Networking Basics

04d - How does Traceroute really work?

Wolfgang Tremmel
academy@de-cix.net

Networking Basics

DE-CIX Academy

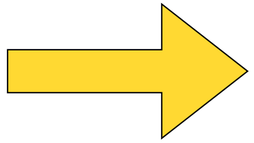
01 - Networks, Packets, and Protocols

02 - Ethernet, 02a - VLANs, 02b - QinQ

03 - IP, 03a - Routing, 03b - Global routing

04a - UDP, 04b - TCP

04c - Internet Control Message Protocol (ICMP)



04d - How does Traceroute really work?

05 - Uni-, Broad-, Multi-, and Anycast

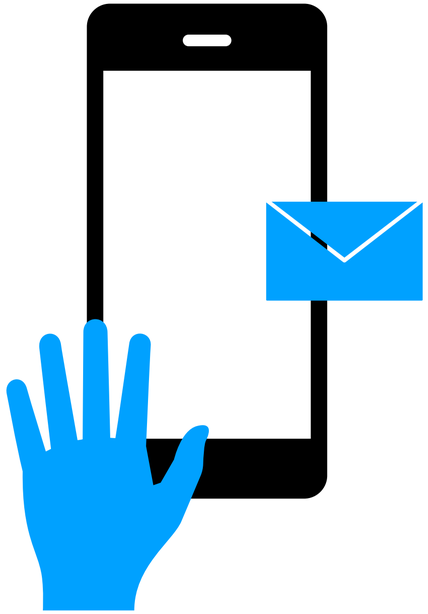
06a - Domain Name System (DNS)

DE-CIX

Reasons for Packets

TCP and UDP

- Why are packets being sent?
  - Because a user clicks on something
  - Or a machine reacts to an event
- Some program on the application layer needs to send data

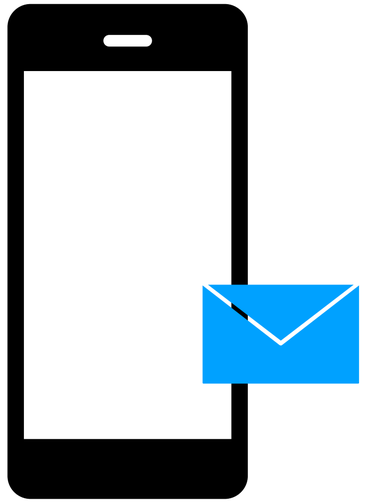


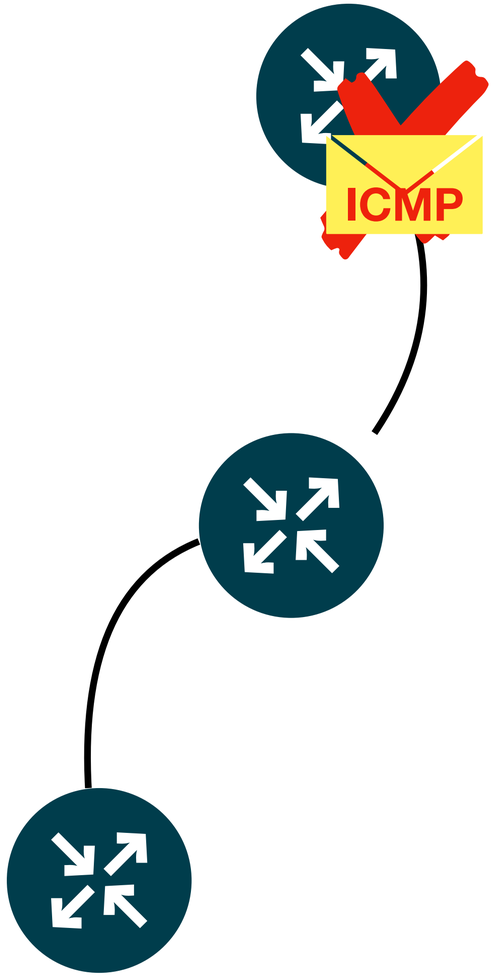
DE CIX

Reason for Packets

ICMP

- This is different for ICMP
- ICMP usually is a reaction to a network event
- Like an error message
- Often sent by a router
  - To indicate an error in transmission for example

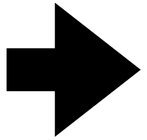




Internet Model

ICMP - Internet Control Message Protocol

- The IP stack is not as strict with layers as the OSI stack
- ICMP uses IP for transport
- But it does not have anything "above" it



Layer	Name
4	**ICMP**
3	Internet
2	Link
1	Physical

DE CIX

```
dhcp-143-152:~ wtremmel$ 
```

Traceroute

DE CIX

Traceroute

You have all seen it...

- Does traceroute tell the "truth"?
- All the truth?
- Can you rely on it when debugging a routing problem?
- And...

