

SolarWinds Technical Reference

Configuring Devices for Flow Collection

Introduction.....	3
Cisco	3
Cisco Catalyst 3560/3750	4
Cisco Catalyst 4500	7
Cisco Catalyst 6500	9
Cisco Nexus 7000/7010.....	11
Cisco ASA 5500.....	14

This paper provides annotated NetFlow configuration examples for devices that present challenges setting up for use with SolarWinds NTA.

Copyright© 1995-2014 SolarWinds Worldwide, LLC. All rights reserved worldwide.

No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, the SolarWinds & Design, ipMonitor, LANsurveyor, Orion, and other SolarWinds marks, identified on the SolarWinds website, as updated from SolarWinds from time to time and incorporated herein, are registered with the U.S. Patent and Trademark Office and may be registered or pending registration in other countries. All other SolarWinds trademarks may be common law marks or registered or pending registration in the United States or in other countries. All other trademarks or registered trademarks contained and/or mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies. Microsoft®, Windows®, and SQL Server® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Revised: 5/28/2014

Introduction

The sections of this document—organized alphabetically by vendor—provide NetFlow configuration examples for network devices that sometimes present problems in preparing them to work with SolarWinds NetFlow Traffic Analyzer.

Cisco

Cisco Catalyst 3560/3750

Cisco Catalyst 4500

Cisco Catalyst 6500

Cisco Nexus 7000

Cisco ASA 5500

For detailed information about setting up devices to use with SolarWinds NetFlow Traffic Analyzer, refer to the section “Setting up Network Devices to Export NetFlow Data” in the SolarWinds NetFlow Traffic Analyzer Administrator Guide.

Cisco Catalyst 3560/3750

Standard 3750 and 3560 switches do not support NetFlow. The 3750-X and 3560-X L3 switches only support NetFlow if they have the C3KX-SM-10G Service module; and in this case the only option is using Flexible NetFlow.

The tasks involved in creating a Flexible NetFlow configuration are:

1. Enabling ingress and egress on the C3KX-SM-10G module uplink ports.
2. Creating and configuring the flow record.
3. Creating and configuring the flow exporter(s).
4. Creating a flow monitor to bind the flow record to the exporter.
5. Applying the flow monitor to the appropriate interface on the device.

The following configuration example creates a custom flow record and flow monitor. Each section in the example—flow record, flow exporter, flow monitor—includes notes that explain what the commands are doing.

Interface Setup

```
!
interface TenGigabitEthernet1/1/1
switchport trunk encapsulation dot1q
switchport mode trunk
ip flow monitor NetFlow input
ip flow monitor NetFlow output
!
interface TenGigabitEthernet1/1/2
switchport trunk encapsulation dot1q
switchport mode trunk
ip flow monitor NetFlow input
ip flow monitor NetFlow output
```

You must enable ingress and egress on the C3KX-SM-10G module uplink ports since they are the only interfaces on the module that support NetFlow export functionality.

Flow Record

```
Flow record NetFlow
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect interface input snmp
collect interface output snmp
collect counter bytes
collect counter packets
```

The flow record part of this configuration example creates the record called “NetFlow” and uses the **match ipv4**, **match transport**, and **collect** commands to define the key fields in the record by which flow data will be processed. For more information on these commands, see this [Cisco command reference](#).

Flow Exporter

```
flow exporter NetFlow-to-Orion
  destination 10.10.10.10
  source vlan254
  transport udp 2055
export-protocol netflow-version 9
```

The flow exporter part of the configuration examples defines an exporter (called “NetFlow-to-Orion”) the **destination** (the IP address of the Orion server) to which flow data will be exported, the **source** interface (here called ‘vlan254’; it’s the interface with the IP address with which Orion is managing the device) from which flow data will be exported, the **transport** protocol and port (udp, 2055—Orion’s collection port) through which the flow data will pass, and the NetFlow **export protocol** (netFlow version 9) that the NetFlow collector should expect and use to process the data.

