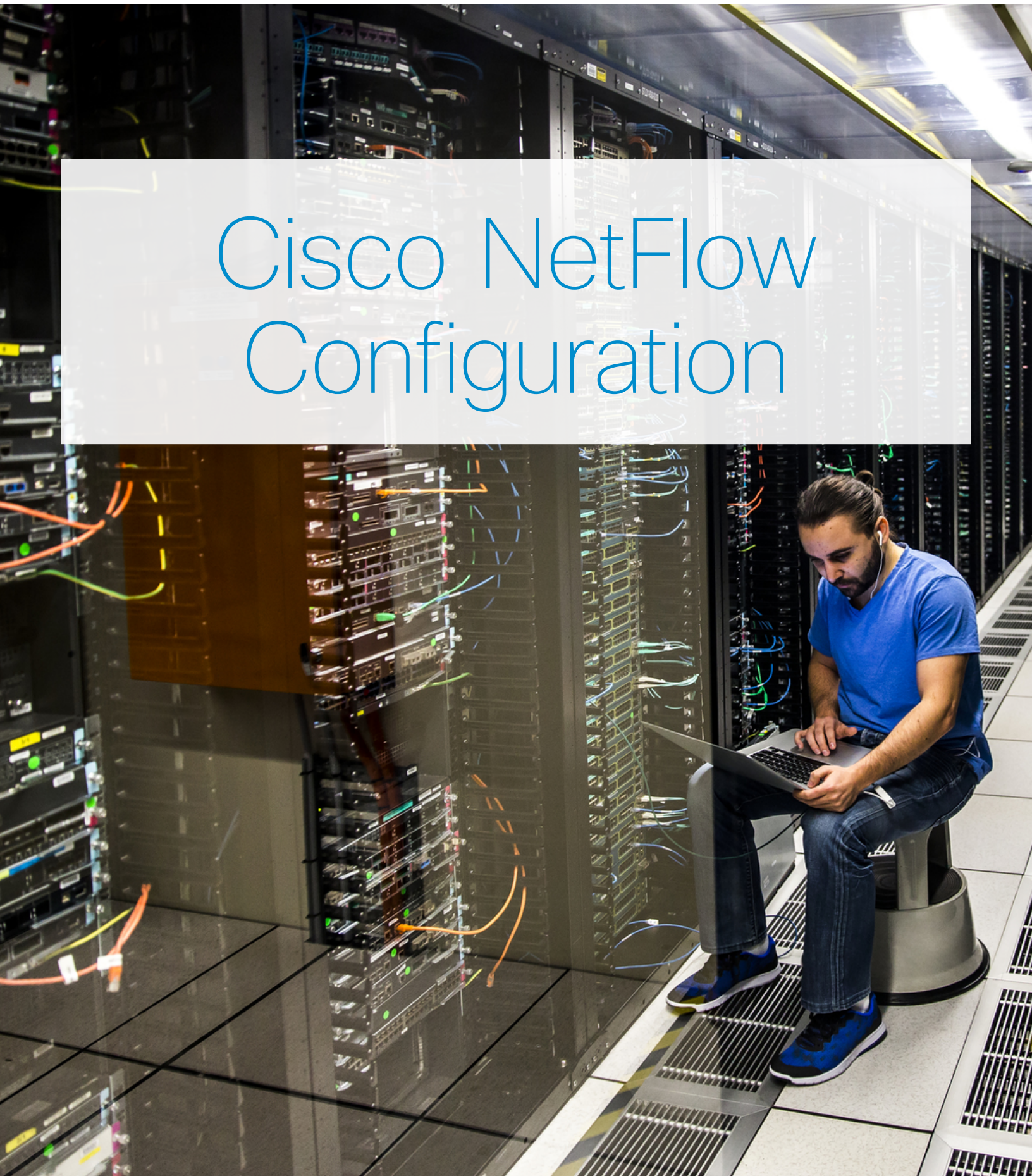

Cisco NetFlow Configuration

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:

http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/12_2sr/nf_12_2sr_book.html

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:

http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/nde.html

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

.