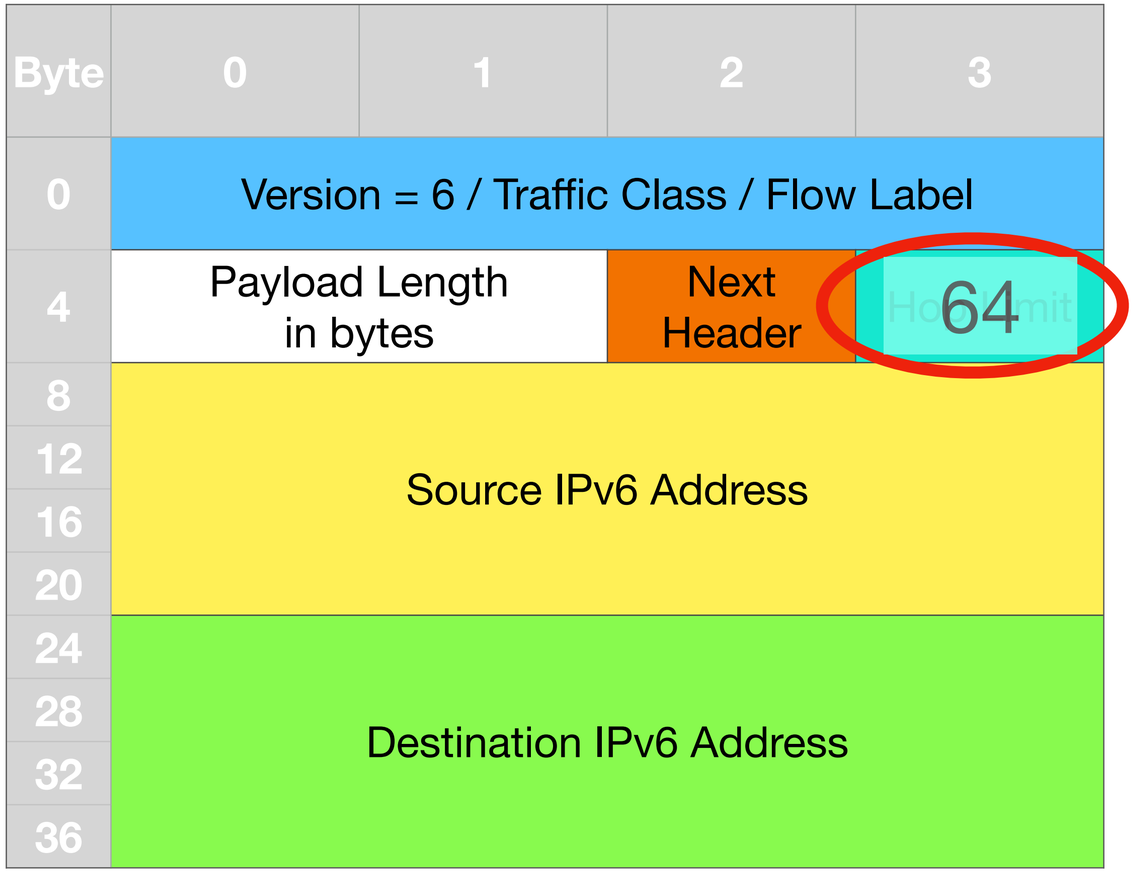
How does it actually work?

DE CIX

Rember the IP header?

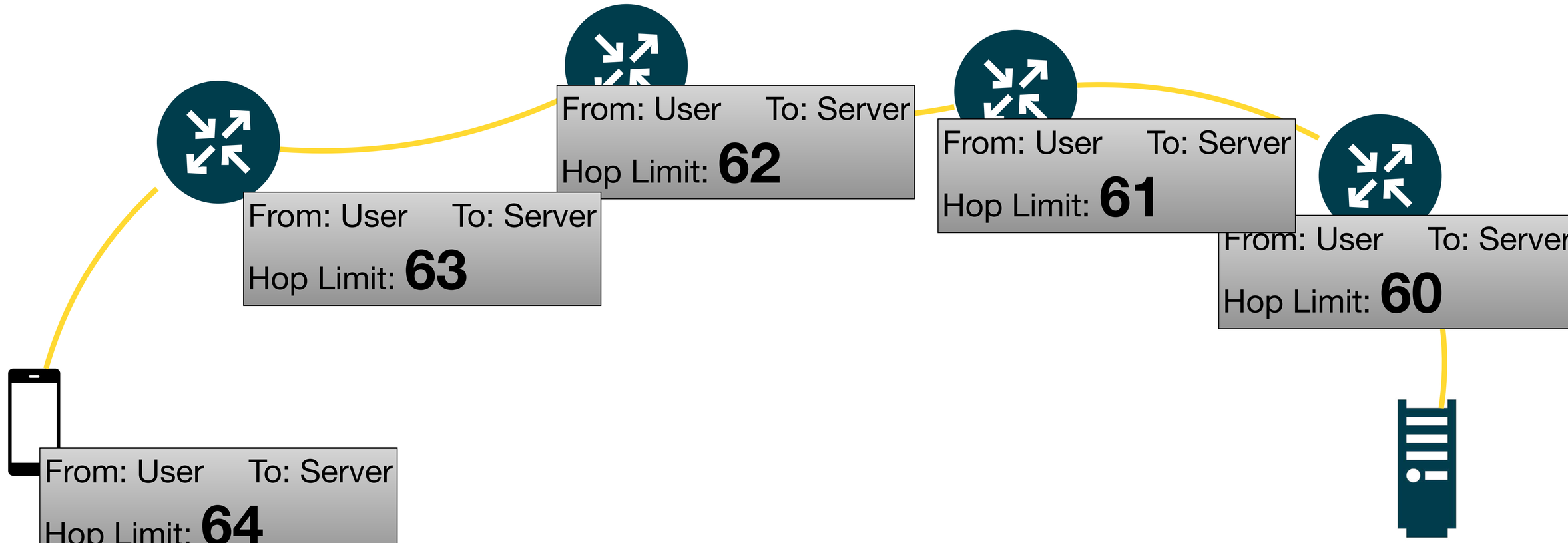
Time To Live / Hop Limit

- Remember the hop limit field in the IPv6 header?
  - In IPv4 it is called "Time to live" but serves the same function
- When a packet is sent, Hop Limit is initialized to a value 1-255
- It is decreased by every router forwarding the packet
- Once it hits zero, the packet is discarded



