NETFLOW FOR ACCOUNTING, ANALYSIS AND ATTACK
Agenda

• Introduction
• Hardware
• Versions
• Accounting and Analysis—MPLS Environment
• Accounting and Analysis—BGP and Autonomous Systems
• Analysis and Attack—Multicast Options
• Attack—Security Features and Applications
• Scaling—Features and Options
• Export—Collector, NAM and Partners
• Evolving NetFlow—IPv6 and Deployment

Acknowledgement Benoit Claise
Agenda

Introduction

• What Is a Flow?
• NetFlow Principles
• NetFlow Cache
• Timers
• NetFlow CLI
NetFlow Origination

- Developed by Darren Kerr and Barry Bruins at Cisco Systems in 1996
  US Patent 6,243,667
- The value of information in the cache was a secondary discovery
  Initially designed as a switching path
- NetFlow is now the primary network accounting technology in the industry
- Answers questions regarding IP traffic: who, what, where, when, and how
# Principle NetFlow Benefits

## Service Provider
- Peering arrangements
- Network planning
- Traffic engineering
- Accounting and billing
- Security monitoring

## Enterprise
- Internet access monitoring (protocol distribution, where traffic is going/coming)
- User monitoring
- Application monitoring
- Charge back billing for departments
- Security monitoring
What Is a Flow?

Defined by Seven Unique Keys:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- TOS byte (DSCP)
- Input logical interface (ifIndex)
NetFlow Principles

- Inbound traffic only
- Unidirectional flow
- Accounts for both transit traffic and traffic destined for the router
- Works with Cisco Express Forwarding or fast switching
  - Not a switching path
- Supported on all interfaces and Cisco IOS® Software platforms
- Returns the subinterface information in the flow records
- Cisco Catalyst® 6500 Series and Cisco 7600 Series enables NetFlow on all interfaces by default
Creating Export Packets

UDP Export Packets

- Approximately 1500 bytes
- Typically contain 20-50 flow records
- Sent more frequently if traffic increases on NetFlow-enabled interfaces
# Flow Export Format

## Usage
- Packet count
- Byte count
- Source IP address
- Destination IP address

## Time of Day
- Start sysUpTime
- End sysUpTime
- Source TCP/UDP port
- Destination TCP/UDP port

## Port Utilization
- Input ifIndex
- Output ifIndex
- Next Hop address
- Source AS number
- Dest. AS number
- Source prefix mask
- Dest. prefix mask

## QoS
- Type of service
- TCP flags
- Protocol
- Type of service
- TCP flags
- Protocol

> Version 5 Is Used in This Example
NetFlow Cache Example

1. Create and update flows in NetFlow cache

<table>
<thead>
<tr>
<th>Srcif</th>
<th>SrclPadd</th>
<th>Dstif</th>
<th>DstIPadd</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>Pkts</th>
<th>Src Port</th>
<th>Src AS</th>
<th>Dst Port</th>
<th>Dst AS</th>
<th>NextHop</th>
<th>Bytes/Pkt</th>
<th>Active</th>
<th>Idle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa1/0</td>
<td>173.100.21.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>11000</td>
<td>00A2</td>
<td>/24</td>
<td>5</td>
<td>00A2</td>
<td>/24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1528</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.3.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>6</td>
<td>40</td>
<td>0</td>
<td>2491</td>
<td>15</td>
<td>/26</td>
<td>196</td>
<td>15</td>
<td>/24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>740</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.20.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>10000</td>
<td>00A1</td>
<td>/24</td>
<td>180</td>
<td>00A1</td>
<td>/24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1428</td>
</tr>
<tr>
<td>Fa1/0</td>
<td>173.100.6.2</td>
<td>Fa0/0</td>
<td>10.0.227.12</td>
<td>6</td>
<td>40</td>
<td>0</td>
<td>2210</td>
<td>19</td>
<td>/30</td>
<td>180</td>
<td>19</td>
<td>/24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1040</td>
</tr>
</tbody>
</table>

- Inactive timer expired (15 sec is default)
- Active timer expired (30 min (1800 sec) is default)
- NetFlow cache is full (oldest flows are expired)
- RST or FIN TCP Flag

2. Expiration

3. Aggregation

4. Export version

- Non-Aggregated Flows—Export Version 5 or 9

5. Transport protocol

- Export Packet
- Export Payload (Flows)

e.g. Protocol-Port Aggregation Scheme Becomes

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Pkts</th>
<th>SrcPort</th>
<th>DstPort</th>
<th>Bytes/Pkt</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>11000</td>
<td>00A2</td>
<td>00A2</td>
<td>1528</td>
</tr>
</tbody>
</table>
NetFlow Processing Order

**Pre-Processing**
- Packet Sampling
- Filtering

**Features and Services**
- IP
- Multicast
- MPLS
- IPv6

**Post-Processing**
- Aggregation schemes
- Non-key fields lookup
- Export
Active/Inactive Timers

- **Inactive time** = The flow expires once no packets are seen for this time duration
- **Active time** = If packets continue to be received on this flow beyond this active time setting then the flow will expire and be exported while a new flow is created
- **Default values on software-based routers: Cisco 10000 and 12000 Series Internet Routers:**
  - Inactive timer: 15 seconds (minimum 1 second)
  - Active timer: 30 minutes (minimum 1 minute)
- **Default values on a Cisco Catalyst 6500 Series and Cisco 7600 Series:**
  - Aging time: 256 seconds
  - Fast aging time: disabled (flows that only switch a few packets and are never used again)
  - Long aging time: 1920 seconds (used to prevent counter wraparound and inaccurate stats)

**Recommendation:** Change normal aging time to 32 seconds and fast aging time to 32 seconds and 32 packets
Flow Timers and Expiration

1st & 3rd Flows – Src 10.1.1.1, Dst 20.2.2.2, Prot 6, Src & Dst port 15, InIF FE0/0, ToS 128
2nd Flow – Src 10.1.1.1, Dst 20.2.2.2, Prot 6, Src & Dst port 15, InIF FE0/0, ToS 192

Router Boots (sysUpTime timer begins)

1st Flow Start (sysUpTime)
1st Flow End (sysUpTime)
1st Flow Expires (sysUpTime)

2nd Flow Start (sysUpTime)
2nd Flow End (sysUpTime)
2nd Flow Expires (sysUpTime)

3rd Flow Start (sysUpTime)

= packet from 1st or 3rd flow

= packet from 2nd flow

UDP Export Packet containing 30-50 flows (sysUpTime & UTC)

• SysUptime - Current time in milliseconds since router booted
• UTC - Coordinated Universal Time can be synchronized to NTP (Network Time Protocol)
NetFlow Configuration Commands

- `ip route-cache flow`
  Per interface
- `ip flow-export version <version> [origin-as|peer-as|bgp-nexthop]`
  e.g. `ip flow-export version 5`
- `ip flow-export destination <address> <port>`
  e.g. `ip flow-export destination 10.0.0.1 65001`
- `ip flow-export source <interface>`
  Default is interface will best route to collector. We recommend configuring and setting a loopback interface.
- `ip flow-aggregation cache <name of aggregation scheme>`
  Selects the aggregation cache
- `ip flow-cache timeout inactive <seconds>`
  Sets the seconds an inactive flow will remain in the cache before expiration. 15 seconds is default
- `ip flow-cache timeout active <minutes>`
  Sets the minutes an active flow will remain in the cache before expiration. 30 minutes is default
- `ip flow-cache entries <number>`
  Sets the maximum number of flow entries in the cache. The default varies dependent on platform.
NetFlow Configuration Commands

