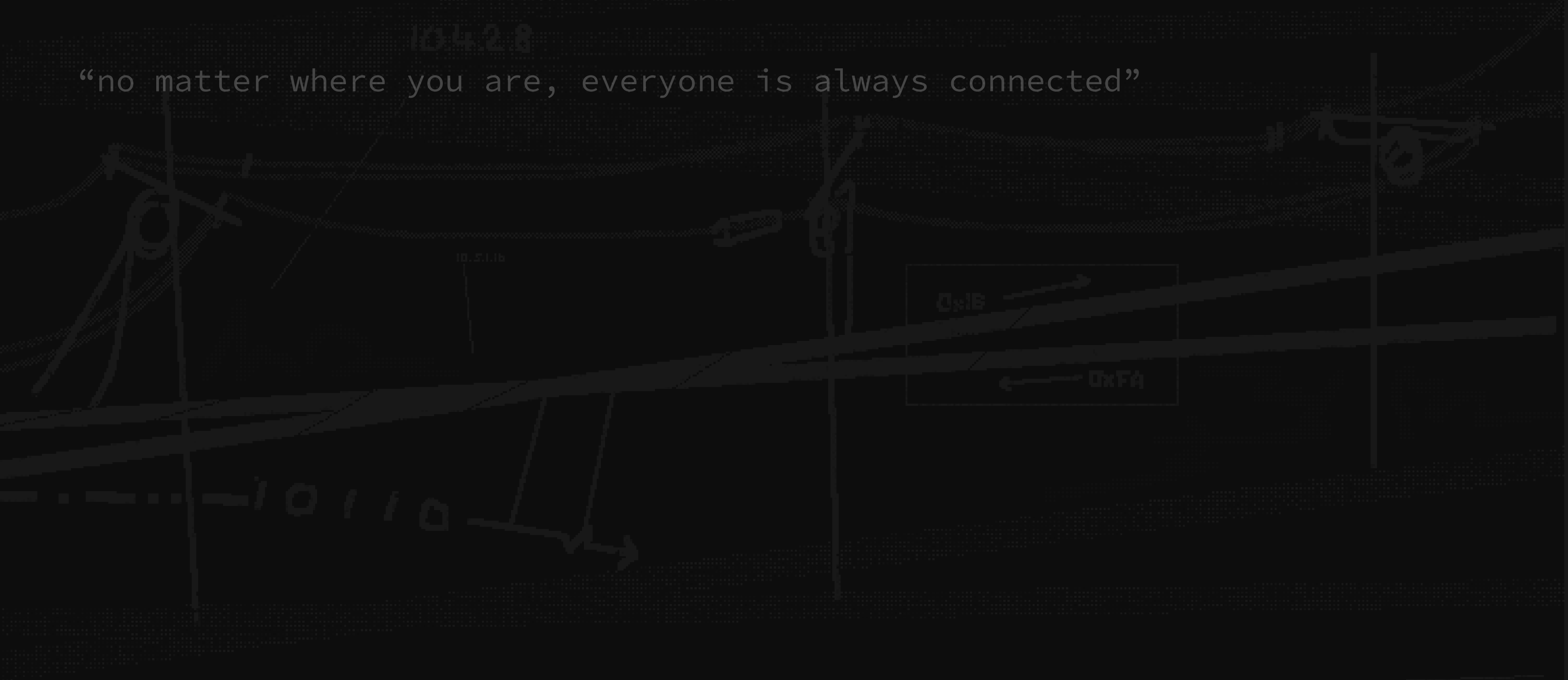
09

Linux on the Network

“no matter where you are, everyone is always connected”



On the Network

Ok, I’ve got to give it to the Cisco folk, networking is a tad complicated.

