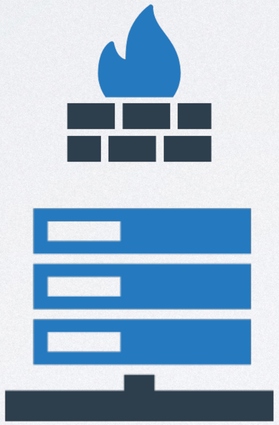
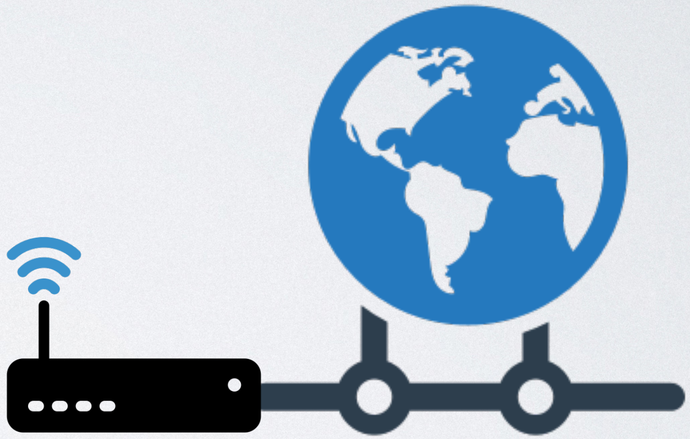
IPTABLES

- netfilter
- reglas
- cadenas
- tablas





iptables [-t tabla] -A/I cadena [opciones] -j acción

```
iptables -t filter -A INPUT -p icmp -j ACCEPT

iptables -A INPUT  -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

IPTABLES - OPCIONES

- **-s** : ip/red origen
- **-d** : ip/red destino
- **-i** : interfaz de entrada
- **-o** : interfaz de salida
- **-m** : carga un módulo
- **-p** : protocolo
  - TCP / UDP
  - **--dport** : puerto de destino
  - **--sport** : puerto de origen
  - **--tcp-flags** : especifica qué flags deben tener los paquetes

(ACK, FIN, PSH, RST, SYN, URG, ALL, NONE)

IPTABLES - MÓDULOS

- **limit**
  - **--limit** : Establece el número de coincidencias para un intervalo de tiempo particular
  - **--limit-burst** : Establece un límite en la cantidad de paquetes que pueden coincidir con una regla a la vez.

Ejemplos:

```
iptables -A INPUT -p tcp -m limit --limit 60/s --limit-burst 20 -j ACCEPT
```

Otro módulos complementarios: **hashlimit, connlimit**

Enlace para ampliar info:
https://www.linuxparty.es/57-seguridad/10423-limitacion-de-velocidad-por-ip-con-iptables.html

- **state / conntrack**
  - **--state** : Filtra por los estados de conexión del paquete:

NEW,ESTABLISHED, RELATED, INVALID

Se pueden usar varios estados separados por comas

Ejemplos:

```
iptables -A INPUT -i enp0s3 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
```

IPTABLES - MÓDULOS

Enlaces para ampliar información:

- https://www.cyberithub.com/iptables-command-in-linux/
- http://redesdecomputadores.umh.es/iptables.htm
- https://wiki.archlinux.org/title/Iptables_(Español)
- https://elbauldelprogramador.com/20-ejemplos-de-iptables-para-sysadmins/

MANGLE

Esta tabla se usa para modificar paquetes. Por ejemplo:

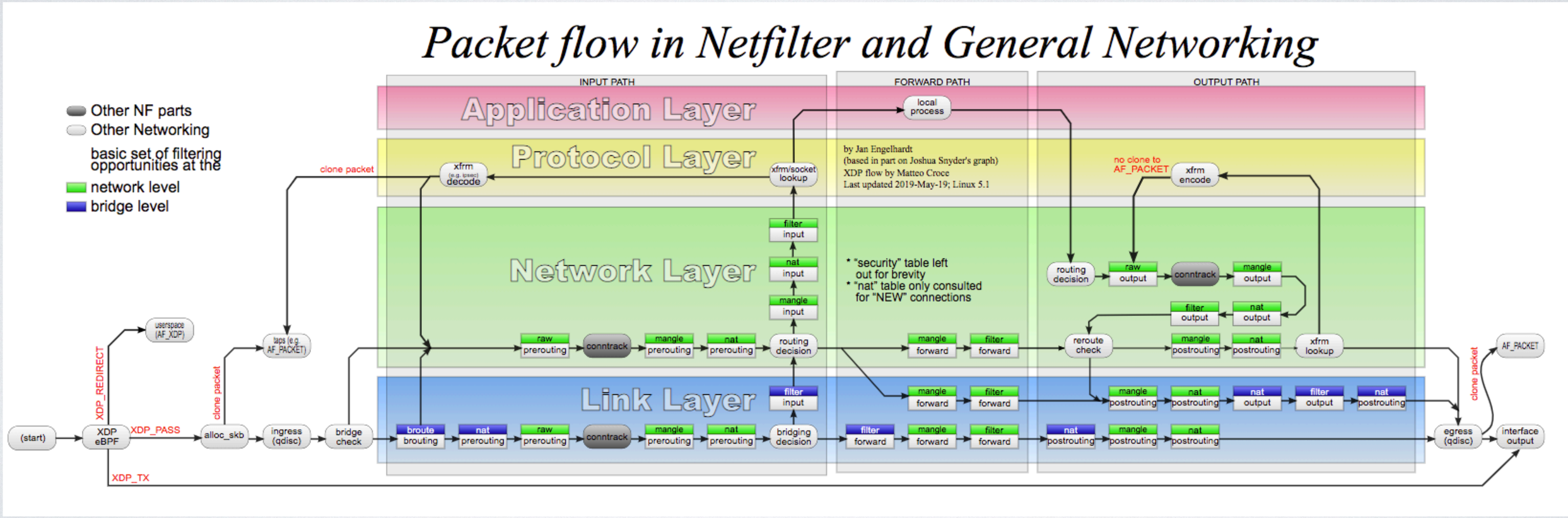
El **TOS** (Type Of Service). Otras aplicaciones lo pueden usar para condicionar su uso en la red, pero en internet puede ocurrir que esta información sea ignorada.

El **TTL** (Time To Live). Es el número de saltos de red válidos que puede soportar el paquete..

El **Mark**. Se pueden marcar paquetes específicos y después usar esta marca para enrutar, limitar el ancho de banca, balancear carga, etc.

RAW

Se usa para indicar paquetes que no tienes que ser rastreados por conntrack



https://commons.wikimedia.org/wiki/File:Netfilter-packet-flow.svg