

Para este ejercicio se creó una topología sencilla, que consta de tres sucursales las cuales tienen un servidor DNS, Web y de Correo.

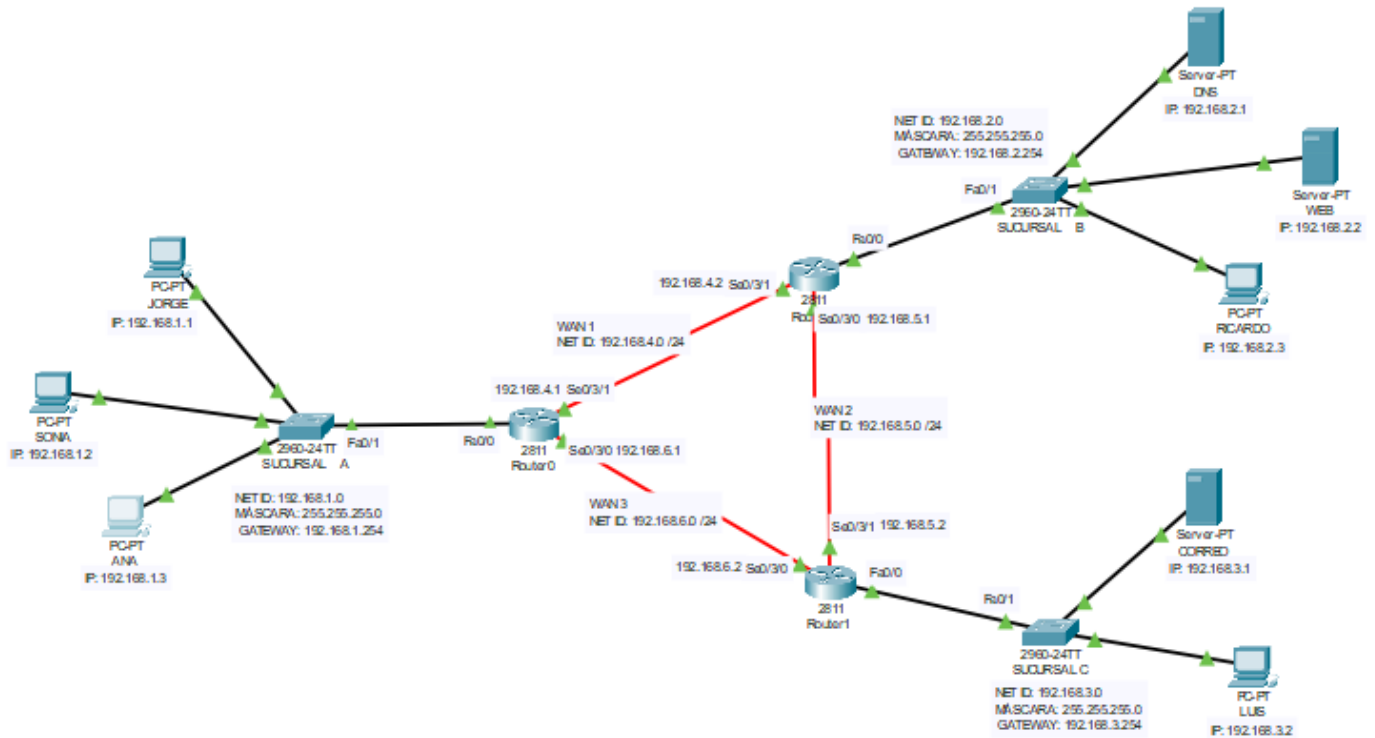


Tabla de direccionamiento

Sucursal	Segmento	Máscara	Rango IP asignables	Gateway	Broadcast
A	192.168.1.0 / 24	255.255.255.0	192.168.1.1 – 192.168.1.254	192.168.1.254	192.168.1.255
B	192.168.2.0 / 24	255.255.255.0	192.168.2.1 – 192.168.2.254	192.168.2.254	192.168.2.255
C	192.168.3.0 / 24	255.255.255.0	192.168.3.1 – 192.168.3.254	192.168.3.254	192.168.3.255