Here’s a rundown of what we’re doing today:
- Understand fundamental networking concepts
- Use tools to discover what services are running on the network
- Using *ufw* to firewall network traffic to and from our system
- Using *ip* to understand network interfaces

IP Addresses and Ports

An *IP address* is a number that represents the location of the system on the network, typically represented as four numbers from 0-255, like so:

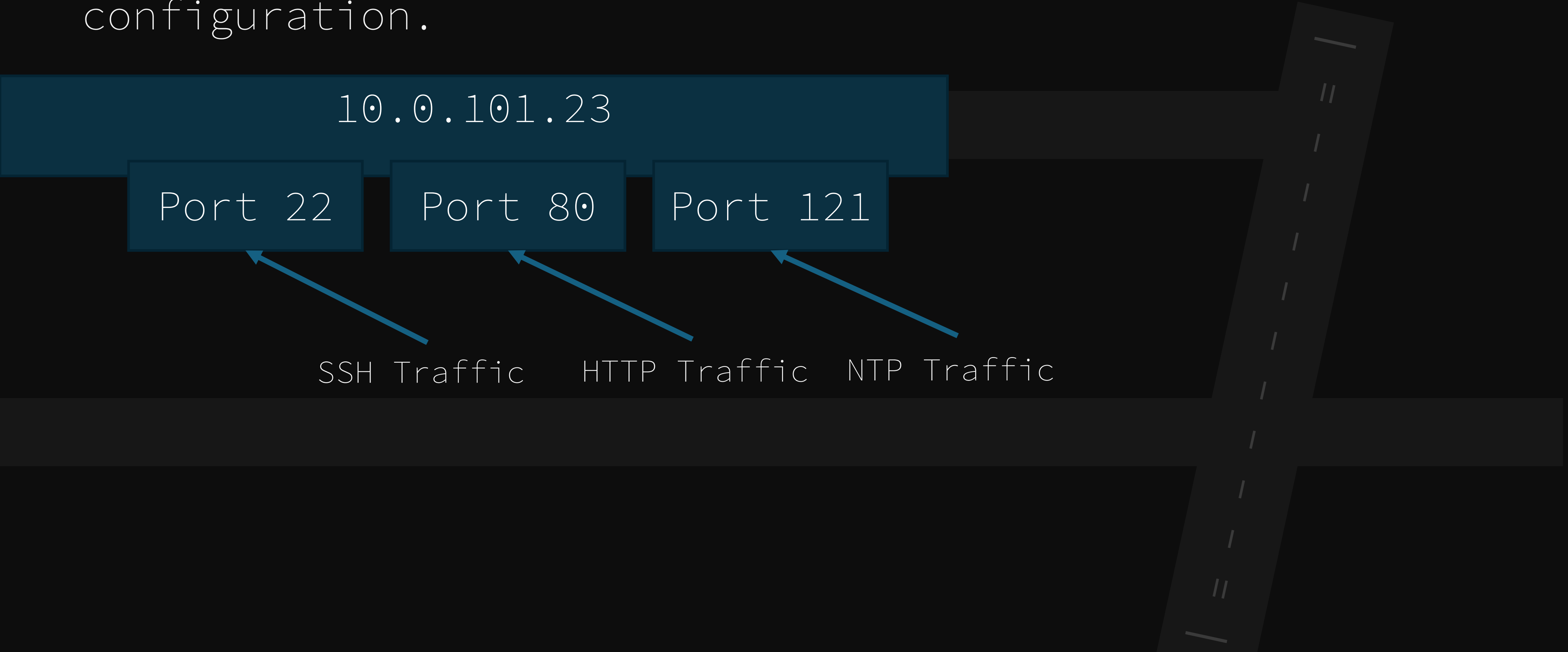
10.0.101.23

Network traffic arrives to the system destined for a specific *port number* on this address, which is a number from 0-65535. The port number 1000 is represented as so (with a colon):

