Netusage™ and NetFlow Deployment Guide

Release 4.0
Wednesday, 25 January 2006

Table of Contents

Introduction

NetUsage™ Console is a “plug-in” appliance that collects network usage data (LAN, WAN or MAN) from Cisco™ routers, NetUsage™ Probes and other Netflow™ data sources. It generates reports that provide visibility of business and shared network usage and can be accessed and configured using a web browser.

Purpose

This document explains how NetUsage™ Console can be deployed in combination with Cisco™ routers acting as Netflow™ data sources in Wide Area Networks built around a variety of common technologies; leased line, frame relay, ATM and MPLS VPN. The detail of configuring the NetUsage™ Console is covered in the Administration Guide. This document focuses on identifying where Netflow™ needs to be enabled in a network, and the commands required to enable it on Cisco routers.

Typical WAN NetFlow Deployment Example

A typical WAN arranged in hub and spoke topologies, where remote sites connect into one or two central hub sites, each with one or more hub WAN routers. In this situation data can be captured by enabling Netflow™ on all of the hub router interfaces, both backbone and WAN. NetUsage™ is able to identify all flows through the router which are sourced from or routed to each WAN interface, and present these in the reports for a given link. A typical centralized deployment is illustrated in Figure 1.

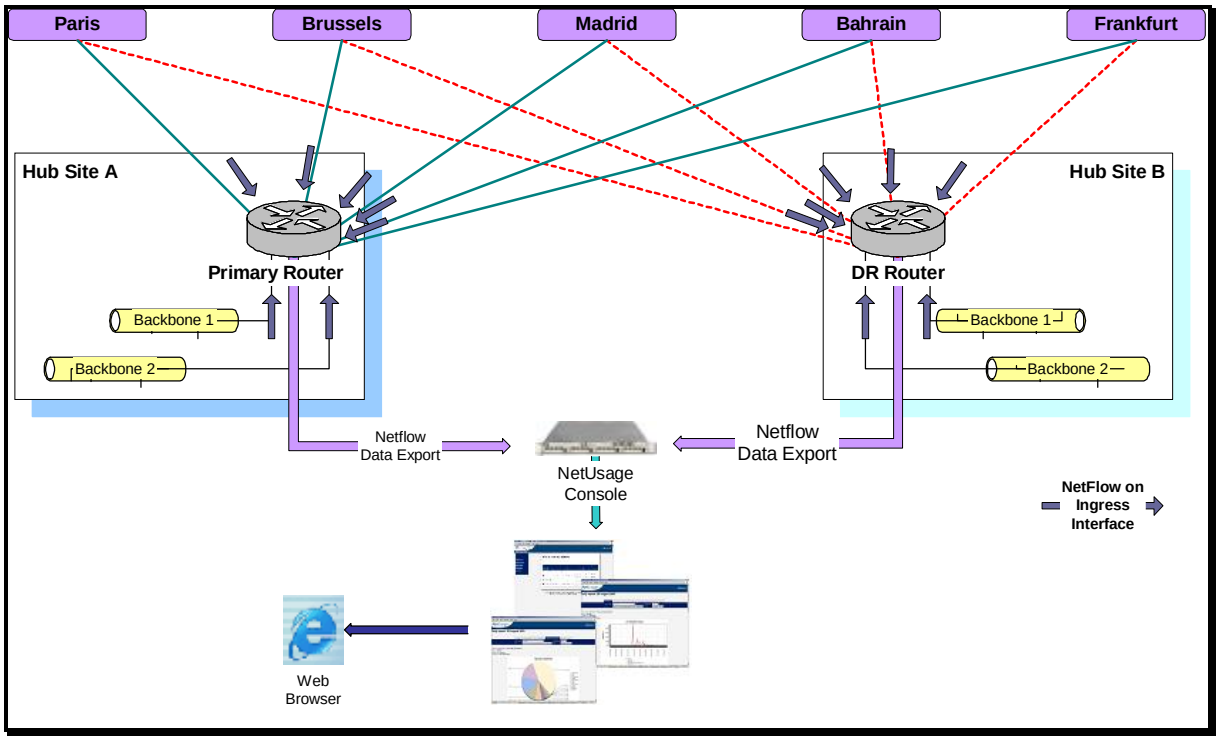
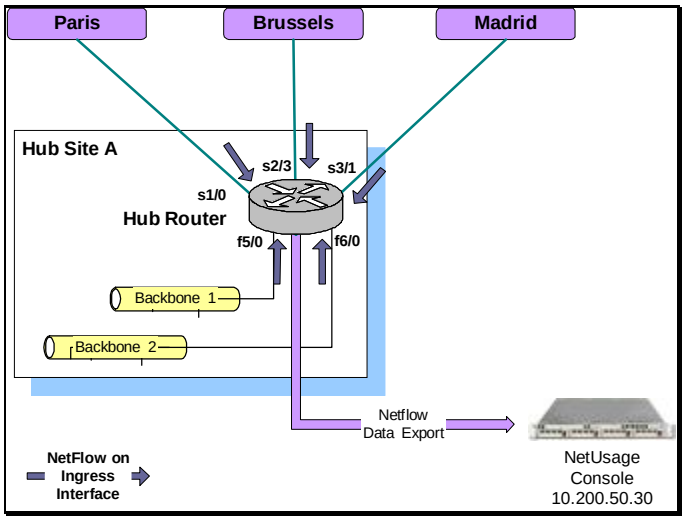


Figure 1- Centralised Deployment on Hub and Spoke Network

Deployment Examples

WAN - Leased Line

A centralized deployment is assumed, as illustrated in the diagram. The commands required to configure NetFlow™ are highlighted below.