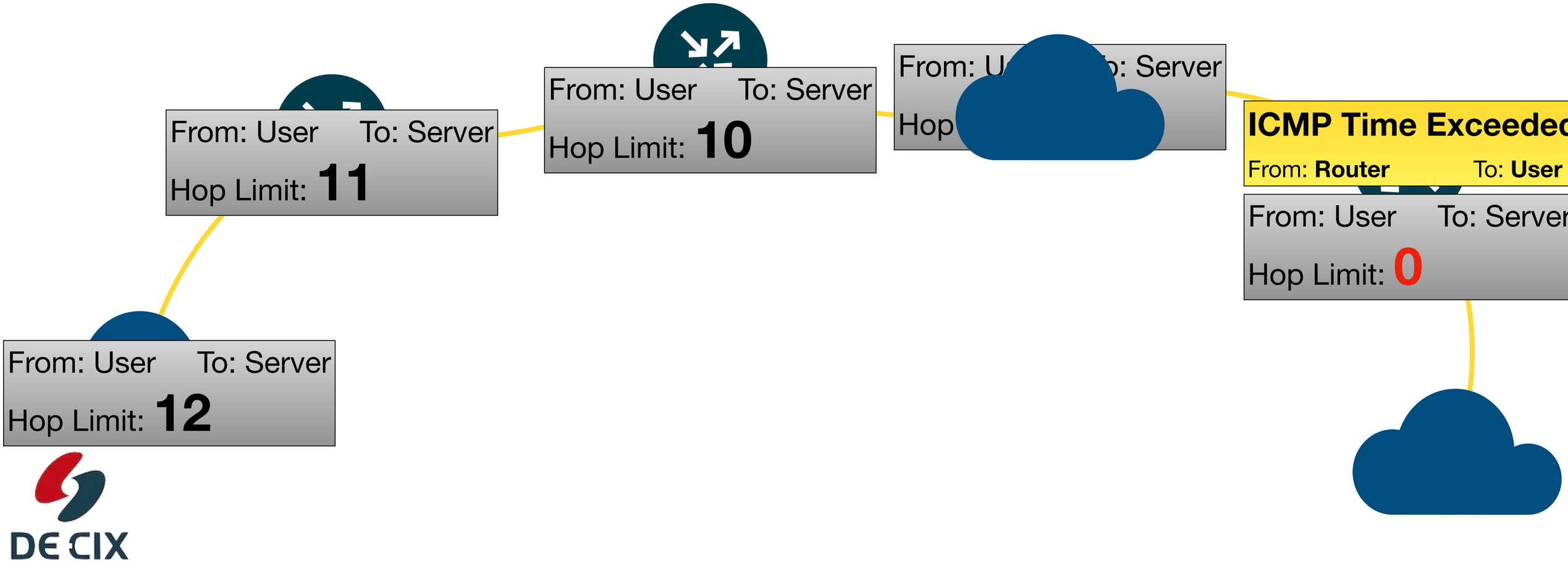
Hop Limit

Decreased at every "hop"



Hop Limit

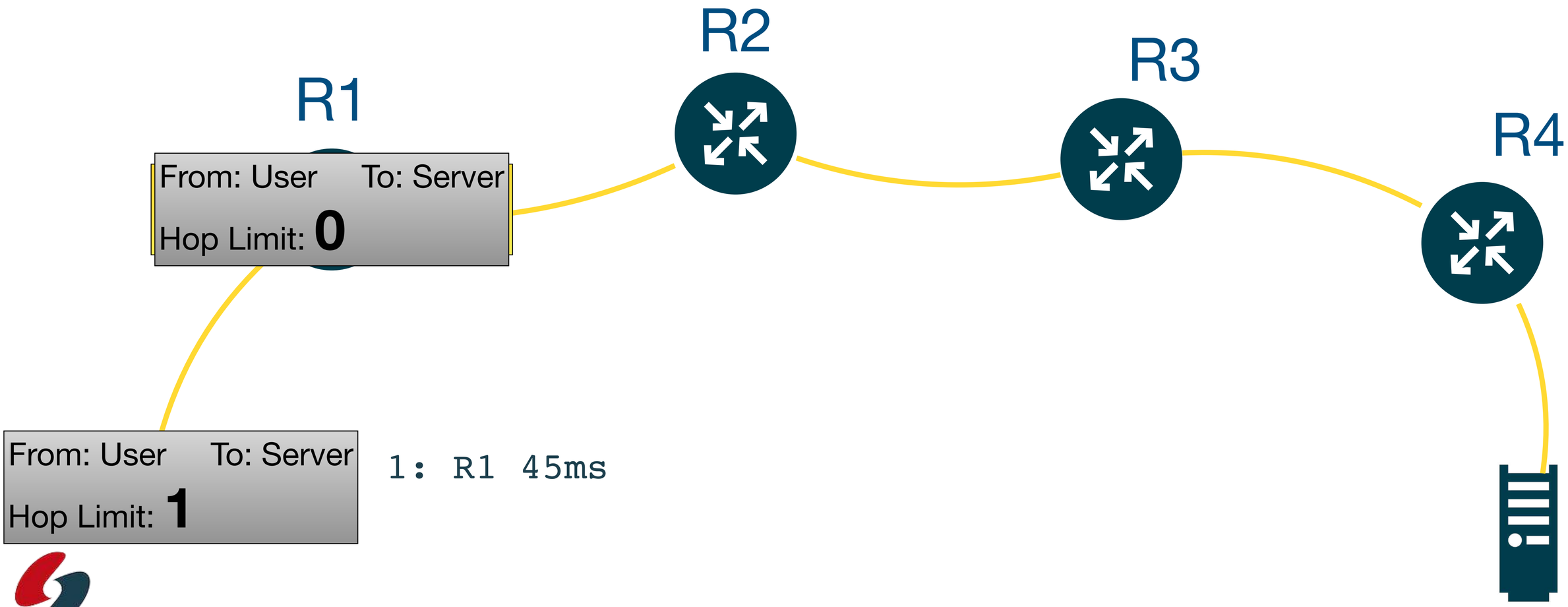
What happens if it hits zero?



