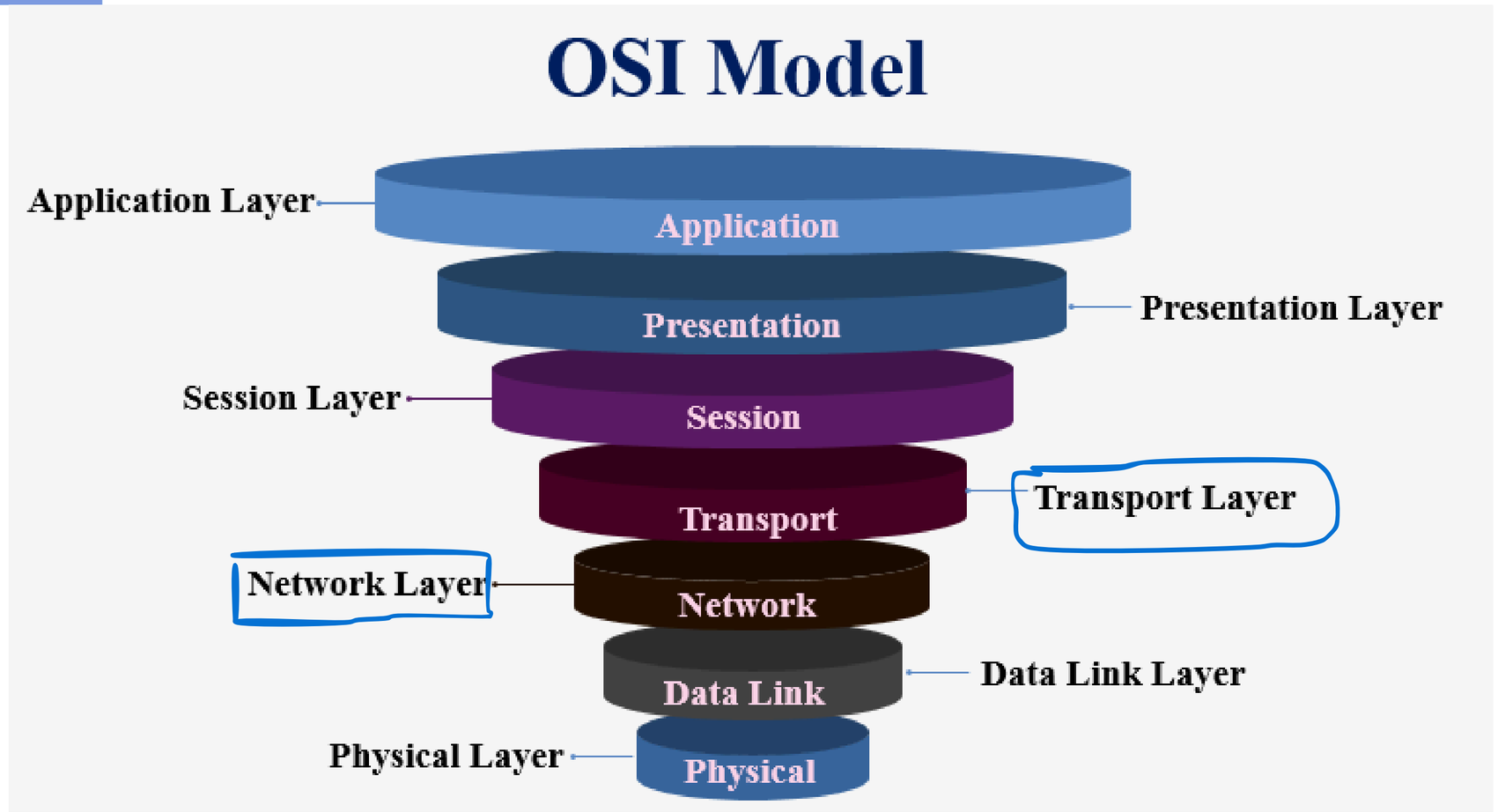
Tutorial-3
Networks

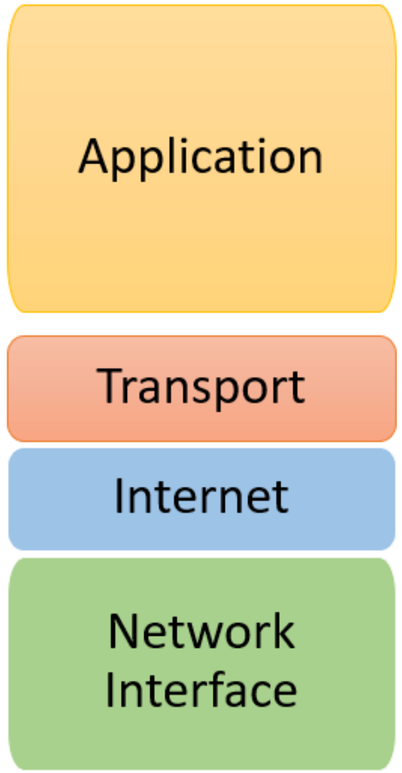
Brief Recap

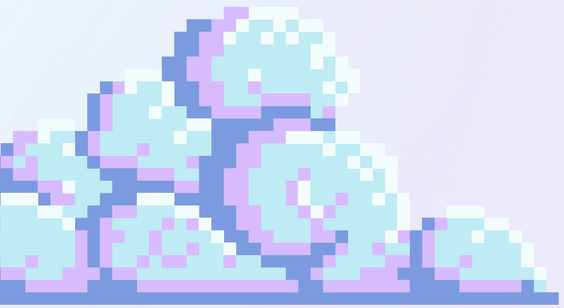
Network Stack



Network Stack

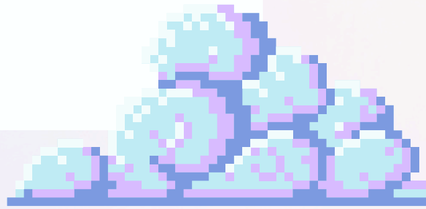
TCP/IP Model

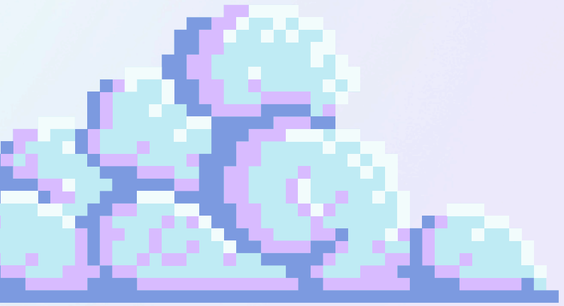




IP Address

- IP (Internet Protocol) address is used to determine the source and destination at **Network** layer for end-to-end delivery.
- Two types of addresses: IPv4 and IPv6
- IPv4 address is 32 bits: 4 octets of 8 bits
  Range: (0.0.0.0 to 255.255.255.255)
- IPv6 is newer and uses 128 bits(8 octets of 16 bits).
  (Range: 0000:0000:0000:0000:0000:0000:0000:0000
  to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff)
- These addresses are not permanent and can change.

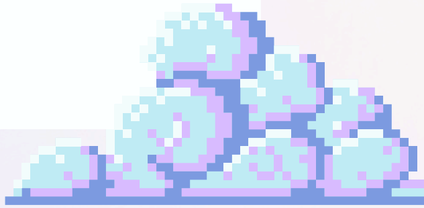




Take-home

Public IP addresses are not unique — all your devices on the same network use your router (or gateway)'s public IP, and you only know others' public ones. Then

1. How do you uniquely identify destinations?
2. If IP addresses don't solve this issue, why use them in the first place?



