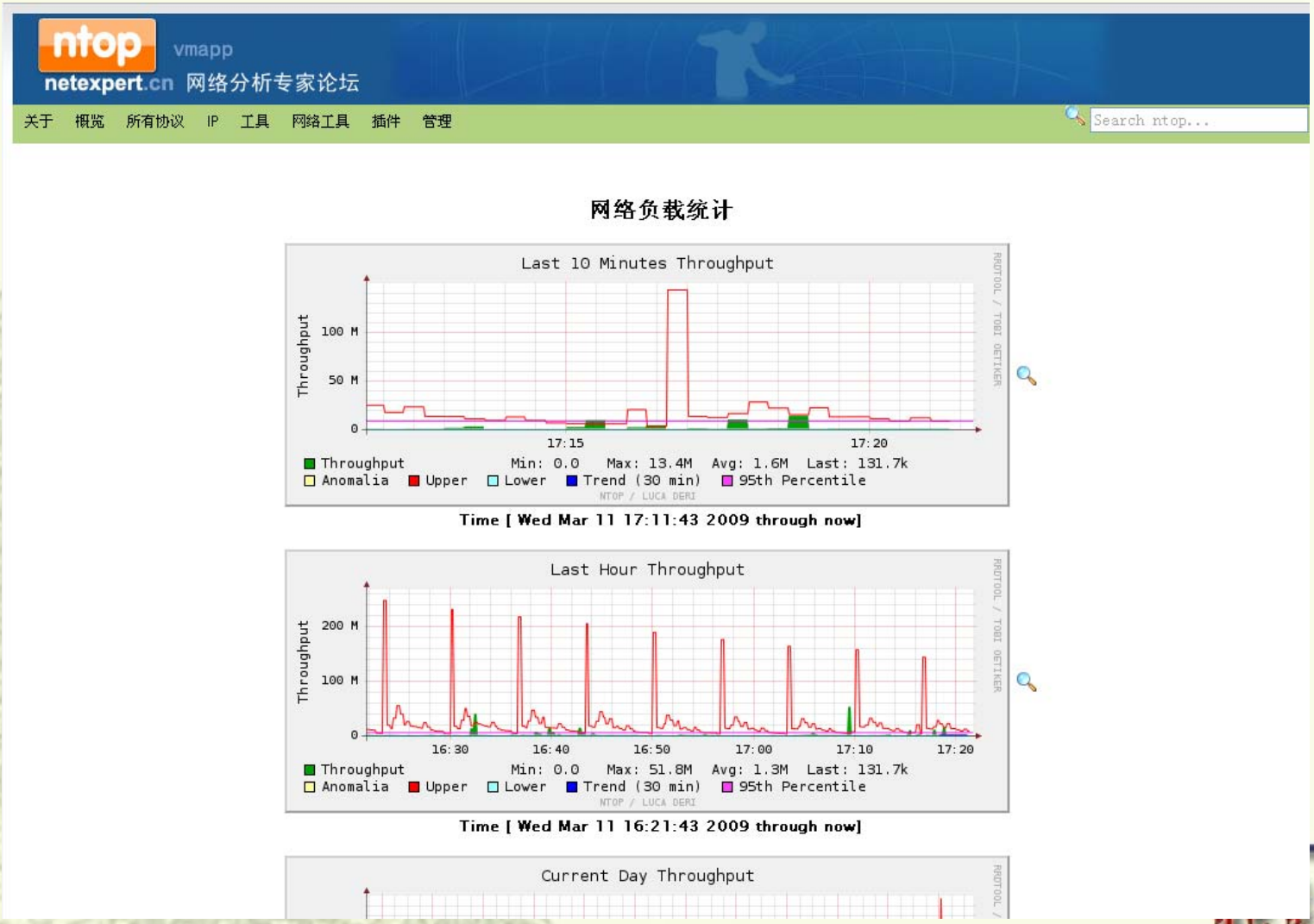
Flow-tools

- Flow-tools is library and a collection of programs used to collect, send, process, and generate reports from NetFlow data.
- Can be used together on a single server or distributed to multiple servers for large deployments.
- The flow-tools library provides an API for development of custom applications for NetFlow export versions 1,5,6 and the 14 currently defined version 8 subversions.
- Version 9 is not supported now