How does Traceroute use this?

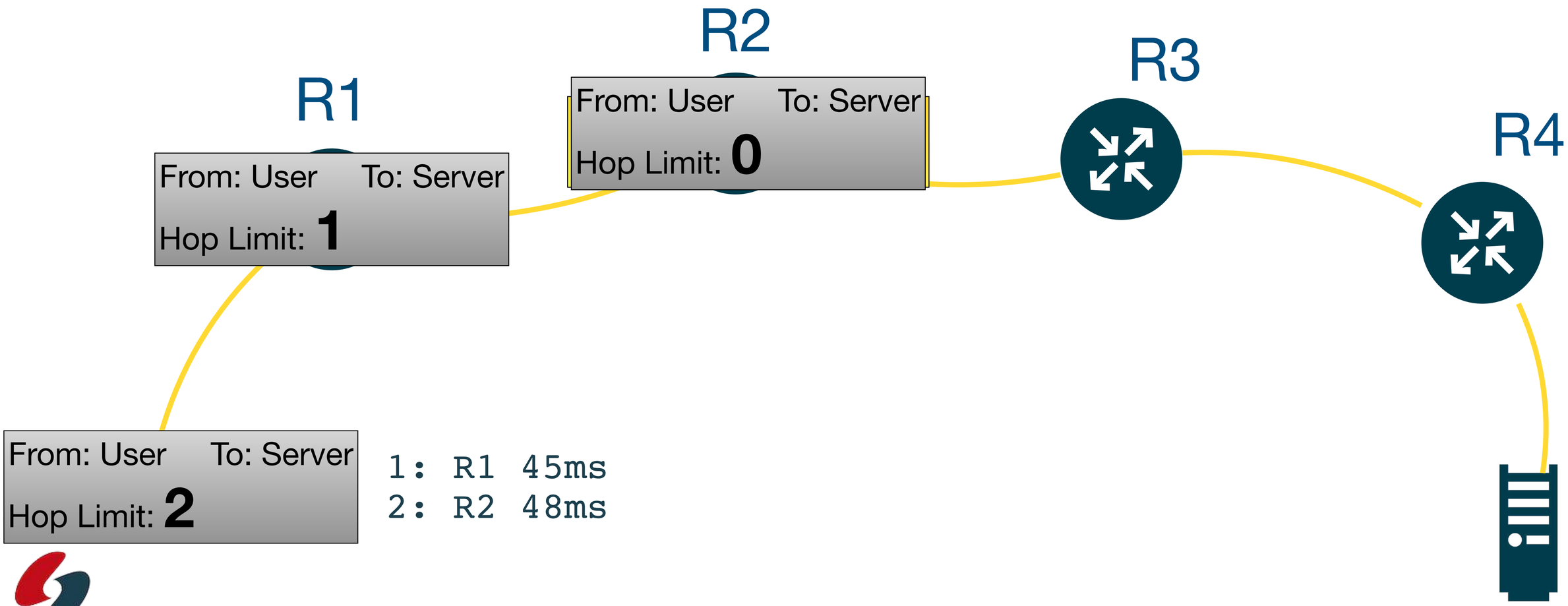
Traceroute

Using Hop Limit / TTL to trace packets



Traceroute

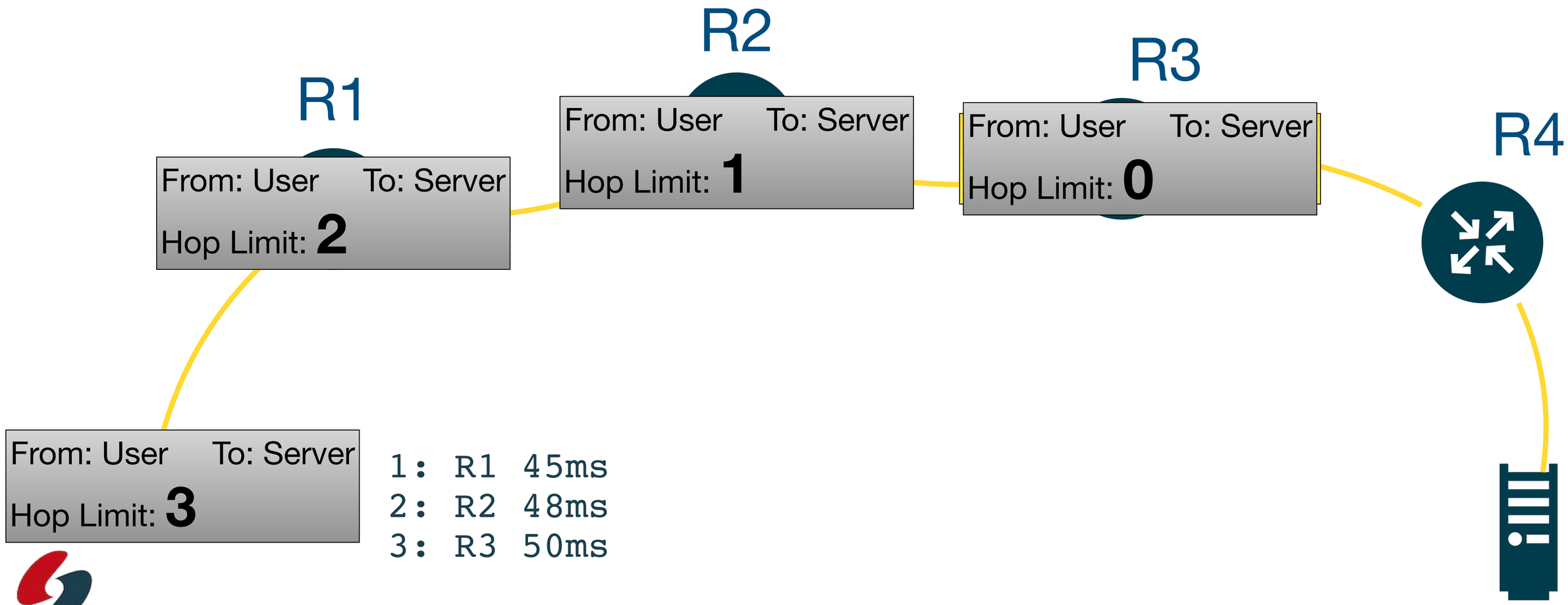