Tabla de redes WAN

WAN	Segmento	Máscara	Rango IP asignables	Gateway	Broadcast
1	192.168.4.0 / 24	255.255.255.0	192.168.4.1 – 192.168.4.254	192.168.4.254	192.168.4.255
2	192.168.5.0 / 24	255.255.255.0	192.168.5.1 – 192.168.5.254	192.168.5.254	192.168.5.255
3	192.168.6.0 / 24	255.255.255.0	192.168.6.1 – 192.168.6.254	192.168.6.254	192.168.6.255

Servidor DNS y WEB

Dominio: www.telnet.com

DNS → IP: 192.168.2.1

WEB → IP: 192.168.2.2

Servidor de Correo

Dominio: @telnet.com

IP: 192.168.3.1

Sucursal	Usuario	Contraseña	Dirección IP
A	JORGE	1234	192.168.1.1
A	SONIA	5678	192.168.1.2
A	ANA	9012	192.168.1.3
B	RICARDO	5367	192.168.2.3
C	LUIS	8313	192.168.3.2

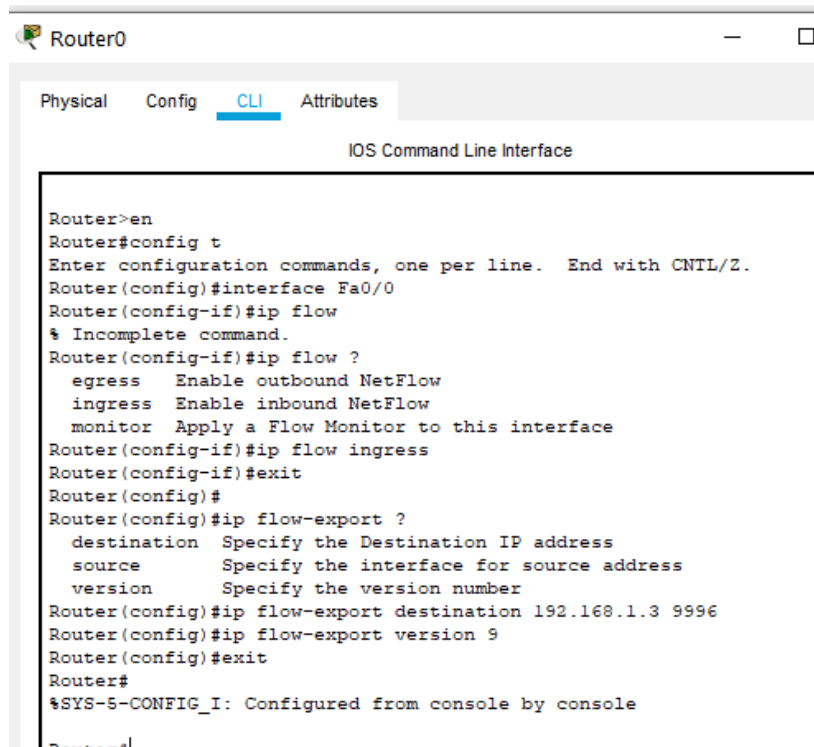
Netflow

Sirve para monitorear el tráfico en la red.

ANA será la encargada de monitorear toda la información del tráfico en la red.

Configuración del Router0

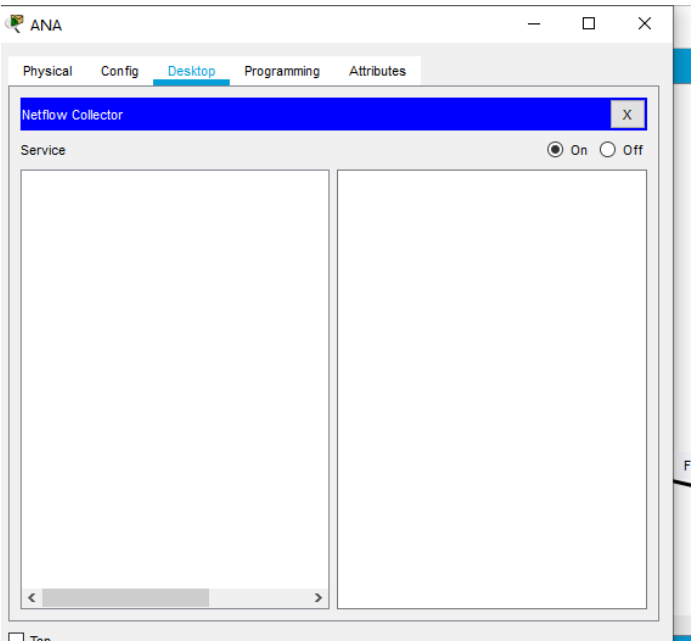
Para analizar el tráfico entrante proveniente de la SUCURSAL A.