10.0.101.23:1000

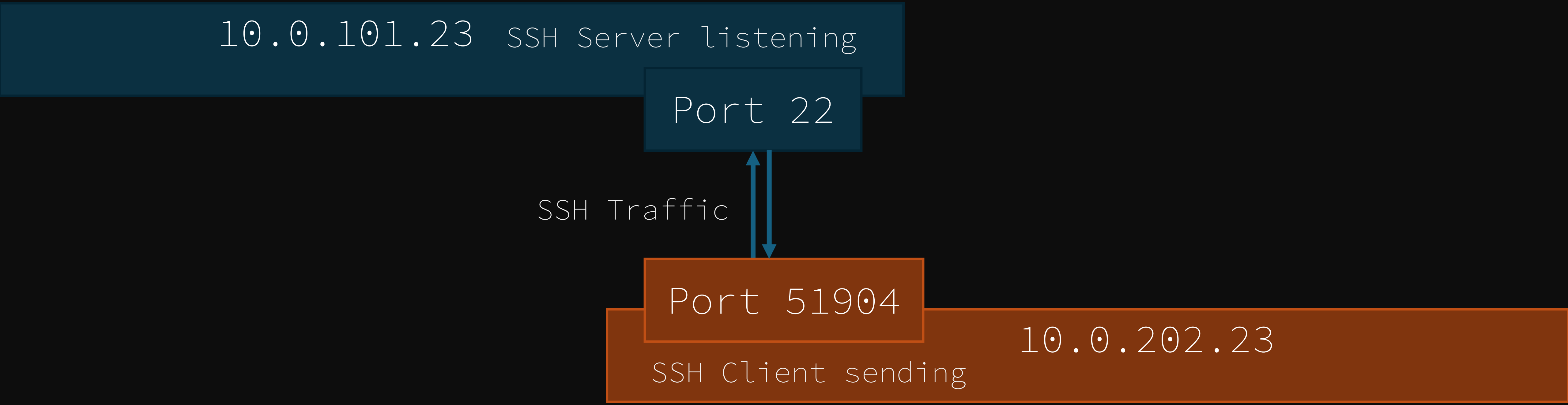
Port Numbers

Applications on the system listen for network traffic to arrive on a specific port defined in its configuration.



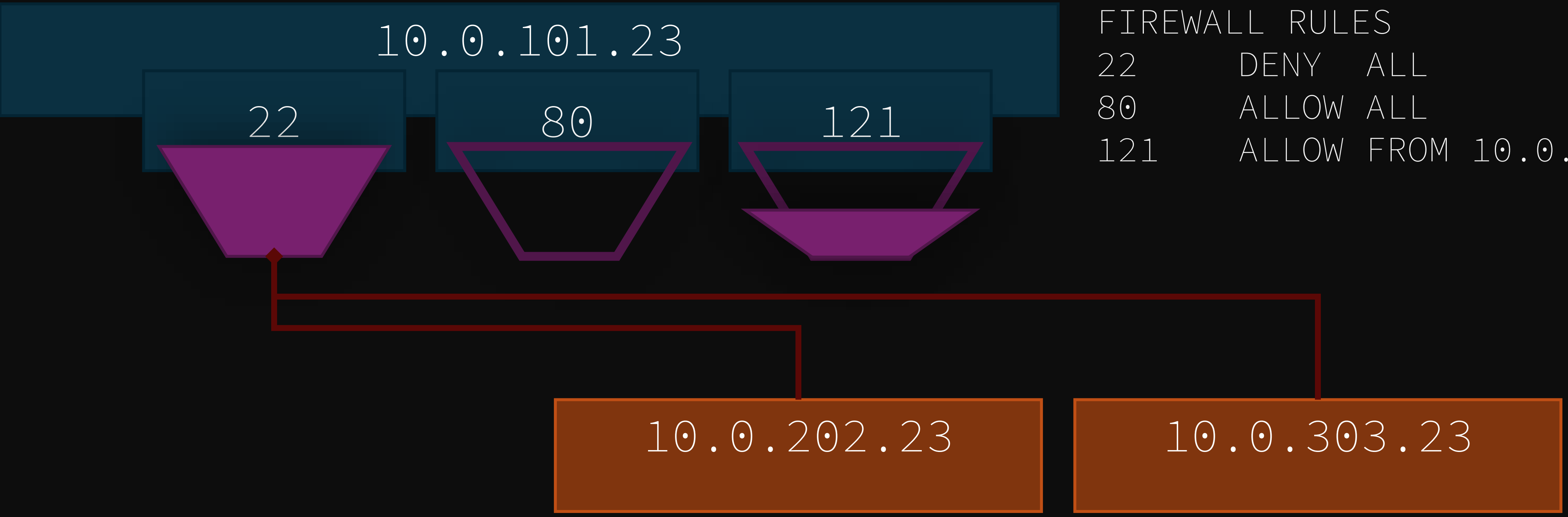
Port Numbers

Applications can communicate with each other across the network using these port numbers.



Firewalls

A firewall, in the context of Linux is simply a filter to allow or deny traffic to or from certain port numbers or IP addresses.

