Cisco NetFlow Configuration
Best Practice / Highlights

- NetFlow configuration varies slightly per hardware model.
- Set active timeout to 1 minute: "ip flow-cache timeout active" is the time interval NetFlow records are exported for long lived flows (e.g. large FTP transfer). 1 minute is recommended and configuration is in minutes in IOS and seconds in MLS and NX-OS.
- Catalyst 6500/7600 require enabling NetFlow export within MSFC and PFC.
- The following command will capture NetFlow within the same VLAN for Catalyst 6500/7600: ip flow ingress layer2-switched vlan {vlanlist}
- NetFlow is based on 7 key fields
  - Source IP address
  - Destination IP address
  - Source port number
  - Destination port number
  - Layer 3 protocol type (ex. TCP, UDP)
  - ToS (type of service) byte
  - Input logical interface
- If one field is different, a new flow is created in the flow cache.
- Enabled NetFlow on EVERY layer-3 interface for complete visibility
- It is best practice to use a NetFlow "source interface" that would never go down such as a loopback interface.
- A "flow record" within Flexible NetFlow (that used in NX-OS) defines the keys that NetFlow uses to identify packets in the flow as well as other fields of interest that NetFlow gathers for the flow.
Cisco IOS NetFlow Configuration Guide

Netflow Configuration

In configuration mode issue the following to enable NetFlow Export:

- `ip flow-export destination <xe_netflow_collector_IP_address> 2055`
- `ip flow-export source <interface>` → (e.g. use a Loopback interface)
- `ip flow-export version 9` → (if version 9 does not take, use version 5)
- `ip flow-cache timeout active 1`
- `ip flow-cache timeout inactive 15`
- `snmp-server ifindex persist`

Enable NetFlow on each layer-3 interface you are interested in monitoring traffic for:

- `interface <interface>`
- `ip flow ingress`

Optional:

- `ip flow-export version 9 origin-as` → (to include BGP origin AS)
- `ip flow-capture mac-addresses` → `show ip cache verbose flow`
- `ip flow-capture vlan-id`

Note: If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T the `ip route-cache flow` command is used to enable NetFlow on an interface. If your router is running Cisco IOS release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later the `ip flow ingress` command is used to enable NetFlow on an interface.

Validate configuration:

- `show ip cache flow`
- `show ip flow export`
- `show ip flow interface`
- `show ip flow export template`

Reference:

Cisco 6500 and 7600 Series IOS NetFlow Configuration Guide

Native IOS Netflow Configuration:

In configuration mode issue the following to enable NetFlow Export:

```
mls nde sender version 5
mls aging long 64
mls aging normal 32
mls nde interface
mls flow ip interface-full
ip flow ingress layer2-switched vlan {vlanlist}

ip flow-export destination <xe_netflow_collector_IP_address> 2055
ip flow-export source <interface> → (e.g. use a Loopback interface)
ip flow-export version 9 → (if version 9 does not take, use version 5)
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
snmp-server ifindex persist
```

Enable NetFlow on each layer-3 interface you are interested in monitoring traffic for:

```
interface <interface>
ip flow ingress
```

Optional:

```
ip flow-capture mac-addresses
ip flow-capture vlan-id
```

Hybrid / CatOS Netflow Configuration:

```
set mls nde <xe_address> 2055
set mls nde version 5
set mls agingtime long 64
set mls agingtime 32
set mls flow full
set mls bridged-flow-statistics enable <vlanlist>
set mls nde enable
```

Validate configuration:

```
show ip cache flow
show ip flow export
show ip flow export template
show mls nde
```

Reference:

Cisco NetFlow Configuration

Catalyst 4500 Series Switch IOS NetFlow Configuration Guide

To use the NetFlow feature, you must have the Supervisor Engine V-10GE (the functionality is embedded in the supervisor engine), or the NetFlow Services Card (WS-F4531) and either a Supervisor Engine IV or a Supervisor Engine V.

