C’est pas le réseau, ça ping Marty!

Cynthia Treger
David Santiago

$ ~~whoami~~ whoarewe

Cynthia Treger
Global Black Belt Azure Networking @Microsoft
cynthiatreger

David Santiago
Cloud Solution Architect @Microsoft
davidsntg

TOOLS-IN-ACTION

TOOLS-IN-ACTION

/ SUMMARY

1. Network 101
   Connectivity, Routing, Filtering…

2. What could go wrong ?

Spoiler alert: It’s not always DNS!

TOOLS-IN-ACTION

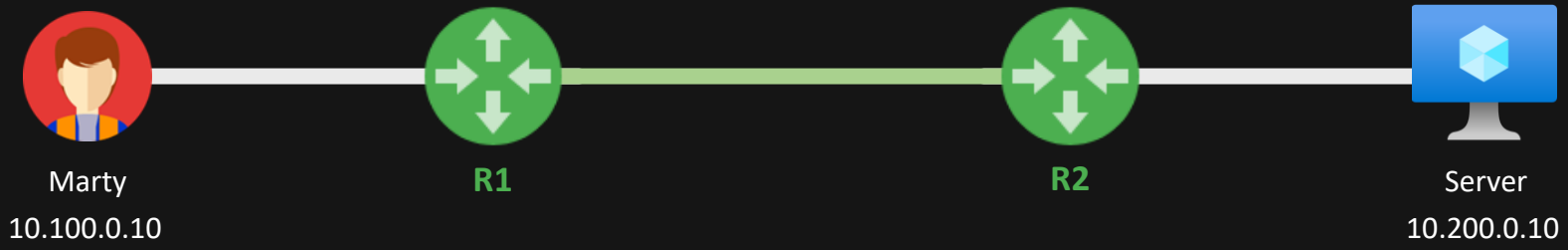
Network 101

/ Back to Basics

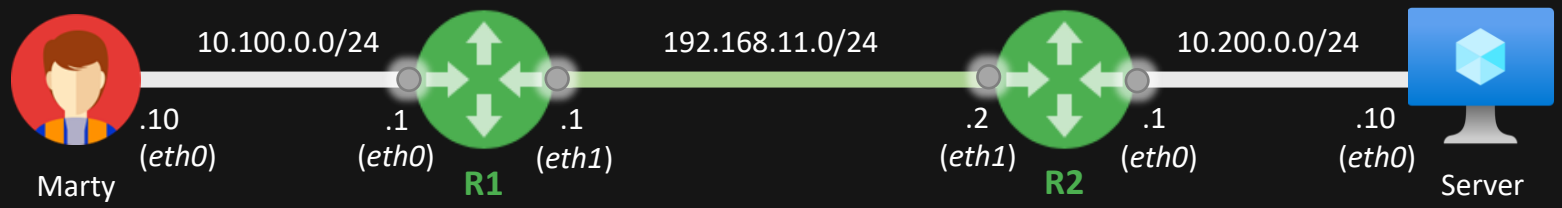
Networking example

IP addressing

Infrastructure

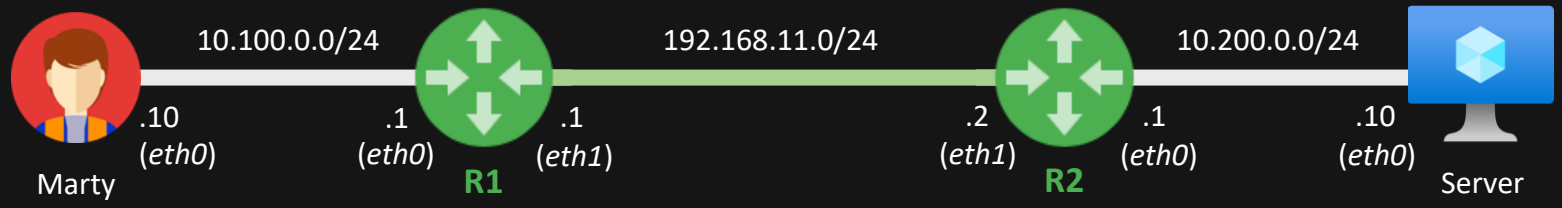


Infrastructure



TOOLS-IN-ACTION

Routing tables

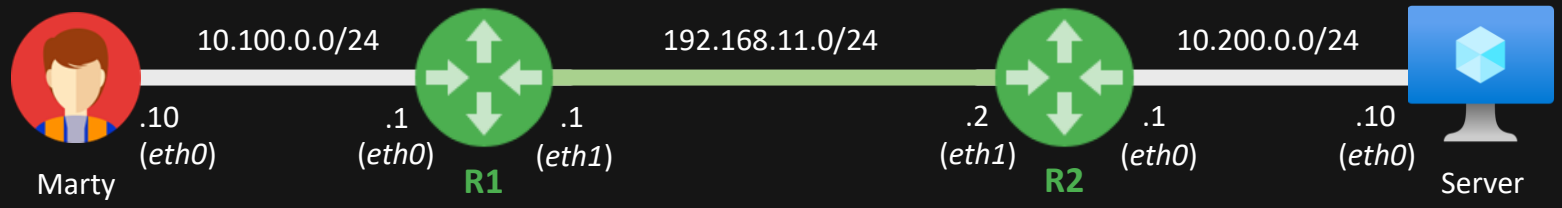


Marty's Routing Table	
Route	Next Hop
10.100.0.0/24	*eth0*
0.0.0.0/0	10.100.0.1

R1's Routing Table	
Route	Next Hop
10.100.0.0/24	*eth0*
192.168.11.0/24	*eth1*

TOOLS-IN-ACTION

Routing tables

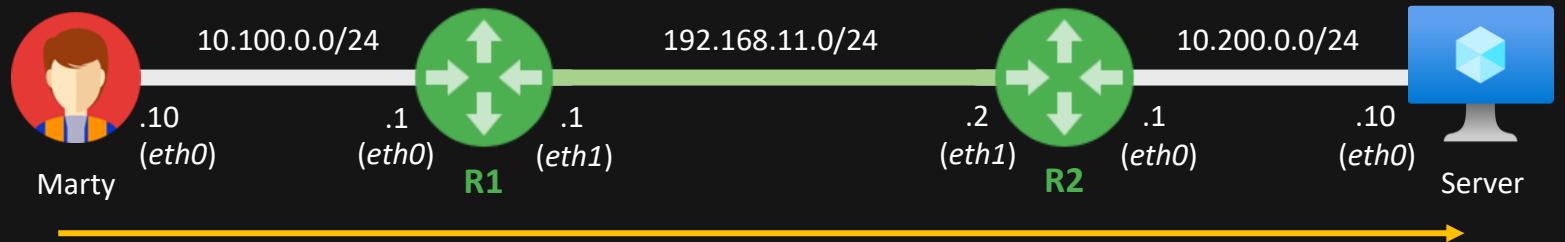


Marty's Routing Table	
Route	Next Hop
10.100.0.0/24	*eth0*
0.0.0.0/0	10.100.0.1

R1's Routing Table	
Route	Next Hop
10.100.0.0/24	*eth0*
192.168.11.0/24	*eth1*
10.200.0.0/24	192.168.11.2

TOOLS-IN-ACTION

Routing tables



Marty's Routing Table	
Route	Next Hop
10.100.0.0/24	*eth0*
0.0.0.0/0	10.100.0.1

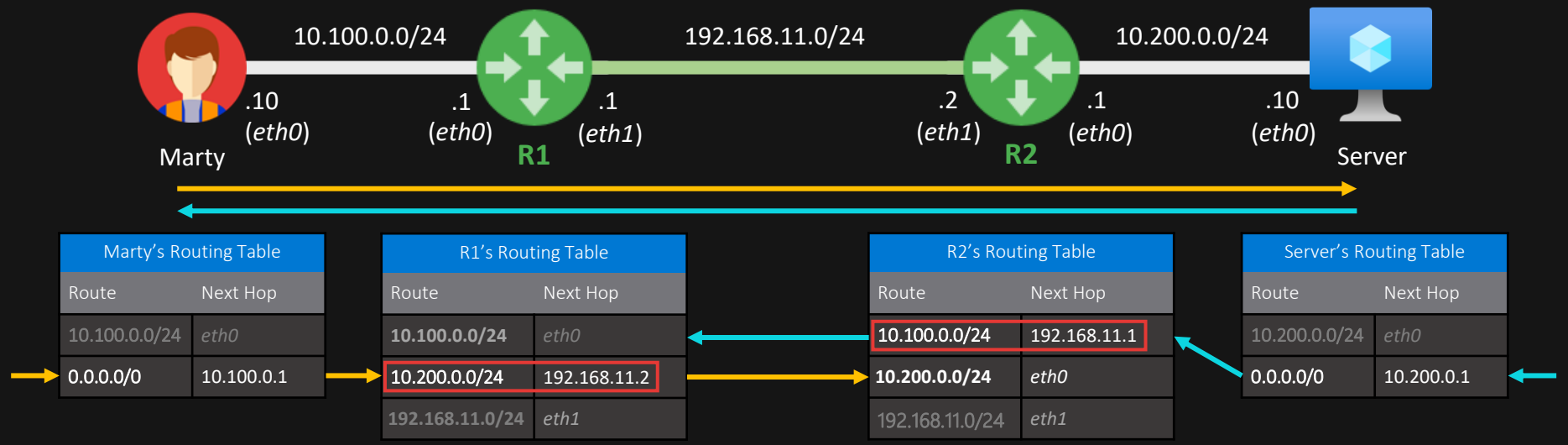
R1's Routing Table	
Route	Next Hop
10.100.0.0/24	*eth0*
10.200.0.0/24	192.168.11.2
192.168.11.0/24	*eth1*

