Networking Basics

04c - Internet Control Message Protocol (ICMP)

Wolfgang Tremmel
academy@de-cix.net

DE-CIX

Where networks meet

Networking Basics

DE-CIX Academy

01 - Networks, Packets, and Protocols

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

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

04a - User Datagram Protocol (UDP)

04b - Transmission Control Protocol (TCP)

04c - Internet Control Message Protocol (ICMP)

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

06a - Domain Name System (DNS)

DE-CIX

Internet Model

IP / Internet Layer

- Data units are called "Packets"
- Provides source to destination transport
  - For this we need addresses
- Examples:
  - IPv4
  - IPv6

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

Internet Model

Transport Layer

- *May* provide flow control, reliability, congestion avoidance
- Also may contain information about the next layer up
- Examples:
  - TCP (flow control, reliability, congestion avoidance)
  - UDP (none of the above)
  - **ICMP**

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

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
5	Application
4	Transport
3	Internet
2	Link
1	Physical

ICMP

Internet Model

ICMP - Internet Control Message Protocol

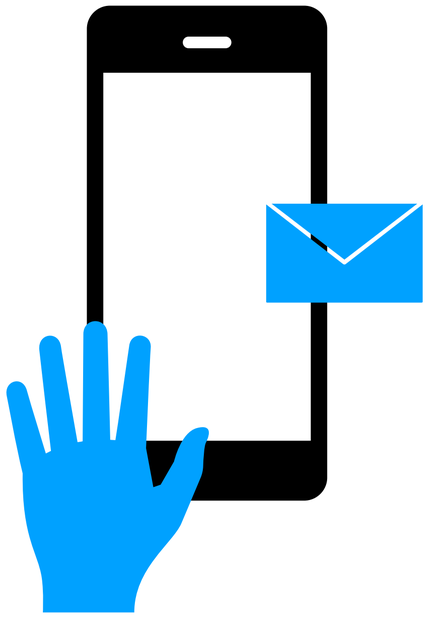
- The IP stack is not as strict with layers as the OSI stack
- ICMP uses IP for transport
- But it does not have anything "above" it
- So what it is needed for anyway?
  - To understand that, lets take a step back and ask about what "Reasons for Packets " are there?

