DISICO

BM Cisco 3750

Manual

Manual Administración de Ancho de Banda QoS
Switch Multilayer Cisco Catalyst 3750.

1.- Guardar Configuración en Archivo .txt

Pasos a seguir:

Core_UV_3750G#show running-config

Luego si se está utilizando Hyperterminal seleccionar todo el texto copiar y pegar en archivo .txt con los siguientes datos, ej:

Conf_3750_20100812-01.txt (Equipo_Año/Mes/Día_Nº de respaldo).

2.- Crear, eliminar, describir y asignar ip/netmask a Vlan's

Core_UV_3750G#configure terminal
Core_UV_3750G(config)#interface Vlan 200
Core_UV_3750G(config-if)#description VLAN PRUEBA 1
Core_UV_3750G(config-if)#ip address 10.50.1.155 255.255.255.0

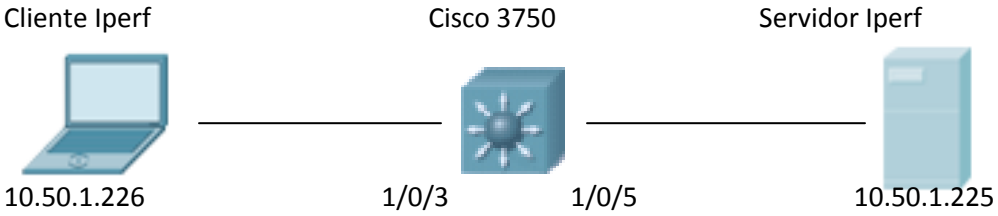
Para eliminar Vlan:

Core_UV_3750G(config)#no interface Vlan 200

3.- Habilitación de Telnet.

Core_UV_3750G#configure terminal
Core_UV_3750G(config)#line vty 0 4 (esto habilita hasta 5 sesiones telnet)
Core_UV_3750G(config-line)#password disico

4.- Esquema de Red de Prueba.



El esquema aquí presentado consta de un cliente Iperf conectado a la interfaz Giga Ethernet 1/0/3 del Switch, el que a su vez se conecta a un servidor Iperf a travez de la interfaz Giga Ethernet 1/0/5. Ambos equipos pertenecen a la Vlan 200 previamente configurada. Es necesario mencionar que en esta herramienta es el cliente quien genera el tráfico de datos en sentido Upload.

5.- Intro Bandwidth Management.

Para iniciar el proceso de administración de ancho de banda es necesario manejar varios aspectos y pasos significativos para la configuración y correcta administración. Dentro de lo que es control de ancho de banda y tráfico, es posible realizar una administración desde un modo general o bien, desde uno específico, dependiendo del análisis previo respecto del ancho de banda y tráfico con el que se trabajará y el que se desea controlar.

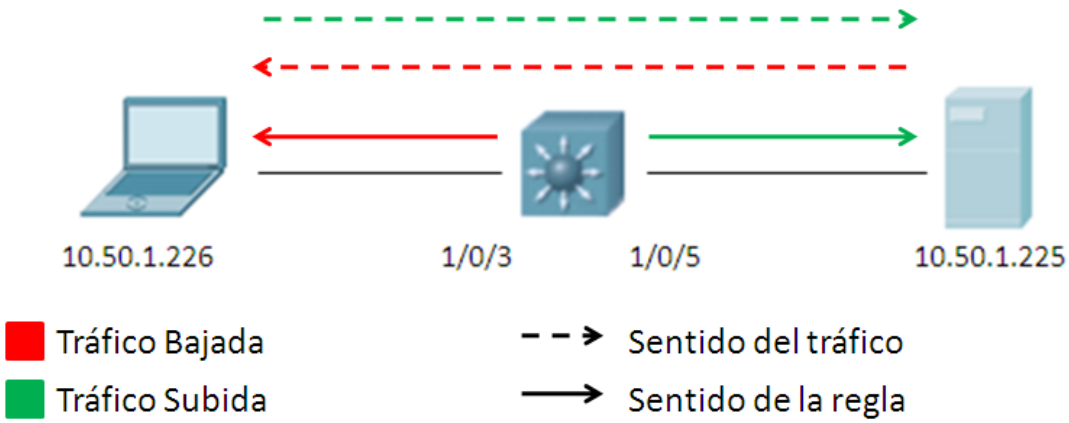
6.- Ancho de Banda en la Interfaz.

El primer comando, y el más general para la administración de ancho de banda es el siguiente:

```
Core_UV_3750G(config)#interface gigabitEthernet 1/0/x
Core_UV_3750G(config-if)#speed auto
```

Con este comando especificamos el ancho de banda de la interfaz según nuestro enlace de 10, 100 o 1000 Mbps. Gracias a esto también se puede reducir nuestro ancho de banda y limitarlo para conexiones que no necesiten un exceso de este.

7.- Control de Tráfico.



