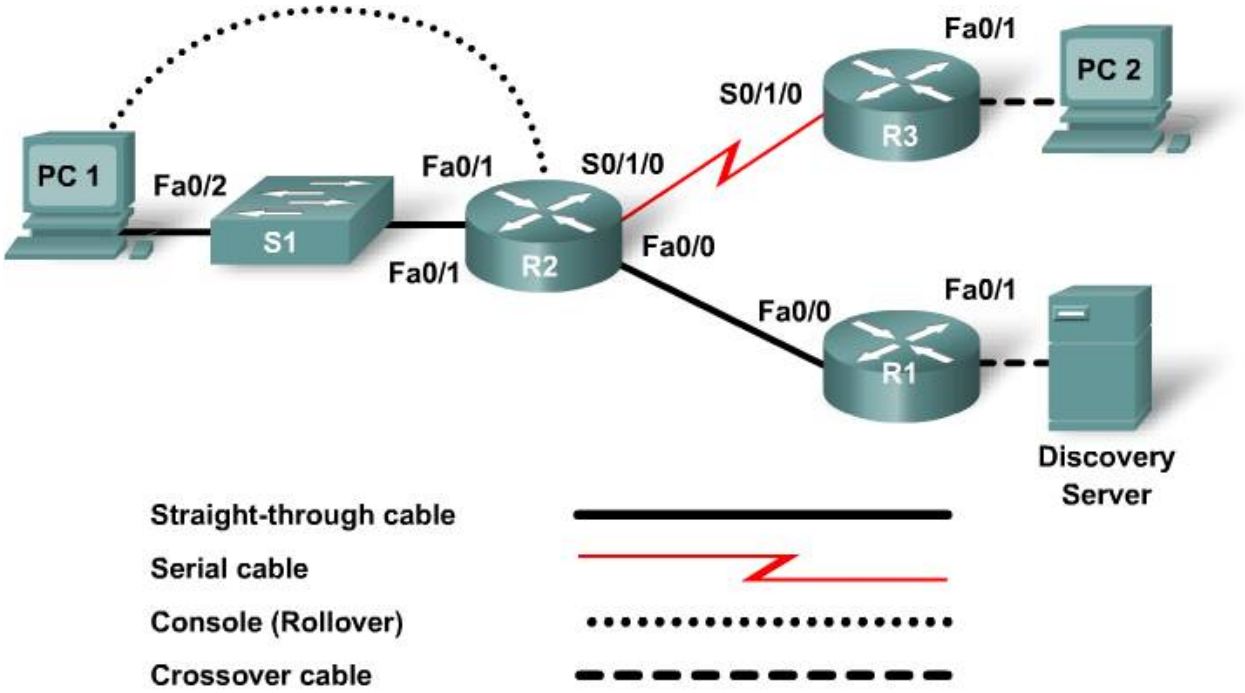
Lab 4.5.5 Diagramming Extranet Traffic Flows



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 10.10.0.1	255.255.0.0 255.255.255.252
R2	FC-CPE-2	Fa0/0 10.10.0.2 Fa0/1 10.0.0.1 S0/1/0 10.10.10.1	255.255.255.252 255.255.255.0 255.255.255.252
R3	ISP	Fa0/1 10.20.0.1 S0/1/0 10.10.10.2	255.255.255.0 255.255.255.252
PC1	Video Workstation	10.0.0.200	255.255.255.0
PC2	Extranet Host	10.20.0.200	255.255.255.0

Objective

- Use NetFlow to diagram FilmCompany Extranet 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?

_____

_____

_____

Why is diagramming extranet traffic flows useful in network administration?

_____

_____

_____

What can be learned from diagramming traffic flows to and from the extranet?

_____

_____

_____

Background / Preparation

FilmCompany is an expanding 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.

Developing a diagram of applications, devices, and traffic flow enables the designer to analyze the proposed design and identify where the network can be improved. The logical topology diagram shows that the servers are identified with the applications that will be used. Areas that require redundancy or increased security are also easier to identify. Redundant paths to the server and security measures, such as a hardware firewall, can be marked on the diagram. The logical design for the network must be aligned with the initial business goals and technical requirements of the customer. The diagram gives the designer and customer a visual idea of what is already on the network and helps to get a better view of what is still required.

In this lab, you will use NetFlow to diagram the flow of traffic to and from two trusted remote partners, or customers, at the stadium to the FilmCompany network. Preparing this diagram requires you to identify the remote hosts and determine the traffic generated across the network, both from the hosts and from the FilmCompany server.