Using Hop Limit / TTL to trace packets



DE CIX

Traceroute

Using Hop Limit / TTL to trace packets

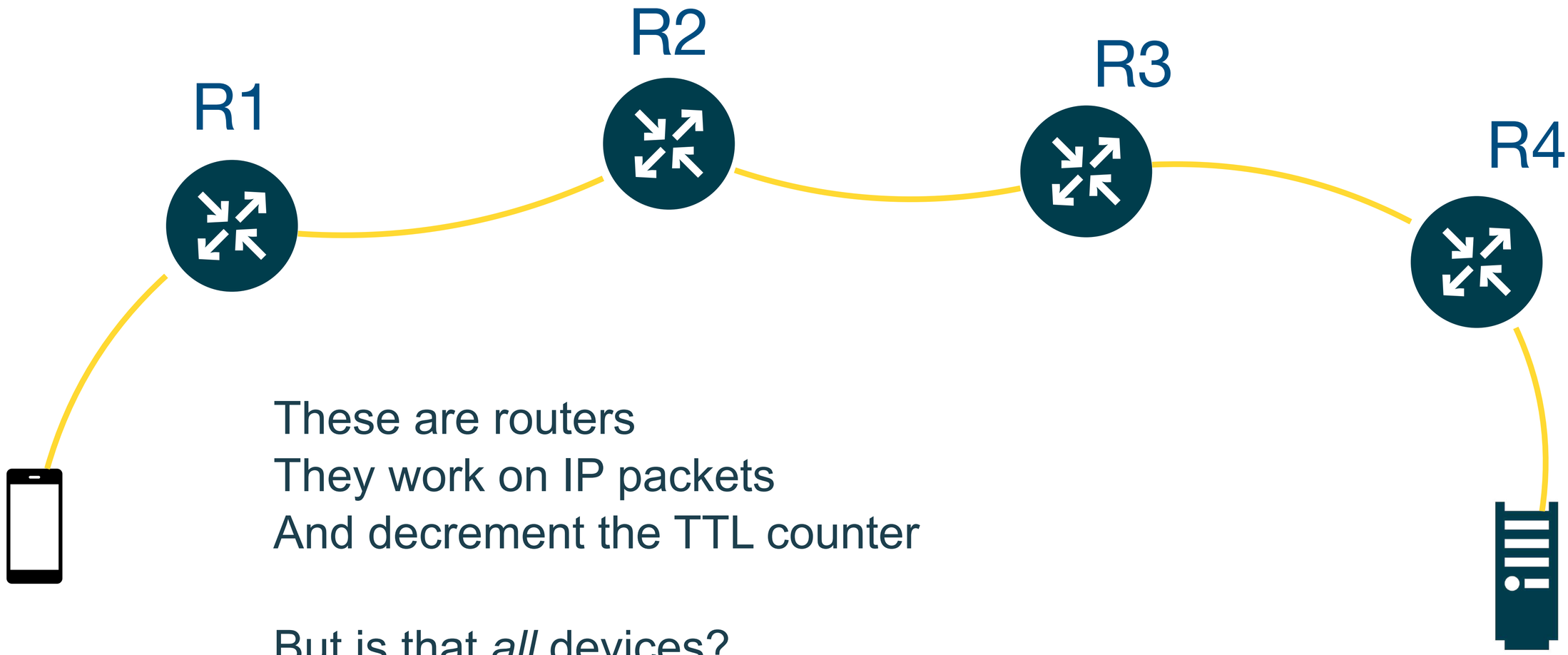


DE CIX

Do I see *all* devices?

Do I see *all* devices?

