ROSE-HULMAN
INSTITUTE OF TECHNOLOGY

CSSE 490
Network Security

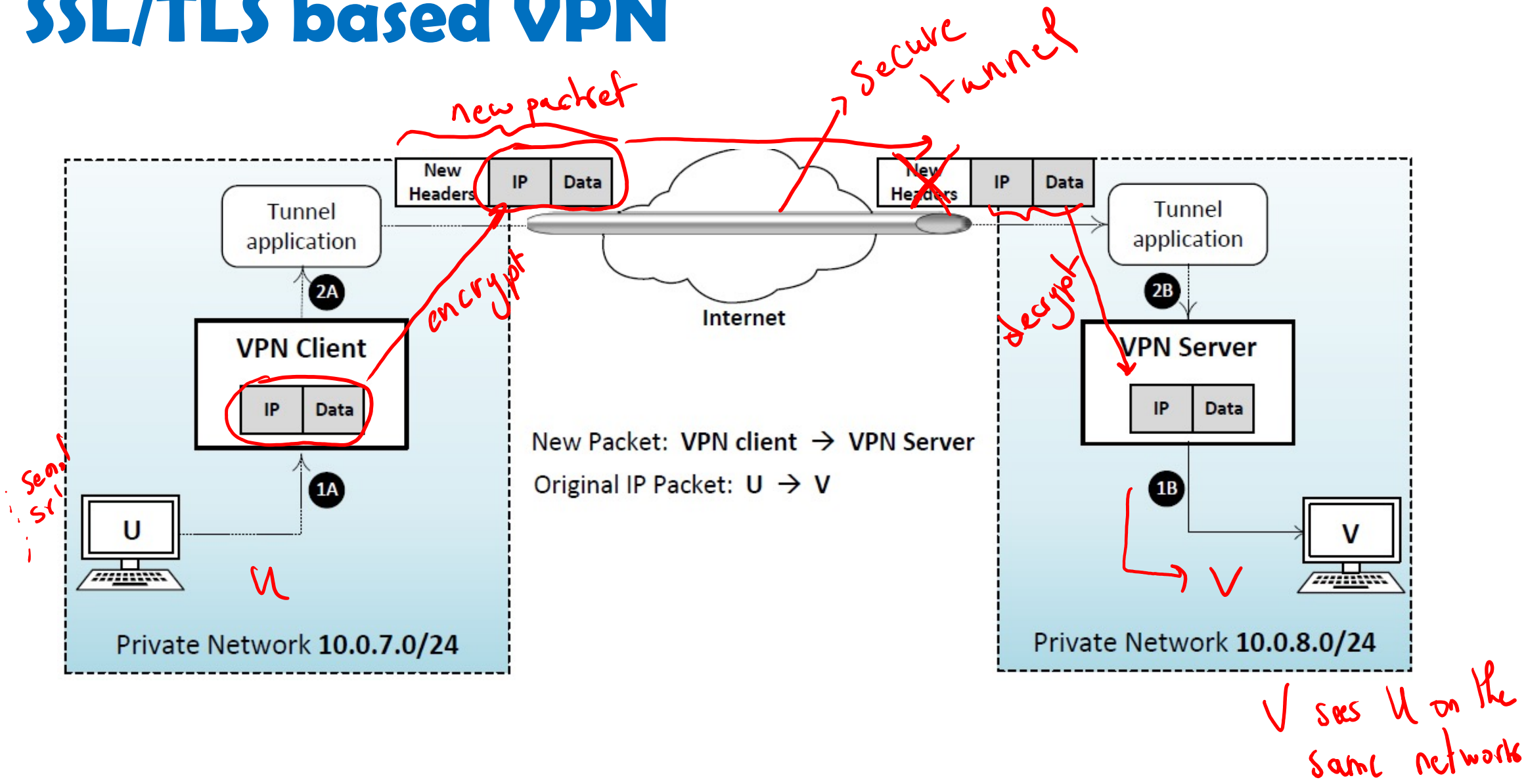
Day 29: Virtual Private Network II

Slides modified from slides designed by Professor Kevin (Wenliang) Du

Outline

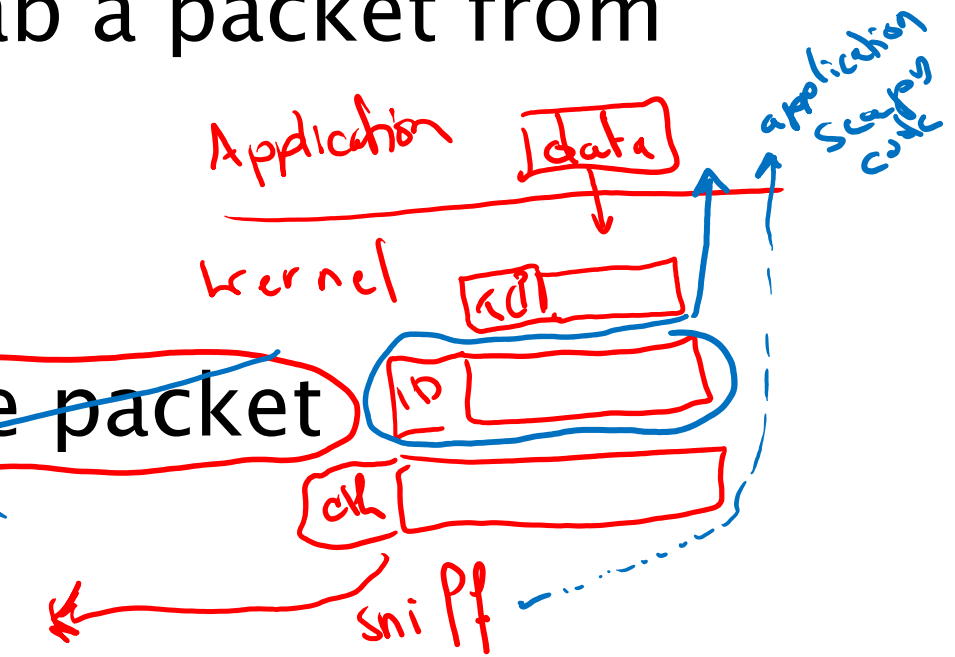
