Resources:
https://en.wikipedia.org/wiki/OpenFlow
https://www.sdxcentral.com/networking/sdn/definitions/what-is-openflow/
https://blog.ipspace.net/2016/12/q-vendor-openflow-limitations.html
- See slides from 9/17 (Chapter 1 Introduction to OpenFlow)

https://oswalt.dev/2011/06/introduction-to-openflow/
https://www.youtube.com/watch?v=t7ElZz417mw
https://www.youtube.com/watch?v=l25Ukkmk6Sk

Advantages of OpenFlow:
- One manager for different hardware (unless virtualized env), such as switches
- Simple & efficient
- Scalable, can perform tasks on a defined group, effectively altering behavior for multiple packets
- Solves the issue of many MAC addresses
- Virtualizes network for cloud as layers of software
- Provides consistency for traffic management by separating controls from hardware
- Offers centralization by requiring less manpower to run, therefore reducing cost
- Self-healing, can manage when some nodes/links fail

Disadvantages of OpenFlow:
- Difficult (not impossible) to change IP addresses / port numbers if you want to use NAT / PAT to translate private IP:port to public IP:port
- A PC cannot provide the same performance that a device meant to handle network infrastructure will (not enough ports or packet performance)
- Not old enough (released in 2011) so not reliable as a out of the box fully tested product
- Implementation of OpenFlow is up to vendors, so its potential may not be good depending on who creates it.
- Centralization increases security risk by lowering the cost to attack the network, requires switch-controller encryption w/ SSL, self signed certificates to authenticate switch & controller. Also may requires rules on ingress to avoid DoS