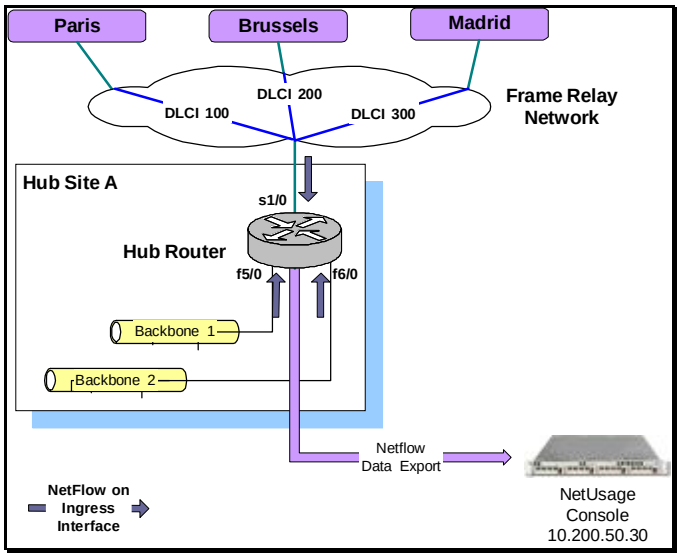
Hub Router NetFlow Configuration

```
interface FastEthernet5/0
 interface description *** Backbone LAN A ***
 ip address 10.200.10.1 255.255.255.252
 ip route-cache flow
!
interface FastEthernet6/0
 interface description *** Backbone LAN B ***
 ip address 10.200.20.1 255.255.255.252
 ip route-cache flow
!
interface Serial1/0
 interface description *** serial WAN link to Paris ***
 ip address 10.70.1.1 255.255.255.252
 ip route-cache flow
 encapsulation ppp
 compress stac
!
interface Serial2/3
 interface description *** serial WAN link to Brussels ***
 ip address 10.70.1.5 255.255.255.252
 ip route-cache flow
 encapsulation ppp
 compress stac
!
interface Serial3/1
 interface description *** serial WAN link to Madrid ***
 ip address 10.70.1.9 255.255.255.252
 ip route-cache flow
 encapsulation ppp
 compress stac

ip flow-export source loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export destination 10.200.50.30 5555
```

WAN - Frame Relay

A centralized deployment is assumed, as illustrated in the diagram. The commands required to configure NetFlow™ are highlighted below. Note that Netflow™ must be enabled on the physical interface, not on the sub-interfaces.

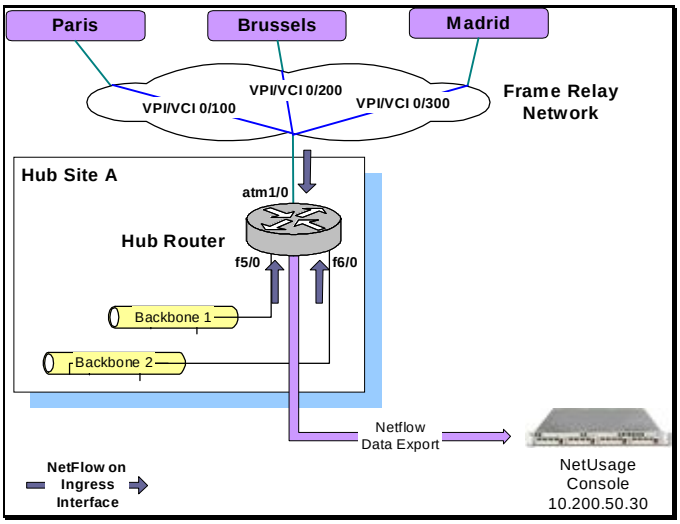


Hub Router NetFlow Configuration

```
interface FastEthernet5/0
 interface description *** Backbone LAN A ***
 ip address 10.200.10.1 255.255.255.252
 ip route-cache flow
!
interface FastEthernet6/0
 interface description *** Backbone LAN B ***
 ip address 10.200.20.1 255.255.255.252
 ip route-cache flow
!
interface Serial1/0
 interface description *** Frame Relay Access port ***
 no ip address
 ip route-cache flow
 encapsulation frame-relay
!
interface Serial1/1.100 point-to-point
 interface description *** pvc to Paris ***
 ip address 10.70.9.1 255.255.255.252
 frame-relay interface-dlci 100
!
interface Serial1/1.200 point-to-point
 interface description *** pvc to Brussels ***
 ip address 10.70.9.5 255.255.255.252
 frame-relay interface-dlci 200
!
interface Serial1/1.300 point-to-point
 interface description *** pvc to Madrid ***
 ip address 10.70.9.9 255.255.255.252
 frame-relay interface-dlci 300
!
ip flow-export source loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export destination 10.200.50.30 5555
```

WAN - ATM

A centralized deployment is assumed, illustrated in the diagram below. The commands required to configure NetFlow™ are highlighted below. Note that Netflow™ must be enabled on the physical interface, noon the sub-interfaces.