- Recap: SSL/TLS-based VPN
- Virtual interfaces
- VPN routing
- VPN path: from the sender
- VPN path: at the server
- VPN path: going back

SSL/TLS based VPN



VPN applications

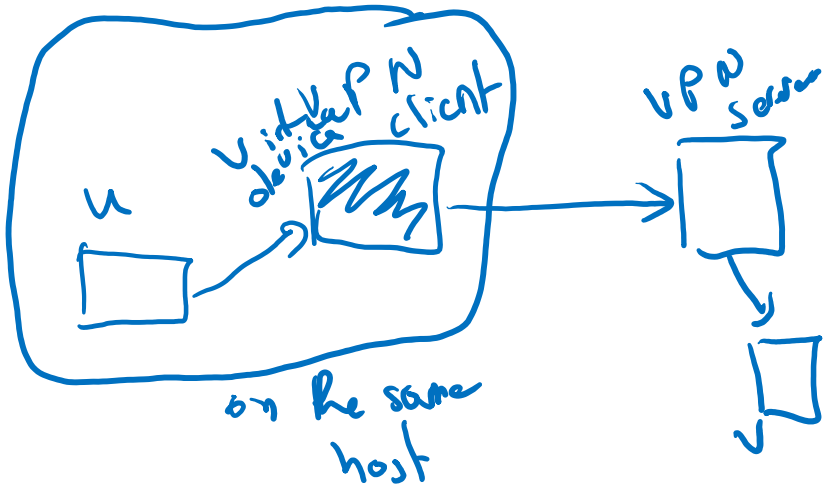
- But how can an application grab a packet from the kernel?



