Configuring NetFlow Data Export

This is a brief guide to setting up NetFlow on various types of device. Note that if your
device isn't listed here it does not mean it is not supported by NetFlow Tracker; please
ask your device vendor for a guide to enabling NetFlow.

Enabling NetFlow Export/NDE on a Cisco Router or Layer 3 Switch

For more information on this subject, visit http://www.cisco.com/go/netflow. We recommend that only people with experience in configuring Cisco devices follow these
steps. If in doubt, contact your network administrator or Cisco consultant. Note that if you are running hybrid mode on a layer 3 switch you must configure IOS on the MSFC
and CatOS on the Supervisor Engine. Native IOS also requires extra commands; these are documented below.

Enabling Netflow Export on an IOS Device

In configure mode on the router or MSFC, issue the following to enable NetFlow Export:

ip cef

This enables Cisco Express Forwarding, which is required for NetFlow in most recent IOS releases.

ip flow-export destination <address> 2055

Use the address of your NetFlow Tracker machine and one of the ports configured in the Listener Ports settings page. Port 2055 is monitored by default.

ip flow-export source loopback 0

The source interface is used to set the source IP address of the NetFlow exports sent by the router. NetFlow Tracker will make SNMP requests of the router on this address. If you experience problems you can set the source interface to an Ethernet or WAN interface instead of the loopback.

ip flow-export version 5 [peer-as | origin-as]

or

ip flow-export version 9 [peer-as | origin-as]

This sets the export version. Version 5 and Version 9 both support all of the features NetFlow Tracker is capable of using; if you have a Native IOS switch you may need to use version 9 to work around a bug – this is described below. If your router uses BGP, you can specify that either the origin or peer ASs are included in exports – it is not possible to include both.

ip flow-cache timeout active 1

This breaks up long-lived flows into one-minute segments.

ip flow-cache timeout inactive 15

This ensures that flows that have finished are exported in a timely manner.

interface <interface>
ip route-cache flow or **ip flow ingress** or **ip route-cache cef**
bandwidth <kbps>
exit
You need to enable NetFlow on each interface through which traffic you are interested in will flow. This will normally be the Ethernet and WAN interfaces. Note that there are several commands to enable NetFlow; the first two above have exactly the same effect. If you are using input filters you need to use the third command. You may also need to set the speed of the interface in kilobits per second. It is especially important to set the speed for frame relay or ATM virtual circuits. Note that a Catalyst 4000 series switch does not support any of the commands to enable NetFlow for an interface; instead NetFlow is enabled for all interfaces using a special command documented below.
show ip flow export
This will show the current NetFlow configuration. Issue this in normal (not configuration) mode.
show ip cache flow
show ip cache verbose flow
These commands issued in normal mode summarise the active flows and give an indication of how much NetFlow data the router is exporting.Enabling NetFlow Export on a 4000 Series Switch
The 4000 and 4500 series switches require a Supervisor IV with a NetFlow Services daughter card (WS-F4531), or a Supervisor V, and IOS version 12.1(19)EW or above to support NetFlow. First configure the device as for an IOS device above, omitting the
command
ip route-cache flow
on each interface, and then issue the following:
ip route-cache flow infer-fields
This ensures routing information is included in the flows.

Enabling NDE on a Native IOS Device

The following commands are required to get NetFlow information on route-switched traffic from a Catalyst 6000 or above; they are not required for a Catalyst 4000 series.
mls netflow
This enables NetFlow on the supervisor.
mls nde sender version 5
or
mls nde sender version 7
This sets the export version. Due to several IOS bugs, the export version you must use on the supervisor is dependent on your hardware configuration and IOS version:
• Distributed Forwarding Cards and 12.1(13)E03, 12.1(18.1)E, 12.2(13.6)S, 12.2(15.1)S, 12.2(17a)SX or above: use version 5. Note that this configuration will cause the Performance Counters to report missed flows that are not actually missed; this is the result of an IOS bug fixed in the SXF strains.
• Distributed Forwarding Cards and older than 12.1(13)E03, 12.1(18.1)E,

12.2(13.6)S, 12.2(15.1)S or 12.2(17a)SX: this configuration will cause serious problems, so please contact Crannog Software if your device matches this description.
• No Distributed Forwarding Cards and 12.0(24)S, 12.2(18)S, 12.3(1) or above: use version 5 and configure the MSFC to export version 9 as described above.
• No Distributed Forwarding Cards and 12.1(13)E03, 12.1(18.1)E, 12.2(13.6)S, 12.2(15.1)S, 12.2(17a)SX or above: use version 5.
• Anything else: use version 7. Note that version 7 may not include AS or subnet mask information.

mls aging long 64
This breaks up long-lived flows into (roughly) one-minute segments.
mls aging normal 32
This ensures that flows that have finished are exported in a timely manner.
mls flow ip interface-full
mls nde interface
or
mls flow ip full

If you have a Supervisor Engine 2 or 720 running IOS version 12.1.13(E) or higher the first two commands are required to put interface and routing information into the NetFlow Exports. This information is unavailable with any earlier IOS version on the Supervisor Engine 2 or 720.
If you have a Supervisor Engine 1 the third command is required to put full information into the NetFlow Exports.
ip flow ingress layer2-switched vlan <vlanlist>
ip flow export layer2-switched vlan <vlanlist>
A PFC3B or PFC3BXL running 12.2(18)SXE or higher is required for this command, which enables NDE for all traffic within the specified VLANs rather than just inter-VLAN traffic.

Configuring NDE on a CatOS Device

A layer 3 switch running CatOS appears as two devices; the MSFC can be configured to export NetFlow information on all the packets it routes by following the instructions
for configuring a
In privileged mode on the Supervisor Engine, issue the following to enable NDE:
set system name <name>
Set the name of your switch. Note that even if the prompt has been set to the name of the switch you still need this command.
set mls nde <address> 2055
Use the address of your NetFlow Tracker machine and one of the ports configured in the Listener Ports settings page. Port 2055 is monitored by default.
set mls nde version 7
This sets the export version. Version 7 is the most recent full export version supported by switches.
set mls agingtime long 64
This breaks up long-lived flows into (roughly) one-minute segments.

set mls agingtime 32
This ensures that flows that have finished are exported in a timely manner.
set mls flow full
This sets the flow mask to full flows. This is required to get useful information from the switch.
set mls bridged-flow-statistics enable <vlanlist>
CatOS 7.(2) or higher is required for this command, which enables NDE for all traffic within the specified VLANs rather than just inter-VLAN traffic.
set mls nde enable
This enables NDE.
show mls nde
show mls debug
These commands can help debug your NDE configuration.