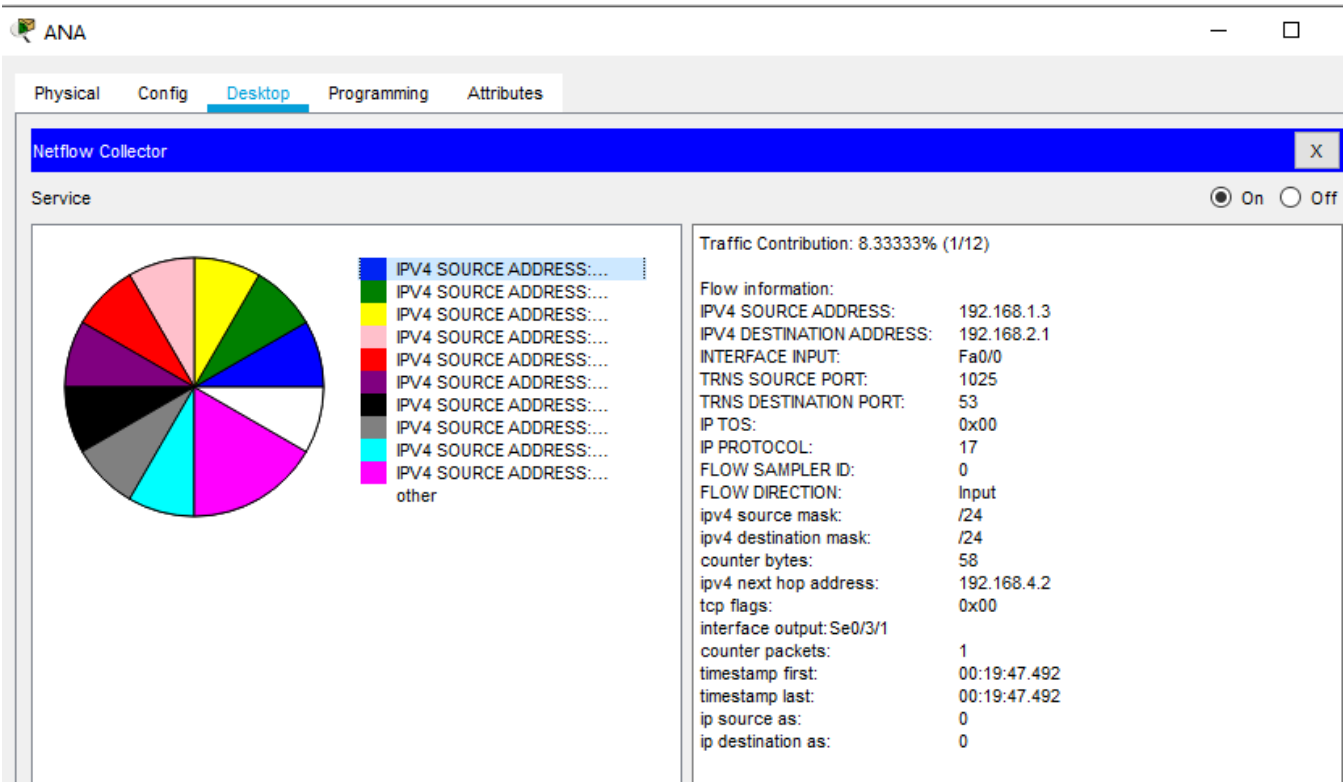
```
Router0
Physical Config CLI Attributes
IOS Command Line Interface

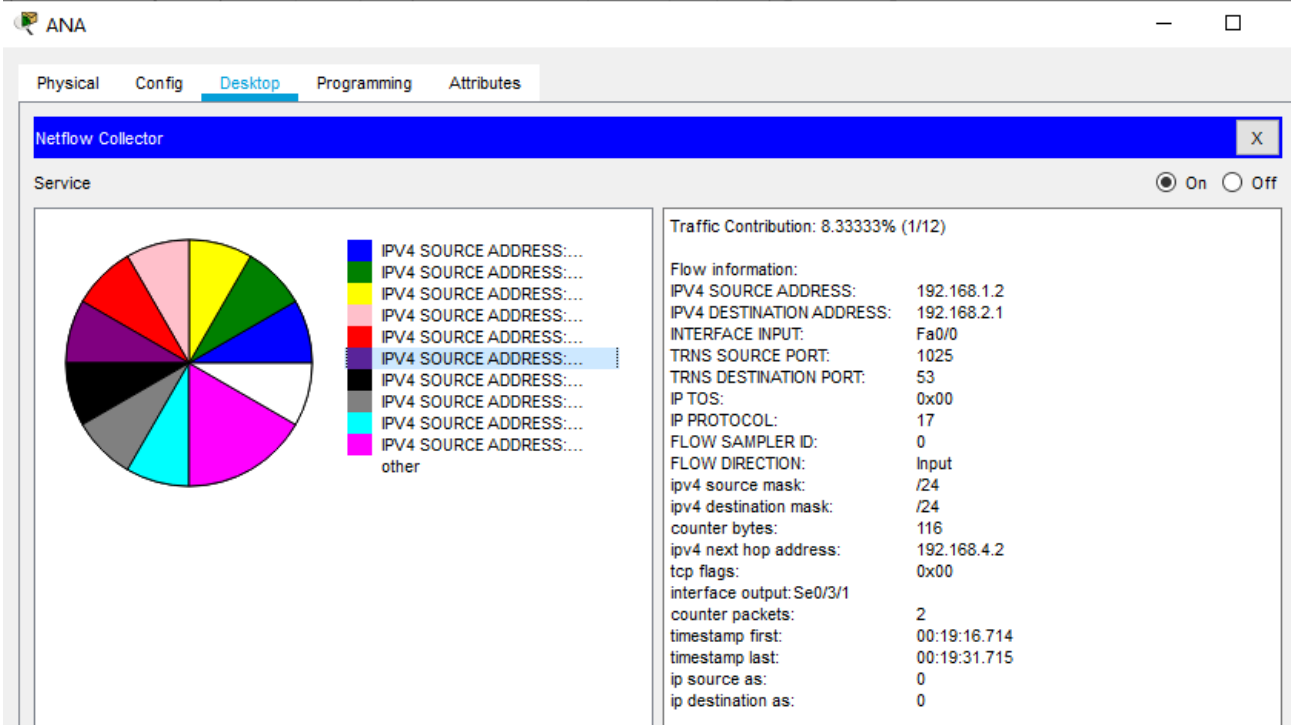
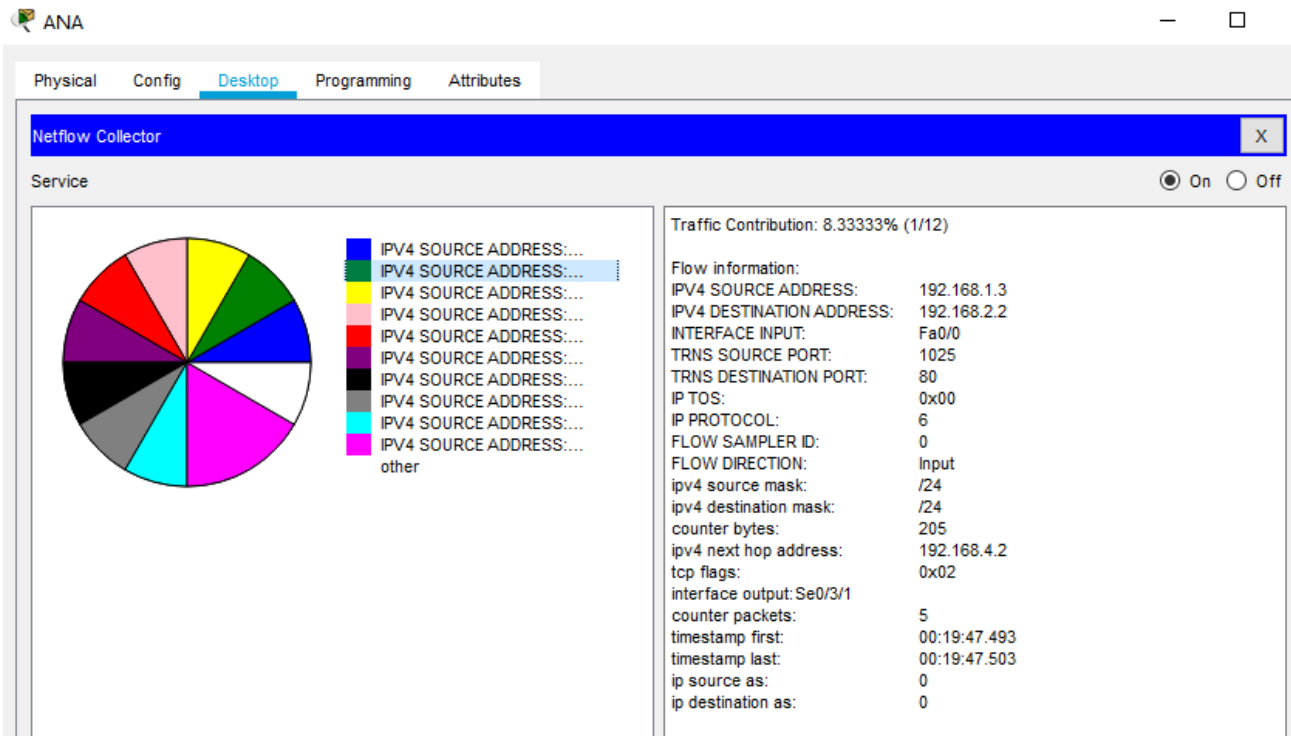
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Fa0/0
Router(config-if)#ip flow
% Incomplete command.
Router(config-if)#ip flow ?
    egress  Enable outbound NetFlow
    ingress Enable inbound NetFlow
    monitor Apply a Flow Monitor to this interface
Router(config-if)#ip flow ingress
Router(config-if)#exit
Router(config)#
Router(config)#ip flow-export ?
    destination Specify the Destination IP address
    source       Specify the interface for source address
    version      Specify the version number
Router(config)#ip flow-export destination 192.168.1.3 9996
Router(config)#ip flow-export version 9
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

