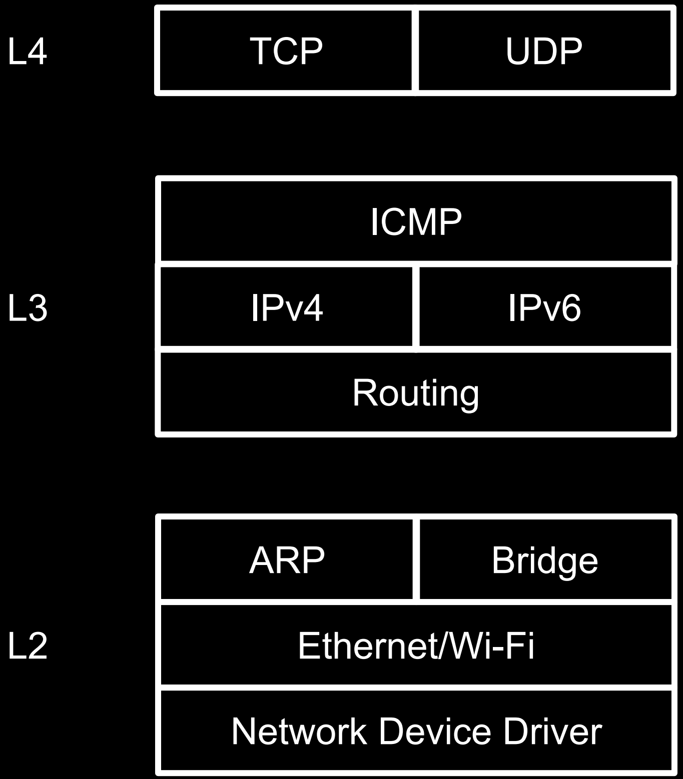
# Linux Network Stack and Netfilter

Taehee Yoo
ap420073@gmail.com

# Linux Network Stack



L4

TCP | UDP

L3

ICMP

IPv4 | IPv6

Routing

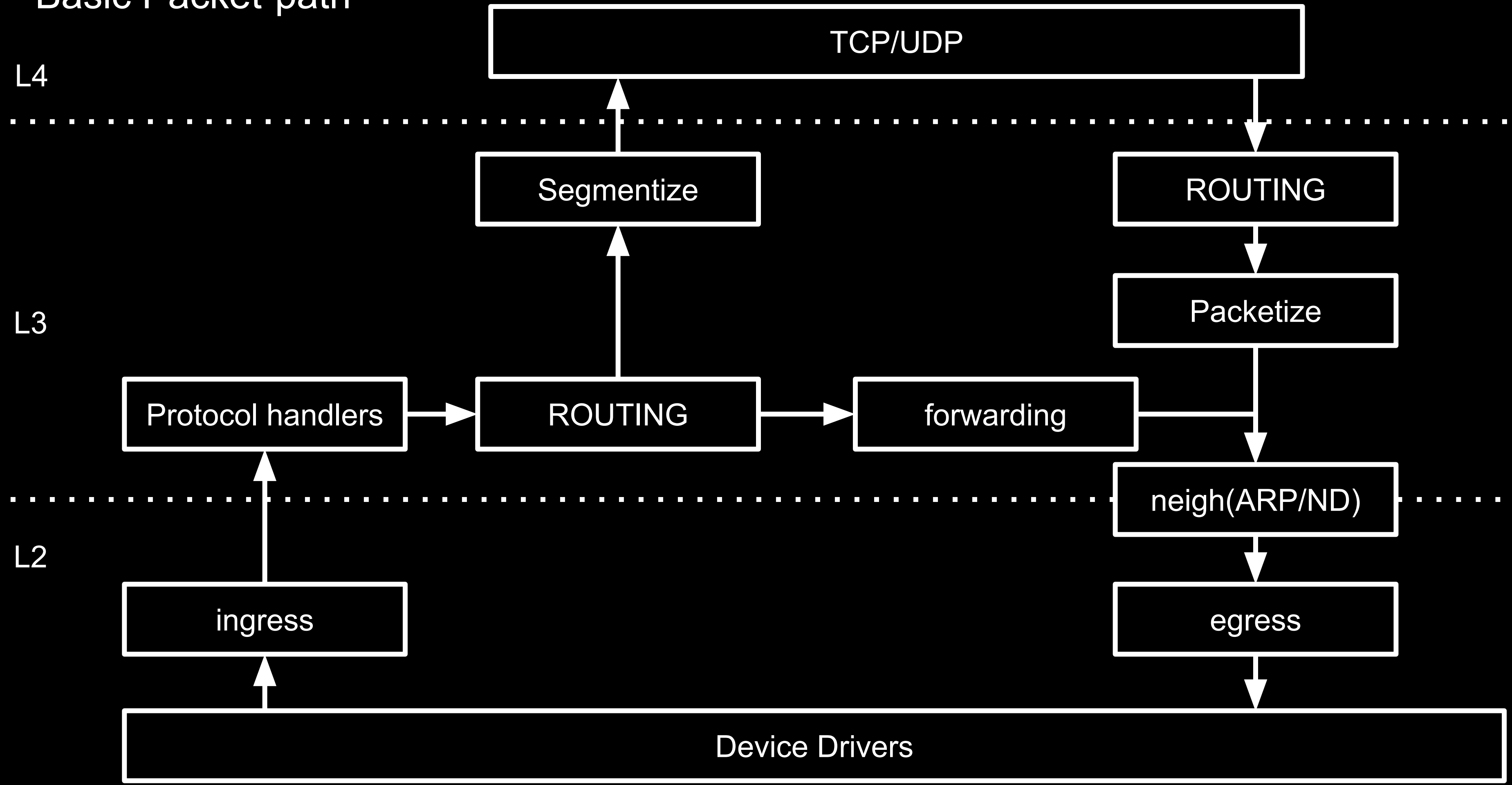
L2

ARP | Bridge

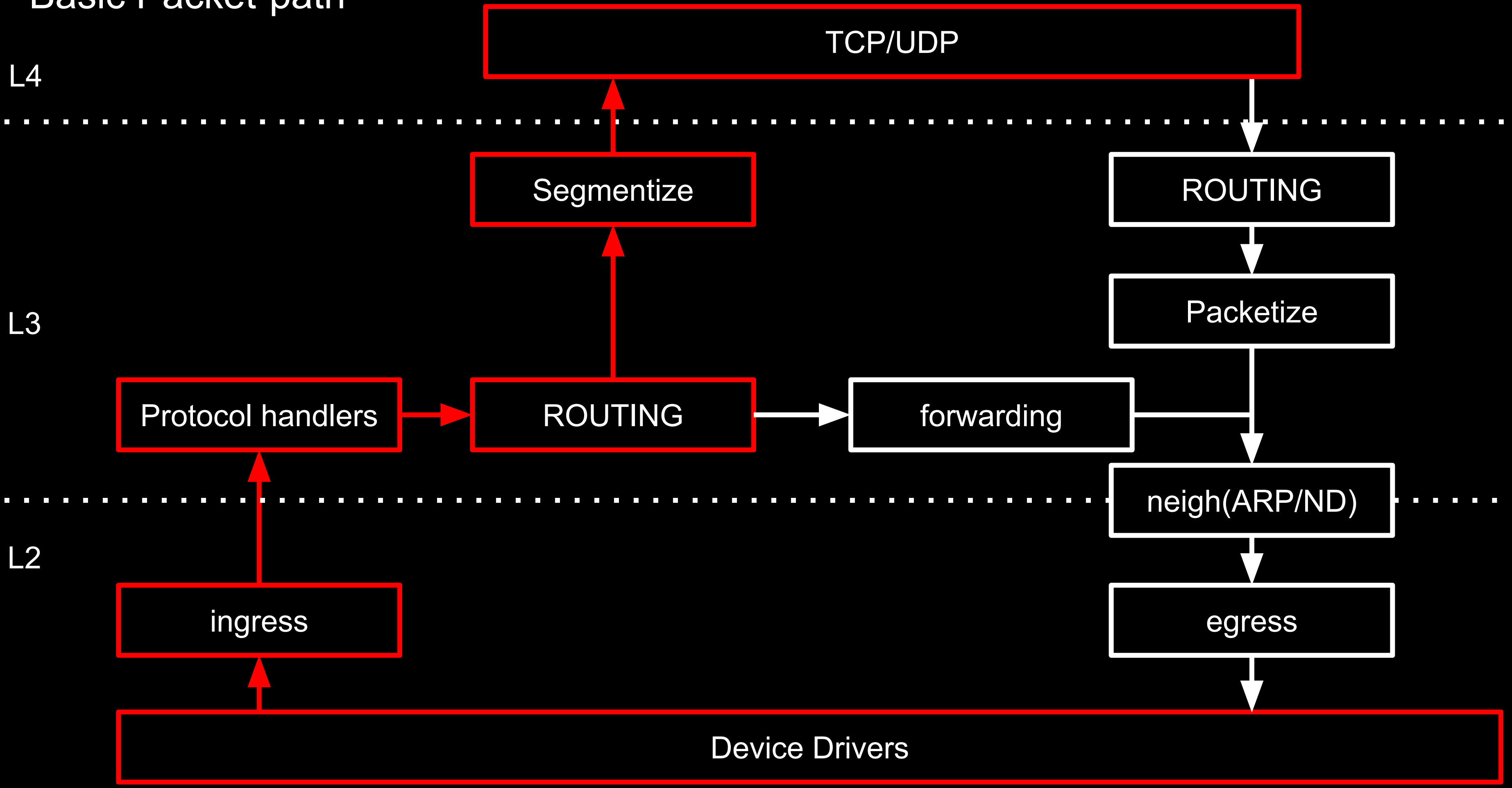
Ethernet/Wi-Fi

Network Device Driver