Layer	Name
4	ICMP
3	Internet
2	Link
1	Physical

Reasons for Packets

TCP and UDP

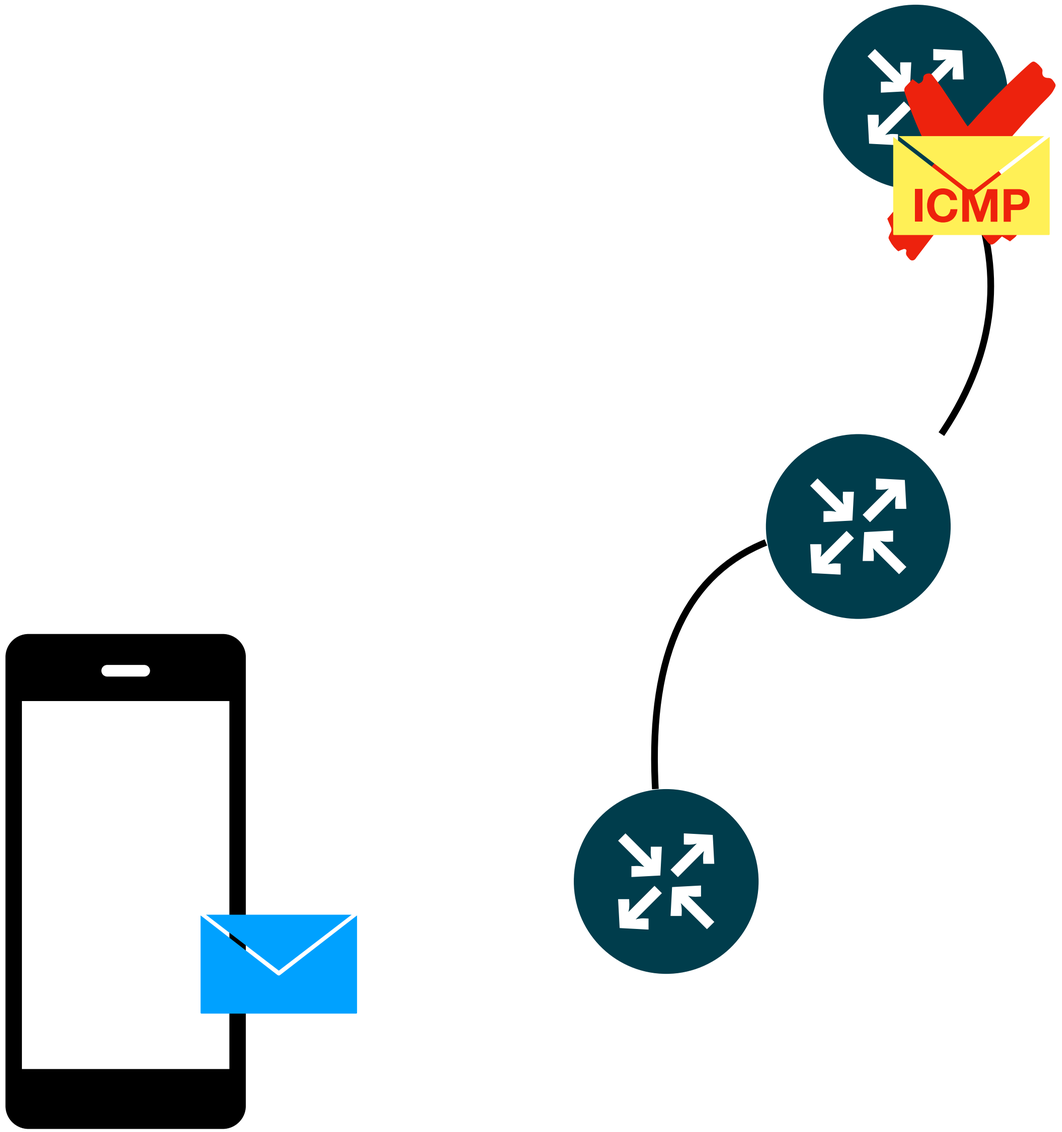
- Why are packets being sent?
  - Because a user clicks on something
  - Or a machine reacts to an event
- Some program on the application layer needs to send data



