TABLAS

No hay ninguna predefinida. Al iniciar se cargan las del fichero /etc/nftables.conf

```
nft add table <familia> <tabla>
nft list tables
nft delete table <familia> <tabla>
nft flush table <familia> <tabla>
```

Familias:

- ip = ipv4
- ip6 = ipv6
- inet = ipv4 e ipv6
- arp = ARP (antiguo arptables)
- bridge = trafico interfaces bridge (ebtables)
- netdev = tráfico que acaba de entrar (hook ingress)

CADENAS

No hay ninguna predefinida. Al iniciar se cargan las del fichero /etc/nftables.conf

Hay dos tipos:

- Base: Define un tipo y un punto de entrada "hook" para los paquetes.
- Normal: Sirve para enlazarse en otra regla, para mejorar la administración

```
nft add chain <familia> <tabla> <cadena>
nft add chain <familia> <tabla> <cadena> { type tipo hook nombre_hook priority prioridad \; }
nft flush chain <familia> <tabla> <cadena>
nft delete chain <familia> <tabla> <cadena>
```

Tipo: puede ser filter, route, o nat.

Chain type	Hooks						
	ingress	prerouting	forward	input	output	postrouting	egress
inet family							
filter	0.9.7 / 5.10	Yes	Yes	Yes	Yes	Yes	No
nat	No	Yes	No	Yes	Yes	Yes	No
route	No	No	No	No	Yes	No	No
ip6 family							
filter	No	Yes	Yes	Yes	Yes	Yes	No
nat	No	Yes	No	Yes	Yes	Yes	No
route	No	No	No	No	Yes	No	No
ip family							
filter	No	Yes	Yes	Yes	Yes	Yes	No
nat	No	Yes	No	Yes	Yes	Yes	No
route	No	No	No	No	Yes	No	No
arp family							
filter	No	No	No	Yes	Yes	No	No
nat	No	No	No	No	No	No	No
route	No	No	No	No	No	No	No
bridge family							
filter	No	Yes	Yes	Yes	Yes	Yes	No
nat	No	No	No	No	No	No	No
route	No	No	No	No	No	No	No
netdev family							
filter	0.6 / 4.2	No	No	No	No	No	- / 5.7
nat	No	No	No	No	No	No	No
route	No	No	No	No	No	No	No

https://wiki.nftables.org/wiki-nftables/index.php/Netfilter_hooks

REGLAS

La utilidad iptables-translate traduce las reglas de iptables al formato nftables.

```
nft add|insert rule [<famiy>] <table> <chain> [handle <value>] [<selectores>] [<acciones>] [comment "Comentario"]
```

(El handle es opcional y sirve para hacer referencia a esa regla)

Algunos sectores

meta:
- oif / oifname <interfaz de salida>
- iif / iifname <interfaz de entrada>

icmp:
- type <tipo icmp>

ip:
- protocol <protocolo>
- daddr <dirección de destino>
- saddr <dirección de origen>

tcp:
- dport <puerto de destino>
- sport <puerto de origen>

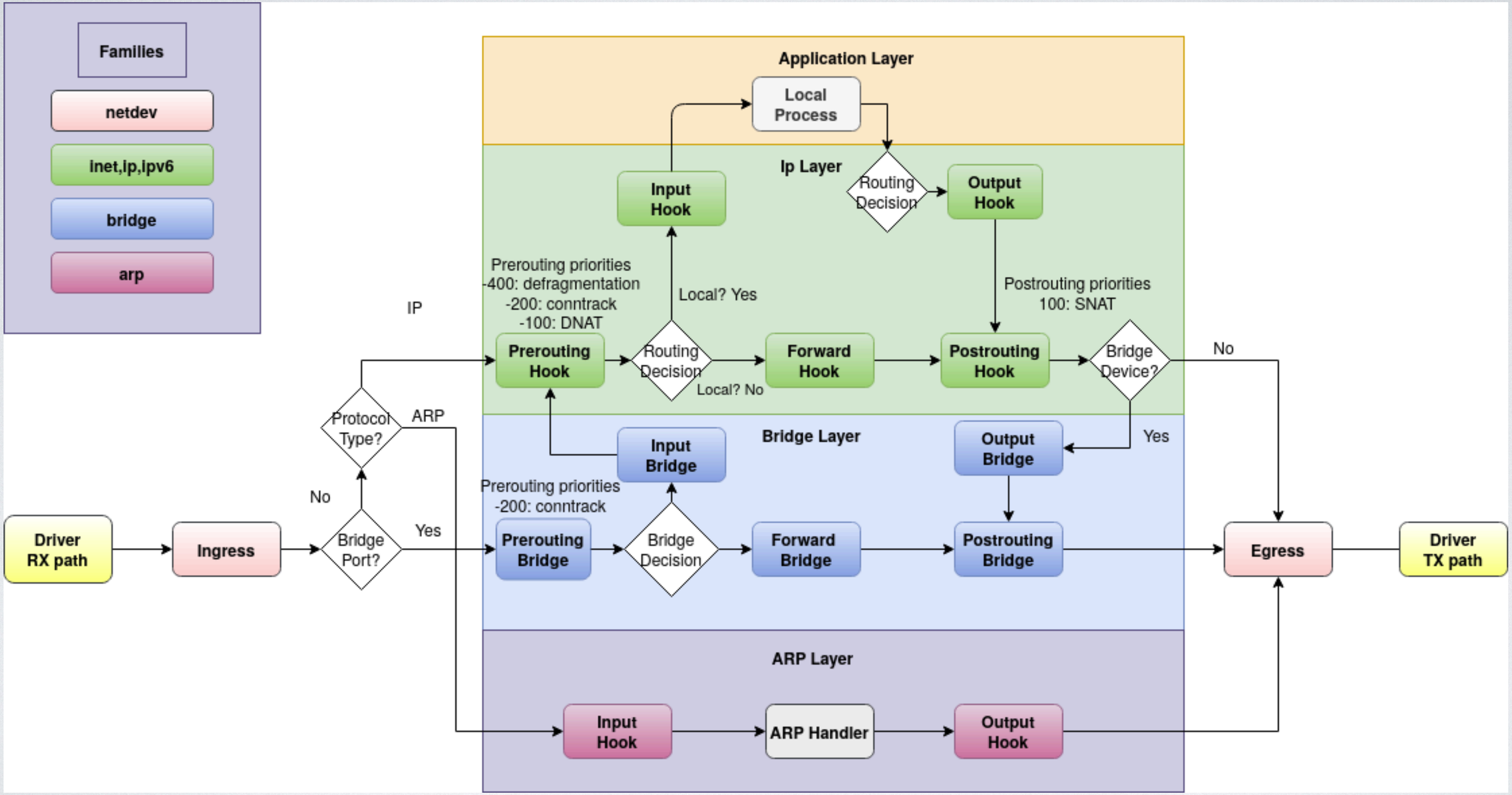
udp:
- dport <puerto de destino>
- sport <puerto de origen>

ct:
- state <new | established | related | invalid>

La acción puede ser (una o más de una) **accept**, **drop**, **queue**, **continue**, **return**, <cadena> **jump**, y <cadena> **goto**

También se les puede añadir: **log**, **reject**, **limit**, **counter**, **nat** (dnat, snat o masquerade)

ℹ️ https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes



https://wiki.nftables.org/wiki-nftables/index.php/Netfilter_hooks