Se puede escoger el trafico entrante o saliente de cierto dispositivo. También la dirección IP de la maquina que guarda los registros del trafico junto al puerto. Finalmente se especifica la versión. Inicialmente ANA no tiene información, porque aún no hay tráfico.



Luego de tener tráfico en la red, podemos ver que Ana obtiene información del monitoreo.





Luego de mandar tráfico a la red, entramos al Router y con el comando **do show ip cache flow** se ve el monitoreo de los paquetes.

```
IP Flow Switching Cache, 278544 bytes
 0 active, 4096 inactive, 7 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
ICMP           7       0.0      1     89     0.0     0.9     15.0
Total:         7       0.0      1     89     0.0     0.9     15.0

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
Router(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Si algún usuario ve la página de la empresa también guarda estas visitas. Vemos el DNS y el HTTP

```
IP Flow Switching Cache, 278544 bytes
 0 active, 4096 inactive, 15 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
ICMP           7       0.0      1     89     0.0     0.9     15.0
TCP-HTTP       4       0.0      4     41     0.0     0.0     15.0
UDP-DNS        4       0.0      1     58     0.0     3.8     15.0
Total:        15       0.0      2     61     0.0     1.4     15.0

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
Router(config)#
```

Conclusión

Monitorear la red de una empresa u organización nos permite ver el flujo de origen y destino de los paquetes, así podemos ver que dispositivos tienen mayor flujo y buscar optimizar estos. También el monitoreo nos permite conocer el día y hora en que un trabajador visita tal página, manda tal correo o incluso con quien se comunica.

Referencias

- <https://ccnadesdecero.es/netflow-funcionamiento-configuracion/> consultado el día 23 de enero de 2021