El segundo comando, es otro utilizado para limitar de forma genérica el tráfico, medido en porcentajes:

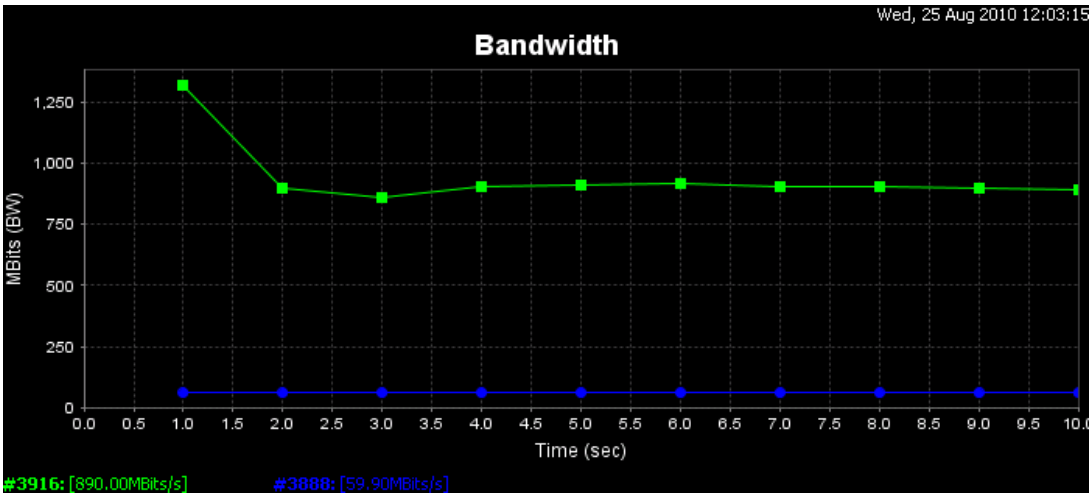
Core_UV_3750G(config)#interface gigabitEthernet 1/0/x
Core_UV_3750G(config-if)#srr-queue bandwidth limit 10

Con este comando limitamos entre un 10% a un 90% el tráfico del total del ancho de banda. En este caso, solo el 10% del ancho de banda total quedará disponible para tráfico de datos.

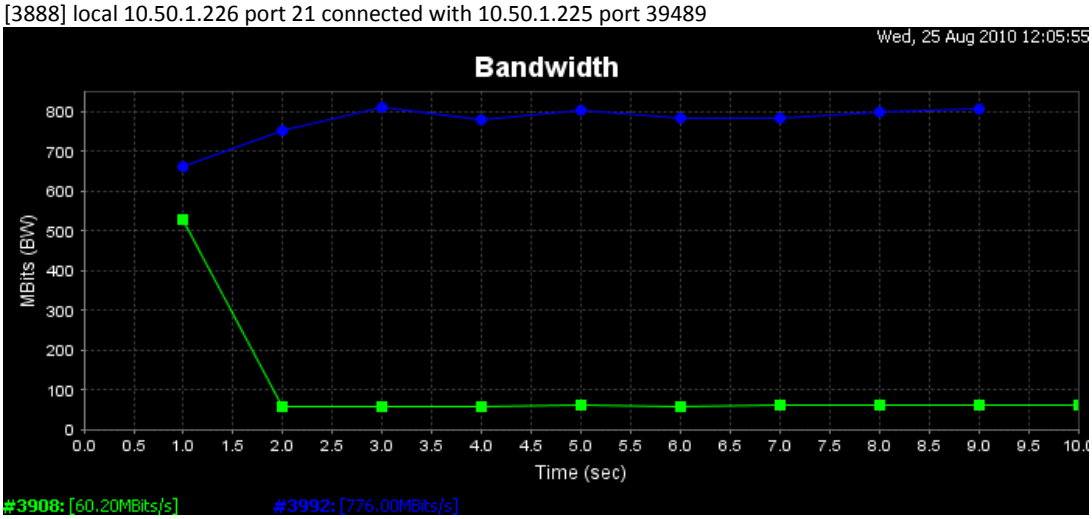
IMPORTANTE: Es de vital importancia lograr reconocer que tipo de tráfico es el que se va a controlar, si es el de bajada o el de subida, ya que dependiendo de la interfaz en que apliquemos este comando es el sentido de tráfico que limitaremos. Este comando regula el tráfico de salida de la interfaz (tráfico output).

De a cuerdo a nuestro esquema y según las pruebas aplicadas mediante la herramienta de ancho de banda Iperf es posible medir e identificar que en la interfaz GigabitEthernet 1/0/3 se regulará el tráfico de subida, mientras que en la interfaz GigabitEthernet 1/0/5 se limitará el tráfico de bajada.