<cut for brevity>

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:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/25ew/configuration/guide/nfswitch.html

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 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.

```
sw3850(config)# flow record LANCOPE1
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:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/flexible_netflow/command_reference/b_fnf_32se_3850_cr_chapter_010.html

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 LANCOPE1
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; key field
sw3X50(config-flow-record)# collect interface output snmp           required
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:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps10745/white_paper_c11-691508_ps10744_Products_White_Paper.html

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**
switch(config-flow-exporter)#**description Export NetFlow to StealthWatch**
switch(config-flow-exporter)#**destination** **<xe_collector_IP_address>**
switch(config-flow-exporter)#**source** **<interface>** → *(e.g. use a Loopback)*
switch(config-flow-exporter)#**transport udp 2055**
switch(config-flow-exporter)#**version 9**

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

switch(config)#f**low monitor standard_v9netflow**
switch(config-flow-monitor)#**record netflow-original**
switch(config-flow-monitor)#**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)
switch(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:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/system_management/configuration/guide/sm_netflow.html

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:

http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0/system_management/configuration/guide/system_9flow.html

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 LANCOPE1**	
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 bps calculation*
asr1k(config-flow-record)#**collect counter packets**	*required; used for pps calculation*
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 anaysis*
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:

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/xe-3s/asr1000/cfg-de-fnflow-exprts-xe.html

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/xe-3s/cfg-avc-xe.html

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:

http://www.cisco.com/en/US/docs/routers/asr9000/software/asr9k_r3.9.1/netflow/configuration/guide/nfc391flow.html

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:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-netflow.html

http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/nfv9_ipv6.html

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 LANCOPE1**	
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; used for pps calculation*
switch(config-flow-record)#**collect timestamp sys-uptime first**	*required; for calculating duration*
switch(config-flow-record)#**collect timestamp sys-uptime last**	*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 anaysis*
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:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/ps6965/prod_white_paper0900aecd804be1cc.html

show ip cache flow

```
LCHQSW01#show ip cache flow

------------------------------------------------------------------------------

Displaying software-switched flow entries on the MSFC in Module 5:

IP packet size distribution (116635425 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .074 .016 .005 .004 .010 .004 .007 .000 .001 .000 .002 .002 .001 .005

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .003 .007 .063 .787 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  136 active, 3960 inactive, 2812503 added
  93810001 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
  272 active, 752 inactive, 5624981 added, 2812503 added to flow
  0 alloc failures, 15446 force free
  1 chunk, 840 chunks added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet        3008      0.0         2    43      0.0      6.9      15.4
TCP-FTP             10      0.0         1    52      0.0      1.8      15.4
TCP-WWW          13984      0.0       938  1491     23.1      0.3       1.7
TCP-SMTP            27      0.0         1    45      0.0      0.7      15.4
TCP-other        46023      0.0       180    48     14.6     14.4      15.3
UDP-DNS          75959      0.1         1    68      0.1      0.4      14.2
UDP-NTP           8009      0.0         1    76      0.0      0.0      15.4
UDP-other      2622929      4.6        35  1231    165.9     19.2      11.2
ICMP             24379      0.0        32   558      1.3     38.6       7.7
IGMP                18      0.0         1    39      0.0      1.0      15.5
IP-other         17907      0.0        13    60      0.4     50.6       1.8
Total:         2812253      4.9        41  1168    205.7     18.9      11.2