Flow Monitor

```
flow monitor NetFlow-Monitor
  description Original Netflow captures
  record ipv4
  exporter NetFlow-to-Orion
cache timeout inact 10
cache timeout act 5
interface TenGigabitEthernet1/1/1
interface TenGigabitEthernet1/1/2
ip flow monitor NetFlow-Monitor input
```

The flow monitor part of the configuration example creates a monitor (called “NetFlow-Monitor”) that uses the **record** and **exporter** commands to bind the flow record (ipv4) to the flow exporter (NetFlow-to-Orion) you already created. The **interface** command defines the interface (two of them, in this case) to which the flow monitor NetFlow-Monitor applies; and the **ip flow monitor** command specifies the capture of ingress data (input) on the two specified interfaces.

The overall configuration without annotations looks like this:

```
flow exporter NetFlow-to-Orion
  destination 10.10.10.10
  source vlan254
  transport udp 2055
flow exporter NetFlow-to-Orion
  destination 10.10.10.10
  source vlan254
  transport udp 2055
export-protocol netflow-v5
flow monitor NetFlow-Monitor
  description Original Netflow captures
  record ipv4
  exporter NetFlow-to-Orion
cache timeout inact 10
cache timeout act 5
interface TenGigabitEthernet1/1/1
interface TenGigabitEthernet1/1/2
ip flow monitor NetFlow-Monitor input
```

For detailed information on available commands and their use see the [Cisco Flexible NetFlow Command Reference](#).

Cisco Catalyst 4500

For processing NetFlow this switch uses Supervisor Engine 5 or Supervisor Engine 7. With SE 5 the Cisco 4500 supports a regular NetFlow (v5) configuration; but with SE 7 the device must be configured for Flexible NetFlow. Note: Supervisor Engine 6 does not support

Supervisor Engine 5

For this setup of the device you can use a regular NetFlow configuration such as:

```
ip route-cache flow infer-fields
ip flow ingress infer-fields
ip flow ingress layer2-switchedConfiguring Devices for NetFlow 5
ip flow-export source <port with the IP address managed in Orion >
ip flow-export version 5
ip flow-export destination <Orion_Server_IP_address> 2055
ip flow-cache timeout active 1
ip flow-cache timeout inactive 45
snmp-server ifindex persist
```

Supervisor Engine 7

A Flexible NetFlow configuration consists in a flow record, a flow exporter, and a flow monitor, each of which includes parameters that you assign appropriate values. For information on the advantages of using Flexible NetFlow, see this [Cisco FAQ](#).

The tasks involved in creating a Flexible NetFlow configuration are:

1. Creating and configuring the flow record.
2. Creating and configuring the flow exporter(s).
3. Creating a flow monitor to bind the flow record to the exporter.
4. Applying the flow monitor to the appropriate interface on the device.

The following configuration example creates a custom flow record and flow monitor. Each section in the example—flow record, flow exporter, flow monitor—includes notes that explain what the commands are doing.

Flow Record

```
flow record ipv4
! match ipv4 tos
match ipv4 protocol
match ipv4 destination address
match transport source-port
match transport destination-port
  match interface input
collect interface output
collect counter bytes
collect counter packets
```

The flow record part of this configuration example creates the record called “ipv4” and uses the **match ipv4**, **match transport**, and **collect** commands to define the key fields in the record by which flow data will be processed. For more information on these commands, see this [Cisco command reference](#).

Flow Exporter

```
flow exporter NetFlow-to-Orion
  destination 10.10.10.10
  source vlan254 (interface with which Orion is managing the device)
  transport udp 2055 (Orion's collection port)
export-protocol netflow-v5
```

The flow exporter part of the configuration examples defines an exporter (called “NetFlow-to-Orion”) the **destination** (the IP address of the Orion server) to which flow data will be exported; the **source** interface (with which IP address with which Orion is managing the device) from which flow data will be exported; the **transport** protocol and port (udp, 2055—Orion’s collection port) through which the flow data will pass; and the NetFlow **export protocol** (NetFlow v5) that the NetFlow collector should expect and use to process the data.

