Linux Networking

LUG @ NC State
Quentin Young

Scope & Topics

- Focus: Networking from a user's POV
- Brief refresher on OSI
- Interfaces
- Routing table
- Iptables
- Network namespaces

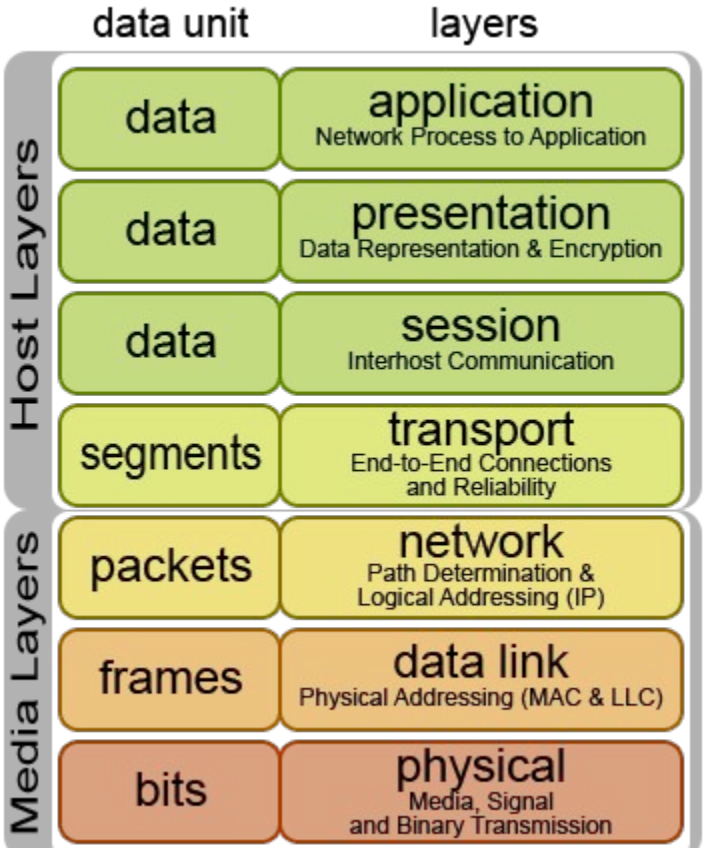
OSI Model

OSI = Open Systems Interconnect

Just a convenient way of organizing and abstracting network layers.

We are primarily interested in layers 2 and 3 (L2, L3)

Specifically Ethernet and IP



Interfaces

- Interfaces are the core unit of everything to do with networking in Linux
- Usually each hardware interface (NIC) has a software interface
    - But not vice versa!
- All traffic that flows in and out of a Linux box is associated at some point or another with an interface
- Bluetooth devices, wifi adapters, Ethernet adapters all get interfaces
- Tunneling & vpn is done via special interfaces
- Static IP, DHCP, up/down, bridges, getting information
- On most distros, this is all handled by the GNOME tool NetworkManager

Terminal session!

Routing table

- Each time a packet is sent, the kernel must decide where to send it (L3)
- This is done by maintaining a lookup table that maps destination to next hop (L3 & L2)
  - In industry parlance this is called the “RIB” = Routing Information Base
- The same table maps the next hop to an interface
  - There is also a separate table called the “FIB” = Forwarding Information Base
- Routing / forwarding tables are easy to examine under Linux!
  - /proc/net/fib_trie

Terminal session!

iptables

```
vagrant@frrdev /p/2/net> sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
```

feeling a bit promiscuous

Or, “where is that stackoverflow post with the iptables nat rule...”

- iptables is a userspace program that controls the kernel’s firewall
- Extremely powerful, it can
  - Block and allow connections
  - Rewrite packets on the fly
  - Reroute packets on the fly
  - Perform very fine-grained pattern matching
  - Enforce very fine-grained policy
- Succeeded by nftables
  - I don’t know how to use nftables so I didn’t cover it

Terminal session! :(

DNS

Or, “why is my resolver set to Time Warner again”

- On Linux, DNS settings are controlled by /etc/resolv.conf
- This is almost always somewhat false
- DNS settings can be sourced from countless places
- NetworkManager, systemd-resolvd, resolvconf, dnsmasq, dhcp...it’s a mess
- But let’s take a look…

Terminal session!

Network namespaces

Or, “I’m not confused enough”

- Anyone familiar with process namespaces (commonly referred to as ‘Docker’)?’
- Network namespaces are like process namespaces...but…for the network :-)
- Essentially allows you to create isolated copies of the network stack
- Namespaces have their own interfaces, routing tables, iptables rules, etc
- Often used for virtualization

Terminal...uh….