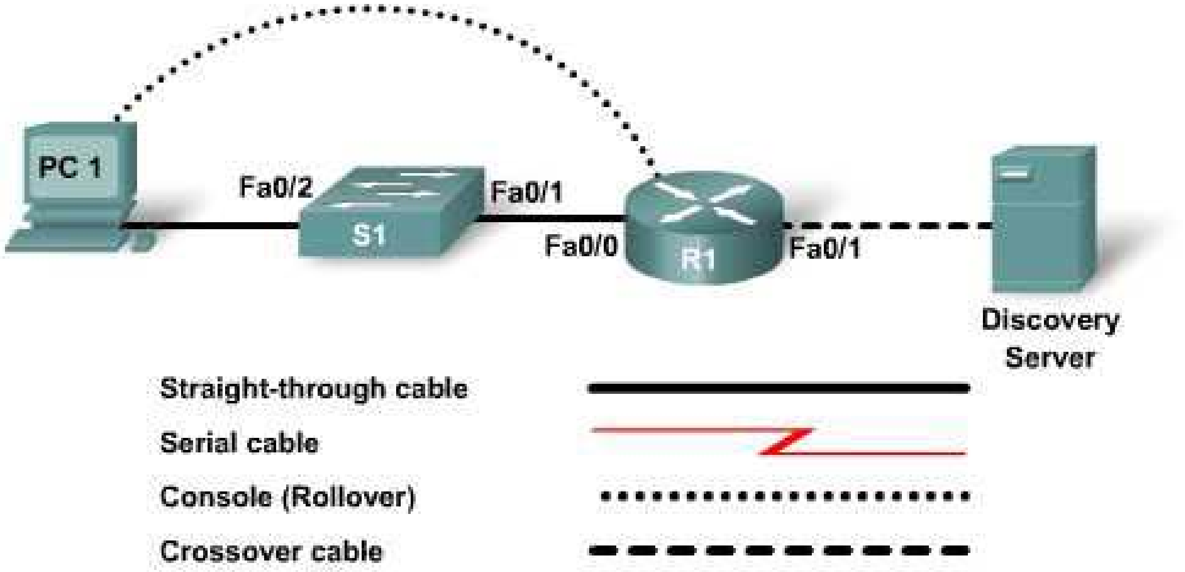
Lab 4.1.2 Characterizing Network Applications



Device Designation	Device Name	Address	Subnet Mask
Discovery Server	Business Services	172.17.1.1	255.255.0.0
R1	FC-CPE-1	Fa0/1 172.17.0.1 Fa0/0 10.0.0.1	255.255.0.0 255.255.255.0
S1	FC-ASW-1	—	—
PC1	Host 1	10.0.0.200	255.255.255.0

Objective

- Configure NetFlow to observe how the traffic flows.

Expected Results and Success Criteria

Before starting this lab, read through the tasks that you are expected to perform. What do you expect the result of performing these tasks will be?

____

____

____

How is an understanding of traffic flow useful in network design and in network administration?

____

____

____

Background / Preparation

Cisco IOS can include a feature called NetFlow that provides information about network users, network applications, peak usage times, and traffic routing. NetFlow can provide the following services:

- Network traffic accounting
- Usage-based network billing
- Network planning
- Security
- Denial of Service monitoring capabilities
- Network monitoring

Cisco routers that have the NetFlow feature enabled generate NetFlow records. These details can be viewed using **`show`** commands or exported from the router and collected using a NetFlow collector.

Although initially implemented by Cisco, NetFlow is emerging as an IETF standard: Internet Protocol Flow Information eXport (IPFIX). See RFC 3954 at http://www.ietf.org/rfc/rfc3954.txt.

NetFlow defines a data flow as a unidirectional sequence of packets that includes all of the following five values:

1. Source IP address
2. Destination IP address
3. Source TCP port
4. Destination TCP port
5. IP protocol

In this lab, you will observe the results of configuring NetFlow. In later labs, you will see how the state of data flows across the current network can be established so that a network upgrade can be planned and implemented.

Step 1: Cable and configure the current network

a. Connect and configure the devices in accordance with the topology and configuration given.

   For this lab, a PC workstation can substitute for a Discovery Server.

b. Ping between Host 1 and Discovery Server to confirm network connectivity.

   Troubleshoot and establish connectivity if the pings fail.