Flow Monitor

```
flow monitor NetFlow-Monitor
  description Original Netflow captures
  record ipv4
  exporter NetFlow-to-Orion
cache timeout inact 10
cache timeout act 5
interface vlan254
ip flow monitor NetFlow-Monitor input
```

The flow monitor part of the configuration example creates a monitor (called “NetFlow-Monitor”) that uses the **record** and **exporter** commands to bind the flow record (ipv4) to the flow exporter (NetFlow-to-Orion) you already created. The **interface** command defines the interface (vlan254, in this case) to which the flow monitor NetFlow-Monitor applies and **ip flow monitor** command specifies the capture of ingress data (input).

The overall configuration without annotations looks like this:

```

flow record ipv4
  ! match ipv4 tos
  match ipv4 protocol
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match interface input
  collect interface output
  collect counter bytes
  collect counter packets
flow exporter NetFlow-to-Orion
  destination 10.10.10.10
  source vlan254
  transport udp 2055
  export-protocol netflow-v5
flow monitor NetFlow-Monitor
  description Original Netflow captures
  record ipv4
  exporter NetFlow-to-Orion
  cache timeout inact 10
  cache timeout act 5
  interface vlan254
  ip flow monitor NetFlow-Monitor input

```

For detailed information on available commands and their use see the [Cisco Flexible NetFlow Command Reference](#).

Cisco Catalyst 6500

The following example includes annotations that explain the requirements for successfully configuring NetFlow on this device.

```
ip route-cache flow
```

This command enables fast switching (CEF) on the device. On this device NetFlow is monitored only for traffic that is fast-switched (CEF).

```

mls ip multicast flow-stat-timer 9
mls aging long 64
mls aging normal 32
mls flow ip interface-full
mls nde sender version 5

```

These Multilayer Switching commands set the named timer (**ip multicast flow stat timer**), the aging intervals for data in the flow cache (**aging long**, **aging normal**) by which export should occur, the flow mask (**flow ip**); and also configure flow export (**nde sender version**) as NetFlow version 5 on the Policy Feature Card (PFC).

```

ip flow-export source IP Address
ip flow-export version 5
ip flow-export destination IP_Address(Orion NPM server) 2055
ip flow ingress layer2-switched vlan x, y, z (separate each VLAN with a comma)
Ip flow ingress

```

These commands set the flow export source (**ip flow-export source**; the IP address must be monitored in Orion), the flow version (**ip flow export version**), the flow export destination (**ip flow-export destination**; the IP of the Orion server with default port 2055), and enable NetFlow (**ip flow ingress layer2-switched**) for Layer 2 switched traffic and Layer 3 traffic (**ip flow ingress**) on the Multilayer Switch Feature Card (MSFC).

The overall configuration without annotations looks like this:

```

ip route-cache flow
mls ip multicast flow-stat-timer 9
mls aging long 64
mls aging normal 32
mls flow ip interface-full
mls nde sender version 52-Configuring Devices for NetFlow
ip flow-export source IP Address
ip flow-export version 5
ip flow-export destination IP_Address(Orion NPM server) 2055
ip flow ingress layer2-switched vlan x, y, z (separate each VLAN with a comma)
Ip flow ingress

```

Cisco Nexus 7000/7010

This device requires a Flexible NetFlow configuration. The following example creates a custom flow record and flow monitor, and applies the monitor to appropriate interfaces. Each section in the example—flow record, flow exporter, flow monitor, and configuration on interfaces—includes notes that explain what the commands are doing.

Sample Flexible NetFlow Configuration

Flow Record

```
flow record OrionNetFlow
match ip tos
match ip protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input (Auto Added)
match interface output (Auto Added)
match flow direction (Auto Added)
collect counter bytes
collect counter packets
```

The flow record part of this configuration example creates the record called “OrionNetFlow” and uses the **match (ipv4, interface, transport)** and **collect (counter)** commands to define the key fields in the record by which flow data will be processed. For more information on these commands, see this [Cisco command reference](#).

Flow Exporter

```
flow exporter NetFlow-to-Orion
destination 10.10.10.10 (Orion Server)
source vlanXXX (Required)
transport udp 2055 (Orion's collection port, 2055 by default. You can use any other port, but you need to add it as a collector in NTA.)
version 9 (This command will put you into another configuration mode - have option to add additional conditions, such as the following line.)
template data timeout 60
```

Note: The `template data timeout 60` command ensures that the template is exported every 1 minute. The default setting is 600 s.

