Seneca | SCHOOL OF INFORMATION TECHNOLOGY, ADMINISTRATION AND SECURITY

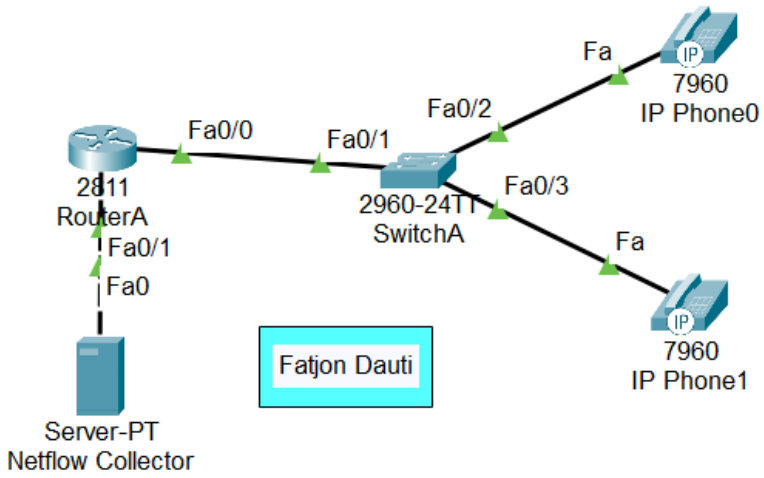
DCN704 – Collaborative Communications

Lab # 4 - Netflow

Student Name: Fatjon Dauti
Student ID #: 151413192

Total marks: 5

Topology



Replace this screenshot with your own topology from Packet Tracer. [1 mark]

IP configuration :

- IP Phone n°1 : 192.168.10.2/24
- IP Phone n°2 : 192.168.10.4/24
- Router Fa0/0 : 192.168.10.1/24 (switch side)
- Router Fa0/1 : 192.168.20.1/24 (Server side)
- Netflow Collector : 192.168.20.2/24

Define all the networking parameters (Switching, Routing, VLANs, DHCP, TFTP, e-phones, etc.) as you did it in previous labs. Be sure that you use a Cisco Router 2811, a Cisco Switch 2960, and Cisco IP Phones 7960.

Step 1 – Netflow Configuration:

Netflow is an application that runs on routers and collects IP traffic information. It can be used for network accounting and security auditing, but it also consumes additional memory on the router.

Configure Netflow collection on router interfaces using the "ip flow" IOS command. The flow can be configured on either ingress (received traffic) or egress (transmitted traffic) direction. It is recommended to configure the flow on the ingress.

```
Router0(config)#interface FastEthernet0/0
```

```
ip flow ingress

ip address 192.168.10.1 255.255.255.0

duplex auto

speed auto
```

Step 2 – Netflow Collector: Configure the ISR 2811 router to send the NetFlow records to the NetFlow collector. Packet Tracer Netflow collection software deployed on end devices (servers or PCs) uses UDP port 9996.

Follow this link to read about the NetFlow version 9 formats.

https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html.

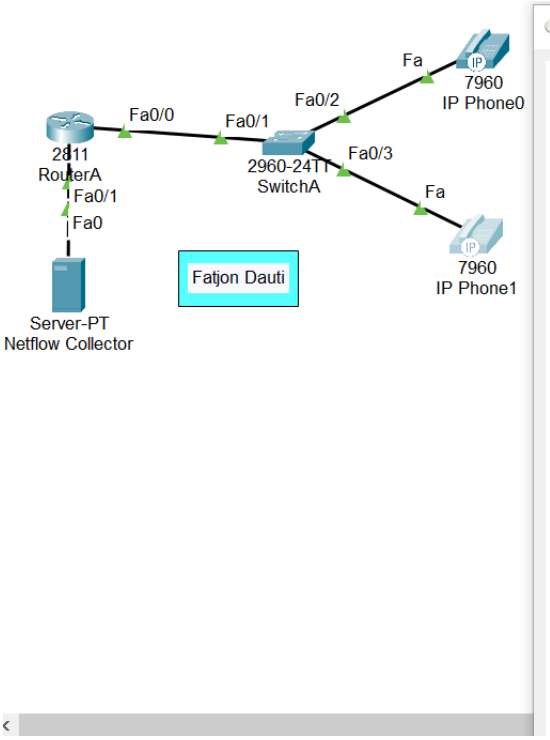
Use the following command to send NetFlow records to the Server-PT.

```
Router0(config)#ip flow-export destination 192.168.20.2 9996

ip flow-export version 9
```

Step 3 - Testing the configuration

Make phone calls from IP Phone n°1 to IP Phone n°2, and viceversa. Use the "**show ip cache flow**" command on the ISR router to display the router's Netflow cache.