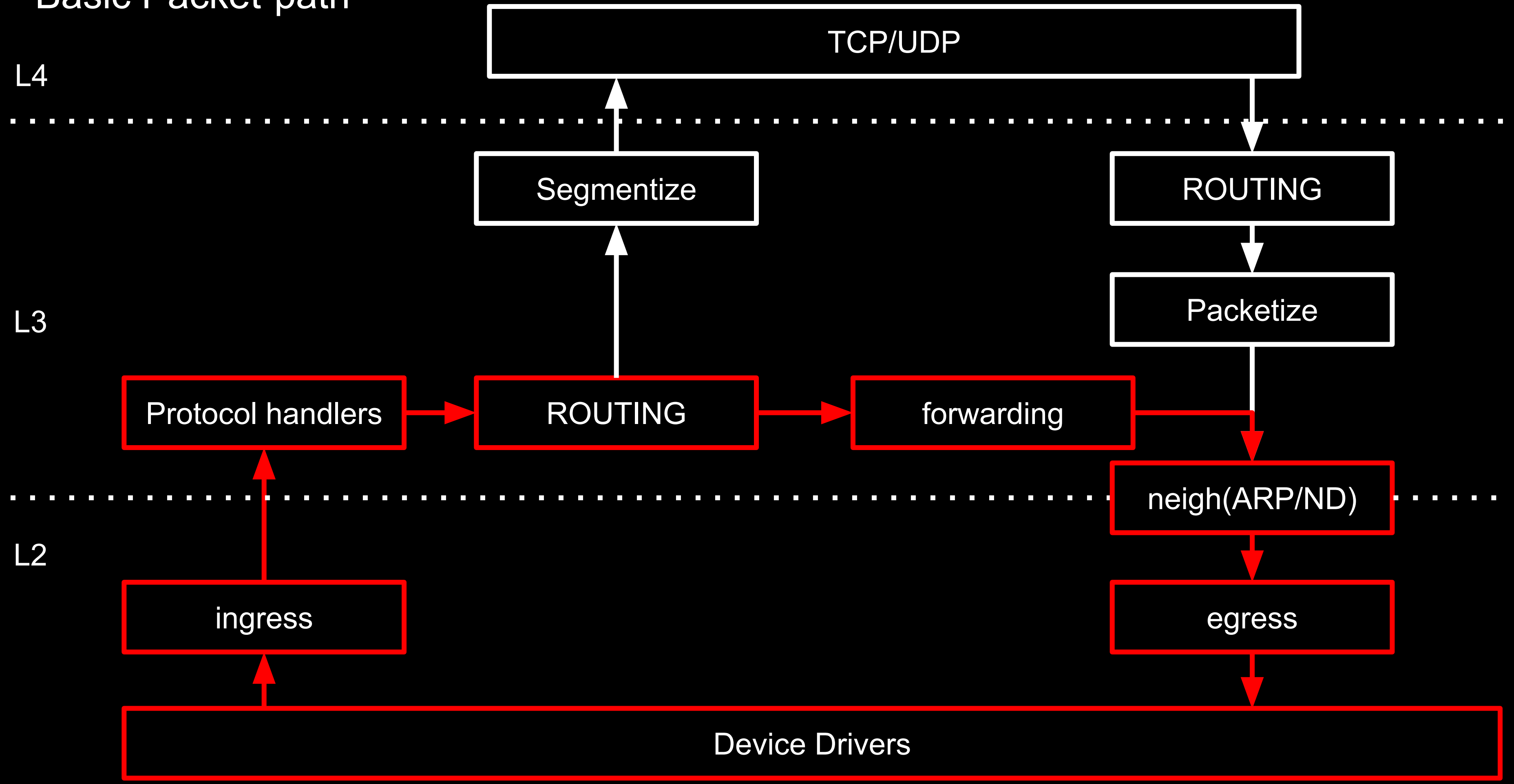
# Basic Packet-path



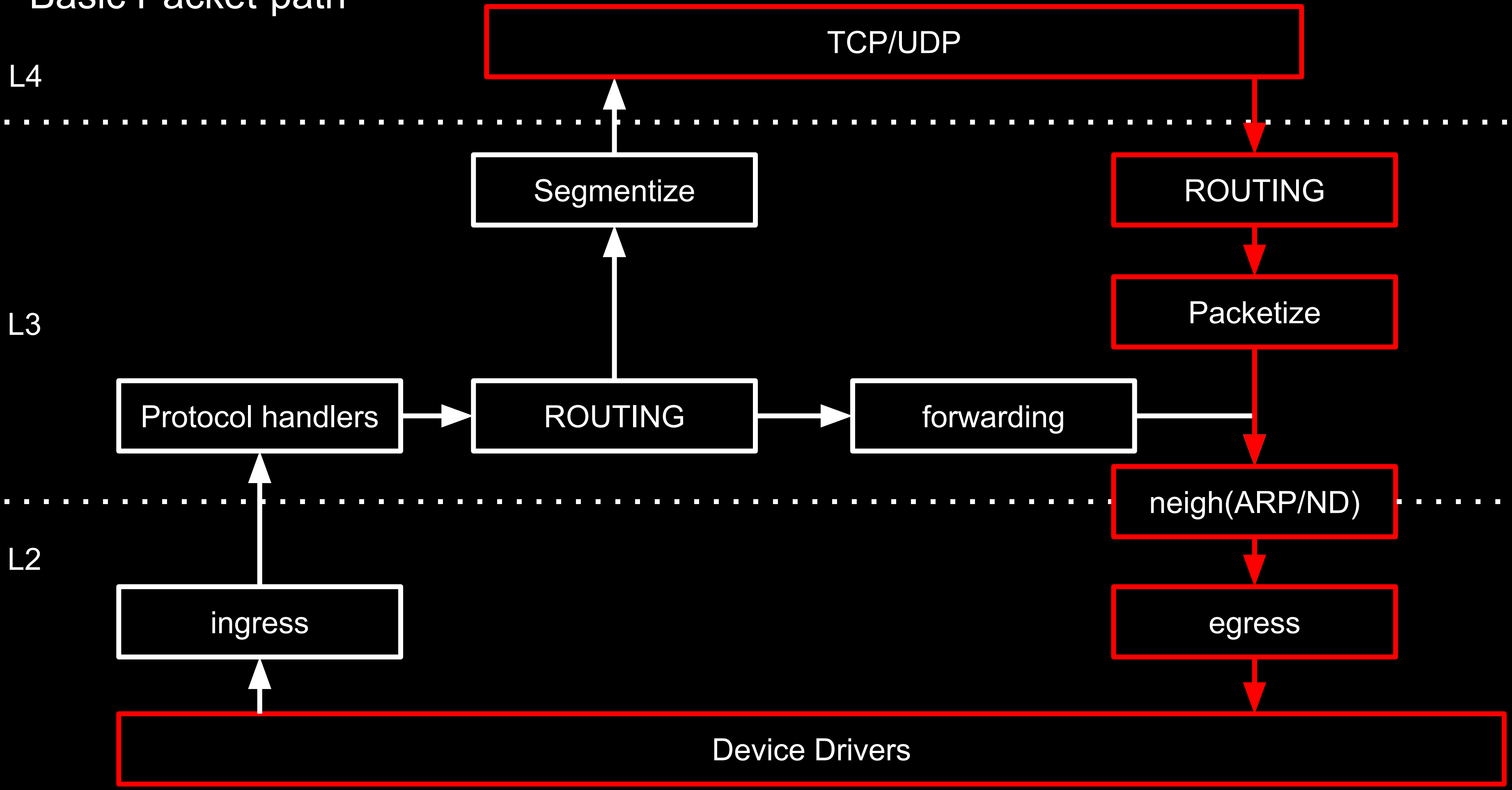
## Basic Packet-path



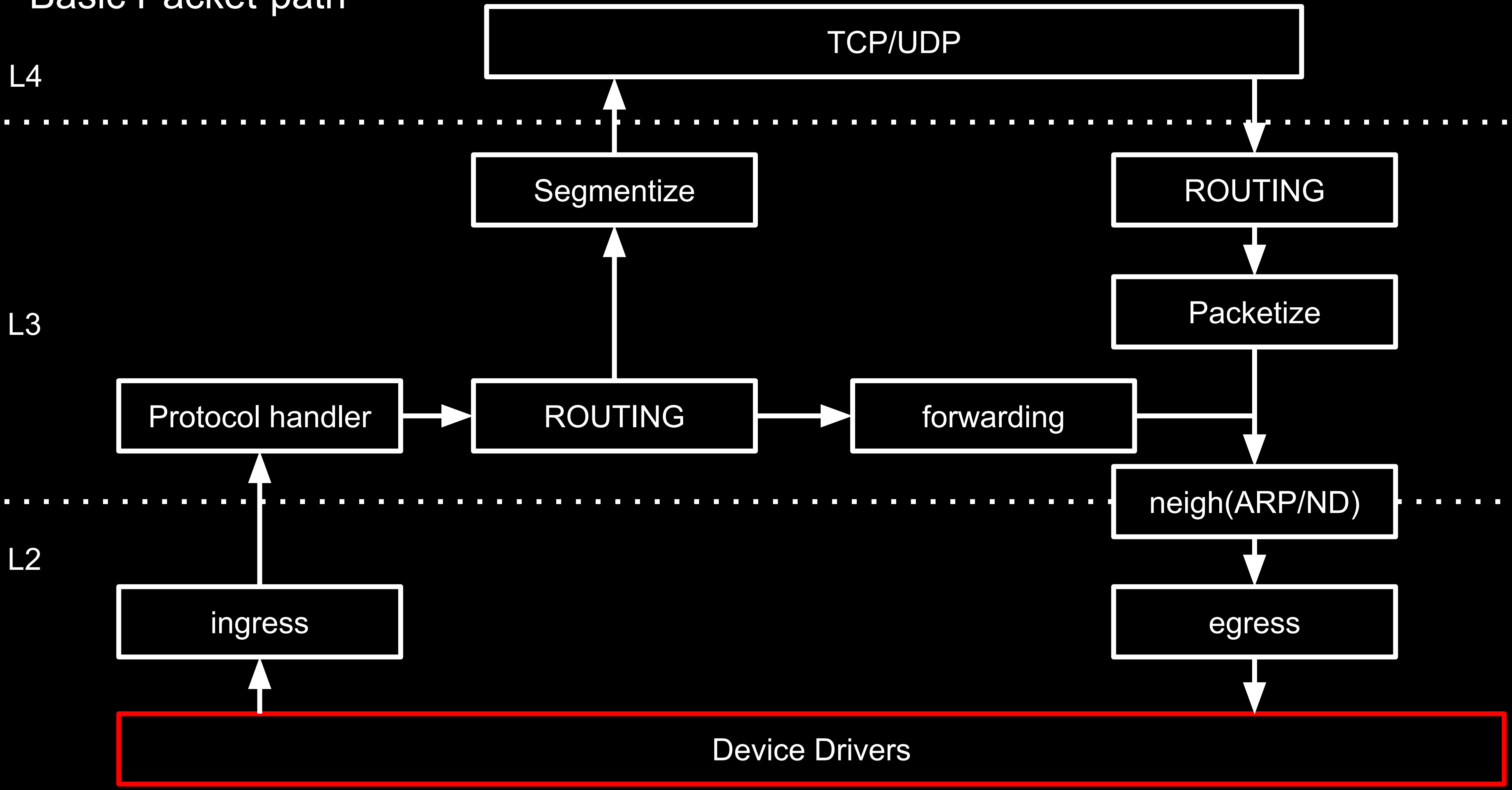
# Basic Packet-path



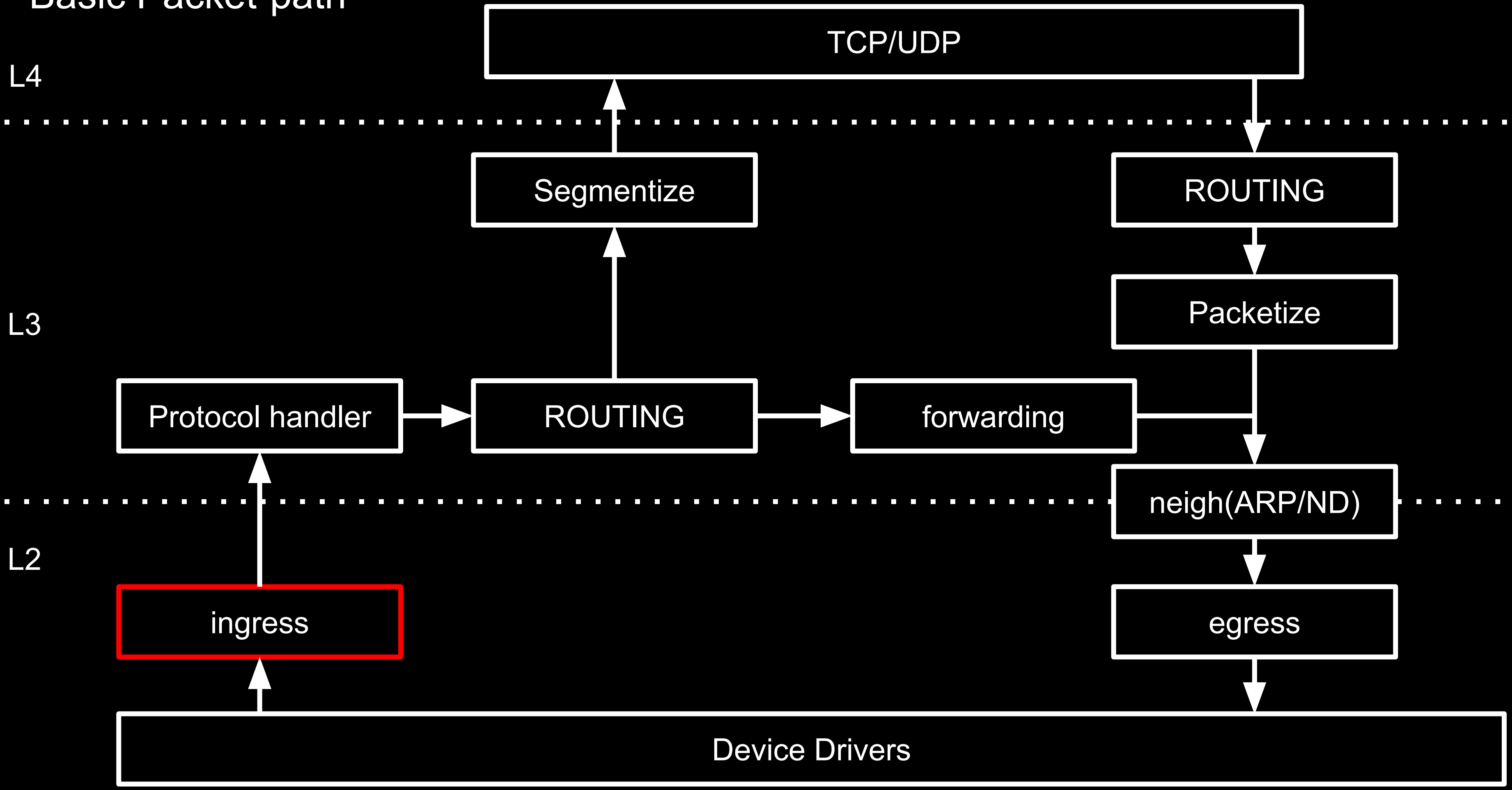
# Basic Packet-path



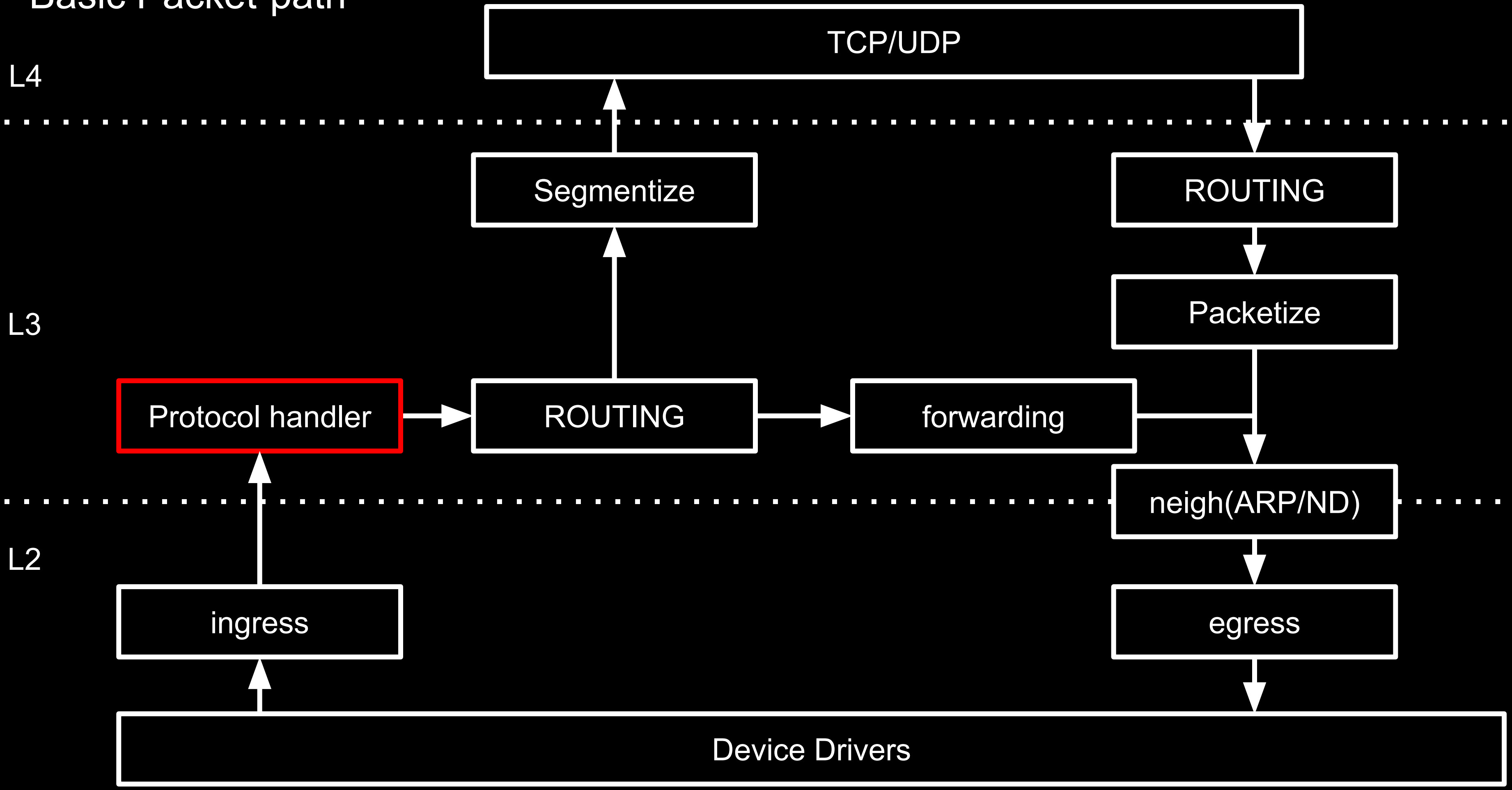