The flow exporter part of the configuration examples defines an exporter (called “NetFlow-to-Orion”) the **destination** to which flow data will be exported, the **source** interface (`vlanXXX`) from which flow data will be exported, the **transport protocol and port** (`udp, 2055`) through which the flow data will pass, and the NetFlow **export protocol** (`Version 9`) that the NetFlow collector should expect and use to process the data.

Flow Monitor

```

flow monitor NetFlow-Monitor
description xxxx
exporter NetFlow-to-Orion
record OrionNetFlow

```

Configuration on Interfaces

Now you need to apply the monitor to appropriate interfaces.

```

interface Ethernet2/1

ip flow monitor NetFlow-Monitor input

ip flow monitor NetFlow-Monitor output

```

The flow monitor part of the configuration example creates a monitor (called “NetFlow Monitor”) that uses the **record** and **exporter** commands to bind the flow record (OrionNetFlow) to the flow exporter (NetFlow-to-Orion) you already created. The interface command defines the **interface** (Ethernet2/1) to which the flow monitor NetFlow Monitor applies and **ip flow monitor** command specifies the capture of both ingress (input) and egress (output) data.

Note: You can enter a VLAN range prior to entering the command above (i.e. `vlan 1 - 3967` instead of each vlan separately).

The overall configuration without annotations looks like this:

```
flow record OrionNetFlow
match ip tos
match ip protocol
match interface input
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
match interface output
match flow direction
collect counter bytes
collect counter packets

flow exporter NetFlow-to-Orion
destination 10.10.10.10
source vlanXXX
transport udp 2055
version 9
template data timeout 60

flow monitor NetFlow-Monitor
description xxxx
record OrionNetFlow
exporter NetFlow-to-Orion

interface Ethernet2/1
ip flow monitor NetFlow-Monitor input
ip flow monitor NetFlow-Monitor output
```

Cisco ASA 5500

Besides the usual target address for flow exports, devices in this series require a service policy that enables flow data to be exported.

The following example includes annotations that explain the requirements for successfully configuring NetFlow on this device.

```
ip flow-export destination inside 1.1.1.1 2055
```

This command sets the export target IP address and port (NTA collector at 1.1.1.1 2055) and designates it as inside the network that includes the ASA device.

```
ip flow-export template timeout-rate 1
```

This command sets the timeout of the current v9 template (in this case it is set to 1 minute) and results in re-sending the template with the flow data as soon as the timeout is reached.

```
ip flow-export delay flow-create 60
```

This command delays the creation of a NetFlow record and so delays exporting flow data until the number of seconds (60 in this case) are reached.

```
ip access-list netflow-export extended permit ip any any
```

This command creates an access list (**access-list**) called **netflow-export** that the device to export flow records from any IP address (outside interface) to any IP address (in this case, the result is that exports will go to the NetFlow collector target as specified in the **ip flow-export destination command**)

```
class-map netflow-export-class
match access-list netflow-export
policy-map global_policy
class netflow-export-class
service-policy global_policy global
flow-export event-type all destination 1.1.1.1
```

Note: If a global policy already exist just add the NetFlow policy map to it.

These commands create the Modular QoS traffic management setup to enable flow packet traffic to get out of the device's outside interfaces and make it to the targeted NetFlow collector:

1. Creates a traffic class (**class-map**) called **netflow-export-class**
2. Specifies that the access list **netflow-export** should be applied (**match**) to this class
3. Selects (**policy-map**) default traffic inspection rules (**global_policy**) for flow traffic
4. Applies (**service-policy**) those rules to all interfaces (**global**) on the device through which flow packets is transferred
5. Specifies that all events that trigger creation of flow records should be targeted at the NTA collector (1.1.1.1).

The overall configuration without annotations looks like this:

```
flow-export destination inside 1.1.1.1 2055
flow-export template timeout-rate 1
flow-export delay flow-create 60
access-list netflow-export extended permit ip any any
class-map netflow-export-class
match access-list netflow-export
policy-map global_policy
class netflow-export-class
flow-export event-type all destination 1.1.1.1
service-policy global_policy global
```