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
V1240         209.182.184.1   Null          10.202.4.91     11 C39D 0807    17
V1240         209.182.184.1   Null          10.202.4.90     11 C39D 0807    17
V1240         209.182.184.1   Null          10.202.2.164    11 C39D 0807    17
V1240         209.182.184.1   Null          10.202.2.163    11 C39D 0807    17
V1240         209.182.184.1   Null          10.202.2.216    11 C39D 0807    17
V1240         209.182.184.1   Null          10.202.2.215    11 C39D 0807    17
V1240         209.182.184.1   Null          10.202.2.213    11 C39D 0807    17
V1240         10.201.1.162    Null          10.203.7.4      11 8006 0807    66
 --More--
```

show ip flow export

```
LCHQSW01#show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Source(1)       10.201.0.1 (Vlan1)
    Destination(1)  10.203.1.108 (2055)
  Version 9 flow records
  2837811 flows exported in 129115 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  11 export packets were dropped due to no fib
  16 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
```

show ip flow interface

```
lchome1#show ip flow interface
Dot11Radio0
  ip flow ingress
FastEthernet4
  ip flow ingress
Vlan1
  ip flow ingress
BVI1
  ip flow ingress
```

show ip flow export template

```
LCHQSW01#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

```
LCHQSW01#show mls nde
 Netflow Data Export enabled
 Exporting flows to  10.203.1.108 (2055)
 Exporting flows from 10.201.0.1 (53191)
 Version: 9
 Layer2 flow creation is enabled on vlan 1,168,192,201-204,208-209,240
 Layer2 flow export is enabled on vlan 1,168,192,201-204,208-209,240
 Include Filter not configured
 Exclude Filter not configured
 Total Netflow Data Export Packets are:
    1177779 packets, 0 no packets, 37561689 records
 Total Netflow Data Export Send Errors:
        IPWRITE_NO_FIB = 0
        IPWRITE_ADJ_FAILED = 0
        IPWRITE_PROCESS = 0
        IPWRITE_ENQUEUE_FAILED = 0
        IPWRITE_IPC_FAILED = 0
        IPWRITE_OUTPUT_FAILED = 0
        IPWRITE_MTU_FAILED = 0
        IPWRITE_ENCAPFIX_FAILED = 0
 Netflow Aggregation Disabled
```

show run | inc mls

```
LCHQSW01#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   |  if-full |   null   |
 |----------+----------+----------+----------|
 |   ipv6   |   null   |   null   |   null   |
 |----------+----------+----------+----------|
 |   mpls   |   null   |   null   |   null   |
 |----------+----------+----------+----------|
 |   mac    |   null   |   null   |   null   |
 |----------+----------+----------+----------|
 NDE for IPv4 is NOT globally enabled!

 l3_mgr_fmask_pending[proto/val]: [ipv6/ no]
 l3_mgr_fie_was_busy[proto/val]:   [ipv6/ no]
 l3_mgr_flowmask[proto:context/fmaskpak_count]: [ipv6: 0 / 1]
 l3_mgr_current_cli_fmask[prot/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
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f          :AdjPtr
------------------------------------------------------------------------------
Pkts          Bytes          Age   LastSeen  Attributes
-------------------------------------------------
10.203.0.10     10.201.3.53     tcp :3544   :5222     Vl1              :0x0
0             0              30    03:32:30   L2 - Dynamic
10.201.0.16     10.201.0.21     tcp :15683  :3268     Vl1              :0x0
5             809            23    03:32:54   L2 - Dynamic
10.242.0.194    10.201.0.25     tcp :1121   :1178     Vl1              :0x0
2             280            31    03:32:30   L3 - Dynamic
10.201.0.10     10.201.3.122    tcp :1115   :139      Vl1              :0x0
0             0              6     03:32:54   L2 - Dynamic
10.201.0.12     192.168.1.111   udp :41838  :dns      Vl168            :0x0
1             56             30    03:32:30   L3 - Dynamic
10.201.1.162    10.201.1.164    tcp :48159  :443      Vl1              :0x0
0             0              9     03:32:52   L2 - Dynamic
10.201.0.21     10.201.0.12     tcp :3268   :15710    Vl1              :0x0
 --More--
```