Server Operation and Intro to Pentesting

Lecture 8 - ECS198F SQ26

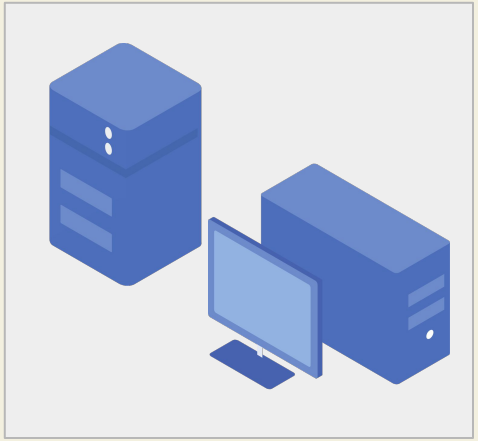
Hosts

Devices at the edge of the network that send and receive Internet data

Ex. laptops, phones, PCs, printers
(the things we're using right now!)

the Internet was made for connecting hosts together

Important subset: Servers
A PC that provides some useful Internet function



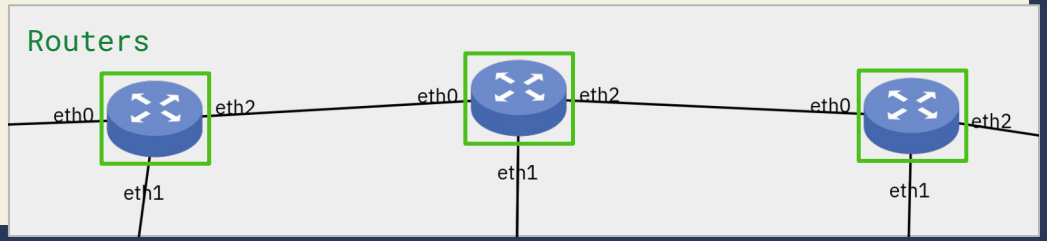
Routers

Main function: routing data across the Internet

routing ≈ postal service

each router is like a postal facility — determines how to move packages **closer** to destination

Purpose: move data (packets) from facility to facility en route to its destination



Network Interfaces

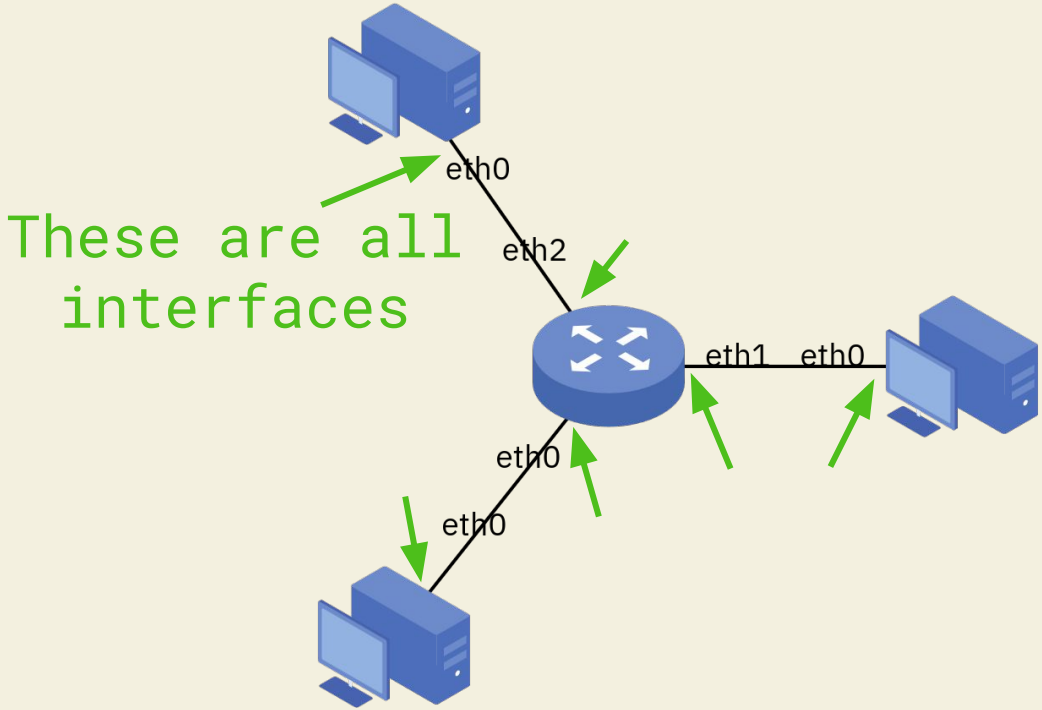
The part of a device's hardware which allows it to connect to a network

Ex. on laptops, a WiFi card
Ex. on other devices, an Ethernet port

Links: the connection between interfaces

- E.g. the WiFi connection between your laptop and the Eduroam access point

Network Interfaces (cont.)