R2's Routing Table	
Route	Next Hop
10.200.0.0/24	*eth0*
192.168.11.0/24	*eth1*

Server's Routing Table	
Route	Next Hop
10.200.0.0/24	*eth0*
0.0.0.0/0	10.200.0.1

TOOLS-IN-ACTION

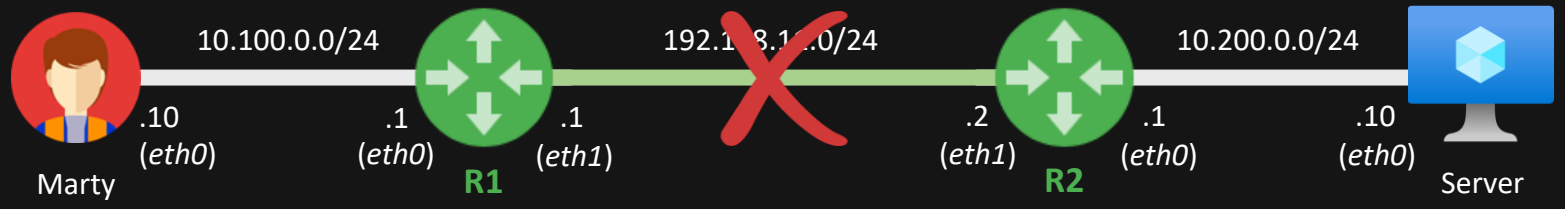
Routing tables



TOOLS-IN-ACTION

TOOLS-IN-ACTION

Civil works impact



Marty's Routing Table	
Route	Next Hop
10.100.0.0/24	*eth0*
0.0.0.0/0	10.100.0.1

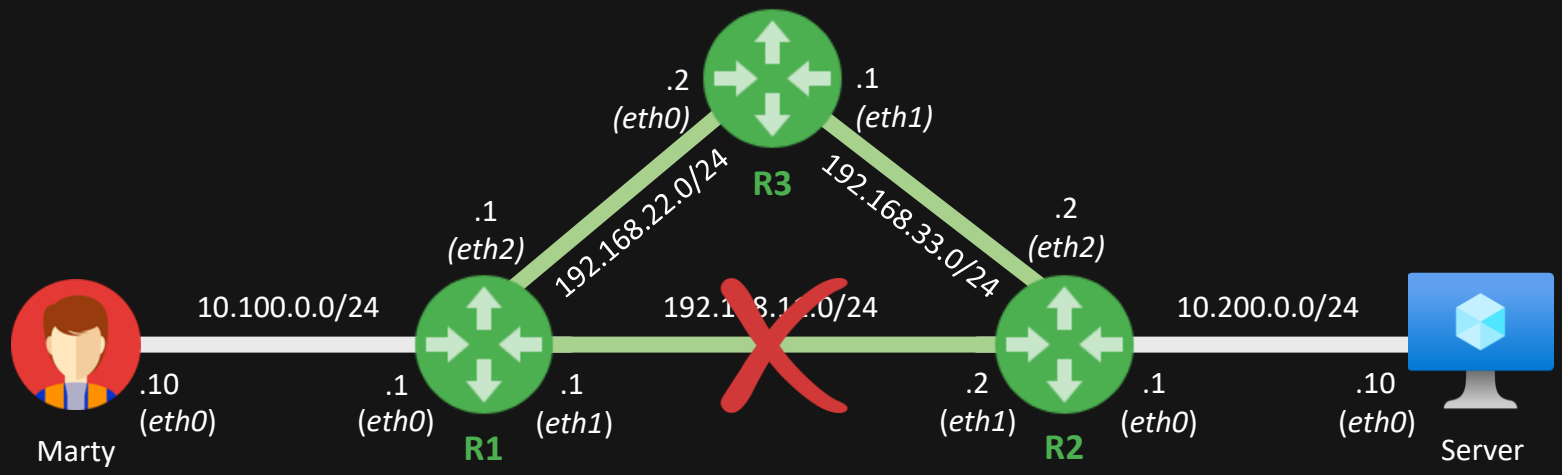
R1's Routing Table	
Route	Next Hop
10.100.0.0/24	*eth0*
~~10.200.0.0/24~~	~~192.168.11.2~~
~~192.168.11.0/24~~	~~*eth1*~~

R2's Routing Table	
Route	Next Hop
~~10.100.0.0/24~~	~~192.168.11.1~~
10.200.0.0/24	*Eth0*
~~192.168.11.0/24~~	~~*eth1*~~

Server's Routing Table	
Route	Next Hop
10.200.0.0/24	*eth0*
0.0.0.0/0	10.200.0.1

TOOLS-IN-ACTION

Path redundancy



Marty's Routing Table	
Route	Next Hop
10.100.0.0/24	*eth0*
0.0.0.0/0	10.100.0.1

R1's Routing Table	
Route	Next Hop
10.100.0.0/24	*Eth0*
~~10.200.0.0/24~~	~~192.168.11.2~~
~~192.168.11.0/24~~	~~*eth1*~~
192.168.22.0/24	*eth2*

R2's Routing Table	
Route	Next Hop
~~10.100.0.0/24~~	~~192.168.11.1~~
10.200.0.0/24	*eth0*
~~192.168.11.0/24~~	~~*eth1*~~
192.168.33.0/24	*eth2*

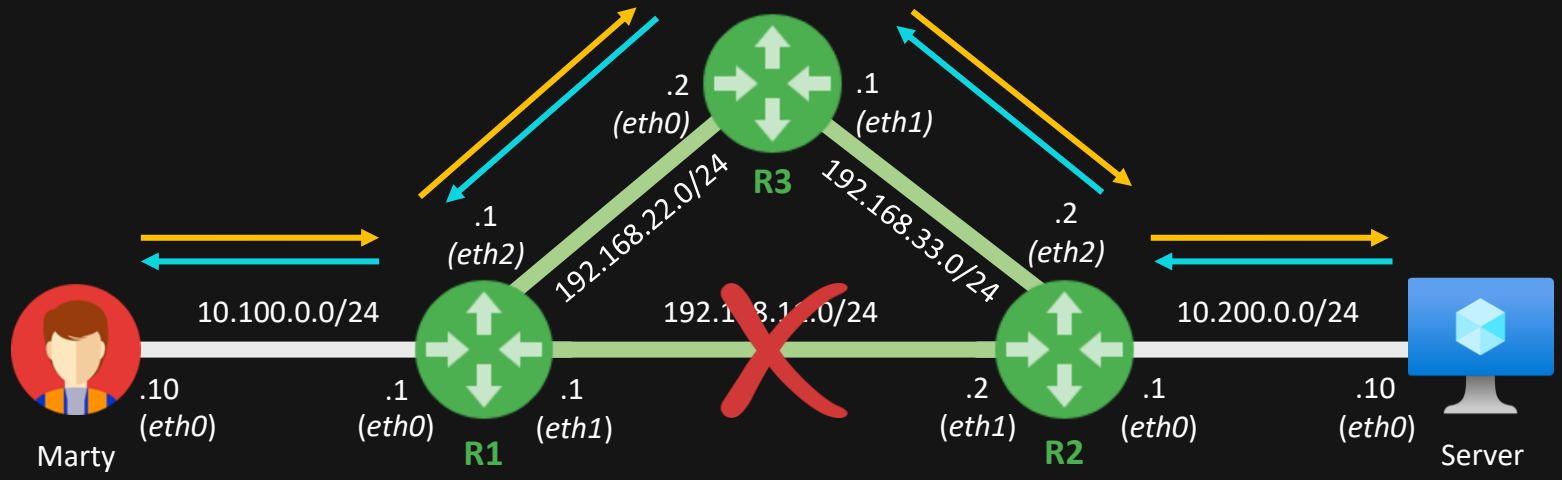
Server's Routing Table	
Route	Next Hop
10.200.0.0/24	*eth0*
0.0.0.0/0	10.200.0.1