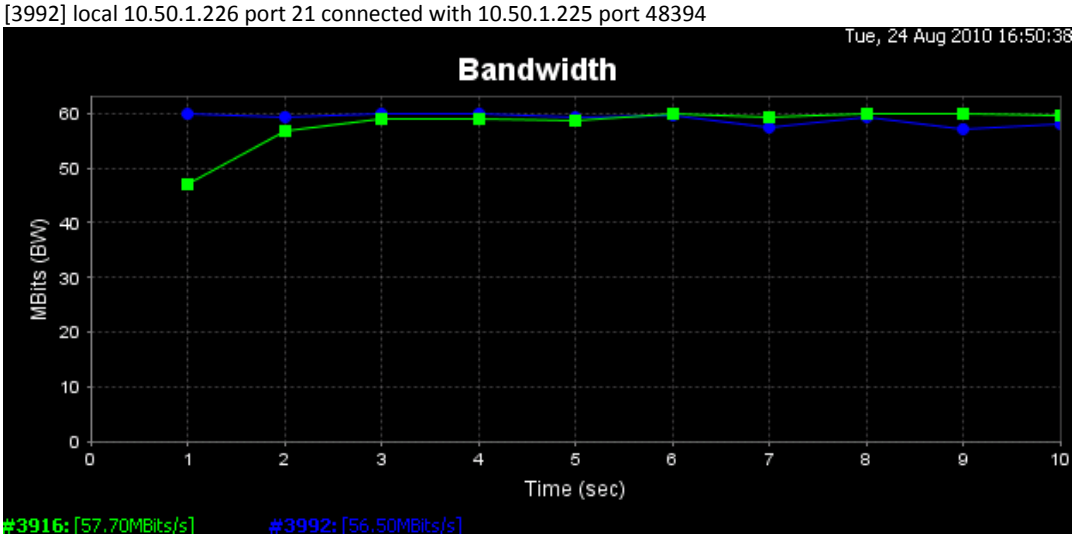
Verde: Tráfico de Subida
Azul: Tráfico de Bajada



Control Tráfico de Bajada Interfaz GigabitEthernet 1/0/3
[3916] local 10.50.1.226 port 1388 connected with 10.50.1.225 port 5001
[3888] local 10.50.1.226 port 21 connected with 10.50.1.225 port 39489



Control Tráfico de Subida Interfaz GigabitEthernet 1/0/5
[3908] local 10.50.1.226 port 1388 connected with 10.50.1.225 port 5001
[3992] local 10.50.1.226 port 21 connected with 10.50.1.225 port 48394



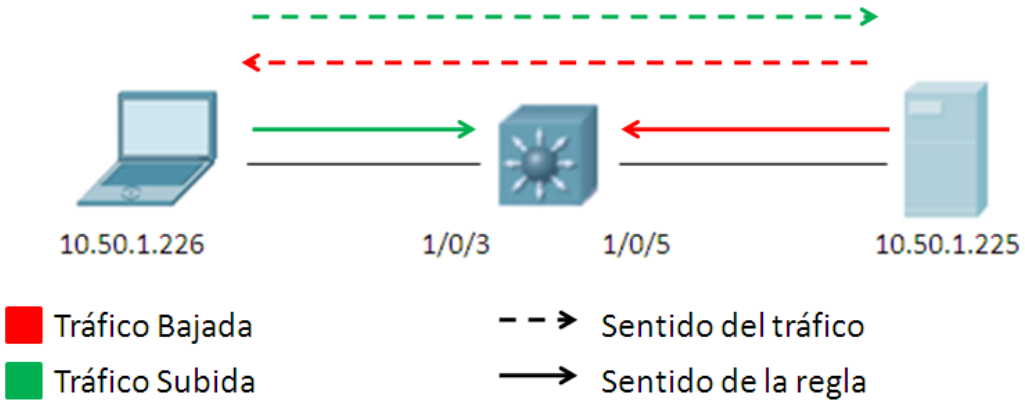
Control Tráfico de Subida/ Bajada Interfaces GigabitEthernet 1/0/5 y 1/0/3
[3916] local 10.50.1.226 port 1388 connected with 10.50.1.225 port 5001

[3992] local 10.50.1.226 port 21 connected with 10.50.1.225 port 55394

8.- Control de Tráfico por Servicio

Para llevar a cabo un control de tráfico más específico y avanzado es necesario desarrollar paso a paso los siguientes puntos:

1º Que tipo de tráfico se va a administrar y cual no.
2º Identificar el tráfico a administrar según protocolos y puertos utilizados.



8.1.- Creación de Listas de Acceso

Crear listas de acceso que identifique única o agrupadamente aquellas direcciones ip, protocolos y puertos a administrar. Ej:

Core_UV_3750G#configure terminal
Core_UV_3750G(config)#access-list 150 permit tcp **any any** eq www
Core_UV_3750G(config)#access-list 151 permit tcp **any any** eq ftp

Esta lista de acceso permite definir y especificar a que o a quienes van a ser aplicadas las políticas de MBW, ya sea a un usuario en particular, una subred, un gateway o una red completa. Esto se define en el campo ANY ANY donde el primer campo corresponde al origen y el segundo el destino, ambos con su respectivo wildcard. Es por esto que si queremos aplicar una política específica para limitar el tráfico de bajada debemos especificar el campo destino y aplicar luego la política en la interfaz WAN ej:

Core_UV_3750G(config)#access-list 150 permit tcp **any 10.50.1.0 0.0.0.255** eq www

Ahora, si queremos limitar el tráfico de subida, debemos especificar el campo origen y aplicar la política en la interfaz LAN. Ej:

Core_UV_3750G(config)#access-list 150 permit tcp **10.50.1.0 0.0.0.255 any** eq www

Ambas políticas unidas limitarán naturalmente el tráfico de bajada y subida.