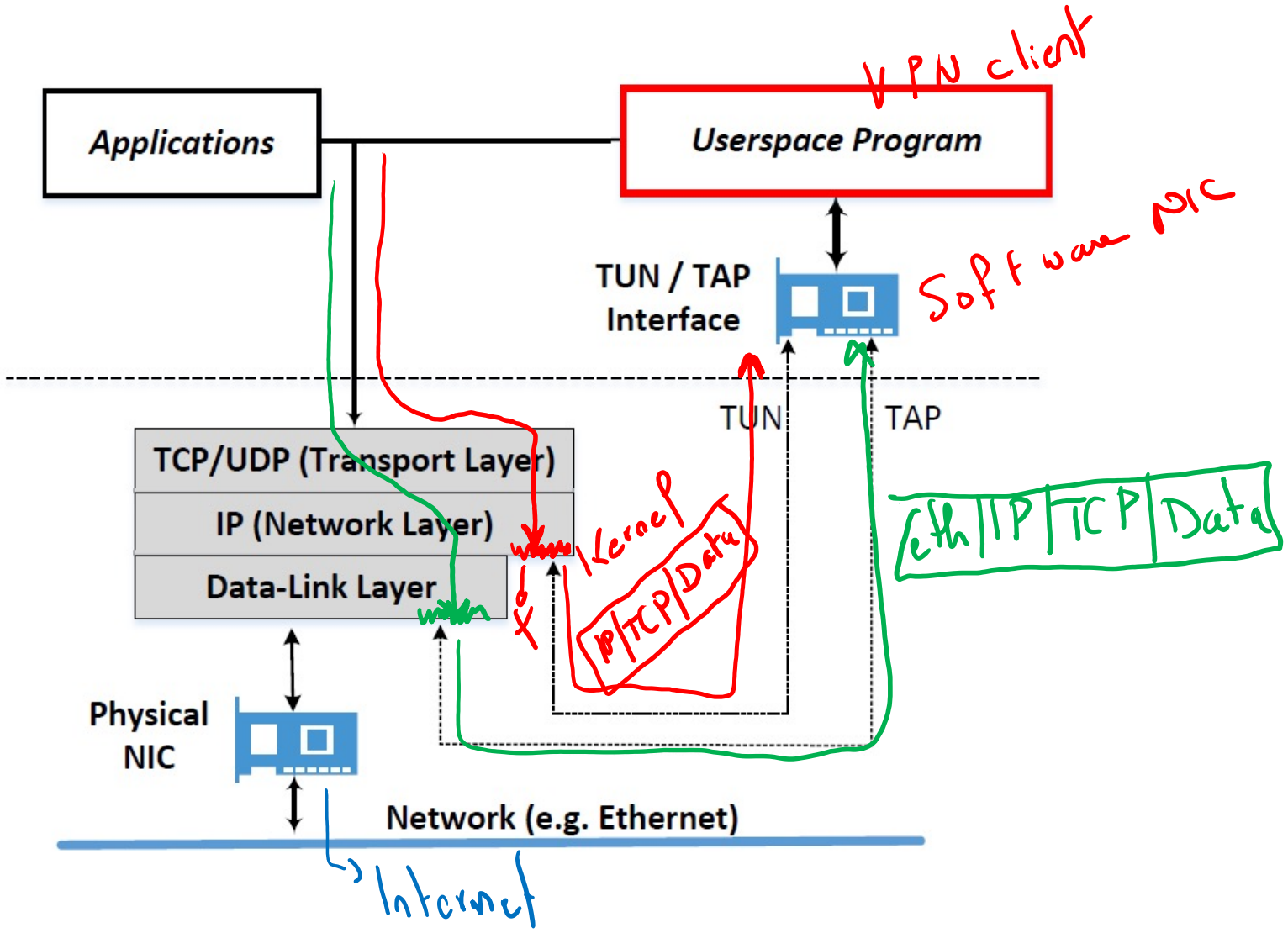
- Sniffing only gets a copy of the packet
- We need to interject into the path of the packet

Virtual interfaces

- **Inject** a device between the original host and the Internet
- This device is a **virtual device**
- Update **routing table** to route to the new device