- `show ip cache [verbose] flow`
  
  Shows NetFlow statistics

- `show ip cache flow aggregation <name of aggregation scheme>`
  
  Shows NetFlow statistics for the configured aggregation scheme

- `show ip flow export`
  
  Shows export statistics

- `clear ip cache flow`
  
  Clears NetFlow statistics

- `clear ip flow stats`
  
  Clears export statistics
router_A#sh ip cache flow
IP packet size distribution (85435 total packets):
1-32    64   96  128  160  192  224  256  288  320  352  384  416  448  480 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
512  544  576 1024 1536 2048 2560 3072 3584 4096 4608 .000 .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
2728 active, 1368 inactive, 85310 added
463824 aged polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
last clearing of statistics never

Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
-------- Flows /Sec /Flow /Pkt /Sec /Flow /Flow
TCP-X                2      0.0         1  1440      0.0       0.0 9.5
TCP-other        82580     11.2         1  1440     11.2       0.0  12.0
Total:           82582     11.2         1  1440     11.2       0.0      12.0

SrcIf    SrcIPaddress    DstIf    DstIPaddress    Pr    SrcP    DstP    Pkts
Et0/0     132.122.25.60   Se0/0     192.168.1.1     06    9AEE  0007    1
Et0/0     139.57.220.28   Se0/0     192.168.1.1     06    708D  0007    1
Et0/0     165.172.153.65  Se0/0     192.168.1.1     06    CB46  0007    1
router_A#sh ip cache verbose flow
IP packet size distribution (23597 total packets):
  1-32  64  96  128  160  192  224  256  288  320  352  384  416  448  480
    .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
    .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1323 active, 2773 inactive, 23533 added
  151644 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Total Flows</th>
<th>Flows /Sec</th>
<th>Packets /Flow</th>
<th>Bytes /Pkt</th>
<th>Flows /Sec</th>
<th>Packets Active(Sec)</th>
<th>Idle(Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-other</td>
<td>22210</td>
<td>3.1</td>
<td>1440</td>
<td>3.1</td>
<td>0.0</td>
<td>12.9</td>
<td></td>
</tr>
<tr>
<td>Total:</td>
<td>22210</td>
<td>3.1</td>
<td>1440</td>
<td>3.1</td>
<td>0.0</td>
<td>12.9</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SrcIf DstIf</th>
<th>SrcIPaddress DstIPaddress Pr TOS Flgs Pkts</th>
<th>Port Msk AS Port Msk AS NextHop</th>
<th>B/Pk Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>216.120.112.114 Se0/0</td>
<td>192.168.1.114</td>
<td>06 00 10 1</td>
</tr>
<tr>
<td>5FA7 /0 0</td>
<td>0007 /0 0</td>
<td>0.0.0.0</td>
<td>1440 0.0</td>
</tr>
<tr>
<td>Et0/0</td>
<td>175.182.253.65 Se0/0</td>
<td>192.168.1.114</td>
<td>06 00 10 1</td>
</tr>
</tbody>
</table>
Agenda

• Introduction
• Hardware
• Versions
• Accounting and Analysis—MPLS Environment
• Accounting and Analysis—BGP and Autonomous Systems
• Analysis and Attack—Multicast Options
• Attack—Security Features and Applications
• Scaling—Features and Options
• Export—Collector, NAM and Partners
• Evolving NetFlow—IPv6 and Deployment
Agenda

Hardware

• Summary
• Software-based platforms
• Cisco Catalyst 6500 Series and Cisco 7600 Series
• Cisco 12000 Series Internet Router
Comprehensive Hardware Support

Cisco 800
Cisco 1700
Cisco 2600
Cisco 3600
Cisco 3700
Cisco 4500/4700
Cisco AS5300/5800
Cisco 7200/7300/7400/7500/
Cisco 4500 ASIC
Cisco Catalyst 6500/Cisco 7600 ASIC
Cisco 4700
Cisco 10000 ASIC
Cisco 12000 ASIC
Switching Path for Software-Based and Cisco 12000 Engine 0/1 Linecards

Cisco 1700, 2500, 2600, 3600, 4500, and 7200 Series Routers
Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router

- Hybrid: Cisco Catalyst OS on PFC/supervisor and Cisco IOS Software on MSFC
- Native Cisco IOS Software: PFC/supervisor and the MSFC both run a single bundled Cisco IOS Software image
- Export is centrally via the supervisor and MSFC, each linecard has its own hardware NetFlow cache and forwarding table, i.e. distributed platform

<table>
<thead>
<tr>
<th></th>
<th>Hybrid</th>
<th>Native 12.1E</th>
<th>Native 12.2SX</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSFCx</td>
<td>v5</td>
<td>v5</td>
<td>v5, v8*</td>
</tr>
<tr>
<td>Sup1a</td>
<td>V7, v8</td>
<td>v7</td>
<td>N/A</td>
</tr>
<tr>
<td>Sup2</td>
<td>V7, v8</td>
<td>v5, v7</td>
<td>v5, v7, v8</td>
</tr>
<tr>
<td>Sup720</td>
<td>v5, v7, v8</td>
<td>v5, v7</td>
<td>v5, v7, v8</td>
</tr>
</tbody>
</table>

*No NetFlow Support on MSFC with Sup1a
Cisco Catalyst 6500 Series and Cisco 7600 Series Supervisor

- **Supervisor 1:**
  
  When destination has no adjacency in FIB the 1st packet goes to MSFC for ARP request; This packet is not counted by the supervisor2
  
  If NetFlow is enabled on the MSFC2, the MSFC2 accounted packets will have DstIf = Null (by limitation)

- **Supervisor 2**—99% of traffic goes through the supervisor 2
MLS Best Design

MLS-Enabled and Export v7 from the SUP2

Export v5 from the MSFC2

And Export in the sc0 vlan
Cisco Catalyst 6500 Series and Cisco 7600 Series Versions and Features

- **Cisco IOS Software Release 12.1(13)E1**
  - PFC2 Source/destination interface information (Hybrid 6.3(6))
  - PFC2 Source/destination AS information
  - PFC2 Support for V5 NetFlow data export (Hybrid 7.5(1))
  - IP Next hop
  - Sampled NetFlow is available on PFC in Cisco IOS
- **Cisco IOS Software Release 12.2(14)SX**
  - Version 8 in native mode
- **PFC3b (Sup720) cards**
  - ToS byte
  - Multicast traffic
- **Hybrid Cisco Catalyst OS 7.2(1)**
  - L2 switched traffic (vlan x to vlan y) support (doesn’t require MSFC)
- **Hybrid Cisco Catalyst OS 7.3(1)**
  - Destination and source IfIndex enabled by default
Cisco Catalyst 6500 Series and Cisco 7600 Series: Native Cisco IOS Software Mode

```
mls flow ip full -> flow mask
mls nde src_address 10.200.8.127 version 7
    -> version 7 export source OR
mls nde sender -> NDE enable + NDE from the PFC uses the
    source configured from the MSFC!!!!!
interface vlan 1
    ip address 10.200.8.127 255.255.255.0
    ip route-cache flow
interface FastEthernet 3/2
    ip address 10.300.8.2 255.255.255.0
    ip route-cache flow

ip flow-export source vlan1 -> version 5 export source
ip flow-export version 5
ip flow-export destination 172.17.246.244 9996
    -> both for version 5 and 7 export
```
Cisco Catalyst 6500 Series and Cisco 7600 Series: Switched Traffic

- L2 switched traffic (vlan x to vlan y) support in Hybrid Catalyst OS 7.2(1); It doesn’t require a MSFC; native mode: not yet available

```
set mls bridged-flow-statistics enable/disable <vlan>
```

- Destination and source IfIndex enabled by default, support in Hybrid 7.3(1)

```
set mls nde {destination-index|source-index} {enable|disable}
```
Cisco Catalyst 4000/4500 Series
NetFlow

• NetFlow services card in Supervisor 4:
  12.1(13)EW supports version 5 without interface tracking
  12.1(19)EW supports version 5 (with interface tracking) and version 8

• NetFlow services card in Supervisor 5:
  12.2(18)EW supports Version 5 and 8

• Prior card was NetFlow Feature Card (NFFC) (now end of sale)
Cisco 12000 Series Internet Routers: NetFlow