8.2.- Creación de Class-map

Generar uno o varios mapeados de clases (class-map) que se integran en una sentencia, basada en un conjunto de listas de acceso.

```
Core_UV_3750G(config)#class-map match-all http(*)          (nombre de la clase "http")
Core_UV_3750G(config-cmap)#match access-group 150
Core_UV_3750G(config-cmap)#exit
Core_UV_3750G(config)#class-map match-all ftp                    (nombre de la clase "ftp")
Core_UV_3750G(config-cmap)#match access-group 151
Core_UV_3750G(config-cmap)#exit
```

(*) Se puede utilizar el comando #class-map match-any (nombre clase) cuando tenemos listas de acceso demasiado grandes y al ser aplicadas en conjunto directamente en una interfaz (en el caso del comando #class-map match-all) puede generar algún tipo de conflicto. Con la opción "any" solo se seleccionan reglas de la lista según corresponda el caso y no todas a la vez como lo hace la opción "all".

8.3.- Creación de Policy-map.

Luego se debe generar uno o varios mapeados de políticas (policy-map), asociando a estas una o varias clases de tráfico, donde se establecerán las políticas de servicio QoS para el tráfico definido en la clase previa. Con esto creamos una política que va a ser un agrupamiento de las classmaps bajo un mismo nombre, en donde vamos a definir qué se hace cuando se cumplen las condiciones que ellas establecen.

```
Core_UV_3750G(config)#policy-map t_input                (nombre de la política "t_input")
Core_UV_3750G(config-pmap)#class http
Core_UV_3750G (config-pmap-c)#police 1m 1000000 exceed-action drop
Core_UV_3750G (config-pmap-c)#set dscp cs2
Core_UV_3750G (config-pmap-c)#exit
Core_UV_3750G(config-pmap)#class ftp
Core_UV_3750G (config-pmap-c)#police 1m 1000000 exceed-action drop
Core_UV_3750G (config-pmap-c)#set dscp ef
Core_UV_3750G (config-pmap-c)#exit
```

8.4.- Asignación de política a interfaz.

Finalmente la política se debe asignar a alguna interfaz, según corresponda el caso y el sentido del tráfico que se esté controlando. Para el siguiente comando no se soportan asignaciones de políticas en sentido output.

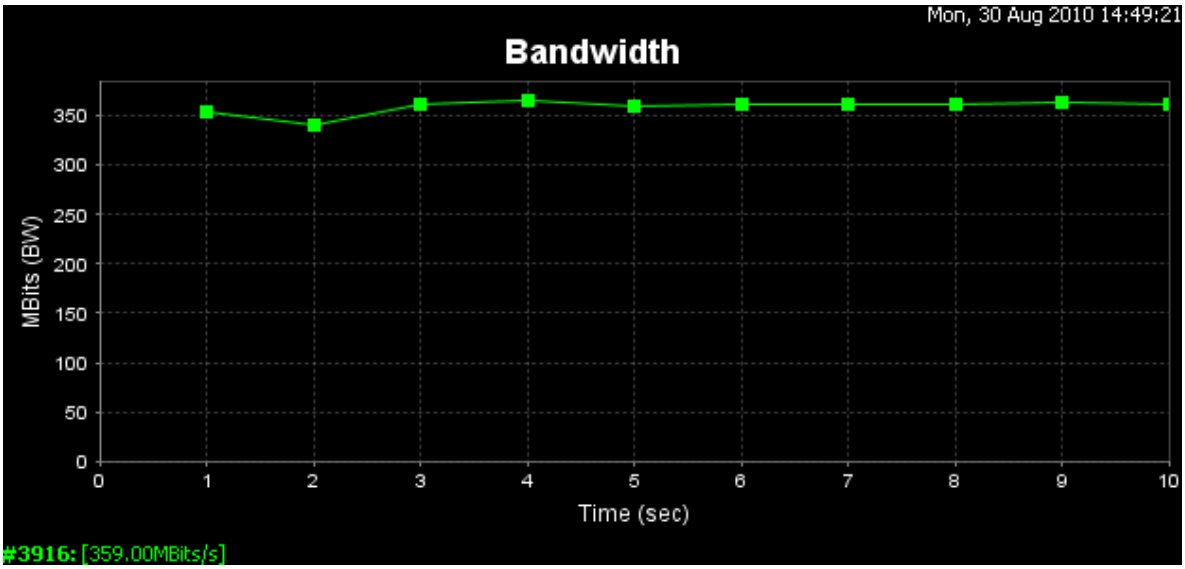
```
Core_UV_3750G(config)#interface gigabitEthernet 1/0/x
Core_UV_3750G(config-if)# service-policy input t_input
Core_UV_3750G(config)# mls qos
```

9.- Pruebas de Medición.

