What You Make Possible
Advanced NetFlow
BRKNMS-3132
Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions and Meet the Engineer
- Visit the Cisco Store to purchase your recommended readings
- Please switch off your mobile phones
- After the event don’t forget to visit Cisco Live Virtual: www.ciscolivevirtual.com
Session Abstract

- This advanced session by the author of a Cisco Press book on the same subject presents the latest NetFlow developments: new features, NetFlow version 9, and its standardization at the IETF. The new Flexible NetFlow feature is covered in detail. Technical details of the new features are addressed with configuration examples, show commands, tricks, and best practice advice. Scenarios such as NetFlow for security and NetFlow for capacity planning are covered. The NetFlow performance impact is also discussed, as well as the support matrix of all NetFlow features.

- This session is for enterprise, service provider, and NREN experts engaged in designing, maintaining, and troubleshooting security, capacity planning, and accounting solutions. Attendees should be familiar with network management basics and should already have some understanding of NetFlow, perhaps by already having taken the introductory session.
The Content of This Session Is...

- **Not about**
  - A level one type of presentation
  - Introduction to IP accounting and NetFlow
  - Marketing slides
  - NetFlow collector details
  - The ecosystem partners applications and mediations
  - Many platform specific details

- **About**
  - New features
  - Advanced information
  - And a few scenarios ...
  - Assuming the NetFlow basics are known
Agenda

- Introduction
- NetFlow Version 9
- Flexible NetFlow
- NetFlow for Security
- NetFlow for Application Visibility and Control
- NetFlow & IP v6
- NetFlow Performance
- NetFlow Standardization
- Support Matrix
- Conclusion
Version 5 Flow Format

Flow Key vs. Non-Key Field

- Packet count
- Byte count
- Start sysUpTime
- End sysUpTime
- Input ifIndex
- Output ifIndex
- Type of service
- TCP flags
- Protocol
- Source IP address
- Destination IP address
- Source TCP/UDP port
- Destination TCP/UDP port
- Next hop address
- Source AS number
- Dest. AS number
- Source prefix mask
- Dest. Prefix mask

Usage
- From/to

Time of Day

Port Utilization

QoS

Routing and Peering

From/to

Application

Routing and Peering
1. Create and update flows in NetFlow cache

<table>
<thead>
<tr>
<th>SrcIPadd</th>
<th>DstIPadd</th>
<th>Protocol</th>
<th>TOS</th>
<th>Flgs</th>
<th>Pkts</th>
<th>Src Port</th>
<th>Src Msk</th>
<th>Dst Port</th>
<th>Dst Msk</th>
<th>NextHop</th>
<th>Bytes/Pkt</th>
<th>Active</th>
<th>Idle</th>
</tr>
</thead>
<tbody>
<tr>
<td>173.100.21.2</td>
<td>10.0.227.12</td>
<td>11</td>
<td>80</td>
<td>10</td>
<td>11000</td>
<td>00A2 /24</td>
<td>5</td>
<td>00A2 /24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1528</td>
<td>1745</td>
<td>4</td>
</tr>
<tr>
<td>173.100.3.2</td>
<td>10.0.227.12</td>
<td>6</td>
<td>40</td>
<td>0</td>
<td>2491</td>
<td>15 /26</td>
<td>196</td>
<td>15 /24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>740</td>
<td>41.5</td>
<td>1</td>
</tr>
<tr>
<td>173.100.20.2</td>
<td>10.0.227.12</td>
<td>11</td>
<td>80</td>
<td>0</td>
<td>10000</td>
<td>00A1 /24</td>
<td>180</td>
<td>00A1 /24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1428</td>
<td>1145.5</td>
<td>3</td>
</tr>
<tr>
<td>173.100.6.2</td>
<td>10.0.227.12</td>
<td>6</td>
<td>40</td>
<td>0</td>
<td>2210</td>
<td>19 /30</td>
<td>180</td>
<td>19 /24</td>
<td>15</td>
<td>10.0.23.2</td>
<td>1040</td>
<td>24.5</td>
<td>14</td>
</tr>
</tbody>
</table>

2. Expiration

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

3. Aggregation

4. Export version

Non-aggregated flows—export version 5 or 9

5. Transport protocol

(UDP, SCTP)
NetFlow Export Version 5 and Main Cache
Configuration Example

Router(config)# interface <slot/port/subinterface>
Router(config-if)# ip flow ingress
Router(config-if)# ip flow egress

Router(config)# ip flow-cache entries <number>
Router(config)# ip flow-cache timeout active <minutes>
Router(config)# ip flow-cache timeout inactive <seconds>

Router(config)# ip flow-export version 5 peer-as
Router(config)# ip flow-export destination 10.10.10.10 1234
Router(config)# ip flow-export source loopback 0
NetFlow Flow Keys on the Router

- By default, the 7 flow keys are:
  - Source IP address, destination IP address, source port, destination port, Layer 3 protocol type, TOS byte (DSCP), input interface

- The 12 NetFlow aggregations allow to reduce/change the number of flow keys
  - Example: source prefix aggregation = source network, source interface
  - Can be seen as a different view of the main cache

- Egress NetFlow, MPLS-aware NetFlow, etc.
  - Will specify new flow keys

- Note: on the Cisco Catalyst®, we speak of the flow mask
  - Define the flow keys
## Flow Keys on the Cisco Catalyst 6500/7600

### The Flow Mask

<table>
<thead>
<tr>
<th>Flow Keys in Orange</th>
<th>VLAN</th>
<th>SRC IP</th>
<th>DST IP</th>
<th>IP Protocol</th>
<th>Src Port</th>
<th>Dst Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full-Interface</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Full</strong></td>
<td>VLAN</td>
<td>SRC IP</td>
<td>DST IP</td>
<td>IP Protocol</td>
<td>Src Port</td>
<td>Dst Port</td>
</tr>
<tr>
<td><strong>Destination-Source-Interface</strong></td>
<td>VLAN</td>
<td>SRC IP</td>
<td>DST IP</td>
<td>IP Protocol</td>
<td>Src Port</td>
<td>Dst Port</td>
</tr>
<tr>
<td><strong>Source-Only</strong></td>
<td>VLAN</td>
<td>SRC IP</td>
<td>DST IP</td>
<td>IP Protocol</td>
<td>Src Port</td>
<td>Dst Port</td>
</tr>
<tr>
<td><strong>Destination-Only</strong></td>
<td>VLAN</td>
<td>SRC IP</td>
<td>DST IP</td>
<td>IP Protocol</td>
<td>Src Port</td>
<td>Dst Port</td>
</tr>
<tr>
<td><strong>Destination-Source</strong></td>
<td>VLAN</td>
<td>SRC IP</td>
<td>DST IP</td>
<td>IP Protocol</td>
<td>Src Port</td>
<td>Dst Port</td>
</tr>
</tbody>
</table>
Extensibility and Flexibility Requirements
Phases Approach

- Traditional NetFlow with the v5 or v8 NetFlow export
  - New requirements: build something flexible and extensible

- Phase One: NetFlow Version 9
  - Advantages: extensibility
    Integrate new technologies/data types quicker (MPLS, IPv6, BGP next hop, etc.)
    Integrate new aggregations quicker
  - Note: for now, the template definitions are fixed

- Phase Two: Flexible NetFlow
  - Advantages: cache and export content flexibility
    User selection of flow keys
    User definition of the records
NetFlow Partners

Traffic Analysis

Denial of Service

Billing

# NetFlow Open Source Tools

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Primary Use</th>
<th>Comment</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cflowd</td>
<td>Traffic Analysis</td>
<td>No longer supported</td>
<td>UNIX</td>
</tr>
<tr>
<td>Flow-tools</td>
<td>Collector Device</td>
<td>Scalable</td>
<td>UNIX</td>
</tr>
<tr>
<td>Flowd</td>
<td>Collector Device</td>
<td>Support V9</td>
<td>BSD, Linux</td>
</tr>
<tr>
<td>FlowScan</td>
<td>Reporting for Flow-Tools</td>
<td></td>
<td>UNIX</td>
</tr>
<tr>
<td>IP Flow</td>
<td>Traffic Analysis</td>
<td>Support V9, IPv4, IPv6, MPLS, SCTP, etc.</td>
<td>Linux, FreeBSD, Solaris</td>
</tr>
<tr>
<td>NetFlow Guide</td>
<td>Reporting Tools</td>
<td></td>
<td>BSD, Linux</td>
</tr>
<tr>
<td>NetFlow Monitor</td>
<td>Traffic Analysis</td>
<td>Supports V9</td>
<td>UNIX</td>
</tr>
<tr>
<td>Netmet</td>
<td>Collector Device</td>
<td>V5, support v9</td>
<td>Linux</td>
</tr>
<tr>
<td>NTOP</td>
<td>Security Monitoring</td>
<td></td>
<td>UNIX</td>
</tr>
<tr>
<td>Stager</td>
<td>Reporting for Flow-Tools</td>
<td></td>
<td>UNIX</td>
</tr>
<tr>
<td>Nfdump/nfsen</td>
<td>Traffic Analysis</td>
<td>Support V5 and v9</td>
<td>UNIX</td>
</tr>
</tbody>
</table>

Different costs: implementation and customization
Agenda

- Introduction
- NetFlow Version 9
- Flexible NetFlow
- NetFlow for Security
- NetFlow for Application Visibility and Control
- NetFlow & IP v6
- NetFlow Performance
- NetFlow Standardization
- Support Matrix
- Conclusion
NetFlow Version 9

- Version 9 is an export protocol
  - No changes to the metering process
- Version 9 is 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, ISR (1800, 2800, 3800), ISR-G2 (1900, 2900, 3900), 2600, 3200, 3600, 3750, cat4500, cat6500, 7200, 7300, 7500, 7600, 10000, 12000 (IOS and IOS-XR), CRS-1, ASR 1000, ASR 9000, ASA 5580, Nexus 7000 and Nexus 1000V
- RFC 3954 Cisco Systems® NetFlow Services Export Version 9
  - NetFlow patent: intellectual property right statement at the IETF website
NetFlow Version 9 Export Packet

Template FlowSet
- Template Record
  - Template ID #1
    (Specific Field Types and Lengths)
  - Template ID #2
    (Specific Field Types and Lengths)

Data FlowSet
- FlowSet ID #1
  - Data Record
    (Field Values)
  - Data Record
    (Field Values)

Data FlowSet
- FlowSet ID #2
  - Data Record
    (Field Values)
NetFlow Version 9 Export Packet

Options Template FlowSet Specifies the Scope: Cache, System, Template, etc.