- Engine 0—software support
- Engine 1—software support
- Engine 2—support in ASICs, however there’s significant performance impact if running many other features concurrently
- Engine 3—support in ASICs
- Engine 4—not supported
- Engine 4+—support in ASICs
Agenda

• Introduction
• Hardware
• Versions
• Accounting and Analysis—MPLS Environment
• Accounting and Analysis—BGP and Autonomous Systems
• Analysis and Attack—Multicast Options
• Attack—Security Features and Applications
• Scaling—Features and Options
• Export—Collector, NAM and Partners
• Evolving NetFlow—IPv6 and Deployment
Agenda

Versions

• Overview
• Version 9
• IPFIX and PSAMP Working Groups
<table>
<thead>
<tr>
<th>NetFlow Version</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Original</td>
</tr>
<tr>
<td>5</td>
<td>Standard and Most Common</td>
</tr>
</tbody>
</table>
| 7               | Specific to Cisco C6500 and 7600 Series Switches  
Similar to Version 5, but Does Not Include AS, Interface,  
TCP Flag and ToS Information |
| 8               | Choice of Eleven Aggregation Schemes  
Reduces Resource Usage |
| 9               | Flexible, Extensible File Export Format to Enable Easier  
Support of Additional Fields and Technologies e.g. MPLS,  
Multicast, BGP Next Hop, and IPv6 |
## Version 8: Flow Format

<table>
<thead>
<tr>
<th>Source Prefix</th>
<th>Protocol-Port</th>
<th>Source-Prefix</th>
<th>Destination-Prefix</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Prefix Mask</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Prefix</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Prefix Mask</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source App Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination App Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source AS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination AS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Timestamp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Timestamp</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Packets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Bytes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: The table indicates which fields are included in each row.*
## Version 8: Flow Format

<table>
<thead>
<tr>
<th>Field</th>
<th>AS-TOS</th>
<th>Protocol-Port-TOS</th>
<th>Source-Prefix-TOS</th>
<th>Destination-Prefix-TOS</th>
<th>Prefix-TOS</th>
<th>Prefix-Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Prefix</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Source Prefix Mask</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Destination Prefix</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Destination Prefix Mask</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Source App Port</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination App Port</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Interface</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Output Interface</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>IP Protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Source AS</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Destination AS</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>TOS</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>First Timestamp</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Last Timestamp</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td># of Flows</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td># of Packets</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td># of Bytes</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
### Version 8: Configuration

3600-4(config)# ip flow-aggregation cache ?

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as</td>
<td>AS aggregation</td>
</tr>
<tr>
<td>as-tos</td>
<td>AS-TOS aggregation</td>
</tr>
<tr>
<td>destination-prefix</td>
<td>Destination Prefix aggregation</td>
</tr>
<tr>
<td>destination-prefix-tos</td>
<td>Destination Prefix TOS aggregation</td>
</tr>
<tr>
<td>prefix</td>
<td>Prefix aggregation</td>
</tr>
<tr>
<td>prefix-port</td>
<td>Prefix-port aggregation</td>
</tr>
<tr>
<td>prefix-tos</td>
<td>Prefix-TOS aggregation</td>
</tr>
<tr>
<td>protocol-port</td>
<td>Protocol and port aggregation</td>
</tr>
<tr>
<td>protocol-port-tos</td>
<td>Protocol, port and TOS aggregation</td>
</tr>
<tr>
<td>source-prefix</td>
<td>Source Prefix aggregation</td>
</tr>
<tr>
<td>source-prefix-tos</td>
<td>Source Prefix TOS aggregation</td>
</tr>
</tbody>
</table>

**Note**—**Do Not** Export Version 5 at the Same Time “ip flow-export version 5”
Why a New Version?

• Previous formats (versions 1, 5, 7, and 8) were fixed format and inflexible
  1) Cisco needed to build a new version each time a customer wanted to export new fields
  2) Partners had to reengineer to support the new export format

Solution: Build a **Flexible** and **Extensible** Export Format!
NetFlow v9 Principles

- Version 9 is an **export format**
- Still a push model
- Send the template regularly (configurable)
- Independent of the UDP transport protocol, it is ready for any reliable transport protocol e.g. TCP, SCTP,…
- Advantage: we can add new technologies/data types very quickly
  
  e.g. MPLS, IPv6, BGP Next Hop, Multicast,…
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 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 v9 Flexible Format

Example of Export Packet Right after Router Boot or NetFlow Configuration

Template FlowSet
- Template Record
  - Template ID
    - (Specific Field Types and Lengths)
- Template Record
  - Template ID
    - (Specific Field Types and Lengths)
- Template Record
  - Template ID
    - (Specific Field Types and Lengths)
- Template Record
  - Template ID
    - (Specific Field Types and Lengths)

Option Template FlowSet
- Template ID
  - Option Data
    - FlowSet ID
    - Option Data Record
      - (Field Values)
    - Option Data Record
      - (Field Values)

Example of Export Packets Containing Mostly Flow Information

Data FlowSet
- Data Record
  - FlowSet ID
  - (Field Values)
- Data Record
  - (Field Values)
- Data Record
  - (Field Values)
- Data Record
  - (Field Values)
- Data Record
  - (Field Values)
- Data Record
  - (Field Values)
NetFlow Version 9 Configuration

Configuring Version 9 Export for the Main Cache

```
router(config)# ip flow-export version?
  1
  5
  9
router(config)# ip flow-export version 9
```

Configuring Version 9 Export for an Aggregation Scheme

```
router(config)# ip flow-aggregation cache as
router(config-flow-cache)# enabled
router(config-flow-cache)# export?
  destination Specify the Destination IP address
  version configure aggregation cache export version
router(config-flow-cache)# export version?
  8 Version 8 export format
  9 Version 9 export format
router(config-flow-cache)# export version 9
```
IETF: IP Flow Information Export (IPFIX) Working Group

• IPFIX is an effort to:
  
  Define the notion of a “standard IP flow”
  
  Devise data encoding for IP flows
  
  Consider the notion of IP flow information export based upon packet sampling
  
  Identify and address any security privacy concerns affecting flow data
  
  Specify the transport mapping for carrying IP flow information (IETF approved congestion-aware transport protocol)
IETF: IP Flow Information Export WG (IPFIX)

- IPFIX website for the charter, email archives, and drafts:
  
  http://ipfix.doit.wisc.edu/

- NetFlow version 9 has been selected as a basis for the IPFIX protocol

- Waiting on minor addition to the NetFlow version 9:
  Standardization of a reliable transport protocol: Stream Control Transport Protocol Partial Reliability (SCTP-PR) or Datagram Congestion Control Protocol (DCCP)
IETF: Packet Sampling WG (PSAMP)

- PSAMP agreed to use IPFIX (NetFlow version 9) for export

- PSAMP is an effort to:
  
  Specify a set of selection operations by which packets are sampled
  
  Describe protocols by which information on sampled packets is reported to applications


- Note: NetFlow is already using some sampling mechanisms
Agenda

- Introduction
- Hardware
- Versions
- **Accounting and Analysis—MPLS Environment**
- Accounting and Analysis—BGP and Autonomous Systems
- Analysis and Attack—Multicast Options
- Attack—Security Features and Applications
- Scaling—Features and Options
- Export—Collector, NAM and Partners
- Evolving NetFlow—IPv6 and Deployment
Agenda

Accounting and Analysis: MPLS Environment

• NetFlow MPLS Features Overview
• MPLS-Aware NetFlow
• MPLS Egress NetFlow
• Output Sampled NetFlow
• Traffic Matrix
NetFlow MPLS Features Overview

- Egress MPLS NetFlow accounting
  Cisco IOS Software Releases 12.0(10)ST and 12.1(5)T
- MPLS-aware NetFlow
  Cisco IOS Software Releases 12.0(24)S, 12.2(18)S, and 12.3(1)
MPLS-Aware NetFlow (v9)