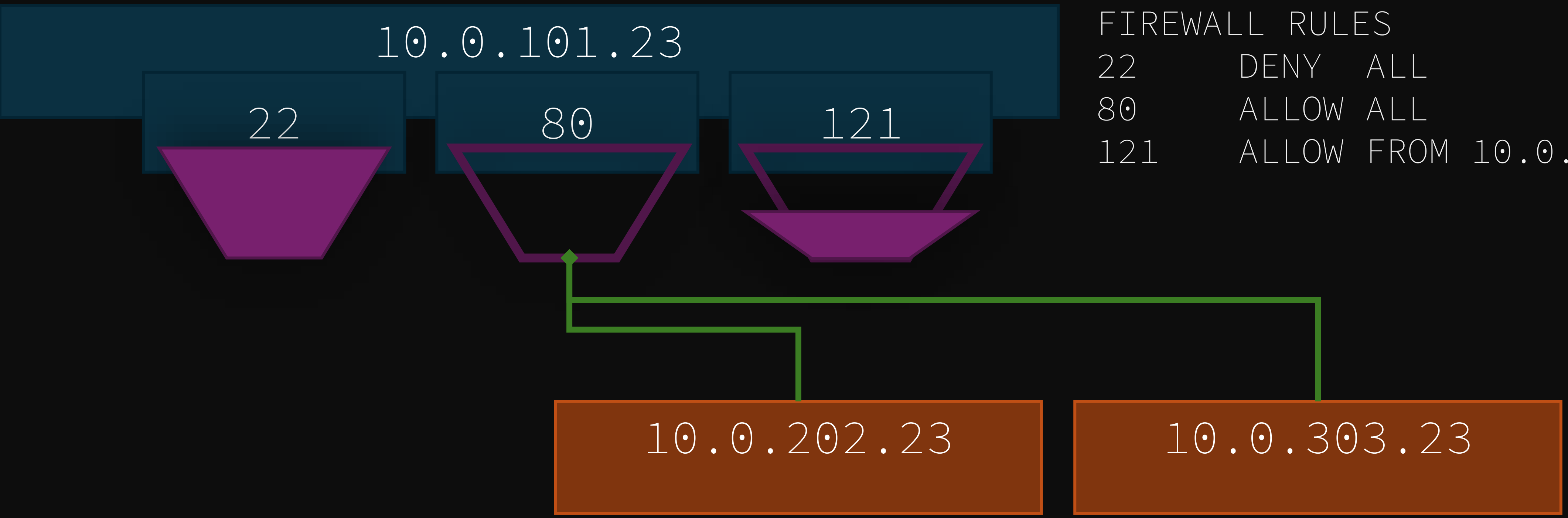


FIREWALL RULES

22	DENY	ALL
80	ALLOW	ALL
121	ALLOW	FROM 10.0.303.0/24

Firewalls

A firewall, in the context of Linux is simply a filter to allow or deny traffic to or from certain port numbers or IP addresses.

