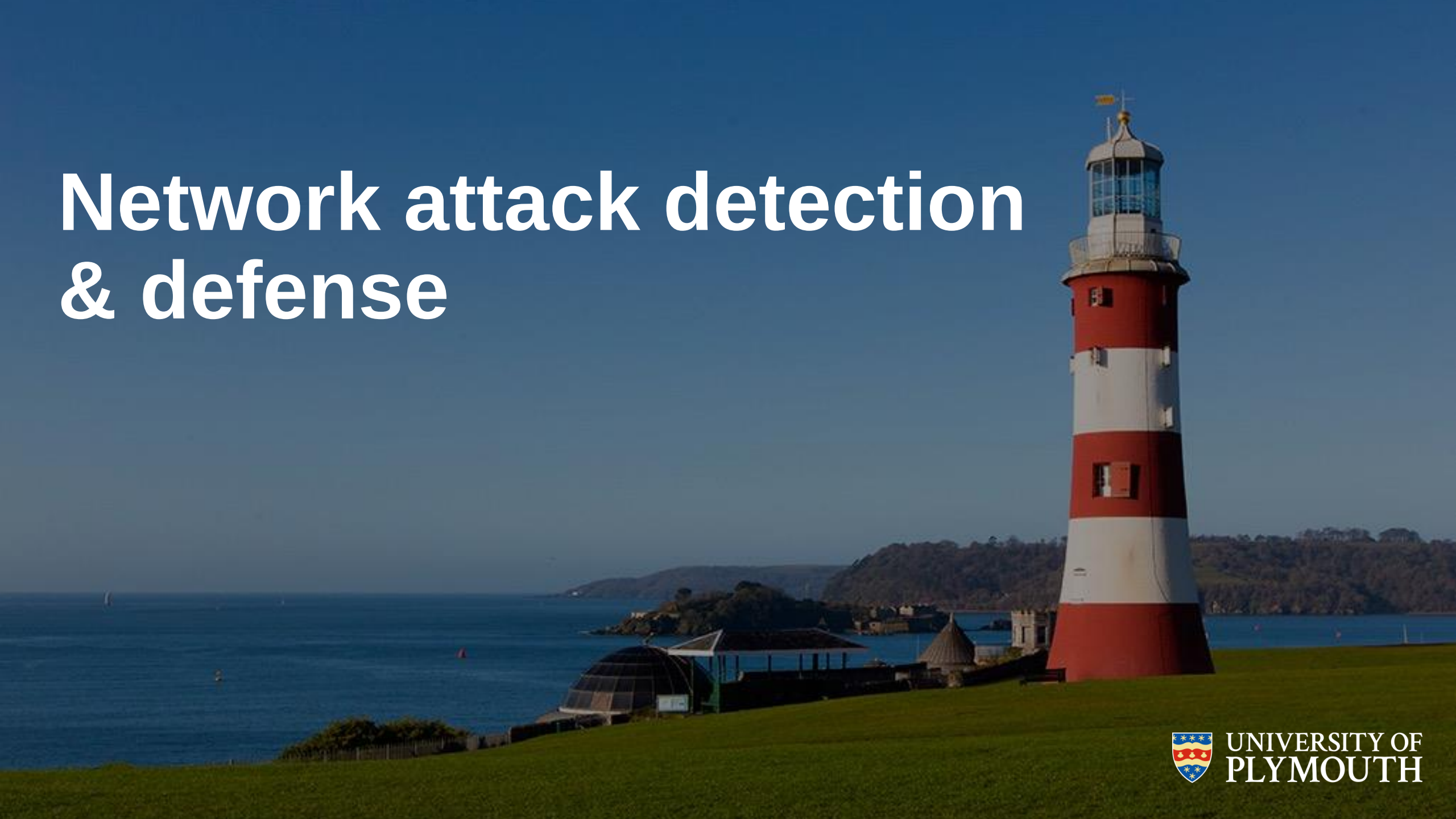
Network attack detection & defense



UNIVERSITY OF PLYMOUTH

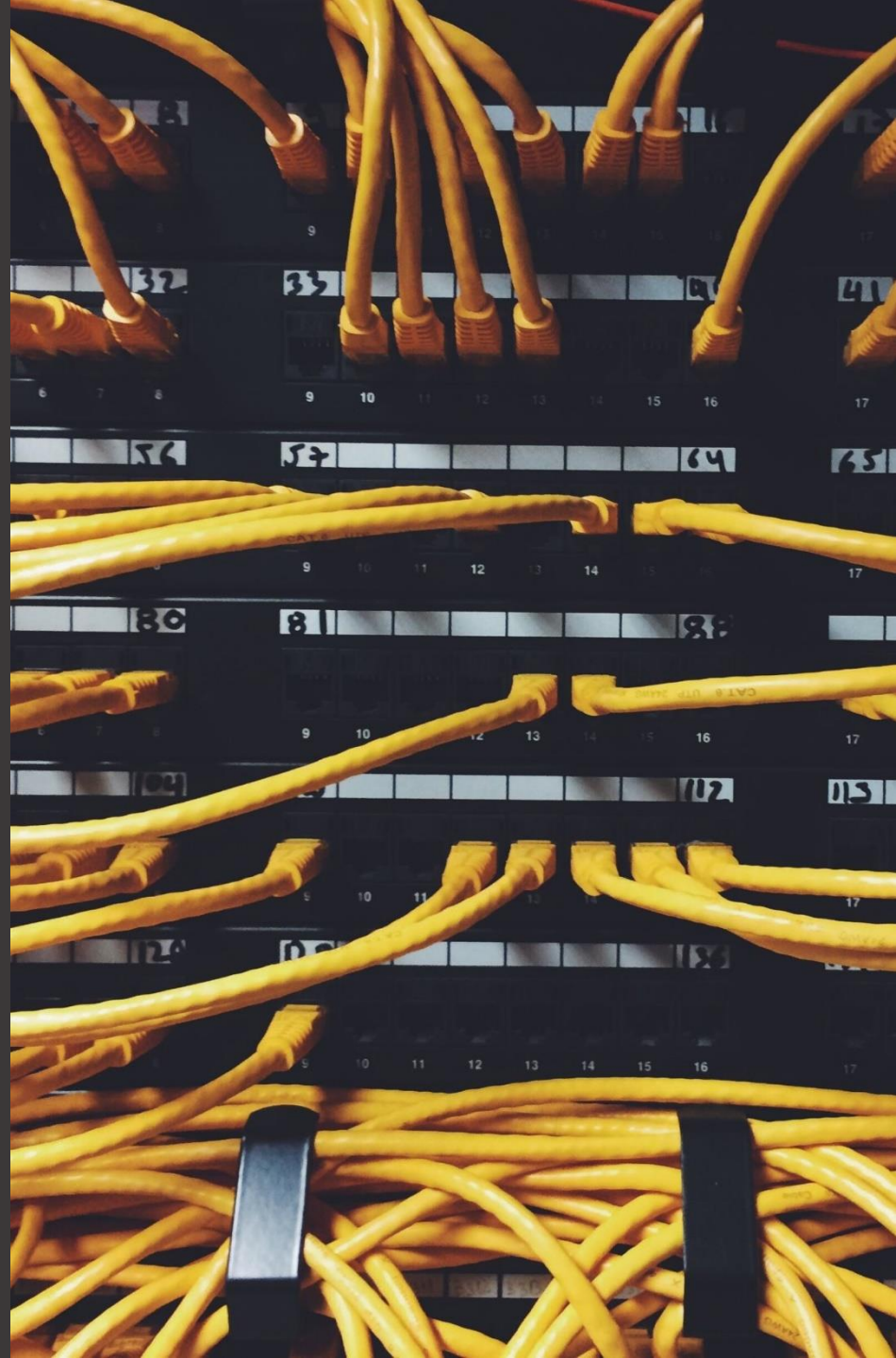
Session Outline

- Authentication:
  - Denial of service attacks
  - Attack mitigation

- Tools for this session:
  - Linux router
  - VMWare Workstation or VMWare Player

Denial of Service attacks

- Mechanisms to deny legitimate users or hosts access to
  - A service
  - Network
  - Internet
- Mounted via a range of methods
  - Block access to network
  - Block access to Internet
  - Block access to a web server
  - Etc



