

# Raw Socket

Prof. Miguel Gomes Xavier

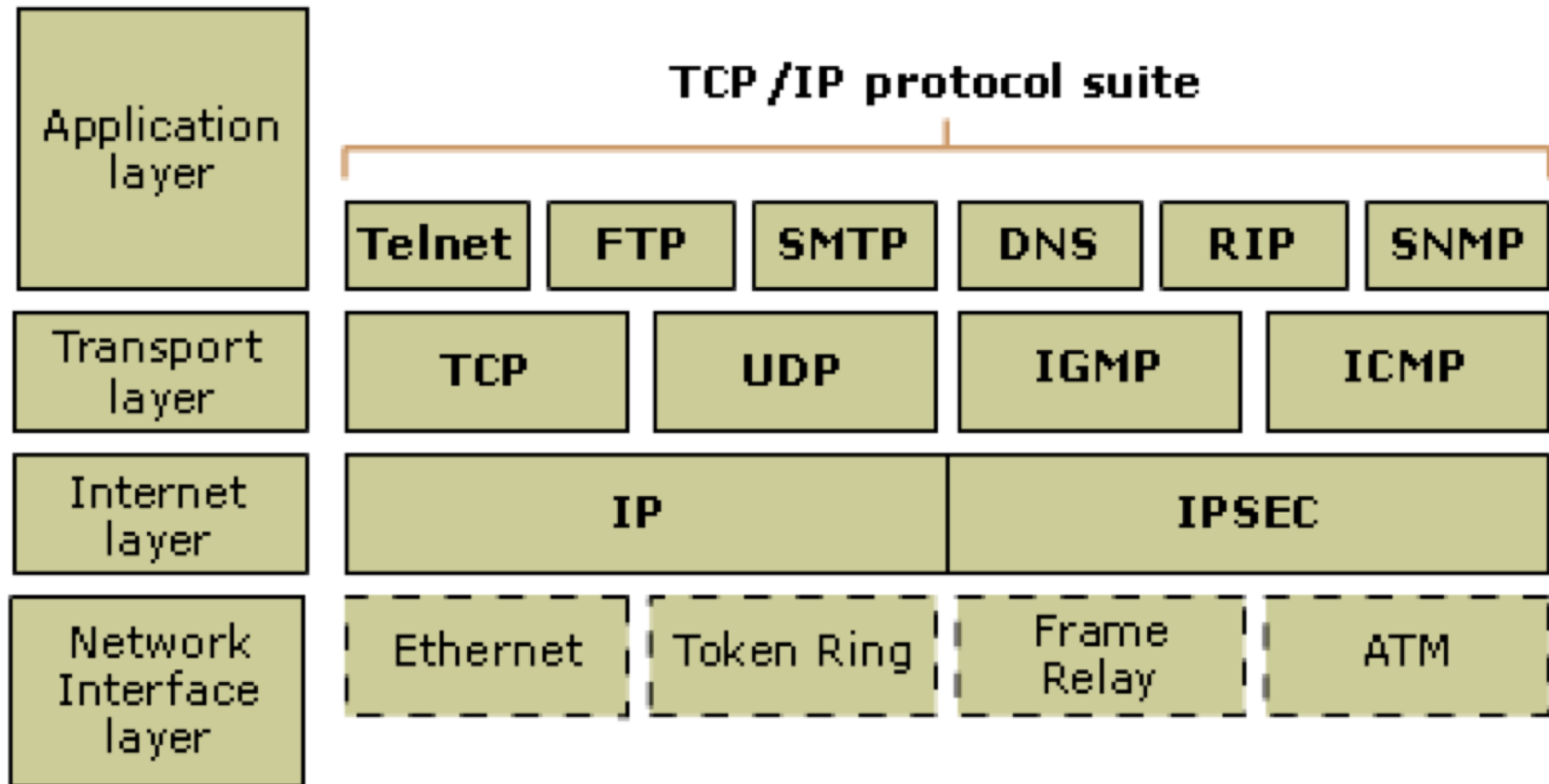
Miguel.xavier@pucrs.br

# O que é Socket Raw?

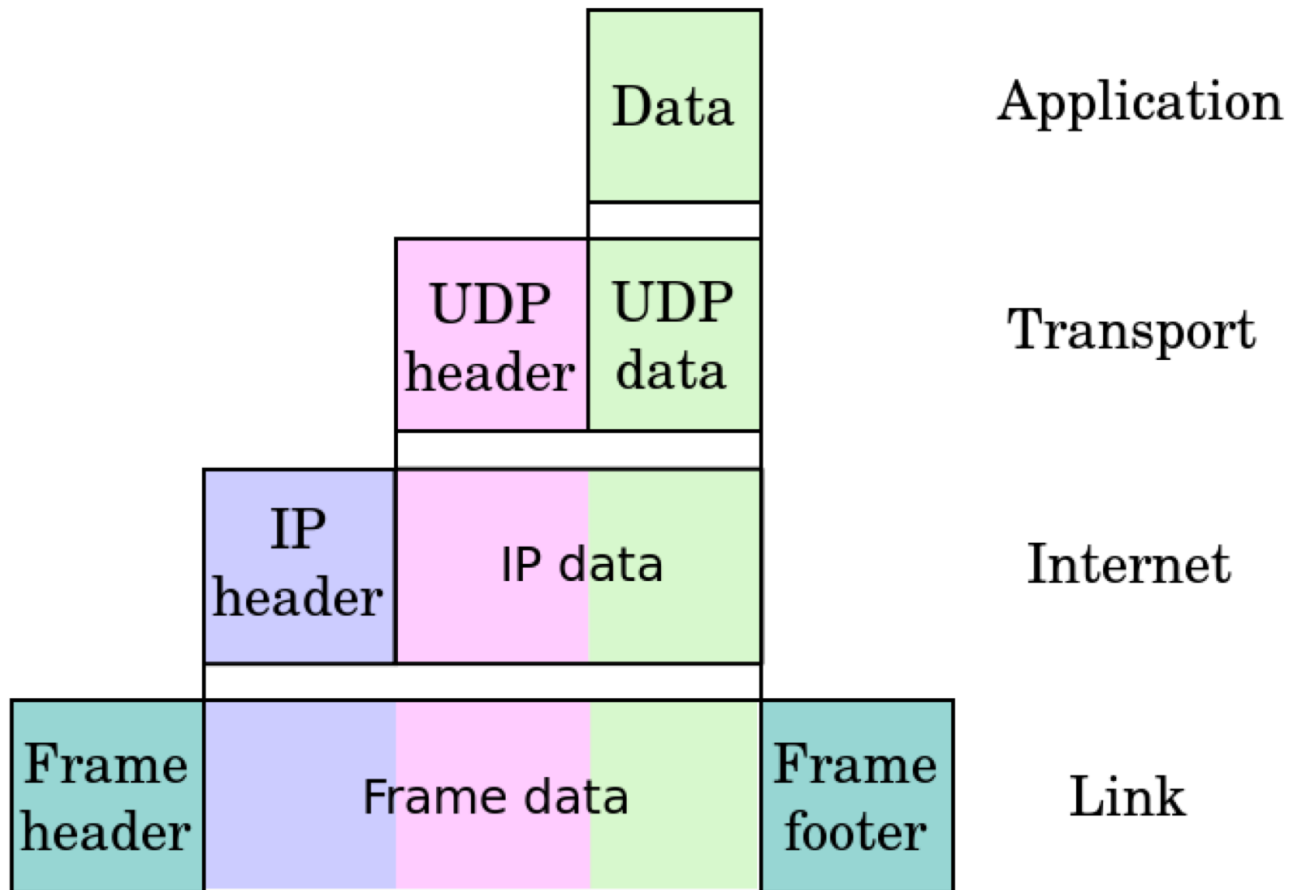
- É um mecanismo que permite o recebimento de pacotes de rede juntamente com seus cabeçalhos
  - raw = bruto, cru
- Normalmente o SO entrega somente o payload (dados) dos pacotes para aplicações específicas
- Com Socket Raw é possível analisar todo o tráfego recebido pela rede

