# GRADO EN INFORMÁTICA
# Planificación e Integración de Sistemas y Servicios
# (2020/2021)

## – Práctica 4 –
## Gestión de prioridad de tráfico en IP

Mediante el uso de iptables para GNU/Linux construir un sistema que clasifique el tráfico RTP y SIP, cada uno de ellos con un tipo para mejorar la calidad de servicio apreciada.

Apartado 1: ENTORNO DE TRABAJO.

Describir detalladamente el entorno de trabajo utilizado para realizar la práctica.

- Trabajar en tres máquinas (se recomiendan virtuales): router, servidor y cliente.
- Configurar dos interfaces de red en el pc que actúe como router, una interfaz para el cliente y otra para el servidor en subredes distintas.
- Configurar tablas de enrutamiento y habilitar ip_forwarding en el router.

Apartado 2: MARCADO DE PAQUETES.

Describir los pasos necesarios para marcar los paquetes del modo deseado:

- Marcar tráfico en RTP y SIP según corresponda a valores correctos de DSCP mediante la tabla *mangle* de iptables.
    - Justificar los valores DSCP utilizados.
- Usando dscp de iptables tratar los flujos de tráfico dando prioridad a RTP y asegurándose que ningún paquete SIP es eliminado.
- Documentar el uso de los parámetros de iptables utilizados.

Apartado 3: ANÁLISIS DEL RENDIMIENTO.

Realizar y describir las siguientes pruebas con y sin marcado de paquetes. Documentar las conclusiones obtenidas.

- Saturar la conexión utilizando iperf
- Generar tráfico SIP (elegir 1 forma de hacerlo):
    - Realizar varias llamadas utilizando Asterisk.
    - Realizar varias llamadas con SIPp .
- Usar iperf para analizar la saturación de la interfaz utilizada, analizar resultados de la calidad de servicio en la comunicación de VoIP configurada (para SIP y para RTP).
    - Capturar flujo con Wireshark para mostrar paquetes marcados.

**SOBRE LA DOCUMENTACIÓN A ENTREGAR (IMPRESCINDIBLE):**

Citar documentación utilizada (manuales, páginas de Internet, guías de referencia, prácticas de años anteriores, etc).

***ENTREGA***

La entrega se realizará mediante la plataforma moodle en formato pdf.

**ANEXO 1:** Ejemplos de marcaje de paquetes bajo GNU/Linux

Máquina origen (configuración del marcado de paquetes salientes con la tabla mangle):

```
iptables -t mangle -I OUTPUT -j DSCP --setdscp 14
```

En el destino (configuración de la gestión de descartes con el módulo limit):

```
iptables -t filter -A INPUT -m dscp --dscp 14 -m limit --limit 5/s -j --limit-burst 5 ACCEPT

iptables -t filter -A INPUT -m dscp --dscp 14 -j DROP
```

**ANEXO 2:** Ejemplo de 7 llamadas cada 2 segundos con SIPp en una misma máquina

```
servidor:    sipp -sn uas

cliente:     sipp -sn uac -r 7 -rp 2000 127.0.0.1
```

**DOCUMENTACIÓN:**

- http://ipset.netfilter.org/iptables-extensions.man.html
- 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