TUN/TAP interfaces



TUN/TAP virtual interface

TUN virtual interface

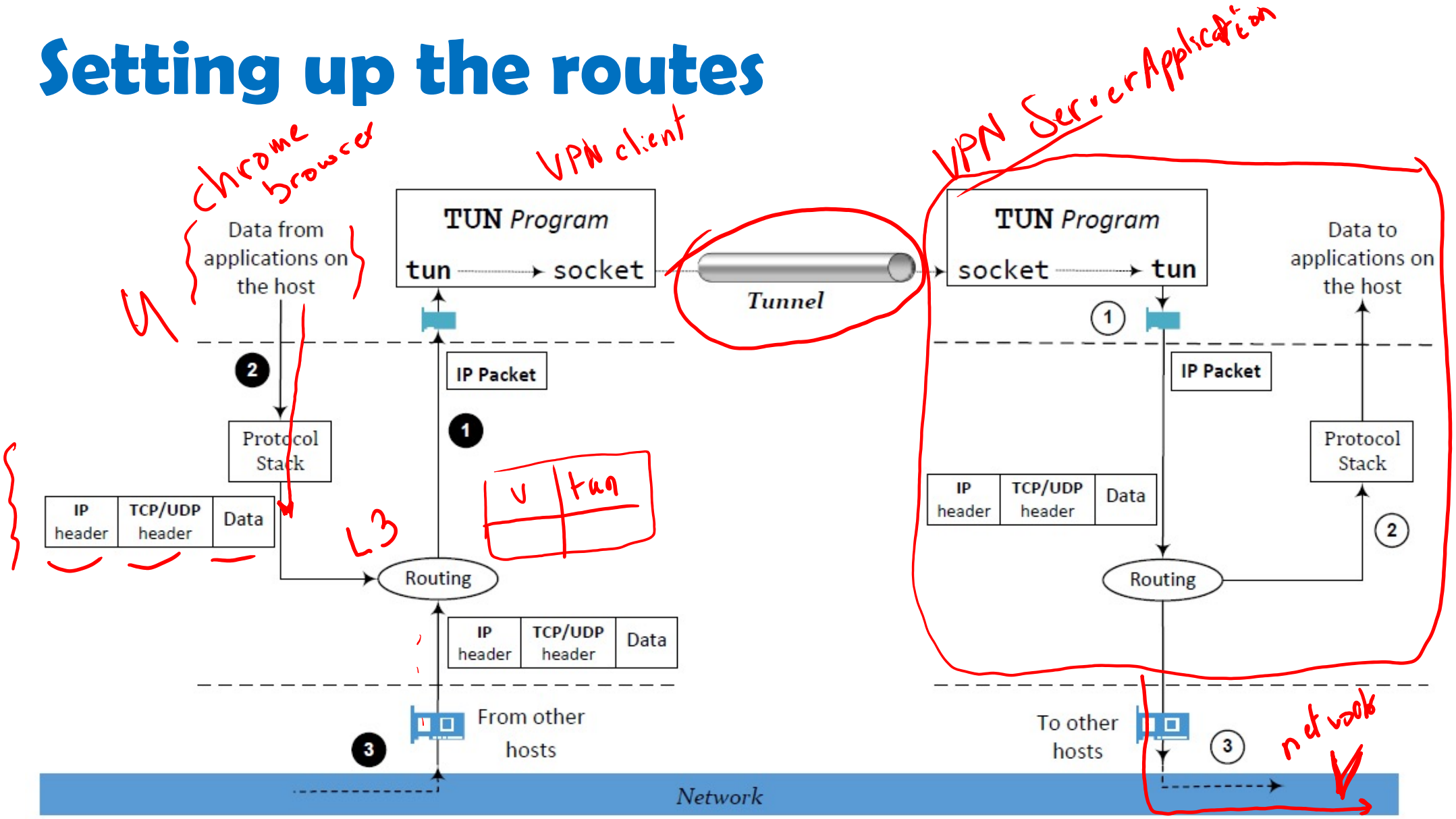
- Works at layer 3
- Sending packet to tun interface
  - get L3 packet to user application
- Need to update routing table