**Template 3**

**Options Template FlowSet**

- Option Template Record
  - Template ID #3
  - (Specific Scope, Field Types and Lengths)

**Data FlowSet**

- FlowSet ID #3
  - OptionData Record (Field Values)
  - OptionData Record (Field Values)
Interface Name Export with NetFlow Version 9

- Example of options template FlowSet
- NetFlow exports the ifIndex
- Instead of the collector polling the ifName MIB variable for a specific ifIndex, the matching (ifIndex, ifName) is sent in an option data record

Router(config)# ip flow-export interface-names
NetFlow Version 9
Main Cache Configuration

- Should you export from the main cache with NetFlow Version 5 or Version 9?
NetFlow Version 9
Aggregation Cache Configuration

```
router(config)# ip flow-aggregation cache bgp-nexthop-tos
router(config-flow-cache)# export destination 11.11.11.11 9999
router(config-flow-cache)# export version ?
  9 Version 9  export format
router(config-flow-cache)# export version 9
router(config-flow-cache)# enabled
```

In this case, we have only version 9. Why?
Agenda

• Introduction
• NetFlow Version 9
• Flexible NetFlow
• NetFlow for Security
• NetFlow for Application Visibility and Control
• NetFlow & IP v6
• NetFlow Performance
• NetFlow Standardization
• Support Matrix
• Appendix
Typical NetFlow Deployment

- NetFlow for Security
- NetFlow for Monitoring
- NetFlow for Core Traffic
- Matrix
- NetFlow for Peering
- Managed Services: Application Visibility

ISP
Flexible NetFlow
Multiple Monitors with Unique Key Fields

Traffic Analysis Cache

<table>
<thead>
<tr>
<th>Key Fields</th>
<th>Packet 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>3.3.3.3</td>
</tr>
<tr>
<td>Destination IP</td>
<td>2.2.2.2</td>
</tr>
<tr>
<td>Source Port</td>
<td>23</td>
</tr>
<tr>
<td>Destination Port</td>
<td>22078</td>
</tr>
<tr>
<td>Layer 3 Protocol</td>
<td>TCP - 6</td>
</tr>
<tr>
<td>TOS Byte</td>
<td>0</td>
</tr>
<tr>
<td>Input Interface</td>
<td>Ethernet 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-Key Fields</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td></td>
</tr>
<tr>
<td>Bytes</td>
<td></td>
</tr>
<tr>
<td>Timestamps</td>
<td></td>
</tr>
<tr>
<td>Next Hop Address</td>
<td></td>
</tr>
</tbody>
</table>

Security Analysis Cache

<table>
<thead>
<tr>
<th>Key Fields</th>
<th>Packet 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>3.3.3.3</td>
</tr>
<tr>
<td>Dest IP</td>
<td>2.2.2.2</td>
</tr>
<tr>
<td>Source Port</td>
<td>23</td>
</tr>
<tr>
<td>Destination Port</td>
<td>22078</td>
</tr>
<tr>
<td>Layer 3 Protocol</td>
<td>TCP - 6</td>
</tr>
<tr>
<td>TOS Byte</td>
<td>0</td>
</tr>
<tr>
<td>Input Interface</td>
<td>Ethernet 0</td>
</tr>
<tr>
<td>SYN Flag</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-Key Fields</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td></td>
</tr>
<tr>
<td>Timestamps</td>
<td></td>
</tr>
</tbody>
</table>

Traffic Analysis Cache

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>Source Port</th>
<th>Dest. Port</th>
<th>Protocol</th>
<th>TOS</th>
<th>Input I/F</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>2.2.2.2</td>
<td>23</td>
<td>22078</td>
<td>6</td>
<td>0</td>
<td>E0</td>
<td>1100</td>
</tr>
</tbody>
</table>
Flexible NetFlow Model

- A single record per monitor
- Potentially multiple monitors per interface
- Potentially multiple exporters per monitor
Service Planning
FNF Configuration – Example

1. Configure the Exporter
Router(config)# flow exporter my-exporter
Router(config-flow-exporter)# destination 1.1.1.1

2. 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

3. Configure the Flow Monitor
Router(config)# flow monitor my-monitor
Router(config-flow-monitor)# exporter my-exporter
Router(config-flow-monitor)# record my-record

4. Apply to an Interface
Router(config)# interface s3/0
Router(config-if)# ip flow monitor my-monitor input
Flexible NetFlow
User-Defined Record Configuration

Router(config)# flow record my-record
Router(config-flow-record)# match
Router(config-flow-record)# collect

Router(config-flow-record)# match ?
application Application Fields
datalink Datalink (layer 2) fields
flow Flow identifying fields
interface Interface fields
ipv4 IPv4 fields
ipv6 IPv6 fields
routing routing attributes
transport Transport layer field

Router(config-flow-record)# collect ?
application Application Fields
counter Counter fields
datalink Datalink (layer 2) fields
flow Flow identifying fields
interface Interface fields
ipv4 IPv4 fields
ipv6 IPv6 fields
routing IPv4 routing attributes
timestamp Timestamp fields
transport Transport layer fields

Specify a Key Field
Specify a Non-Key Field
# Flexible Flow Record: Key Fields

## Flow
- Sampler ID
- Direction

## Interface
- Input
- Output

## Layer 2
- Source VLAN
- Dest VLAN
- Dot1q VLAN
- Dot1q priority
- 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**
- **Options bitmap**
- **Fragmentation Offset**
- **Version**
- **Identification**
- **Precedence**
- **Header Length**
- **DSCP**
- **Total Length**
- **TOS**

## 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**
## Flexible Flow Record: Key Fields

<table>
<thead>
<tr>
<th><strong>Routing</strong></th>
<th><strong>Transport</strong></th>
<th><strong>Application</strong></th>
<th><strong>Multicast</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>src or dest AS</td>
<td>Destination Port</td>
<td>TCP Flag: ACK</td>
<td>Replication Factor*</td>
</tr>
<tr>
<td>Peer AS</td>
<td>Source Port</td>
<td>TCP Flag: CWR</td>
<td>RPF Check Drop*</td>
</tr>
<tr>
<td>Traffic Index</td>
<td>ICMP Code</td>
<td>TCP Flag: ECE</td>
<td>Is-Multicast</td>
</tr>
<tr>
<td>Forwarding Status</td>
<td>ICMP Type</td>
<td>TCP Flag: FIN</td>
<td></td>
</tr>
<tr>
<td>IGP Next Hop</td>
<td>IGMP Type*</td>
<td>TCP Flag: PSH</td>
<td></td>
</tr>
<tr>
<td>BGP Next Hop</td>
<td>TCP ACK Number</td>
<td>TCP Flag: RST</td>
<td></td>
</tr>
<tr>
<td>Input VRF Name</td>
<td>TCP Header Length</td>
<td>TCP Flag: SYN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Sequence Number</td>
<td>TCP Flag: URG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Window-Size</td>
<td>UDP Message Length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Source Port</td>
<td>UDP Source Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Destination Port</td>
<td>UDP Destination Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Urgent Pointer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes

NEW: 2 or 4 bytes | NEW: 2 or 4 bytes
### Flexible Flow Record: Non-Key Fields

- Plus any of the potential “key” fields: will be the value from the first packet in the flow

<table>
<thead>
<tr>
<th>Counters</th>
<th>Timestamp</th>
<th>IP v4</th>
<th>IP v4 and IP v6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>sysUpTime First Packet</td>
<td>Total Length Minimum (*)</td>
<td>Total Length Minimum (**)</td>
</tr>
<tr>
<td>Bytes Long</td>
<td>sysUpTime First Packet</td>
<td>Total Length Maximum (*)</td>
<td>Total Length Maximum (**)</td>
</tr>
<tr>
<td>Bytes Square Sum</td>
<td></td>
<td>TTL Minimum</td>
<td></td>
</tr>
<tr>
<td>Bytes Square Sum Long</td>
<td></td>
<td>TTL Maximum</td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packets Long</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Flow Exporter Configuration

flow exporter <exporter-name>
  destination <ipv4-address> [vrf <vrf-name>]
  dscp <value>
  export-protocol [netflow-v5 | netflow-v9]
  option {exporter-stats | interface-table | sampler-table | vrf-table | application-table} timeout <value in sec>
  source <interface-name>
  template data timeout <value in sec>
  transport udp <destination-port>
  ttl <value>
  output-features

Five Types of Options
Data Record

New in 12.4(20)T
NetFlow Exported Packets Go Through QoS, Crypto-Map, etc…
Transition Steps from Traditional NetFlow to Flexible NetFlow

- First, flexible NetFlow metering process with NetFlow Version 5 flow records and Version 5 export
- Second, flexible NetFlow metering process with NetFlow Version 5 flow records and Version 9 export
- Third, user-defined flow records with Version 9 export

Router(config)# flow monitor my-monitor
Router(config-flow-monitor)# record netflow ipv4 ?
  as                      AS aggregation schemes
  as-tos                  AS and TOS aggregation schemes
  bgp-nexthop-tos         BGP next-hop and TOS aggregation schemes
  destination-prefix      Destination Prefix aggregation schemes
  destination-prefix-tos  Destination Prefix and TOS aggregation schemes
  original-input         Traditional IPv4 input NetFlow
  original-output         Traditional IPv4 output NetFlow
Flexible Monitor Configuration

```plaintext
flow monitor <monitor-name>
  record <record-name>
  exporter <exporter-name>
  cache type {normal | immediate | permanent}
  cache entries <number-of-entries>
  cache timeout {active | inactive | update} <value-in-seconds>
  statistics packet protocol
  statistics packet size

Collect Size Distribution Statistics

Collect Protocol Distribution Statistics

Three Types of Cache: See Next Slides
```
Three Types of NetFlow Caches

- Normal cache (traditional NetFlow)
  - More flexible active and inactive timers: one second minimum

- Immediate cache
  - Flow accounts for a single packet
  - Desirable for real-time traffic monitoring, DDoS detection, logging
  - Desirable when only very small flows are expected (ex: sampling)
  - Caution: may result in a large amount of export data

- Permanent cache
  - To track a set of flows without expiring the flows from the cache
  - Entire cache is periodically exported (update timer)
  - After the cache is full (size configurable), new flows will not be monitored
  - Uses update counters rather than delta counters
Complete Permanent Flexible NetFlow Configuration Example

- Per DSCP accounting flow record definition:

```
Router(config)# flow record my-dscp-record
Router(config-flow-record)# match ipv4 dscp
Router(config-flow-record)# match interface input
Router(config-flow-record)# collect counter bytes long
Router(config-flow-record)# collect counter packets long

Router(config)# flow monitor my-dscp-monitor
Router(config-flow-record)# description dscp:bytes and packets
Router(config-flow-record)# record my-dscp-record
Router(config-flow-record)# cache type permanent
Router(config-flow-record)# cache entries 256

Router(config)# interface GigabitEthernet 0/1
Router(config-if)# ip flow monitor my-dscp-monitor input
```
Complete Permanent Flexible NetFlow Configuration Example

Router# show flow monitor my-dscp-monitor cache
  Cache type: Permanent
  Cache size: 256
  Current entries: 0
  High Watermark: 0

  Flows added: 0
  Updates sent (1800 secs) 0

<table>
<thead>
<tr>
<th>IP DSCP</th>
<th>INTF INPUT</th>
<th>bytes long perm</th>
<th>pkts long perm</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>Gi0/1</td>
<td>1000</td>
<td>10</td>
</tr>
<tr>
<td>0x01</td>
<td>Gi0/1</td>
<td>500</td>
<td>5</td>
</tr>
</tbody>
</table>

Extra Options:
CSV, Table, Record

Flow Keys in Upper Case
Flexible NetFlow Activation per Interface

Router(config-if)# ip flow monitor <monitor-name>
    [sampler <sampler-name>]
    [input | output] [unicast | multicast]

For the Input or Output Traffic.
Does not Determine the Flow Key

- Deterministic or random sampling

Router(config)# sampler <sampler-name>
    mode [deterministic | random] <value N> out-of <value M>

Need the “Match Flow Sampler” in the Record for Accuracy Determination
Useful Show Commands

- List of all possible information elements
  - `show flow exporter export-ids netflow-v9`

- Template assignment
  - `show flow exporter template`

- High watermark in the cache
  - `show flow monitor <flow-monitor> statistics`

- NetFlow configuration
  - `show running flow [exporter | monitor | record]`
NetFlow Deployment Scenarios

**Security Flow Monitor**
- Protocol
- Ports
- IP addresses
- TCP flags

**Managed Service Application Visibility**
- IP addresses
- Application
- DSCP

**NetFlow for Core Traffic Matrix**
- Source/destination AS
- IP addresses (src/dest)
- BGP next hop
- Protocols
- DSCP

**Server Flow Monitor**
- Standard seven keys

**Peering Flow Monitor**
- Destination AS
- Source traffic index
- BGP next hop
- DSCP
Flexible NetFlow Platforms, Features

- **Platforms:**
  - 800, 1700, ISR (1800, 2800, 3800), ISR-G2 (890, 1900, 2900, 3900), 2600, 2800, 3700, 3800, 7200, 7301, 12000, Nexus 7000, Nexus 1000V, Catalyst 4500, cat6500 sup 2T, ASR1000, ASR 9000, CRS-1

- **Some traditional NetFlow features are not yet supported with flexible NetFlow:**
  - Input filters (integration with modular QoS CLI)
  - SCTP
  - MIB
Agenda

• Introduction
• NetFlow Version 9
• Flexible NetFlow
• NetFlow for Security
• NetFlow for Application Visibility and Control
• NetFlow & IP v6
• NetFlow Performance
• NetFlow Standardization
• Support Matrix
• Conclusion
What Does a DoS Attack Look Like?

