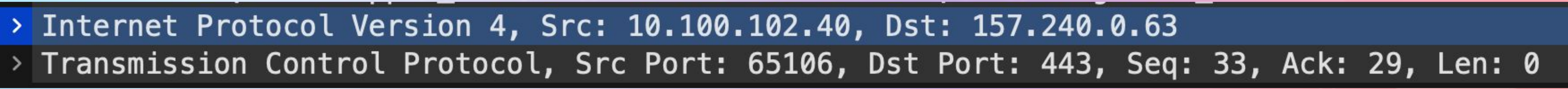
Sentinel

Networking - Network Layer
Subnets

DEFENDING OUR DIGITAL WAY OF LIFE

Network layer

- The layer responsible for delivering the packet to its final destination
- Protocol - IP
- Using IP addresses
- View on Wireshark:



```
> Internet Protocol Version 4, Src: 10.100.102.40, Dst: 157.240.0.63
> Transmission Control Protocol, Src Port: 65106, Dst Port: 443, Seq: 33, Ack: 29, Len: 0
```

IP Address - Reminder

- A unique identifier for every device on the network.
- Expressed as a set of four numbers, each one ranges between 0-255.
- Examples:
  - 192.168.1.1
  - 1.2.3.4
  - 123.154.32.232

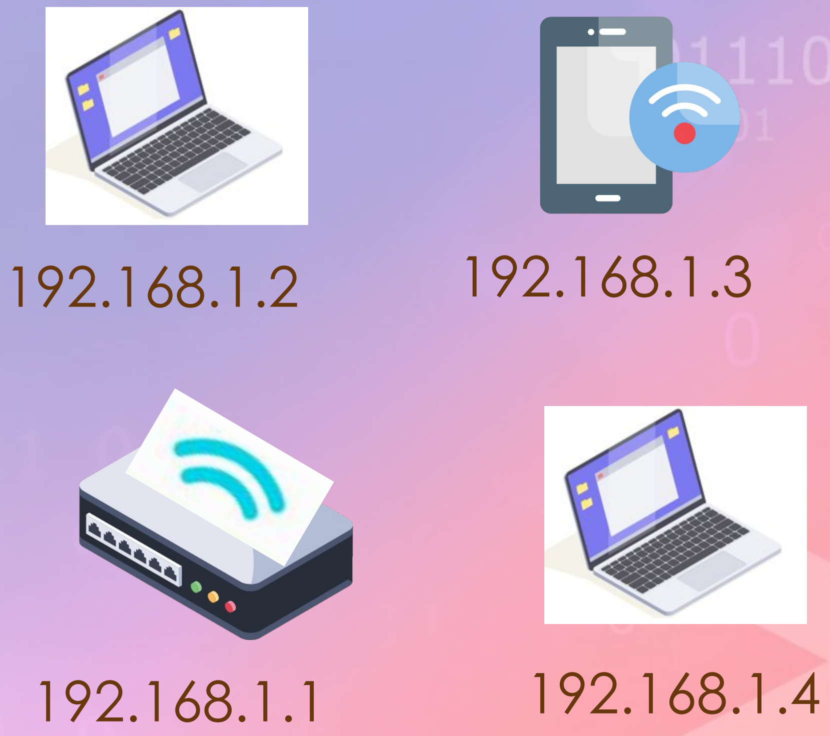
192.168.20.100

LAN - Local Area Network

- A small network of devices that can talk directly to each other, on the same location (not very far from each other).
- LAN’s are separated by ROUTERS used as gateways.
- Examples:
  - Home WiFi network
  - School network
  - **Not** the internet
  - **Not** a nation-wide cellular network (e.g Singtel)

IP Addresses in a LAN

- Devices in the same LAN usually have similar IP addresses.
- Let’s see it for ourselves!

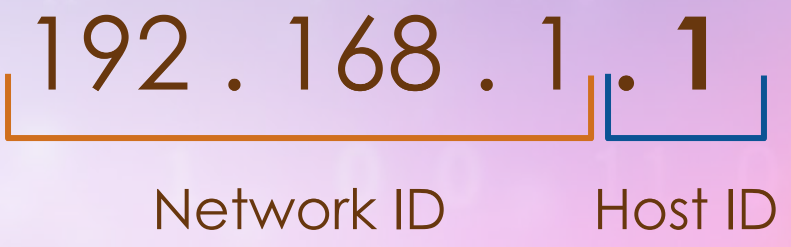


Demo - view all devices in LAN

- Let’s open CMD and run the script **get_lan_devices.py**.
    - Try it yourself.
- See all the IP addresses? Those are the devices in your LAN.
- See that all the IP addresses are similar?
- They are all in the same **subnet**.

Subnets

- Each IP address have 2 parts:
  - **Network part** - identifies the network. Like a surname.
  - **Host part** - identifies the device itself. Like a first name.
- IP addresses with the same network part are in the same **subnet**.
- It's like they are from the same family.
- For example:



192 . 168 . 1 . **1**

Network ID

Host ID

Subnets - example

- Let’s say the **subnet** of my home WiFi is 192.168.1.x.
- Which of the following IPs are in this subnet?
    - 192.168.1.1 V
    - 192.168.1.20 V
    - 192.168.0.1 X
    - 10.0.1.1 X

Problem

- Are those 2 IPs in the same **subnet**?