TOOLS-IN-ACTION

Rerouting

TOOLS-IN-ACTION

R"'s Routing Table	
Route	Next Hop
10.100.0.0/24	192.168.11.1
10.200.0.0/24	192.168.22.2
192.168.11.0/24	*eth0*
192.168.22.0/24	*eth1*



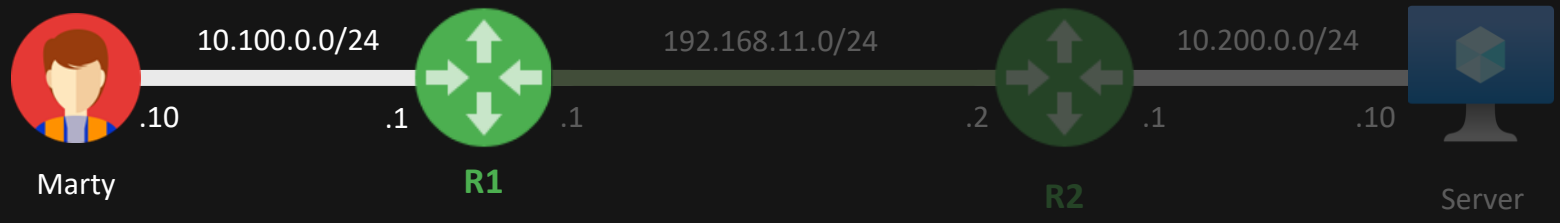
Marty's Routing Table	
Route	Next Hop
10.100.0.0/24	*eth0*
0.0.0.0/0	10.100.0.1

R1's Routing Table	
Route	Next Hop
10.100.0.0/24	*Eth0*
10.200.0.0/24	192.168.22.2
~~192.168.11.0/24~~	~~*eth1*~~
192.168.22.0/24	*eth2*

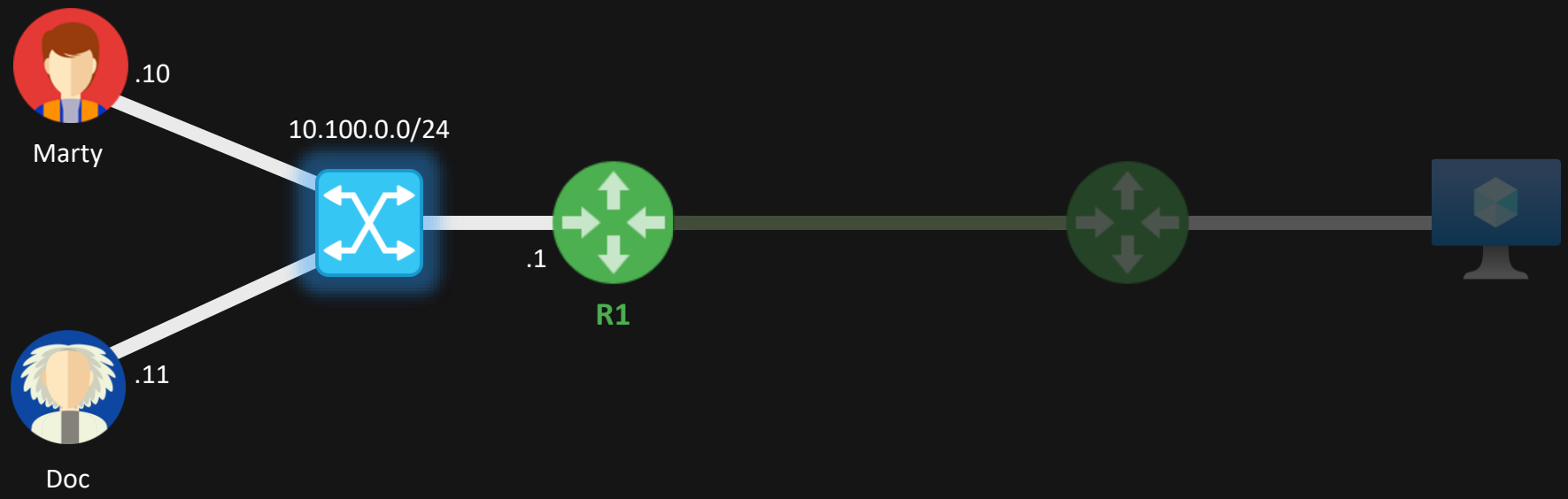
R2's Routing Table	
Route	Next Hop
10.100.0.0/24	192.168.33.1
10.200.0.0/24	*Eth0*
~~192.168.11.0/24~~	~~*eth1*~~
192.168.33.0/24	*eth2*