Verify Daughter Card:

Switch# show module all

Mod | Submodule       | Model     | Serial No.    | Hw | Status
---|-----------------|-----------|---------------|----|--------
1.  | Netflow Services Card | WS-F4531 | JAB062209CG   | 0.2| Ok     
2.  | Netflow Services Card | WS-F4531 | JAB062209CG   | 0.2| Ok     

Netflow Configuration

In configuration mode on the 4500 issue the following to enable NetFlow Export:

- ip flow ingress
- ip flow ingress infer-fields
- ip flow-export destination <xe_netflow_collector_IP_address> 2055
- ip flow-export source <interface>  → (e.g. use a Loopback interface)
- ip flow-export version 5
- ip flow-cache timeout active 1
- ip flow-cache timeout inactive 15
- snmp-server ifindex persist

Validate configuration:

- show ip cache flow
- show ip flow export
- show ip flow interface

Reference:

Cisco NetFlow Configuration

Cisco 3850 NetFlow Configuration

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Cisco Bug Search Tool and the release notes for your platform and software release.

1. Create a Flow Record (specify the fields to export)

A flow record defines the information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. You specify a series of “match” and “collect” commands that tell the router which fields to include in the outgoing NetFlow PDU.

The “match” fields are the “key” fields. They are used to determine the uniqueness of the flow. The “collect” fields are just extra info that include to provide more detail to the collector for reporting and analysis.

The fields marked with required below, are fields required for StealthWatch to accept and build a flow record.

sw3850(config)# flow record LANCPE1
sw3850(config-flow-record)# description NetFlow record format to send to StealthWatch
sw3850(config-flow-record)# match datalink mac source address input
sw3850(config-flow-record)# match datalink mac destination address input
sw3850(config-flow-record)# match datalink vlan input key field
sw3850(config-flow-record)# match ipv4 ttl key field, provides pathing info
sw3850(config-flow-record)# match ipv4 tos required; key field
sw3850(config-flow-record)# match ipv4 protocol required; key field
sw3850(config-flow-record)# match ipv4 source address required; key field
sw3850(config-flow-record)# match ipv4 destination address required; key field
sw3850(config-flow-record)# match transport source-port required; key field
sw3850(config-flow-record)# match transport destination-port required; key field
sw3850(config-flow-record)# match interface input required; key field
sw3850(config-flow-record)# collect interface output required; used for computing bps rates
sw3850(config-flow-record)# collect counter bytes long required; used for bps calculation
sw3850(config-flow-record)# collect counter packets long required; used for pps calculation
sw3850(config-flow-record)# collect timestamp absolute first required; for calculating duration
sw3850(config-flow-record)# collect timestamp absolute last required; for duration
Cisco 3850 NetFlow Configuration

2. Create a Flow Exporter (specify where/how NetFlow is to be sent)

   sw3850(config)#flow exporter NETFLOW_TO_STEALTHWATCH
   sw3850(config-flow-exporter)#description Export NetFlow to StealthWatch
   sw3850(config-flow-exporter)#destination <fc_collector_IP_address>
   sw3850(config-flow-exporter)#source <interface> → (e.g. use a Loopback)
   sw3850(config-flow-exporter)#transport udp 2055

3. Create a Flow Monitor (tie the Flow Record to the Flow Exporter)

   sw3850(config)#flow monitor IPv4_NETFLOW
   sw3850(config-flow-monitor)#record LANCOPe1
   sw3850(config-flow-monitor)#exporter NETFLOW_TO_STEALTHWATCH
   sw3850(config-flow-monitor)#cache timeout active 60

4. Assign Flow Monitor to selected interfaces

   Repeat this step on every interface you are interested in monitoring traffic for.

   sw3850(config)#interface <interface> → (e.g. VLAN1 or g2/1)
   sw3850(config-if)#ip flow monitor IPv4_NETFLOW input

Validate configuration:

   show flow record LANCOPe1
   show flow monitor IPv4_NETFLOW statistics
   show flow monitor IPv4_NETFLOW cache

Reference:

Cisco 3560X & 3750X NetFlow Configuration

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Cisco Bug Search Tool and the release notes for your platform and software release.