Transport Layer Protocols

TCP
(Transmission Control Protocol)

- Most popular protocol
- Connection-oriented (sender and reciever both know each other)
- Has a bigger header due to more info (>=20 bytes).

UDP
(Unified Datagram Protocol)

- Connectionless (reciever and sender don't know each other).
- Has a small header (8 bytes).
- Better choice when streaming or transferring a lot of data.

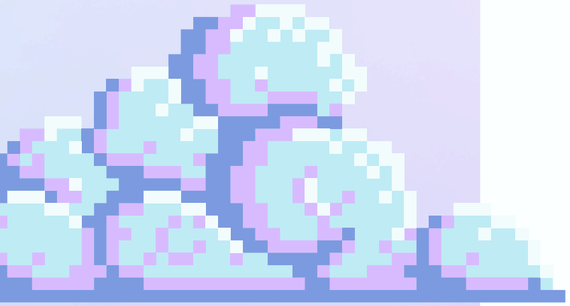
REMINDER!

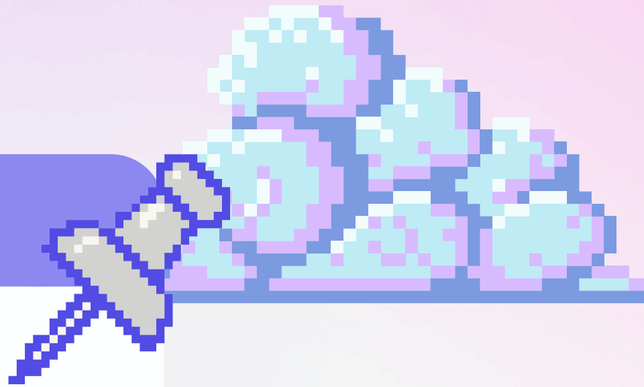
Install Wireshark if you haven't done so yet.

CONTINUE

Basic Network Commands

- The terminal can be used to execute a lot of useful network commands.
- Lets see some basic ones.





CODE ALONG!

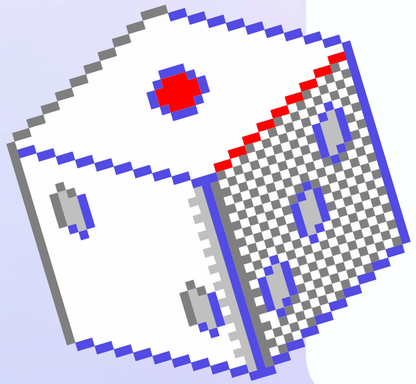
Run the commands on your own terminal

IFCONFIG

- Lists all available network interfaces (don't worry if you don't know what they are yet).
- Also lists properties such as IPv4, IPv6 and data transferred and received.

Syntax: ifconfig

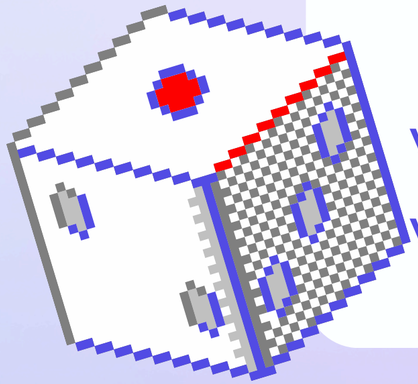
(ipconfig on Windows)



VNSTAT

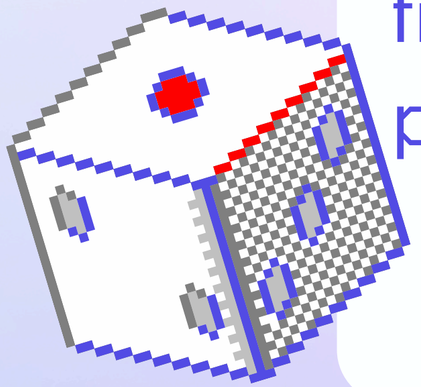
- Install using: sudo apt install vnstat (use macports for Mac)
- Used for monitoring network traffic
- Syntax:

vnstat -tr [time_in_seconds] -i [interface_name]
vnstat -l -i [interface_name]



NETCAT

Used for hosting a server/talking as a client from the terminal. Can send UDP and TCP packets.