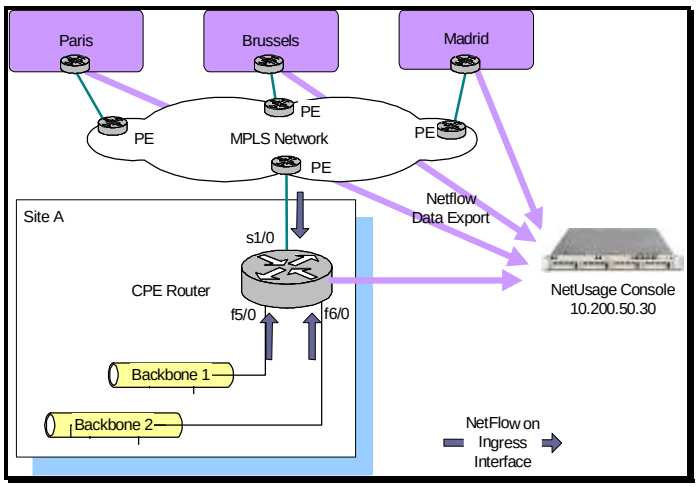


Hub Router NetFlow Configuration

```
interface FastEthernet5/0
 interface description *** Backbone LAN A ***
 ip address 10.200.10.1 255.255.255.252
 ip route-cache flow
!
interface FastEthernet6/0
 interface description *** Backbone LAN B ***
 ip address 10.200.20.1 255.255.255.252
 ip route-cache flow
!
interface ATM1/0
 interface description *** ATM Access port ***
 no ip address
 ip route-cache flow
!
interface ATM1/0.100 point-to-point
 interface description *** pvc to Paris ***
 ip address 10.70.9.1 255.255.255.252
 pvc 0/100
 encapsulation aal5snap
!
interface ATM1/0.200 point-to-point
 interface description *** pvc to Brussels ***
 ip address 10.70.9.5 255.255.255.252
 pvc 0/200
 encapsulation aal5snap
!
interface ATM1/0.300 point-to-point
 interface description *** pvc to Madrid ***
 ip address 10.70.9.9 255.255.255.252
 pvc 0/300
 encapsulation aal5snap
!
ip flow-export source loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export destination 10.200.50.30 5555
```

WAN – MPLS NetFlow™ Enabled on CPE

MPLS provides a VPN which allows "any to any" communication. At each customer site a Customer Premises Equipment (CPE) router terminates the circuit, which feeds into the carriers MPLS network. At the other end of each link is the vendors PE router. Normally MPLS runs on the PE, and the link between this and the CPE operates as a standard Frame Relay, ATM or leased line WAN link.



Because the MPLS network is used as an "any to any" service, there is no PVC or DLCI going to each remote site to report against at central hub sites. Instead reporting on the traffic in and out of any given site requires enabling NetFlow™ on all interfaces on that sites local WAN router (CPE).

The actual commands required depend on the technology used for the local tail connection; refer to the leased line, Frame Relay, or ATM commands already discussed. The only difference is that they are enabled at all sites, not just at a hub site. The example configuration below is for a Frame Relay configuration; commands for one router are shown, and similar commands must be applied to every sites WAN router.

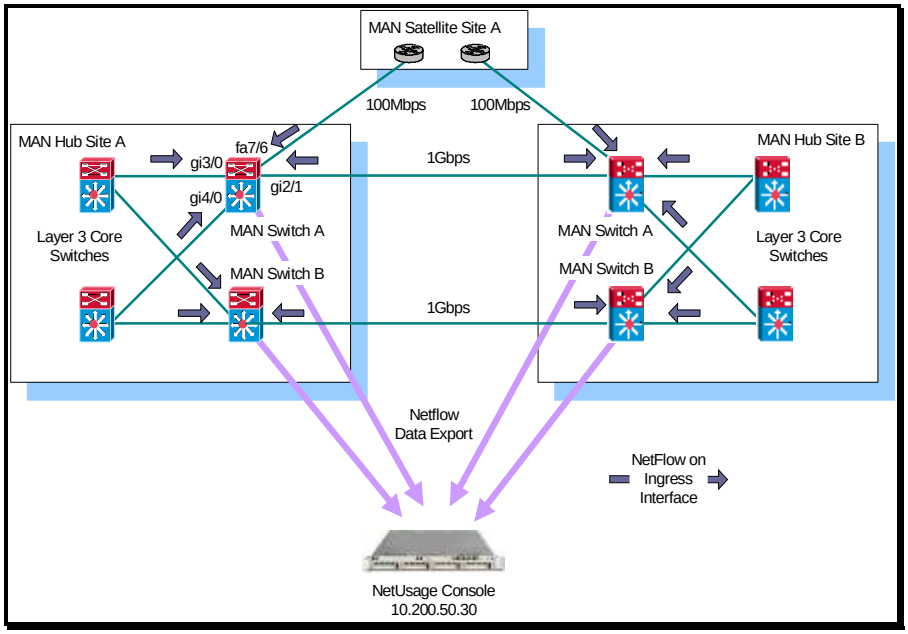
CPE Site A Router NetFlow Configuration

```
interface FastEthernet5/0
 interface description *** Backbone LAN A ***
 ip address 10.200.10.1 255.255.255.252
 ip route-cache flow
!
interface FastEthernet6/0
 interface description *** Backbone LAN B ***
 ip address 10.200.20.1 255.255.255.252
 ip route-cache flow
!
interface Serial1/0
 interface description *** Frame Relay Access port ***
 no ip address
 ip route-cache flow
 encapsulation frame-relay
!
interface Serial1/1.100 point-to-point
 interface description *** Link to MPLS network ***
 ip address 10.70.9.1 255.255.255.252
 frame-relay interface-dlci 100
!
ip flow-export source loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export destination 10.200.50.30 5555
```