Server's Routing Table	
Route	Next Hop
10.200.0.0/24	*eth0*
0.0.0.0/0	10.200.0.1

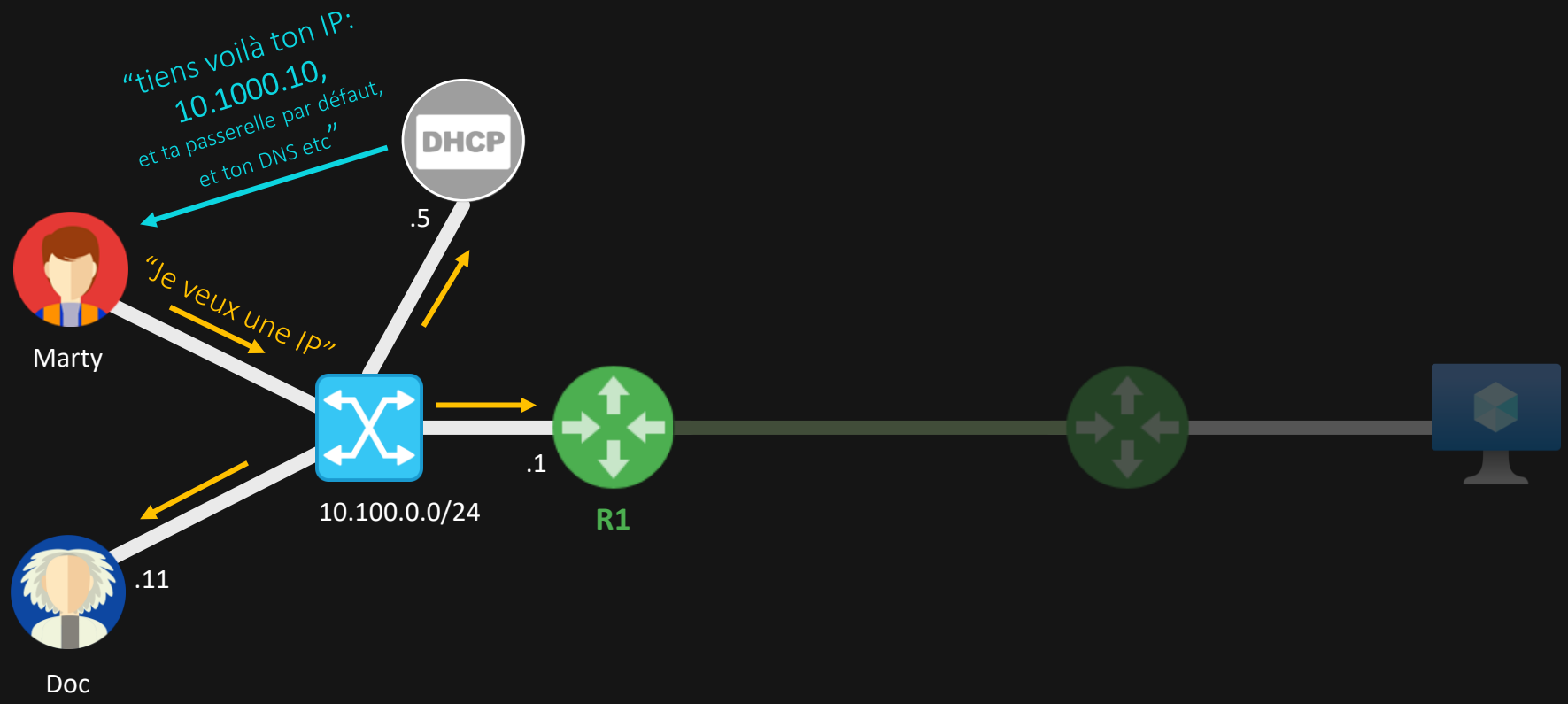
LAN connectivity



LAN connectivity

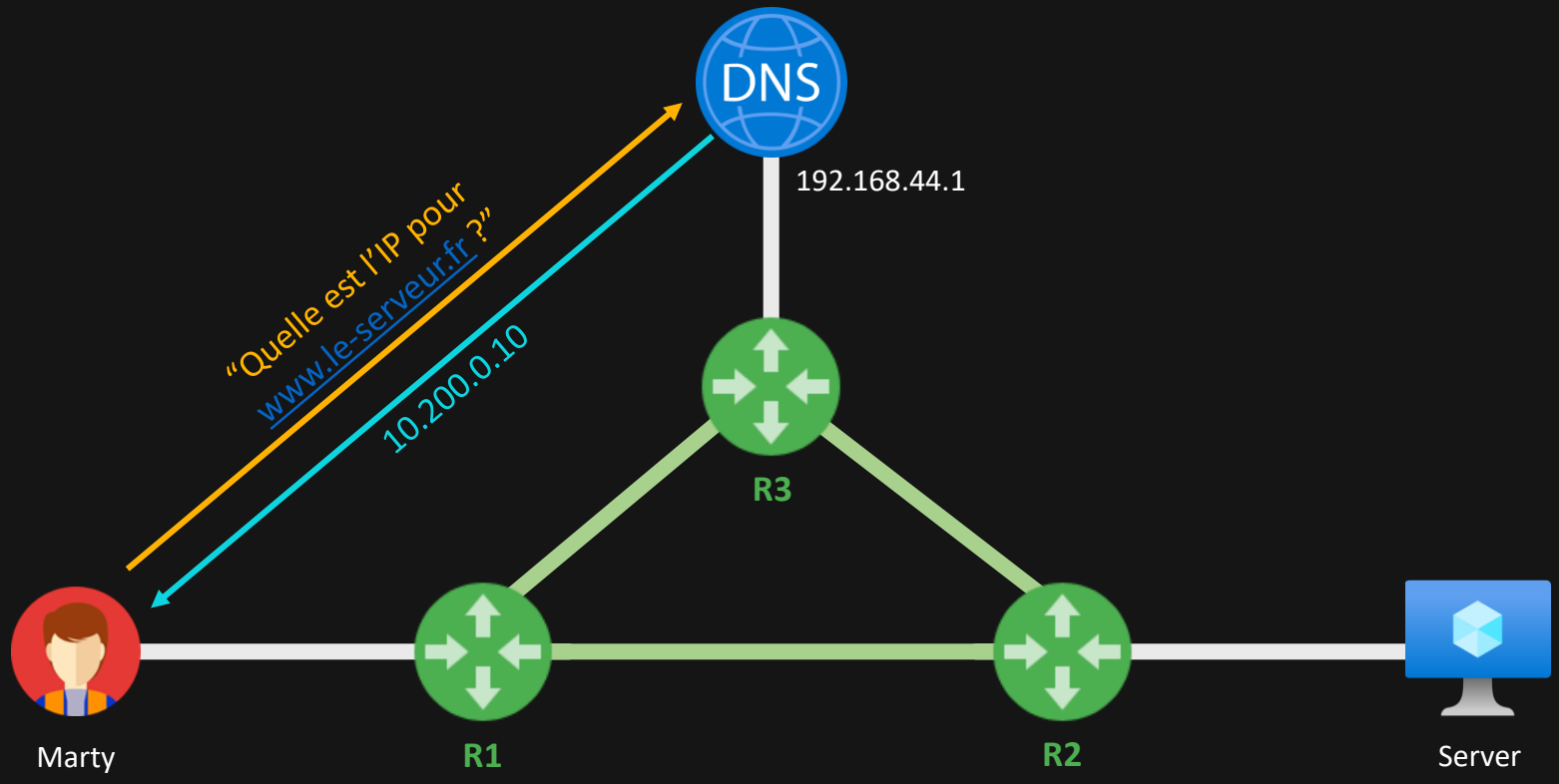


DHCP



TOOLS-IN-ACTION

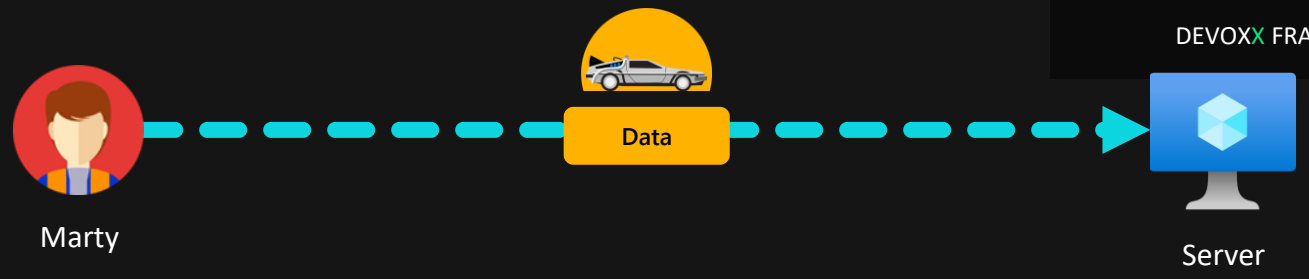
DNS



> 10.100.0.10
> /24
> 10.100.0.1
> DNS = 192.168.44.1

CONNECTIVITY

OSI model



7	Application Layer	HTTP, DNS, SMTP...
6	Presentation Layer	JPEG, MPEG, IMAP...
5	Session Layer	RPC(Sockets)...
4	Transport Layer	TCP UDP
3	Network Layer	IP ICMP IPSec...
2	Data Link Layer	ARP VLAN STP...
1	Physical Layer	Hubs Fiber...

Encapsulation

HTTP header	Data				Data
TCP header	HTTP header	Data			TCP Segment UDP Packet
IP header	TCP header	HTTP header	Data		IP Datagram
MAC header	IP header	TCP header	HTTP header	Data	Frame
1000110101001011...					Bit

Decapsulation

7 6 5 4 3 2 1

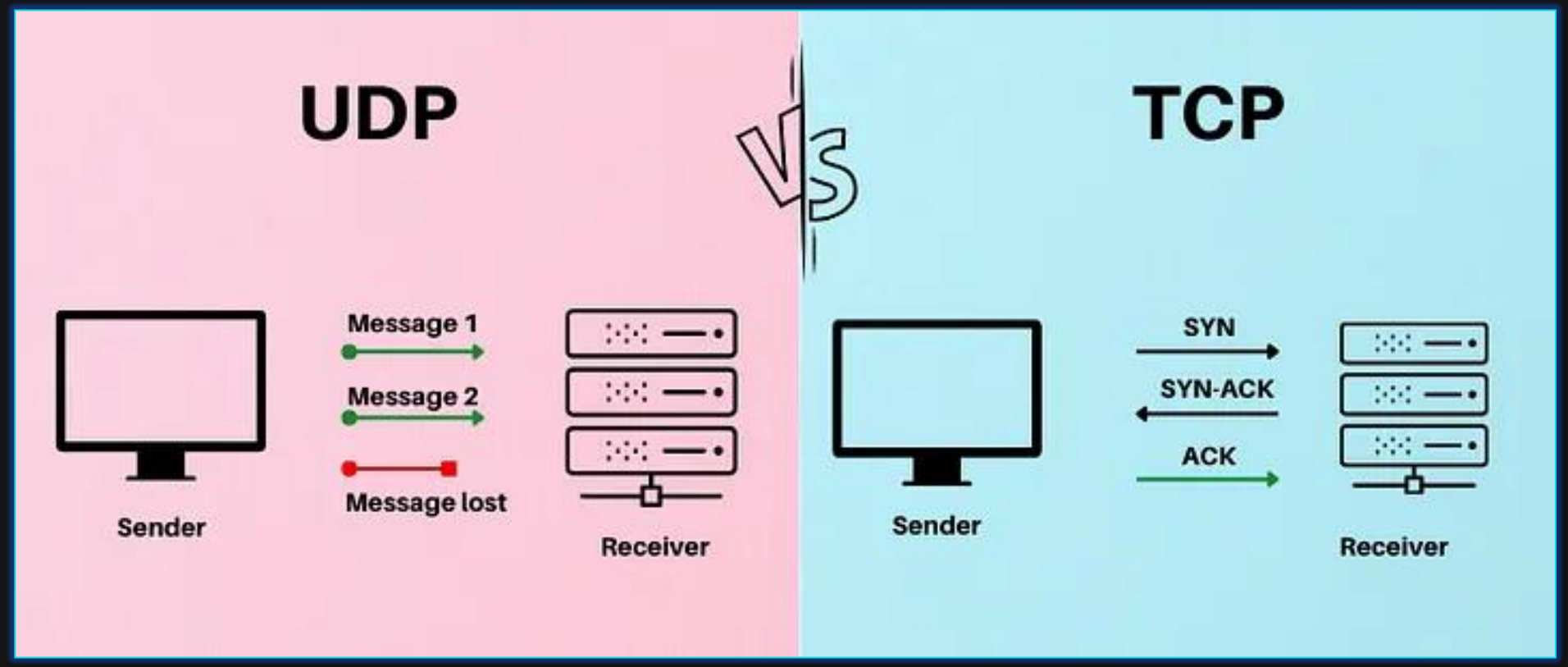
- Source MAC address
- Destination MAC address
- Frame control
- Sequence control