L3 vs L1/2 devices



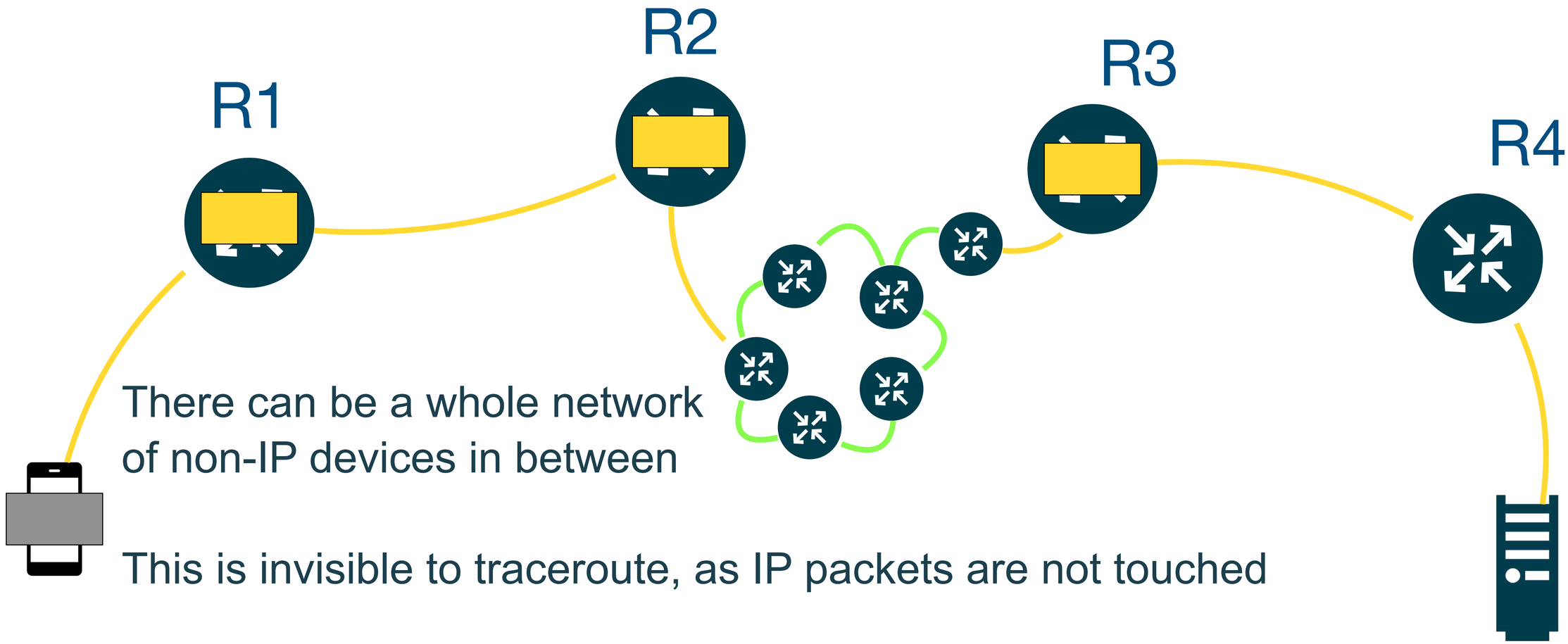
These are routers
They work on IP packets
And decrement the TTL counter

But is that *all* devices?

DE CIX

Do I see *all* devices?