- Enable on MPLS interfaces
- Tracks ingress traffic
- NetFlow version 9 only
- Option of IP and MPLS output or MPLS aggregation (top label aggregation)
- Supported in Cisco IOS Software Releases 12.3(1), 12.2(18)S, and 12.0(26)S1

  Release 12.0(24)S on the Cisco 12000 Series Internet Router
MPLS-Aware NetFlow (v9) Fields

- **Key fields (uniquely identifies the flow)**
  - Input ifIndex
  - Source IP address
  - Destination IP address
  - Protocol
  - Source port
  - Destination port
  - ToS byte

- **Additional export fields**
  - Flows
  - Packets
  - Bytes
  - Timestamps (sysUptime)
  - IP Next Hop
  - Output interface
  - Accumulation of TCP Flags
  - Type of the top label: LDP, BGP, VPN, ATOM, TE tunnel MID-PT, unknown
  - The FEC mapping to the top label

- Key fields are both MPLS and IP fields-based
- Supported in Cisco IOS Software Releases 12.3(1), 12.2(18)S, and 12.0(26)S1
- Release 12.0(24)S on the Cisco 12000 Series Internet Router
# MPLS-Aware NetFlow Configuration

**ip flow-cache mpls label-positions** `[label-position-1 [label-position-2 [label-position-3]]] [no-ip-fields] [mpls-length]

<table>
<thead>
<tr>
<th>label-position-n</th>
<th>Position of an MPLS Label in the Incoming Label Stack; Label Positions Are Counted from the Top of the Stack, Starting with 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-ip-fields</td>
<td>Controls the capture and reporting of MPLS flow fields. If the no-ip-fields keyword is not specified, the following IP related flow fields are included:</td>
</tr>
<tr>
<td></td>
<td>• Source IP address</td>
</tr>
<tr>
<td></td>
<td>• Destination IP address</td>
</tr>
<tr>
<td></td>
<td>• Transport layer protocol</td>
</tr>
<tr>
<td></td>
<td>• Source application port number</td>
</tr>
<tr>
<td></td>
<td>• Destination application port number</td>
</tr>
<tr>
<td></td>
<td>• IP type of service (ToS)</td>
</tr>
<tr>
<td></td>
<td>• TCP flag (the result of a bitwise OR of TCP)</td>
</tr>
<tr>
<td>mpls-length</td>
<td>Controls the Reporting of Packet Length; If the mpls-length Keyword Is Specified, the Reported Length Represents the Sum of MPLS Packet Payload Length and the MPLS Label Stack Length; If the mpls-length Keyword Is Not Specified, Only the Length of the MPLS Packet Payload Is Reported</td>
</tr>
</tbody>
</table>
Cisco 12000 Series Internet Routers
MPLS-Aware NetFlow (v9)

- Engines 0, 1, 2, and 3
  - Up to 3 labels and IP packet header fields
- Engine 4
  - Not supported
- Engine 4+
  - 1 label and IP packet header field
- MPLS-Aware NetFlow supported in Cisco IOS Software Release 12.0(24)S
- MPLS-Aware NetFlow top label aggregation supported in Cisco IOS Software Release 12.0(25)S
# MPLS-Aware NetFlow Top Label Aggregation Fields

<table>
<thead>
<tr>
<th>Key fields (uniquely identifies the flow)</th>
<th>Additional export fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input ifIndex</td>
<td>Flows</td>
</tr>
<tr>
<td>The top incoming MPLS labels with experimental bits and end-of-stack bit</td>
<td>Packets</td>
</tr>
<tr>
<td></td>
<td>Bytes</td>
</tr>
<tr>
<td></td>
<td>Timestamps (sysUptime)</td>
</tr>
<tr>
<td></td>
<td>IP Next Hop</td>
</tr>
<tr>
<td></td>
<td>Output interface</td>
</tr>
<tr>
<td></td>
<td>Accumulation of TCP Flags</td>
</tr>
<tr>
<td></td>
<td>Type of the top label: LDP, BGP, VPN, ATOM, TE tunnel MID-PT, unknown</td>
</tr>
<tr>
<td></td>
<td>The FEC mapping to the top label</td>
</tr>
</tbody>
</table>

- Key fields are both MPLS and IP fields based are not tracked
- Supported in Release 12.0(25)S
Egress MPLS NetFlow

- For Layer 3 VPN accounting
- Enable on IP interface
- Tracks egress traffic
- Only tracks MPLS to IP i.e. traffic coming from the core

```
router(config-if)#tag-switching ip flow egress
```

- NetFlow version 5 and version 8
- Can be enabled on sub-interfaces
- All other NetFlow commands still apply
- Supported in Releases, 12.0(10)ST, 12.1(5)T, and 12.0(22)S
Output Sampled NetFlow

- Enable on IP interface
- Tracks egress traffic
- Tracks both MPLS to IP and IP to IP
- Only supported on Cisco 12000 Series engine 3 (IP Service Engine (ISE)) linecard
- Supported in Release 12.0(24)S
  - Release 12.0(26)S added input interface

```
router(config-if)#ip route-cache flow sampled [input|output]
```
MPLS-Aware NetFlow: The Core Traffic Matrix

- Internal traffic matrix is PoP to PoP, the PoP being the AR or CR
- External traffic matrix PoP to BGP AS
Agenda

• Introduction
• Hardware
• Versions
• Accounting and Analysis—MPLS Environment
• Accounting and Analysis—BGP and Autonomous Systems
• Analysis and Attack—Multicast Options
• Attack—Security Features and Applications
• Scaling—Features and Options
• Export—Collector, NAM and Partners
• Evolving NetFlow—IPv6 and Deployment
Agenda

Accounting and Analysis: BGP and Autonomous

- Peering Agreement
- Autonomous System
- BGP Next-Hop
- NetFlow Collector 5.0 BGP Features
- BGP Policy Accounting
NetFlow: Peering Agreement

Public Routers 1, 2, 3 Month of September—Outbound Traffic

- Uunet 32%
- Digex
- Erols
- BBN
- AT&T
- AMU
- C&W
- JHU
- PACBell Internet Service
- RCN
- OARnet
- SURAnet
- Compuserve
- OL
- ABSNET
- WebTV
- WEC
NetFlow Autonomous System

Configuring Peer-AS
- Source AS = AS 103
- Destination AS = AS 105

Configuring Origin-AS
- Source AS = AS 101
- Destination AS = AS 106

router(config)#ip flow-export version 5
origin-as record origin AS
peer-as record peer AS
BGP next-hop

- Supported only in version 9 export
- For traffic engineering/analysis (traffic matrix) and possible billing applications
- Fields that are exported include all those found in version 5 export including IP Next Hop
- Adds 16 bytes to each NetFlow flow record (goes from 64 bytes to 80 bytes), while CPU increase is negligible
- Supported in Cisco IOS Software Releases 12.0(15)S, 12.2(14)S, and 12.3(1)
BGP next-hop

- The IGP resolved next hop router 3 so IP next-hop is router 3
- The BGP next-hop is router 5 by default
- If “neighbor a.b.c.d next-hop self” is configured (disables BGP next-hop calculation) then BGP next-hop is router 4
NetFlow Version 9 Configuration

Configuring Version 9 Export

```
pamela(config)# ip flow-export version ?
  1
  5
  9
pamela(config)# ip flow-export version 9
```

Configuring Version 9 Export with BGP Next-Hop

```
pamela(config)# ip flow-export version 9 ?
  bgp-nexthop record BGP NextHop
  origin-as record origin AS
  peer-as record peer AS
  <cr>
pamela(config)# ip flow-export version 9 bgp-nexthop
```
NetFlow BGP Next-Hop TOS Aggregation

- Key fields (uniquely identifies the flow)
  - Origin AS
  - Destination AS
  - Inbound interface
  - DSCP
  - Next BGP hop
  - Output interface