TUN/TAP virtual interface

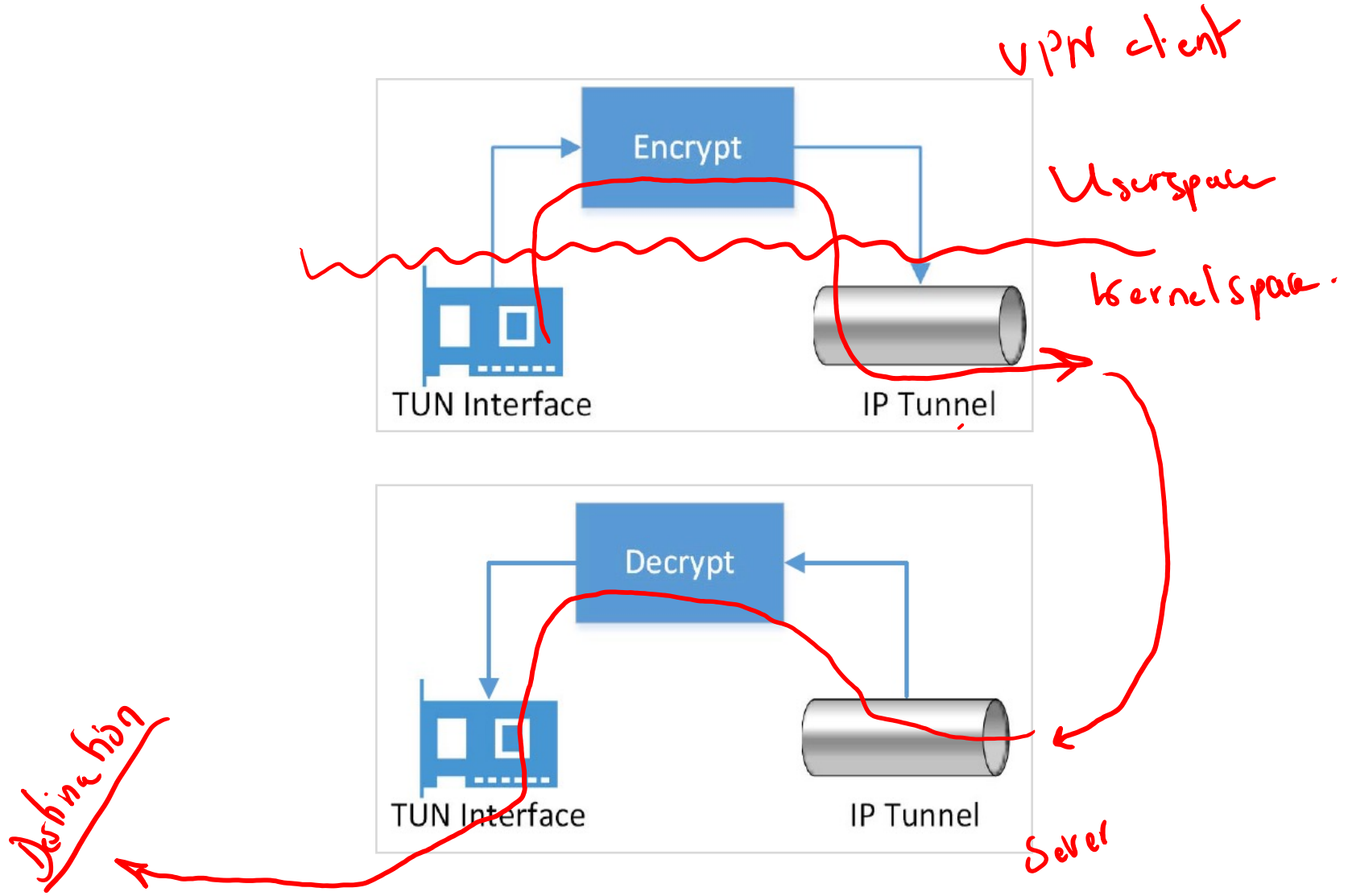
TAP virtual interface

- Works at layer 2
- Used to provide virtual adapters for virtualization

Setting up the routes

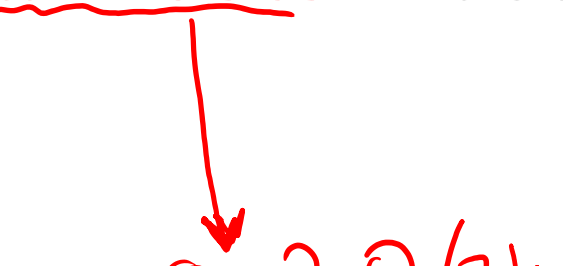


Looking closer



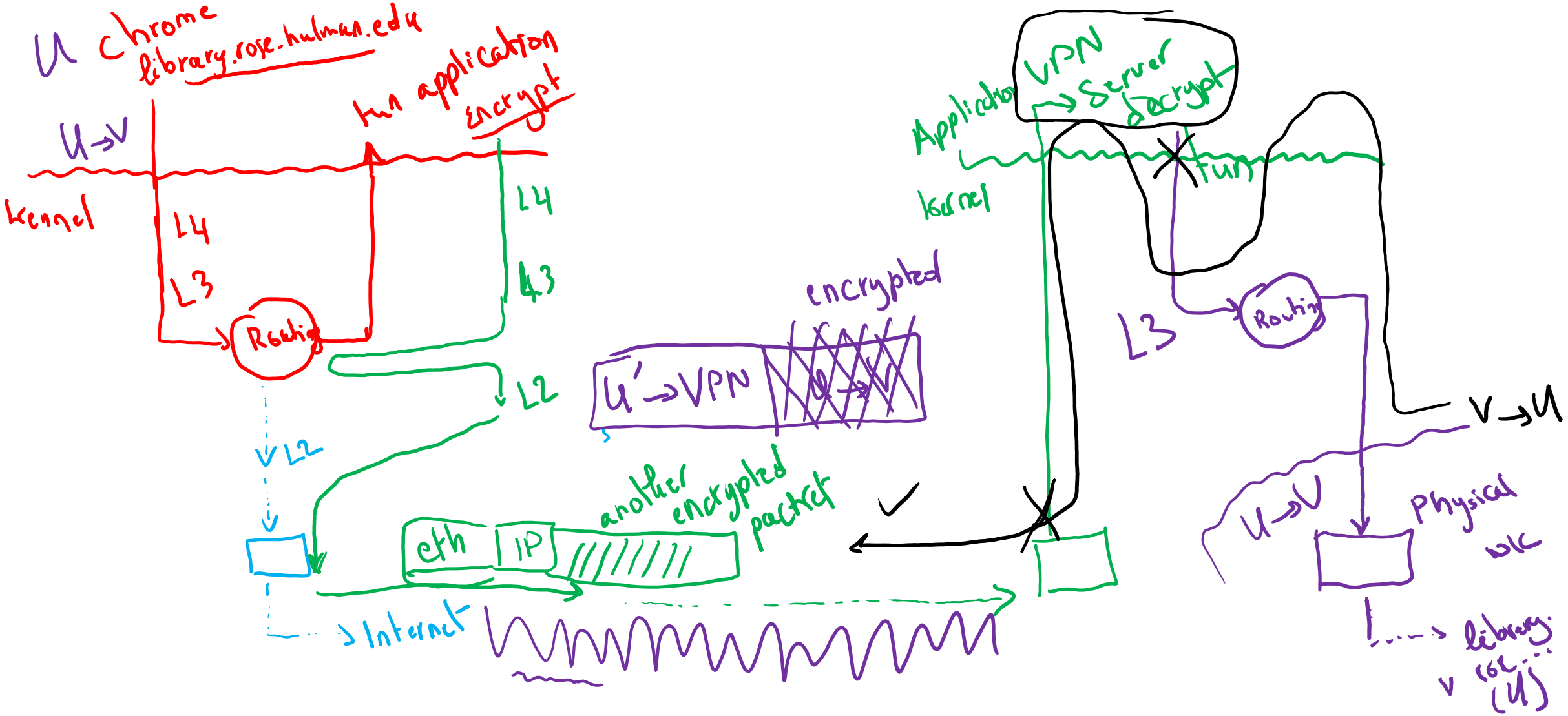
Routing table changes

- Must update the routing table ✓
- All traffic going to **internal hosts** must go to tun interface




```
sudo route add -net 10.0.0.0/24 tun0
```

Going to the private network



~~Returning to the sender~~ Listening to 2 interfaces.

```
pkt = select(                    );

if(pkt comes from tun)
    // client stuff: encrypt

else
    // decrypt
```