# Basic Packet-path



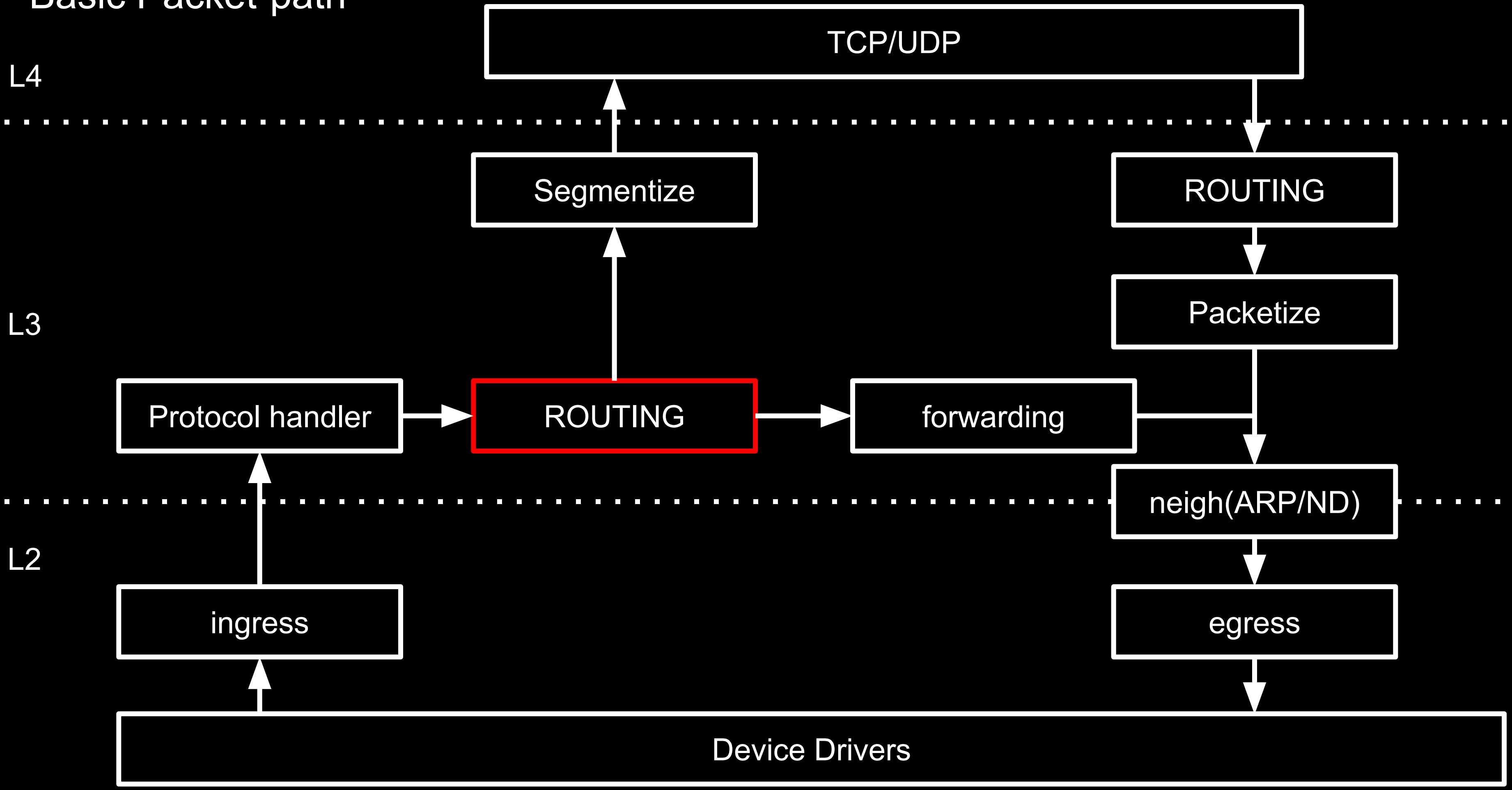
# Basic Packet-path



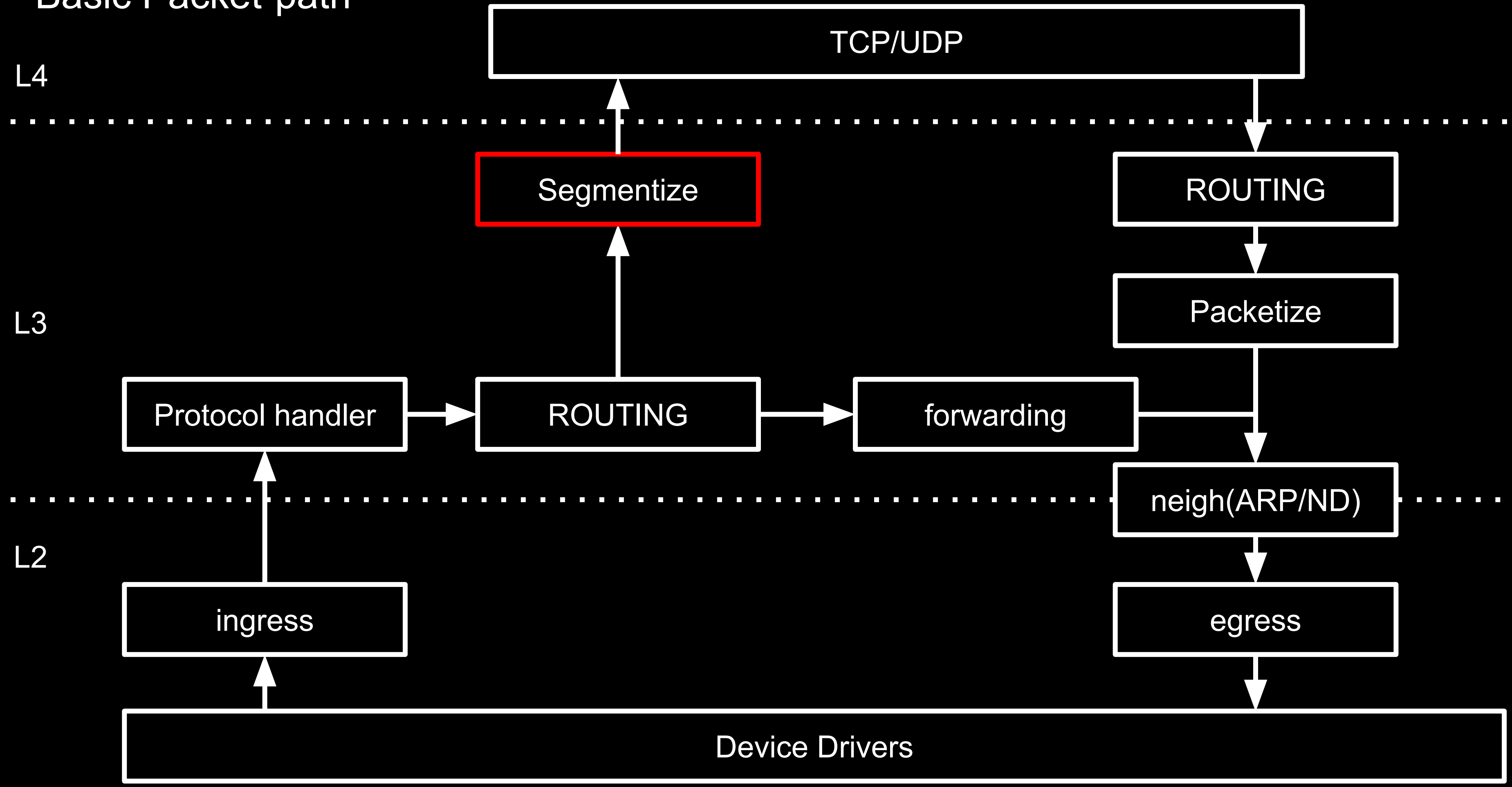
# Basic Packet-path



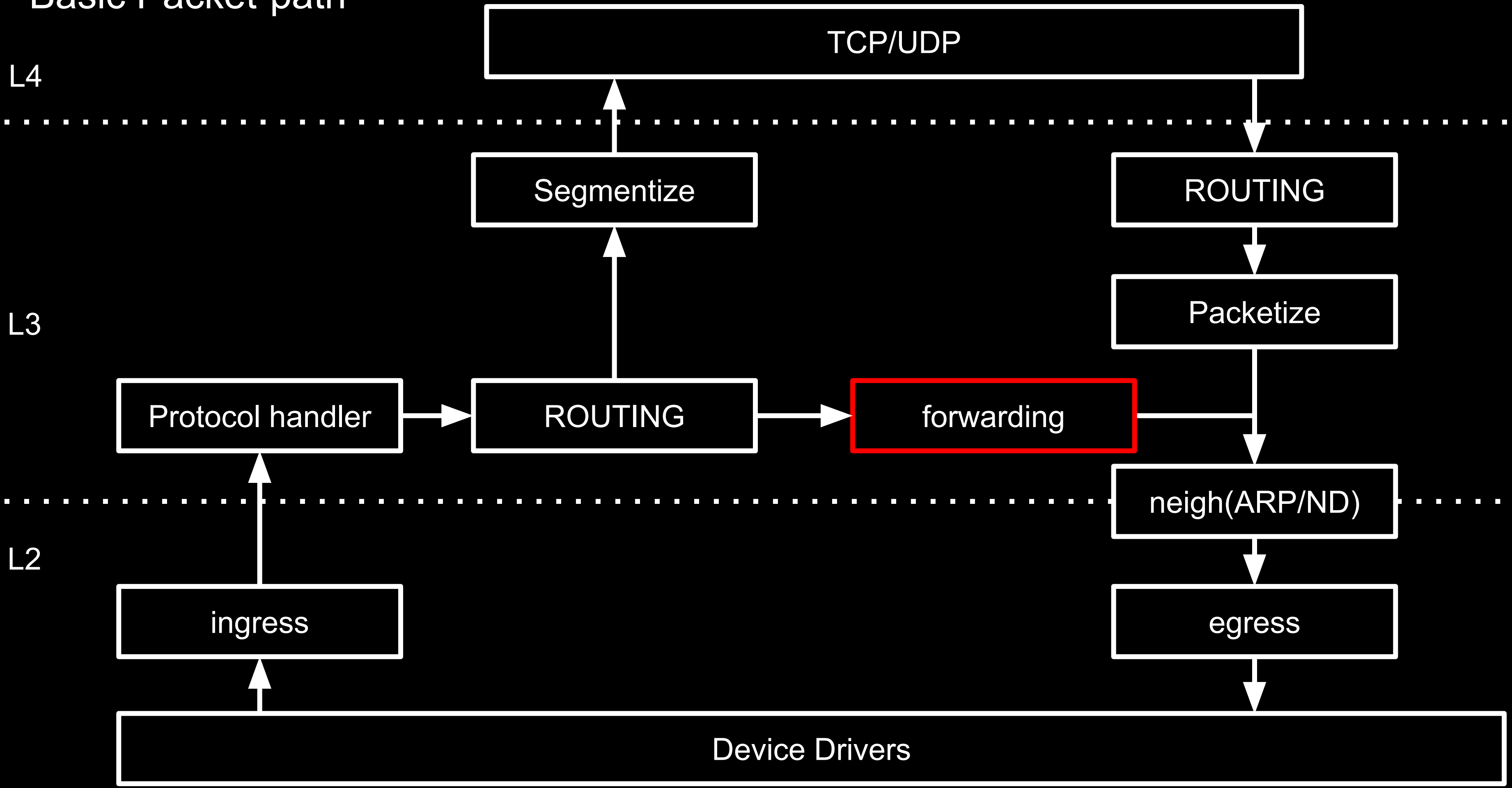
# Basic Packet-path



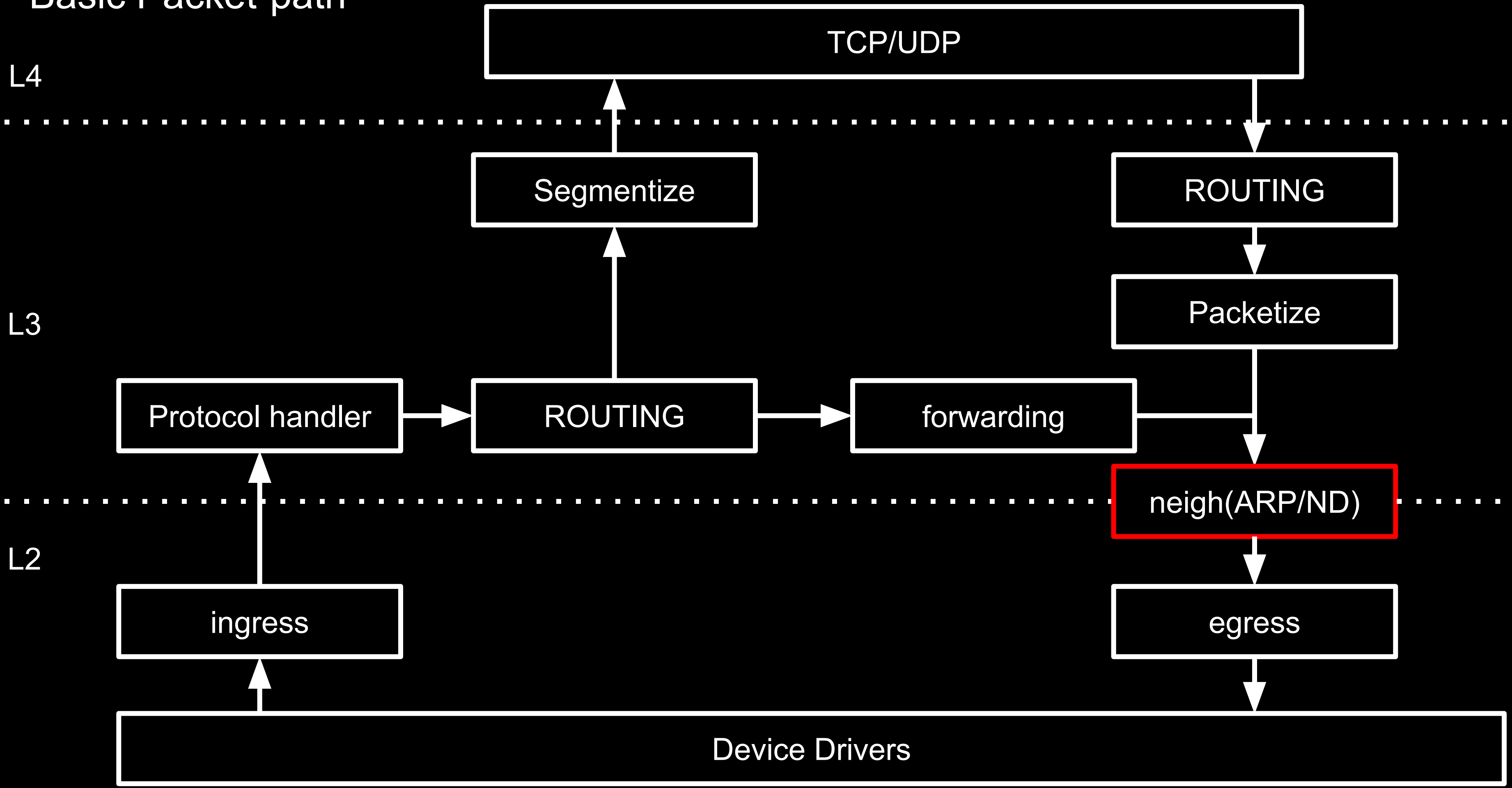
# Basic Packet-path



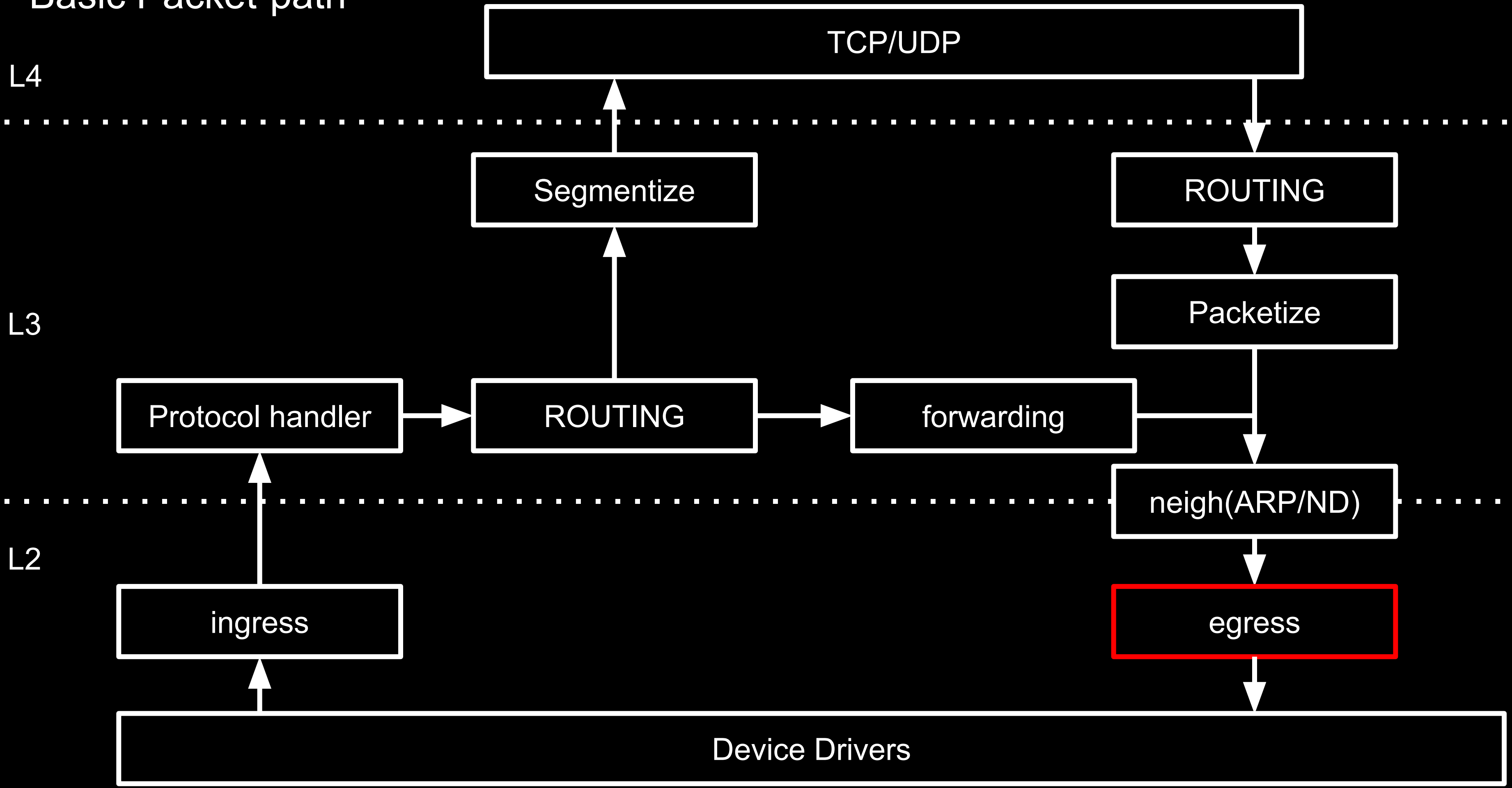
# Basic Packet-path



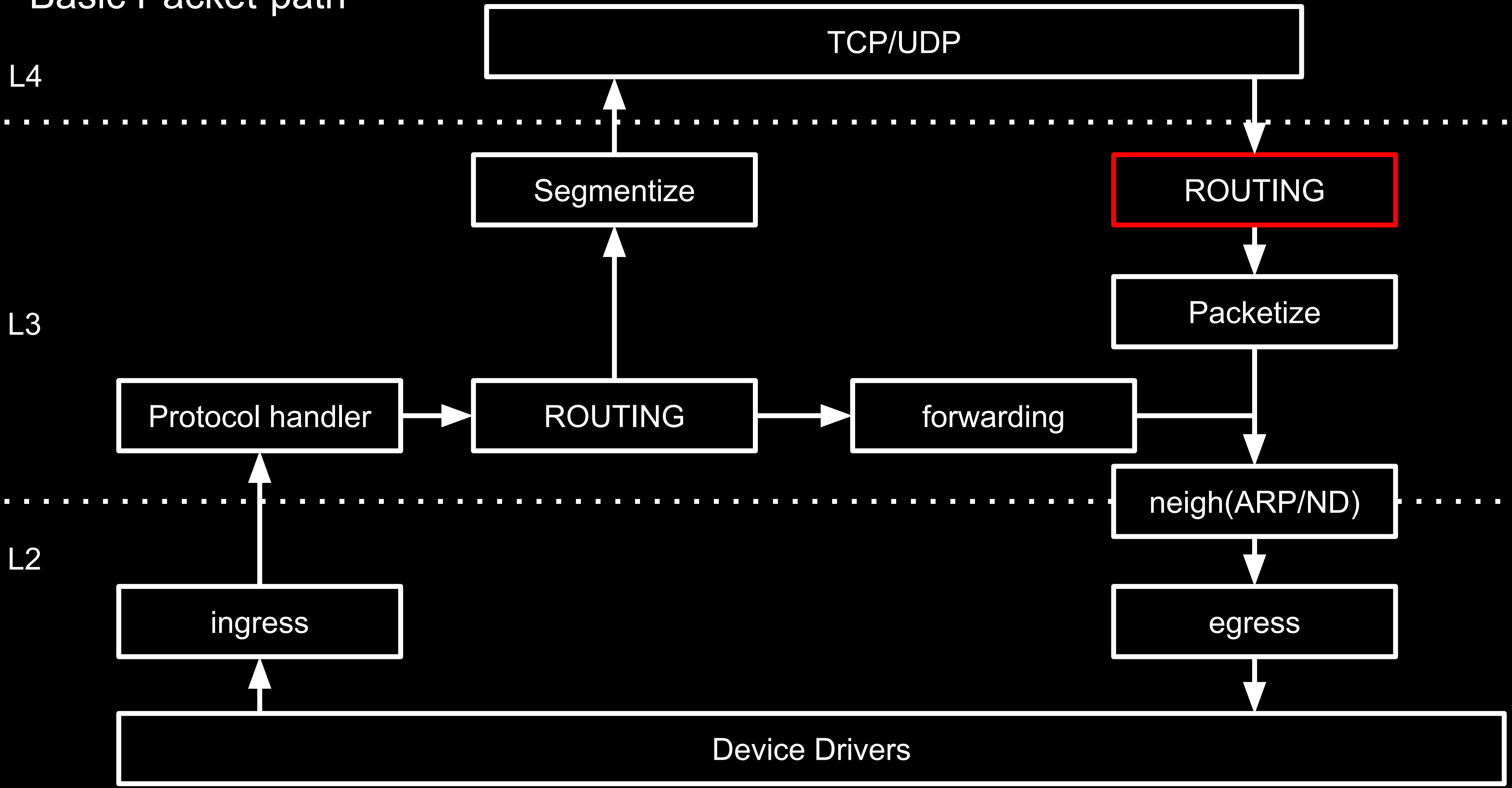