- Source IP address
- Destination IP address
- Datagram sequence order

- Source port
- Destination port
- Sequence number

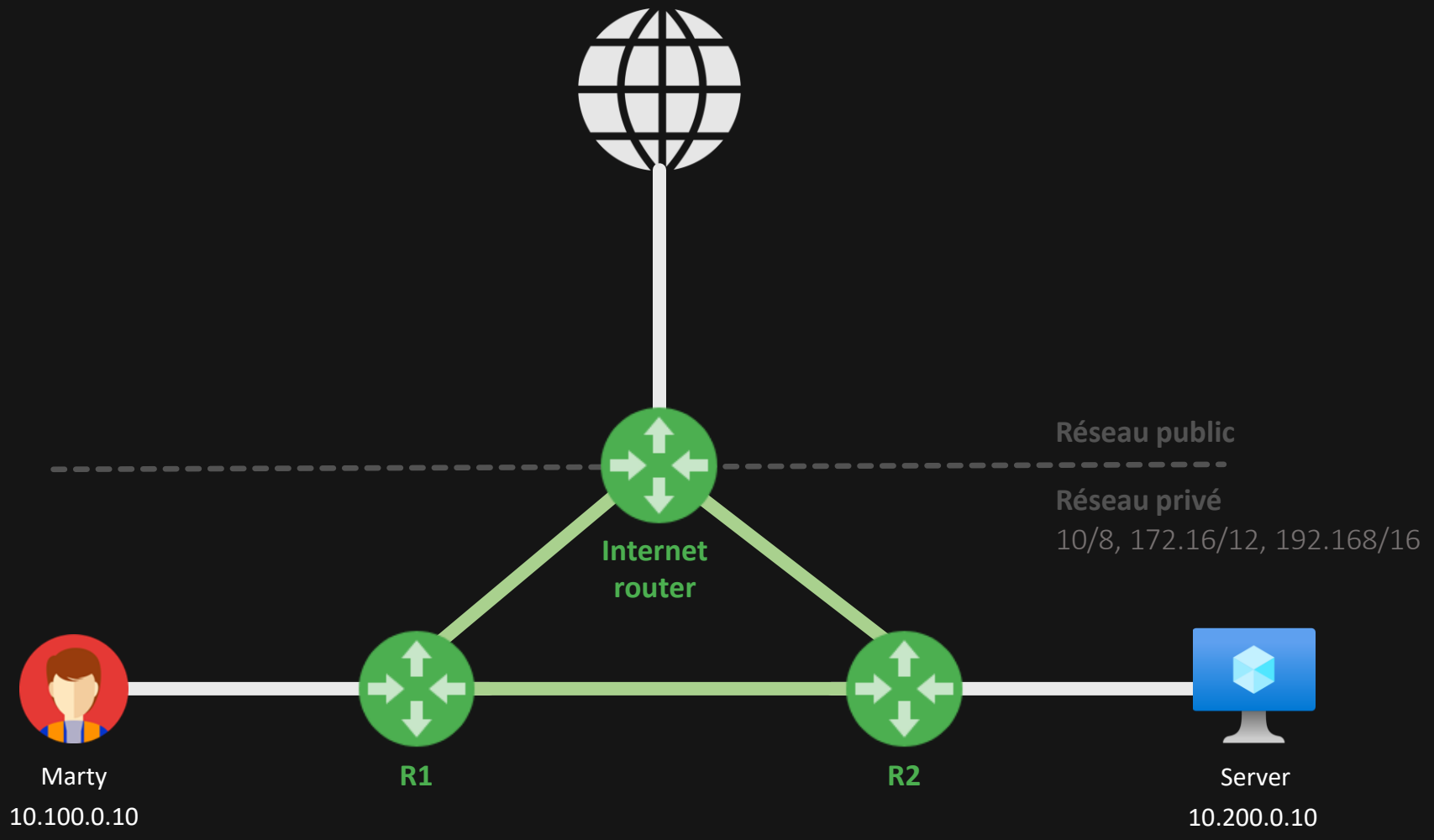
TOOLS-IN-ACTION

UDP vs TCP

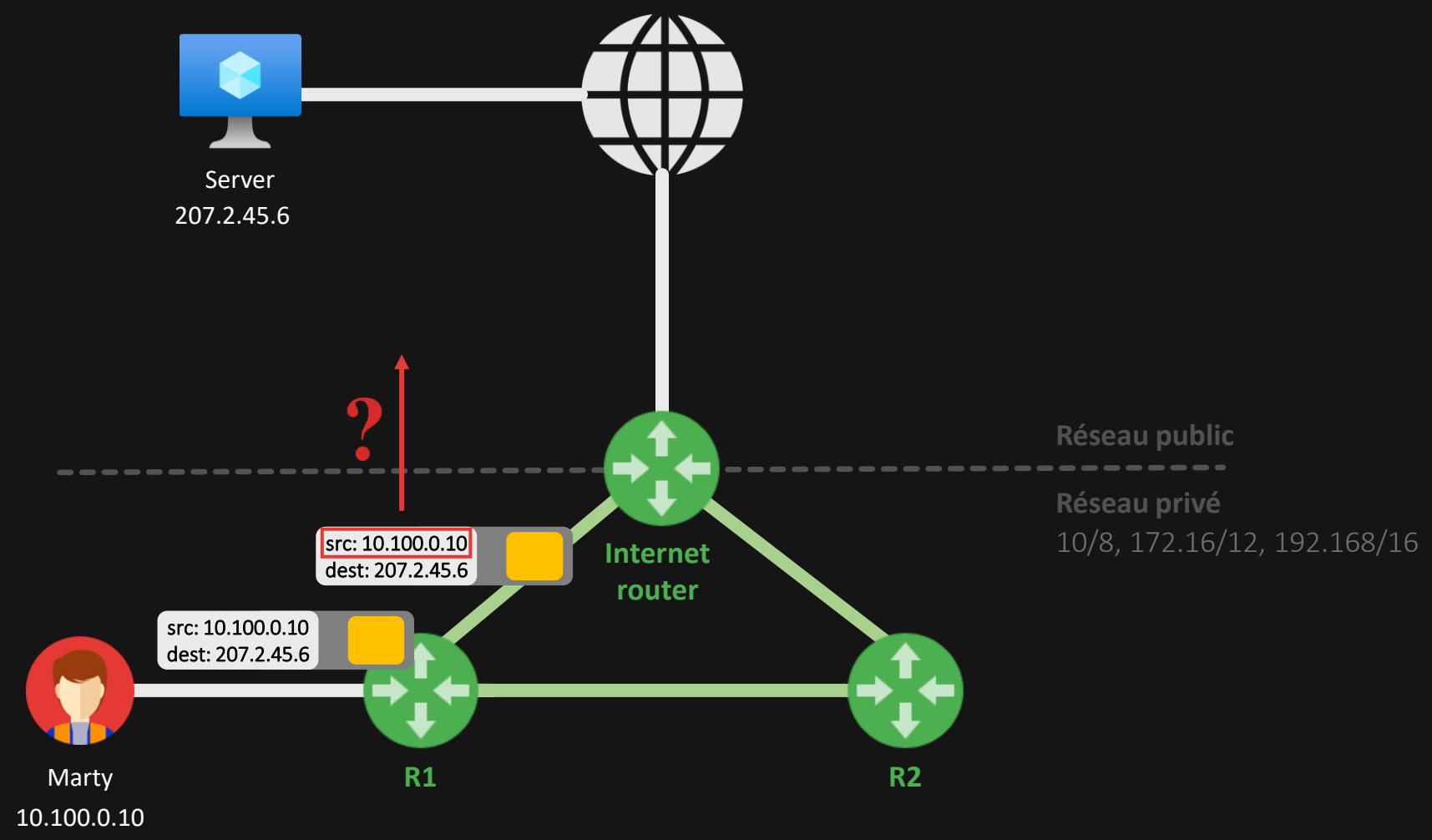


UDP vs TCP

Private network vs public network

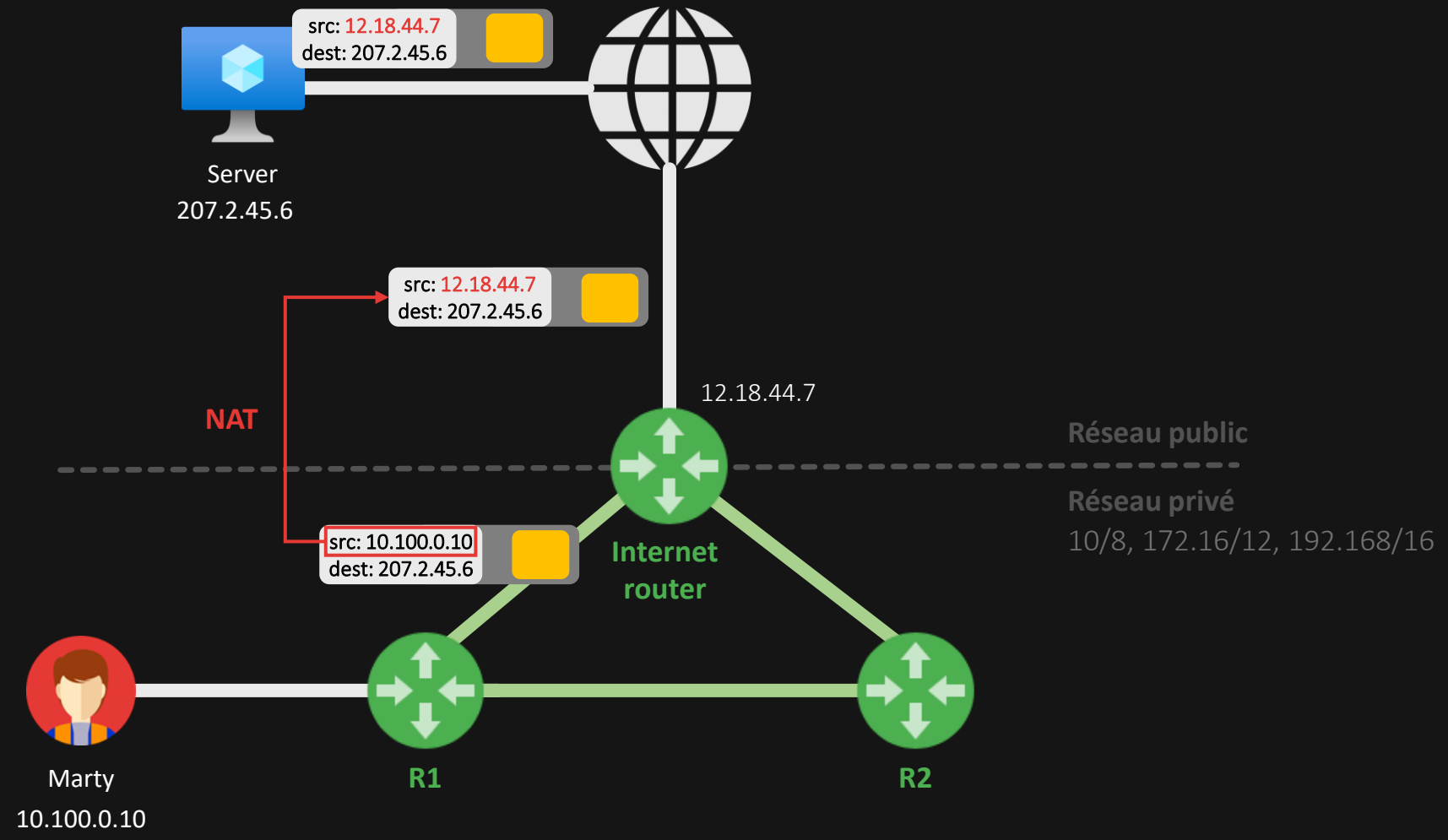


Internet access



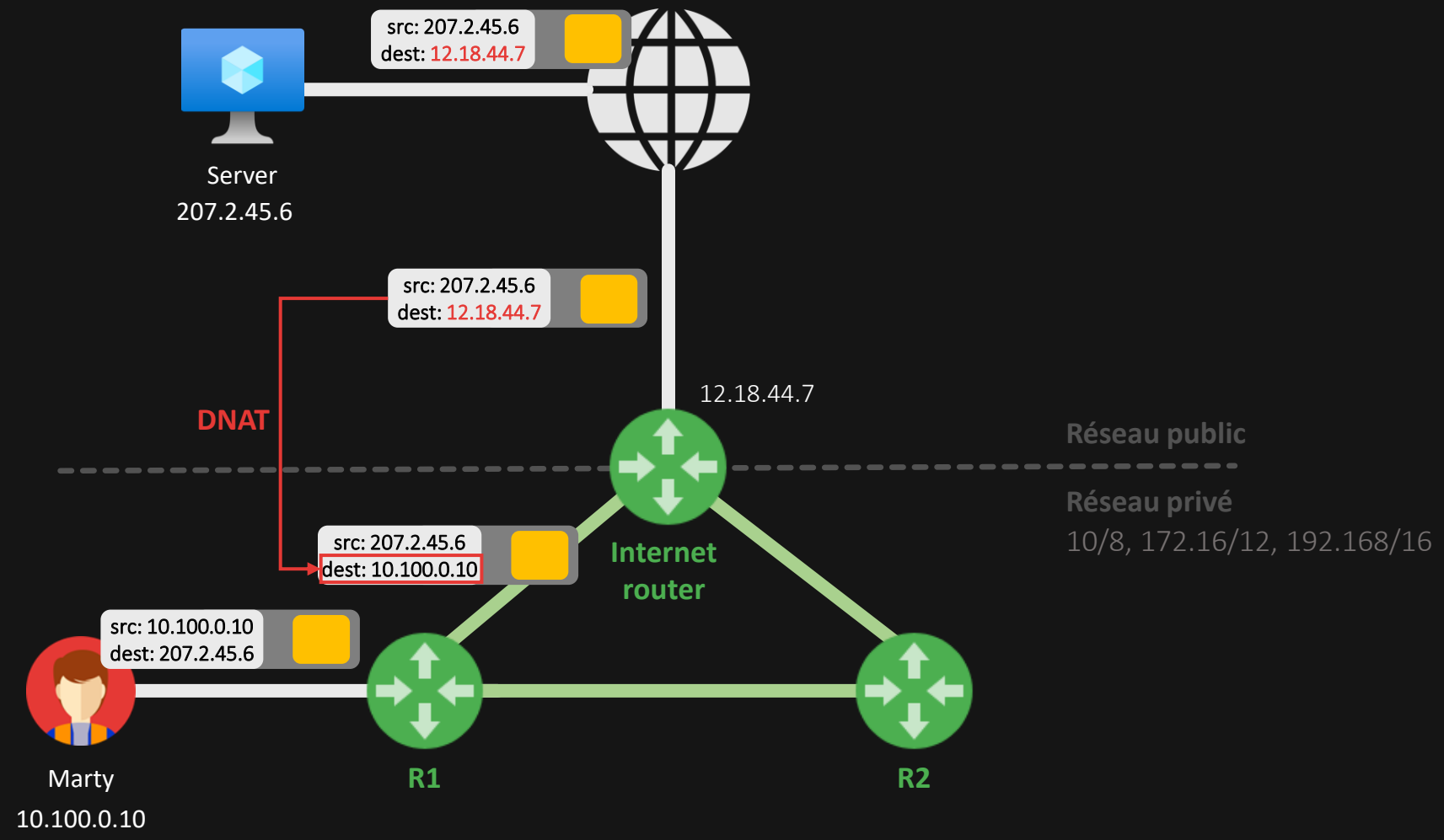
TOOLS-IN-ACTION

Internet access



TOOLS-IN-ACTION

Internet access



TOOLS-IN-ACTION

Latency, Bandwidth & Throughput

Latency

- The amount of time it takes data to move back and forth along a connection

Bandwidth

- The total capacity of a connection to move data

Throughput

- The actual amount of data that moves across a connection during a given time.