Block access to the network - attack

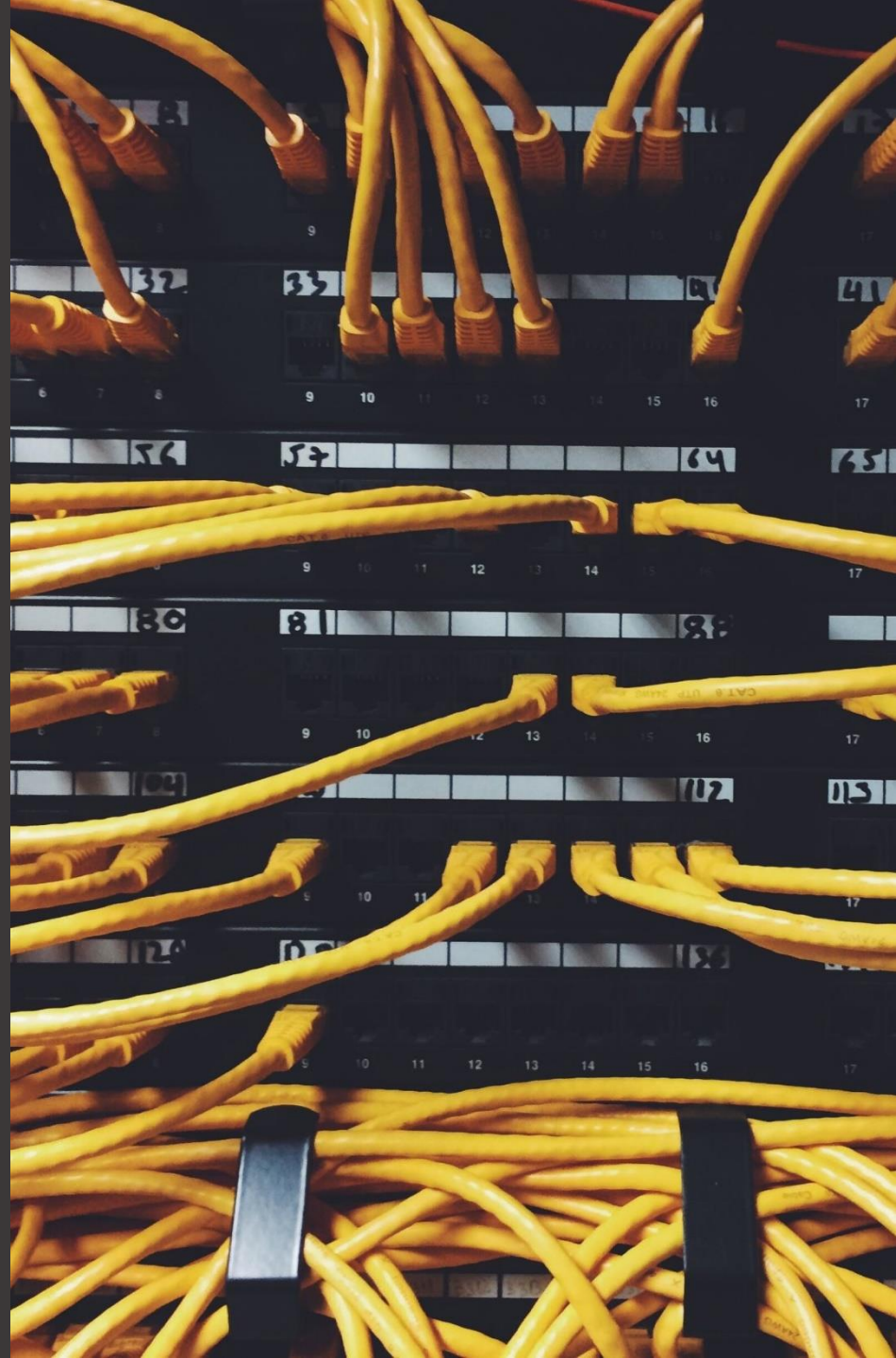
- One example – DHCP
  - Used by typical hosts to get an IP address and access the network
  - Based on a DHCP server that leases IP addresses from a pool
- Examples of attacks
  - Rogue DHCP server – server that connects to the network and leases IP addresses in the wrong range
  - DHCP starvation attack – attacker that uses up all the IP addresses in the DHCP server pool
- Detection – clients do not get an IP address or get a “wrong” IP address and cannot connect to the Internet