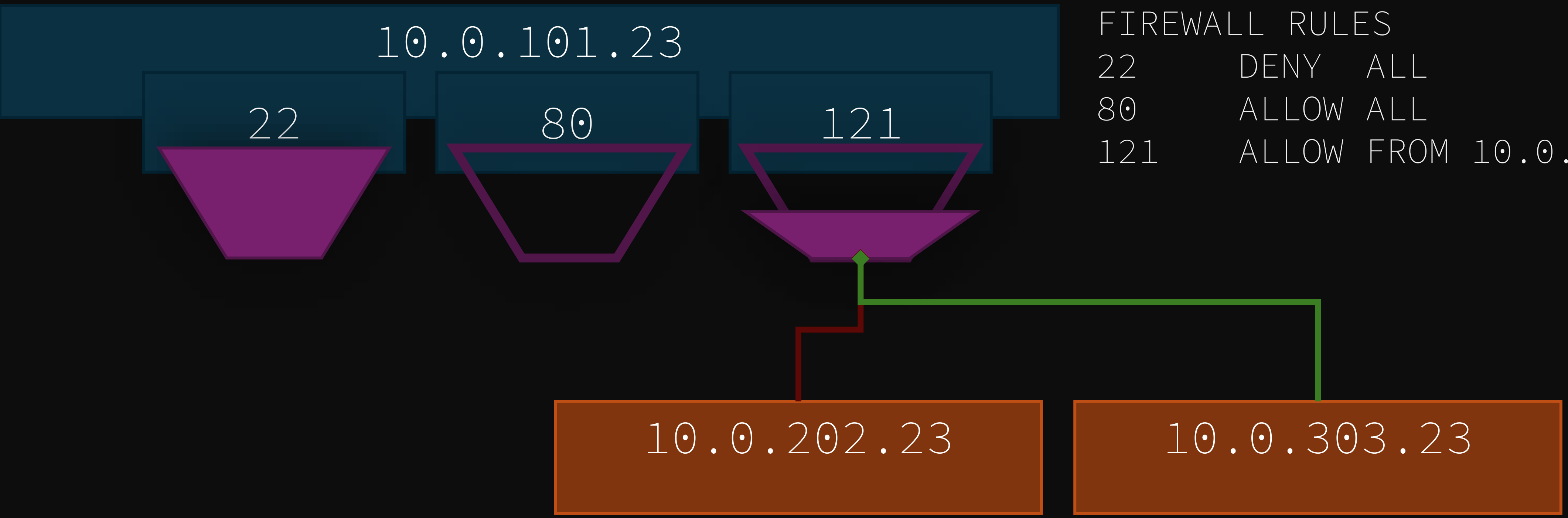


FIREWALL RULES

22	DENY	ALL
80	ALLOW	ALL
121	ALLOW	FROM 10.0.303.0/24

Firewalls

A firewall, in the context of Linux is simply a filter to allow or deny traffic to or from certain port numbers or IP addresses.