# Basic Packet-path



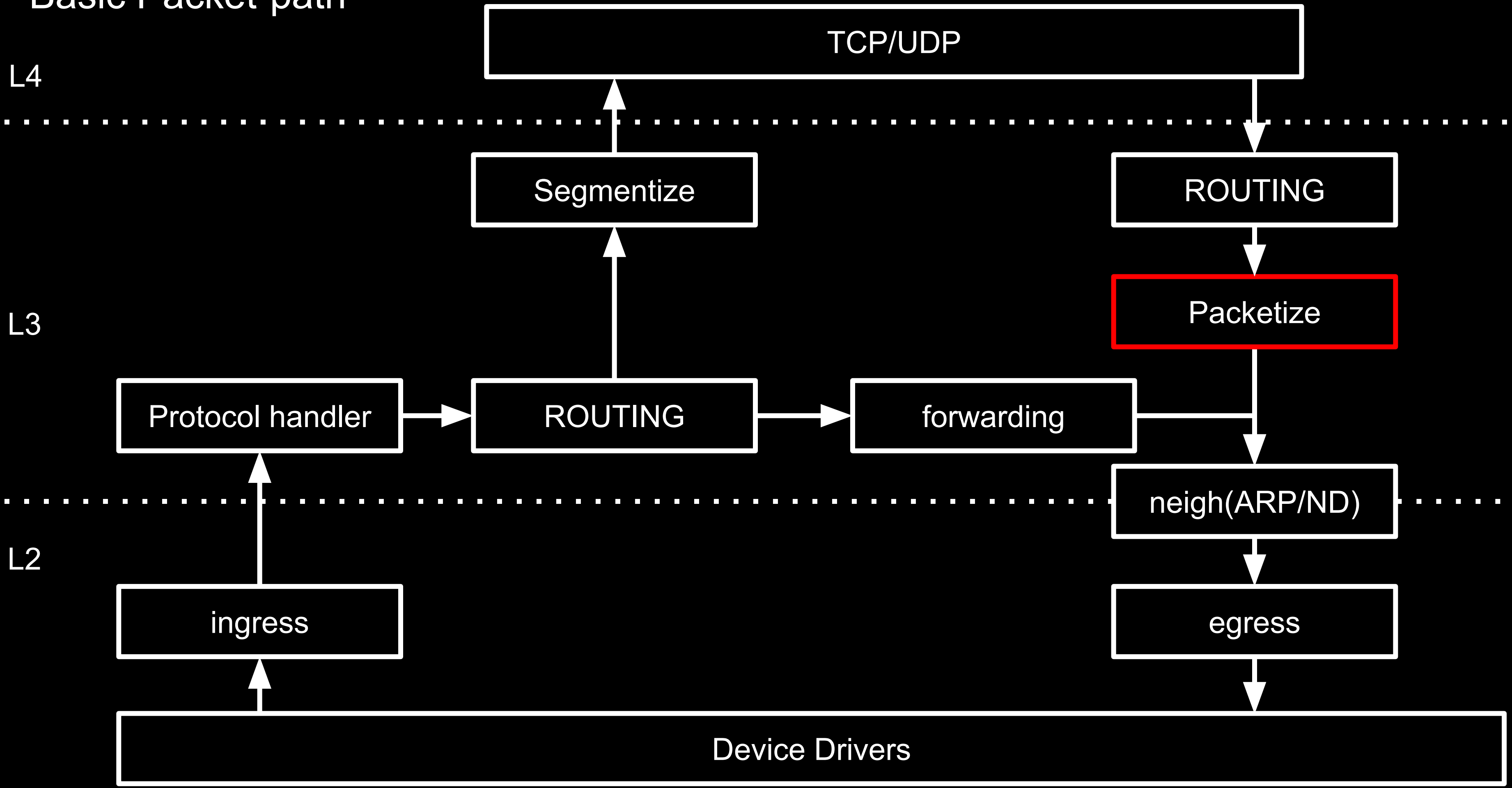
# Basic Packet-path



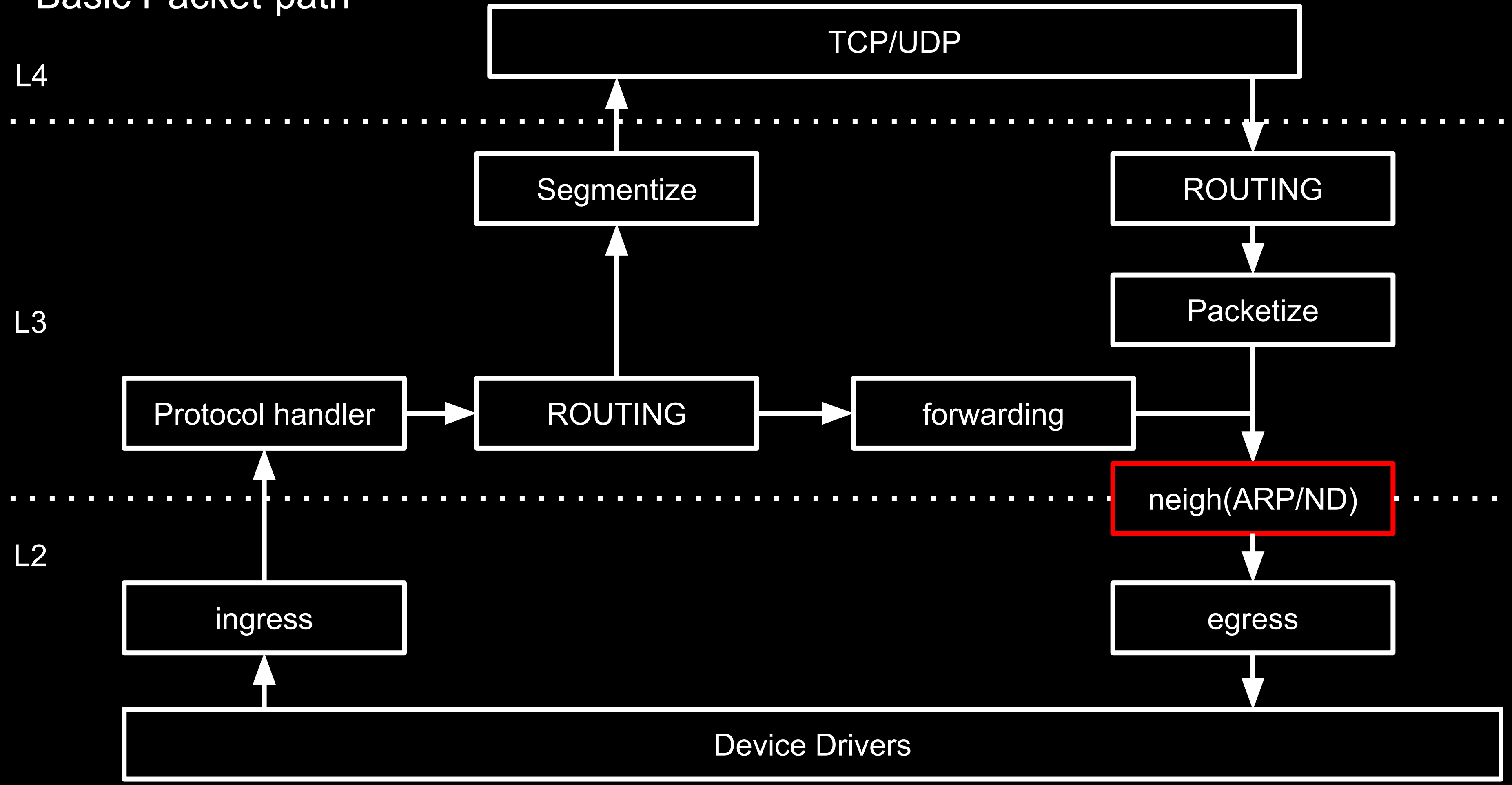
# Basic Packet-path



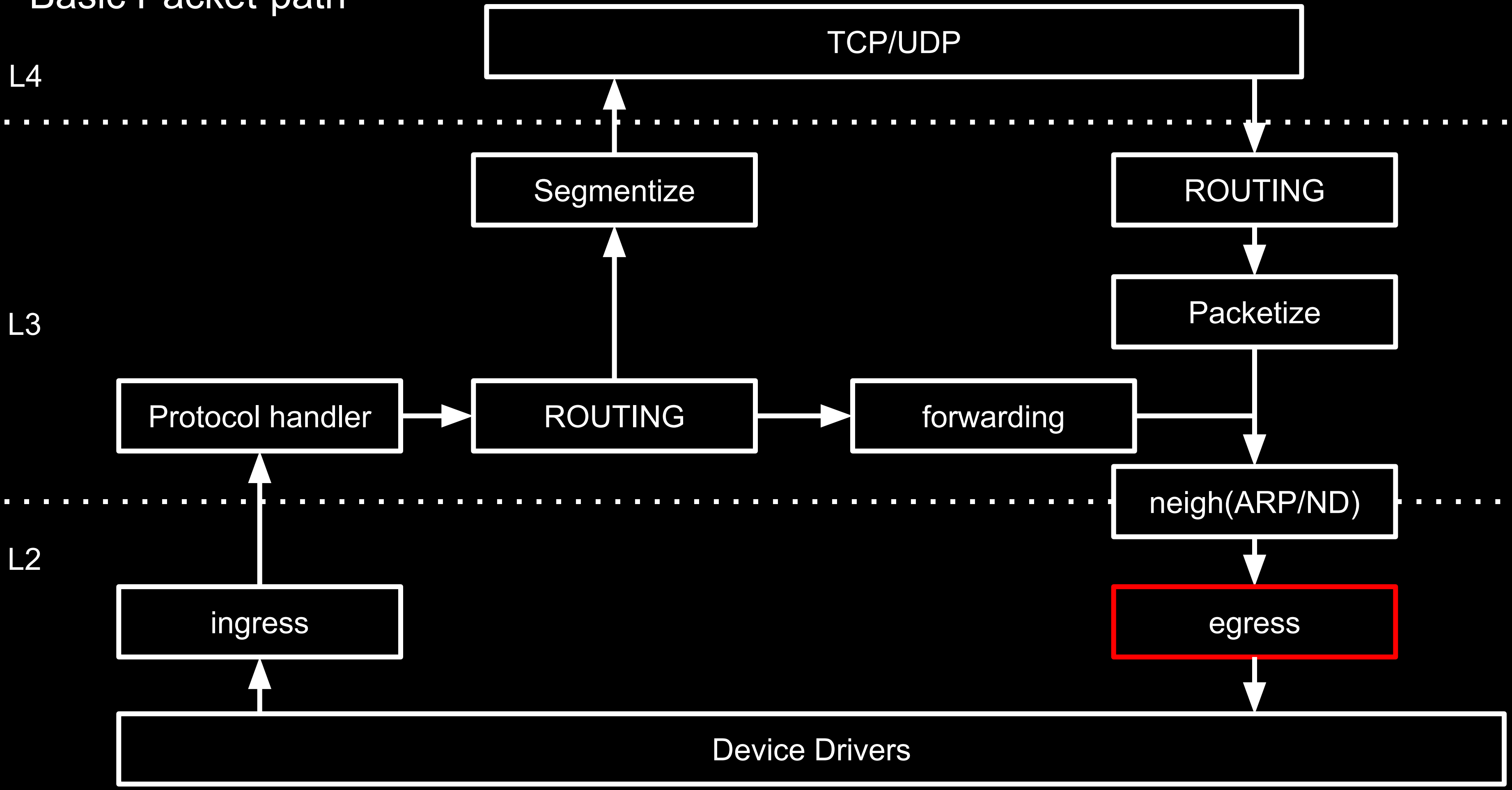
# Basic Packet-path



# Basic Packet-path



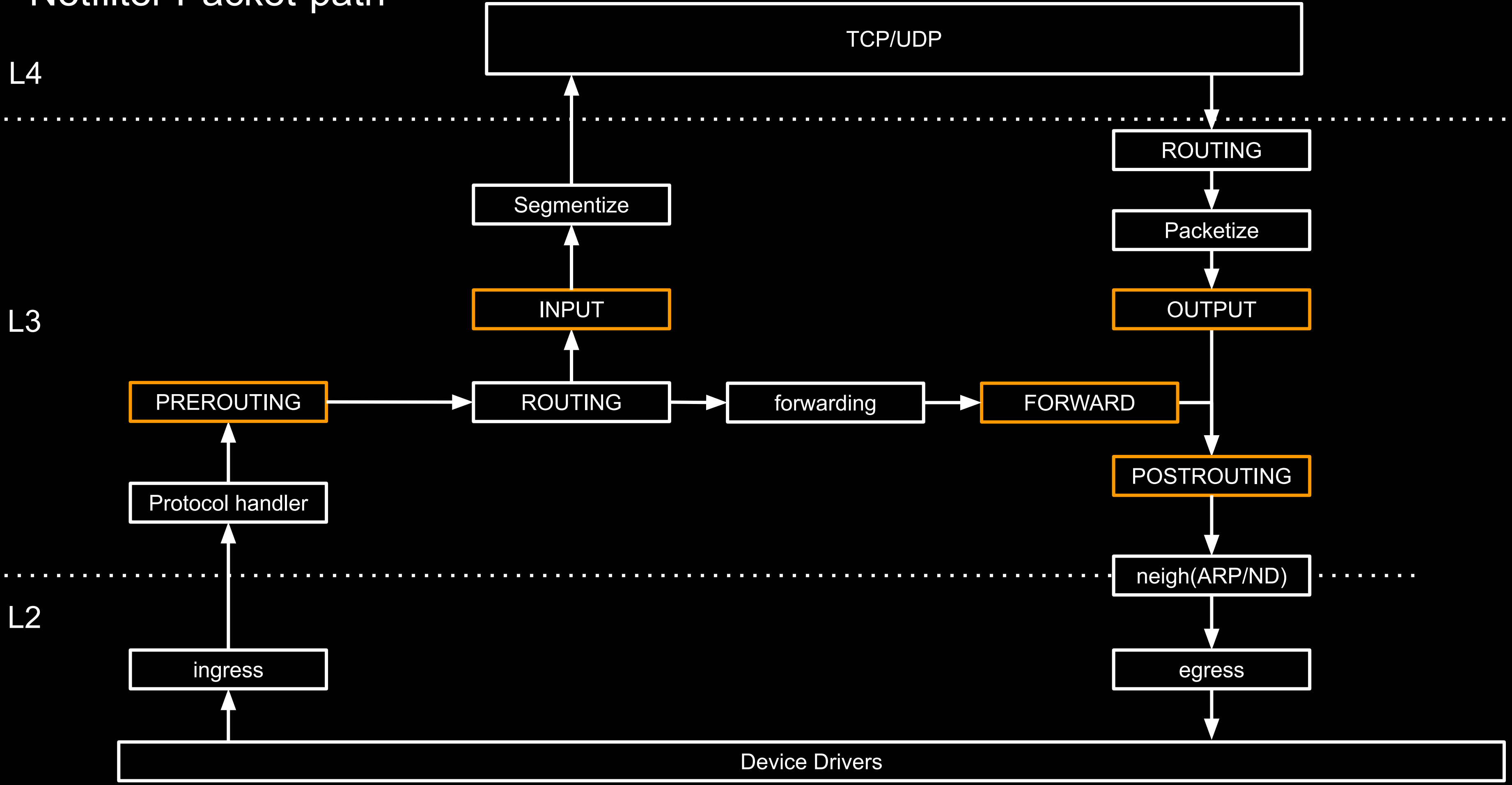