  10.0.1.1

  10.0.2.2

- We don’t know! How long is the **network ID**?

Is it only the first byte?	10.x.x.x
The first two bytes?	10.0.x.x
The first three bytes?	10.0.1.x

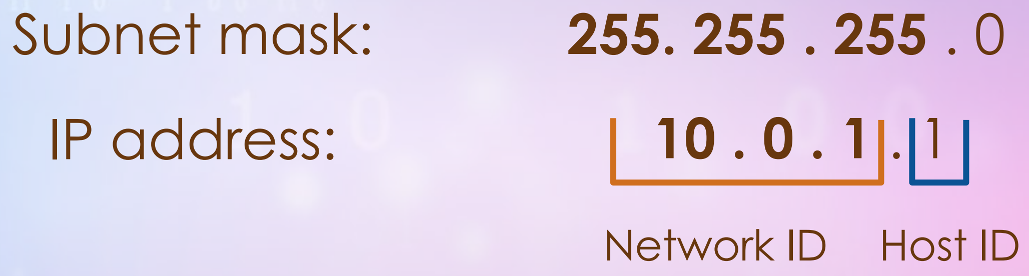
Subnet masks

- Subnet masks tell us **how much of the IP address is the network ID.**

  255 - means that this byte is part of the *network ID*

  0 - means that this byte is part of the *host ID*

- For example:
  - 255.255.255.0 - means that first 3 bytes are the network ID.



Subnet mask: **255. 255 . 255** . 0

IP address: **10 . 0 . 1** . 1

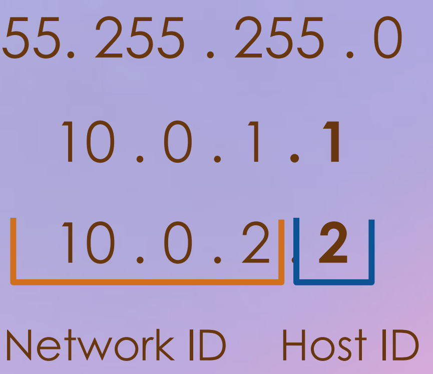
Network ID Host ID

Subnet masks - example

- Let’s say that we have 2 IP addresses:

10.0.1.1

10.0.2.2



255. 255 . 255 . 0

10 . 0 . 1 . **1**

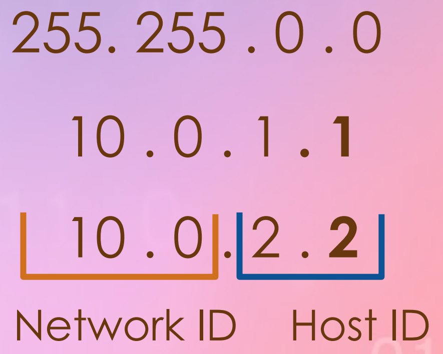
10 . 0 . 2 . **2**

Network ID Host ID

Not in the same subnet!

The subnet mask is 255.255.255.0.

Are they in the same subnet?



255. 255 . 0 . 0

10 . 0 . 1 . **1**

10 . 0 . 2 . **2**

Network ID Host ID

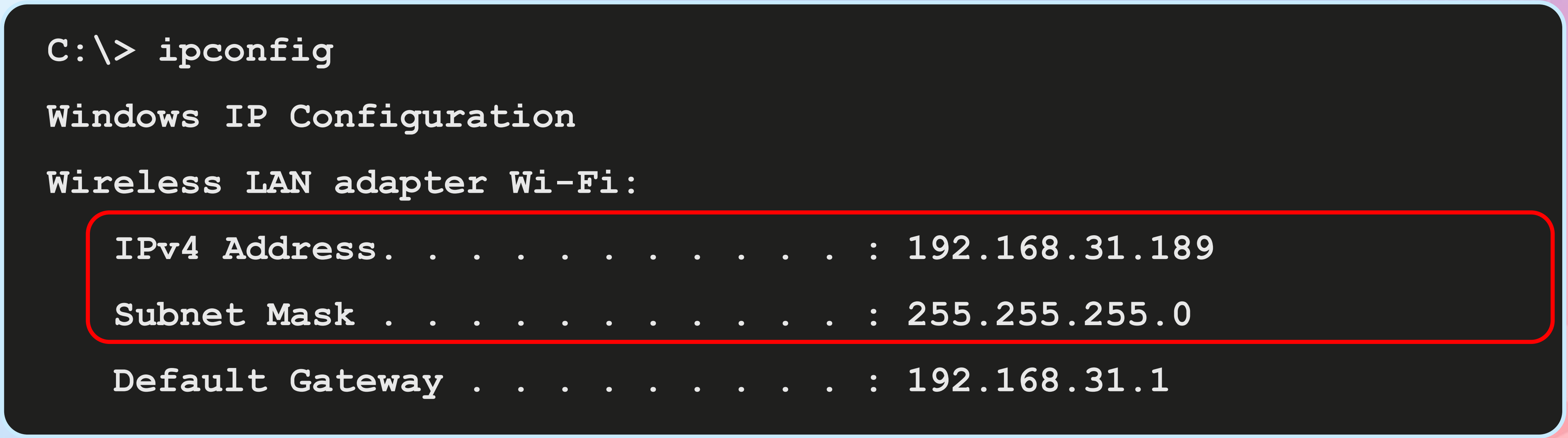
Same subnet!