MAN – Gigabit/Fast Ethernet

A dual hub MAN topology with a centralized Netflow deployment is assumed, as illustrated in the diagram.

The commands required to configure NetFlow™ are highlighted below. These assume that the MAN switches are Catalyst 6500s running NativeIOS.



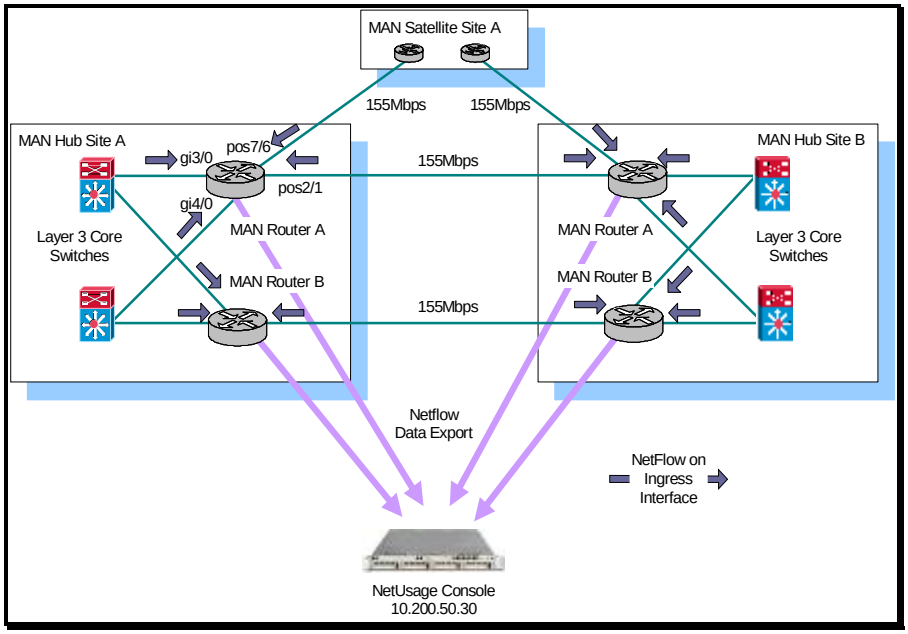
Hub Site A, MAN Switch A NetFlow Configuration

```
interface Gigabitethernet3/0
 interface description *** Link to Core Switch A ***
 ip address 10.200.10.1 255.255.255.252
 ip route-cache flow
!
interface GigabitEthernet4/0
 interface description *** Link to Core Switch B ***
 ip address 10.200.20.1 255.255.255.252
 ip route-cache flow
!
interface GigabitEthernet2/1
 interface description *** MAN Link to Hub Site B ***
 ip address 10.70.49.1 255.255.255.252
 ip route-cache flow
!
interface FastEthernet7/6
 interface description *** MAN Link to Satellite Site C ***
 ip address 10.70.9.1 255.255.255.252
 ip route-cache flow
!
ip flow-export source loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export destination 10.200.50.30 5555
mls netflow
mls flow ip full
mls aging normal 32
mls aging long 64
no mls aging fast
mls nde sender version 5
```

MAN – POS (Packet over Sonet)

A dual hub MAN topology with a centralized Netflow deployment is assumed, as illustrated in the diagram.

The commands required to configure NetFlow™ are highlighted below. These assume that the MAN links are terminated on routers eg. Cisco 7304.