# Basic Packet-path



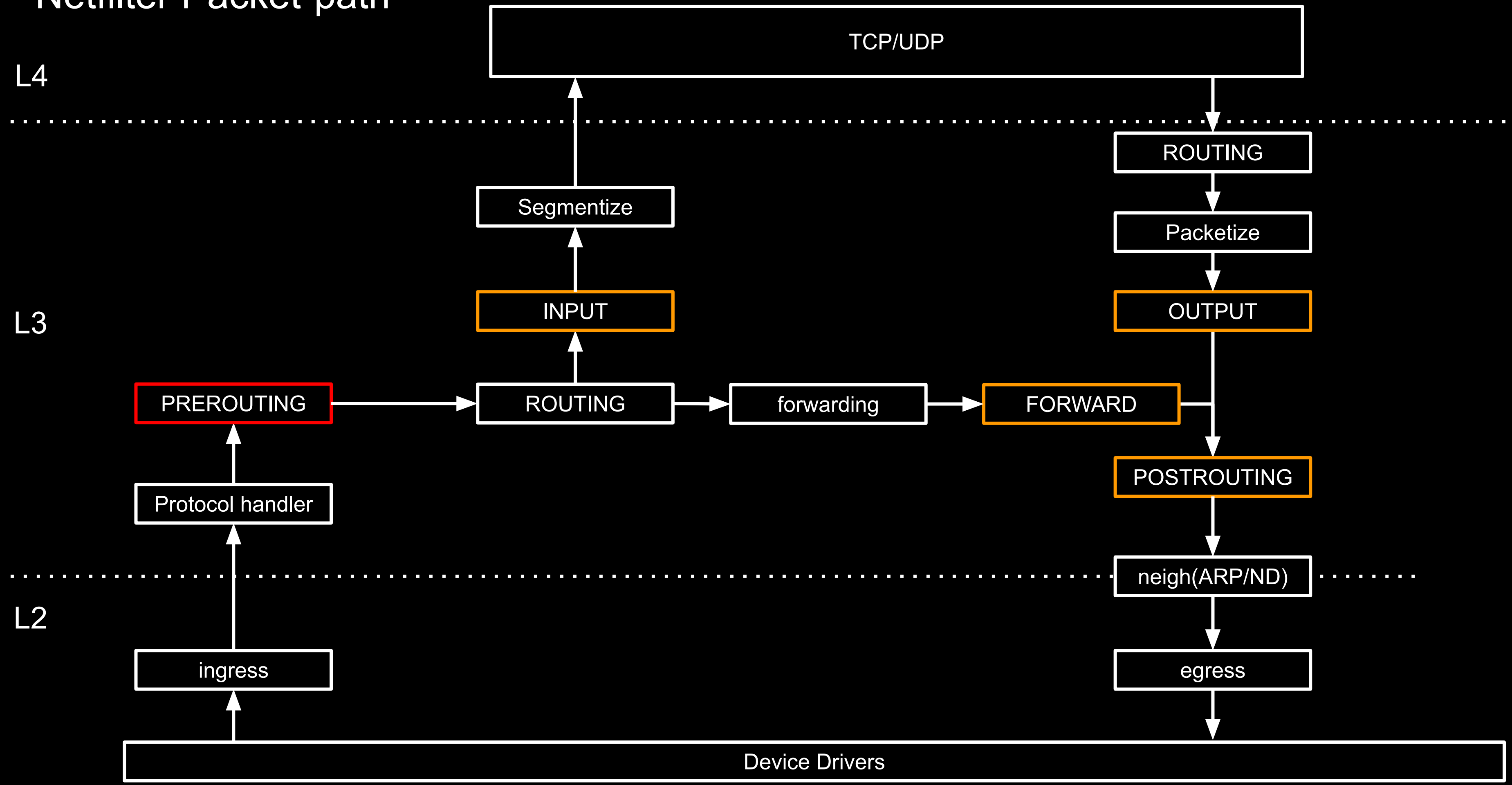
# netfilter?

- Linux Firewall Framework
    - Packet Filtering
    - Connection Tracking
    - NAT
    - Packet mangling
- user-space
    - Xtables{iptables, ip6tables, arptables, ebtables}
    - nft
    - conntrack

# Netfilter Packet-path

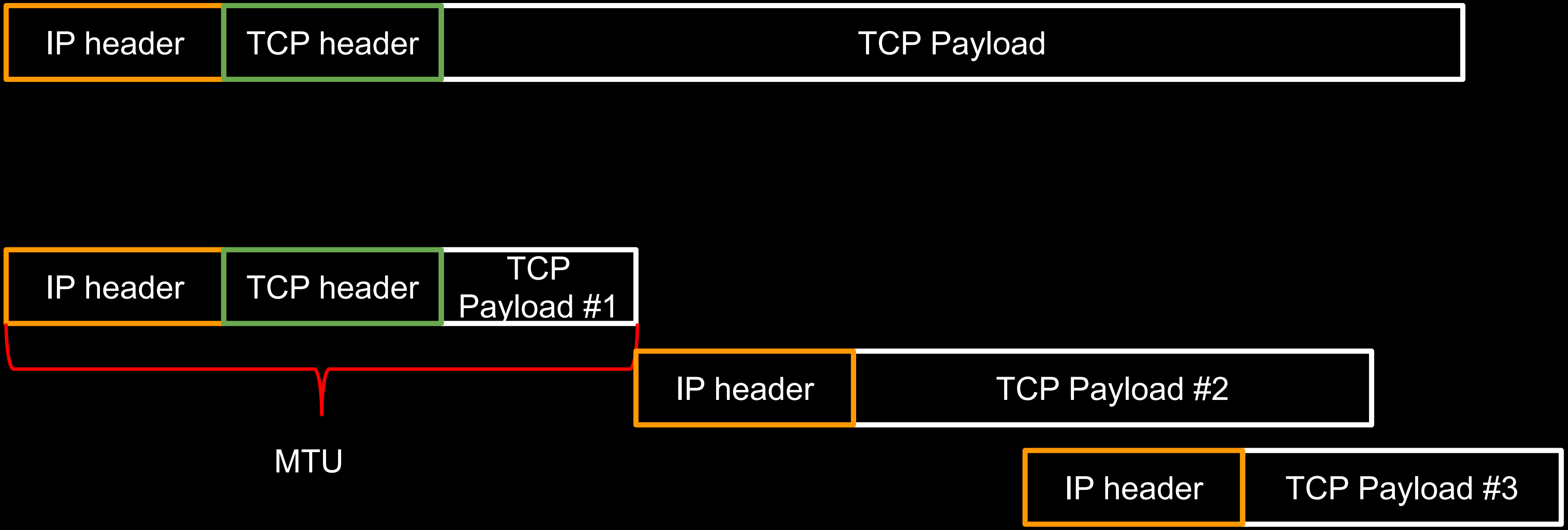