Block access to the network - mitigation

- Rely on switches

- Allow DHCP only from recognised ports
  - Block DHCP traffic from other ports

- Allow only a limited number of MAC addresses on each port
  - Attackers cannot spoof large number of MAC addresses to starve the DHCP server

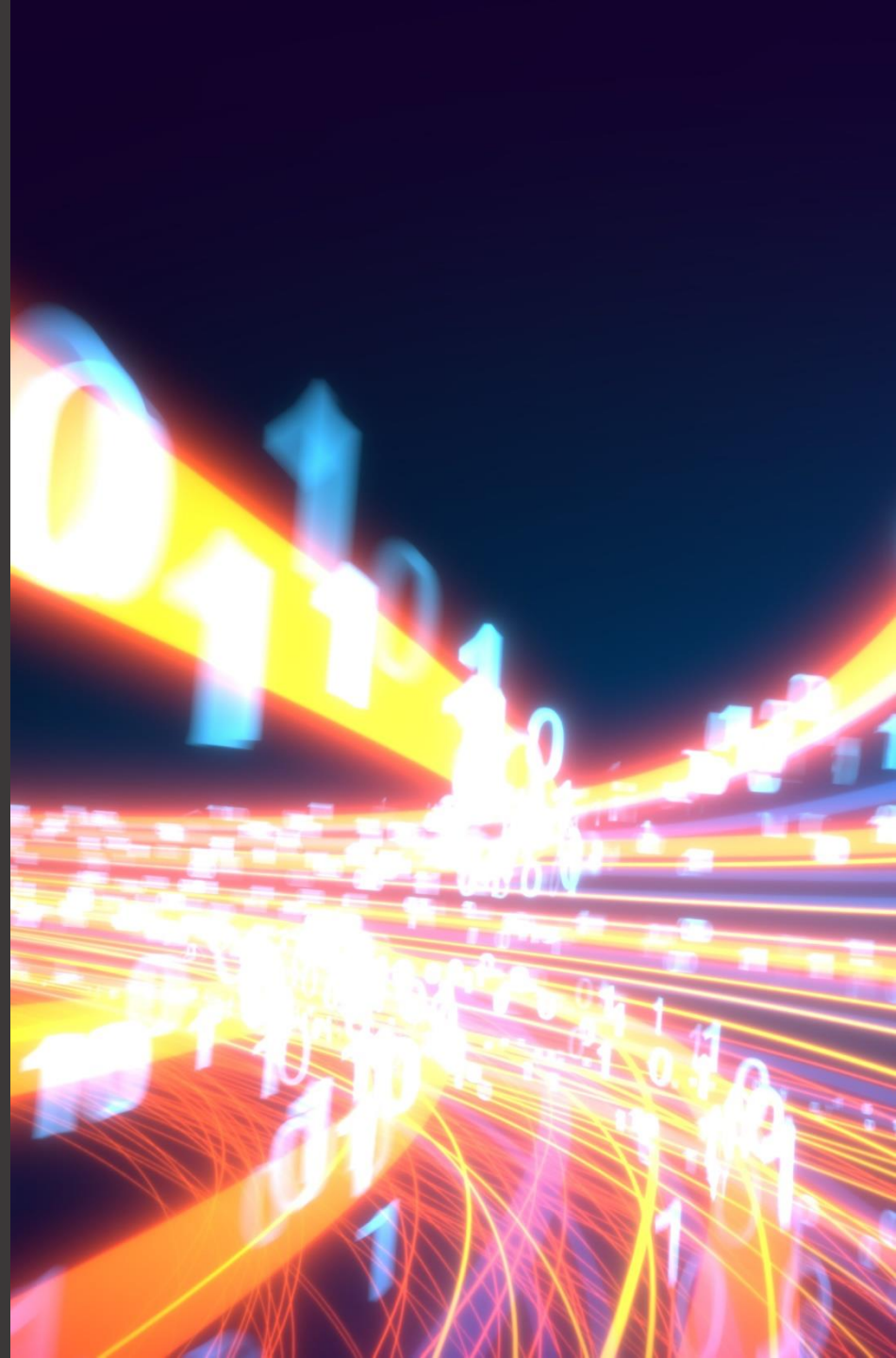


Web server DoS - attack

- Flood the server with traffic/requests until the server cannot reply to genuine requests
- A server would have a limited number of “slots” to support clients
- If an attacker places more requests than the number of slots, the server cannot accept any further requests and legitimate clients are rejected