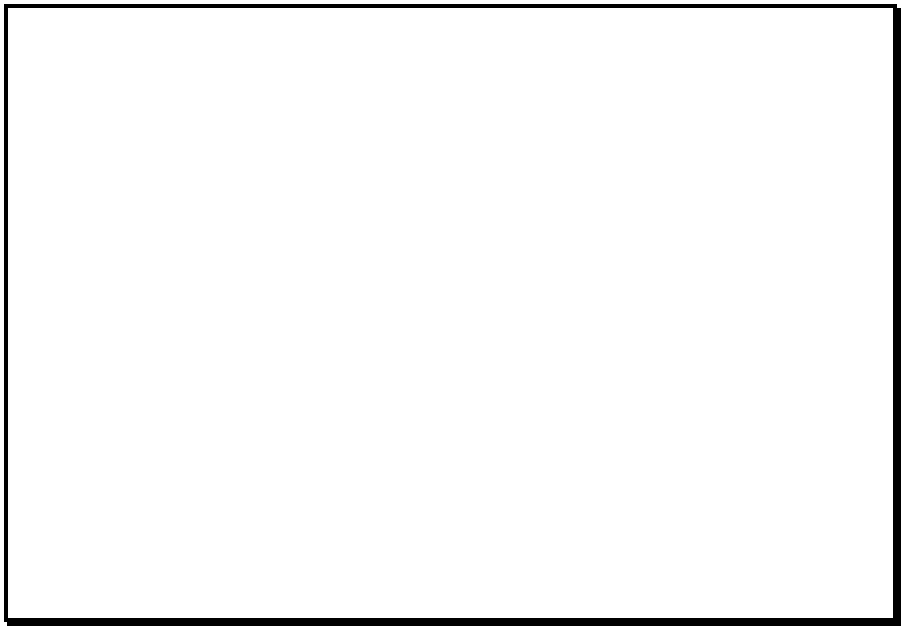
Hub Site A, MAN Router A NetFlow Configuration

```
interface Gigabitethernet3/0
 interface description *** Link to Core Switch A ***
 ip address 10.200.10.1 255.255.255.252
 ip route-cache flow
!
interface GigabitEthernet4/0
 interface description *** Link to Core Switch B ***
 ip address 10.200.20.1 255.255.255.252
 ip route-cache flow
!
interface POS2/1
 interface description *** MAN Link to Hub Site B ***
 ip address 10.70.49.1 255.255.255.252
 ip route-cache flow
!
interface POS7/6
 interface description *** MAN Link to Satellite Site C ***
 ip address 10.70.9.1 255.255.255.252
 ip route-cache flow
!
ip flow-export source loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export destination 10.200.50.30 5555
```

LAN – Access and Core Switches Monitoring

The access switch uplinks can be monitored by exporting NetFlows from Distribution Layer Switches.

The distribution switch uplinks can be monitored by exporting NetFlows from Distribution Layer Switches or Core Layer Switches.



Hybrid Configuration

Catalyst 6500 Supervisor "CatOS" Configuration

```
set mls nde 10.200.50.30 5555
set mls nde version 7
set mls flow full
set mls agingtime long 64
set mls agingtime 32
set mls nde enable
```

Catalyst 6500 MSFC "IOS" Configuration

```
interface vlan 10
 interface description *** Link to Core
Switch A***
 ip address 10.200.10.1 255.255.255.252
 ip route-cache flow
!
interface vlan 50
 interface description *** Link to User
Access Switch 54 ***
 ip address 10.200.20.1 255.255.255.252
 ip route-cache flow
!
ip flow-export source loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export destination 10.200.50.30
5555
```

Native Configuration

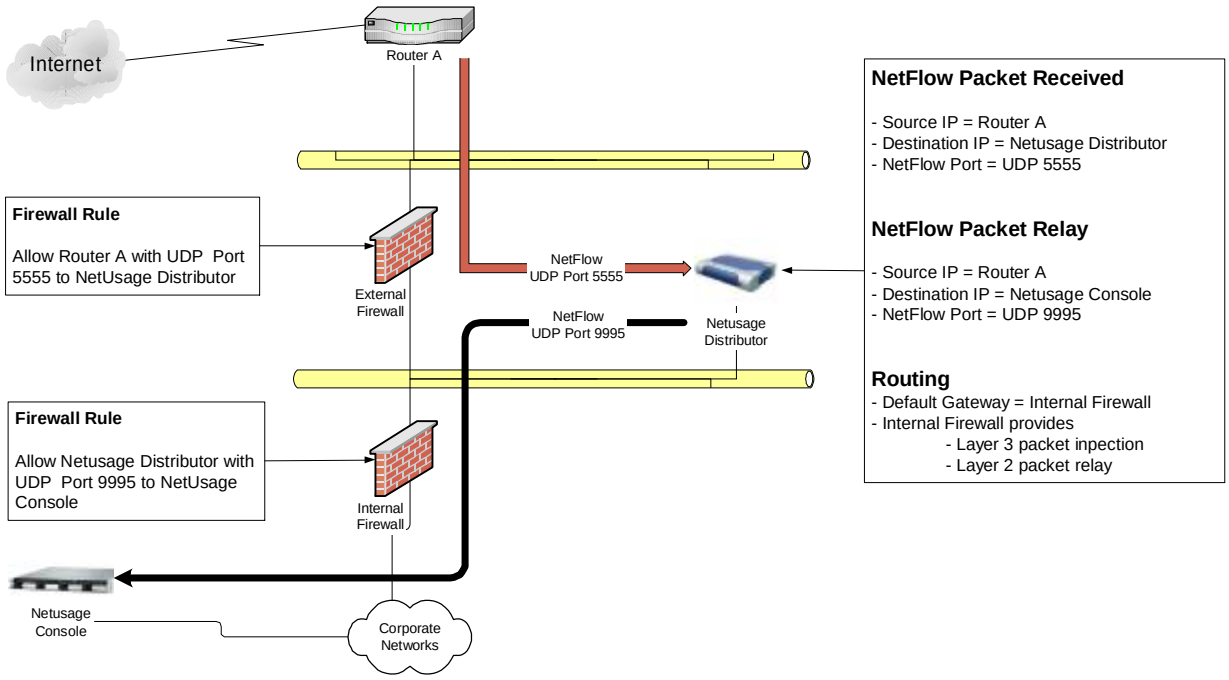
Catalyst 6500 Native IOS Configuration for Supervisor Export

```
mls netflow
mls flow ip full
mls aging normal 32
mls aging long 64
no mls aging fast
mls nde sender version 5
```