Flexible NetFlow is supported on Catalyst 3560-X and 3750-X (Cat3k-X) Series Switches on the 10GE Service Module. Previously unsupported on the platform, the service module can enable hardware-supported, line-rate NetFlow on all traffic that traverses the module.

1. Create a Flow Record (specify the fields to export)

A flow record defines the information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. You specify a series of "match" and "collect" commands that tell the router which fields to include in the outgoing NetFlow PDU. The "match" fields are the "key" fields. They are used to determine the uniqueness of the flow. The "collect" fields are just extra info that to include to provide more detail to the collector for reporting and analysis.

The fields marked with **required** below, are fields required for StealthWatch to accept and build a flow record.

```
sw3X50(config)# flow record LANC0PE1
sw3X50(config-flow-record)# description NetFlow record format to send to StealthWatch
sw3X50(config-flow-record)# match datalink mac source address input
sw3X50(config-flow-record)# match datalink mac destination address input
sw3X50(config-flow-record)# match ipv4 ttl key field; provides pathing info
sw3X50(config-flow-record)# match ipv4 tos required; key field
sw3X50(config-flow-record)# match ipv4 protocol required; key field
sw3X50(config-flow-record)# match ipv4 source address required; key field
sw3X50(config-flow-record)# match ipv4 destination address required; key field
sw3X50(config-flow-record)# match transport source-port required; key field
sw3X50(config-flow-record)# match transport destination-port required; key field
sw3X50(config-flow-record)# collect interface input snmp required
sw3X50(config-flow-record)# collect interface output snmp
sw3X50(config-flow-record)# collect counter bytes required; used for bps calculation
sw3X50(config-flow-record)# collect counter packets required; used for pps calculation
sw3X50(config-flow-record)# collect timestamp sys-uptime first required; for duration
sw3X50(config-flow-record)# collect timestamp sys-uptime last required; for duration
```
Cisco 3560X & 3750X NetFlow Configuration

2. Create a Flow Exporter (specify where/how NetFlow is to be sent)
   sw3x50(config)#flow exporter NETFLOW_TO_STEALTHWATCH
   sw3x50(config-flow-exporter)#description Export NetFlow to StealthWatch
   sw3x50(config-flow-exporter)#destination <fc_collector_IP_address>
   sw3x50(config-flow-exporter)#source <interface> → (e.g. use a Loopback)
   sw3x50(config-flow-exporter)#transport udp 2055

3. Create a Flow Monitor (tie the Flow Record to the Flow Exporter)
   sw3x50(config)#flow monitor IPv4_NETFLOW
   sw3x50(config-flow-monitor)#record LANCOPE1
   sw3x50(config-flow-monitor)#exporter NETFLOW_TO_STEALTHWATCH
   sw3x50(config-flow-monitor)#cache timeout active 60

4. Assign Flow Monitor to selected interfaces
   Repeat this step on every interface you are interested in monitoring traffic for.
   sw3x50(config)#interface <interface> → (e.g. VLAN1 or g2/1)
   sw3x50(config-if)#ip flow monitor IPv4_NETFLOW input

Validate configuration:
  show flow record LANCOPE1
  show flow monitor IPv4_NETFLOW statistics
  show flow monitor IPv4_NETFLOW cache

Reference:
Cisco Nexus 7000 NetFlow Configuration—using netflow-original

The Cisco Nexus 7000 switch runs Cisco NX-OS operating system. Configuring Netflow is a little different than in traditional IOS devices. Follow the below 5 steps to enable Netflow monitoring.

1. Enable Netflow Feature and set timeouts
   ```
   switch(config)#feature netflow
   switch(config)#flow timeout active 60
   switch(config)#flow timeout inactive 15
   ```

2. Create a Flow Record (specify the fields to export)
   We will use the Nexus predefined record of “netflow-original” for this configuration.
   See Creating a Flow Record section of appendix for creating a custom flow record.

