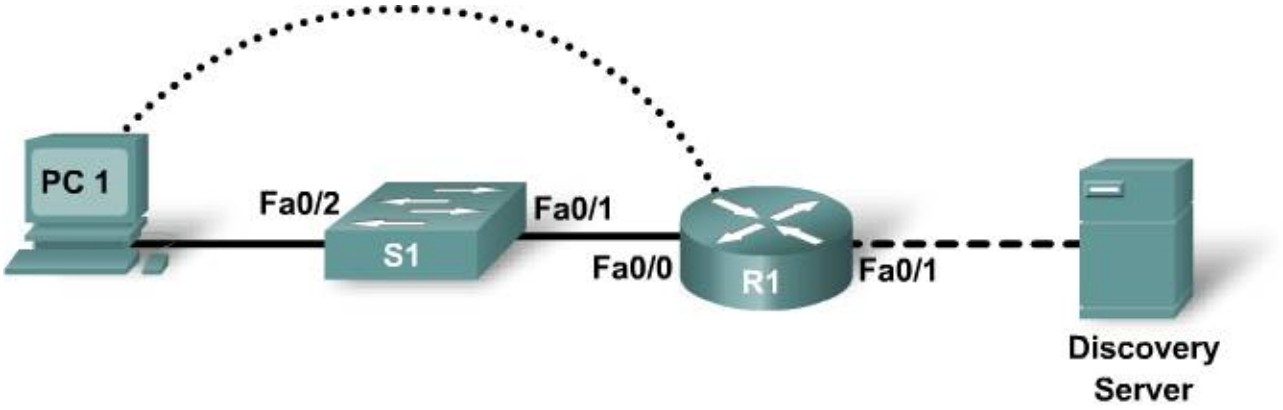
Lab 4.5.1 Identifying Traffic Flows



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	Host1	10.0.0.200	255.255.255.0

Objective

- Describe what is meant by application traffic flows.

640-802 CCNA Exam Objective

This lab contains skills that relate to the following CCNA exam objective:

- Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network.

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 administration?

_____

_____

_____

How will a network administrator know if the network devices can handle the amount of traffic?

_____

_____

_____

Background / Preparation

FilmCompany is an expanding small advertising company moving into interactive advertising media, including video presentations. This company has just been awarded a large big video support contract by the StadiumCompany. With this new contract, FilmCompany expects to see their business grow approximately 70 percent.

To facilitate this expansion, the state of data flow across the current network has to be established so that the network upgrade can be planned and implemented.

In this lab, you will use the Cisco routers IOS NetFlow feature capture and view data flow information.

Step 1: Cable and configure the current network

NOTE: If the PC used in this lab is also connected to your Academy LAN or to the Internet, ensure that you record the cable connections and TCP/IP settings so that these can be restored at the conclusion of the lab.

a. Referring to the topology diagram, connect the console (or rollover) cable to the console port on the router and the other cable end to the host computer with a DB-9 or DB-25 adapter to the COM 1 port. Ensure that power has been applied to both the host computer and router.

b. Establish a HyperTerminal or other terminal emulation program to the router.

   NOTE: Your instructor may substitute for Discovery Server an equivalent server for this lab.

c. From the command prompt on Host1, ping between Host1 and Discovery Server to confirm network connectivity. Troubleshoot and establish connectivity if the pings fail.

Step 2: Configure NetFlow on the interfaces

From the global configuration mode, issue the following commands to configure NetFlow:

```
FC-CPE-1(config)#interface fastethernet 0/0
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
```


Step 3: Verify the NetFlow configuration

a. From the privileged EXEC mode, issue the **show ip flow interface** command.

```
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.

b. From the privileged EXEC mode, issue the following command to ensure that flow cache statistics are reset:

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

Step 4: Create network data traffic

A range of network application data flows is to be generated and captured. Generate as many of the data flows shown below as is possible in your lab. Your instructor will advise you of the particular applications that are available to be used in this lab.

a. Ping the Discovery Server from Host1 to generate a data flow.

From the command line of Host1, issue the command **ping 172.17.1.1 -n 200**

b. Telnet to the Discovery Server from Host1.

If Discovery Server is being used, issue the command **telnet server.discovery.ccna** from the command prompt of Host1.

If Discovery Server is not being used, DNS is not configured, or if a terminal program such as HyperTerminal or TeraTerm is being used, telnet from Host1 to 172.17.1.1.

c. On Host1, launch a web browser and enter the URL http://server.discovery.ccna

If Discovery Server is not being used or DNS is not configured, then use http://172.17.1.1 to access the web services configured on that server.

d. Use FTP to download a file.

On Host1, launch a web browser and enter the URL **ftp://server.discovery.ccna**, or issue **ftp server.discovery.ccna** from the command line. If DNS is not configured use the IP address 172.17.1.1 instead of the domain name.

Download a file from the server.

NOTE: If the email client program is not installed on Host1, download that program file for use in the next step.

e. If email accounts have been configured using the POP3 and SMTP services on Discovery Server, send an email using one of these accounts.

Step 5: View the data flows

At the conclusion of the data flow, view the details by issuing the **show ip cache flow** command from privileged EXEC mode.

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

Output similar to this will be displayed.


```
IP packet size distribution (3969 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .351 .395 .004 .011 .001 .005 .009 .001 .002 .005 .001 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .013 .000 .195 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 1368 added
  22316 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, 0 chunks added
  last clearing of statistics 02:50:15
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           9      0.0        13    47      0.0       5.2      10.8
TCP-FTP             28      0.0         7    62      0.0       0.8      10.4
TCP-WWW             64      0.0         7   138      0.0       0.3       2.1
TCP-other           16      0.0        75   840      0.1       0.0       4.1
UDP-DNS            878      0.0         1    72      0.0       0.0      15.4
UDP-other          347      0.0         3    88      0.1       4.5      15.5
ICMP                26      0.0         1    70      0.0       0.8      15.4
Total:            1368      0.1         2   318      0.3       1.2      14.6
< output omitted >
```

From your output, list the name of each protocol with the number of flows.

_____

_____

_____

_____

_____

_____

_____

What was the total number of packets generated? _____

Which protocol generated the most packets? _____

Which protocol produced the most bytes per flow? _____

Which protocol's flows were on the network the longest time? _____

Which protocol used the longest amount of network time? _____

Step 6: 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 7: Reflection

Create a projected applications document listing the applications planned to use the network.

Application Type	Application	Protocol	Priority	Comments