- **Typical DoS attacks** have the same (or similar) entries:
  - Input interface, destination IP, one packet per flow, constant bytes per packet (B/Pk)

- **Export to a security-oriented collector:** Lancope, Arbor
### Flexible Flow Record: Key Fields

<table>
<thead>
<tr>
<th><strong>Flow</strong></th>
<th><strong>IP v4</strong></th>
<th><strong>IP v6</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampler ID</td>
<td>IP (Source or Destination)</td>
<td>IP (Source or Destination)</td>
</tr>
<tr>
<td>Direction</td>
<td>Payload Size</td>
<td>Payload Size</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Prefix (Source or Destination)</td>
<td>Prefix (Source or Destination)</td>
</tr>
<tr>
<td>Input</td>
<td>Packet Section (Header)</td>
<td>Packet Section (Header)</td>
</tr>
<tr>
<td>Output</td>
<td>Packet Section (Payload)</td>
<td>Packet Section (Payload)</td>
</tr>
<tr>
<td><strong>Layer 2</strong></td>
<td>Mask (Source or Destination)</td>
<td>Mask (Source or Destination)</td>
</tr>
<tr>
<td>Source VLAN</td>
<td>TTL</td>
<td>Minimum-Mask (Source or Destination)</td>
</tr>
<tr>
<td>Dest VLAN</td>
<td>Options bitmap</td>
<td>DSCP</td>
</tr>
<tr>
<td>Dot1q VLAN</td>
<td>Protocol</td>
<td>Protocol</td>
</tr>
<tr>
<td>Dot1q priority</td>
<td>Version</td>
<td>Extension Headers</td>
</tr>
<tr>
<td>Source MAC address</td>
<td>Fragmentation Flags</td>
<td>Traffic Class</td>
</tr>
<tr>
<td>Destination MAC address</td>
<td>Fragmentation Offset</td>
<td>Flow Label</td>
</tr>
<tr>
<td></td>
<td>Identification</td>
<td>Length</td>
</tr>
<tr>
<td></td>
<td>Header Length</td>
<td>Option Header</td>
</tr>
<tr>
<td></td>
<td>Total Length</td>
<td>Next-header</td>
</tr>
<tr>
<td></td>
<td>IP (Source or Destination)</td>
<td>Header Length</td>
</tr>
<tr>
<td></td>
<td>Source MAC address</td>
<td>Version</td>
</tr>
<tr>
<td></td>
<td>Destination MAC address</td>
<td>Payload Length</td>
</tr>
<tr>
<td></td>
<td>IP (Source or Destination)</td>
<td></td>
</tr>
</tbody>
</table>
# Flexible Flow Record: Key Fields

<table>
<thead>
<tr>
<th>Routing</th>
<th>Transport</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>src or dest AS</td>
<td>Destination Port</td>
<td>Application ID</td>
</tr>
<tr>
<td>Peer AS</td>
<td>Source Port</td>
<td></td>
</tr>
<tr>
<td>Traffic Index</td>
<td>ICMP Code</td>
<td>Replication Factor*</td>
</tr>
<tr>
<td>Forwarding Status</td>
<td>ICMP Type</td>
<td>RPF Check Drop*</td>
</tr>
<tr>
<td>IGP Next Hop</td>
<td>IGMP Type*</td>
<td>Is-Multicast</td>
</tr>
<tr>
<td>BGP Next Hop</td>
<td>TCP ACK Number</td>
<td></td>
</tr>
<tr>
<td>Input VRF Name</td>
<td>TCP Source Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Destination Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Urgent Pointer</td>
<td></td>
</tr>
</tbody>
</table>

|  | Transport                          |  |  |
|  | TCP Flag: ACK                      |  |  |
|  | TCP Flag: CWR                      |  |  |
|  | TCP Flag: ECE                      |  |  |
|  | TCP Flag: FIN                      |  |  |
|  | TCP Flag: PSH                      |  |  |
|  | TCP Flag: RST                      |  |  |
|  | TCP Flag: SYN                      |  |  |
|  | TCP Flag: URG                      |  |  |
|  | UDP Message Length                 |  |  |
|  | UDP Source Port                    |  |  |
|  | UDP Destination Port               |  |  |
Flexible Flow Record: Key Fields

- Counters
  - Bytes
  - Bytes Long
  - Bytes Square Sum
  - Bytes Square Sum Long
  - Packets
  - Packets Long

- Timestamp
  - sysUpTime First Packet

- IP v4
  - Total Length Minimum (*)
  - Total Length Maximum (*)
  - TTL Minimum
  - TTL Maximum

- IP v4 and IP v6
  - Total Length Minimum (**)
  - Total Length Maximum (**)

(*) IPV4_TOTAL_LEN_MIN, IPV4_TOTAL_LEN_MAX
(**) IP_LENGTH_TOTAL_MIN, IP_LENGTH_TOTAL_MAX

- Plus any of the potential “key” fields: will be the value from the first packet in the flow
Useful Fields for Security Monitoring

- **Attacks that Use Consistent Packet Size or Worms that Use Consistent Packet Size**

- **Several Flows with the Same Fragment Offset: Same Packet Sent Over and Over**

- **Flow Issued From the Same Origin**

- **Very Large Packets or Attacks that Might Always Have The Same Generated Identification**

[Diagram showing IP packet structure with annotations for different types of attacks and scenarios related to security monitoring.]
The Forwarding Status

- Unknown (00b)
- Forwarded (01b)
- Dropped (10b) → ACL, QoS
- Consumed (11b) → Destined to the router (ex: management traffic)

Router(config)# flow record forwarding-status
Router(config-flow-record)# ...
Router(config-flow-record)# match routing forwarding status
Packet Section Fields

- Contiguous chunk of a packet of a user configurable size, used as a key or a non-key field
- Sections used for detailed traffic monitoring, DDoS attack investigation, worm detection, other security applications
- Chunk defined as flow key, should be used in sampled mode with immediate aging cache

```
collect or match ipv4 header <size in bytes>
```

- Starts at the beginning of the IPv4 header

```
collect or match ipv4 payload <size in bytes>
```

- Immediately follows the IPv4 header
Flexible NetFlow TopTalkers

Flow filtering, aggregation and sorting can be combined to select what information and how it will be displayed.

- New in 12.4(22)T
- Top ten protocols observed:

```
Router# show flow monitor monitor-name cache filter options ... aggregation options sort options
```

```
Router# show flow monitor <monitor> cache aggregate ipv4 protocol sort highest counter bytes top 10
```
Flexible NetFlow Top Talkers { Examples

- Top ten IP addresses that are sending the most packets

  ```
  Router# show flow monitor <monitor> cache
  aggregate ipv4 source address
  sort highest counter bytes top 10
  ```

- Top five destination addresses to which we’re routing most traffic from the 10.10.10.0/24 prefix

  ```
  Router# show flow monitor <monitor> cache
  filter ipv4 destination address 10.10.10.0/24
  aggregate ipv4 destination address
  sort highest counter bytes top 5
  ```

- Five VLANs that we’re sending the least bytes to:

  ```
  Router# show flow monitor <monitor> cache
  aggregate datalink dot1q vlan output
  sort lowest counter bytes top 5
  ```

- Top 20 sources of one-packet flows:

  ```
  Router# show flow monitor <monitor> cache
  filter counter packet 1
  aggregate ipv4 source address
  sort highest flow packet top 20
  ```
Flexible NetFlow Top Talkers

Example

- The top 100 pairs of IP addresses with one or two packet(s) that are destined for My Servers Network

Router# show flow monitor <monitor> cache
filter ipv4 destination address 10.10.10.0/24
counter packet regex[1-2]
aggregate ipv4 source address
ipv4 destination address
sort highest flow top 100
Embedded Event Manager 3.0
Flexible NetFlow Event Detector

```plaintext
flow record <my-record>
  match ipv4 ttl
  match ipv4 source address
  match ipv4 destination address

flow exporter <my-exporter>
  destination 10.10.10.10

flow monitor <my-monitor>
  record <my-record>
  exporter <my-exporter>

event manager applet security-applet
  event nf monitor-name "<my-monitor>" event-type create event1
  entry-value "5" field ipv4 ttl entry-op lt  action 1.0 syslog msg
  "flow record with low TTL"
```

- If a flow record with TTL < 5, send a syslog message
Detect that some packets target the CPU…

Router# show flow monitor <my-monitor> cache

Cache type: Normal
Cache size: 4096
Current entries: 5
High Watermark: 5

Flows added: 32
Flows aged: 27
  - Active timeout (1 800 secs) 0
  - Inactive timeout ( 15 secs) 27
  - Event aged 0
  - Watermark aged 0
  - Emergency aged 0

IPV4 SRC ADDR   IPV4 DST ADDR   IP TTL
=================  ===============  ======
168.192.1.1      10.48.72.79           3

*Dec 18 2008 11:45:04.904 UTC: %HA_EM-6-LOG: security-applet: flow record with low TTL
Security and Traditional NetFlow

- “NetFlow L2 and Security Monitoring”
  - Source MAC address, destination MAC address, Received VLAN ID field (802.1q and Cisco’s ISL), Transmitted VLAN ID, Time-to-live, Identification, Packet length, ICMP type and code, Fragment offset

- “NetFlow Top Talkers”
  - Must be configured
  - Potentially match statements, working as a filter
  - Can be retrieved via the CISCO-NETFLOW-MIB (cnfTopFlowsTable)

- “NetFlow Dynamic Top Talkers”
  - On the fly with show commands: does not require router config modifications
  - But not available with the MIB
  - Potentially match statements, working as a filter
  - “show ip flow top <N> <aggregate-field> <sort-criteria> <match-criteria>”
  - Almost as powerful as the “Flexible NetFlow Top Talkers”
Cisco Adaptive Security Appliances (ASA)
5580—NetFlow Export Version 9

- Logging in high-performance environments is nontrivial, NetFlow is replacing syslog
- Flow event information can now be exported through NetFlow v9
  - Information about NAT modifications to the traffic
  - Information about Flows denied by security policy
  - Information about AAA/usernames associated with flows
  - Bidirectional flows
- Provides scalable logging
  - 10-Gbps flows, 100-k connections per second = lots of logs
- Adds new NetFlow fields to represent security related parameters
- NetFlow export is the logical evolution in logging technology
Agenda

- Introduction
- NetFlow Version 9
- Flexible NetFlow
- NetFlow for Security
- NetFlow for Application Visibility and Control
- NetFlow & IP v6
- NetFlow Performance
- NetFlow Standardization
- Support Matrix
- Conclusion
What is NBAR?

Network Based Application Recognition

- Classification of L3-L7 Application traffic
- Can be used with Protocol Discovery to get an idea of what the traffic patterns in the network
- Can be used with MQC (Modular QoS Control) to control the traffic patterns in the network
- Flexible NetFlow (FNF) integration: NBAR can export traffic data to a NetFlow Collector
- Supported devices: ISR-G1 (85x, 87x, 18xx, 28xx, 38xx), ISR-G2 (86x, 88x, 89x, 19xx, 29xx, 39xx), 2600XM, 3700, 7200, 7301, 7304-NPE, ASR1000, 7600 FlexWAN and SIP-200, catalyst 6000 supervisor 32 PISA (now End-of-Live),
  - Note2: NBAR2 (next slide) only supported on ISR-G2 and ASR1000
What is NBAR2?