DALL·E Prompt: A close-up view of the Golden Gate Bridge in San Francisco, illuminated against the vibrant night sky, seen from an aerial perspective, reminiscent of a scene from a futuristic movie.

What could go wrong?

$ curl

- Command that lets you send or receive data from a website or file on a network.

```
$ curl 10.200.0.10
curl: (28) Failed to connect to 10.200.0.10 port 80: Connection timed out
```

TOOLS-IN-ACTION

$ ping

TOOLS-IN-ACTION

How it works:

- Sends Internet Control Message Protocol (ICMP) packets to a specified address.
- If the target server returns an ICMP echo reply, it is connected to the network.

Example:

```
$ ping 10.200.0.10
PING 10.200.0.10 (10.200.0.10) 56(84) bytes of data.
^C
--- 10.200.0.10 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2098ms
```

Possible Root Causes:

- The host is down
- There is no route from Marty to the host
- Firewall blocking the connection

Network troubleshooting #1

Display the kernel routing table

- Using `ip route`:

```
marty@devoxx:~$ ip route
default via 10.100.0.1 dev eth0 proto dhcp src 10.100.0.10 metric 100
10.100.0.0/24 dev eth0 proto kernel scope link src 10.100.0.10
168.63.129.16 via 10.100.0.1 dev eth0 proto dhcp src 10.100.0.10 metric 100
169.254.169.254 via 10.100.0.1 dev eth0 proto dhcp src 10.100.0.10 metric 100
```

- Using `netstat`:

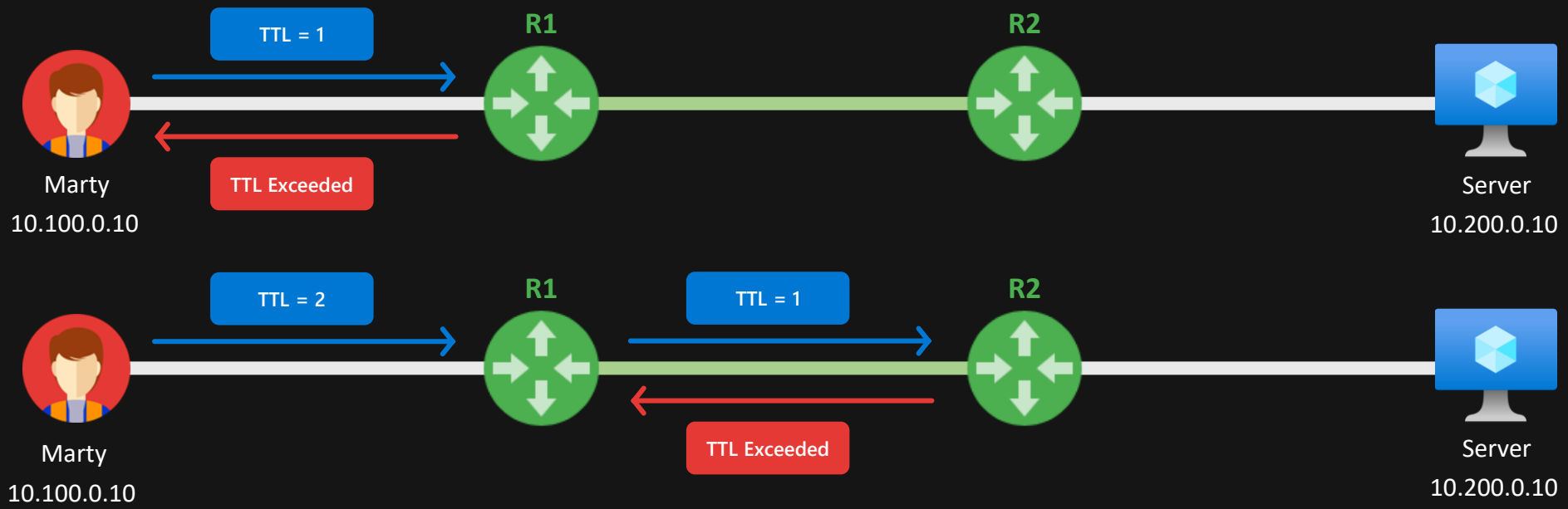
```
marty@devoxx:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.100.0.1      0.0.0.0         UG        0 0          0 eth0
10.100.0.0      0.0.0.0         255.255.255.128 U         0 0          0 eth0
168.63.129.16   10.100.0.1      255.255.255.255 UGH       0 0          0 eth0
169.254.169.254 10.100.0.1      255.255.255.255 UGH       0 0          0 eth0
```

$ traceroute

Two functions:

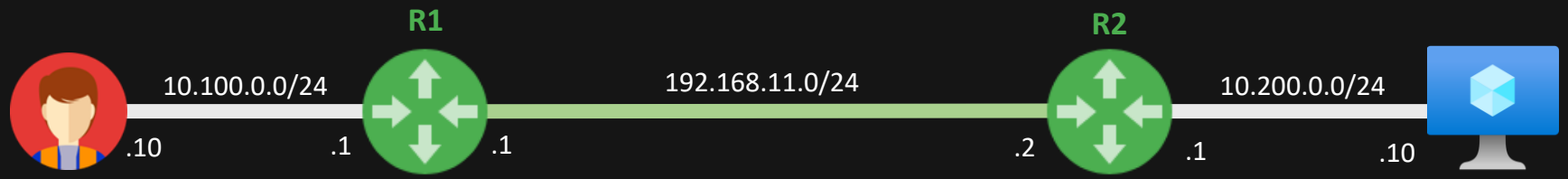
- Identifies each hop (that replies) in the path from a client computer to the destination entered in the `traceroute` command.
- Measures the round trip time for each hop in the path

How it works:



TOOLS-IN-ACTION

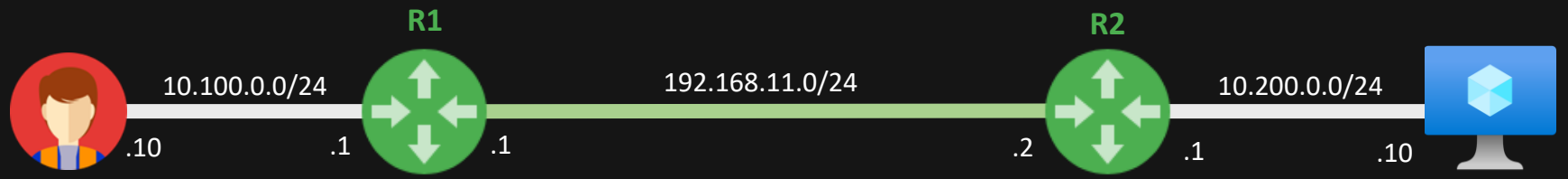
$ traceroute




```
marty@devoxx:~$ traceroute 10.200.0.10
traceroute to 10.200.0.10 (10.200.0.10), 30 hops max, 60 byte packets
 1  10.100.0.1 2.682 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
```

TOOLS-IN-ACTION

$ traceroute




```
marty@devoxx:~$ traceroute 10.200.0.10
traceroute to 10.200.0.10 (10.200.0.10), 30 hops max, 60 byte packets
 1  10.100.0.1  2.920 ms
 2  192.168.11.2 (192.168.11.2)  5.085 ms
 3  10.200.0.10 (10.200.0.10)  6.980 ms
```

TOOLS-IN-ACTION

Network troubleshooting #2

```
marty@devoxx:~$ ping 10.200.0.10
PING 10.200.0.10 (10.200.0.10) 56(84) bytes of data.
64 bytes from 10.200.0.10: icmp_seq=1 ttl=63 time=6.74 ms
64 bytes from 10.200.0.10: icmp_seq=2 ttl=63 time=3.66 ms
64 bytes from 10.200.0.10: icmp_seq=3 ttl=63 time=3.88 ms
64 bytes from 10.200.0.10: icmp_seq=4 ttl=63 time=5.21 ms
^C
--- 10.200.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 3.659/4.872/6.744/1.231 ms
```

```
marty@devoxx:~$ curl 10.200.0.4
curl: (7) Failed to connect to 10.200.0.4 port 80: Connection refused
```

Possible Root Causes:

- No service listening on the specified port (:80)
- Firewall blocking the connection