3. Create a Flow Exporter (specify where/how NetFlow is to be sent)
   ```
   switch(config)#flow exporter netflow_to_stealthwatch
decription Export NetFlow to StealthWatch
destination <xe_collector_IP_address>
source <interface> → (e.g. use a Loopback)
transport udp 2055
version 9
   ```

4. Create a Flow Monitor (tie the Flow Record to the Flow Exporter)
   ```
   switch(config)#flow monitor standard_v9netflow
   record netflow-original
   exporter netflow_to_stealthwatch
   ```

5. Assign Flow Monitor to selected interfaces
   Repeat this step on every interface you are interested in monitoring traffic for.
   ```
   switch(config)#interface <interface> → (e.g. VLAN1 or g2/1)
   ip flow monitor standard_v9netflow input
   ```

Validate configuration:

   show flow record netflow-original
   show flow monitor standard_v9netflow statistics
   show flow monitor standard_v9netflow cache

Reference:

Cisco Nexus 1000v NetFlow Configuration - using netflow-original

The Cisco Nexus 1000v switch is a virtual switch that runs Cisco NX-OS. Configuring Netflow is a little different than in traditional IOS devices. Follow the below 4 steps to enable Netflow monitoring.

1. Create a Flow Record (specify the fields to export)
   We will use the Nexus predefined record of “netflow-original” for this configuration.
   See Creating a Flow Record section of appendix for creating a custom flow record.

2. Create a Flow Exporter (specify where/how NetFlow is to be sent)
   ```
   n1000v(config)# flow exporter netflow_to_stealthwatch
   n1000v(config-flow-exporter)# description Export NetFlow to StealthWatch
   n1000v(config-flow-exporter)# destination <xe_collector_IP_address>
   n1000v(config-flow-exporter)# source mgmt 0
   n1000v(config-flow-exporter)# transport udp 2055
   n1000v(config-flow-exporter)# version 9
   ```

3. Create a Flow Monitor (tie the Flow Record to the Flow Exporter)
   ```
   n1000v(config)# flow monitor standard_v9netflow
   n1000v(config-flow-monitor)# record netflow-original
   n1000v(config-flow-monitor)# exporter netflow_to_stealthwatch
   n1000v(config-flow-monitor)# timeout active 60
   n1000v(config-flow-monitor)# timeout inactive 15
   ```

4. Assign Flow Monitor to selected interfaces
   Repeat this step on every interface you are interested in monitoring traffic for.
   ```
   n1000v(config)# interface <interface> → (e.g. VLAN1 or g2/1)
   n1000v(config-if)# ip flow monitor standard_v9netflow input
   ```

Validate configuration:

- show flow record netflow-original
- show flow monitor standard_v9netflow statistics
- show flow monitor standard_v9netflow cache

Reference:
Cisco ASR 1000 NetFlow Configuration

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Cisco Bug Search Tool and the release notes for your platform and software release.

Flexible NetFlow is supported on Catalyst 3560-X and 3750-X (Cat3k-X) Series Switches on the 10GE Service Module. Previously unsupported on the platform, the service module can enable hardware-supported, line-rate NetFlow on all traffic that traverses the module.

1. Create a Flow Record (specify the fields to export)
A flow record defines the information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. You specify a series of “match” and “collect” commands that tell the router which fields to include in the outgoing NetFlow PDU. The “match” fields are the “key” fields. They are used to determine the uniqueness of the flow. The “collect” fields are just extra info that to include to provide more detail to the collector for reporting and analysis.