# Netfilter Packet-path



# Netfilter PREROUTING hook

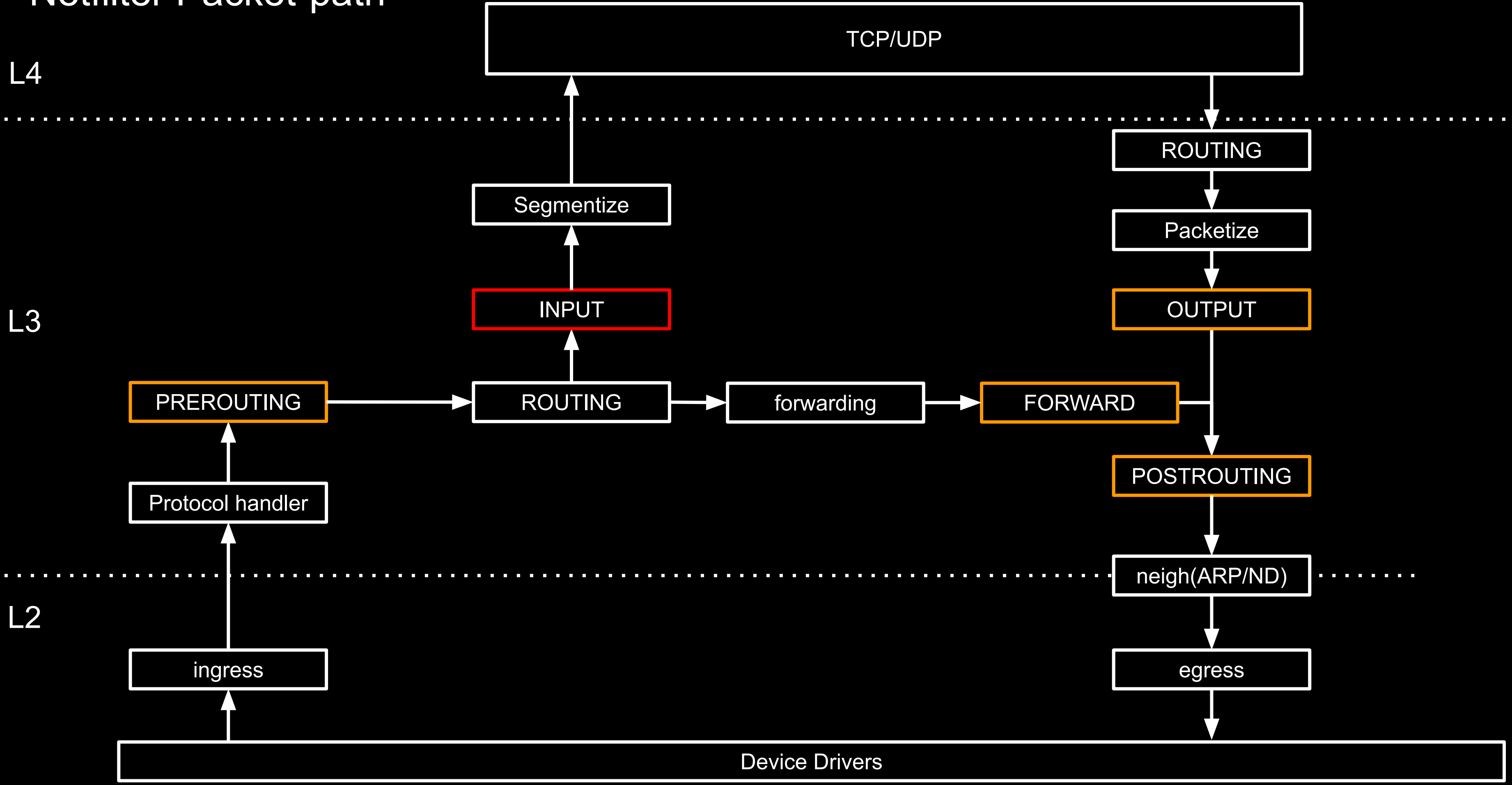
- Defragment



## Netfilter PREROUTING hook

- Defragment
- Session Initialization
- DNAT(Destination NAT)
- *iptables -t nat -I PREROUTING -j DNAT --to 1.1.1.1*
- *nft add rule ip nat PREROUTING dnat to 1.1.1.1*