- Complete redesign compared to NBAR
- Up to 900 applications
  - Platform independent signatures, combine NBAR and SCE Application Library
  - Common application library for NBAR2 across platforms
  - Consistent application Id across Cisco
- Advanced Classification Techniques
  - Support of IPv4, IPv6 and nested traffic (IPv6 transition method, ...)
  - Leverage classification techniques from SCE (Multi-Packet Engine)
  - Classification per Categories, Sub-Categories and Attributes
- Signatures delivery through Protocol Pack
  - Decoupling signatures upgrade from base image
  - Non-disruptive installation of new Protocol Pack
- Up to 121 custom applications
## NBAR 2 Protocol Library

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix (ICA, CGP, IMA, SB)</td>
<td>12.4(1)M</td>
<td>2.5</td>
</tr>
<tr>
<td>PCA anyware</td>
<td>12.4(1)M</td>
<td>2.3</td>
</tr>
<tr>
<td>Novadigm</td>
<td>12.4(1)M</td>
<td>2.3</td>
</tr>
<tr>
<td>SAP</td>
<td></td>
<td>2.5</td>
</tr>
<tr>
<td>Oracle</td>
<td>15.1(2)T</td>
<td>2.3</td>
</tr>
<tr>
<td>CIFSv1</td>
<td>15.1(2)T</td>
<td>3.1.0S</td>
</tr>
<tr>
<td>CIFSv2</td>
<td>15.1(2)T</td>
<td>3.1.0S</td>
</tr>
</tbody>
</table>

Flexible NetFlow—NBAR Integration

Configuration Example

```
router(config)# flow record <app_record>
router(config-flow-record)# match interface input
router(config-flow-record)# match ipv4 source address
router(config-flow-record)# match ipv4 destination address
router(config-flow-record)# match application name account-on-resolution
router(config-flow-record)# collect counter packets
router(config-flow-record)# collect counter bytes

router(config)# flow exporter <app_collector>
router(config-flow-exporter)# destination <ip address>
router(config-flow-exporter)# option interface-table
router(config-flow-exporter)# option application-table
router(config-flow-exporter)# option application-attributes

router(config)# flow monitor <app_monitor>
router(config-flow-monitor)# record <app_record>
router(config-flow-monitor)# exporter <app_collector>
router(config-flow-monitor)# cache timeout event transaction-end

router(config)# interface eth0/0
router(config-if)# ip flow monitor <app_monitor> input
```

“match application name”: calls NBAR
“account-on-resolution” (ASR1000): accurate accounting until classification

Export the full list of supported application

ASR1000: Export the full list of attributes per application (next slide)
### Traffic Categorization

Categorization of applications into meaningful terms

Simplification of control configuration and report aggregation

<table>
<thead>
<tr>
<th>Categories</th>
<th>Sub-Categories</th>
<th>Application-Group</th>
<th>P2P-technology</th>
<th>Tunnel</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>file-sharing</td>
<td>client-server</td>
<td>ftp-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>browsing</td>
<td>other</td>
<td>other</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>net-admin</td>
<td>routing-protocol</td>
<td>ipsec-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td>other</td>
<td>tunneling-protocols</td>
<td>imap-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td>internet-privacy</td>
<td>network-management</td>
<td>irc-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td>instant-messaging</td>
<td>voice-video-chat</td>
<td>kerberos-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>email</td>
<td>collaboration</td>
<td>ldap-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td>newsgroup</td>
<td>authentication-services</td>
<td>sqlsvr-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>voice-and-video</td>
<td>database</td>
<td>netbios-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td>business-and-productivity-tools</td>
<td>naming-services</td>
<td>nntp-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>industrial-protocols</td>
<td>terminal</td>
<td>smtp-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td>gaming</td>
<td>streaming</td>
<td>snmp-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td>obsolete</td>
<td>p2p-networking</td>
<td>fasttrack-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>trojan</td>
<td>p2p-file-transfer</td>
<td>gnutella-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td>layer3-over-ip</td>
<td>control-and-signaling</td>
<td>skinny-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>location-based-services</td>
<td>inter-process-rpc</td>
<td>edonkey-emule-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>layer2-non-ip</td>
<td>remote-access-terminal</td>
<td>bittorrent-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>network-protocol</td>
<td>smtp-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td></td>
<td>commercial-media-distribution</td>
<td>windows-live-messanger-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>rich-media-http-content</td>
<td>yahoo-messenger-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>license-manager</td>
<td>flash-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td></td>
<td>epayment</td>
<td>skype-group</td>
<td>n</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>storage</td>
<td>corba-group</td>
<td>y</td>
<td>y</td>
<td>unassigned</td>
</tr>
<tr>
<td></td>
<td>backup-systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>one-click-hosting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Flexible NetFlow—NBAR Integration Configuration Example

**Global Application ids across Cisco**

```plaintext
Router# show flow mon <app_mon> cache

<table>
<thead>
<tr>
<th>IPV4 SRC ADDR</th>
<th>IPV4 DST ADDR</th>
<th>APP NAME</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.1</td>
<td>10.0.1.2</td>
<td>nbar edonkey</td>
<td></td>
</tr>
<tr>
<td>10.0.1.1</td>
<td>10.0.1.2</td>
<td>nbar ssh</td>
<td></td>
</tr>
<tr>
<td>10.0.1.1</td>
<td>10.0.1.2</td>
<td>nbar http</td>
<td></td>
</tr>
<tr>
<td>10.0.1.1</td>
<td>10.0.1.2</td>
<td>NBAR lunar_light</td>
<td></td>
</tr>
</tbody>
</table>
```

**NBAR** = Custom Applications
(lunar_light is a user defined application)

**nbar** = Static Applications
Reporting Example (Plixer)
Medianet Performance Monitoring

```plaintext
class-map match-all telepresence-CS4
  match dscp cs4
class-map match-all SAP-HTTP
  match access-group name web-app
!
ip access-list extended web-app
  permit tcp any host 10.1.1.10 eq www
  permit tcp host 10.1.1.10 eq www any
!
policy-map type performance-monitor all-apps
class telepresence-CS4
  flow monitor inline
    record default-rtp
    exporter ecmd-rtp-1-capture
  monitor metric rtp
    clock-rate 96 48000
    clock-rate 112 90000
    clock-rate 101 8000

class SAP-HTTP
  flow monitor inline
    record default-tcp
    exporter ecmd-rtp-1-capture
!
interface FastEthernet0/0
  service-policy type performance-monitor input all-apps
  service-policy type performance-monitor output all-apps
```
Medianet Performance Monitoring

- Aggregation over all stored intervals

RTP Performance Metrics:
- Jitter, packet loss
- Min, mean, max

Router# show performance monitor history
...
start time                                           01:51:31
============
*history bucket number                              : 1
*counter flow                                        : 1
counter bytes                                      : 162329
counter bytes rate                           (Bps) : 5410
*counter bytes rate per flow                      : 5410
*counter bytes rate per flow min                  : 5410
*counter bytes rate per flow max                  : 5410
counter packets                                    : 773
*counter packets rate per flow                     : 25
counter packets dropped                            : 0
*routing forwarding-status reason                  : Unknown
interface input                                    : Fa0/0
interface output                                   : Vi1000
monitor event                                      : false
ipv4 dscp                                          : 32
ipv4 ttl                                           : 58
application media bytes counter                    : 146869
application media packets counter                  : 773
application media bytes rate                       : 4895
*application media bytes rate per flow             : 4895
*application media bytes rate per flow min         : 4895
*application media bytes rate per flow max         : 4895
*application media packets rate                    : 25
application media event                            : Normal
*transport rtp flow count                           : 1
transport rtp jitter mean                        (usec) : 476
transport rtp jitter minimum                      (usec) : 1
transport rtp jitter maximum                      (usec) : 1997
*transport rtp payload type                        : 96
transport event packet-loss counter                : 0
*transport event packet-loss counter min           : 0
*transport event packet-loss counter max           : 0
transport packets expected counter                 : 773
transport packets lost counter                     : 0
*transport packets lost counter minimum            : 0
*transport packets lost counter maximum            : 0
transport packets lost rate                        ( % ) : 0.00
*transport packets lost rate min                   ( % ) : 0.00
*transport packets lost rate max                   ( % ) : 0.00
IOS Performance Agent

- **IOS Performance Agent (IOS PA)** provides visibility into application and network performance
  - Available as software feature in base IOS image
  - Supported hardware - 880, 890, and ISR G2
- Collect ART (Application Response Time) metrics and report to Cisco NAM or partner reporting tool
- Can be deployed standalone or with WAAS Express
- When deployed with WAAS Express, will also report WAAS optimization statistics
- Available in 15.2(1)T
## Flexible NetFlow Integration with Performance Agent

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Time - av</td>
<td>Client Network Delay (CND) - av</td>
</tr>
<tr>
<td>Response Time - min</td>
<td>Client Network Delay (CND) - min</td>
</tr>
<tr>
<td>Response Time - max</td>
<td>Client Network Delay (CND) - max</td>
</tr>
<tr>
<td>Number of responses</td>
<td>Server Network Delay (SND) - av</td>
</tr>
<tr>
<td>Number of late responses</td>
<td>Server Network Delay (SND) - min</td>
</tr>
<tr>
<td>Number of responses by response time</td>
<td>Server Network Delay (SND) - max</td>
</tr>
<tr>
<td>(7-bucket histogram)</td>
<td>Total Delay (TD) - av</td>
</tr>
<tr>
<td>Number of connections (sessions)</td>
<td>Total Delay (TD) - min</td>
</tr>
<tr>
<td>Application Delay (AD) - av</td>
<td>Total Delay (TD) - max</td>
</tr>
<tr>
<td>Application Delay (AD) - min</td>
<td>Total Delay (TD) - max</td>
</tr>
<tr>
<td>Application Delay (AD) - max</td>
<td>Total Transaction Time - av</td>
</tr>
<tr>
<td>Network Delay (ND) - av</td>
<td>Total Transaction Time - min</td>
</tr>
<tr>
<td>Network Delay (ND) - min</td>
<td>Total Transaction Time - max</td>
</tr>
<tr>
<td>Network Delay (ND) - max</td>
<td>Number of Transactions</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Response Time – avg
- Response Time – min
- Response Time - max
- Number of responses
- Number of late responses
- Number of responses by response time (7-bucket histogram)
- Number of connections (sessions)
- Application Delay (AD) - avg
- Application Delay (AD) - min
- Application Delay (AD) - max
- Network Delay (ND) - avg
- Network Delay (ND) - min
- Network Delay (ND) - max
### Performance Based Routing (PfR): Configuration Templates - Options

#### Traffic Class Config
- Encoded Traffic-Class ID,
- Source prefix, Source mask,
- Destination prefix, Destination mask,
- Protocol,
- DSCP,
- Source port min, Source port max,
- Destination port min, Destination port max,
- Application Name,
- Policy id

#### External Interface Config
- BR address,
- External interface id,
- BR interface name,
- Link capacity,
- RSVP reserved bandwidth pool,
- Maximum ingress bandwidth,
- Maximum egress bandwidth,
- BGP Community
- Link group Name,
- Cost nickname, Cost type
- Cost discard rollup count

#### Internal Interface Config
- BR address
- Internal interface id
- BR interface name

#### Policy Config
- Policy id
- pfr-map name
- State
- Threshold
- Priority
- Variance
- MOS
- Link group Name

#### Reason Config
- Reason id
- Reason text
Agenda

- Introduction
- NetFlow Version 9
- Flexible NetFlow
- NetFlow for Security
- NetFlow for Application Visibility and Control
- NetFlow & IP v6
- NetFlow Performance
- NetFlow Standardization
- Support Matrix
- Appendix
NetFlow & IPv6

- **Traditional NetFlow**
  - Native IPv6 supported: 12.3(7)T, 12.2(33)SXH, 12.2(33)SRB
  - Beginning with Cisco IOS® Release 12.4(20)T, traditional NetFlow for IPv6 is being replaced by flexible NetFlow for IPv6

- **Flexible NetFlow**
  - Native IPv6 supported
  - NBAR 2 and IPv6 in 15.2(1)T
  - IPv6 transition techniques (IPv6 inside IPv4)
    - Can detect now teredo, isatap, 6to4, 6rd
    - Classification inside isatap, 6to4, 6rd in 15.2(2)T
  - Export on the top of IPv6: supported (15.2(2)T, Nexus 4.2.1)
Agenda

- Introduction
- NetFlow Version 9
- Flexible NetFlow
- NetFlow for Security
- NetFlow for Application Visibility and Control
- NetFlow & IP v6
- NetFlow Performance
- NetFlow Standardization
- Support Matrix
- Conclusion
Performance Challenge
Moving Bottleneck

- Consumes a lot of CPU
  - Packet sampling
  - Metering process in hardware
- Collisions in the cache
  - Improved the hash function
  - Increased the cache size
- Consumes much bandwidth
  - Flexible flow record per...interface, per direction
  - Export cache type per collector
  - Flow sampling
- CPU impact, accuracy impact, and bandwidth impact
CPU Impact
NetFlow Performance Paper Tests

- Paper at www.cisco.com/go/netflow under Technical Documents
- 0, 1, and 2 NetFlow data export destinations
- Initial performance after enabling
- v8 aggregation vs. v5, v9 performance
- Full NetFlow vs. 1:100 sampled NetFlow
- Tested hardware: Cisco 1841, 2600, 2811, 2851, 3640, 3745, 3845, 7200, 7301, 7500, 12000
  -> will be updated soon with newest platform
CPU Impact
Finding Summary

