How-To Configure NetFlow v5 & v9 on Cisco® Routers
Visibility into the network is an indispensable tool for network administrators. Network visibility can be achieved through daily troubleshooting, bandwidth capacity planning, application monitoring, understanding network utilization, QoS traffic views, and identifying security gaps or compliance issues.

NetFlow provides network administrators with data to understand the movement of traffic in the network. Real-time and historic views that come with NetFlow aid in understanding network behavior and help reduce and resolve issues related to bandwidth, application performance, and improper traffic classification. This enables efficient network operation that will in turn lower costs and drive higher business revenues through better utilization of network infrastructure.

In this tech tips document, we’ll take a quick view of Cisco NetFlow, and walk you through the steps to configure NetFlow versions v5 & v9 on a Cisco router.

**What is NetFlow?**

NetFlow is an IP traffic accounting technology that was originally developed by Cisco as a switching technology. Later as the value of information in the packets were discovered, NetFlow evolved, and is now the de-facto standard for bandwidth monitoring and traffic analytics.

**Why is Enabling NetFlow Important?**

Enabling NetFlow on your routing and switching devices allows you to collect traffic statistics from that device. When traffic passes through the interfaces of a NetFlow enabled device, relevant information about the IP conversation is captured and stored in the NetFlow cache. This information can then be exported to a flow analyzer tool based on user specified timeouts to:

- Understand application and bandwidth usage patterns to ensure optimal usage of bandwidth
- Quickly troubleshoot traffic spikes & bottlenecks, Internet or application slowness, voice & video traffic issues, etc.
- Detect security and network behavioral anomalies
- Verify the performance of QoS policies
- Perform capacity planning and save costs by taking informed decisions
NetFlow in Your Network

NetFlow is completely transparent to the existing network; it does not involve any connection-setup protocol either between routers or any other networking device or end station. It also does not require any external change, either to the traffic or packets or to any other networking device. Also, NetFlow need not be enabled on all device interfaces but can be performed independently on specific interfaces that need to be monitored.

As seen in the above diagram, NetFlow data is exported from the specific interfaces that need to be monitored from the routing or switching devices (NetFlow Exporter) in the network. This NetFlow Data is exported to a centralized NetFlow Collector Analyzer that processes and generates reports. Network administrators can selectively invoke NetFlow Data Export (NDE) on a router or on a per-sub interface basis to gain traffic performance and control in required network locations.
What is NetFlow Version 5?
The NetFlow v5, or traditional NetFlow, is the most widely used and supports Autonomous System (AS) reporting and a few additional fields. All flows are calculated when they come into an interface (i.e. inbound) and outbound traffic is reported using inbound flows from the other interfaces. Because of this, it’s generally advised that NetFlow v5 be enabled on all interfaces of the device; else outbound utilization on some interfaces may be understated. The packet format is fixed and is always the same and hence is easy to decipher for most NetFlow collection and network traffic reporting packages.

What is NetFlow Version 9?
NetFlow flow-record format is known as NetFlow version 9—the Flexible NetFlow technology. The distinguishing feature of the NetFlow Version 9 format is that it is template-based. Templates provide a flexible flow export with user defined key and non-key fields. It has the ability to monitor a wide range of IP packet information which is absent in traditional NetFlow. This format provides the versatility needed to support new fields and record types. Flexible NetFlow accommodates custom fields such as MPLS labels, IPv6 traffic, NBAR protocols, Multicast IP traffic, VLAN ID, real-time performance of media flows, etc.

How-To Configure NetFlow on a Cisco Router

Configuring NetFlow v5
The following is a set of commands that are issued on a Cisco router to enable NetFlow version 5 on the FastEthernet 0/1 interface and export to the machine 10.199.15.103 (IP Address of the NetFlow collector) on port 2055 (UDP port to export NetFlow packets).

```
Router2951#enable
Password:*****
Router2951#configure terminal
router2951(config)#interface FastEthernet 0/1
router2951(config-if)#ip route-cache flow
router2951(config-if)#exit
router2951(config)#ip flow-export destination 10.199.15.103 2055
```

This command has to be executed on all the L3/VLAN interfaces

The hostname or IP address of the NetFlow Collector server

The port number used to send NetFlow packets.
Configuring NetFlow v9

Flexible NetFlow is comprised of 3 components:

1. Flow Record
2. Flow Exporter
3. Flow Monitor

The following is a set of commands that are issued on a Cisco router to enable Flexible NetFlow on the FastEthernet 0/1 interface and export to the machine 10.199.15.103 (IP Address of NetFlow collector) on port 2055 (UDP port to export NetFlow packets).