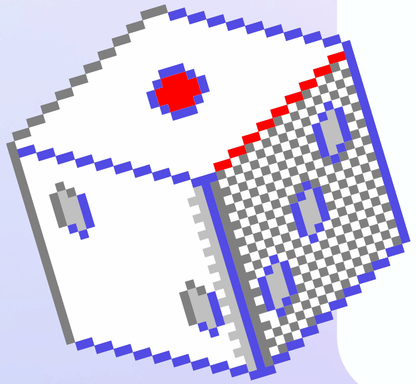
NETCAT SYNTAX

Setting up a server:

- nc -l [-k] <port> (for tcp)
- nc -l -u [-k] <port> (for udp)

Connecting as client:

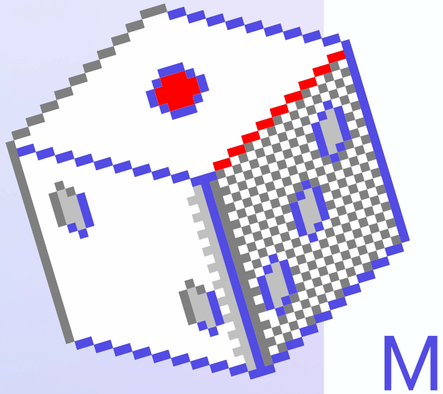
- Omit the -l flag
- nc [-u] <ip> <port>



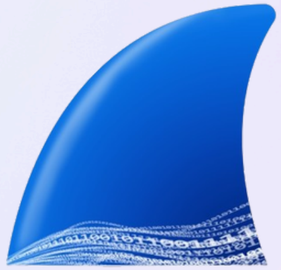
HOST

- Find info about websites/IPs like alternate IP addresses, who is managing their mail, etc.

Syntax: host [IP/domain]



More useful commands: traceroute, ping



Wireshark

what's wireshark

Sources

Chapter 1. Introduction - Wireshark	What is Wireshark? | Definition from TechTarget	About Wireshark	
wireshark · 1	techtarget · 2	wireshark · 3	View 2 more

Answer

Wireshark is a powerful, open-source network protocol analyzer widely used for capturing and analyzing network traffic. It enables users to see what's happening on their networks at a detailed level, making it an essential tool for network troubleshooting, protocol analysis, and security monitoring.