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

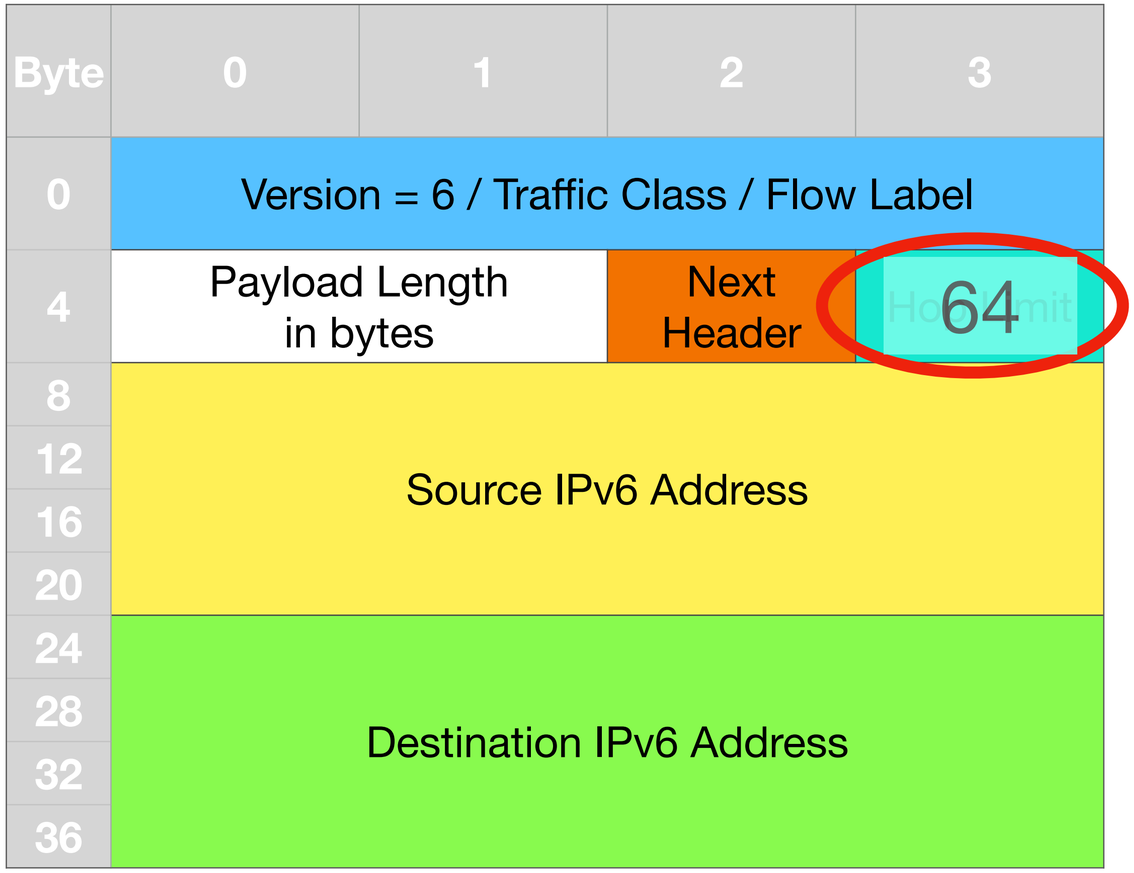


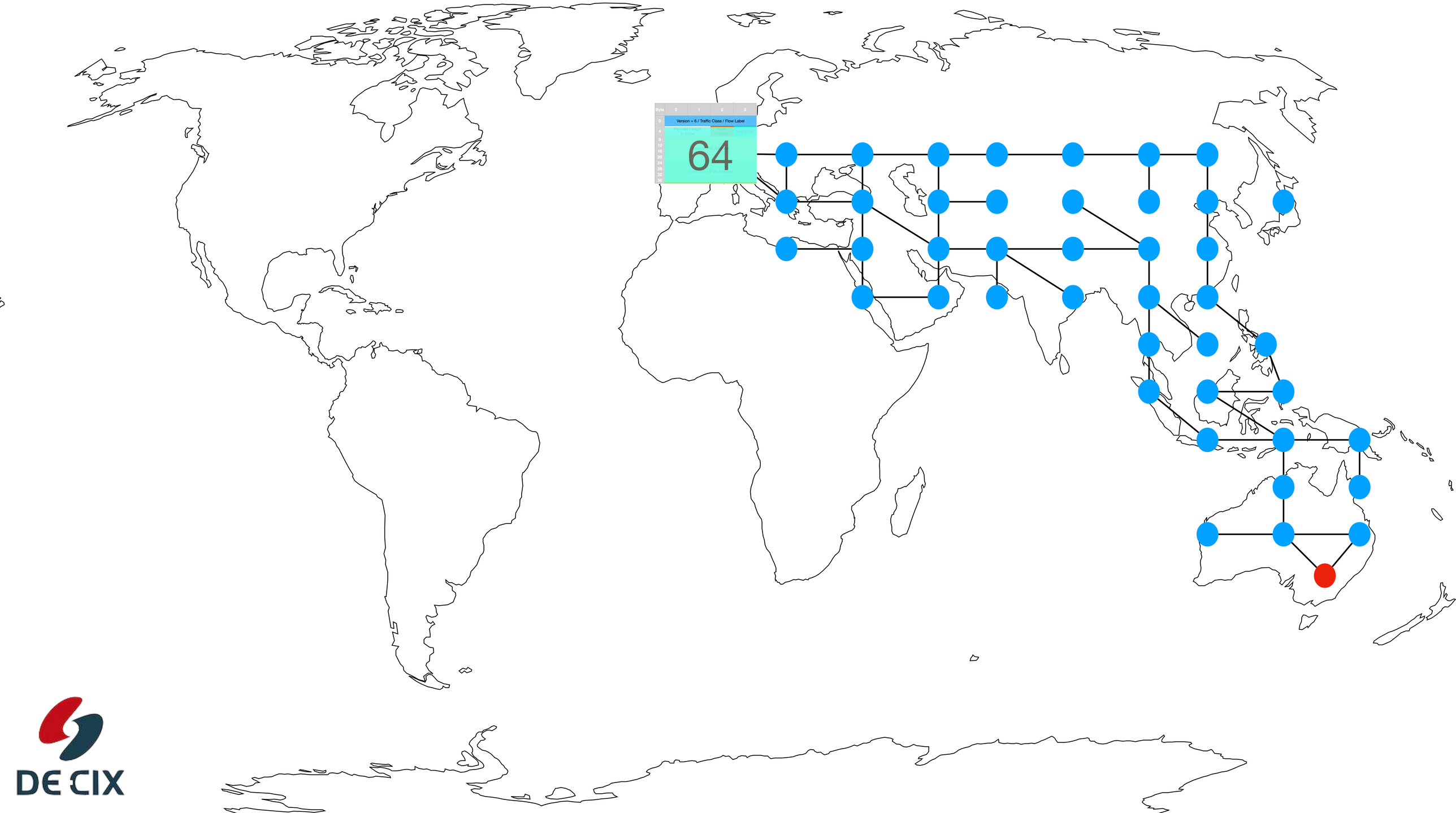
ICMP Example