In this Lab, PC2 represents a host on the FilmCompany extranet that communicates with the FilmCompany network.

Step 1: Cable and configure the current network

NOTE: If the PCs used in this lab are 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. Cable the topology given in the diagram. Ensure that power has been applied to both the host computer and router.

b. Establish a HyperTerminal or other terminal emulation program to the routers and configure the hostname and interfaces shown in the table.

c. Set a clock rate on the DCE interface of the serial link between R2 and R3. Routing will have to be configured on the three routers to establish data communications.

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

d. From PC1, ping PC2 and Discovery Server to confirm network connectivity. Troubleshoot and establish connectivity if the pings fail.

Step 2: Configure NetFlow on router FC-CPE-1 interfaces

From the global configuration mode, issue the following commands to configure NetFlow on the router FC-CPE-1.

```
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
FC-CPE-1(config-if)#end
```

Step 3: Verify the NetFlow configuration

a. From the privileged EXEC mode on router FC-CPE-1, 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: Configure NetFlow on router FC-CPE-2 interfaces

From the global configuration mode, issue the following commands to configure NetFlow on the router FC-CPE-2:

```
FC-CPE-2(config)#interface fastethernet 0/0
FC-CPE-2(config-if)#ip flow egress
FC-CPE-2(config-if)#ip flow ingress
FC-CPE-2(config-if)#interface fastethernet 0/1
FC-CPE-2(config-if)#ip flow ingress
FC-CPE-2(config-if)#ip flow egress
FC-CPE-2(config-if)#interface serial 0/1/0
FC-CPE-2(config-if)#ip flow ingress
FC-CPE-2(config-if)#ip flow egress
FC-CPE-2(config-if)#end
```

Step 5: Verify the NetFlow configuration

a. From the privileged EXEC mode on router FC-CPE-2, issue the **show ip flow interface** command.

```
FC-CPE-2#show ip flow interface
```



```
FastEthernet0/0
  ip flow ingress
  ip flow egress
FastEthernet0/1
  ip flow ingress
  ip flow egress
Serial0/1/0
  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-2#clear ip flow stats
```

Step 6: Configure NetFlow on router ISP interfaces

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

```
ISP(config)#interface fastethernet 0/1
ISP(config-if)#ip flow ingress
ISP(config-if)#ip flow egress
ISP(config-if)#interface serial 0/1/0
ISP(config-if)#ip flow ingress
ISP(config-if)#ip flow egress
ISP(config-if)#end
```

Step 7: Verify the NetFlow configuration

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

```
ISP#show ip flow interface
FastEthernet0/1
  ip flow ingress
  ip flow egress
Serial0/1/0
  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:

```
ISP#clear ip flow stats
```

Step 8: Create network data traffic

Ideally, a range of network application data flows between the trusted extranet host PC2 and PC1 on the FilmCompany LAN should 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 and to be used in this lab.

To simulate data traffic between the two PCs:

a. Ping between them.

b. Attempt to establish a Telnet session between the two PCs.

c. If you have rights, enable file sharing and copy a file in both directions between the two PCs.

Step 9: View the data flows

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

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

FC-CPE-2#show ip cache verbose flow

ISP#show ip cache verbose flow
```

b. Examine the output and record the different data flows for each router.

Router FC-CPE-1 Data Flows

Application Type	Source	Destination	Comments

Router FC-CPE-2 Data Flows

Application Type	Source	Destination	Comments

Router ISP Data Flows

Application Type	Source	Destination	Comments

c. Discuss and compare the data flows for each router. Particularly consider how these flows differ from the previous Labs and the implications this has in understanding which network devices and resources are used for particular flows.

Step 10: 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.

Challenge

This lab simulates the flow of traffic to and from FilmCompany and from selected trusted partners and customers. These data flows for a production network would be much more extensive and recorded over a greater period of time, perhaps a full working week. Additionally, remote access from trusted sites would most likely be established using VPNs (Virtual Private Networks) across the Internet or a WAN.

On the FilmCompany initial current network topology shown on the next page, add two trusted remote site hosts attached to the "far" side of the cloud icon. Draw a circle that encloses the remote access links to the FilmCompany network and server. In this case study, initially the FilmCompany remote sites access its network across the Internet.

One of the objects of this analysis is to establish the benefits of using a dedicated WAN link using Frame Relay for the stadium-based remote sites to access the FilmCompany network.

Then, using the data flows recorded in this lab as a starting point, use different colors to mark on the diagram the different extranet data flows between the trusted remote hosts and devices on the FilmCompany network.

Diagram traffic flows to and from selected trusted partners, customers, and vendors.