Silktools


iSiLK 0.1.2 - g42r.isilk - root@162.105.67.42:/data/log/g42r.isilk
File Edit Tools Graph View Help
Query
Info
Files
Excel
Filter
Uniq
Count
Set
Quick Graph
g42r.isilk
Imported Query Result
Untitled rwcount time-series
Time Series Graph - by
Time Series Graph - pa
Time Series Graph - re
Time Series Graph - bytes
(no command line equivalent)
Local file: D:\MyDoc\isilk\g42r.isilk\Time_Series_Graph_-_bytes-8iqa.png.asc
Time series graph (12 bins): Volume in Bytes
date
24.0 k
18.0 k
12.0 k
6.0 k
01:00
2009/3/7
01:15
2009/3/7
01:30
2009/3/7
01:45
2009/3/7

Ntop

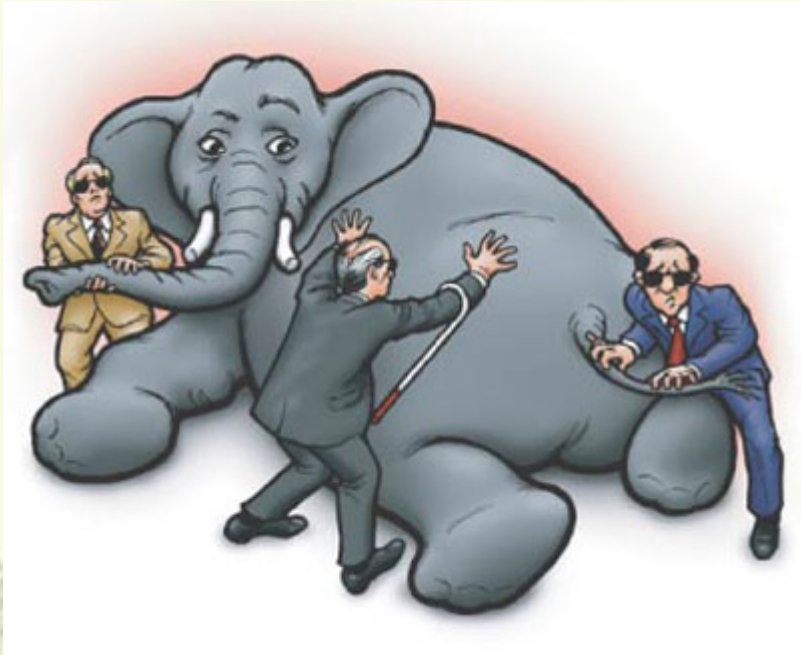

ntop
vmapp
netexpert.cn 网络分析专家论坛
关于 概览 所有协议 IP 工具 网络工具 插件 管理
Search ntop...
网络负载统计
Last 10 Minutes Throughput
Throughput
100 M
50 M
0
17:15
17:20
Throughput Min: 0.0 Max: 13.4M Avg: 1.6M Last: 131.7k
Anomalia Upper Lower Trend (30 min) 95th Percentile
NTOP / LUCA DERI
Time [Wed Mar 11 17:11:43 2009 through now]
Last Hour Throughput
Throughput
200 M
100 M
0
16:30
16:40
16:50
17:00
17:10
17:20
Throughput Min: 0.0 Max: 51.8M Avg: 1.3M Last: 131.7k
Anomalia Upper Lower Trend (30 min) 95th Percentile
NTOP / LUCA DERI
Time [Wed Mar 11 16:21:43 2009 through now]
Current Day Throughput

未完…

- Some equipments can’t support netflow-based IPv6 flow data collecting/exporting
  - Update version or device
  - Use nProbe or YAF instead
- Performance impact
  - http://www.cisco.com/en/US/tech/tk812/technologies_white_paper0900aecd802a0eb9.shtml
- Open questions
  - sampling
  - Algorithms
  - Data mining
  - Auto discovery
  - ……

总结

- 流量分析是网络运行的重要工具
- IPv6下的流量分析：挑战与机遇



谢谢

- 幻灯片内容多来自网络，未一一列出引用
- Cisco公司Sang提供了丰富的资料