ICMP Example

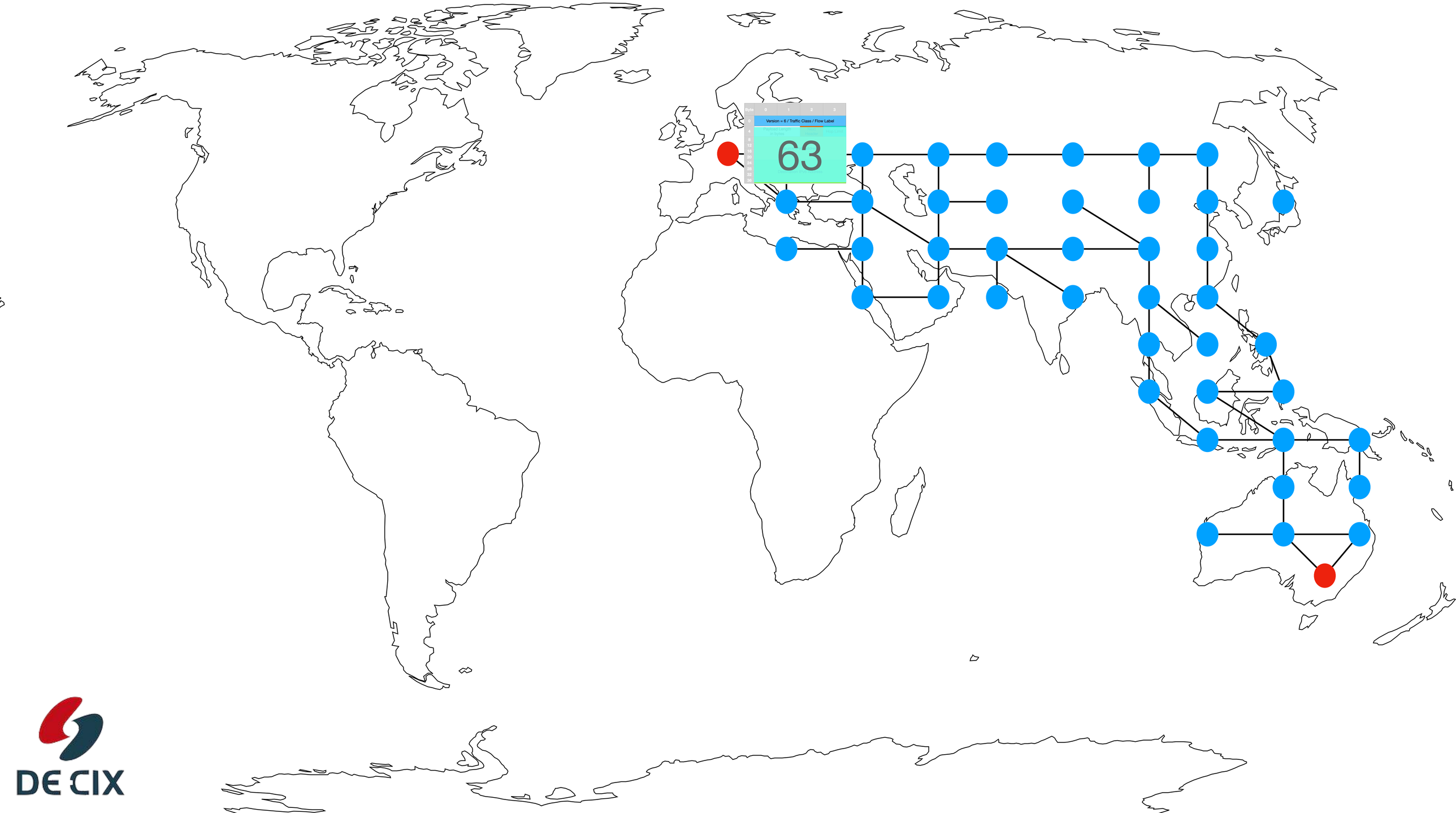
Time Exceeded

- 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

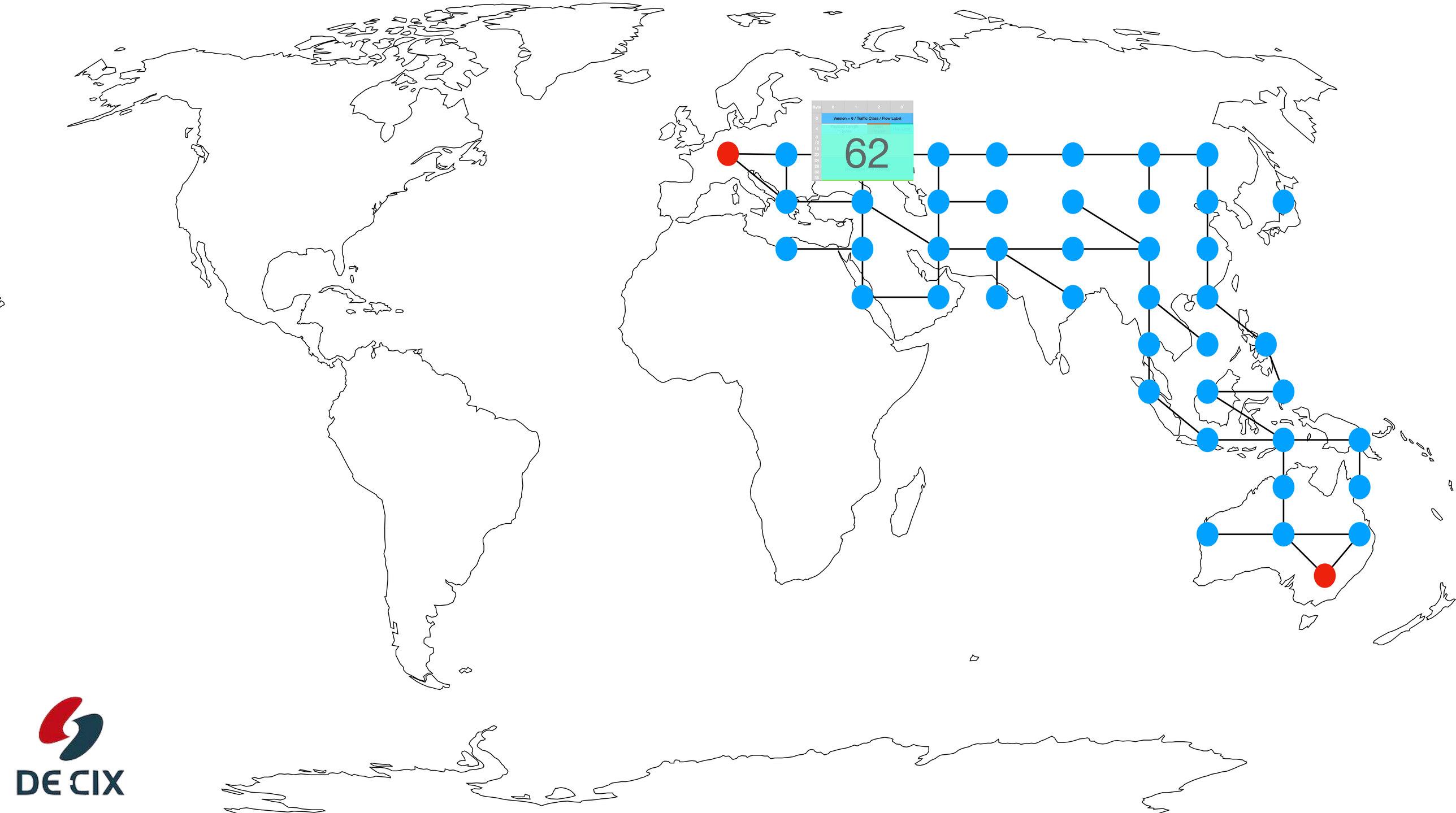



Byte
0
1
2
3
Version = 6 / Traffic Class / Flow Label
Payload Length = 0 bytes
Next Header
Hop Limit
Source Address
Destination Address
64