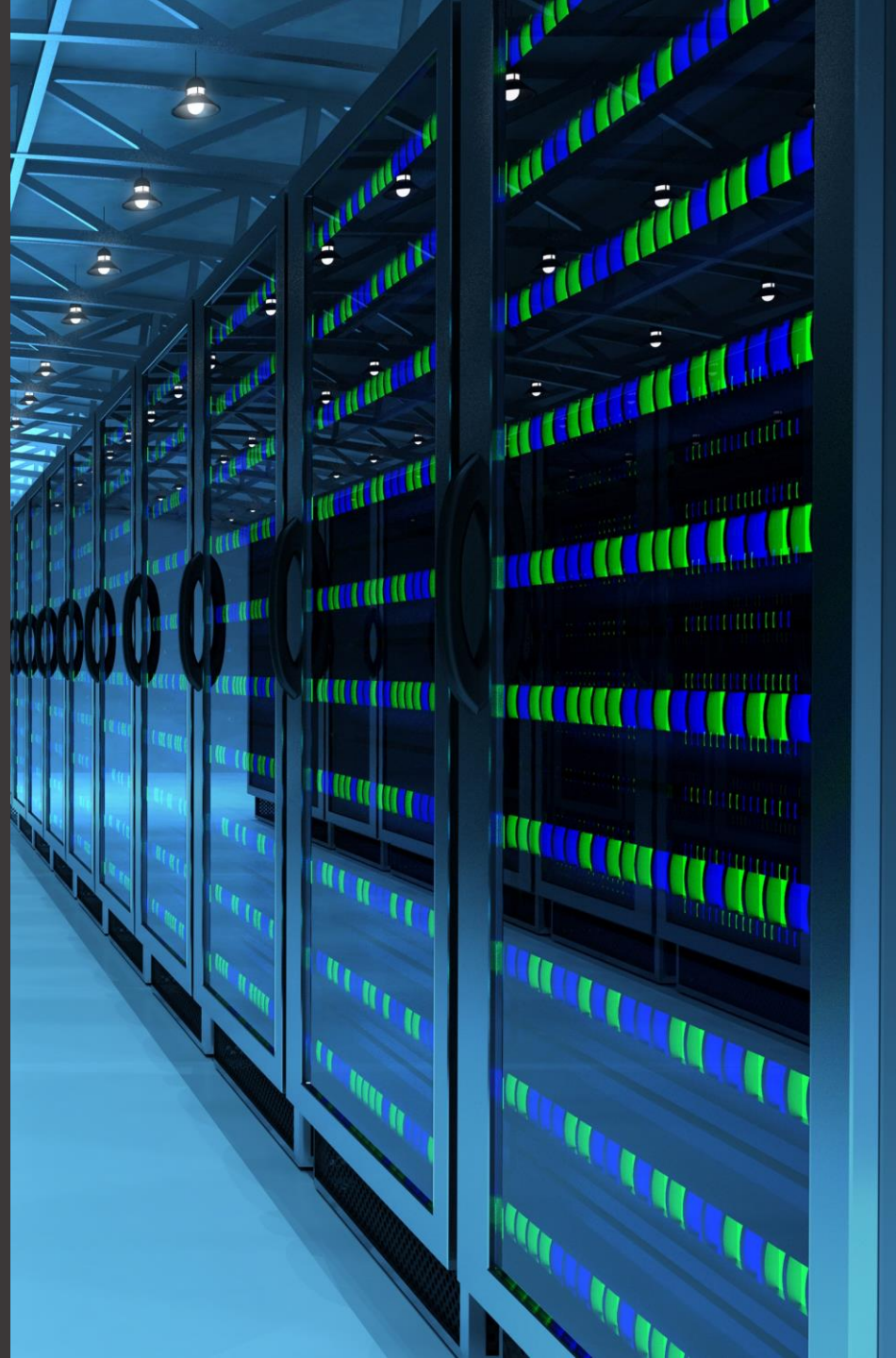
Web server DoS - mitigation

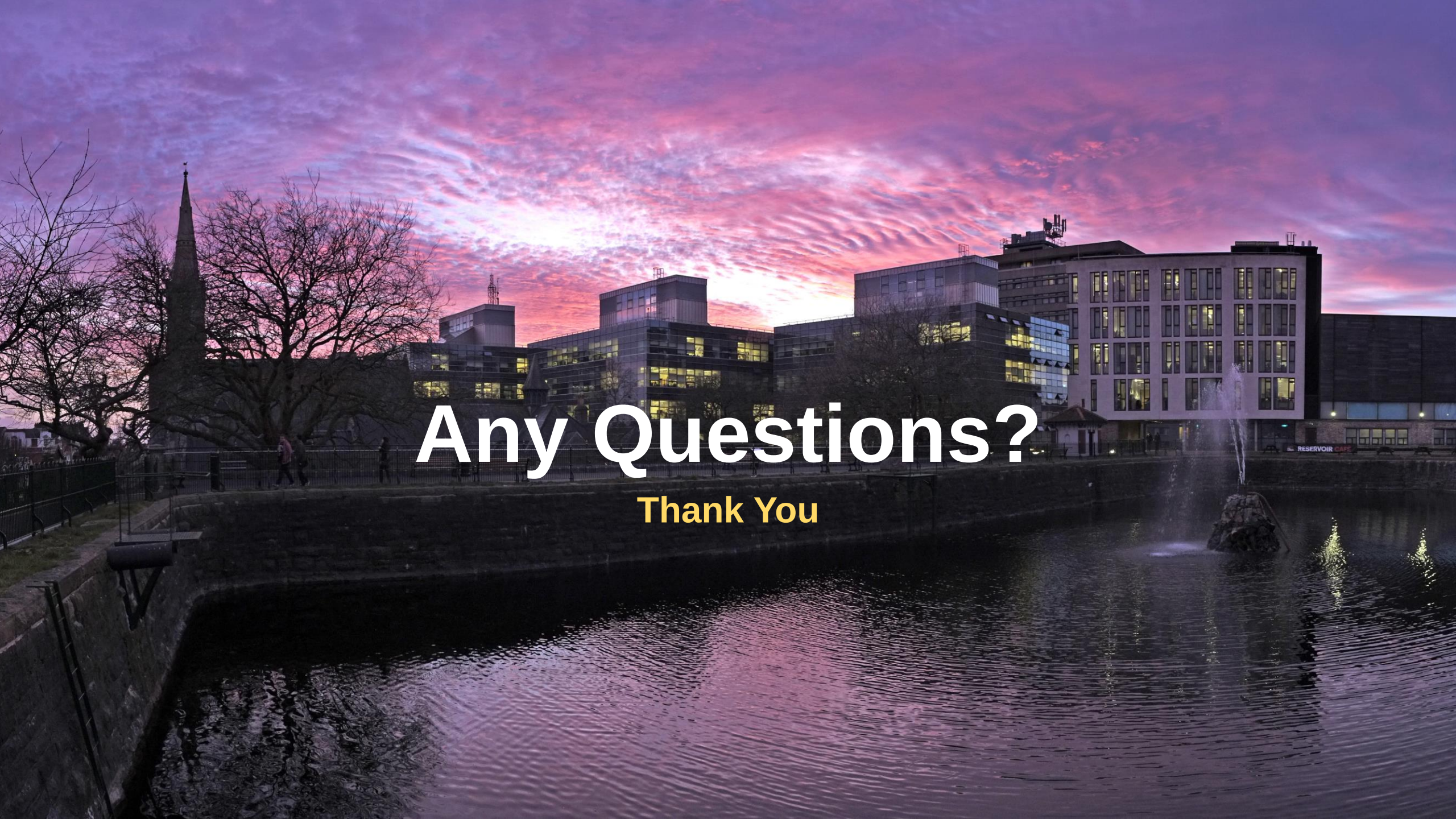
- Control incoming traffic on the web server
- Limit the number of connections from an IP address
  - This has limited effectiveness
  - DDoS still possible



Network environment

- Physical
  - Several machines connected with Ethernet cables to a physical switch and then to internet
- Virtual
  - Create several virtual machines and network devices connected in a virtual environment
  - eve-ng
    - Used by network designers/engineers to replicate/test large networks without the need of physical devices




Any Questions?
Thank You