# Pilha de Protocolos

## TCP/IP model

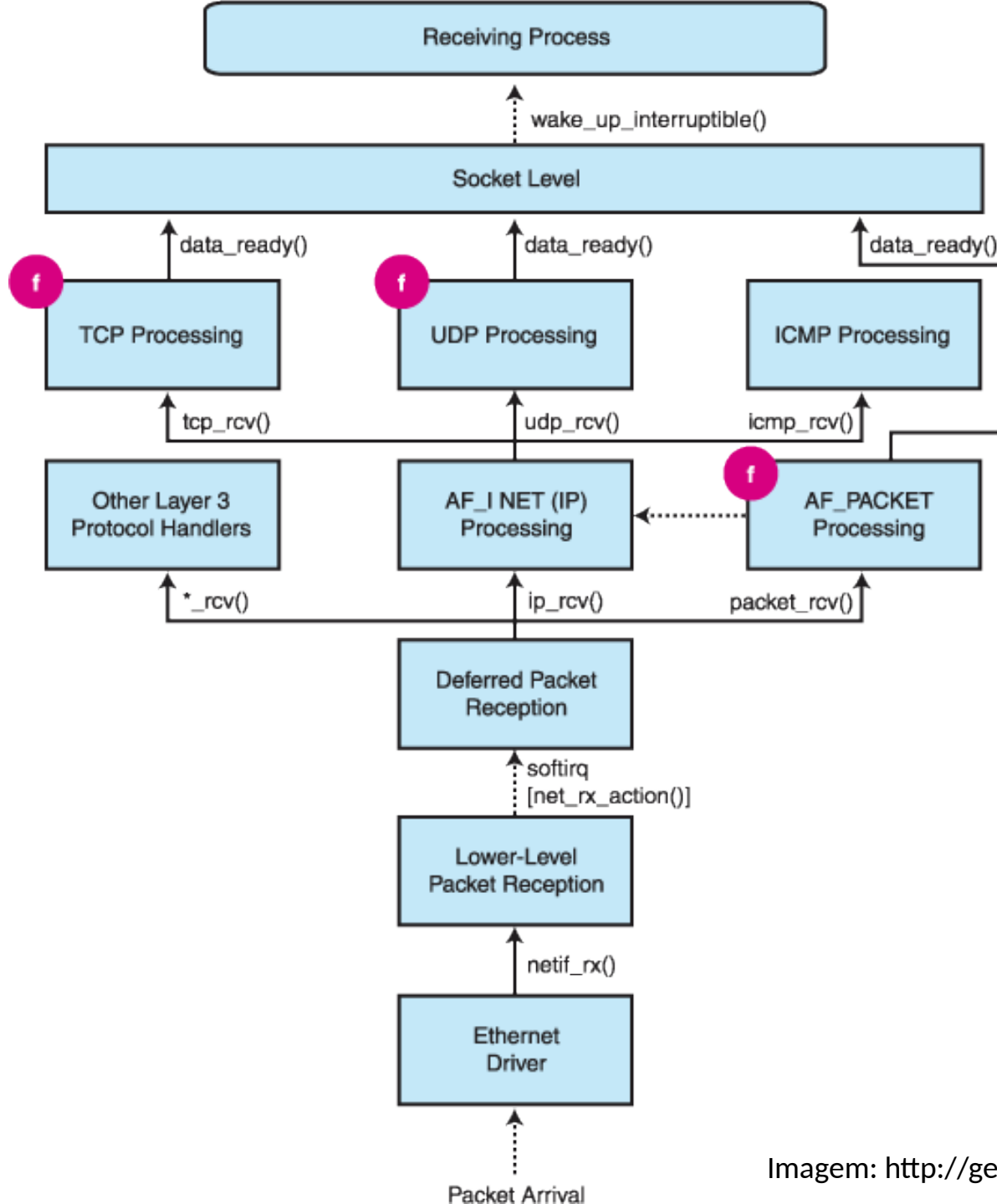


# Pilha de Protocolos



# Como funciona?

- `int socket(int domain, int type, int protocol);`
- **domain:** Protocol Family e/ou Address Family
  - protocolos são agrupados por similaridade
- **type:** Tipo de protocolo
  - subdivide o domínio em grupos com possivelmente mais de um protocolo
- **protocol:** Protocolo que será utilizado.



# Exemplos

- `int socket(int domain, int type, int protocol);`
- Socket TCP
  - `socket(AF_INET, SOCK_STREAM, 0);`
- Socket UDP
  - `socket(AF_INET, SOCK_DGRAM, 0);`
- Socket Raw:
  - `socket (AF_PACKET, SOCK_RAW, htons(ETH_P_ALL));`

# Exemplo de sniffer simples

```
/* Criação do socket */
```

```
fd = socket (PF_PACKET, SOCK_RAW, htons(ETH_P_ALL))
```

```
/* Colocar a interface de rede em modo promíscuo */
```

```
strncpy(ethreq.ifr_name, "eth0", IFNAMSIZ);
```

```
ioctl(fd, SIOCGIFFLAGS, &ethreq);
```

```
ethreq.ifr_flags |= IFF_PROMISC;
```

```
ioctl(fd, SIOCSIFFLAGS, &ethreq);
```

```
/* Ler os dados recebidos */
```

```
len = read (fd, buffer, buf_sz);
```



# Exemplo de envio/recebimento de quadros Ethernet

- Baixar exemplo disponível no Moodle
- Descompactar e compilar o código:
  - `tar xzf raw_socket_eth.tar.gz`
  - `cd raw_socket_eth`
  - `Make`
- Executar o programa de recebimento:
  - `sudo ./raw_eth_rcv eth0`
- Executar o programa de envio:
  - `sudo ./raw_eth_send eth0`

Obs: executar Wireshark para verificar o conteúdo dos quadros Ethernet enviados e recebimento