The subnet mask is 255.255.0.0.

Are they in the same subnet?

How to check my subnet?

Use the cmd command **ipconfig**.



```
C:\> ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

   IPv4 Address. . . . . . . . . . . : 192.168.31.189

   Subnet Mask . . . . . . . . . . . : 255.255.255.0

   Default Gateway . . . . . . . . . : 192.168.31.1
```

We can see that our subnet is 192.168.31.x

IP ranges

- What is the valid IP address range in a subnet?
- Let’s look at 192.168.1.x:
  - Lowest possible address - 192.168.1.0
    - Called the **Network address**.
    - Can’t be an IP address of a device (it’s the address of the subnet itself).
  - Highest possible address - 192.168.1.255
    - Called the **Broadcast address**.
    - Can’t be an IP address of a device (used to message all of the devices in the subnet at once).
- We’re left with **254** possible IP addresses in the subnet.

Subnet sizes

- Subnets come in different sizes.
- The standard ones are called **Classes**.
    - 255.0.0.0 - **Class A**

      $256^3 - 2 = 16,777,214$ valid addresses in a Class A subnet
    - 255.255.0.0 - **Class B**

      $256^2 - 2 = 65,534$ valid addresses in a Class B subnet
    - 255.255.255.0 - **Class C**

      $256 - 2 = 254$ valid addresses in a Class C subnet
- Most home network are Class C (no need for more than 254 addresses).

CIDR

- **Subnet masks** indicate how many **bytes** of the IP address are the network ID.
- **CIDR** -
  - another way to write subnets
  - subnet name + how many **bits** of the IP address are the network ID.
- Examples:
  - 192.168.1.0/24 24 bits = 3 bytes - subnet is **192.168.1.x**
  - 10.0.0.0/16 16 bits = 2 bytes - subnet is **10.0.x.x**

CIDR - example

- **10.1.0.0/16**
  - What is the lowest possible address (network name)? **10.1.0.0**
  - What is the highest possible address (broadcast)? **10.1.255.255**
  - Is 192.168.1.1 in the subnet? **No**
  - Is 10.1.2.3 in the subnet? **Yes**
  - Is 10.0.0.1 in the subnet? **No**

Classless subnets

- Subnets are not limited to classes.
- IP address length is 4 bytes == 32 bits
  - What if the network part is 10 bits? or 15? or 30?
  - The split to network/host parts will be in the middle of a byte
- Example:
  - 192.168.0.0/20
    - IPs in this subnet will start with the first 20 bits of 192.168.0.0
  - We have to convert to binary to calculate the exact range
- Pros - more control over the network size (more efficient)
- Cons - not intuitive, hard to tell at first glance if IP is in subnet

Classless subnets - example

IP (decimal - base 10) 192 . 168 . 0 . 0 / 20

IP (binary - base 2) 11000000 . 10101000 . 00000000 . 00000000

Network ID Host ID

- The network part in this subnet is 20 bits long
- It means that all IP addresses in this subnet must start with these 20 bits
- In subnet mask notation:

Subnet Mask (binary - base 2) **11111111 . 11111111 . 1111**0000 . 00000000

Subnet Mask (decimal - base 10) **255 . 255 . 240** . 0

Classless subnets - example

IP (decimal - base 10)	192 . 168 . 0 . 0 / 20
IP (binary - base 2)	11000000 . 10101000 . 00000001 . 00000001

Network ID Host ID

Lowest address (binary)	**11000000 . 10101000 . 0000**0000 . 00000000
Lowest address (decimal)	**192 . 168** . 0 . 0
Highest address (binary)	**11000000 . 10101000 . 0000**1111 . 11111111
Highest address (decimal)	**192 . 168** . 15 . 255

Classless subnets - example

- 192.168.0.0/20
  - Lowest address (network name) is **192.168.0.0**
  - Highest address (broadcast) is **192.168.15.255**
  - Valid IP addresses range is **192.168.0.1 - 192.168.15.254**
    - How many addresses? 32-20 bits = 2^{12}
    - Without the network name and broadcast address:
      - 2^{12} - 2 = 4094 valid IP addresses
  - The subnet mask of /20 is **255.255.240.0**

What did we learn?

- What is a **LAN** (Local Area Network)
- What is a **subnet**
- How to find the **network ID** and the **host ID** in an IP address
- How to identify a subnet
  - Subnet Name + Subnet Mask (e.g, 192.168.1.0 + 255.255.255.0)
  - or CIDR (e.g, 192.168.1.0/24)
- Special addresses in a subnet
  - Lowest - network address
  - Highest - broadcast address