Insert the screenshot of this command output here. [1 mark]



RouterA

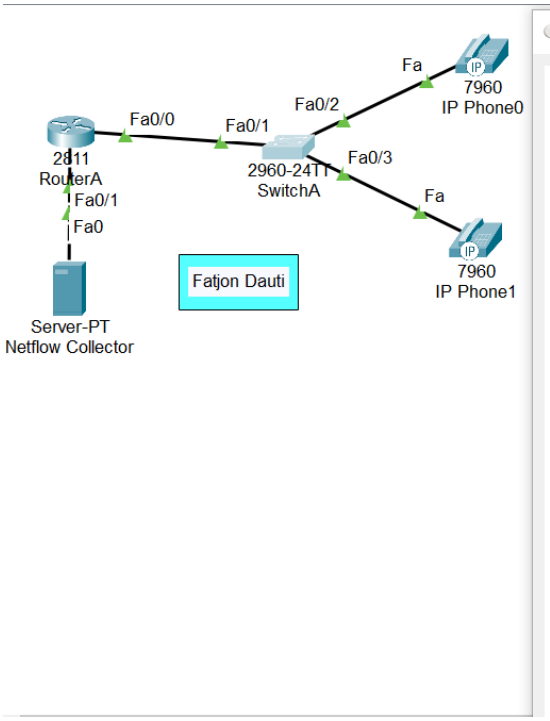
Physical Config CLI Attributes

IOS Command Line Interface

```
RouterA#show ip cache flow
IP packet size distribution (177 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .989 .011 .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, 38 added
  0 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, 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
TCP-SKINNY          35      0.0         3    40      0.0      10.3    1982.0
UDP-DHCP             1      0.0         2    88      0.0       1.0    1982.0
Total:              36      0.0         3    41      0.0      10.0    1982.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         192.168.10.2    Local         192.168.10.1    06 0401 07d0    23
Fa0/0         192.168.10.4    Local         192.168.10.1    06 0402 07d0    29
RouterA#
```

Repeat more phone calls (at least one-minute long calls) and issue the **show ip cache flow** command again.

Insert the screenshot of this command output here. [1 mark]