- Larger number of cache entries will have an increasing level of impact to CPU
  - This is much more visible on the low end systems (LES)
- Having multiple exporters does not add significant CPU impact
- NetFlow v9 and NetFlow v5 export have similar CPU impact
- Flexible NetFlow does add a slight CPU load
  - More visible on lower end platforms
  - However this difference is seen at large flow counts that are not expected to be seen on LES
  - FNF CPU load is higher (compared to traditional NetFlow) for higher number of packet per second
CPU Impact

NetFlow Sampling

- **Flow sampling** only available on the Catalyst 6500 and 7600
- With random packet based sampling, we can evaluate the accuracy of the observed flow records
Configuring Packet Based Sampling

```
flow record <my-record>
    match flow sampler
    match ...
    collect counter bytes squared long
    collect ...

flow exporter <my-exporter>
    option sampler-table
    ...

flow monitor <my-monitor>
    record <my-record>
    cache type normal
    exporter <my-exporter>
    ...

flow sampler <my-sampler>
    mode random 1 out-of 100

interface pos3/0
    ip flow monitor <my-monitor> <my-sampler> ingress|egress
    multicast|unicast
```

See next slide
Accuracy Impact
Random Packet NetFlow Sampling


- Square sum of bytes available in flexible NetFlow

```
\[
StdErr_{rel}[^{\text{\#Packets}}] = \frac{StdErr_{abs}[^{\text{\#Packets}}]}{\text{Sum}_{f}} = \frac{\sqrt{\frac{N^2}{n} \cdot \left( \sigma^2_{\mu_f} \cdot P_f + \mu_{\mu_f}^2 \cdot (P_f - P_f^2) \right)}}{N_f \cdot \mu_{\mu_f}}
\]
```
Flexible NetFlow in Hardware on Catalyst 6500/Sup2T

- System Scalability. Up to ~512K (with 99% utilization efficiency) cached flows for Forwarding Engine. Per direction, per DFC => 13 million flow entries
- Sampled NetFlow. Effective hardware-based sampling to improve and preserve NetFlow table utilization
- Ingress & Egress NetFlow. Useful for example to track packets decapsulated after tunneling mechanisms
- Per Interface or Sub-Interface activation
- Bridged NetFlow. Capability of creating and tracking bridged IP flows
- TCP Flags are now exported as part of the flow information. Very useful to understand TCP flow directions and to detect denial of service attacks
- IPv4, IPv6 and Layer 2 Flows support
- Export version 5 (the most used) and export version 9 (the most flexible) are both supported
- VRF aware export
- Hitless ISSU
Yielding NetFlow Data Export Feature

- Specific to the cat6500/Sup2T

```
Cat6500(config)# flow hardware export threshold <70>
```
Flexible NetFlow in Hardware on ASR 1000

- **System Scalability.** Up to ~1M cached flows for Forwarding Engine, in hardware
- **Sampled NetFlow.** Effective hardware-based sampling
- **Ingress & Egress NetFlow.**
- **Per Interface or Sub-Interface activation**
- **TCP Flags** are now exported as part of the flow information. Very useful to understand TCP flow directions and to detect denial of service attacks
- **Hardware based Export** hardware acceleration for export
- **Export version 5** (the most used) and export version 9 (the most flexible) are both supported
- **IPv4, Application layer (NBAR) Flow support** in XE 3.1.1S
- **VRF aware export**
- **Hitless ISSU** in IOS XE 3.2.0S
Flexible NetFlow in Hardware on Nexus 7000

- System Scalability. Up to ~500K (with 95% utilization efficiency) cached flows for Forwarding Engine
- Sampled NetFlow. Effective hardware-based sampling to improve and preserve NetFlow table utilization
- Egress NetFlow. Useful for example to track packets de-capsulated after tunneling mechanisms
- Per Interface or Sub-Interface activation
- Bridged NetFlow. Capability of creating and tracking bridged IP flows
- TCP Flags are now exported as part of the flow information. Very useful to understand TCP flow directions and to detect denial of service attacks
- IPv4, IPv6 and Layer 2 Flows support
- Export version 5 (the most used) and export version 9 (the most flexible) are both supported
- VRF aware export
- Hitless ISSU and process restartability
- Flexible NetFlow CLI look & feel
Flexible NetFlow in Hardware on Catalyst 4500/Sup7

- System Scalability. Up to ~128K cached flows
- Sampled NetFlow. Effective hardware-based sampling to improve and preserve NetFlow table utilization
- Ingress & Egress NetFlow, IPv4, IPv6 and Layer 2 Flows support
- Per Interface, Sub-Interface or Vlan activation
- Bridged NetFlow. Capability of creating and tracking bridged IP flows
- TCP Flags are now exported as part of the flow information. Very useful to understand TCP flow directions and to detect denial of service attacks
- Export version 5 (the most used) and export version 9 (the most flexible) are both supported
- VRF aware export, Hitless ISSU
- Note: on SUP2, netflow lite: packet sampling + no caching, exported with IPFIX
NetFlow in Hardware on Catalyst 3750-X and 3560-X
3KX-SM-10G Service Module

- System Scalability. Up to ~32K cached flows
- Sampled NetFlow. Effective hardware-based sampling to improve and preserve NetFlow table utilization
- Ingress & Egress NetFlow
- Per Interface, Sub-Interface or Vlan activation
- Bridged NetFlow. Capability of creating and tracking bridged IP flows
- TCP Flags are now exported as part of the flow information. Very useful to understand TCP flow directions and to detect denial of service attacks
- IPv4, IPv6 and Layer 2 Flows support
- Export version 9
- VRF aware export
- 3KX-SM-10G
NetFlow in Hardware on CRS Family

- System Scalability. Up to ~1M cached flows per Line Card
- Sampled NetFlow. Effective hardware-based sampling from 1:1 to 1:64K – 100kpps/LC (ingress + egress)
- Ingress & Egress NetFlow
- Per Interface or Sub-Interface support
- TCP Flags Very useful to understand TCP flow directions and to detect denial of service attacks
- Export version 9 – 50K Flows/s export per LC
- IPv4, IPv6, MPLS Flows support
- VRF aware export
- Hitless ISSU and process restartability
- Flexible NetFlow Pre-defined aggregation only
Reducing Performance Impact

CPU and Memory Impact on the Network Element, Collector, and Network

- Flexible NetFlow (collect only what is really required)
- Aging timers
- Sampled NetFlow
- Leverage distributed architectures (VIP, linecards)
- Flow masks (only Cisco Catalyst 6500/7600)
- Aggregation schemes (v8 on router or on collector)
- Filters (router or collector)
- Data compression (collector)
- Increase collection bucket sizes (collector)
- Place collector and router on the same LAN segment/dedicated interface
## Bandwidth Impact

### Case 1: Traditional NetFlow

Router# show ip flow export
Flow export is enabled
  Exporting flows to 1.1.1.1 (9999)
  Exporting using source IP address 198.198.198.11
  Version 5 flow records
  29 flows exported in 4 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures

Router# clear ip flow stats

- `cnfESExportRate (NETFLOW-MIB)`, “number of bytes exported per second”
- The counter for this MIB object only contain L3 bytes: Layer 2 encapsulation needs to be added
**Bandwidth Impact**

*Case 2: Flexible NetFlow*

```
Router(config)# flow exporter <exporter>
Router(config-flow-exporter)# destination 1.1.1.1
Router(config)# ip route 1.1.1.1 255.255.255.255 Null 0

Router(config)# ip cef accounting per-prefix
```

- MIB counter only contain L3 bytes, Layer 2 encapsulation needs to be added
- This method is also valid for traditional NetFlow
- CEF-MIB available in 12.4(20)T
Agenda

- Introduction
- NetFlow Version 9
- Flexible NetFlow
- NetFlow for Security
- NetFlow for Application Visibility and Control
- NetFlow & IP v6
- NetFlow Performance
- NetFlow Standardization
- Support Matrix
- Conclusion
IETF: IP Flow Information Export

WG (IPFIX)

- RFC3954 Cisco Systems NetFlow Services Export Version 9
- RFC3917 Requirements for IP Flow Information Export
  - Gathers all IPFIX requirements for the IPFIX evaluation process
- RFC3955 Evaluation of Candidate Protocols for IPFIX
- RFC5102 Information Model for IP Flow Information Export
- RFC5103 “Bidirectional Flow Export using IP Flow Information Export (IPFIX)”
IETF: IP Flow Information Export WG (IPFIX)

- **IPFIX protocol specifications**
  - Changes in terminology but same NetFlow Version 9 principles
  - Improvements vs. NetFlow Version 9: SCTP-PR, security, variable length information element, IANA registration, etc.
  - **Generic streaming protocol**, not flow-centric anymore
  - Security:
    - Threat: confidentiality, integrity, authorization
    - Solution: DTLS on SCTP-PR

- **IPFIX information model**
  - Most NetFlow Version 9 information elements ID are kept
  - Proprietary information element specification

- **Is IPFIX important to you?**
IETF: Packet Sampling WG (PSAMP)

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

- **Sampling and filtering techniques for IP packet selection**
  - To be compliant with PSAMP, we must implement at least one of the mechanisms: sampled NetFlow, NetFlow input filters are already implemented

- **PSAMP protocol specifications**
  - Agreed to use IPFIX for export protocol

- **Information model for packet sampling export**
  - Extension of the IPFIX information model
Agenda

• Introduction
• NetFlow Version 9
• Flexible NetFlow
• NetFlow for Security
• NetFlow for Application Visibility and Control
• NetFlow & IP v6
• NetFlow Performance
• NetFlow Standardization
• Support Matrix
• Conclusion
# Traditional NetFlow

## Exporting Process

<table>
<thead>
<tr>
<th>Feature</th>
<th>Software</th>
<th>C6500</th>
<th>C7600</th>
<th>C12000</th>
<th>C10000</th>
<th>C4500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.0(1)</td>
<td>12.1(2)E</td>
<td>12.1(2)E</td>
<td>12.0(14)S</td>
<td>12.0(19)SL</td>
<td>12.1(13)EW</td>
</tr>
<tr>
<td>Version 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.0(3)T</td>
<td>12.2(14)SX</td>
<td>12.2(14)SX</td>
<td>12.0(6)S</td>
<td>12.0(19)SL</td>
<td>12.1(19)EW</td>
</tr>
<tr>
<td>Version 9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.3</td>
<td>12.2(18)SXF</td>
<td>12.2(18)SXF</td>
<td>12.0(24)S</td>
<td>12.2(31)SB</td>
<td></td>
</tr>
<tr>
<td>Dual Export</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(2)T</td>
<td>12.2(17d)SXB</td>
<td>12.2(17d)SXB</td>
<td></td>
<td>12.2(15)BX</td>
<td>12.1(19)EW</td>
</tr>
<tr>
<td>VRF Destination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.4(4)T</td>
<td></td>
<td>12.2(33)SRA</td>
<td></td>
<td>12.0(32)S</td>
<td></td>
</tr>
<tr>
<td>Reliable Export</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.3(4)T</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Product Manager Contact: jgriviau@cisco.com
### Traditional NetFlow

**Exporting Process**

<table>
<thead>
<tr>
<th>Feature</th>
<th>CRS-1</th>
<th>XR12000</th>
<th>ASR1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 5</td>
<td></td>
<td></td>
<td>2.1</td>
</tr>
<tr>
<td>Version 8</td>
<td></td>
<td></td>
<td>2.1</td>
</tr>
<tr>
<td>Version 9</td>
<td>3.2</td>
<td>3.3.0</td>
<td>2.1</td>
</tr>
<tr>
<td>Dual Export</td>
<td>3.4.0</td>
<td>3.4.0</td>
<td>2.1</td>
</tr>
<tr>
<td>VRF Destination</td>
<td>3.2</td>
<td>3.3.0</td>
<td></td>
</tr>
<tr>
<td>Reliable Export</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Available Now**