Catalyst 6500 Native IOS Configuration for MSFC Export

```
interface vlan 10
 interface description *** Link to Core Switch
A***
 ip address 10.200.10.1 255.255.255.252
 ip route-cache flow
!
interface gigabit 4/2
 interface description *** Link to User Access
Switch 54 ***
 ip address 10.200.20.1 255.255.255.252
 ip route-cache flow
!
ip flow-export source loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export destination 10.200.50.30 5555
```

Firewall Monitoring using Netusage Distributor

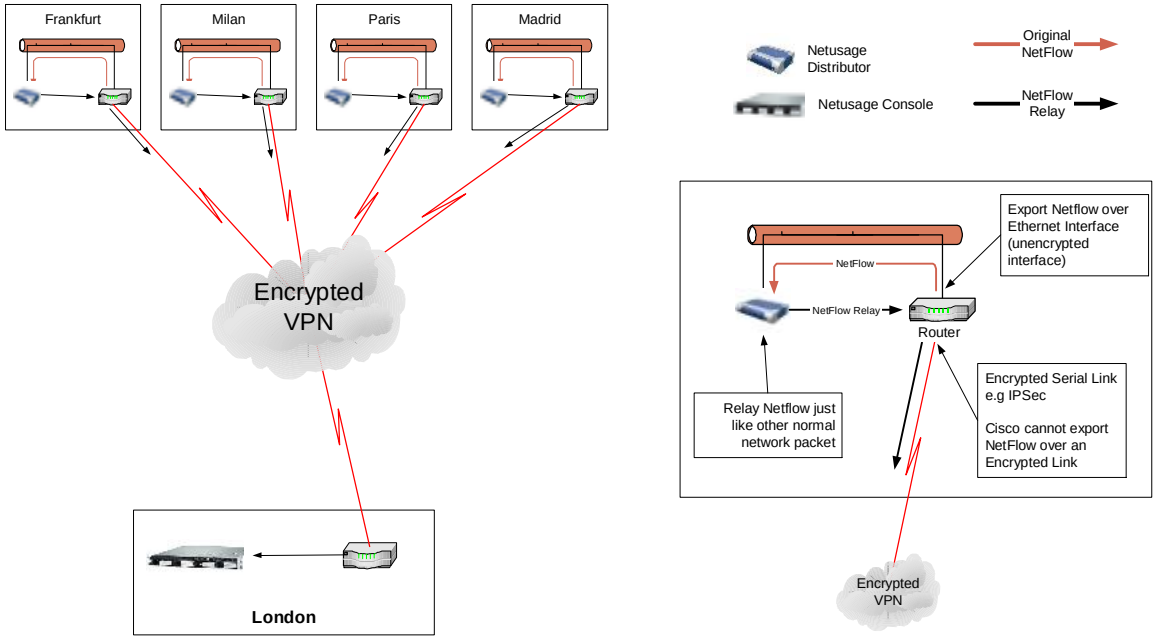



```
Rule for External Firewall
   -  allow [Router A] udp 5555 to Netusage Distributor

Rule for Internal Firewall
   -  allow [Router A] udp 9995 to Netusage Console

Netusage Distributor
   -  Netflow Packet Received
         o  Source IP = Router A
         o  Destination IP = Netusage Distributor
         o  Netflow Port = UDP 5555
   -  Netflow Packet Relay
         o  Source IP = Router A
         o  Destination IP = Netusage Console
         o  Netflow Port = UDP 9995
```

Encrypted VPN Monitoring




```
Rule for External Firewall
   -  allow [Router A] udp 5555 to Netusage Distributor

Rule for Internal Firewall
   -  allow [Router A] udp 9995 to Netusage Console

Netusage Distributor
   -  Netflow Packet Received
         o  Source IP = Router A
         o  Destination IP = Netusage Distributor
         o  Netflow Port = UDP 5555
   -  Netflow Packet Relay
         o  Source IP = Router A
         o  Destination IP = Netusage Console
         o  Netflow Port = UDP 9995
```

Appendix A - Configuring Cisco Routers

There are two key steps to enabling Netflow™ on a router:

- Enabling Netflow™ on each interface which requires monitoring
- Enabling Netflow™ Data Export to send flow data to the NetUsage™ appliance

Cisco IOS Router commands

Sample configuration commands to suit each network technology are included in the following sections for illustration.