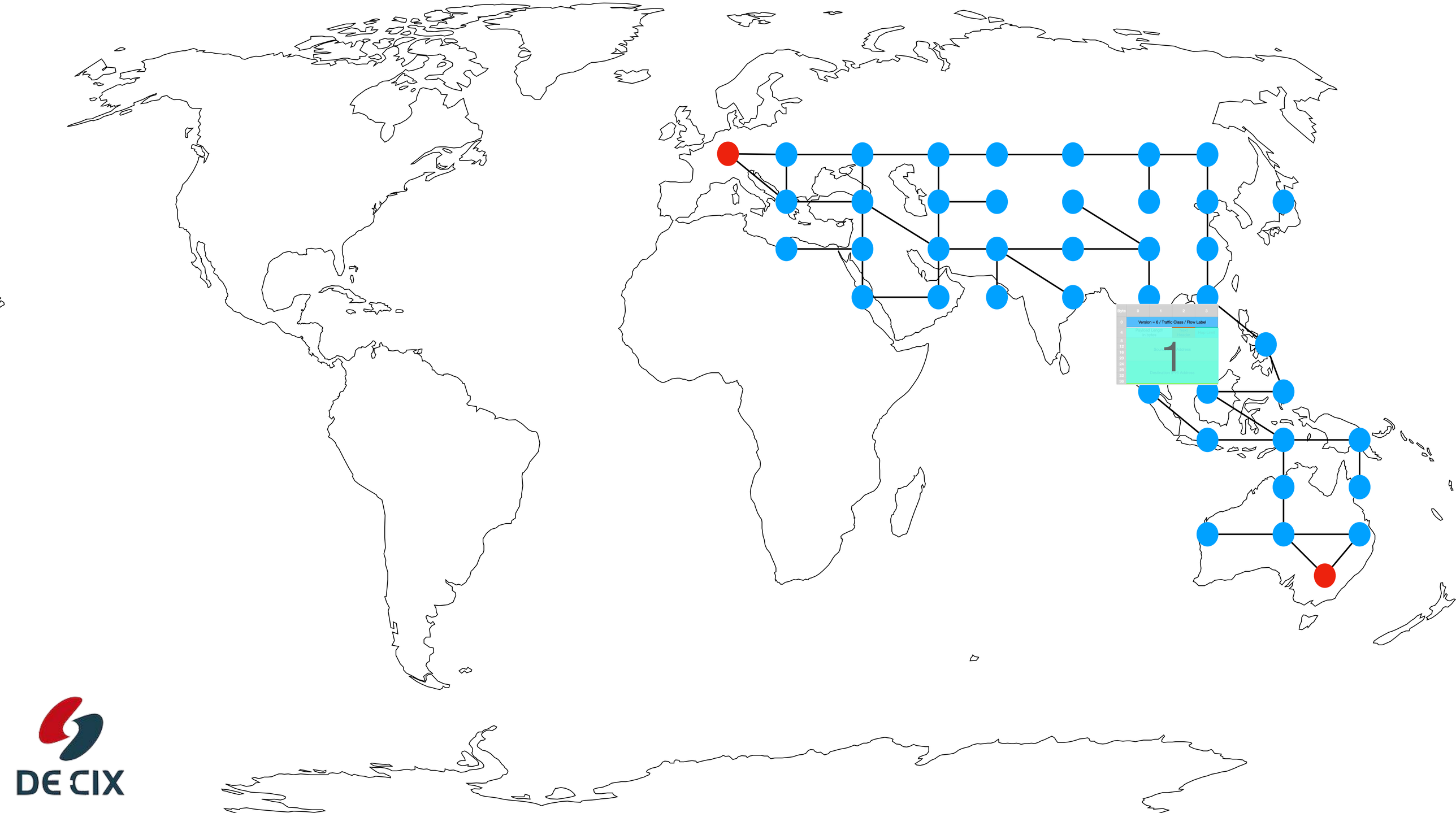
DE CIX


Byte
0
1
2
3
0
Version = 6 / Traffic Class / Flow Label
4
Payload Length
in bytes
Header
Next Hdr
8
12
16
20
24
28
32
36
Hop Limit
63