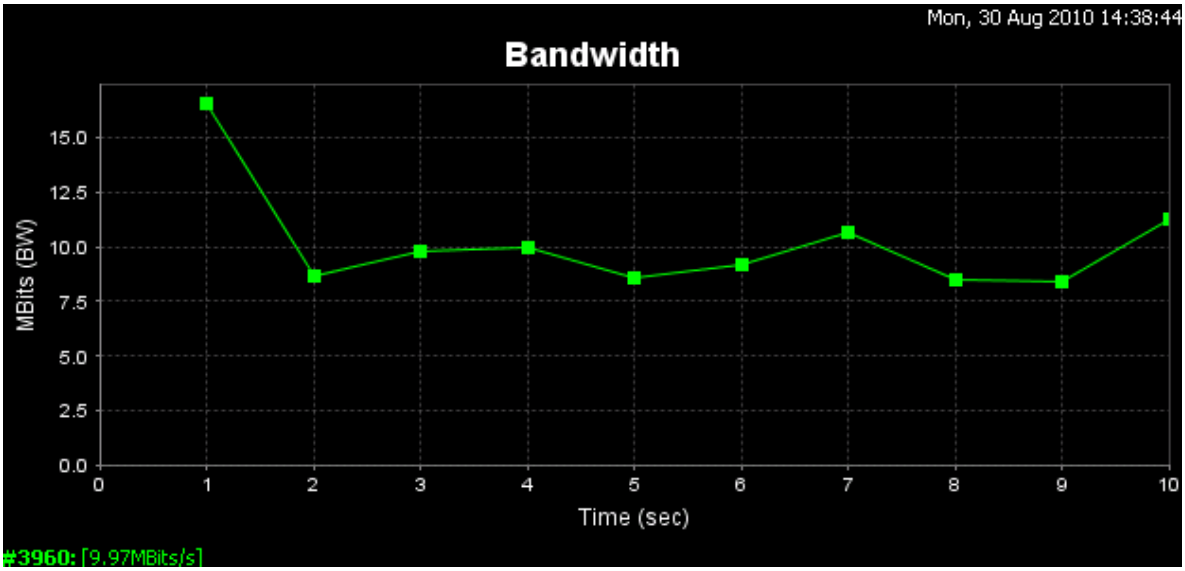
Las siguientes pruebas realizadas y sus resultados son reflejo de la aplicación de las políticas a la interfaz correspondiente. En el primer caso se valida el control de tráfico al aplicar una política de 10 Mbps específicamente con el comando.

Core_UV_3750G (config-pmap-c)#police 10m 1000000 exceed-action drop

En este primer caso la política será aplicada a la interfaz GigaEthernet 1/0/3 con lo cual se limitará el tráfico de subida.



[3960] local 10.50.1.226 port 1198 connected with 10.50.1.43 port 21
Test a Puerto 21 Sin Política

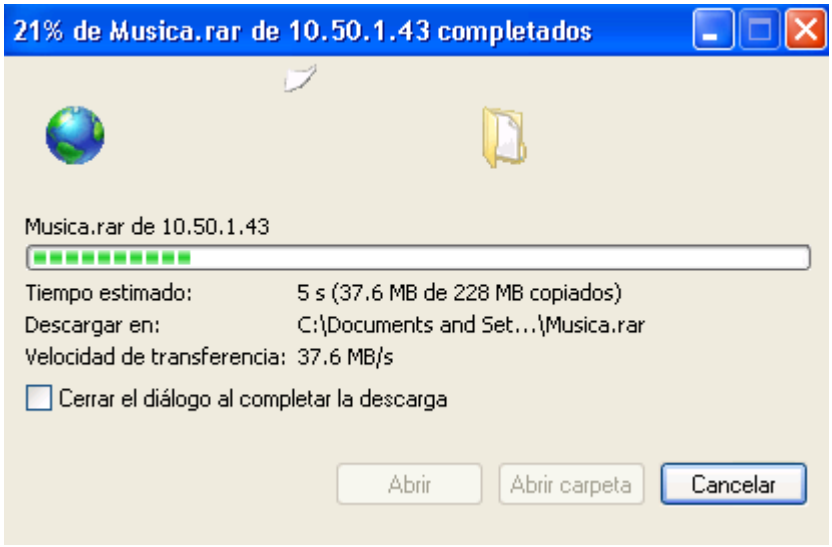


[3960] local 10.50.1.226 port 1209 connected with 10.50.1.43 port 21
Test a Puerto 21 con política de 10Mbps

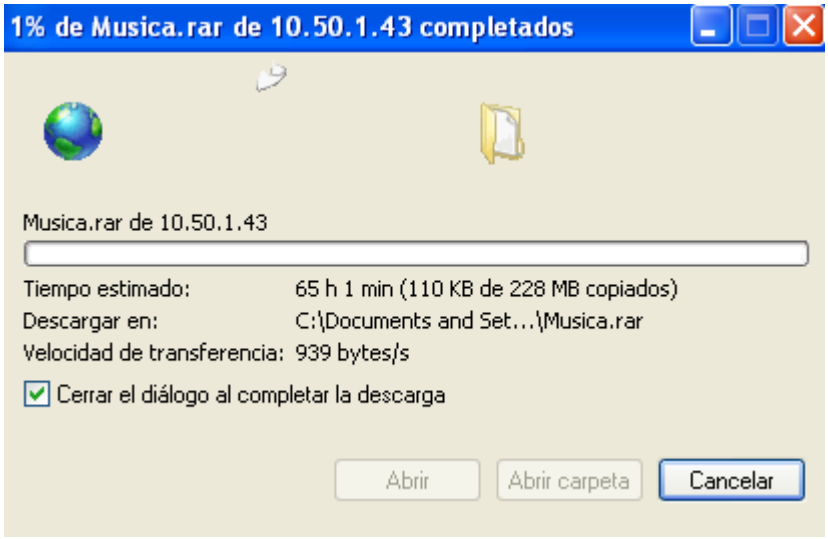
La segunda prueba, valida el control de tráfico de bajada al aplicar una política de 800 bps específicamente con el comando:

Core_UV_3750G (config-pmap-c)#police 8000 8000 exceed-action drop

En este segundo caso la política será aplicada a la interfaz GigaEthernet 1/0/5 con lo cual se limitará el tráfico de bajada. Para esto se instala un servidor de pruebas ftp y se realiza la descarga de un archivo lo suficientemente pesado para poder apreciar de mejor manera la aplicación de esta política.