Network Interface (Demo)

Open a terminal/cmd

Windows: run `ipconfig`
Linux/Mac: run `ifconfig`

Each interface has a **MAC Address**
In-use interfaces should have an **IP Address**
(more on these later)

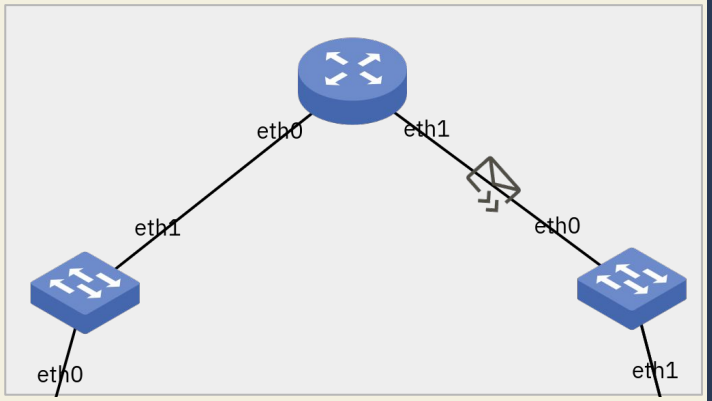
Network Data – Packets

Packets ≈ Packages

- Packages are moved from facility to facility, towards destination
  - Packets are moved from router to router towards destination
- At each router, the packet's destination address is read

  → next router to send it to is decided

Routing: step-by-step sending *across networks* that gets a packet closer to its destination



Addressing

Packages can only be routed to buildings with addresses

Packets can only be routed to devices with **IP addresses**

IP = Internet Protocol

IPv4 Address

Ex. `192.168.0.1`

Structure: 32 bits stuck together

(4 groups of 8 bits)

Identifies Internet devices

IPv4 Address (Cont.)


```
192 = 11000000
168 = 10101000
  0 = 00000000
  1 = 00000001
```

Subnet Mask

Devices can only directly communicate with other devices on their network

Subnet masks define the size of a network

E.g. 255.255.255.0

Subnet Mask (Cont.)

Binary:

```
  255         255         255         0
11111111 . 11111111 . 11111111 . 00000000
```

Subnet masks must be continuous 1s followed by continuous 0s

1s are network bits, 0s are host bits

Subnet Mask (Cont.)


```
192.168.0.1     = 11000000 . 10101000 . 00000000 . 00000001
255.255.255.0 = 11111111 . 11111111 . 11111111 . 00000000
```

Any IP address with the same network portion is on the same network

E.g. 192.168.0.2, 192.168.0.30, 192.168.0.250

But NOT 192.169.0.1, 200.168.0.1, 192.168.1.1

Services

An application running on a computer which operates over the network

In a clean directory, you can run:

```
python -m http.server
```

Ports

Suppose a server (192.168.0.10) is hosting a website and SSH

When I communicate with it, how do I tell it if I want to access SSH (i.e. and *not* the website?)

Solution: more numbers

Ports (Cont.)

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

22		Yes	Assigned	Yes[12]	Secure Shell (SSH),[11] secure logins, file transfers (scp, sftp) and port forwarding
80		Yes		Yes[12]	Hypertext Transfer Protocol (HTTP)[51][52] uses TCP in versions 1.x and 2. HTTP/3 uses QUIC,[53] a transport protocol on top of UDP.
443		Yes		Yes[12]	Hypertext Transfer Protocol Secure (HTTPS)[51][52] uses TCP in versions 1.x and 2. HTTP/3 uses QUIC,[53] a transport protocol on top of UDP.

Solution

Send a packet to the server saying

> “I want to access 192.168.0.10:22”

Pentesting