**Not Available**

**Roadmap**
### Traditional NetFlow

#### Metering Process

<table>
<thead>
<tr>
<th>Feature</th>
<th>Software</th>
<th>C6500</th>
<th>C7600</th>
<th>C12000</th>
<th>C10000</th>
<th>C4500</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>12.0(1)</td>
<td>12.1(27b)E1</td>
<td>12.2(18)SXF</td>
<td>12.0(22)S</td>
<td>12.2(15)BX</td>
<td>12.1(13)EW</td>
</tr>
<tr>
<td>IPv6</td>
<td>12.3(7)T</td>
<td>12.2(33)SXH</td>
<td>12.2(33)SRB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast</td>
<td>12.3</td>
<td>12.2(18)SXF</td>
<td>12.2(18)SXF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BGP Next Hop</td>
<td>12.3</td>
<td>12.2(18)SXF</td>
<td>12.2(33)SRA</td>
<td>12.0(26)S</td>
<td>12.2(31)SB</td>
<td></td>
</tr>
<tr>
<td>Per Interface</td>
<td>Yes</td>
<td>12.2(33)SXH</td>
<td>12.2(33)SRB</td>
<td>No Sub</td>
<td>12.2(15)BX</td>
<td></td>
</tr>
<tr>
<td>Per VRF Interface</td>
<td>Yes</td>
<td>12.2(33)SXH</td>
<td>12.2(33)SRB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOS Support</td>
<td>Yes</td>
<td>12.2(17b)SXA</td>
<td>12.2(17b)SXA</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Packet Sampling</td>
<td>12.3(24)</td>
<td>12.2(17b)SXA</td>
<td></td>
<td>12.0(11)S</td>
<td>12.2(31)SB</td>
<td></td>
</tr>
<tr>
<td>Min Prefix Aggr.</td>
<td>12.1(2)T</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>12.2(28)SB</td>
</tr>
<tr>
<td>MPLS Egress with EXP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS Egress</td>
<td>12.2(2)T</td>
<td>12.2(33)SXJ</td>
<td></td>
<td></td>
<td></td>
<td>12.2(31)SB</td>
</tr>
<tr>
<td>MPLS Aware</td>
<td>12.3(8)T</td>
<td></td>
<td>12.2(33)SRA</td>
<td>12.0(24)S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS Label Exp.</td>
<td>12.2SB</td>
<td></td>
<td>12.2(33)SRB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS Aggregate.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12.2(31)SB</td>
</tr>
</tbody>
</table>

**Available Now**

- **For Your Reference**

**Roadmap**

- No SUPVI
# Traditional NetFlow

## Metering Process

<table>
<thead>
<tr>
<th>Feature</th>
<th>CRS-1</th>
<th>XR12000</th>
<th>ASR1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>3.2.0</td>
<td>3.3.0</td>
<td>2.1</td>
</tr>
<tr>
<td>IPv6</td>
<td>3.5.0</td>
<td>3.6.0</td>
<td></td>
</tr>
<tr>
<td>Multicast</td>
<td>3.2</td>
<td>3.3</td>
<td></td>
</tr>
<tr>
<td>BGP Next Hop</td>
<td>3.3</td>
<td>3.3</td>
<td>2.1</td>
</tr>
<tr>
<td>Per Interface</td>
<td>3.3.0</td>
<td>3.3.0</td>
<td>2.1</td>
</tr>
<tr>
<td>TOS Support</td>
<td>3.2</td>
<td>3.3</td>
<td>2.1</td>
</tr>
<tr>
<td>Packet Sampling</td>
<td>3.2</td>
<td>3.3</td>
<td>2.1</td>
</tr>
<tr>
<td>Min Prefix Aggr.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS Egress with EXP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS Egress</td>
<td>3.2</td>
<td>3.5.0</td>
<td></td>
</tr>
<tr>
<td>MPLS Aware</td>
<td>3.3.1</td>
<td>3.5.0</td>
<td></td>
</tr>
<tr>
<td>MPLS Label Expo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS Aggregate.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Available Now** | **Not Available** | **Roadmap**
## Traditional NetFlow

### Metering Process

<table>
<thead>
<tr>
<th>Feature</th>
<th>Software</th>
<th>C6500</th>
<th>C7600</th>
<th>C12000</th>
<th>C10000</th>
<th>C4500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress/Output NetFlow</td>
<td>12.3(11)T</td>
<td>12.0(10)ST</td>
<td>12.0(10)ST</td>
<td>12.2(31)SB</td>
<td>12.2(25)EW</td>
<td></td>
</tr>
<tr>
<td>Bridged NF</td>
<td>12.2(18)SXE1</td>
<td>12.2(18)SXE1</td>
<td>12.2(18)SXE1</td>
<td>12.2(18)SXE1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Filters</td>
<td>12.3(4)T</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP Flags</td>
<td>12.1(2)T</td>
<td>12.0(10)ST</td>
<td>12.0(10)ST</td>
<td>12.2(28)SB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mac Address</td>
<td>12.3(14)T</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Exports</td>
<td>12.3(14)T</td>
<td></td>
<td>12.2(33)SRA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vlan Export</td>
<td>12.4(4)T</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Traditional NetFlow

## Metering Process

<table>
<thead>
<tr>
<th>Feature</th>
<th>CRS-1</th>
<th>XR12000</th>
<th>ASR1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress/Output NetFlow</td>
<td>3.2</td>
<td>3.3</td>
<td>2.1</td>
</tr>
<tr>
<td>Bridged NF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Filters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP Flags</td>
<td>3.2</td>
<td>3.3</td>
<td>2.1</td>
</tr>
<tr>
<td>Mac Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Exports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vlan Export</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Available Now**

**Not Available**

**Roadmap**
# Miscellaneous Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Software</th>
<th>C6500</th>
<th>C7600</th>
<th>C12000</th>
<th>C10000</th>
<th>ASR1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetFlow MIB with Top Talker</td>
<td>12.3(11)T</td>
<td></td>
<td>12.2(33)SXH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Top Talker CLI</td>
<td>12.4(4)T</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISSU NetFlow</td>
<td></td>
<td></td>
<td>12.2(33)SRB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ifIndex to Name Map</td>
<td>12.4(4)T</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**For Your Reference**

Available Now

Not Available

Roadmap
# Traditional NetFlow

**Metering Process, Sampled NetFlow**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Software</th>
<th>C6500</th>
<th>C7600</th>
<th>C12000</th>
<th>C10000</th>
<th>C4500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systematic Sampling</td>
<td>12.3(11)T</td>
<td></td>
<td></td>
<td>12.0(11)S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random Sampling</td>
<td>12.4(9)T</td>
<td></td>
<td></td>
<td>12.0(33)S</td>
<td>12.2(31)SB</td>
<td></td>
</tr>
<tr>
<td>Output Sampled NetFlow</td>
<td></td>
<td></td>
<td></td>
<td>12.0(24)S</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Available Now] [Not Available] [Roadmap]
## Traditional NetFlow
Metering Process, Sampled NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>CRS-1</th>
<th>XR12000</th>
<th>ASR1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systematic Sampling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random Sampling</td>
<td>3.2</td>
<td>3.3</td>
<td>2.1</td>
</tr>
<tr>
<td>Output Sampled NetFlow</td>
<td></td>
<td></td>
<td>2.1</td>
</tr>
<tr>
<td>Flow Sampling</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Available Now**
- **Not Available**
- **Roadmap**
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco ISR</th>
<th>Cisco ISR-G2</th>
<th>Cisco 72/73xx</th>
<th>ASR1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Flexible NetFlow CLI</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Multiple User Defined Caches</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>User Defined Flow Record</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Normal Cache</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Immediate Cache</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>Radar</td>
</tr>
<tr>
<td>Permanent Cache</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>Radar</td>
</tr>
<tr>
<td>Dynamic TopNTalkers</td>
<td>12.4(22)T</td>
<td>15.0(1)M</td>
<td>12.4(22)T</td>
<td>Radar</td>
</tr>
<tr>
<td>FNF EEM Monitor</td>
<td>12.4(22)T</td>
<td>15.0(1)M</td>
<td>12.4(22)T</td>
<td>Radar</td>
</tr>
</tbody>
</table>

### Sampling

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco ISR</th>
<th>Cisco ISR-G2</th>
<th>Cisco 72/73xx</th>
<th>ASR1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Flow support</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Random Sampling 1:M</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Random Sampling N:M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Platform Feature Comparison

### Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>C6500/Sup2T</th>
<th>C4500/Sup7</th>
<th>C3KX-SM-10G</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Flexible NetFlow CLI</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>Multiple User Defined Caches</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>User Defined Flow Record</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>Normal Cache</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>Immediate Cache</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>Radar</td>
</tr>
<tr>
<td>Permanent Cache</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>Radar</td>
</tr>
<tr>
<td>Dynamic TopNTalkers</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>FNF EEM Monitor</td>
<td>Radar</td>
<td>IOS XE 3.1.0SG</td>
<td></td>
</tr>
</tbody>
</table>

**Sampling**

<table>
<thead>
<tr>
<th>Feature</th>
<th>C6500/Sup2T</th>
<th>C4500/Sup7</th>
<th>C3KX-SM-10G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Flow support</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>Random Sampling 1:M</td>
<td>12.2(50)SY</td>
<td>Radar</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>Random Sampling N:M</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Platform Feature Comparison
### Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Nexus 7000</th>
<th>Nexus1000V</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Flexible NetFlow CLI</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>Multiple User Defined Caches</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>User Defined Flow Record</td>
<td>4.0</td>
<td></td>
</tr>
<tr>
<td>Normal Cache</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>Immediate Cache</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permanent Cache</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic TopNTalkers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FNF EEM Monitor</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sampling</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Flow support</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>Random Sampling 1:M</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>Random Sampling N:M</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
</tbody>
</table>

Available Now | Not Available | Roadmap

© 2012 Cisco and/or its affiliates. All rights reserved. BRKNMS-3132 Cisco Public
## Platform Feature Comparison

### Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>CRS-1</th>
<th>XR12000</th>
<th>ASR9000</th>
<th>C12000</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Flexible NetFlow CLI</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Multiple User Defined Caches</td>
<td>Radar</td>
<td>Radar</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>User Defined Flow Record</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Normal Cache</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Immediate Cache</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Permanent Cache</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Dynamic TopNTalkers</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>FNF EEM Monitor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sampling</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Flow support</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Random Sampling 1:M</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Random Sampling N:M</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Available Now**: Green
- **Not Available**: Red
- **Roadmap**: Blue
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco ISR</th>
<th>Cisco ISR-G2</th>
<th>Cisco 72/73xx</th>
<th>ASR 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress support</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Egress support</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Per Interface</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Per Sub-Interface</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>On VRF Interface</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Per Vlan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per Class-map</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>On CoPP Interface</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Platform Feature Comparison

### Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>C6500/Sup2T</th>
<th>C4500/Sup7</th>
<th>C3KX-SM-10G</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress support</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
</tr>
<tr>
<td>Egress support</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
</tr>
<tr>
<td>Per Interface</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
</tr>
<tr>
<td>Per Sub-Interface</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
</tr>
<tr>
<td>On VRF Interface</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
</tr>
<tr>
<td>Per Vlan</td>
<td>15.1(1)SY</td>
<td>15.1(1)SY</td>
<td>15.1(1)SY</td>
</tr>
<tr>
<td>Per Class-map</td>
<td>Radar*</td>
<td>Radar*</td>
<td>Radar*</td>
</tr>
<tr>
<td>On CoPP Interface</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
<td>12.2(50)SY</td>
</tr>
</tbody>
</table>