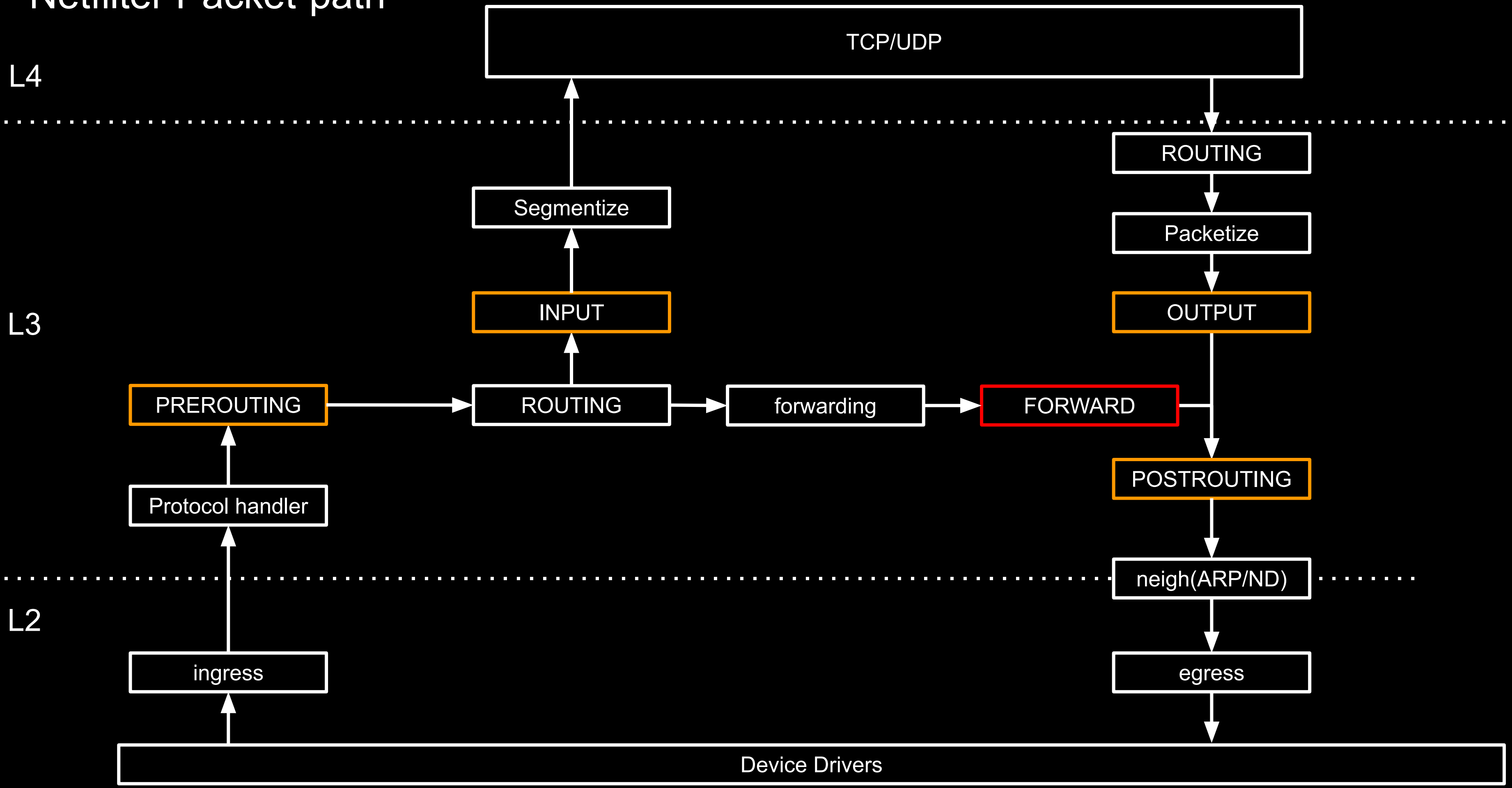
# Netfilter Packet-path



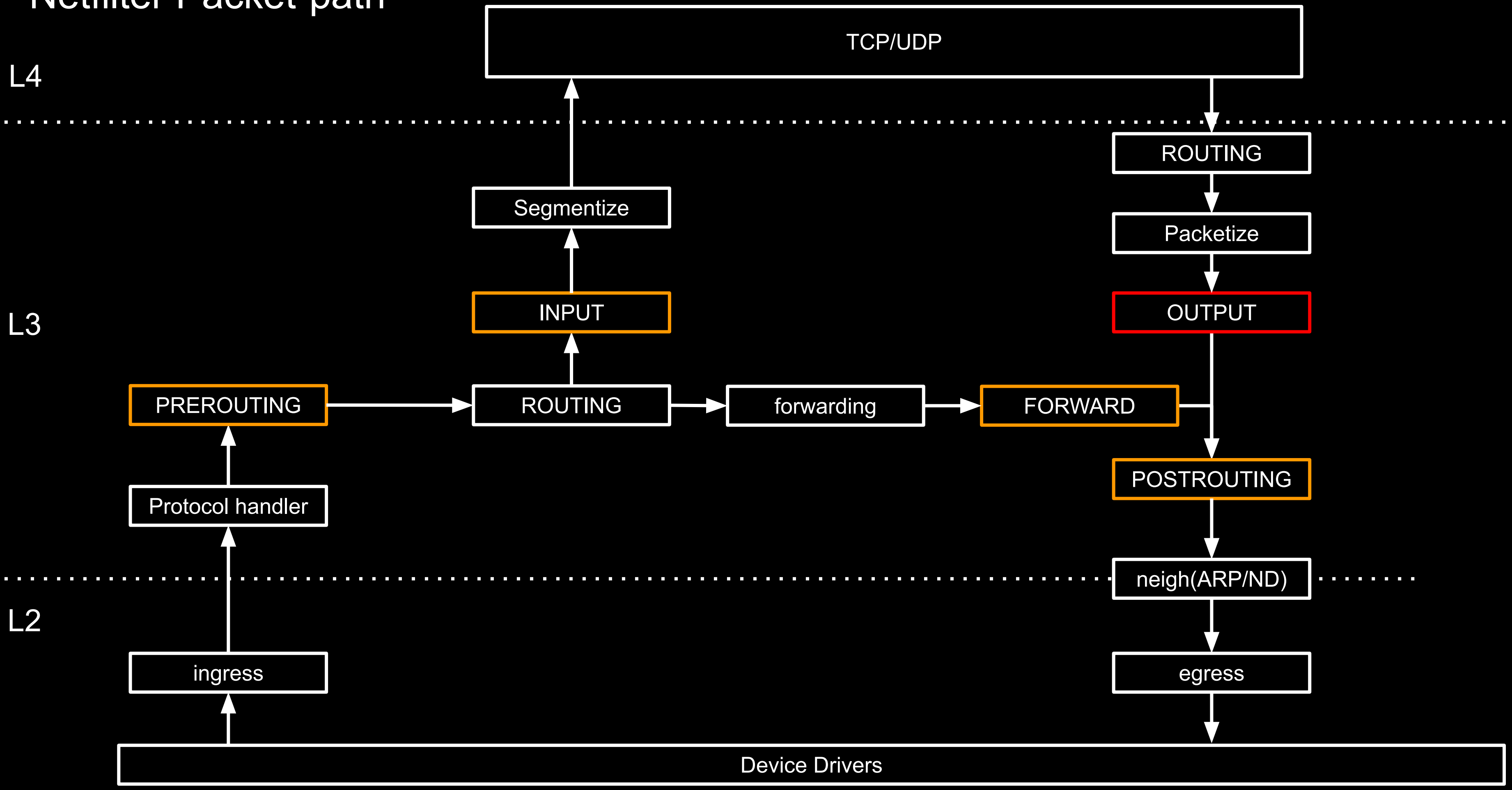
# Netfilter INPUT hook

- SNAT (Source NAT)
- *iptables -I INPUT -p tcp -s 1.1.1.1  -j ACCEPT*
- *nft add rule ip filter INPUT ip protocol 6 ip saddr 1.1.1.1 accept*

# Netfilter Packet-path



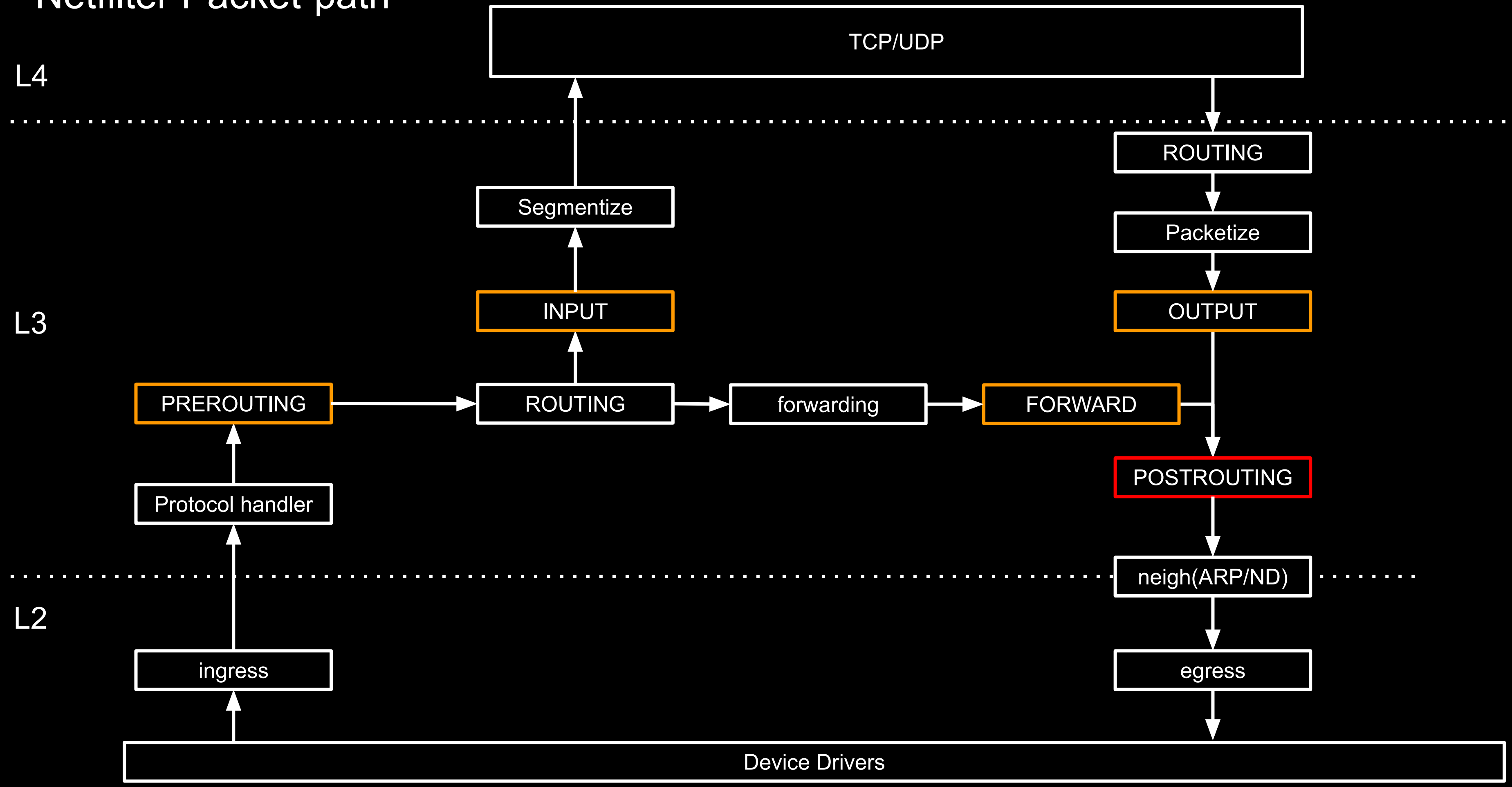
# Netfilter Packet-path



# Netfilter OUTPUT hook

- Session Initialization
- DNAT (Destination NAT)
- *iptables -I OUTPUT -p udp -d 2.2.2.2 -j DROP*
- *nft add rule ip filter OUTPUT ip protocol 17 ip daddr 2.2.2.2 drop*