The fields marked with required below, are fields required for StealthWatch to accept and build a flow record.

```
    asr1k(config)# flow record LANCOPES
    asr1k(config-flow-record)# match ipv4 protocol required; key field
    asr1k(config-flow-record)# match ipv4 source address required; key field
    asr1k(config-flow-record)# match ipv4 destination address required; key field
    asr1k(config-flow-record)# match transport source-port required; key field
    asr1k(config-flow-record)# match transport destination-port required; key field
    asr1k(config-flow-record)# match interface input required; key field
    asr1k(config-flow-record)# match ipv4 tos required; key field
    asr1k(config-flow-record)# collect interface output required; used for computing bps rates
    asr1k(config-flow-record)# collect counter bytes required; used for pps calculation
    asr1k(config-flow-record)# collect counter packets required; for calculating duration
    asr1k(config-flow-record)# collect timestamp sys-uptime first required; for calculating duration
    asr1k(config-flow-record)# collect timestamp sys-uptime last required; for calculating duration
    asr1k(config-flow-record)# collect flow sampler optional; used to obtain sampling rate
    asr1k(config-flow-record)# collect routing next-hop address ipv4 optional; used for closest interface determination
    asr1k(config-flow-record)# collect ipv4 dscp optional; used to generate QoS reports
    asr1k(config-flow-record)# collect ipv4 ttl minimum optional; provides pathing info
    asr1k(config-flow-record)# collect ipv4 ttl maximum optional; provides pathing info
    asr1k(config-flow-record)# collect transport tcp flags optional; security analysis
    asr1k(config-flow-record)# collect routing destination as optional; enable if you use BGP
```
Cisco ASR 1000 NetFlow Configuration

6. Create a Flow Exporter (specify where/how NetFlow is to be sent)
   asr1k(config)#flow exporter NETFLOW_TO_STEALTHWATCH
   asr1k(config-flow-exporter)#description Export NetFlow to StealthWatch
   asr1k(config-flow-exporter)#destination <fc_collector_IP_address>
   asr1k(config-flow-exporter)#source <interface> → (e.g. use a Loopback)
   asr1k(config-flow-exporter)#transport udp 2055
   asr1k(config-flow-exporter)#version 9

7. Create a Flow Monitor (tie the Flow Record to the Flow Exporter)
   asr1k(config)#flow monitor IPv4_NETFLOW
   asr1k(config-flow-monitor)#record LANCOPe1
   asr1k(config-flow-monitor)#exporter NETFLOW_TO_STEALTHWATCH
   asr1k(config-flow-monitor)#cache timeout active 60
   asr1k(config-flow-monitor)#cache timeout inactive 15

8. Assign Flow Monitor to selected interfaces
   Repeat this step on every interface you are interested in monitoring traffic for.
   asr1k(config)#interface <interface> → (e.g. VLAN1 or g2/1)
   asr1k(config-if)#ip flow monitor IPv4_NETFLOW input

If the ASR is being used for NAT and you would like to log the NAT translations within StealthWatch, run the following command:

   ip nat log translations flow-export v9 udp destination X.X.X.X YYYY

Where X.X.X.X is the FlowCollector IP and YYYY is the configured NetFlow Export port.

Validate configuration:

   show flow record LANCOPe1
   show flow monitor IPv4_NETFLOW statistics
   show flow monitor IPv4_NETFLOW cache

Reference:
Cisco ASR 9000 NetFlow Configuration

Consider the following restrictions when configuring NetFlow in Cisco IOS XR software: You must configure a source interface. If you do not configure a source interface, the exporter will remain in a disabled state. Cisco IOS XR software supports export format Version 9 only. You must configure a valid record map name for every flow monitor map. Please refer to the below reference link for detailed steps. The ASR9000 can sample flow export, Lancope recommends export 1:1 where possible for 100% visibility and accounting. This will be specific to the environment being deployed in.