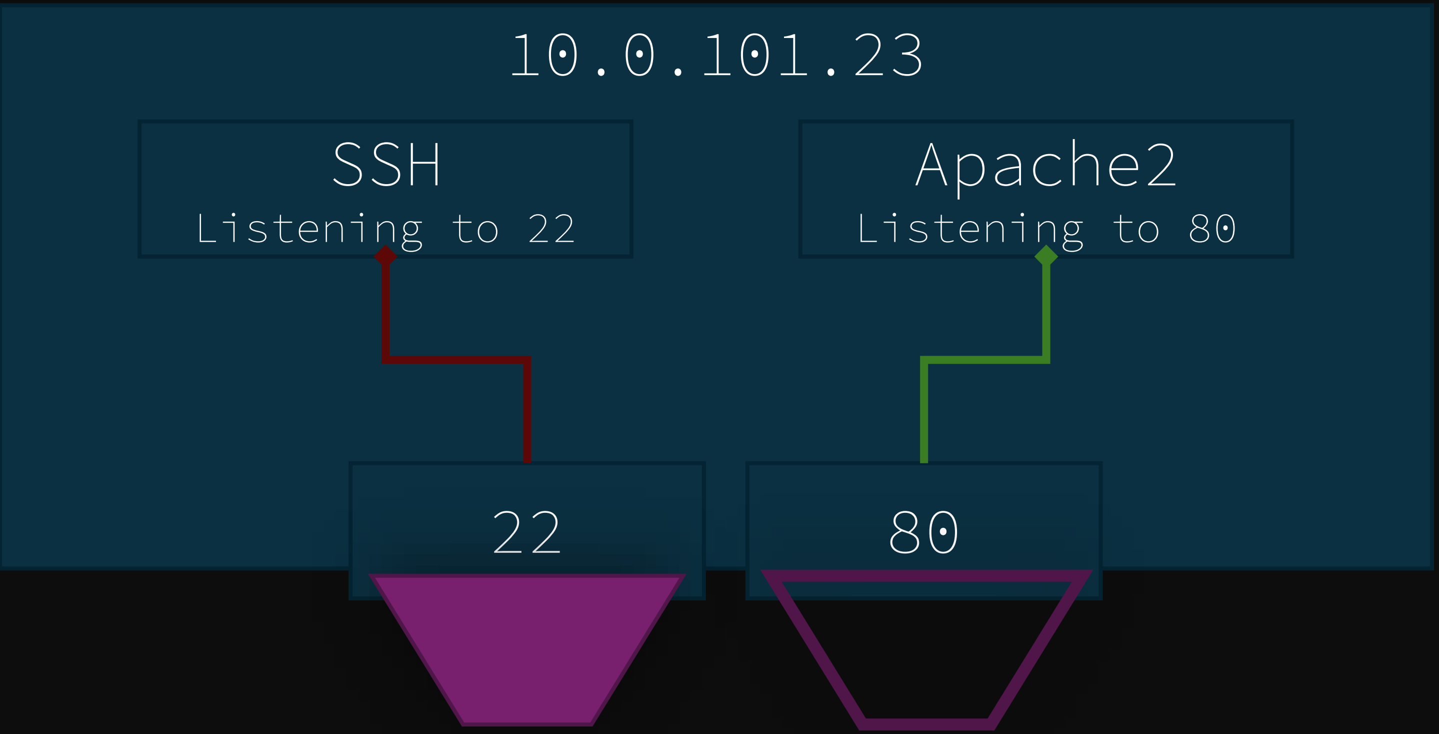


FIREWALL RULES

22	DENY	ALL
80	ALLOW	ALL
121	ALLOW	FROM 10.0.303.0/24

Firewalls

By using firewalls, we can explicitly filter which traffic is allowed into our system.

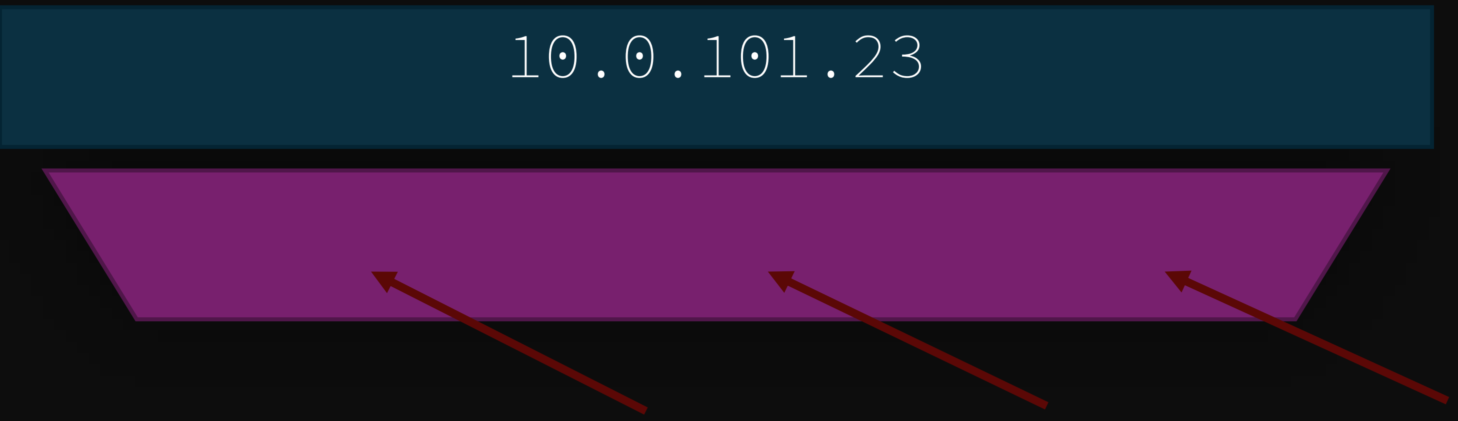


FIREWALL RULES

22	DENY	ALL
80	ALLOW	ALL

Firewalls

By *default*, we want all traffic into our system to be denied. This makes sure there are no paths of entry into our system other than what we need.