- Additional export fields
  - Flows
  - Packets
  - Bytes
  - Timestamps (sysUptime)

- Note IP Next-Hop isn’t included
- Available now in releases 12.0(26)S, 12.2(18)S and 12.3(1)
Recently Released NetFlow Collector (NFC) 5.0 Has BGP-Specific Enhancements:

- NFC collects NetFlow records and sits as a passive BGP peer to receive full BGP table from router
- Allows for BGP attribute correlation to NFC flow records
- Fields include:
  - BGP AS path
  - BGP Next Hop (if not provided via router)
  - BGP community (in NFC 5.1)
BGP Policy Accounting vs. NetFlow

- BGP Policy Accounting (BGP PA) allows ISP’s to account for IP traffic differentially by assigning counters based on:
  - BGP community-list
  - AS number
  - AS-path
  - Destination IP address
- Counters for up to 64 buckets
- BGP policy accounting uses SNMP (CISCO-BGP-POLICY-ACCOUNTING-MIB and cbpAcctTable)
- NetFlow provides timestamping and flow information (IP, (sub)interfaces, ToS, protocol, TCP Flags, etc.) for each flow
- Cisco NetFlow Collector (NFC) and NetFlow partners can adjunct both BGP community-list and AS-path to NetFlow statistics
Agenda

• Introduction
• Platforms
• Versions
• Accounting and Analysis—MPLS Environment
• Accounting and Analysis—BGP and Autonomous Systems
• Analysis and Attack—Multicast Options
• Attack—Security Features and Applications
• Scaling—Features and Options
• Export—Collector, NAM and Partners
• Evolving NetFlow—IPv6 and Deployment
Agenda

Analysis and Attack—Multicast Options

• Switching Path Implications for NetFlow Multicast
• Multicast—Traditional NetFlow
• Multicast NetFlow Ingress
• Multicast NetFlow Egress
• RPF (Reverse Path Forwarding) Failures
Multicast NetFlow

Three Types of NetFlow Implementations for Multicast Traffic:

1. Traditional NetFlow
2. Multicast NetFlow Ingress
3. Multicast NetFlow Egress
Switching Path Implications for NetFlow Multicast

• Does each outgoing interface generate a separate flow?
• Do the bytes and packets reflect input or output numbers?
Multicast: Traditional NetFlow

Traditional NetFlow Configuration

- **Interface Ethernet 0**
  - `ip route-cache flow`

- **ip flow-export version 9**

- **ip flow-export destination 127.0.0.1 9995**

Flow Record Created in NetFlow Cache

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPadd</th>
<th>DstIf</th>
<th>DstIPadd</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>SrcPort</th>
<th>SrcMsk</th>
<th>DstPort</th>
<th>DstMsk</th>
<th>NextHop</th>
<th>Bytes</th>
<th>Packets</th>
<th>Active</th>
<th>Idle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Null</td>
<td>224.10.10.100</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>00A2</td>
<td>/24</td>
<td>00A2</td>
<td>/24</td>
<td>23100</td>
<td>21</td>
<td>1745</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

- There is only one flow per NetFlow configured input interface
- Destination interface is marked as “Null”
- Bytes and Packets are the *incoming* values

Note: C 6500/7600 Accounts for Multicast Traffic in This Way in PFC3b (Sup720)

(N, G) - (10.0.0.2, 224.10.10.100)

<table>
<thead>
<tr>
<th>10.0.0.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>127.0.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth 1</td>
</tr>
<tr>
<td>Eth 2</td>
</tr>
<tr>
<td>Eth 3</td>
</tr>
</tbody>
</table>

NetFlow Collector Server

ip route-cache flow

ip flow-export version 9

ip flow-export destination 127.0.0.1 9995

Note: C 6500/7600 Accounts for Multicast Traffic in This Way in PFC3b (Sup720)
Multicast NetFlow Ingress (v9)

Multicast NetFlow Ingress Configuration

- Interface Ethernet 0
  - `ip multicast netflow ingress`

- `ip flow-export version 9`

- `ip flow-export destination 127.0.0.1 9995`

Flow Record Created in NetFlow Cache

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPAdd</th>
<th>DstIf</th>
<th>DstIPAdd</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>SrcPort</th>
<th>SrcMsk</th>
<th>DstPort</th>
<th>DstMsk</th>
<th>NextHop</th>
<th>Bytes</th>
<th>Packets</th>
<th>Active</th>
<th>Idle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Null</td>
<td>224.10.10.100</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>00A2</td>
<td>/24</td>
<td>00A2</td>
<td>/24</td>
<td></td>
<td>69300</td>
<td>63</td>
<td>1745</td>
<td>4</td>
</tr>
</tbody>
</table>

- There is only one flow per NetFlow configured input interface
- Destination interface is marked as “Null”
- Bytes and Packets are the **outgoing** values
Multicast NetFlow Egress (v9)

Multicast NetFlow Egress Configuration

- Interface Ethernet 1
  ip multicast netflow egress
- Interface Ethernet 2
  ip multicast netflow egress
- Interface Ethernet 3
  ip multicast netflow egress

- ip flow-export version 9
- ip flow-export destination 127.0.0.1 9995

Flow Records Created in NetFlow Cache

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPAdd</th>
<th>DstIf</th>
<th>DstIPAdd</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>SrcPort</th>
<th>SrcMsk</th>
<th>DstPort</th>
<th>DstMsk</th>
<th>NextHop</th>
<th>Bytes</th>
<th>Packets</th>
<th>Active</th>
<th>Idle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Eth 1</td>
<td>224.10.10.100</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>00A2</td>
<td>/24</td>
<td>00A2</td>
<td>/24</td>
<td>23100</td>
<td>21</td>
<td>1745</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Eth 2</td>
<td>224.10.10.100</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>00A2</td>
<td>/24</td>
<td>00A2</td>
<td>/24</td>
<td>23100</td>
<td>21</td>
<td>1745</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Eth0</td>
<td>10.0.0.2</td>
<td>Eth 3</td>
<td>224.10.10.100</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>00A2</td>
<td>/24</td>
<td>00A2</td>
<td>/24</td>
<td>23100</td>
<td>21</td>
<td>1745</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

- There is one flow per Multicast NetFlow Egress configured output interface
- One of the 7 Key fields that define a unique flow has changed from source interface to destination interface
- Bytes and Packets are the outgoing values
Multicast NetFlow: RPF
(Reverse Path Forwarding) Failures

• If “ip multicast netflow rpf-failure” is configured globally
  packets that have fields that should come from another
  input interface are blocked e.g. source IP and input
  interface doesn’t agree with the routing table

• When this feature is enabled globally:

  Router(config)# ip multicast netflow rpf-failure

  the RPF failures are recorded as flows in the
  NetFlow cache

• Once configured, there will be a new field in the NetFlow
  cache called “RPF Fail” to count flows that fail and how
  many times
Multicast NetFlow: Summary

- Supported via NetFlow version 9 export format
- Performance: Ingress vs. Egress
  Multicast NetFlow Ingress and traditional NetFlow will have similar performance numbers
  Multicast NetFlow Egress will have performance impact that is proportional to the number of interfaces on which it is enabled (include input interfaces)
- Availability
  Cisco IOS Software Releases 12.0(27)S, 12.2(18)S, and 12.3(1)
  Not supported on the Cisco 12000 Series Internet Router
- Cisco Cisco Catalyst 6500 Series and Cisco 7600 Series
  Do not currently support the tracking of multicast traffic via NetFlow due to current ASIC limitation
  Will have this support in a future supervisor
Agenda

• Introduction
• Platforms
• Versions
• Accounting and Analysis—MPLS Environment
• Accounting and Analysis—BGP and Autonomous Systems
• Analysis and Attack—Multicast Options
• **Attack**—Security Features and Applications
• Scaling—Features and Options
• Export—Collector, NAM and Partners
• Evolving NetFlow—IPv6 and Deployment
Agenda