1. **Configuring an Exporter Map**
   - router(config)# flow exporter-map FLOW_TO_SW
   - router(config- FLOW_TO_SW)# destination <xe_collector_IP_address>
   - router(config- FLOW_TO_SW)# source <interface> → (e.g. use a Loopback)
   - router(config- FLOW_TO_SW)# transport udp 2055
   - router(config- FLOW_TO_SW)# version v9

2. **Configuring a Monitor Map**
   - router(config)# flow monitor-map IPv4_NETFLOW
   - router(config- IPv4_NETFLOW)# record ipv4
   - router(config- IPv4_NETFLOW)# cache timeout active 60
   - router(config- IPv4_NETFLOW)# cache timeout inactive 15
   - router(config- IPv4_NETFLOW)# exporter FLOW_TO_SW

3. **Applying a Monitor Map to an Interface**
   - router(config)# interface <interface> → (e.g. gigabitEthernet 0/0/0/0)
   - router(config-if)# flow ipv4 monitor IPv4_NETFLOW ingress

**Validate configuration:**

- show flow exporter-map FLOW_TO_SW
- show flow monitor-map IPv4_NETFLOW

**Reference:**

IPv6 NetFlow Export

Review the below reference links for detailed understanding of IPv6 NetFlow export.

In configuration mode issue the following to enable NetFlow Export:

```
ipv6 flow-export destination <xe_netflow_collector_IP_address> 2055
ip flow-export source <interface> → (e.g. use a Loopback interface)
ipv6 flow-export version 9
ipv6 flow-cache timeout active 1
ipv6 flow-cache timeout inactive 15
snmp-server ifindex persist
```

Enable NetFlow on each layer-3 interface you are interested in monitoring traffic for:

```
interface <interface>
ipv6 flow ingress
```

Optional:

```
ipv6 flow-export version 9 origin-as → (to include BGP origin AS)
```

Validate configuration:

```
show ip cache flow
```

Reference:

Appendix: Creating a Flow Record & Various Show Commands

Creating a Flow Record

A flow record defines the information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. If you would like to build a custom flow record outside of the predefined “netflow-original”, you would specify a series of “match” and “collect” commands that tell the router which fields to include in the outgoing NetFlow PDU.

The “match” fields are the “key” fields. They are used to determine the uniqueness of the flow. The “collect” fields are just extra info that we include to provide more detail to the collector for reporting and analysis.

You don’t want to modify the “match” fields much. The seven match entries shown below should always be included in your FnF config. The “collect” fields however can vary quite a bit depending on how much info you want to send to the collector. The configuration listed below is recommended for all StealthWatch installations.

The fields marked with required below, are fields required for StealthWatch to accept and build a flow record.

```
switch(config)#flow record LANCOP1
switch(config-flow-record)#match ipv4 protocol required; key field
switch(config-flow-record)#match ipv4 source address required; key field
switch(config-flow-record)#match ipv4 destination address required; key field
switch(config-flow-record)#match transport source-port required; key field
switch(config-flow-record)#match transport destination-port required; key field
switch(config-flow-record)#match interface input required; key field
switch(config-flow-record)#match ipv4 tos required; key field
```

```
switch(config-flow-record)#collect interface output required; used for computing bps rates
switch(config-flow-record)#collect counter bytes required; used for bps calculation
switch(config-flow-record)#collect counter packets required; for calculating duration
switch(config-flow-record)#collect timestamp sys-uptime first required; for calculating duration
```

```
switch(config-flow-record)#collect routing next-hop address ipv4 optional; used for closest interface determination
```

```
switch(config-flow-record)#collect ipv4 dscp optional; used to generate QoS reports
switch(config-flow-record)#collect ipv4 ttl minimum optional; provides pathing info
switch(config-flow-record)#collect ipv4 ttl maximum optional; provides pathing info
switch(config-flow-record)#collect transport tcp flags optional; security analysis
```

```
switch(config-flow-record)#collect routing destination as optional; enable if you use BGP
```

Once the “Flow Record” has been created you would tie it to a “Flow Monitor”

