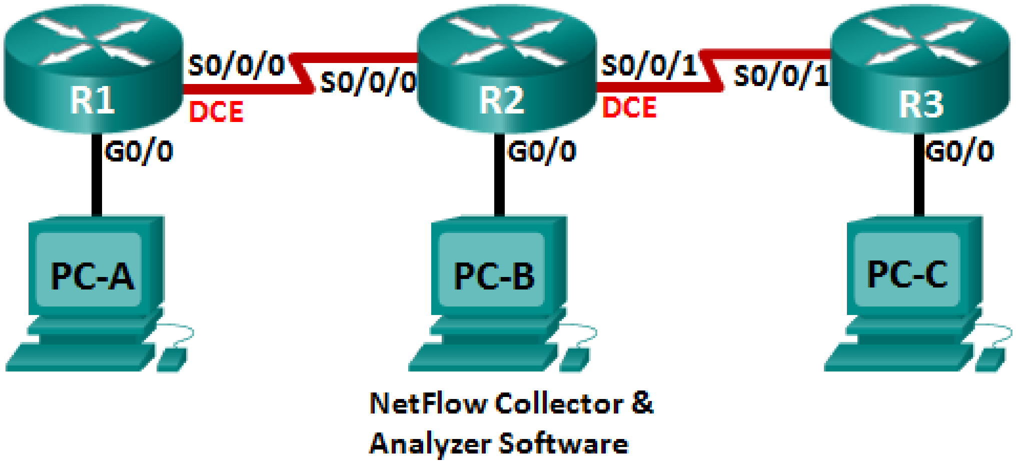
Lab – Collecting and Analyzing NetFlow Data

Topology



Addressing Table

Device	Interface	IP Address	Default Gateway
R1	G0/0	192.168.1.1/24	N/A
	S0/0/0 (DCE)	192.168.12.1/30	N/A
R2	G0/0	192.168.2.1/24	N/A
	S0/0/0	192.168.12.2/30	N/A
	S0/0/1 (DCE)	192.168.23.1/30	N/A
R3	G0/0	192.168.3.1/24	N/A
	S0/0/1	192.168.23.2/30	N/A
PC-A	NIC	192.168.1.3	192.168.1.1
PC-B	NIC	192.168.2.3	192.168.2.1
PC-C	NIC	192.168.3.3	192.168.3.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure NetFlow on a Router

Part 3: Analyze NetFlow Using the CLI

Part 4: Explore NetFlow Collector and Analyzer Software

Background / Scenario

NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch. NetFlow enables network and security monitoring, network planning, traffic analysis, and IP accounting. It is important not to confuse NetFlow's purpose and results with that of packet capture hardware and software. Packet capturing records all possible information exiting or entering a network device for later analysis, NetFlow targets specific statistical information.

Flexible NetFlow is the latest NetFlow technology, improving on the original NetFlow by adding the capability to customize the traffic analysis parameters. Flexible NetFlow uses the Version 9 export format. Starting with Cisco IOS Release 15.1, many useful Flexible NetFlow commands are supported.

In this lab, you will configure NetFlow to capture both ingress (incoming) and egress (outgoing) packets. You will use **show** commands to verify that NetFlow is operational and gathering statistical information. You will also explore available options for NetFlow collection and analysis software.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and routers.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

a. Disable DNS lookup.

b. Configure device names as shown in the topology.

c. Assign **class** as the encrypted privileged EXEC mode password.

d. Assign **cisco** as the console and vty passwords and enable login.

e. Encrypt the plain text passwords.

f. Configure a MOTD banner to warn users that unauthorized access is prohibited.

g. Configure **logging synchronous** for the console line.

h. Set the clock rate for all DCE serial interfaces at **128000**.

i. Configure the IP addresses as listed in the Addressing Table.

j. Configure OSPF using Process ID 1 and advertise all networks. Ethernet interfaces should be passive.

k. Create a local database on R3 with the username **admin** and password **cisco** with the privilege level at **15**.

l. On R3, enable the HTTP service and authenticate HTTP users by using the local database.

m. Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Step 5: Verify end-to-end connectivity.

All devices should be able to ping other deices in the topology. Troubleshoot as necessary until end-to-end connectivity is established.

Note: It may be necessary to disable the PC firewall for pings between PCs to be successful.

Part 2: Configure NetFlow on a Router

In Part 2, you will configure NetFlow on router R2. NetFlow will capture all ingress and egress traffic on the R2 serial interfaces and export the data to the NetFlow collector, PC-B. Flexible NetFlow Version 9 will be used to export to the NetFlow collector.

Step 1: Configure NetFlow capture.