L3 vs L1/2 devices



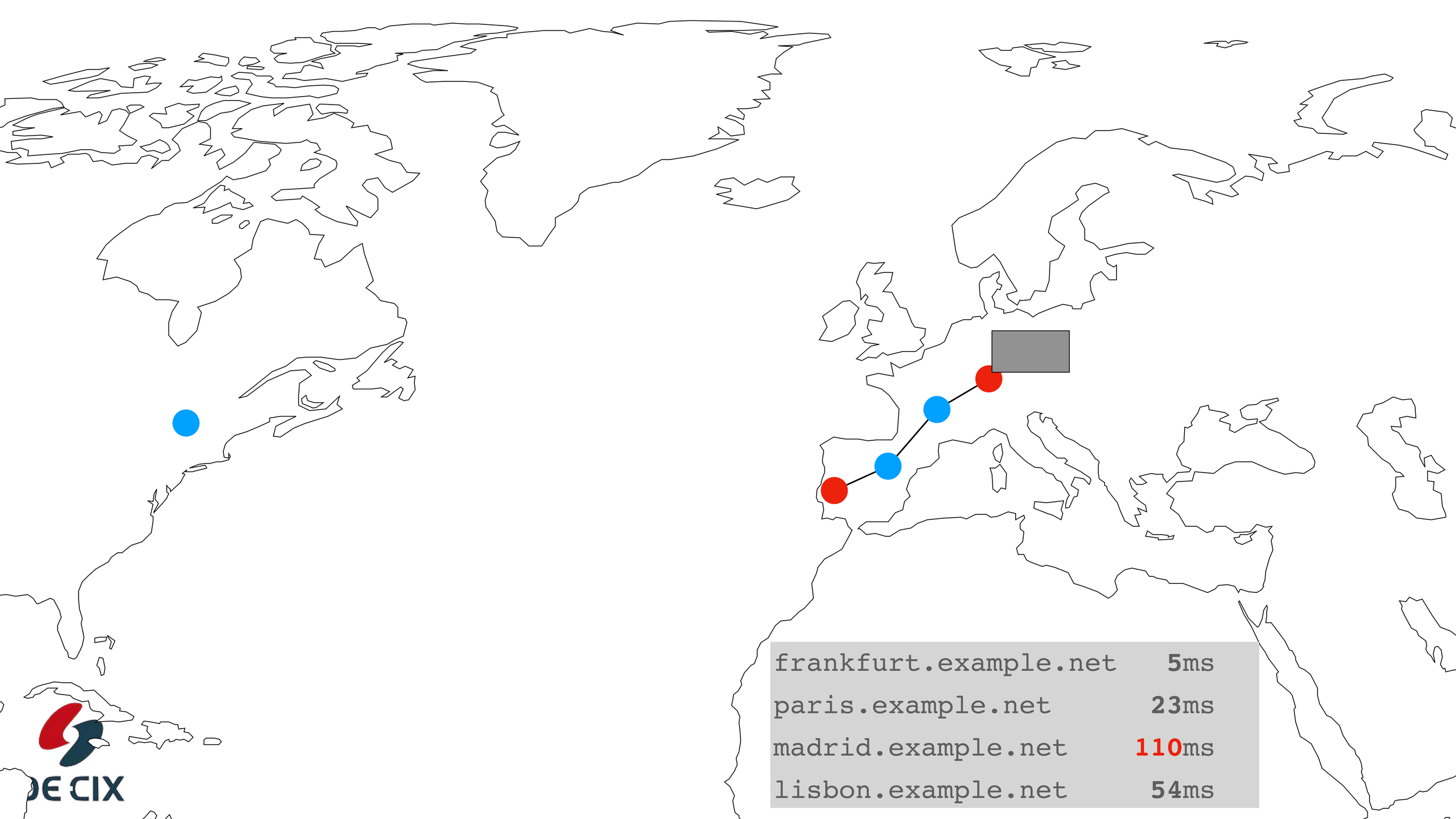
There can be a whole network of non-IP devices in between

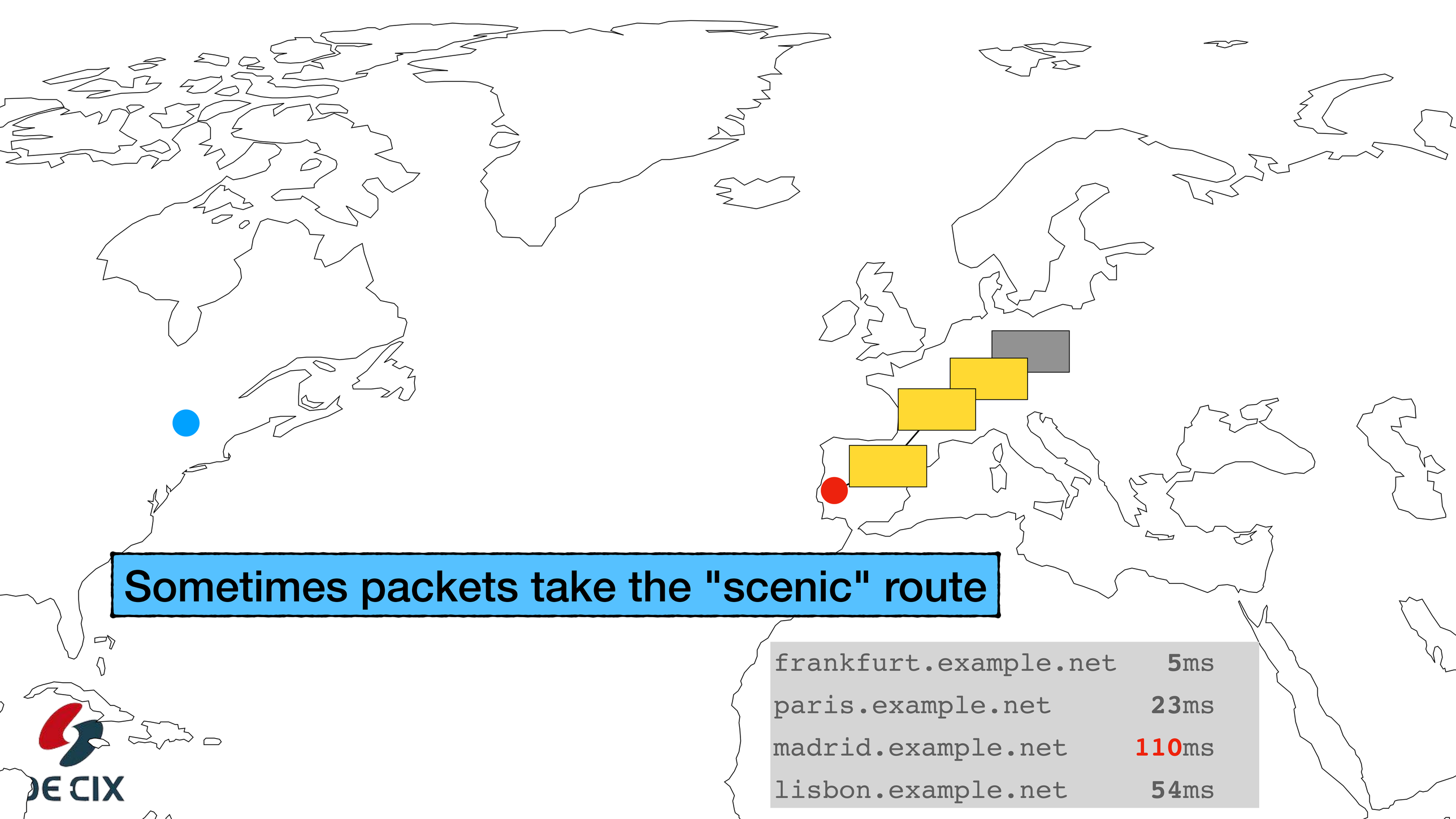
This is invisible to traceroute, as IP packets are not touched