Attack—Security Features and Applications

- What does a DoS Look Like?
- Tracing DoS Attack with NetFlow
- DoS Attack Example: Arbor Networks
- NetFlow MIB
- Tunnels with NetFlow
- How Cisco IT Uses NetFlow
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.xx.6.69 77 aaa 49 194.yy.yy.2 1308 bbb 6 1 40
29 192.xx.6.222 1243 aaa 49 194.yy.yy.2 1774 bbb 6 1 40
29 192.xx.6.108 1076 aaa 49 194.yy.yy.2 1869 bbb 6 1 40
29 192.xx.6.159 903 aaa 49 194.yy.yy.2 1050 bbb 6 1 40
29 192.xx.6.54 730 aaa 49 194.yy.yy.2 2018 bbb 6 1 40
29 192.xx.6.136 559 aaa 49 194.yy.yy.2 1821 bbb 6 1 40
29 192.xx.6.216 383 aaa 49 194.yy.yy.2 1516 bbb 6 1 40
29 192.xx.6.111 45 aaa 49 194.yy.yy.2 1894 bbb 6 1 40
29 192.xx.6.29 1209 aaa 49 194.yy.yy.2 1600 bbb 6 1 40
... ... ... ... ... ... ... ... ...

Typical DoS Attacks Have the Same NetFlow Flow Entries:

- Input Interface (SrcIf)
- Destination IP (DstIf)
- 1 Packet per flow (Pkts)
- Bytes per packet (B/Pk)
Tracing DoS Attack with NetFlow

1. To show high rate flows
   
   `router#show ip cache flow | include (K|M)`

2. To show all flows to one destination leverage
   
   “`router#sh ip cache flow | include <destination>”` example:

   ```
   router#sh ip cache flow | inc 194.yy.yy.2
   ...
   SrcIf  SrcIPaddress  Srp  SrpAS  DstIf  DstIPaddress  DstP  DstAS  Pr  Pkts  B/Pk
   29  192.xx.6.69  77  aaa  49  194.yy.yy.2  1308  bbb  6  1  40
   29  192.xx.6.222  1243  aaa  49  194.yy.yy.2  1774  bbb  6  1  40
   29  192.xx.6.108  1076  aaa  49  194.yy.yy.2  1869  bbb  6  1  40
   29  192.xx.6.159  903  aaa  49  194.yy.yy.2  1050  bbb  6  1  40
   ...
   ```

3. To look for known attack signatures e.g. if we know of an attack using UDP port 666 (Hex 029A) we run
   
   `router#show ip cache flow | inc 029A`
DoS: Technical Alternatives after NetFlow

- **ACLs**
  - Manual
  - Performance impact

- **Unicast Reverse Path Forwarding (uRPF)**
  - Automate with BGP
  - Only stops nonexisting sources

- **CAR:**
  - Automate via QPPB (QoS Policy Propagation with BGP)
  - Performance impact
DoS: Administrative Alternatives after NetFlow

• If source address of flow is not spoofed (falsified):
  
  Use Routing table for prefix from which IP source comes
  (“show ip route <source ip>” and/or “show ip cef <source ip>”)

  For source IP or source/peer AS use Internet Routing Registry
  (IRR: Europe whois.ripe.net, Asia-Pac whois.apnic.net, USA and
  rest whois.arin.net)

  direct site contact (abuse@domain)

• If source address of flow is spoofed (falsified):
  
  Trace packet flow back through the network using NetFlow

  Find upstream ISP via NetFlow incoming interface on edge router

  Upstream ISP needs to continue the tracing
DoS Attack Example: Arbor Networks

1. Profile: Baseline Traffic Patterns in the Network
2. Monitor: Analyze Traffic for Anomalies
3. Detect: Forward Anomaly Fingerprints to Controllers
4. Trace: Trace the Attack to Its Source
5. Filter: Recommends Filters (X)

Configure NetFlow Export to Arbor DoS Collector(s)
NetFlow MIB

- Snapshot of current ‘live’ NetFlow cache via SNMP
- Administration and configuration of NetFlow using the MIB interface
- NetFlow MIB cannot be used to retrieve all flow information due to scalability
- Example objects available:
  - Packet size distribution
  - Number of bytes exported per second
  - Number of flows
- This is targeted at Denial of Service (DoS) attacks, security monitoring and remote locations where export to a local NetFlow collector is not possible
- Available now in Release 12.3(7)T
Powerful Insight into Tunnels with NetFlow

- NetFlow lets you break out both pre and post encryption
- Support for both GRE and IPSec encryption
- Tested with 12.3 images
How Cisco IT Uses NetFlow

- Characterize IP traffic and account for how and where it flows
  - Total avoidance of SQL slammer worm
  - Transitioned from managed DSL service to internet VPN
  - Detection of unauthorized WAN traffic
  - Validation of QoS parameters and BW allocation
  - Analysis of VPN traffic and tele-commuter behavior
  - Calculating total cost of ownership for applications

<table>
<thead>
<tr>
<th>Use of NetFlow</th>
<th>NMS and Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Monitoring</td>
<td>Network Traffic Analysis by Application with BGP; Anomaly Detection Arbor Networks</td>
</tr>
<tr>
<td>WAN Aggregation and Edge</td>
<td>Network Traffic Analysis by Application, for Capacity Planning Using NetQOS</td>
</tr>
<tr>
<td>Core routers and Nat Gateway</td>
<td>Collection of Historical Data, Useful for Forensics and Diagnostics with Flow Tools</td>
</tr>
</tbody>
</table>
Agenda

- Introduction
- Hardware
- Versions
- Accounting and Analysis—MPLS Environment
- Accounting and Analysis—BGP and Autonomous Systems
- Analysis and Attack—Multicast Options
- Attack—Security Features and Applications
- Scaling—Features and Options
- Export—Collector, NAM and Partners
- Evolving NetFlow—IPv6 and Deployment
Agenda

Scaling—Features and Options

• Memory Utilization
• Sampled NetFlow
• Enabling NetFlow on SubInterface
• NetFlow Input Filters
• NetFlow Performance
• Advice—Reducing Performance Impact
• Advice—Deployment
## Memory Utilization

- A NetFlow cache entry (a single flow) is 64 bytes

<table>
<thead>
<tr>
<th>Platform</th>
<th>Default NetFlow Cache Size (Entries)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2600</td>
<td>4k</td>
</tr>
<tr>
<td>3600</td>
<td>4k</td>
</tr>
<tr>
<td>3700</td>
<td>4k</td>
</tr>
<tr>
<td>7200 w/ 64MB DRAM</td>
<td>64k</td>
</tr>
<tr>
<td>7200 w/ 128MB DRAM</td>
<td>128k</td>
</tr>
<tr>
<td>7500 w/ 64MB DRAM</td>
<td>64k</td>
</tr>
<tr>
<td>7500 w/ 128MB DRAM</td>
<td>128k</td>
</tr>
<tr>
<td>Cisco Catalyst 6500 Series and Cisco 7600 Series Sup1/PFC1</td>
<td>32k</td>
</tr>
<tr>
<td>Cisco Catalyst 6500 Series and Cisco 7600 Series Sup2/PFC2</td>
<td>32k</td>
</tr>
<tr>
<td>C6500 / 7600 Sup720/PFC3b</td>
<td>256k</td>
</tr>
<tr>
<td>12000 w/ 64MB DRAM</td>
<td>64k</td>
</tr>
<tr>
<td>12000 w/ 128MB DRAM</td>
<td>64k</td>
</tr>
</tbody>
</table>