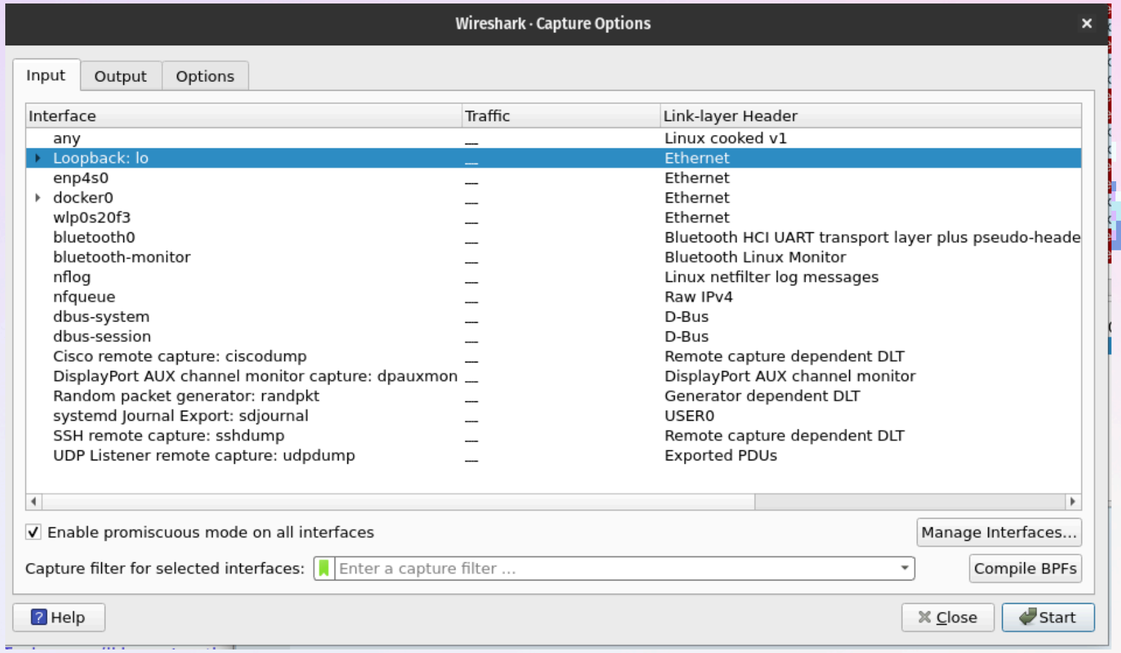
Key Features

- **Packet Capture**: Wireshark captures network packets in real-time, allowing users to inspect the data being transmitted over the network. It supports various media types, including Ethernet, Wi-Fi, and USB.
- **User Interface**: The application features a graphical user interface (GUI) that displays captured packets in a structured format. It typically presents information in three panels: a list of packets, detailed packet information, and a raw data view.
- **Filtering and Analysis**: Wireshark provides advanced filtering capabilities, enabling users to focus on specific types of traffic. This feature is crucial for diagnosing network issues and analyzing security threats.

Running Wireshark

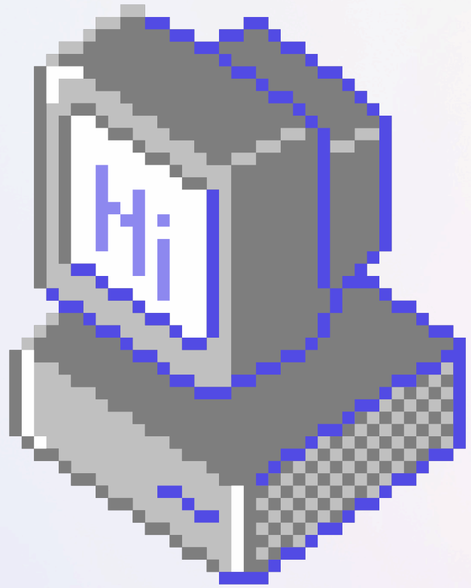
```
# while installing, you'll see a message box. click YES and then run:
sudo usermod -a -G wireshark <your_username>

# when you try to run wireshark, you may be told that there is an
# error executing  <some_path_i_forgot>
sudo chmod +x  <that_path>
```

Interfaces in Wireshark



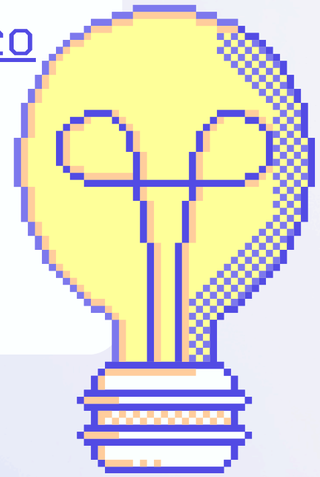
For now, you can think of these as being analogous to devices/ways of connecting to the internet e.g. bluetooth, ethernet, USB, WLAN, etc.

Today, you'll be using the 'any' and 'Loopback' (to see packets you send to yourself) interfaces.



Further Resources

1. https://beej.us/guide/bgnet/
2. https://www.devdungeon.com/content/using-libpcap-c



Thank you!