UNIVERSIDAD DE CASTILLA - LA MANCHA

Planificación e
Integración de
Sistemas y
Servicios

ESCUELA SUPERIOR DE INFORMÁTICA

Práctica 4
Gestión de prioridad de tráfico en IP

Autores:
José Antonio SANTACRUZ GALLEGO
Silvestre SÁNCHEZ-BERMEJO SÁNCHEZ

Profesor:
Jesús BLANCO

23 de diciembre de 2021

Índice

Apartado 1: Entorno de trabajo **3**

Apartado 2: Marcado de paquetes **3**

Apartado 3: Análisis del rendimiento **4**

Enlace al repositorio **4**

Bibliografía **4**

Apartado 1: Entorno de trabajo

Para el entorno de trabajo vamos a usar dos maquinas virtuales, una que tendrá el rol de cliente, y otra de servidor. Siendo el PC anfitrión el que haga de router.

Creamos dos subredes distintas, una será la del servidor, y otra la del cliente. Para configurar las tablas de enrutamiento utilizaremos ifconfig

Asignaremos como subred para el cliente la siguiente: 10.10.1.0/24
Creamos la interfaz de red del cliente, el cual va a tener como ip 10.10.1.2, y a continuación creamos una ruta para la conexión con el router

```
Sudo ifconfig eth0:Cliente 10.10.1.2 netmask 255.255.255.0 broadcast 10.10.1.255
```

```
Sudo route add -net 10.10.1.0/24 gw 10.10.1.1 dev eth0:Cliente
```

A continuación, activaremos el ip_forwarding de la siguiente manera:
Editaremos el archivo */etc/sysctl.conf, y modificamos la línea:*

```
net.ipv4.ip_forward = 1
```

Con un valor de 0, el ip forwarding estaría desactivado. Para activar el cambio, ejecutaremos

```
sysctl -p
```

Apartado 2: Marcado de paquetes

Marcamos el tráfico RTP y SIP en la interfaz del cliente. Para esto utilizaremos la tabla mangle. El trafico RTP lo marcamos con Expedited Forwarding (ef) , el cual indica la máxima prioridad, ya que no nos interesa perder estos paquetes, ya que perderíamos datos de la comunicación de voz. Por otro lado, el trafico SIP lo marcamos con Assured Forwarding 11 (af11), ya que este tráfico se utiliza para la señalización durante la llamada y para establecer las comunicaciones; por lo que no es necesario marcarlo con una máxima prioridad

Tráfico SIP

```
Sudo iptables -t mangle -A OUTPUT -p udp -m udp –dport 5060 -j DSCP --set-dscp-ckass af11
Sudo iptables -t mangle -A OUTPUT -p tcp -m tcp –dport 5060 -j DSCP --set-dscp-ckass af11
```

Tráfico RTP

```
Sudo iptables -t mangle -A OUTPUT -p udp -m udp –dport 6970:6999 -j DSCP     --set-dscp-
class ef
Sudo iptables -t mangle -A OUTPUT -p tcp -m tcp –dport 6970:6999 -j DSCP     --set-dscp-
class ef
```

Apartado 3: Análisis del rendimiento

Para crear la saturación de la conexión usando la herramienta **iperf** usaremos los comandos

```
Sudo iperf -c <ip_servidor>
```

para el lado del cliente, y

```
Sudo iperf -s
```

para el lado del servidor

Enlace al repositorio

Repositorio del grupo 7:
https://github.com/JASantacruz/PISS-21-G7

Bibliografía

https://www.acens.com/wp-content/images/2014/07/wp-acens-iptables.pdf
https://www.acens.com/wp-content/images/2014/07/wp-acens-iptables.pdf
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_0/qos/configuration/guide/nexus1000v_qos/qos_6dscp_val.pdf
http://sipp.sourceforge.net/doc/reference.html