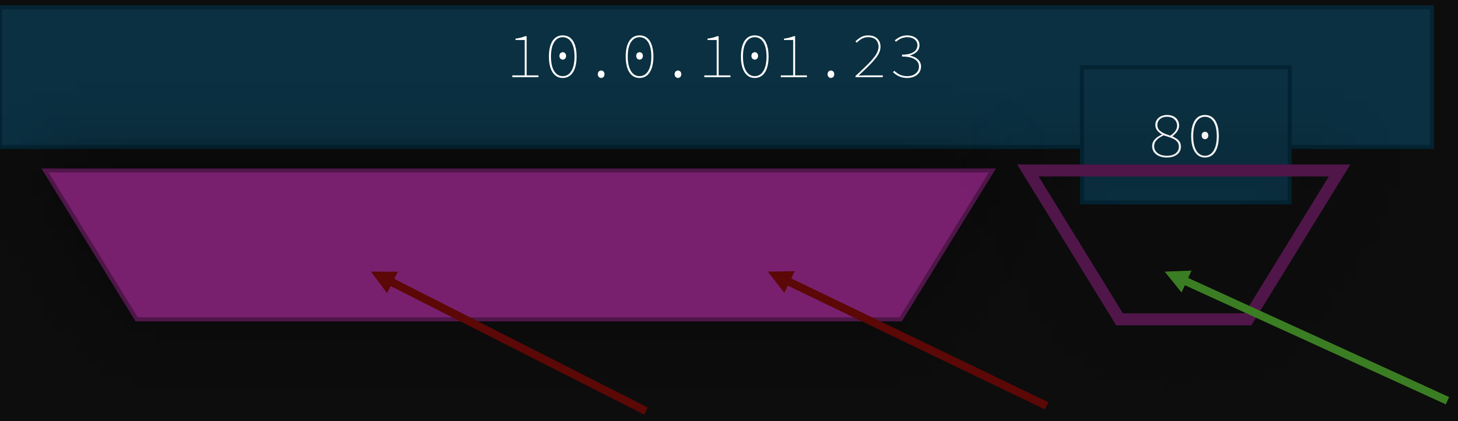


10.0.101.23

FIREWALL RULES
DEFAULT DENY ALL

Firewalls

After setting the default behavior to deny, we can now allow specific ports to be open.



FIREWALL RULES

80	ALLOW	ALL
DEFAULT	DENY	ALL

It’s Not That Complicated

in terminal

```
# ufw enable

# ufw default deny

# ufw logging high
```

UFW is the *Uncomplicated Firewall*. It’s simple to use and installed by default.

Setting *default deny* ensures that all traffic that does not match a rule is denied.

TCP vs UDP

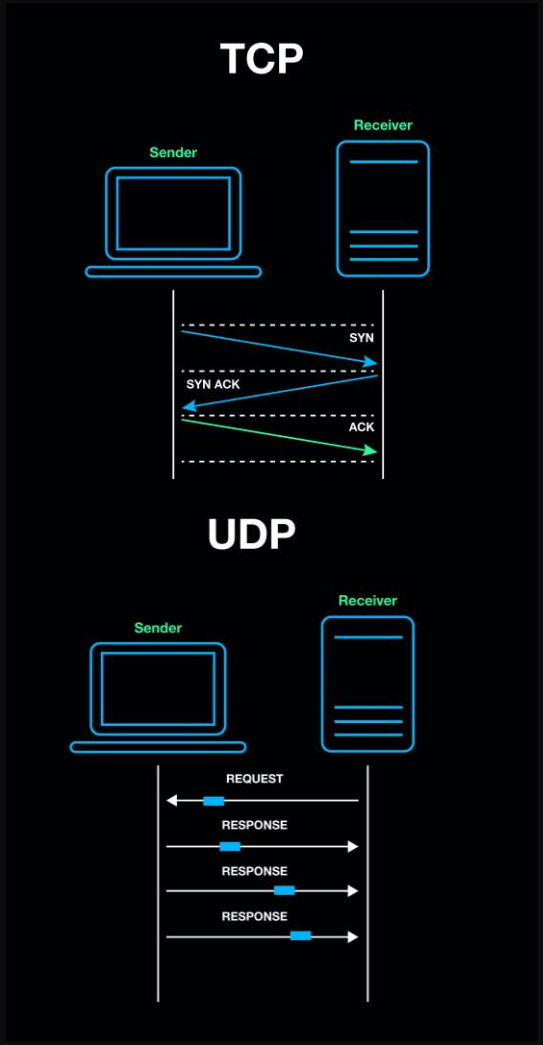
TCP and UDP are two different protocols of transmission across a network.

TCP stands for Transmission Control Protocol.

It utilizes a three-way handshake to ensure a reliable connection and transmission.

UDP stands for User Datagram Protocol.

It is a connectionless protocol designed to be speedy but does not guarentee reliability.



Why it Matters

Different services may receive packets using either TCP or UDP. *Most, but NOT ALL services use TCP.*

When setting a firewall rule, pay attention to which protocol is used by a service.