Reference:
show ip cache flow

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Total Flows</th>
<th>Flows/Sec</th>
<th>Flows/Pkt</th>
<th>Packets/Sec</th>
<th>Pkts/Sec</th>
<th>Active</th>
<th>Idle</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-TELnet</td>
<td>3008</td>
<td>0.0</td>
<td>2 93</td>
<td>0.0</td>
<td>6.9</td>
<td>15.4</td>
<td></td>
</tr>
<tr>
<td>TCP-FTP</td>
<td>10</td>
<td>0.0</td>
<td>1 51</td>
<td>0.0</td>
<td>1.8</td>
<td>15.4</td>
<td></td>
</tr>
<tr>
<td>TCP-IPX</td>
<td>1994</td>
<td>0.0</td>
<td>938 1441</td>
<td>3.1</td>
<td>0.3</td>
<td>1.7</td>
<td></td>
</tr>
<tr>
<td>TCP-HTTP</td>
<td>27</td>
<td>0.0</td>
<td>1 45</td>
<td>0.0</td>
<td>0.7</td>
<td>15.4</td>
<td></td>
</tr>
<tr>
<td>TCP-other</td>
<td>4623</td>
<td>0.0</td>
<td>160 40</td>
<td>14.6</td>
<td>14.4</td>
<td>15.3</td>
<td></td>
</tr>
<tr>
<td>UDP-DNS</td>
<td>75959</td>
<td>0.1</td>
<td>1 60</td>
<td>0.1</td>
<td>0.4</td>
<td>14.2</td>
<td></td>
</tr>
<tr>
<td>UDP-NTCP</td>
<td>8009</td>
<td>0.0</td>
<td>1 76</td>
<td>0.0</td>
<td>0.0</td>
<td>15.4</td>
<td></td>
</tr>
<tr>
<td>UDP-other</td>
<td>3152955</td>
<td>4.6</td>
<td>35 1231</td>
<td>165.9</td>
<td>19.2</td>
<td>13.2</td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>24797</td>
<td>0.0</td>
<td>32 556</td>
<td>1.1</td>
<td>18.6</td>
<td>7.7</td>
<td></td>
</tr>
<tr>
<td>IOMP</td>
<td>18</td>
<td>0.0</td>
<td>1 59</td>
<td>0.0</td>
<td>0.0</td>
<td>15.3</td>
<td></td>
</tr>
<tr>
<td>IP-Other</td>
<td>17907</td>
<td>0.0</td>
<td>15 60</td>
<td>0.4</td>
<td>58.6</td>
<td>1.6</td>
<td></td>
</tr>
</tbody>
</table>

Total: 2621253

show ip flow export

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10.201.102.4.91</td>
<td>11 C99D 9007 17</td>
<td>V140</td>
<td>UDP</td>
<td>10.201.102.141</td>
<td>11 C99D 9007 17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.202.2.126</td>
<td>11 C99D 9007 17</td>
<td>V140</td>
<td>UDP</td>
<td>10.201.102.141</td>
<td>11 C99D 9007 17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.202.2.216</td>
<td>11 C99D 9007 17</td>
<td>V140</td>
<td>UDP</td>
<td>10.201.102.141</td>
<td>11 C99D 9007 17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.201.1.140</td>
<td>11 C99D 9007 66</td>
<td>V140</td>
<td>UDP</td>
<td>10.201.1.140</td>
<td>11 C99D 9007 66</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cisco NetFlow Configuration

Best Practice / Highlights

Cisco IOS NetFlow Configuration Guide

Cisco 6500 & 7600 NetFlow Configuration Guide

Catalyst 4500 NetFlow Configuration Guide

Cisco 3850 NetFlow Configuration Guide

Cisco 3560 & 3750 NetFlow Configuration Guide

Cisco Nexus 7000 NetFlow Configuration

Cisco Nexus 1000v NetFlow Configuration

Cisco ASR 9000 NetFlow Configuration

Appendix

show ip flow interface

```
lohome1#show ip flow interface
Dot11Radio0
  ip flow ingress
FastEthernet4
  ip flow ingress
Vlan1
  ip flow ingress
PV1
  ip flow ingress
```

show ip flow export template

```
LCQSW01#show ip flow export template
Template Options flag = 1
Total number of Templates added = 3
Total active Templates = 3
Flow Templates active = 2
Flow Templates added = 2
Option Templates active = 1
Option Templates added = 1
Template ager polls = 1132420
Option Template ager polls = 566291
Main cache version 9 export is enabled
Template export information
  Template timeout = 30
  Template refresh rate = 20
  Option export information
  Option timeout = 30
  Option refresh rate = 20
```