Routerr2951#enable
Password:******
Routerr2951#configure terminal

//Creating Flow Record
routerr2951(config)# flow record NTArecord
routerr2951 (config-flow-record)# match ipv4 source address
routerr2951 (config-flow-record)# match ipv4 destination address
routerr2951 (config-flow-record)# match ipv4 protocol
router2951 (config-flow-record)# match transport source-port
router2951 (config-flow-record)# match transport destination-port
router2951 (config-flow-record)# match ipv4 tos
router2951 (config-flow-record)# match interface input
router2951 (config-flow-record)# collect interface output
router2951 (config-flow-record)# collect counter bytes
router2951 (config-flow-record)# collect counter packets

//Creating Flow Exporter
router2951(config)# flow exporter NTAexport
router2951 (config-flow-exporter)# destination 10.199.15.103
router2951 (config-flow-exporter)# source GigabitEthernet0/1
router2951 (config-flow-exporter)# transport udp 2055
router2951 (config-flow-exporter)# template data timeout 60

//Creating Flow Monitor
router2951(config)# flow monitor NTAmonitor
router2951(config-flow-monitor)# record NTArecord
router2951(config-flow-monitor)# exporter NTAexport
router2951(config-flow-monitor)# cache timeout active 60
router2951(config-flow-monitor)# cache timeout inactive 15

//Associating the Monitor to an Interface
router2951(config)# int FastEthernet0/1
router2951(config-if)# ip flow monitor NTAmonitor input

//Save configuration to memory
router2951#write
How-To Verify if NetFlow is Getting Exported from Your Router

Now that your router has been set up to export NetFlow data, perform these steps in this optional task to verify if NetFlow data export is operational to display the statistics for NetFlow data export.

Version 5 flow records

show ip flow export command will show you the current NetFlow configuration.

```
router2951# show ip flow export
Flow export v5 is enabled for main cache
Export source and destination details:
VRF ID: Default
Source(1) 10.199.10.1 (GigabitEthernet0/1)
Destination(1) 10.199.15.103 (2055)
```

Version 5 flow records

169422708 flows exported in 5647450 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

Version 9 flow records

show flow exporter exporter-name command will show you the stats of the Flow exporter.

```
router2951#show flow exporter NTAexport
Flow exporter NTAexport:
Description: User defined
Export protocol: NetFlow Version 9
Transport Configuration:
Destination IP address: 10.199.15.103
```
Once NetFlow is configured on the routers, the NetFlow packets are sent to the designated server or collector. Keep in mind that NetFlow can bring in thousands of flows per second depending on the size of the network and the traffic. Having a tool in place that collects all NetFlow packets and presents them in an easy to understand, comprehensive view helps you effectively manage your bandwidth.

**SolarWinds® NetFlow Traffic Analyzer**

*SolarWinds NetFlow Traffic Analyzer* (NTA) is one such example of a software based NetFlow collector that gathers network traffic data, correlates it into a useable format, and then presents it to the user in a Web-based interface.

SolarWinds NTA analyzes the NetFlow Export data that comes from Cisco devices to provide valuable information on how your bandwidth is consumed and by whom.

Key benefits of using NTA are:

- Obtain real-time analysis of peak traffic in the network
- Perform bandwidth sizing for new applications on the network
- Easily troubleshoot and understand network pain points like network choke or slowness
- Quickly detect unauthorized WAN traffic and network behavior anomalies
- View details to verify if QoS policies are met and need to be changed

SolarWinds NTA gives you a comprehensive customizable view of your network traffic on a single page.
Not ready for a full solution? Download our FREE Tool, **NetFlow Configurator**, to remotely and quickly configure NetFlow v5 via SNMP on Cisco devices. NetFlow Configurator also facilitates setting up collectors for Cisco NetFlow data, specifying the ports on which the collectors are listening, and enabling monitoring of inbound and outbound (ingress/egress) traffic data per interface.

This tool is 100% free and yours to keep forever.

**References**

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT Pros, we strive to eliminate the complexity in IT management software that many have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack®, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more at http://www.solarwinds.com.