Examples are: ATM Networks, MPLS Networks

DE CIX

About round-trip time

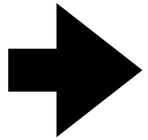

frankfurt.example.net 5ms
paris.example.net 23ms
madrid.example.net 110ms
lisbon.example.net 54ms
DE CIX


Sometimes packets take the "scenic" route
frankfurt.example.net 5ms
paris.example.net 23ms
madrid.example.net 110ms
lisbon.example.net 54ms
DE CIX

Conclusion

Conclusion

ICMP - Internet Control Message Protocol



Layer	Name
4	ICMP
3	Internet
2	Link
1	Physical

- ICMP packets are sent by network devices if an exception occurs
- Traceroute uses this to show a path of routers *towards* a destination
  - There may non-IP devices in the path which are not shown
  - The names of the devices can be misleading
  - The time value is a round-trip time, and the way back from a device may be longer
- Do not rely on traceroute as your *only* debugging tool

DE CIX

Thank you!

academy@de-cix.net

Interested in more webinars? Please subscribe to our mailing list at https://lists.de-cix.net/wws/subscribe/academy

DE-CIX Management GmbH | Lindleystr. 12 | 60314 Frankfurt | Germany
Phone + 49 69 1730 902 0 | sales@de-cix.net | www.de-cix.net

Links and further reading

Links and further reading

- Internet protocol - https://en.wikipedia.org/wiki/Internet_Protocol
- Protocol stack - https://en.wikipedia.org/wiki/Protocol_stack
  - Transport Layer: https://en.wikipedia.org/wiki/Transport_layer
  - Datagram: https://en.wikipedia.org/wiki/Datagram
- IP Network Model: https://en.wikipedia.org/wiki/Internet_protocol_suite
- IPv4
  - IPv4 - https://en.wikipedia.org/wiki/IPv4
- IPv6
  - IPv6 itself - https://en.wikipedia.org/wiki/IPv6
  - IPv6 header - https://en.wikipedia.org/wiki/IPv6_packet
- History of Internet and IP
  - Internet Hall of Fame - https://internethalloffame.org
  - Defense Advanced Research Projects Agency (DARPA) - https://www.darpa.mil
  - ARPANET - https://www.darpa.mil/about-us/timeline/arpanet
  - The "Protocol Wars" - https://en.wikipedia.org/wiki/Protocol_Wars

Links and further reading

- ICMPv4:
  - Wikipedia: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol
  - Definition in RFC792
  - Depreciation of some ICMP types: RFC6918
  - IANA list of ICMP types and codes: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml
- ICMPv6:
  - Wikipedia: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol_for_IPv6
  - Definition in RFC4443 (first definition, now obsolete, was in RFC1885)
  - IANA list of ICMPv6 types and codes: https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml

Some notable traceroute clients

- Paris traceroute
  - tries to be more accurate by controlling package header contents
  - https://paris-traceroute.net
- Layer Four Traceroute
  - Implements additional features like AS number display
  - Uses TCP, UDP and ICMP
  - https://pwhois.org/lft/index.who
- Matts Traceroute
  - Nice graphical interface
  - https://www.bitwizard.nl/mtr/
- tralXroute
  - tries to detect Internet Exchanges
  - https://github.com/gnomikos/tralXroute
- RIPE Atlas
  - measurement network of probes which can traceroute back to you
  - https://atlas.ripe.net

Internet RFCs (Standards)

- There are too many RFCs dealing with IPv4 and IPv6 to be listed here
- Just go to https://tools.ietf.org/html/ and use the search field
- How does something become RFC? https://www.rfc-editor.org/pubprocess/
- The IETF - Internet Engineering Task Force