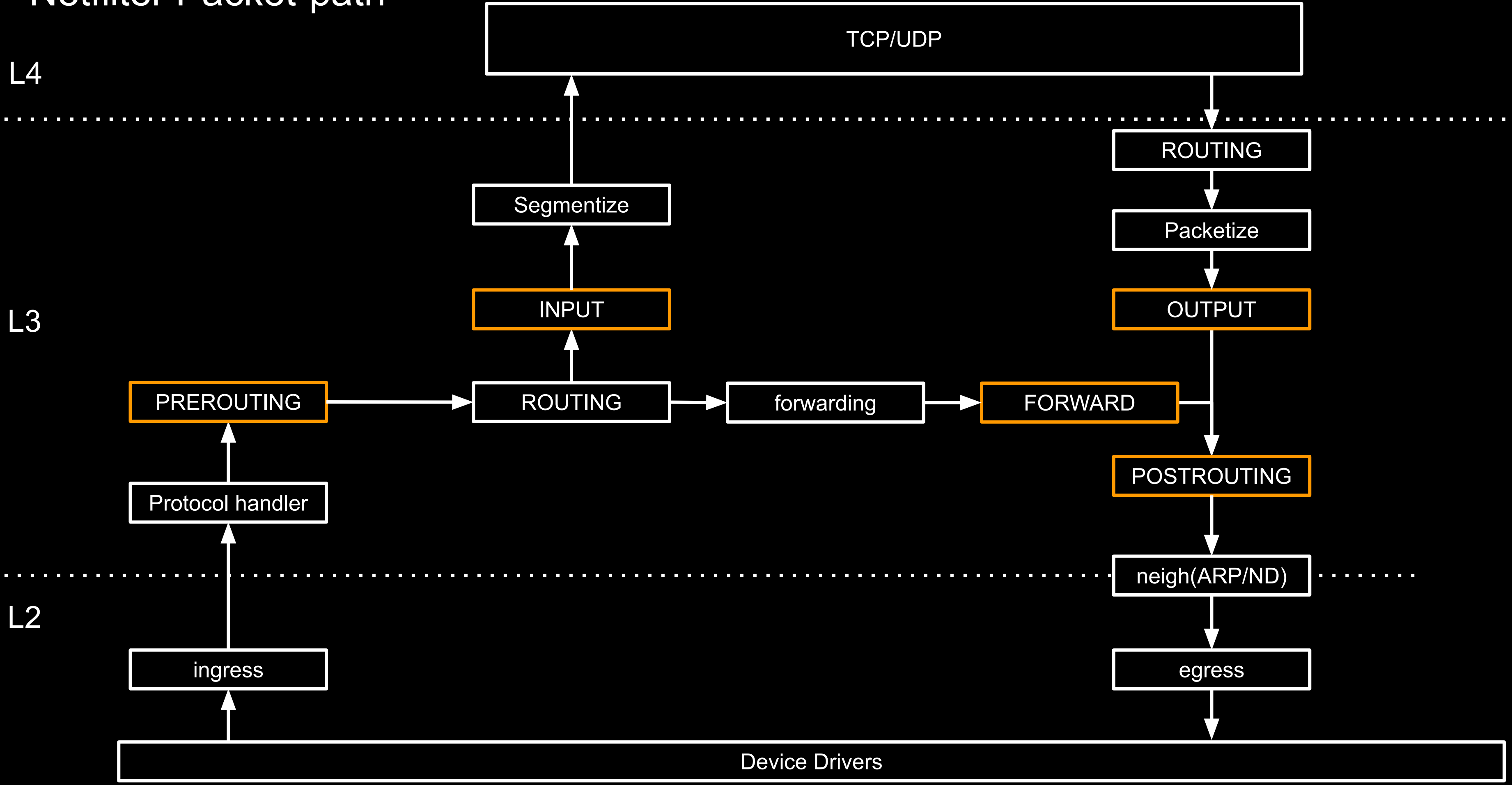
# Netfilter Packet-path



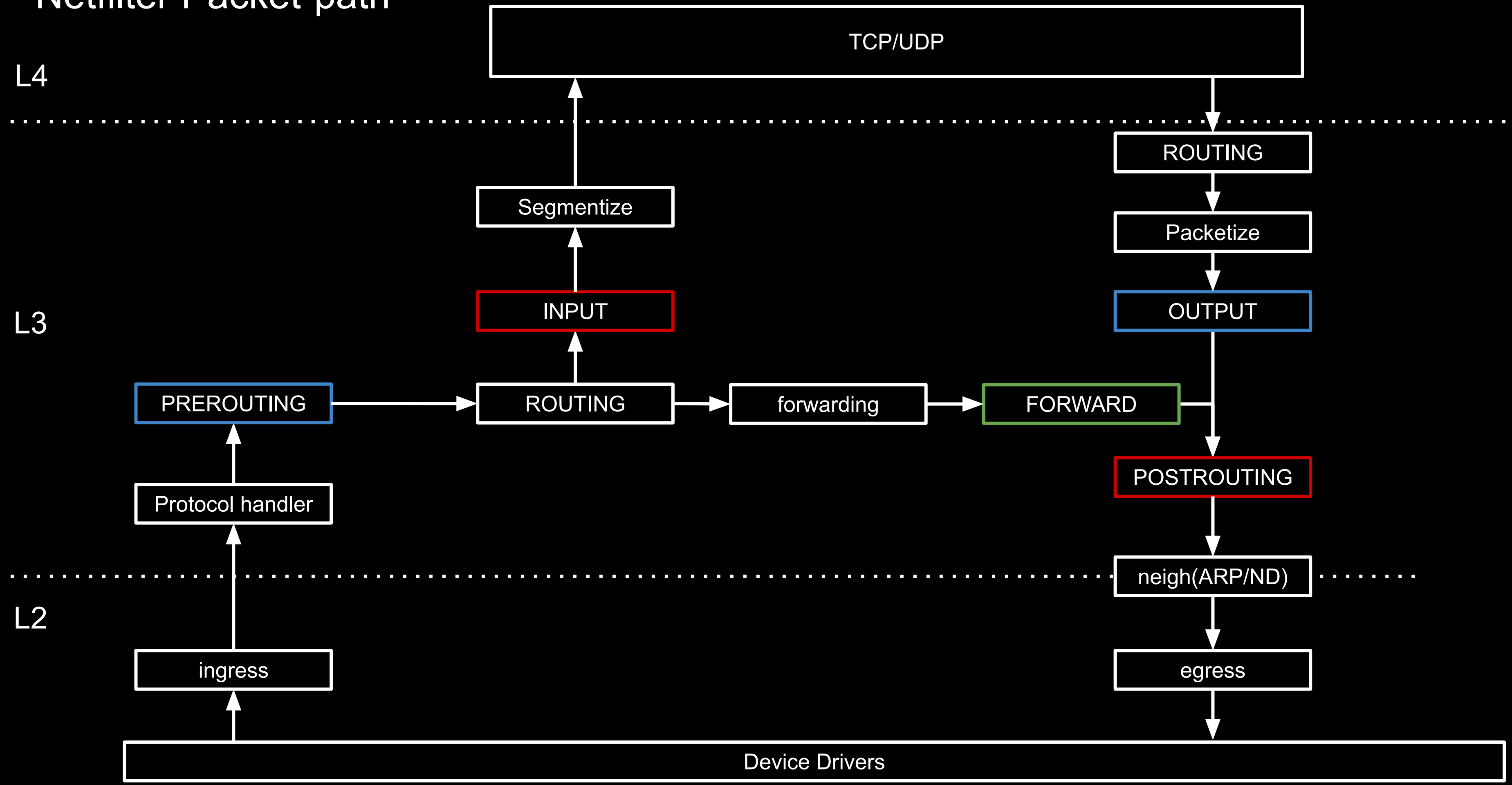
# Netfilter POSTROUTING hook

- SNAT/MASQUERADE (Source NAT)
- *iptables -t nat -I POSTROUTING -d 2.2.2.2 -j MASQUERADE*
- *nft add rule nat POSTROUTING ip daddr 2.2.2.2 masquerade*

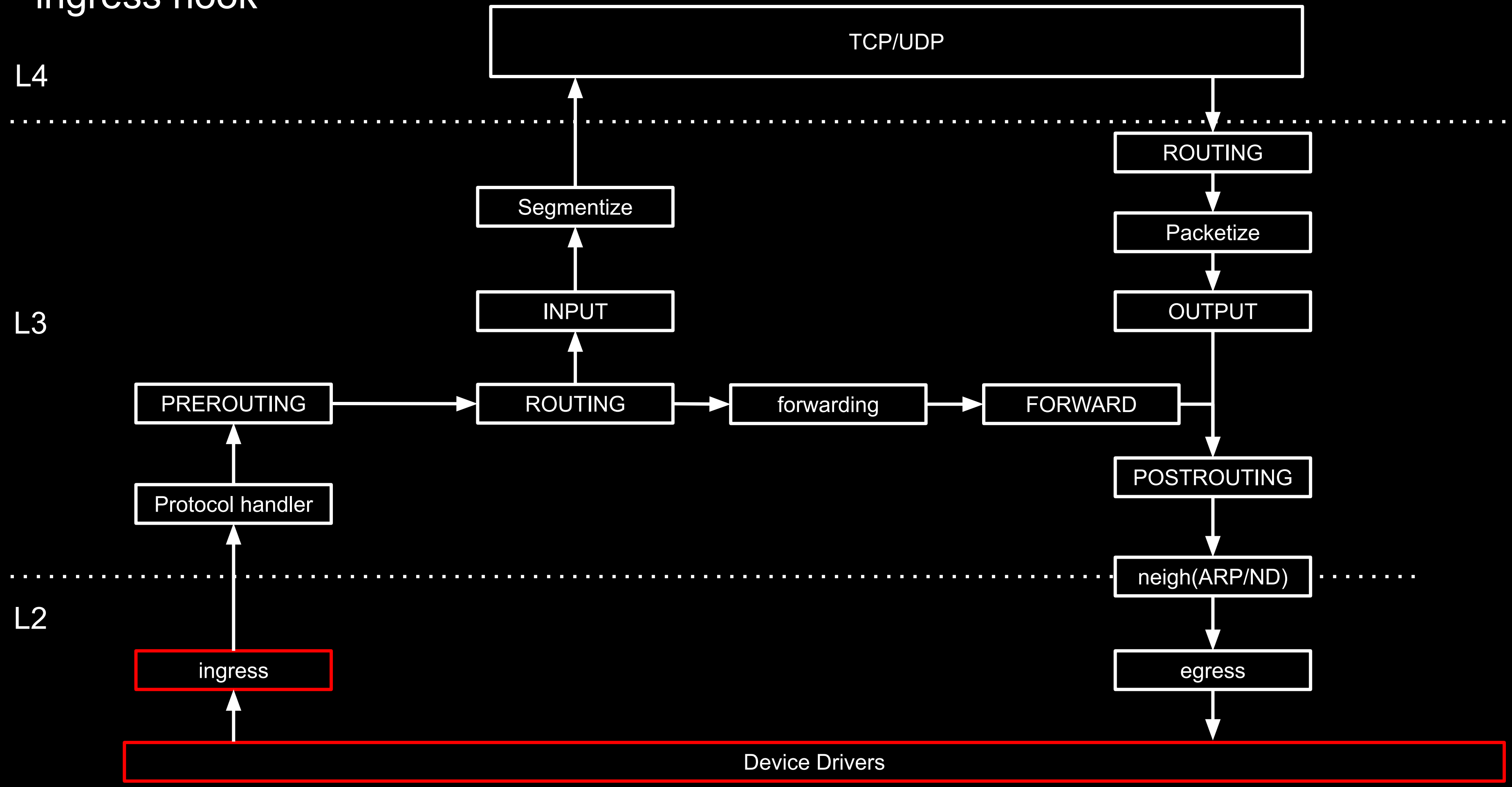
# Netfilter Packet-path



# Netfilter Packet-path



# ingress hook



L4

TCP/UDP

ROUTING

Segmentize

Packetize

L3

INPUT

OUTPUT

PREROUTING

ROUTING

forwarding

FORWARD

POSTROUTING

Protocol handler

neigh(ARP/ND)

L2

ingress

egress

Device Drivers

# Device Driver + ingress hook

- Netfilter ingress hook
- XDP
  - driver XDP (Device Driver)
  - generic XDP (L2 ingress hook)
  - bpfilter (Device Driver or L2 ingress)

# END