**Configuration:**
```
router(config-if)#ip flow-cache entries <number>
```
Sampled NetFlow

- **Deterministic**
  - Original type
    - Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router (Release 12.1(13)E)
    - Cisco 12000 Series Internet Router (Releases 12.0(11)S and 12.0(14)ST)
- **Random (recommended per statistical principles)**
  - Releases 12.0(26)S, 12.2(18)S, and 12.3(2)T
  - Cisco 12000 Cisco 12000 Series Internet Router (Release 12.0(28)S)
- **Time-based**
  - Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router (Release 12.1(13)E)
Sampling Accuracy

DETERMINISTIC SAMPLING
Sampling Interval: 1 in 5 Packets
Missed Flows: 2 out of 5  ■  ■  (35%)

RANDOM SAMPLING
Sampling Interval: 1 in 5 Packets
Random Sampling Overcomes Rhythmic Network Patterns
Cisco Catalyst 6500 Series and Cisco 7600 Series Sampled NetFlow

- Support for both time and (packet-based) deterministic sampling
- Sampling rate is configurable only for the whole box
- Accuracy of NetFlow on the platform comes from tuning the aging timers correctly
- A way of minimizing packet loss, is using Distributed Forwarding Card (DFC) cards, spreading the incoming packet load evenly onto different VLANs on different cards
- Currently available in Release 12.1(13)E
## Cisco 12000 Series Internet Routers
### Sampled NetFlow

<table>
<thead>
<tr>
<th>Engine</th>
<th>“Full” NetFlow</th>
<th>Sampled NetFlow</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>1</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>2</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>3</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>4</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>4+</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Despite ASIC Support in Engine 2, 3 and 4+ Linecards ‘Full NetFlow’ Still Inflicts a Heavy Burden on Memory and Therefore Sampled NetFlow Is Preferred
Configuring NetFlow onto Subinterface

- Receive NetFlow information only on the specific subinterface(s) of interest
- Reduces CPU and memory impact on router as well as export traffic and collector sizing needs

```
Router(config-if)#ip flow ingress
```

- New “ip flow ingress” command is easier to distinguish between egress NetFlow commands
- Same “ip flow ingress” command can now be used to configure NetFlow on the main interface
- Available now in Releases 12.2(14)S and 12.2(15)T

Note: NetFlow Has Always Exported Subinterface Information
NetFlow Input Filters: Overview

• Pre-filters traffic prior to NetFlow processing
• Modular QoS CLI (MQC) provides the filtering mechanism for NetFlow classification by:
  - IP source and destination addresses
  - Layer 4 protocol and port numbers
  - Incoming interface
  - ToS byte (includes DSCP and IP precedence)
  - MAC address
  - Layer 2 information (such as Frame Relay DE bits or Ethernet 802.1p bits)
  - Network-Based Application Recognition (NBAR)
• Ability to sample filtered data at different rates, depending on how interesting the traffic is
• Currently available in Release 12.3(4)T
NetFlow Input Filters: Example

- **Packets**
  - VOIP
    - Tight Filter for Traffic of High Importance
    - 1:1 Sampling
  - VPN
    - Moderately-Tight for Traffic of Medium Importance
    - 1:100 Sampling
  - Best Effort
    - Default Wide Open Filter for Traffic of Low Importance
    - 1:10000 Sampling

- NetFlow Cache

New
NetFlow Input Filters

- Flow filter prevents flows from entering NetFlow cache
- Increases scalability and decreases CPU usage
- Filters are based on MQC class maps
- User can match flows from a certain port/source with ACL
- Define traffic class (match ACL) and flow sampling per match
- Available now in Release 12.3(4)T

Diagram:

- Packets
- Traffic Filter High Importance: Sample 1:1 from Server B
- Traffic Filter Low Importance: Sample 1:100 from Subnet A
NetFlow Performance Paper Tests

- Access lists (ACLs) 200 and 500 lines
- 0, 1, and 2 NetFlow data export destinations
- Initial performance after enabling
- V8 Aggregation vs. v5
- Configuring AS origin or peer
- Policy Based-Routing (PBR)
- “Full” NetFlow vs. 1:100 sampled NetFlow
- Hardware: Cisco 2600, 3600, 7200 NPE-400 and NSE-1, 7500 RSP8 VIP4-80 with CEF and dCEF, 12000 Engine 1 Linecard dCEF
NetFlow Performance Paper Conclusions

• Additional CPU utilization

<table>
<thead>
<tr>
<th>Number of Active Flows</th>
<th>Additional CPU Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>10,000</td>
<td>&lt;4%</td>
</tr>
<tr>
<td>45,000</td>
<td>&lt;12%</td>
</tr>
<tr>
<td>65,000</td>
<td>&lt;16%</td>
</tr>
</tbody>
</table>

• NetFlow data export (single/dual)
  
  No significant impact

• NetFlow v5 vs. v8: little or not impact

• NetFlow feature acceleration:
  
  >200 lines of ACLs and/or Policy Based-Routing (PBR)

• NetFlow vs. sampled NetFlow on the Cisco 12000 series internet routers
  
  23% vs. 3% (65,000 flows, 1:100)
Performance Testing NetFlow Version 9

- Similar CPU and throughput numbers result from configuration of both NetFlow version 5 and 9
- CPU is slightly higher immediately following initial boot up or configuration
  
  Caused by sending template flowsets to collector
- BGP Next-Hop performance is almost identical to v5 results, however MPLS-aware NetFlow is a bit more
NetFlow Performance Summary

- Enabling NetFlow version 5 and exporting increases the CPU utilization by around 15%
  Maximum of 20% depending on the hardware
- Enabling NetFlow version 8 increases the CPU utilization by 2 to 5% above version 5, depending on the number of aggregations enabled with a multiple of 6% for multiple aggregations
- NetFlow is done in hardware on the Cisco Catalyst 6500 Series supervisor; only the export takes CPU cycles
- NetFlow version 9: similar results as version 5
- Memory usages is 64 bytes per flow; so to have room for 64,000 flows 4 MB of DRAM is required
Technical Advice: Reducing Performance Impact

Reduce CPU and memory impact on the router, collector, or network:

- Aging timers
- Sampled NetFlow
- Leverage distributed architectures (VIP, Linecards)
- Flow masks (only Cisco Catalyst 6500 Series and Cisco 7600 Series)
- Enable on specific subinterface
- Aggregation schemes (v8 on router or on collector)
- Filters (router or collector)
- Data compression (collector)
- Increase collection bucket sizes (collector)
- Collector and router can be placed on the same LAN segment (network)
Agenda

• Introduction
• Hardware
• Versions
• Accounting and Analysis—MPLS Environment
• Accounting and Analysis—BGP and Autonomous Systems
• Analysis and Attack—Multicast Options
• Attack—Security Features and Applications
• Scaling—Features and Options
• Export—Collector, NAM and Partners
• Evolving NetFlow—IPv6 and Deployment
Agenda

Export—Collector, NAM and Partners

- NetFlow Multiple Export Destinations
- NetFlow Collector (NFC)
- NFC 5.0
- NetFlow Partners
- NAM
- Troubleshooting
NetFlow Multiple Export Destinations

- Two identical streams of NetFlow data are sent to the two destination hosts (collectors); currently the limit is two destinations

  ```
  router(config)#ip flow-export destination 1.1.1.1 9996
  router(config)#ip flow-export destination 2.2.2.2 9997
  ```

- Main and aggregation caches supported
- Available now in Releases 12.0(19)S, 12.0(19)ST, 12.2(2)T, and 12.2(14)S
- Available in Cisco Catalyst 6500 Series and Cisco 7600 Series in Cat 8.3 and Release 12.2(14)S on MSFC3 and Sup720
NFC Overview

What Does NFC Do?

• Collect (ASCII or binary)
• Filter
• Aggregate (standard selection or cafeteria)
• Compress
• Integrate external data into output e.g. adding BPG attributes
• Map ranges of values from one or more fields to user-defined strings
• Web-based GUI (NFC 5.0) to sort, graph, export, filter, and drill down on report data
• Export e.g. .csv export to MS Excel
NFC 5.0 Features

What Is New in NFC 5.0?