**Available Now**

**Not Available**

**Roadmap**
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Nexus 7000</th>
<th>Nexus1000V</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress support</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>Egress support</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>Per Interface</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>Per Sub-Interface</td>
<td>4.0</td>
<td></td>
</tr>
<tr>
<td>On VRF Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per Vlan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per Class-map</td>
<td></td>
<td></td>
</tr>
<tr>
<td>On CoPP Interface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>CRS-1</th>
<th>XR12000</th>
<th>ASR 9000</th>
<th>C12000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress support</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Egress support</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Per Interface</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Per Sub-Interface</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>On VRF Interface</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Per Vlan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per Class-map</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On CoPP Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Available Now**: Green
- **Not Available**: Blank
- **Roadmap**: Dark Orange
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco ISR</th>
<th>Cisco ISR-G2</th>
<th>Cisco 72/73xx</th>
<th>ASR 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exporter</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetFlow v5 Export Format</td>
<td>12.4(22)T</td>
<td>15.0(1)M</td>
<td>12.4(22)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>NetFlow v9 Export Format</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>IPFIX Export Format</td>
<td>Radar</td>
<td></td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>IPFIX Structured Data</td>
<td>Radar</td>
<td></td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Export over UDP</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Export over SCTP (Reliable)</td>
<td>Radar*</td>
<td></td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Export over IPv4</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>Export over IPv6</td>
<td>15.2(2)T</td>
<td></td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Exporter MTU Configuration</td>
<td>Radar</td>
<td></td>
<td>Radar*</td>
<td></td>
</tr>
<tr>
<td>Export in a VRF</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.2.0S</td>
</tr>
<tr>
<td>FNF QOS output features</td>
<td>12.4(20)T</td>
<td>15.0(1)M</td>
<td>12.4(20)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
</tbody>
</table>
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>C6500/Sup2T</th>
<th>C4500/Sup7</th>
<th>C3KX-SM-10G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exporter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetFlow v5 Export Format</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>NetFlow v9 Export Format</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td></td>
</tr>
<tr>
<td>IPFIX Export Format</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>IPFIX Structured Data</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Export over UDP</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>Export over SCTP (Reliable)</td>
<td>Radar</td>
<td>Radar*</td>
<td></td>
</tr>
<tr>
<td>Export over IPv4</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>Export over IPv6</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Exporter MTU Configuration</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Export in VRF</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td></td>
</tr>
<tr>
<td>FNF QOS output features</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td></td>
</tr>
</tbody>
</table>
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Nexus 7000</th>
<th>Nexus 1000V</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exporter</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetFlow v5 Export Format</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>NetFlow v9 Export Format</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>IPFIX Export Format</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>IPFIX Structured Data</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>Export over UDP</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>Export over SCTP (Reliable)</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>Export over IPv4</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>Export over IPv6</td>
<td>4.2(1)</td>
<td></td>
</tr>
<tr>
<td>Exporter MTU Configuration</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>Export in VRF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FNF QOS output features</td>
<td>4.0</td>
<td></td>
</tr>
</tbody>
</table>
## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>CRS-1</th>
<th>XR12000</th>
<th>ASR9000</th>
<th>C12000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exporter</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetFlow v5 Export Format</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetFlow v9 Export Format</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>IPFIX Export Format</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>IPFIX Structured Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export over UDP</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Export over SCTP (Reliable)</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>Export over IPv4</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>Export over IPv6</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>Exporter MTU Configuration</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>Export in a VRF</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>FNF QOS output features</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td></td>
</tr>
</tbody>
</table>

- **Available Now**
- **Not Available**
- **Roadmap**
## Platform Feature Comparison

### Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco ISR</th>
<th>Cisco ISR-G2</th>
<th>Cisco 72/73xx</th>
<th>ASR1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Unicast Flows</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>IPv4 Predefined Aggregations</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>IPv4 Multicast Flows</td>
<td>12.4(22)T</td>
<td>15.0(1)M</td>
<td>12.4(22)T</td>
<td>Radar</td>
</tr>
<tr>
<td>IPv4 Multicast Replication Factor</td>
<td>12.4(22)T</td>
<td>15.0(1)M</td>
<td>12.4(22)T</td>
<td>Radar</td>
</tr>
<tr>
<td>IPv4 Header Section Field</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>IPv4 Payload Section Field</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>UDP Fields</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>TCP Fields</td>
<td>12.4(9)T</td>
<td>15.0(1)M</td>
<td>12.4(9)T</td>
<td>IOS XE 3.1.1S</td>
</tr>
<tr>
<td>SCTP Fields</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Application Name (NBAR) Field</td>
<td>15.0(1)M</td>
<td>15.0(1)M</td>
<td>15.0(1)M</td>
<td>IOS XE 3.1.1S</td>
</tr>
</tbody>
</table>

*Available Now: Green; Not Available: Grey; Roadmap: Radar*
## Platform Feature Comparison
### Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>C6500/Sup2T</th>
<th>C4500/Sup7</th>
<th>C3KX-SM-10G</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Flows</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Unicast Flows</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>IPv4 Predefined Aggregations</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td></td>
</tr>
<tr>
<td>IPv4 Multicast Flows</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>IPv4 Multicast Replication Factor</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td></td>
</tr>
<tr>
<td>IPv4 Header Section Field</td>
<td></td>
<td>IOS XE 3.1.0SG</td>
<td></td>
</tr>
<tr>
<td>IPv4 Payload Section Field</td>
<td></td>
<td>IOS XE 3.1.0SG</td>
<td></td>
</tr>
<tr>
<td>UDP Fields</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>TCP Fields</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>SCTP Fields</td>
<td></td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Application Name (NBAR) Field</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Platform Feature Comparison
### Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Nexus 7000</th>
<th>Nexus 1000V</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Flows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Unicast Flows</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>IPv4 Predefined Aggregations</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>IPv4 Multicast Flows</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>IPv4 Multicast Replication Factor</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>IPv4 Header Section Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Payload Section Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP Fields</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>TCP Fields</td>
<td>4.0</td>
<td>4.0(4)SV1</td>
</tr>
<tr>
<td>SCTP Fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Name (NBAR) Field</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>CRS-1</th>
<th>XR 12000</th>
<th>ASR 9000</th>
<th>C 12000</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Unicast Flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Predefined Aggregations</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>IPv4 Multicast Flows</td>
<td>3.5.0</td>
<td>3.5.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>IPv4 Multicast Flows</td>
<td>3.5.0</td>
<td>3.5.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>IPv4 Header Section Field</td>
<td></td>
<td></td>
<td></td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>IPv4 Payload Section Field</td>
<td></td>
<td></td>
<td></td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>UDP Fields</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>TCP Fields</td>
<td>3.2</td>
<td>3.3.0</td>
<td>3.9(1)</td>
<td>12.0(33)S</td>
</tr>
<tr>
<td>SCTP Fields</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Application Name (NBAR) Field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Available Now**
- **Not Available**
- **Roadmap**
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco ISR</th>
<th>Cisco ISR-G2</th>
<th>Cisco 72/73xx</th>
<th>ASR 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Unicast Flows</td>
<td>12.4(20)T</td>
<td>15.0(1)M</td>
<td>12.4(20)T</td>
<td></td>
</tr>
<tr>
<td>IPv6 Predefined Aggregations</td>
<td>12.4(20)T</td>
<td>15.0(1)M</td>
<td>12.4(20)T</td>
<td></td>
</tr>
<tr>
<td>IPv6 Multicast Flows</td>
<td>12.4(22)T</td>
<td>15.0(1)M</td>
<td>15.0(1)M</td>
<td>Radar</td>
</tr>
<tr>
<td>IPv6 Multicast Replication Factor</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>IPv6 Header Section Field</td>
<td>12.4(20)T</td>
<td>15.0(1)M</td>
<td>12.4(20)T</td>
<td></td>
</tr>
<tr>
<td>IPv6 Payload Section Field</td>
<td>12.4(20)T</td>
<td>15.0(1)M</td>
<td>12.4(20)T</td>
<td></td>
</tr>
<tr>
<td>UDP Fields</td>
<td>12.4(20)T</td>
<td>15.0(1)M</td>
<td>12.4(20)T</td>
<td></td>
</tr>
<tr>
<td>TCP Fields</td>
<td>12.4(20)T</td>
<td>15.0(1)M</td>
<td>12.4(20)T</td>
<td></td>
</tr>
<tr>
<td>SCTP Fields</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Application Name (NBAR) Field</td>
<td></td>
<td></td>
<td>15.2(1)T</td>
<td>IOS XE 3.5.0S</td>
</tr>
</tbody>
</table>

Available Now:  Available Now
Not Available: Not Available
Roadmap: Roadmap
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>C6500/Sup2T</th>
<th>C4500/Sup7</th>
<th>C3KX-SM-10G</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Flows</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Unicast Flows</td>
<td>Available Now</td>
<td>Available Now</td>
<td>Available Now</td>
</tr>
<tr>
<td>IPv6 Predefined Aggregations</td>
<td>Available Now</td>
<td>Available Now</td>
<td>Available Now</td>
</tr>
<tr>
<td>IPv6 Multicast Flows</td>
<td>Available Now</td>
<td>Available Now</td>
<td>Available Now</td>
</tr>
<tr>
<td>IPv6 Multicast Replication Factor</td>
<td>Available Now</td>
<td>Available Now</td>
<td>Available Now</td>
</tr>
<tr>
<td>IPv6 Header Section Field</td>
<td>Available Now</td>
<td>Available Now</td>
<td>Available Now</td>
</tr>
<tr>
<td>IPv6 Payload Section Field</td>
<td>Available Now</td>
<td>Available Now</td>
<td>Available Now</td>
</tr>
<tr>
<td>UDP Fields</td>
<td>Available Now</td>
<td>Available Now</td>
<td>Available Now</td>
</tr>
<tr>
<td>TCP Fields</td>
<td>Available Now</td>
<td>Available Now</td>
<td>Available Now</td>
</tr>
<tr>
<td>SCTP Fields</td>
<td>Available Now</td>
<td>Available Now</td>
<td>Available Now</td>
</tr>
<tr>
<td>Application Name (NBAR) Field</td>
<td>Available Now</td>
<td>Available Now</td>
<td>Available Now</td>
</tr>
</tbody>
</table>

- `Available Now`: Feature is available now.
- `Not Available`: Feature is not available.
- `Roadmap`: Future availability information.

**Notes:**
- IPv6 Header Section Field: Radar indicates planned support in future releases.
- UDP, TCP, SCTP Fields: Available with specific releases.
- Application Name (NBAR) Field: Available with specific releases.
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Nexus 7000</th>
<th>Nexus 1000V</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPv6 Flows</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Unicast Flows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Predefined Aggregations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Multicast Flows</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>IPv6 Multicast Replication Factor</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>IPv6 Header Section Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Payload Section Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP Fields</td>
<td>4.0</td>
<td></td>
</tr>
<tr>
<td>TCP Fields</td>
<td>4.0</td>
<td></td>
</tr>
<tr>
<td>SCTP Fields</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Name (NBAR) Field</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Available Now**
- **Not Available**
- **Roadmap**
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>CRS-1</th>
<th>XR12000</th>
<th>ASR9000</th>
<th>C12000</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Flows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Unicast Flows</td>
<td>3.5.0</td>
<td>3.6.0</td>
<td>3.9(1)</td>
<td></td>
</tr>
<tr>
<td>IPv6 Predefined Aggregations</td>
<td>3.5.0</td>
<td>3.6.0</td>
<td>3.9(1)</td>
<td></td>
</tr>
<tr>
<td>IPv6 Multicast Flows</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>IPv6 Multicast Replication Factor</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>IPv6 Header Section Field</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>IPv6 Payload Section Field</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>UDP Fields</td>
<td>3.5.0</td>
<td>3.6.0</td>
<td>3.9(1)</td>
<td></td>
</tr>
<tr>
<td>TCP Fields</td>
<td>3.5.0</td>
<td>3.6.0</td>
<td>3.9(1)</td>
<td></td>
</tr>
<tr>
<td>SCTP Fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Name (NBAR) Field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Available Now: Green
Not Available: Blank
Roadmap: Radar
<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco ISR</th>
<th>Cisco ISR-G2</th>
<th>Cisco 72/73xx</th>
<th>ASR 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Flows</td>
<td>12.4(22)T</td>
<td>15.0(1)M</td>
<td>12.4(22)T</td>
<td>Radar</td>
</tr>
<tr>
<td>MPLS Flows</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>MPLS + IPv4 Flows</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>MPLS + IPv6 Flows</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>Ingress VRF name Field</td>
<td>15.0(1)M</td>
<td>15.0(1)M</td>
<td>15.0(1)M</td>
<td>IOS XE 3.5.0S</td>
</tr>
<tr>
<td>Class-map Name (C3PL) Field</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
</tr>
<tr>
<td>4 Bytes AS Field</td>
<td>15.1(4)M</td>
<td></td>
<td></td>
<td>IOS XE 3.2.0S</td>
</tr>
<tr>
<td>MIB OID Field</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
</tr>
</tbody>
</table>
# Platform Feature Comparison

## Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>C 6500/Sup2T</th>
<th>C 4500/Sup7</th>
<th>C 3KX-SM-10G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Flows</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td>Radar</td>
</tr>
<tr>
<td>MPLS Flows</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>MPLS + IPv4 Flows</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>MPLS + IPv6 Flows</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>MPLS + IPv6/IPv4 Flows</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress VRF name Field</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td></td>
</tr>
<tr>
<td>Class-map Name (C3PL) Field</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>4 Bytes AS Field</td>
<td>12.2(50)SY</td>
<td>IOS XE 3.1.0SG</td>
<td></td>
</tr>
<tr>
<td>MIB OID Field</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
</tr>
</tbody>
</table>

Available Now | Not Available | Roadmap
## Platform Feature Comparison

### Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>Nexus 7000</th>
<th>Nexus 1000V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Flows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS Flows</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>MPLS + IPv4 Flows</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>MPLS + IPv6 Flows</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>MPLS + IPv6/IPv4 Flows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress VRF name Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class-map Name (C3PL) Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Bytes AS Field</td>
<td>4.2(1)</td>
<td></td>
</tr>
<tr>
<td>MIB OID Field</td>
<td>Radar</td>
<td></td>
</tr>
</tbody>
</table>
### Platform Feature Comparison

#### Flexible NetFlow

<table>
<thead>
<tr>
<th>Feature</th>
<th>CRS-1</th>
<th>XR12000</th>
<th>ASR9000</th>
<th>C12000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Flows</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>MPLS Flows</td>
<td>3.3.1</td>
<td>3.5.0</td>
<td>3.9(1)</td>
<td></td>
</tr>
<tr>
<td>MPLS + IPv4 Flows</td>
<td>3.3.1</td>
<td>3.5.0</td>
<td>3.9(1)</td>
<td></td>
</tr>
<tr>
<td>MPLS + IPv6 Flows</td>
<td>3.5.0</td>
<td>3.6.0</td>
<td>3.9(1)</td>
<td></td>
</tr>
<tr>
<td>MPLS + IPv6/IPv4 Flows</td>
<td>3.6.0</td>
<td>3.6.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress VRF name Field</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>Class-map Name (C3PL) Field</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
<tr>
<td>4 Bytes AS Field</td>
<td>3.4.0</td>
<td>3.4.0</td>
<td>3.9(1)</td>
<td></td>
</tr>
<tr>
<td>MIB OID Field</td>
<td>Radar</td>
<td>Radar</td>
<td>Radar</td>
<td></td>
</tr>
</tbody>
</table>

- **Available Now**: Green
- **Not Available**: Light Blue
- **Roadmap**: Orange
Agenda

• Introduction
• NetFlow Version 9
• Flexible NetFlow
• NetFlow for Security
• NetFlow for Application Visibility and Control
• NetFlow & IP v6
• NetFlow Performance
• NetFlow Standardization
• Support Matrix
• Conclusion
Recommended Reading

- Continue your Cisco Live learning experience with further reading from Cisco Press

Available Onsite at the Cisco Company Store
NetFlow Summary and Conclusion

- NetFlow is a mature Cisco IOS feature (in Cisco IOS since 1996)
- NetFlow provides input for accounting, performance, security, application visibility, and billing applications
- Cisco standardizes on NetFlow/IPFIX: NetFlow 9 and Flexible NetFlow consistency across many devices, including in hardware now
  - NetFlow v9 eases the exporting of additional fields
  - Flexible NetFlow is a major enhancement
- NetFlow is deployable today!
- NetFlow has IETF and industry leadership
- A lot of innovation around NetFlow. Stay tuned for more
- NetFlow/IPFIX export will become THE push mechanism 😊
References

▪ NetFlow
  – http://www.cisco.com/go/netflow

▪ Cisco network accounting services
  – Comparison of Cisco NetFlow versus other available accounting technologies

▪ Cisco IT case study

▪ A complete white paper

▪ NetFlow product manager: Jean Charles Griviaud
  – jgriviau@cisco.com
Meet the Engineer

To make the most of your time at Networkers at Cisco Live 2011, schedule a Face-to-Face Meeting with a top Cisco Engineer.

Designed to provide a "big picture" perspective as well as "in-depth" technology discussions, these face-to-face meetings will provide fascinating dialogue and a wealth of valuable insights and ideas.

Visit the Meeting Centre reception desk located in the Meeting Centre in World of Solutions.
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit [www.ciscolive.com](http://www.ciscolive.com).
Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions, booth 1042
- Come see demos of many key solutions and products in the main Cisco booth 2924
- Visit www.ciscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
  - Facebook: https://www.facebook.com/ciscoliveus
  - Twitter: https://twitter.com/#!/CiscoLive
  - LinkedIn Group: http://linkd.in/CiscoLI
Appendix: Traditional NetFlow
`show ip cache flow`

router# show 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 .125 .125 .250 .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 .500 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2728 active, 1368 inactive, 85310 added
  463824 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>Packets /Sec</th>
<th>Active (Sec)</th>
<th>Idle (Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-X</td>
<td>2</td>
<td>0.0</td>
<td>1</td>
<td>1440</td>
<td>0.0</td>
<td>0.0</td>
<td>9.5</td>
</tr>
<tr>
<td>TCP-other</td>
<td>82580</td>
<td>11.2</td>
<td>1</td>
<td>1440</td>
<td>11.2</td>
<td>0.0</td>
<td>12.0</td>
</tr>
<tr>
<td>Total:</td>
<td>82582</td>
<td>11.2</td>
<td>1</td>
<td>1440</td>
<td>11.2</td>
<td>0.0</td>
<td>12.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>DstIPaddress</th>
<th>Pr</th>
<th>SrcP DstP</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>132.122.25.60</td>
<td>Se0/0</td>
<td>192.168.1.1</td>
<td>06</td>
<td>9AEE 0007</td>
<td>1</td>
</tr>
<tr>
<td>Et0/0</td>
<td>139.57.220.28</td>
<td>Se0/0</td>
<td>192.168.1.1</td>
<td>06</td>
<td>708D 0007</td>
<td>1</td>
</tr>
<tr>
<td>Et0/0</td>
<td>165.172.153.65</td>
<td>Se0/0</td>
<td>192.168.1.1</td>
<td>06</td>
<td>CB46 0007</td>
<td>1</td>
</tr>
</tbody>
</table>
‘show ip cache verbose flow’

router# show 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
0.000  0.000  0.000  0.000  0.000  0.000  0.000  0.000  0.000  0.000  0.000  0.000  0.000  0.000
512  544  576  1024  1536  2048  2560  3072  3584  4096  4608
0.000  0.000  0.000  1.000  0.000  0.000  0.000  0.000  0.000  0.000  0.000

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>Packets Active(Sec)</th>
<th>Idle(Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-other</td>
<td>22210</td>
<td>3.1</td>
<td>1</td>
<td>1440</td>
<td>3.1</td>
<td>0.0</td>
</tr>
<tr>
<td>Total:</td>
<td>22210</td>
<td>3.1</td>
<td>1</td>
<td>1440</td>
<td>3.1</td>
<td>0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>DstIPaddress</th>
<th>Pr</th>
<th>TOS</th>
<th>Flgs</th>
<th>Pkts</th>
<th>NextHop</th>
<th>B/Pk</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>216.120.112.114</td>
<td>Se0/0</td>
<td>192.168.1.1</td>
<td>06</td>
<td>00</td>
<td>10</td>
<td>1</td>
<td>140</td>
<td>0.0</td>
<td>1</td>
</tr>
<tr>
<td>5FA7 /0 0</td>
<td>0007 /0 0</td>
<td>0.0.0.0</td>
<td>1440</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Et0/0</td>
<td>175.182.253.65</td>
<td>Se0/0</td>
<td>192.168.1.1</td>
<td>06</td>
<td>00</td>
<td>10</td>
<td>1</td>
<td>140</td>
<td>0.0</td>
<td>1</td>
</tr>
</tbody>
</table>
NetFlow Export Version 5 and Main Cache Configuration Example

Router # show ip flow export
Flow export v5 is enabled for main cache
  Exporting flows to 10.48.71.129 (9991)
  Exporting using source interface Loopback0
Version 5 flow records
  1303552 flows exported in 332208 udp datagrams
  0 flows failed due to lack of export packet
  2 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
  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
NetFlow Export Version 8 and Aggregation Configuration Example

Router(config)# ip flow-aggregation cache <cache type>
Router(config-flow-cache)# cache entries <number>
Router(config-flow-cache)# cache timeout active <minutes>
Router(config-flow-cache)# cache timeout inactive <seconds>
Router(config-flow-cache)# mask destination minimum <value>
Router(config-flow-cache)# mask source minimum <value>
Router(config-flow-cache)# export destination 10.10.10.10 1234
Router(config-flow-cache)# enabled
NetFlow Export Version 8 and Aggregation Configuration Example

Router # show ip flow export

... Cache for <cache-type> aggregation:
Exporting flows to 1.1.1.1 (9999)
Exporting using source IP address 192.1.1.5
1303631 flows exported in 332227 udp datagrams
...
Appendix: NetFlow for Capacity Planning
### The Core Traffic Matrix Traffic Engineering and Capacity Planning

<table>
<thead>
<tr>
<th>Rome Exit Point</th>
<th>Paris Exit Point</th>
<th>London Exit Point</th>
<th>Munich Exit Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rome Entry Point</td>
<td>NA (*)</td>
<td>... Mb/s</td>
<td>... Mb/s</td>
</tr>
<tr>
<td>Paris Entry Point</td>
<td>... Mb/s</td>
<td>NA (*)</td>
<td>... Mb/s</td>
</tr>
<tr>
<td>London Exit Point</td>
<td>... Mb/s</td>
<td>... Mb/s</td>
<td>NA (*)</td>
</tr>
<tr>
<td>Munich Exit Point</td>
<td>... Mb/s</td>
<td>... Mb/s</td>
<td>NA (*)</td>
</tr>
</tbody>
</table>

(*) Potentially Local Exchange Traffic
Core Capacity Planning the Big Picture

1. The ability to offer SLAs is dependent upon ensuring that core network bandwidth is adequately provisioned

2. Adequate provisioning (without gross over provisioning) is dependent upon accurate core capacity planning

3. Accurate core capacity planning is dependent upon understanding the core traffic matrix and flows and mapping these to the underlying topology

4. A tool for what if scenarios
BGP Next Hop TOS Aggregation

Typical Example

- **AS1**
- **AS2**
- **AS3**
- **AS4**
- **AS5**

**IP Core with BGP Routes Only**
- **MPLS Core**
- **Server Farm 1**
- **Server Farm 2**

- **Internal Traffic:** PE to PE
- **External Traffic Matrix:** PE to BGP AS

- **Customers**
# NetFlow BGP Next Hop TOS

**Aggregation Flow Keys**

**Key Fields (Uniquely Identifies the Flow)**
- Origin AS
- Destination AS
- Inbound Interface
- Output Interface
- ToS/DS C P (*)
- BGP Next Hop

**Additional Export Fields**
- Flows
- Packets
- Bytes
- First SysUptime
- Last SysUptime

(*) Before Any Recoloring
Core Traffic Matrix with Flexible NetFlow

Key Fields (Uniquely Identifies the Flow)
- Origin AS
- Destination AS
- Inbound Interface
- Output Interface
- ToS/DSCP (*)
- BGP Next Hop

Less flow records, less CPU impact

Potentially choose higher sampling rate for a better accuracy

(*) Before Any Recoloring

Additional Export Fields
- Flows
- Packets
- Bytes
- First SysUptime
- Last SysUptime
Core Traffic Matrix with Flexible NetFlow Configuration Example

- Export less flow records with a permanent cache
- However, must know the maximum number of entries

```
flow record traffic-matrix-record
  match routing destination as
  match interface input
  match ipv4 dscp
  match routing next-hop address ipv4 bgp
  collect counter bytes long
  collect timestamp sys-upptime first
  collect timestamp sys-upptime last

flow monitor traffic-matrix-monitor
  record traffic-matrix-record
  cache entries 10000
  cache type normal
  exporter capacity-planning-collector

interface pos3/0
  ip flow monitor traffic-matrix-monitor
```
Permanent Flexible NetFlow Configuration Using EEM + Cron + CLI

Export the content the permanent cache every one hour

If the time is synchronized across routers (NTP), we have a synchronized export (snapshot)