Configure NetFlow data capture on both serial interfaces. Capture data from ingress and egress packets.

```
R2(config)# interface s0/0/0
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
R2(config-if)# interface s0/0/1
R2(config-if)# ip flow ingress
R2(config-if)# ip flow egress
```

Step 2: Configure NetFlow data export.

Use the **ip flow-export destination** command to identify the IP address and the UDP port of the NetFlow collector to which the router should export NetFlow data. UDP Port number 9996 will be used for this configuration.

```
R2(config)# ip flow-export destination 192.168.2.3 9996
```

Step 3: Configure the NetFlow export version.

Cisco routers running IOS 15.1 support NetFlow versions 1, 5, and 9. Version 9 is the most versatile export data format, but is not backward-compatible with earlier versions. Use the **ip flow-export version** command to set the NetFlow version.

```
R2(config)# ip flow-export version 9
```

Step 4: Verify the NetFlow configuration.

a. Issue the **show ip flow interface** command to review the NetFlow capture interface information.

```
R2# show ip flow interface
Serial0/0/0
  ip flow ingress
  ip flow egress
Serial0/0/1
  ip flow ingress
  ip flow egress
```

b. Issue the **show ip flow export** command to review the NetFlow data export information.

```
R2# show ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.2.3 (9996)
  Version 9 flow records
  388 flows exported in 63 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 fixup failures
```

Part 3: Analyze NetFlow Using the CLI

In Part 3, you will generate data traffic between R1 and R3 to observe NetFlow technology.

Step 1: Generate data traffic between R1 and R3.

a. Telnet from R1 to R3 using the IP address 192.168.3.1. Enter the password **cisco** to enter the user EXEC mode. Enter the password **class** to enable global EXEC mode. Issue the **show run** command to generate some Telnet traffic. Keep your Telnet session active for now.

b. From R3, issue the **ping 192.168.1.1 repeat 1000** command to ping the R1 G0/0 interface. This will generate ICMP traffic through R2.

c. From PC-A, browse to R3 using the 192.168.3.1 IP address. Login as **admin** with the password **cisco**. Keep the browser open after you have logged into R3.

Note: Make sure the pop-up blocker is disabled on your browser.

Step 2: Display a summary of the NetFlow accounting statistics.

On R2, issue the **show ip cache flow** command to display changes to the summary of NetFlow data, including packet size distribution, IP flow information, captured protocols, and interface activity. Notice the protocols now display in the summary data.

```
R2# show ip cache flow
IP packet size distribution (5727 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .147 .018 .700 .000 .001 .001 .001 .001 .011 .009 .001 .002 .000 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .001 .097 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 114 added
  1546 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  0 active, 1024 inactive, 112 added, 112 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics 00:07:35
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           4      0.0        27    43      0.2       5.0      15.7
TCP-WWW            104      0.2        14   275      3.4       2.1       1.5
ICMP                 4      0.0      1000   100      8.8      27.9      15.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Total:              112      0.2        50   146     12.5       3.1       2.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    43
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    40
```

Step 3: End the Telnet and browser sessions.

a. Issue the **exit** command on R1 to disconnect from the Telnet session to R3.

b. Close the browser session on PC-A.

Step 4: Clear NetFlow accounting statistics.

a. On R2, issue the **clear ip flow stats** command to clear NetFlow accounting statistics.

```
R2# clear ip flow stats
```

b. Re-issue the **show ip cache flow** command to verify that the NetFlow accounting statistics have been reset. Notice that, even though you are no longer generating data through R2, data is being picked up by NetFlow. In the example below, the destination address for this traffic is multicast address 224.0.0.5, or OSPF LSA data.

```
R2# show ip cache flow
IP packet size distribution (124 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 2 added
  1172 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  2 active, 1022 inactive, 2 added, 2 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 00:09:48
```

```
Protocol          Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------          Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
IP-other              2      0.0       193    79      0.6    1794.8       5.7
Total:                2      0.0       193    79      0.6    1794.8       5.7


SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/0       192.168.12.1    Null          224.0.0.5       59 0000 0000    35

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/0/1       192.168.23.2    Null          224.0.0.5       59 0000 0000    33
```

Part 4: Explore NetFlow Collector and Analyzer Software

NetFlow Collector and Analyzer Software is available from many vendors. Some software is provided as freeware, others are not. The following URL provides a summary web page of some of the Freeware NetFlow software available:
http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/networking_solutions_products_genericcontent0900aecd805ff72b.html

Review this web page to acquaint yourself with some of the available NetFlow Collector and Analyzer software products.

Reflection

1. What is the purpose of NetFlow collector software?

2. What is the purpose of NetFlow analyzer software?

3. What are the seven critical fields used by the original NetFlow to distinguish flows?

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.