- Web-based user interface
- XML configuration
- Report generator
- MPLS/VPN PE-PE traffic reports
- BGP peer for attribute correlation
- Interface name mapping
- DNS lookup
- MPLS/EXP support
- Self-describing header
- Generic field mapping
- Max burst rate support
- V5 sampled NetFlow header support
- Enhanced logging
- IPv6 support

Platform Requirements:

- Solaris 8/9
- HP-UX 11i
- Red Hat Enterprise Linux

Note: 2-4 GB RAM and Dual Processors Recommended
NFC 5.0 Key Features: Web-Based Interface

NFC Reports Provide the User with the Ability to Sort, Graph, Export, Filter, and Drill Down on Report Data
# NetFlow Partners

## Traffic Analysis
- Arbor Networks
- Micromuse
- HP
- InfoVista
- NetQoS
- Concord
- Quallaby
- Caida
- Crannog Software
- Evident Software
- WiredCity
- Adlex

## Collection
- Flow-Tools
- Xacct
- Narus
- Caida
- NetQoS
- Micromuse
- Crannog Software

## Denial of Service
- Arbor Networks
- Micromuse
- HP
- InfoVista
- NetQoS
- Concord
- Quallaby
- Caida
- Crannog Software
- Evident Software
- WiredCity
- Adlex

## Billing
- Portal
- Digiquant
- NetQoS
NetFlow on the Network Analysis Module (NAM)

- NetFlow collection and analysis combined
- Instant results ie. ‘plug-and-play’
- NAM offers powerful combination of NetFlow and RMON (mini-RMON, RMON1, RMON2, HCMON, SMON, and DSMON)
- RMON2 can provide additional application level visibility (L5-7)
- ART—Application Response Time MIB
- Packet decoding
- Detail analysis of traffic of interest

### RMON/NetFlow Support in NAM GUI

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>RMON and NF</td>
</tr>
<tr>
<td>Hosts</td>
<td>RMON and NF</td>
</tr>
<tr>
<td>Conversations</td>
<td>RMON and NF</td>
</tr>
<tr>
<td>Voice</td>
<td>RMON</td>
</tr>
<tr>
<td>VLAN</td>
<td>RMON</td>
</tr>
<tr>
<td>ART</td>
<td>RMON</td>
</tr>
<tr>
<td>DiffServ</td>
<td>RMON</td>
</tr>
<tr>
<td>Portstats</td>
<td>RMON</td>
</tr>
</tbody>
</table>
Plug-and-Play with NAM Web-Based GUI

Bar Charts, Pie Charts, Usage, etc…

Troubleshooting

Drill Down

Setting Alarm Thresholds
Troubleshooting: Missing Flows?

1) Router Problem
   Cache (show ip cache flow)
   Export (show ip flow export)

2) NetFlow Collector Problem
   Show tech-support
   netstat -s

3) Transfer Problem
   (Only Remaining Explanation)
Missing Flows? (1) Router Problem (Cache)

Router#sh ip cache flow (excerpt)
IP Flow Switching Cache, 4456704 bytes
2 active, 65534 inactive, 226352 added
3792086 ager polls, 0 flow alloc failures
Active flows timeout in 40 minutes
Inactive flows timeout in 20 seconds
82038 flows exported in 34439 udp datagrams, 0 failed
last clearing of statistics 00:14:23

- **Alloc failures**: number of times the NetFlow code tried to allocate a flow but could not
- **Failed**: number of flows that could not be exported by the router because of output interface limitations
Missing Flows? (1) Router Problem (Export)

Router#sh ip flow export
   Flow export is enabled
   Exporting flows to 151.99.57.3 (9996)
   Exporting using source interface Loopback0
   Version 5 flow records, origin-as
   2304658131 flows exported in 219987515 udp datagrams
   0 flows failed due to lack of export packet
   167 export packets were sent up to process level
   0 export packets were punted to the RP
   3490 export packets were dropped due to no fib
   7012 export packets were dropped due to adjacency issues
   0 export packets were dropped enqueuing for the RP
   0 export packets were dropped due to IPC rate limiting
   0 export packets were dropped due to output drops
Missing Flows?
(2) NetFlow Collector Problem

• The NetFlow collector “show tech-support”

  udpPort: 9996, receivedFlows: 80277(0),
  receivedFlowrecords: 1771469(0)
  discardedFlows: 0, missedFlowrecords: 1115(0),
  socNum: 13, rcvQSize: 26000

• The NetFlow collector “netstat –s”

  udpInDatagrams = 14034  udpInErrors = 0
  udpInCksumErrs = 0  udpInOverflows = 3218
Agenda

• Introduction
• Hardware
• Versions
• Accounting and Analysis—MPLS Environment
• Accounting and Analysis—BGP and Autonomous Systems
• Analysis and Attack—Multicast Options
• Attack—Security Features and Applications
• Scaling—Features and Options
• Export—Collector, NAM and Partners
• Evolving NetFlow—IPv6 and Deployment
Agenda

Evolving NetFlow—IPv6 and Futures

• IPv6
• Deployment
• Summary
NetFlow and IPv6

- Based on NetFlow version 9
- Support for both ingress and egress traffic
- "Full NetFlow" i.e. non-sampled
- Data export is currently still IPv4
- Available now in Release 12.3(7)T
NetFlow Deployment: Rules of Thumb

• Aggregate on router/switch rather than on the collector
• If exporting version 8 on router don’t also export another version (7, 8 or 9)
• Data export over a dedicated interface/VLAN for easier troubleshooting and management
• Keep collector on LAN interface 1 hop away:
  Avoid drops
  WAN interfaces have less bandwidth to afford
• NetFlow export creates ~1% to 1.5% of the interface throughput that NetFlow is enabled on
NetFlow Deployment: Thoughts

Packets Will Create the Identical Flow Information at Each Router/Switch Along Its End-to-End Journey, with the Exception of the Incoming Interface

Edge NetFlow positives:
• Interface is key field
• Full NetFlow and sampled NetFlow options
• Account for all CE/end user traffic

Edge considerations:
• IP addressing pre or post NAT
• Collectors:
  a) # required
  b) locations
  c) aggregating all data

Core NetFlow positives:
• TCP flags tracking on 12000
• IP addressing pre or post NAT
• Collectors can be centrally located

Core considerations:
• Amount of collection information
• Is all information accounted for
The Needs

- **Accounting**: Primary Cisco accounting technology; Current economic environment drives need to cost-justify, and charge for IT network rollout/service provider premium services

- **Analysis**: Key Cisco IOS network management feature
  - **Traffic matrix**: Primary technology for building core traffic matrices

- **Attack**: Primary technology for identifying denial of service attacks
The Tools

- Comprehensive hardware support
- Versions 5, 7, 8 and 9
- Four MPLS technology alternatives
- Five BGP technology options
- Three multicast technology alternatives
- Denial of service and IPSec options
- Scaling features and options
- Export—Collector, NAM and Partners
NetFlow Summary

• NetFlow is a mature Cisco IOS feature (in Cisco IOS since 1996)
• Cisco has IETF/industry leadership
• Version 9 eases the exporting of additional fields
• A lot of new features have been added
References

• NetFlow
  www.cisco.com/go/netflow

• Cisco Network Accounting Services
  Comparison of Cisco NetFlow versus other available accounting technologies

• Cisco IT Case Study
  business.cisco.com/prod/tree.taf%3Fasset_id=106882&IT=104252&public_view=true&kbns=1.html

• Cisco NetFlow Collector/Analyzer
  www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/index.htm
Complete Your Online Session Evaluation!

**WHAT:** Complete an online session evaluation and your name will be entered into a daily drawing

**WHY:** Win fabulous prizes! Give us your feedback!

**WHERE:** Go to the Internet stations located throughout the Convention Center

**HOW:** Winners will be posted on the onsite Networkers Website; four winners per day