RouterA

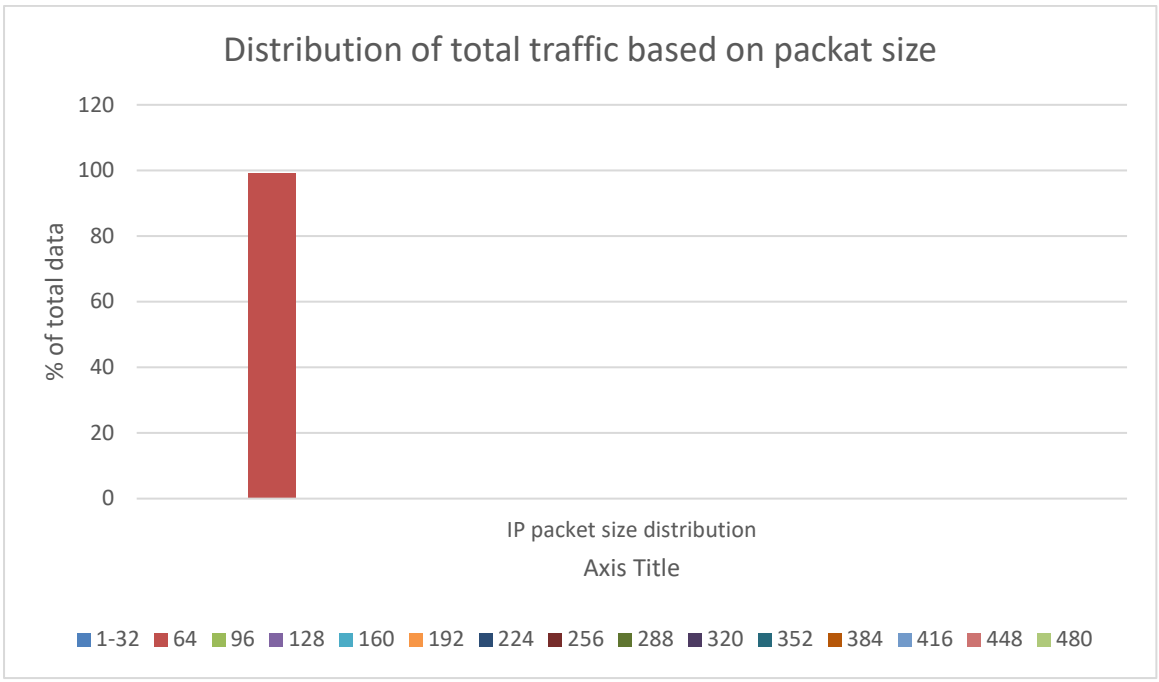
Physical Config CLI Attributes

IOS Command Line Interface

```
RouterA#show ip cache flow
IP packet size distribution (276 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .993 .007 .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, 60 added
  3 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, 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
TCP-SKINNY          57      0.0         4    40      0.1      11.2    1982.0
UDP-DHCP             1      0.0         2    88      0.0       1.0    1982.0
Total:              58      0.0         4    40      0.1      11.0    1982.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         192.168.10.2    Local         192.168.10.1    06 0401 07d0     4
Fa0/0         192.168.10.4    Local         192.168.10.1    06 0402 07d0     3
```

Answer the following questions. **[1 mark]**

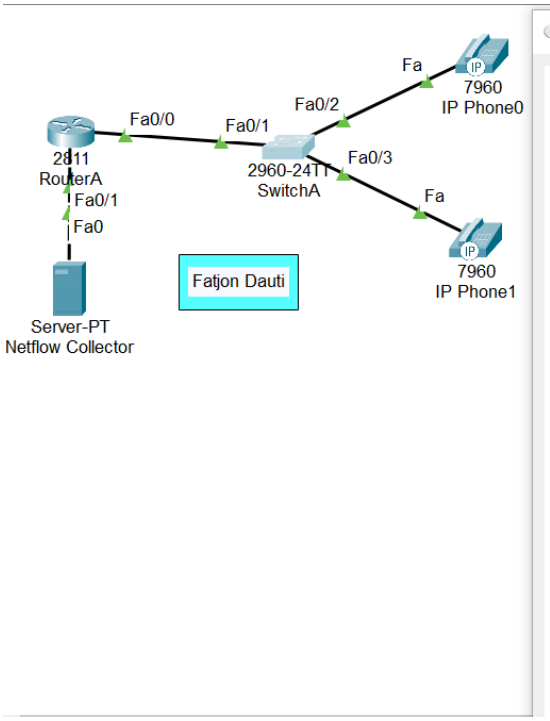
1. Make a histogram showing packet size ranges on the horizontal axis and the percentage of the total traffic in the vertical axis. Insert the histogram here.



2. How big is the IP flow switching cache? 278544 bytes
3. How big is the IP sub flow cache? 34056 bytes
4. What signaling protocol is used? SKINNY (SCCP)
   Does it run over TCP or UDP? TCP

Below is an example of a typical output.

Replace this information and insert the screenshot of this command output here. [1 mark]



RouterA

Physical Config CLI Attributes

IOS Command Line Interface

```
RouterA#show ip cache flow
IP packet size distribution (276 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .993 .007 .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, 60 added
  3 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, 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
TCP-SKINNY          57      0.0         4    40      0.1      11.2    1982.0
UDP-DHCP             1      0.0         2    88      0.0       1.0    1982.0
Total:              58      0.0         4    40      0.1      11.0    1982.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         192.168.10.2    Local         192.168.10.1    06 0401 07d0     4
Fa0/0         192.168.10.4    Local         192.168.10.1    06 0402 07d0     3
```

Text form:

```
RouterA#show ip cache flow
IP packet size distribution (276 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .993 .007 .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, 60 added
  3 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, 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
TCP-SKINNY          57      0.0         4    40      0.1      11.2    1982.0
UDP-DHCP             1      0.0         2    88      0.0       1.0    1982.0
Total:              58      0.0         4    40      0.1      11.0    1982.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         192.168.10.2    Local         192.168.10.1    06 0401 07d0     4
Fa0/0         192.168.10.4    Local         192.168.10.1    06 0402 07d0     3
RouterA#
```

```
!SwitchA
enable
config t
hostname SwitchA
line con 0
logging synchronous
exec-timeout 0 0
!
int range f0/2-3
switchport voice vlan 1
!
vlan 10
name voice
int range f0/2-3
switchport voice vlan 10
!

!RouterA
enable
config t
hostname RouterA
line con 0
logging synchronous
exec-timeout 0 0
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.10.3
ip dhcp pool voice
net 192.168.10.0 255.255.255.0
default-router 192.168.10.1
option 150 ip 192.168.10.1
!
int f0/0
ip add 192.168.10.1 255.255.255.0
no shut
int f0/1
ip add 192.168.20.1 255.255.255.0
no shut
!
!configure phones
telephony-service
ip source-address 192.168.10.1 port 2000
max-dn 2
max-ephones 2
auto assign 1 to 2
create cnf-files
!
ephone-dn 1
number 101
ephone-dn 2
number 102
!
```