Step 2: Configure NetFlow on the interfaces

NetFlow is configured to monitor data flows in or out of specific router interfaces. **Ingress** captures traffic that is being received by the interface. **Egress** captures traffic that is being transmitted by the interface. In this lab, the traffic will be monitored on both router interfaces and in both directions from within the console session.

a. From the global configuration mode, issue the following commands:

```
FC-CPE-1(config)#interface fastethernet 0/0
FC-CPE-1(config-if)#ip flow ?
```

Note the two options available:

____

____

Which option captures traffic that is being received by the interface? __________

Which option captures traffic that is being transmitted by the interface? __________

b. Complete the NetFlow configuration.

```
FC-CPE-1(config-if)#ip flow egress
FC-CPE-1(config-if)#ip flow ingress
FC-CPE-1(config-if)#interface fastethernet 0/1
FC-CPE-1(config-if)#ip flow ingress
FC-CPE-1(config-if)#ip flow egress
FC-CPE-1(config-if)#exit
FC-CPE-1(config)#end
```

Step 3: Verify the NetFlow configuration

a. From the privileged EXEC mode, issue the **`show running-configuration`** command.

For each FastEthernet interface, what statement from the running-configuration denotes that NetFlow is configured?

interface FastEthernet0/0:

____

____

interface FastEthernet0/1:

____

____

b. From the privileged EXEC mode, issue the command:

```
FC-CPE-1#show ip flow ?
```

Note the three options available:

____

____

____

```
FC-CPE-1#show ip flow interface
FastEthernet0/0
  ip flow ingress
  ip flow egress
FastEthernet0/1
  ip flow ingress
  ip flow egress
```

Confirm that the output shown above is displayed. Troubleshoot your configuration if this output is not displayed.

Step 4: Create network data traffic

a. The captured data flow can be examined using the **`show ip cache flow`** command issued from the privileged EXEC mode.

```
FC-CPE-1#show ip cache flow
```

Issuing this command before any data traffic has flowed should produce output similar to the example shown here.

```
IP packet size distribution (0 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .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, 0 bytes
  0 active, 0 inactive, 0 added
  0 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec)
Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP
Pkts
```

b. List the seven highlighted column headings and consider what use this information may be in characterizing the network.

____

____

____

____

____

____

____

____

c. To ensure that flow cache statistics are reset, from privileged EXEC mode issue the command:

```
FC-CPE-1# clear ip flow stats
```

d. Ping the Business Server from Host 1 to generate a data flow.

From the command line of Host 1, issue the command **`ping 172.17.1.1 -n 200`**

Step 5: View the data flows

a. At the conclusion of the data flow, the details of the flow can be viewed. From privileged EXEC mode, issue the command:

```
FC-CPE-1#show ip cache flow
```

Output similar to that shown below will be displayed. Some values and details may be different in your lab.

```
IP packet size distribution (464 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .900 .096 .000 .000 .000 .000 .002 .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
  5 active, 4091 inactive, 48 added
  1168 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17416 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec)
Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow
/Flow
UDP-DNS             31      0.0         1    72      0.0       0.0
15.5
UDP-other           10      0.0         2    76      0.0       4.1
15.2
ICMP                 2      0.0       200    60      0.3     198.9
15.3
Total:              43      0.0        10    61      0.3      10.2
15.5

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP
Pkts
< output omitted >
```

b. Examine your output and list details that indicate data flow.

____

____

____

____

____

____

____

____

Step 6: Stop the NetFlow capture

a. To deactivate NetFlow capture, issue the **no ip flow** command at the interface configuration prompt.

```
FC-CPE-1(config)#interface fastethernet 0/0
FC-CPE-1(config-if)#no ip flow ingress
FC-CPE-1(config-if)#no ip flow egress
FC-CPE-1(config)#interface fastethernet 0/1
FC-CPE-1(config-if)#no ip flow ingress
FC-CPE-1(config-if)#no ip flow egress
```

b. To verify that NetFlow is deactivated, issue the **`show ip flow interface`** command from the privileged EXEC mode.

```
FC-CPE-1#show ip flow interface
FC-CPE-1#
```

No output is displayed if NetFlow is off.

Step 7: Clean up

Erase the configurations and reload the routers and switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Step 8: Reflection

Consider the possible range of data flow types across a network and how a tool like NetFlow could be implemented to assist in analyzing those flows.

____

____

____

____

____

____