Test de descarga archivo FTP sin política aplicada.



Test de descarga archivo FTP con política aplicada.

Para realizar la instalación de un servidor ftp (vsftpd) realizar instalación mediante el siguiente flash de ayuda.

http://www.lovemytool.com/blog/2008/06/ostu_iperf.html

IMPORTANTE: En estos casos es necesario tener en cuenta que la descarga o subida de archivos por ftp se realiza por sesión, es por esto que se utilizan otros puertos para la transmisión de estos y no el puerto 21 como tal. Para identificar los puertos utilizados verificar con el comando netstat –n. Luego aplicar la regla para este rango de puertos según corresponda.

9.- Potenciales Dificultades y Consideraciones.

Dificultades:

1° El Switch multicapa Catalyst 3750 Cisco debe ser visto no tan solo como un switch sino que a su vez también como un router, ya que es capaz de realizar muchas labores como tal.

2° Tener muy claros los conceptos de Vlan, Telnet, Ancho de Banda, Tráfico, política entrante, política saliente, tráfico de bajada, trafico de subida, servicios con sus respectivos puertos, funcionamiento de listas de acceso, unidades y equivalencias de medición, concepto cliente servidor, familiarización con la herramienta Iperf, entre otros.

3° Comprender el sentido del tráfico, este es quizás el punto que más cuesta comprender desde el punto de vista lógico, en base a la estructura cliente servidor y quién es el encargado de enviar los datos de un lado a otro.

4° Comprender el uso de Iperf, ya que es una herramienta que por defecto genera y envía tráfico por parte del cliente, hacia el servidor de forma Upload

5° Comprender el efecto que tiene las reglas en el tráfico, detectando el sentido de este y los efectos que esto provoca en bajada y subida.

10.- QoS Radios Online Core.

Creación de ACL Radios Online (solo incluir trasmisiones puerto 80 y 443)

(config)#access-list 2000 deny any 10.100.50.0 0.0.0.255 (aplicar esta línea solo si se quiere liberar de la política a DISICO 10.100.50.0 u otra dependencia).

```
Core_UV_3750G#conf t
(config)#access-list 2000 permit tcp host 208.80.54.28 eq www any
(config)#access-list 2000 permit tcp host 208.80.54.28 eq 443 any
(config)#access-list 2000 permit tcp host 64.86.101.202 eq www any
(config)#access-list 2000 permit tcp host 64.86.101.202 eq 443 any
(config)#access-list 2000 permit tcp host 200.73.6.195 eq www any        (radio Carolina)
(config)#access-list 2000 permit tcp host 209.88.205.240 eq www any  (radio Cooperativa)
(config)#access-list 2000 permit tcp host 200.27.214.28 eq www any    (radio Infinita)
(config)#access-list 2000 permit tcp host 66.175.96.43 eq www any     (radio Los 40)
(config)#access-list 2000 permit tcp host 190.8.65.10 eq www any      (radio Horizonte)
```

IP's: 208.80.54.28 y 64.86.101.202
(Radios: Rock & Pop, Activa, Corazón, Futuro, Pudahuel, Imagina)

Creación de Clase:

```
Core_UV_3750G(config)#class-map match-any radios
Core_UV_3750G(config-cmap)#match access-group 2000
```

Creación de Política:

```
Core_UV_3750G(config)#policy-map t_input
Core_UV_3750G(config-pmap)#class radios
Core_UV_3750G(config-pmap-c)#police 8000 8000
Core_UV_3750G(config-pmap-c)#set dscp default
```

Asignación interfaz WAN:

```
Core_UV_3750G(config)#interface gigabitEthernet 1/0/24
Core_UV_3750G(config-if)#service-policy input t_input

Core_UV_3750G(config)#interface gigabitEthernet 2/0/24
Core_UV_3750G(config-if)#service-policy input t_input
```

Las conexiones a radio online con otro tipo de puerto de transmisión será deshabilitado con la ACL encargada de bloquear todos los puertos que no se utilizan.

Habilitación servicio QoS:

```
Core_UV_3750G(config)#mls qos
```

11.- Política Emergencia Restricción total 5Mb.

Política Emergencia Restricción total 5Mb

```
(config)# access-list 2100 permit tcp any 10.100.20.0 0.0.0.255 (ATM Ambiental)
(config)# access-list 2100 permit tcp any 10.100.10.0 0.0.0.255 (Auditoria)
(config)# access-list 2100 permit tcp any 10.100.15.0 0.0.0.255 (C.Del Mar)
(config)# access-list 2100 permit tcp any 10.100.4.0 0.0.0.255  (Derecho)
(config)# access-list 2100 permit tcp any 10.100.11.0 0.0.0.255 (Enfermeria)
(config)# access-list 2100 permit tcp any 10.100.8.0 0.0.0.255    (FACEA)
(config)# access-list 2100 permit tcp any 10.100.5.0 0.0.0.255    (Ciencias)

 (config)#class-map match-any limite5
 (config-cmap)#match access-group 2100

 (config)#policy-map t_input
 (config-pmap-c)#police 5m 1000000
```

(config-pmap-c)#set dscp default

(config)#interface gigabitEthernet 1/0/24
(config-if)# service-policy input t_input

(config)#interface gigabitEthernet 2/0/24
(config-if)# service-policy input t_input

(config)#mls qos

12.- QoS Flash TV online.