Letting Traffic In

in terminal

```
# ufw allow 22/tcp

# ufw allow 123/udp
```

We can allow traffic destined to certain ports on the system using *ufw allow*.

Here, we allow TCP traffic coming in on port 22 and UDP traffic coming in on port 123.

Do this command for all ports that are required to be open.

What Ports Do I Let In?

Each service that interacts with the network has a certain port number associated with it. Look at the services that are required on the system, and open its necessary port.

For example, if *sshd* was a required service, you would let in port 22 TCP.

If you are at all unsure, look up the default port number for the services you are trying to let through!

Scenario

You are serving a web server using Apache2. You need to set up the firewall to allow <u>HTTP internet traffic</u> to the web server using UFW.

What command should I run?

The Listeners Lurk

in terminal

```
# netstat -tulpn
Active Internet connections (only serve
Proto Recv-Q Send-Q Local Address
tcp          0      0 127.0.0.54:53
tcp          0      0 127.0.0.1:631
tcp          0      0 0.0.0.0:445
.
.
.
tcp6         0      0 :::25
tcp6         0      0 :::21
tcp6         0      0 :::139
```

Run *netstat -tulpn* to view a list of services currently listening for traffic. Notice how *vsftpd* and *smbd* are among the running network processes. Any non-critical service (not part of the system nor mentioned in the README) should be removed.

Network Interfaces

Network interfaces are the link between the system and a network.

- A physical network interface is an actual hardware connection to a network
- A virtual network interface is not necessarily an actual hardware connection but represents a network device

Viewing Interface Information

in terminal

```
# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536
    link/loopback 00:00:00:00:00:00 brd
2: enp2s0: <NO-CARRIER,BROADCAST,MULTIC
    link/ether c8:2a:14:3b:29:46 brd ff
3: wlp3s0: <BROADCAST,MULTICAST,UP,LOWE
    link/ether e4:ce:8f:5a:ee:d5 brd ff
```

This command shows us all of the available network interfaces on the system.

Viewing Interface Information

in terminal

```
# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536
    link/loopback 00:00:00:00:00:00 brd
2: enp2s0: <NO-CARRIER,BROADCAST,MULTIC
    link/ether c8:2a:14:3b:29:46 brd ff
3: wlp3s0: <BROADCAST,MULTICAST,UP,LOWE
    link/ether e4:ce:8f:5a:ee:d5 brd ff
```

We can view

- The interface name (lo, enp2s0, wlp3s0)
- The type of interface (loopback, ether)
- The MAC address of the interface

Viewing Interface Information

in terminal

```
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536
    link/loopback 00:00:00:00:00:00 brd
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft
    inet6 ::1/128 scope host noprefixro
       valid_lft forever preferred_lft
2: enp2s0: <NO-CARRIER,BROADCAST,MULTIC
    link/ether c8:2a:14:3b:29:46 brd ff
3: wlp3s0: <BROADCAST,MULTICAST,UP,LOWE
    link/ether e4:ce:8f:5a:ee:d5 brd ff
    inet 10.0.0.122/24 brd 10.0.0.255 s
```

This command lets us view IP address information in more detail for each interface.

Viewing Interface Information

in terminal

```
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536
    link/loopback 00:00:00:00:00:00 brd
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft
    inet6 ::1/128 scope host noprefixro
       valid_lft forever preferred_lft
2: enp2s0: <NO-CARRIER,BROADCAST,MULTIC
    link/ether c8:2a:14:3b:29:46 brd ff
3: wlp3s0: <BROADCAST,MULTICAST,UP,LOWE
    link/ether e4:ce:8f:5a:ee:d5 brd ff
    inet 10.0.0.122/24 brd 10.0.0.255 s
```

We can view

- IP addresses available

- The broadcast address

Looping Back

The loopback address is a special address that loops all traffic back to your system.

The loopback address is

```
          127.0.0.0/8
```

Meaning all addresses between

```
          127.0.0.0 and 127.255.255.255
```

Will loop back to the system.

In Linux it is represented as the virtual interface *lo*

This address is especially useful for connecting to network services on your own system.

Recap

You learned key networking terms and their application in Linux, such as:

- IP address
- Port number
- Firewall

You learned proper firewall configuration using *ufw*.

You learned how to view services listening on the network using *netstat*.

You learned how to find key information about network interfaces using the *ip* command.