NOTES:

- Only the relevant lines of the configuration have been shown.
- When using sub-interfaces Netflow™ must be enabled on the physical interface, not on the sub-interface.
- These examples assume the NetUsage™ unit has been installed on the network with IP address `10.200.50.30`
- Netflow™ data is to be exported using UDP port 5555 (the NetUsage™ appliance listens on this port by default, but can be configured for another port if required)
- Centralized Deployment: by enabling Netflow™ on both the WAN interfaces and the backbone ethernet interfaces of the hub router all flows, which traverse the WANs are captured; this means no configuration is required at the remote site locations.
- Distributed Deployment: by enabling Netflow™ on the WAN interfaces on the routers at both ends of each link all flows that traverse the WAN are captured; this means configuration is required at both the central and the remote site locations. In this situation NetFlow™ does not need to be enabled on the backbone interfaces of the routers.
- Data will be exported from the routers using Netflow™ Version 5 format - see the *Cisco Netflow™ Brief Paper* for an explanation of export format versions.
- To ensure that the source IP address of each routers Netflow™ datagrams is correct, it is advisable to set the source interface explicitly in the relevant line of the config:

  ```
  ip flow-export source Loopback0
  ```

  The NetUsage™ Console should then be configured to accept data from the loopback IP address of each router acting as a data source.
- To ensure that the router Netflow™ export is matched to the NetUsage™ Console reporting interval, it is advisable to set the export timing explicitly in the relevant line of the config:

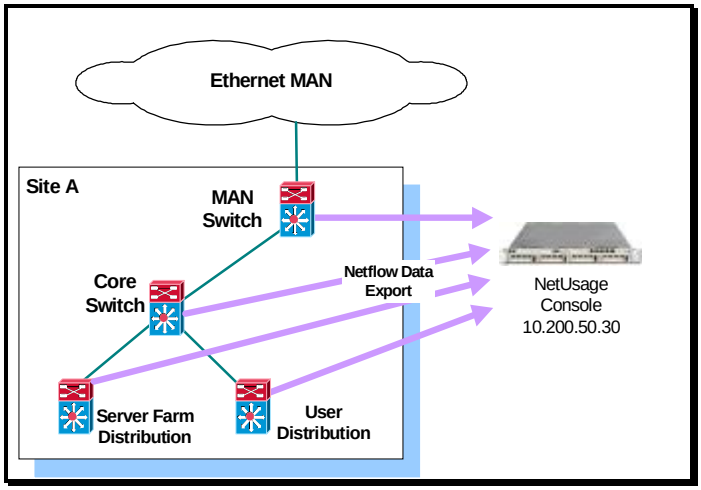
  ```
  ip flow-cache timeout active 1  (=> 1 minute)
  ip flow-cache timeout inactive 15  (=> 15 seconds)
  ```

Deployment Process

Router CPU is normally not an issue unless the CPU utilisation is running at 50% or more before enabling Netflow. Where routers are running at high utilization levels and CPU utilisation is a concern then Netflow can be enabled in a very granular fashion, one router at a time, or even one interface at a time, to check the impact. The traffic generated by enabling Netflow data export is also minimal in practice. However this can be calculated in advance if desired; refer to the Cisco Netflow Briefing Paper for further details.

Appendix B - Configuring Cisco Catalyst 6500 switches

The Cisco Catalyst 6500 platform can be operated in “Hybrid” mode, running “CatOS” software on the Supervisor card and “IOS” software on the MSFC daughter card (routing module). In this scenario the vast majority of the traffic will be Layer3 switched in hardware by the PFC module on the Supervisor. So for most deployments it is sufficient to configure Netflow on the Supervisor. If the small amount of MSFC software switched traffic (typically <1%) must also be captured then Netflow must be enabled separately on the MSFC.



Data exported from the Supervisor will be sourced from the “sc0” interface IP address; this cannot be altered. The data exported from the MSFC will be sourced from a configurable address, typically a loopback.

When the Cisco Catalyst 6500 platform is operated in “Native” mode it runs a single unified IOS image on both the Supervisor and the MSFC (routing module). Just as in the “Hybrid” case the vast majority of the traffic will be Layer3 switched in hardware on the Supervisor via the PFC module. However unlike the “Hybrid” case the data exported from the Supervisor will be sourced from the same IP address configured as the source for the MSFC export (typically a loopback). For native deployments NDE should always be configured for both Supervisor and MSFC.

In both Hybrid and Native deployments the Supervisor exports data for hardware/PFC switched flows for all ports on the switch as soon as Netflow Data Export (NDE) is enabled; there is no option to selectively enable on a per-port basis. However as the Netflow cache is created in hardware the only impact caused by enabling Netflow export is the data export function itself, which causes minimal CPU impact.

On the MSFC Netflow caching is enabled on a per-interface basis like any other IOS based router.

