

Control de ancho de Banda y QoS con Linux Kernel 2.6

Jorge Luis Sarmiento M.



#include <disclaimer.h>



“Para una correcta administracion de nuestra red, debemos administrar adecuadamente nuestro mas apreciado recurso: la capacidad de transmision de data”



*“Yo no tengo internet asi que no
necesito QoS”*



iptables -t mangle

- Que es un marcado de paquetes?
- Para que nos sirve?
- `# iptables -t mangle -A FORWARD -s 192.168.1.20 -p tcp -dport 1214 -j MARK - -set-mark 4`



La magia de iproute2

- Manejo de múltiples tablas de ruteo / default gateways.
- Soporte de políticas de ruteo de acuerdo a marcas en los paquetes.



El comando ip

- # ip link show
- # ip address show
- # ip route show
 - # ip route add default via <gw> table <table_name>
 - # ip route list table <tabla>
- # ip neigh show
 - # ip neigh delete <ip address> dev eth0
- # ip rule list
 - # ip rule add fwmark <mark_number> <table_name>



Ejemplo practico: agregar una salida a internet via speedy

```
# cat /etc/iproute2/route_tables
```

- 255 local
- 254 main
- 253 default
- 201 speedy

```
# ip route add default via 192.168.1.1 table speedy
```

```
# ip rule add fwmark 1 table speedy
```

```
# iptables -t mangle -A OUTPUT -p tcp - -dport 1214 -j MARK -  
-set mark 1
```



Y si quiero balancear mi navegacion entre ambos proveedores?

- # ip route add default scope global nexthop via <gw_lan> dev <lan_eth> weight 1 nexthop via <gw_speedy> dev <speedy_eth> weight 1



El comando tc

- Permite realizar “traffic shaping” de nuestra conexion.
- El algoritmo que define como nuestra va a ser manejada nuestra cola es el “Queueing Discipline” (qdisc).
- Cuando una disciplina de encolamiento puede ser subdividida, las subdivisiones se llaman “classes” y el encolamiento es considerado “Classful qdisc”.
- Las “Classful qdisc” tienen clasificadores (classifiers) que define por que clase va a salir un paquete, estos clasificadores puede ser definidor por filtros (filters).



HTB Queueing Discipline

- “Hierarchical Token Bucket”
- Es mas simple, eficiente y exacto que el famoso cbq.
- Permite asignar maximos y minimos a una clase.



- `# tc qdisc add dev eth0 root handle 1: htb default 20`
- `# tc class add dev eth0 parent 1: classid 1:1 htb rate 10 mbit burst 15k`
- `# tc class add dev eth0 parent 1:1 classid 1:10 htb rate 5 mbit burst 15k`
- `# tc class add dev eth0 parent 1:1 classid 1:20 htb rate 3 mbit ceil 5 mbit burst 15k`
- `# tc class add dev eth0 parent 1:1 classid 1:30 htb rate 2 mbit ceil 5 mbit burst 15k`
- `# tc filter add dev eth0 protocol ip handle 1 fw classid 1:10`
- `# tc filter add dev eth0 protocol ip handle 2 fw classid 1:20`
- `# tc filter add dev eth0 protocol ip handle 3 fw classid 1:30`



Aparte de mejorar mi acceso a internet, para que mas puede servir?

- Evitar saturacion en la LAN en momentos de transmision de grandes cantidades de data.
- Evitar un exceso de carga en el HD de un servidor de archivos.
- Creacion de boxes transparentes de control de trafico utilizando bridge + ebtables + tc
- Reducir riesgo de dos attacks controlando ese bw.



Links de interes

<http://lartc.org/>

Linux Advanced Routing and Traffic Control How-to

<http://luxik.cdi.cz/~devik/qos/htb/>

HTB Homepage



PREGUNTAS



- Gracias por la atencion brindada



"Debian rules, but Gentoo is teh_way"