Creación de ACL TV online

Core_UV_3750G#conf t
(config)#access-list 2010 permit tcp any eq 1935 any

Creación de Clase:

Core_UV_3750G(config)#class-map match-any tv
Core_UV_3750G(config-cmap)#match access-group 2010

Creación de Política:

Core_UV_3750G(config)#policy-map t_input
Core_UV_3750G(config-pmap)#class tv
Core_UV_3750G(config-pmap-c)#police 8000 8000
Core_UV_3750G(config-pmap-c)#set dscp default

12.- QoS Megaupload.

Creación de ACL Megaupload

Core_UV_3750G#conf t
(config)#access-list 2020 permit tcp any eq 800 any
(config)#access-list 2020 permit tcp any eq 1723 any
(config)#access-list 2020 permit tcp 174.140.0.0 0.0.255.255 eq www any
(config)#access-list 2020 permit tcp 95.211.0.0 0.0.255.255 eq www any
(config)#access-list 2020 permit tcp 69.5.0.0 0.0.255.255 eq www any
(config)#access-list 2020 permit tcp host 209.222.128.242 eq www any

Creación de Clase:

Core_UV_3750G(config)#class-map match-any megaupload
Core_UV_3750G(config-cmap)#match access-group 2020

Creación de Política:

```
Core_UV_3750G(config)#policy-map t_input
Core_UV_3750G(config-pmap)#class megaupload
Core_UV_3750G(config-pmap-c)#police 8000 8000
Core_UV_3750G(config-pmap-c)#set dscp default
```

13.- Política Restricción total puertos Ej: Disico.

(config)#access-list 2500 deny tcp any 10.100.50.0 0.0.0.255 eq 3389
(Sin política Remoto hacia 10.100.50.0)

(config)#access-list 2500 deny tcp any eq www 10.100.50.0 0.0.0.255
(Sin política puerto 80 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 443 10.100.50.0 0.0.0.255
(Sin política https puerto 443 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 22 10.100.50.0 0.0.0.255
(Sin política ssh puerto 22 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq domain 10.100.50.0 0.0.0.255
(Sin política puerto 53 que va a 10.100.50.0)

(config)#access-list 2500 deny udp any eq domain 10.100.50.0 0.0.0.255
(Sin política puerto 53 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq smtp 10.100.50.0 0.0.0.255
(Sin política puerto 25 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq pop3 10.100.50.0 0.0.0.255
(Sin política puerto 110 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq telnet 10.100.50.0 0.0.0.255
(Sin política puerto 23 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq ftp 10.100.50.0 0.0.0.255
(Sin política puerto 21 que va a 10.100.50.0)

(config)#access-list 2500 deny udp any eq syslog 10.100.50.0 0.0.0.255
(Sin política puerto 514 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 161 10.100.50.0 0.0.0.255
(Sin política snmp puerto 161 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 445 10.100.50.0 0.0.0.255
(Sin política carpetas puerto 445 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 587 10.100.50.0 0.0.0.255

(Sin política correo puerto 587 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 873 10.100.50.0 0.0.0.255
(Sin política rsync puerto 873 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any range 993 995 10.100.50.0 0.0.0.255
(Sin política correo puertos 993-995 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any range 135 139 10.100.50.0 0.0.0.255
(Sin política windows puertos 135-139 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 2725 10.100.50.0 0.0.0.255
(Sin política BD SQL puerto 2725 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 3690 10.100.50.0 0.0.0.255
(Sin política subversion puerto 3690 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 4848 10.100.50.0 0.0.0.255
(Sin política java puerto 4848 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 10000 10.100.50.0 0.0.0.255
(Sin política webmin puerto 10000 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 3700 10.100.50.0 0.0.0.255
(Sin política puerto 3700 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 3820 10.100.50.0 0.0.0.255
(Sin política puerto 3820 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 3920 10.100.50.0 0.0.0.255
(Sin política puerto 3920 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 1434 10.100.50.0 0.0.0.255
(Sin política puerto 1434 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 1433 10.100.50.0 0.0.0.255
(Sin política puerto 1433 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 7676 10.100.50.0 0.0.0.255
(Sin política puerto 7676 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 8180 10.100.50.0 0.0.0.255
(Sin política puerto 8180 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 8181 10.100.50.0 0.0.0.255
(Sin política puerto 8181 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 8686 10.100.50.0 0.0.0.255

(Sin política puerto 8686 que va a 10.100.50.0)

(config)#access-list 2500 deny tcp any eq 8080 10.100.50.0 0.0.0.255
(Sin política puerto 8080 que va a 10.100.50.0)

(config)#access-list 2500 permit tcp any 10.100.50.0 0.0.0.255
(Política a todo lo que va a 10.100.50.0)

IMPORTANTE: Si se desean liberar más puertos de la política seguir patrón de reglas las cuales deben ser agregadas antes de la última regla que se encarga de aplicar la política a todos el resto de puertos que no estén declarados previamente.