The actual commands for enabling on the Supervisor and MSFC are illustrated below.

Hybrid Configuration:

- Catalyst 6500 Supervisor "CatOS" Configuration

```
set mls nde 10.200.50.30 5555
set mls nde version 7
set mls flow full
set mls agingtime long 64
set mls agingtime 32
set mls nde enable
```

- Catalyst 6500 MSFC "IOS" Configuration

```
interface vlan 10
 interface description *** Link to Core Switch A***
 ip address 10.200.10.1 255.255.255.252
 ip route-cache flow
!
interface vlan 50
 interface description *** Link to User Access Switch 54 ***
 ip address 10.200.20.1 255.255.255.252
 ip route-cache flow
!
ip flow-export source loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export destination 10.200.50.30 5555
```

Native Configuration:

- Catalyst 6500 Native IOS Configuration for Supervisor Export

```
mls netflow
mls flow ip full
mls aging normal 32
mls aging long 64
no mls aging fast
mls nde sender version 5
```

- Catalyst 6500 Native IOS Configuration for MSFC Export

```
interface vlan 10
 interface description *** Link to Core Switch A***
 ip address 10.200.10.1 255.255.255.252
 ip route-cache flow
!
interface gigabit 4/2
 interface description *** Link to User Access Switch 54 ***
 ip address 10.200.20.1 255.255.255.252
 ip route-cache flow
!
ip flow-export source loopback0
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
ip flow-export destination 10.200.50.30 5555
```

Appendix C - Verifying NetFlow™ Export

The commands used to verify that NetFlow™Data Export has been correctly configured and is working vary by platform. The relevant commands are shown below. Also included are the commands to check CPU utilization so that the impact of enabling NetFlow™export can be monitored.

Standard IOS Router:

- Verifying NetFlow™ data is being cached and exported

```
show ip cache flow
show ip flow export
```

- Monitoring CPU utilisation

```
show processes cpu
```

Catalyst 6500 in Hybrid Mode

- Verifying NetFlow™ data is being cached and exported from the Supervisor/PFC

```
show mls nde
```

- Monitoring CPU utilization on the Supervisor/PFC

```
ps -c
```

- Verifying NetFlow™ data is being cached and exported from the MSFC

```
show ip cache flow
show ip flow export
```

- Monitoring CPU utilization on the MSFC

```
show processes cpu
```

Catalyst 6500 in Native Mode

- Verifying NetFlow™ data is being cached and exported from the Supervisor/PFC

```
show mls nde
```

- Verifying NetFlow™ data is being cached and exported from the MSFC

```
show ip cache flow
show ip flow export
```

- Monitoring CPU utilization

```
show processes cpu
```

Appendix D - Deployment Checklist

Step	Task	Completed
1	Physical Installation, and Ethernet patching	
2	Connect to console port using serial cable and PC with terminal emulation package. Login using default administrator account, user “admin”, password “admin”	
3	From the *Administration Menu* displayed on the asynch console select Option 1 to configure basic IP networking parameters: • IP Address • Subnet mask • Default gateway • DNS server(s)	
4	Reboot using *Administration Menu* Option 8 so that new IP settings take effect	
5	Verify IP connectivity using “ping” from another device on the network	
6	Connect to console using SSH, and login using default administrator account, user “admin”, password “admin”	
7	Use the *Administration Menu* Option 3 to configure NTP servers, and Option 5 to configure the local timezone.	
8	Connect to the Web Admin GUI using a web browser and login using default administrator account, user “admin”, password “admin”	
90	Navigate to *Admin* > *Network Devices* page. A list of auto-discovered Netflow™ data sources is displayed, marked with gold “Unknown” status icons. Click on the “add” link beside each one which you wish to monitor. Status icon will change to green for “Active”.	
10	Navigate to *Admin* > *Links* page. A list of auto-discovered links is displayed, marked with gold “Unknown” status icons. Click on the “add” link beside each one to add the links you wish to monitor. Enter and save the link parameters.	
11	Navigate to *Reports* >*Traffic* homepage. Live reports (accessed by setting date equal to the current date) will be available for view after 10 minutes.	
12	After 24 hours *Network Summary* reports for the previous 24 hour period will be available.	

Appendix E - Sources of Further Information

Web Site

- § NetUsage™ www.netusage.net
- § Cisco NetFlow™ www.cisco.com/go/netflow

Product Sheets

- § NetUsage Product Suite Overview www.netusage.net/products.htm
- § NetUsage Traffic Reporter www.netusage.net/traffic_reporter.htm
- § NetUsage Host Reporter www.netusage.net/host_reporter.htm
- § NetUsage Business Reporter www.netusage.net/business_reporter.htm
- § NetUsage Cost Reporter www.netusage.net/cost_reporter.htm

White Papers

- § Cisco NetFlow Briefing Paper www.netusage.net/case_studies.htm
- § WANs & MANs Deployment Paper www.netusage.net/case_studies.htm

Contact Address

Apoapsis Limited
The Bridge
12-16 Clerkenwell Road
London EC1M 5PQ
Email : info@netusage.net