

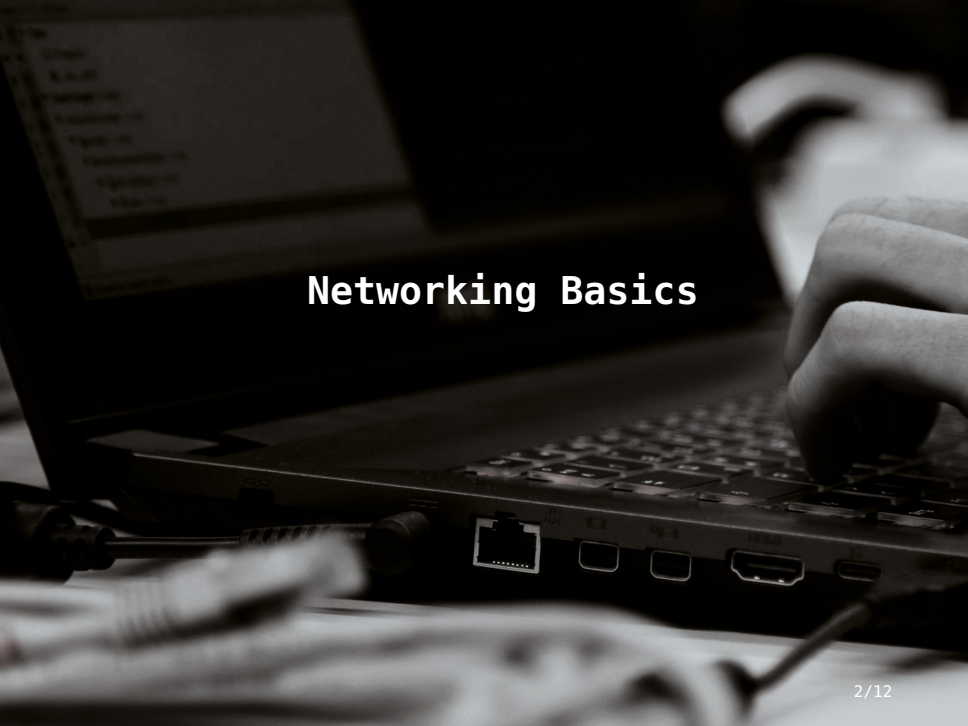


Network

Michael Preisach

May 17 2019

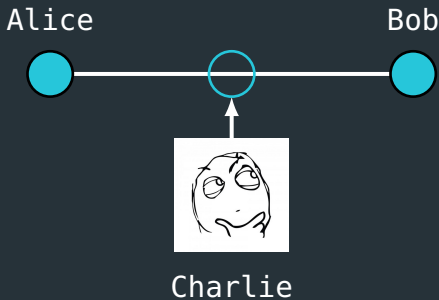
Networking Basics

A black and white photograph of a person's hand typing on a laptop keyboard. The laptop screen is visible in the background, showing some text. The text 'Networking Basics' is overlaid in the center of the image.

Networking Basics



- How do you get the traffic between Alice and Bob?



Networking Basics



- Alice and Bob are connected directly:
 - Use two bridged interfaces on your computer and connect them to Alice and Bob
- Alice and Bob are connected via a hub
 - Just plug in to one port of the hub



Networking Basics



- Alice and Bob are connected via a switch:
 - Managed switch: Mirror the port of either Alice or Bob to Charlie
 - Unmanaged switch: use a managed switch



Networking Basics



- How do you capture the traffic?
 - tcpdump (CLI)
 - Wireshark (GUI)

Example: Capturing traffic from eth0

```
sudo tcpdump -i eth0 -w capture.dump
```

Wireshark

A black and white photograph of a person's hand typing on a laptop keyboard. The laptop screen is visible in the background, showing some text. The word 'Wireshark' is overlaid in the center of the image in a white, sans-serif font. The laptop's ports, including a USB port and a FireWire port, are visible on the side.



- How do you capture the traffic?
 - tcpdump (CLI)
 - Wireshark (GUI)

Example: Capturing traffic from eth0

```
sudo tcpdump -i eth0 -w capture.dump
```


A black and white photograph of a person's hands typing on a laptop keyboard. The laptop screen is visible in the background, showing a list of items. The word "Wireshark" is overlaid in white text in the center of the image. The laptop's ports, including a USB port, a FireWire port, and a Thunderbolt port, are visible on the side.

Wireshark



- Find the interesting parts in a dump: Filter packets
 - tcpdump (CLI)
 - Wireshark (GUI)

Example: Capturing traffic from eth0

```
sudo tcpdump -i eth0 -w capture.dump
```