(config)#class-map match-any disico
(config-cmap)#match access-group 2500

(config)#policy-map t_input
(config-pmap-c)#police 8000 8000
(config-pmap-c)#set dscp default

(config)#interface gigabitEthernet 1/0/24
(config-if)# service-policy input t_input

(config)#interface gigabitEthernet 2/0/24
(config-if)# service-policy input t_input

(config)#mls qos

Puertos P2P

Puertos Premium Megaupload: 800, 1723

(config-pmap-c)#set ip dscp ?
<0-63> Differentiated services codepoint value
af11 Match packets with AF11 dscp (001010)
af12 Match packets with AF12 dscp (001100)
af13 Match packets with AF13 dscp (001110)
af21 Match packets with AF21 dscp (010010)
af22 Match packets with AF22 dscp (010100)
af23 Match packets with AF23 dscp (010110)
af31 Match packets with AF31 dscp (011010)
af32 Match packets with AF32 dscp (011100)
af33 Match packets with AF33 dscp (011110)
af41 Match packets with AF41 dscp (100010)
af42 Match packets with AF42 dscp (100100)
af43 Match packets with AF43 dscp (100110)
cs1 Match packets with CS1(precedence 1) dscp (001000)
cs2 Match packets with CS2(precedence 2) dscp (010000)
cs3 Match packets with CS3(precedence 3) dscp (011000)
cs4 Match packets with CS4(precedence 4) dscp (100000)
cs5 Match packets with CS5(precedence 5) dscp (101000)
cs6 Match packets with CS6(precedence 6) dscp (110000)
cs7 Match packets with CS7(precedence 7) dscp (111000)
default Match packets with default dscp (000000)
ef Match packets with EF dscp (101110)

111110	Reservado (routing y control)
111100	Reservado (routing y control)
111010	Reservado (routing y control)
111000	Reservado (routing y control)
110110	Reservado (routing y control)
110100	Reservado (routing y control)
110010	Reservado (routing y control)
110000	Reservado (routing y control)
101110	Expedited (Premium)
101100	Configurable por el usuario
101010	Configurable por el usuario
101000	Configurable por el usuario
100110	Assured Clase 4 Preced. Alta
100100	Assured Clase 4 Preced. Media
100010	Assured Clase 4 Preced. Baja
100000	Configurable por el usuario

011110	Assured Clase 3 Preced. Alta
011100	Assured Clase 3 Preced. Media
011010	Assured Clase 3 Preced. Baja
011000	Configurable por el usuario
010110	Assured Clase 2 Preced. Alta
010100	Assured Clase 2 Preced. Media
010010	Assured Clase 2 Preced. Baja
010000	Configurable por el usuario
001110	Assured Clase 1 Preced. Alta
001100	Assured Clase 1 Preced. Media
001010	Assured Clase 1 Preced. Baja
001000	Configurable por el usuario
000110	Configurable por el usuario
000100	Configurable por el usuario
000010	Configurable por el usuario
000000	Best Effort (default)

DSCP (Decimal)	DSCP	CoS
0	Default	0
8	CS1	1
10	AF11	1
12	AF12	1
14	AF13	1
16	CS2	2
18	AF21	2
20	AF22	2
22	AF23	2
24	CS3	3
26	AF31	3
28	AF32	3
30	AF33	3
32	CS4	4
34	AF41	4
36	AF42	4
38	AF43	4
40	CS5	5
42		5
44		5
46	EF	5
48	CS6	6
56	CS7	7

ASA(config)# snmp-server enable
ASA(config)# snmp-server host dmz1 10.50.1.72 community *monitor*
ASA(config)# snmp-server community *monitor*
ASA(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart

1. Entre al modo EXEC privilegiado escribiendo **enable**.
Si se le pide una contraseña, introduzca **class** (si no funciona, consulte al instructor).
Core_UV_3750G>**enable**
2. Elimine el archivo de información de la base de datos de la VLAN.
Core_UV_3750G#**delete flash:vlan.dat**

Delete filename [vlan.dat]?**[Enter]**
Delete flash:vlan.dat? [confirm]**[Intro]**
Si no hay ningún archivo VLAN, aparece el siguiente mensaje:
%Error deleting flash:vlan.dat (No such file or directory)
3. Elimine el archivo de configuración inicial de la NVRAM del switch.
Switch#**erase startup-config**
Como respuesta, aparecerá la siguiente petición de entrada:
Erasing the nvram filesystem will remove all files! Continue? [confirm]
Presione **Intro** para confirmar.
La respuesta deberá ser:
Erase of nvram: complete
Core_UV_3750G#**reload**
Como respuesta, aparecerá la siguiente petición de entrada:
System configuration has been modified. Save? [yes/no]:
b. Escriba **n** y luego presione **Intro**.
Como respuesta, aparecerá la siguiente petición de entrada:
Proceed with reload? [confirm]**[Intro]**
La primera línea de la respuesta será:
Reload requested by console.
La siguiente petición de entrada aparecerá después de que el switch se recargue:
Would you like to enter the initial configuration dialog? [yes/no]:
c. Escriba **n** y luego presione **Intro**.
Como respuesta, aparecerá la siguiente petición de entrada:
Press RETURN to get started! **[Intro]**