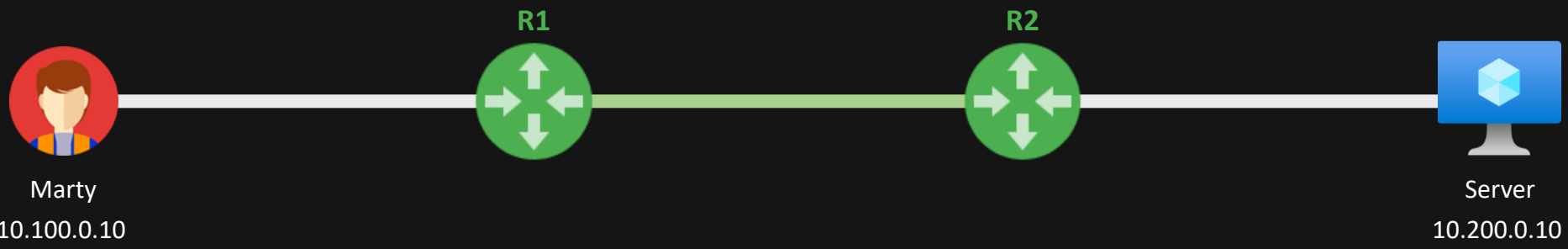
$ netstat

- Command that show network connections, routing tables, and a number of network interface & network protocol statics.

```
root@server:~$ netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      575/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      857/sshd: /usr/sbin
tcp6       0      0 :::22                   :::*                    LISTEN      857/sshd: /usr/sbin
udp        0      0 127.0.0.1:323           0.0.0.0:*                           714/chronyd
udp        0      0 127.0.0.1:25224         0.0.0.0:*                           1135/ruby
udp        0      0 127.0.0.53:53           0.0.0.0:*                           575/systemd-resolve
udp        0      0 10.100.0.4:68           0.0.0.0:*                           573/systemd-network
udp6       0      0 ::1:323                 :::*                                714/chronyd
```

TOOLS-IN-ACTION

$ curl




```
marty@devoxx:~$ curl 10.200.0.10

Hello Devoxx France!
```

TOOLS-IN-ACTION

$ sockperf *– for latency, packet loss …*

```
marty@devoxx:~$ sockperf pp -i 10.200.0.10 -m 64

sockperf: == version #3.6-no.git ==
sockperf[CLIENT] send on:sockperf: using recvfrom( ) to block on socket(s)

[ 0] IP = 10.200.0.10      PORT = 11111 # UDP
sockperf: Warmup stage (sending a few dummy messages)...
sockperf: Starting test...
sockperf: Test end (interrupted by timer)
sockperf: Test ended
sockperf: [Total Run] RunTime=1.000 sec; Warm up time=400 msec; SentMessages=192; ReceivedMessages=191
sockperf: ========== Printing statistics for Server No: 0
sockperf: [Valid Duration] RunTime=0.552 sec; SentMessages=107; ReceivedMessages=107
sockperf: ====> avg-latency=2579.605 (std-dev=396.137)
sockperf: # dropped messages = 0; # duplicated messages = 0; # out-of-order messages = 0
sockperf: Summary: Latency is 2579.605 usec
sockperf: Total 107 observations; each percentile contains 1.07 observations
sockperf: ---> <MAX> observation = 5068.870
sockperf: ---> percentile 99.999 = 5068.870
sockperf: ---> percentile 99.990 = 5068.870
sockperf: ---> percentile 99.900 = 5068.870
sockperf: ---> percentile 99.000 = 3932.427
sockperf: ---> percentile 90.000 = 2911.623
sockperf: ---> percentile 75.000 = 2690.890
sockperf: ---> percentile 50.000 = 2474.818
sockperf: ---> percentile 25.000 = 2339.955
sockperf: ---> <MIN> observation = 2016.383
```

TOOLS-IN-ACTION

$ sockperf *– for throughput*

```
marty@devoxx:~$ sockperf throughput --tcp -i 10.200.0.10 -p 12345 -m 1500 -t 20
sockperf: == version #3.6-no.git ==
sockperf[CLIENT] send on:
[ 0] IP = 10.200.0.10      PORT = 12345 # TCP
sockperf: Warmup stage (sending a few dummy messages)...
sockperf: Starting test...
sockperf: Test end (interrupted by timer)
sockperf: Test ended
sockperf: Total of 1535781 messages sent in 20.001 sec

sockperf: NOTE: test was performed, using msg-size=1500. For getting maximum throughput consider using --msg-size=1472
sockperf: Summary: Message Rate is 76787 [msg/sec], Packet Rate is about 153574 [pkt/sec] (2 ip frags / msg)
sockperf: Summary: BandWidth is 109.845 MBps (878.757 Mbps)
```

TOOLS-IN-ACTION

Alternatives:

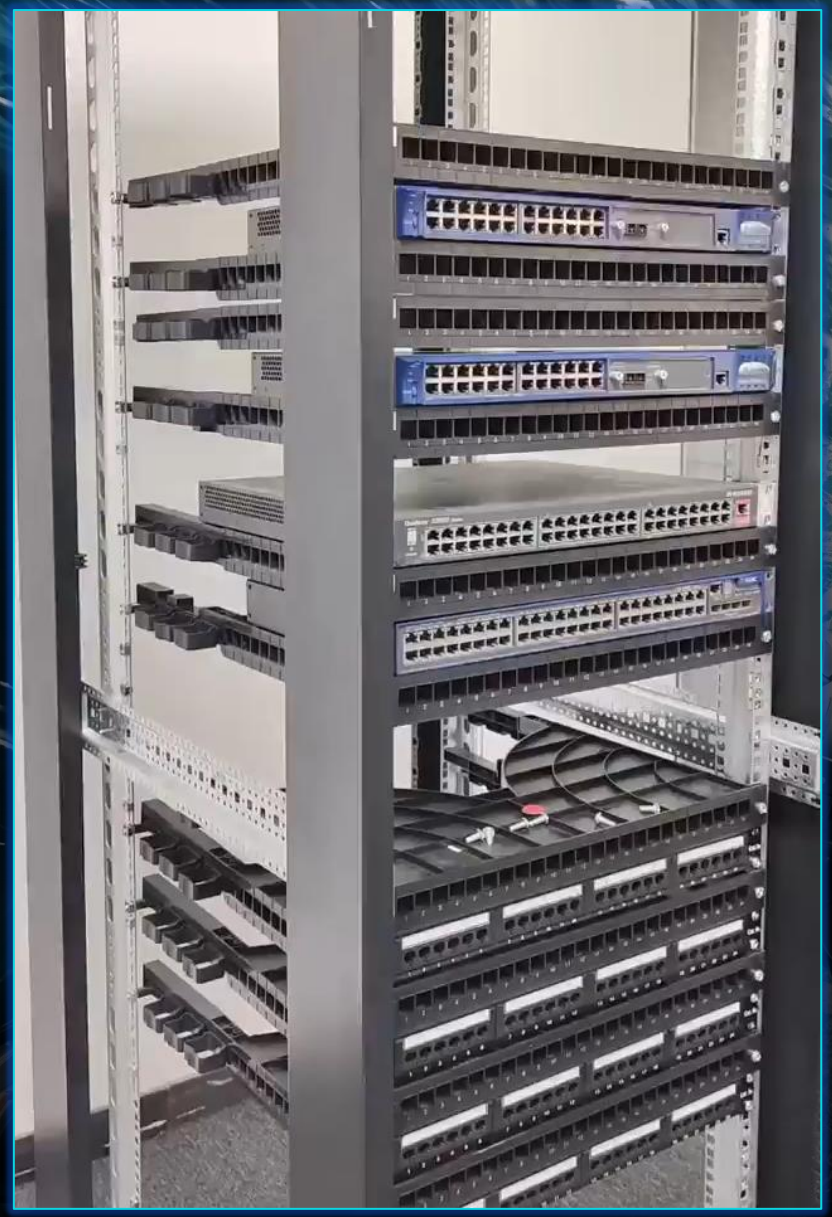
- Ntttcp, iperf, iperf3, Tcptrack

$ dig – *for DNS*

```
marty@devoxx:~$ dig www.backtothefuture.com

; <<>> DiG 9.16.48-Ubuntu <<>> www.backtothefuture.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10964
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.backtothefuture.com.       IN      A

;; ANSWER SECTION:
www.backtothefuture.com. 1800   IN      CNAME   ext-sq.squarespace.com.
ext-sq.squarespace.com. 6       IN      A       198.49.23.145
ext-sq.squarespace.com. 6       IN      A       198.185.159.144
ext-sq.squarespace.com. 6       IN      A       198.49.23.144
ext-sq.squarespace.com. 6       IN      A       198.185.159.145

;; Query time: 32 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Apr 04 10:37:08 UTC 2024
;; MSG SIZE  rcvd: 149
```

www.diggui.com

TOOLS-IN-ACTION



THANKS
FOR WATCHING

DEVOXX FRANCE 2024