show mls nde

```
LCQSW01#show mls nde
Netflow Data Export enabled
Exporting flows to 10.203.1.108 (2054)
Exporting flows from 10.201.0.1 (53191)
Version: 9
Layer2 flow creation is enabled on vlan 1,168,192,201-204,100-206,240
Layer2 flow export is enabled on vlan 1,168,192,201-204,200-206,240
Include Filter not configured
Exclude Filter not configured
Total Netflow Data Export Packets are:
  1177779 packets, 0 no packets, 37541599 records
Total Netflow Data Export Send Errors:
  IPWRITE_NO_FIFO = 0
  IPWRITE_AGJ_FAILED = 0
  IPWRITE_PROCESS = 0
  IPWRITE_ENQUEUE_FAILED = 0
  IPWRITE_IPC_FAILED = 0
  IPWRITE_OUTPUT_FAILED = 0
  IPWRITE_NETU_FAILED = 0
  IPWRITE_ENCAPPX_FAILED = 0
Netflow Aggregation Disabled
```

show run | inc mls

```
LCQSW01#show run | inc mls
mls aging long 64
mls aging normal 32
mls netflow interface
mls flow ip interface-full
mls nde sender
mls cef error action reset
```
show l3-mgr flowmask

LCHQSW01#show l3-mgr flowmask
  current flowmask registries for protocol:
          | fmask\idx|  00  |  01  |  10  |
          | ip       | null | ip-full | null |
          | ipv6     | null | null    | null |
          | mpls     | null | null    | null |
          | mac      | null | null    | null |
          | ---------|------|---------|------|
NDF for IPv4 is NOT globally enabled!

l3_mg_flowmask[proto/fold]: [ipv6/ no]
l3_mg_flow currently in use: [ipv6/ no]
l3_mg_flows[proto/context/fmask]{pack_count} [IPv6: 0 / 1]
l3_mg_current_flowmask{proto/val}: [ip / if-full ]
current ip flowmask for unicast: if-full
current ipv6 flowmask for unicast: null

show mls netflow table-contention summary

LCHQSW01#show mls netflow table-contention summary
Earl in Module 5
Summary of Netflow CAM Utilization (as a percentage)

TCAM Utilization : 2%
ICAM Utilization : 0%
Netflow Creation Failures : 0
Netflow CAM aliases : 0

show mls netflow ip

LCHQSW01#show mls netflow ip
Displaying Netflow entries in Active Supervisor EARL in module 5

| Pkts | Bytes | SrcIP | Port | SrcPort:DestPort | Src/i/f | :AdjPt
|------|-------|-------|------|------------------|---------|-------
| 10.203.0.10 | 10.201.3.53 | top :3544 | 1528 | V11 | :0X0 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 10.201.3.12 | 10.200.1.21 | top :15603 | 3260 | V11 | :0X0 |
| 5 | 609 | 23 | 03:32:54 | L2 - Dynamic |
| 10.242.194 | 10.201.0.25 | top :1121 | 1176 | V11 | :0X0 |
| 1 | 280 | 31 | 03:32:50 | L3 - Dynamic |
| 10.201.0.10 | 10.201.3.12 | top :1115 | 139 | V11 | :0X0 |
| 0 | 0 | 6 | 03:32:54 | L2 - Dynamic |
| 10.201.0.12 | 192.168.1.111 | udp :41830 | dns | V11 | :0X0 |
| 1 | 56 | 30 | 03:32:30 | L3 - Dynamic |
| 10.201.1.162 | 10.201.1.154 | tcp :48159 | 443 | V11 | :0X0 |
| 0 | 0 | 9 | 03:32:52 | L2 - Dynamic |
| 10.201.0.21 | 10.201.0.12 | top :3268 | 15710 | V11 | :0X0 |

--More--