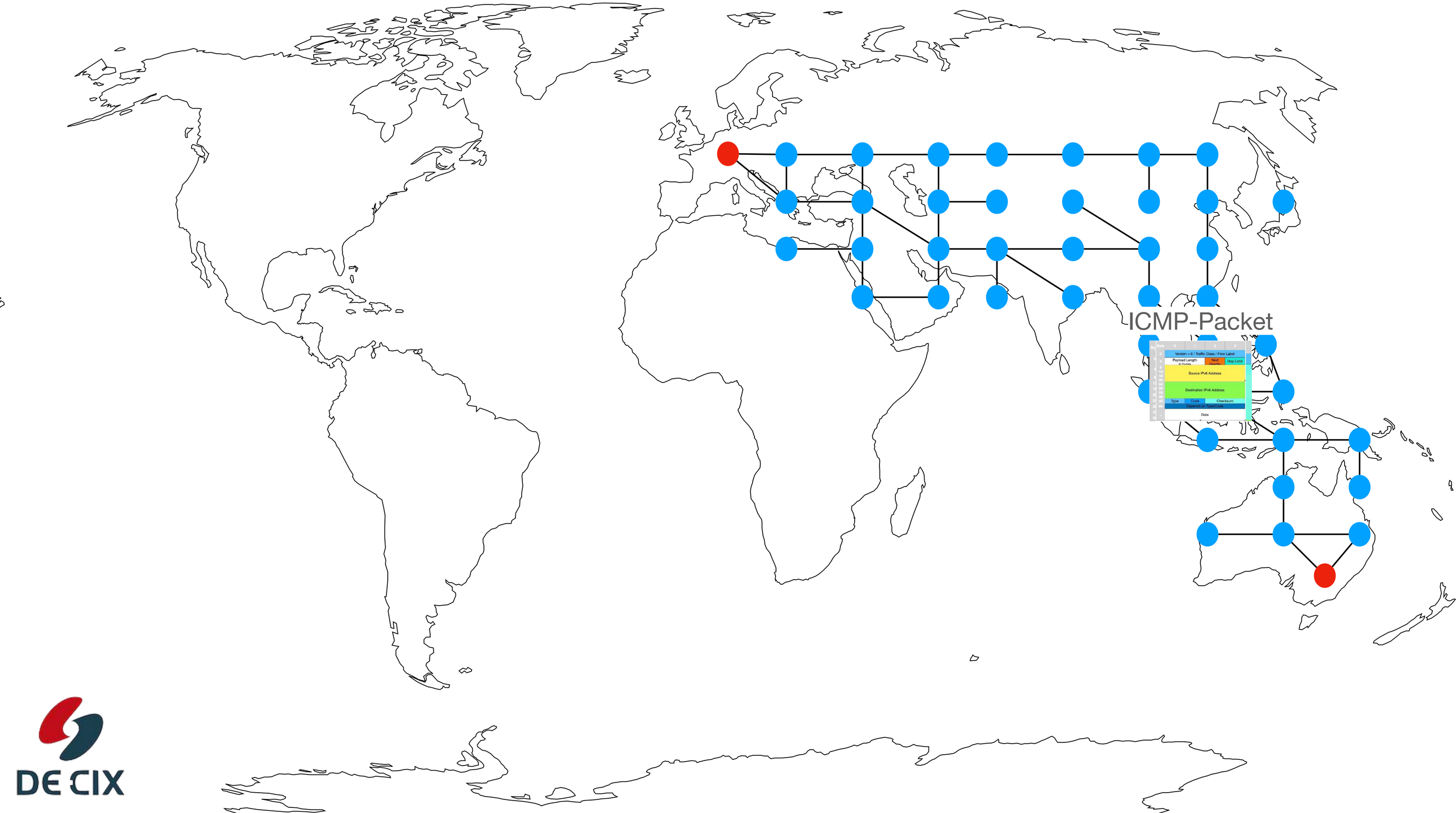
DE CIX



DE CIX



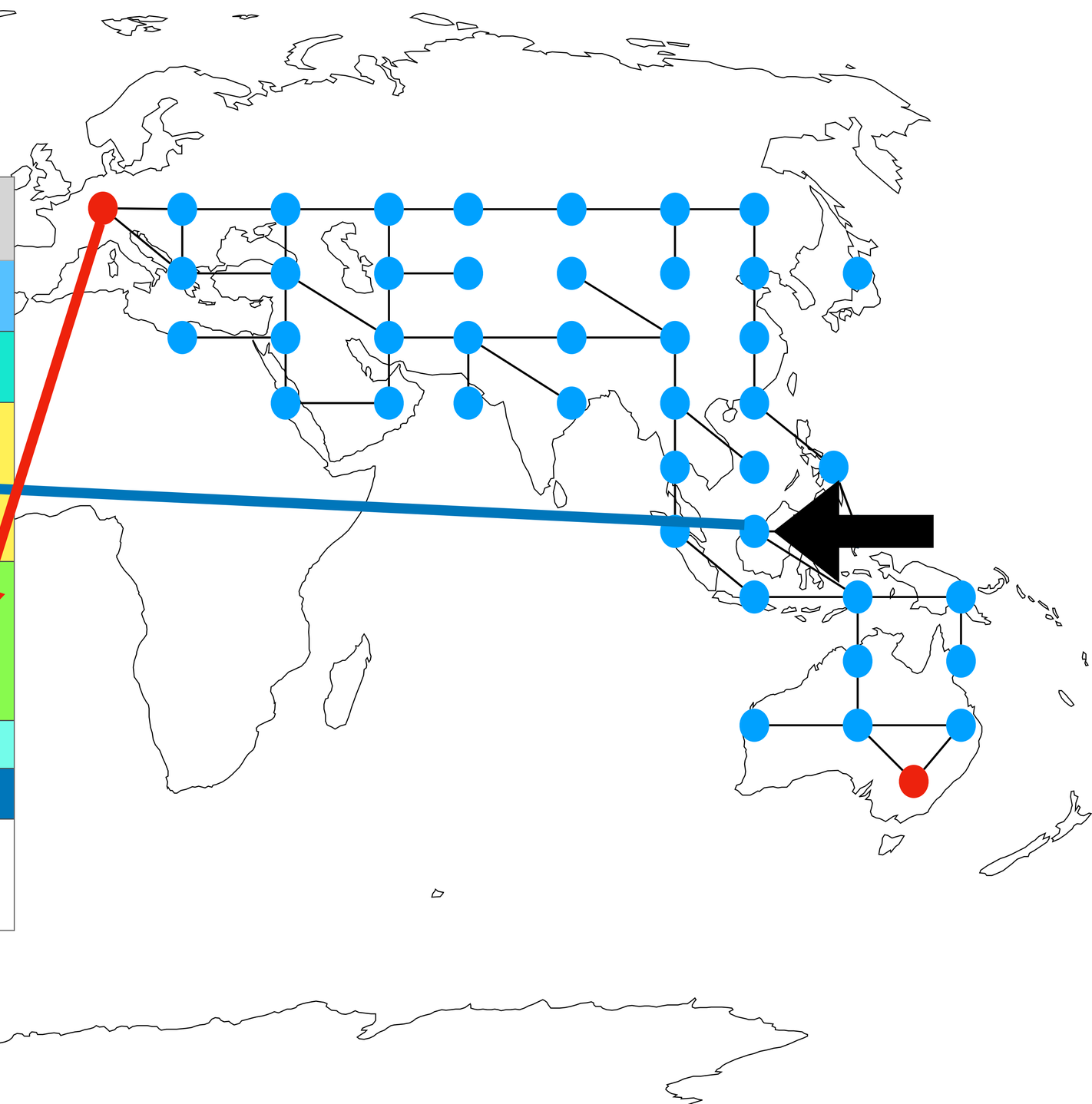
DE CIX


ICMP-Packet
Byte
0
1
2
3
Version = 6 / Traffic Class / Flow Label
Payload Length in Bytes
Next Header
Hop Limit
Source IPv6 Address
Destination IPv6 Address
Type
Code
Checksum
Depends on Type/Code
Data

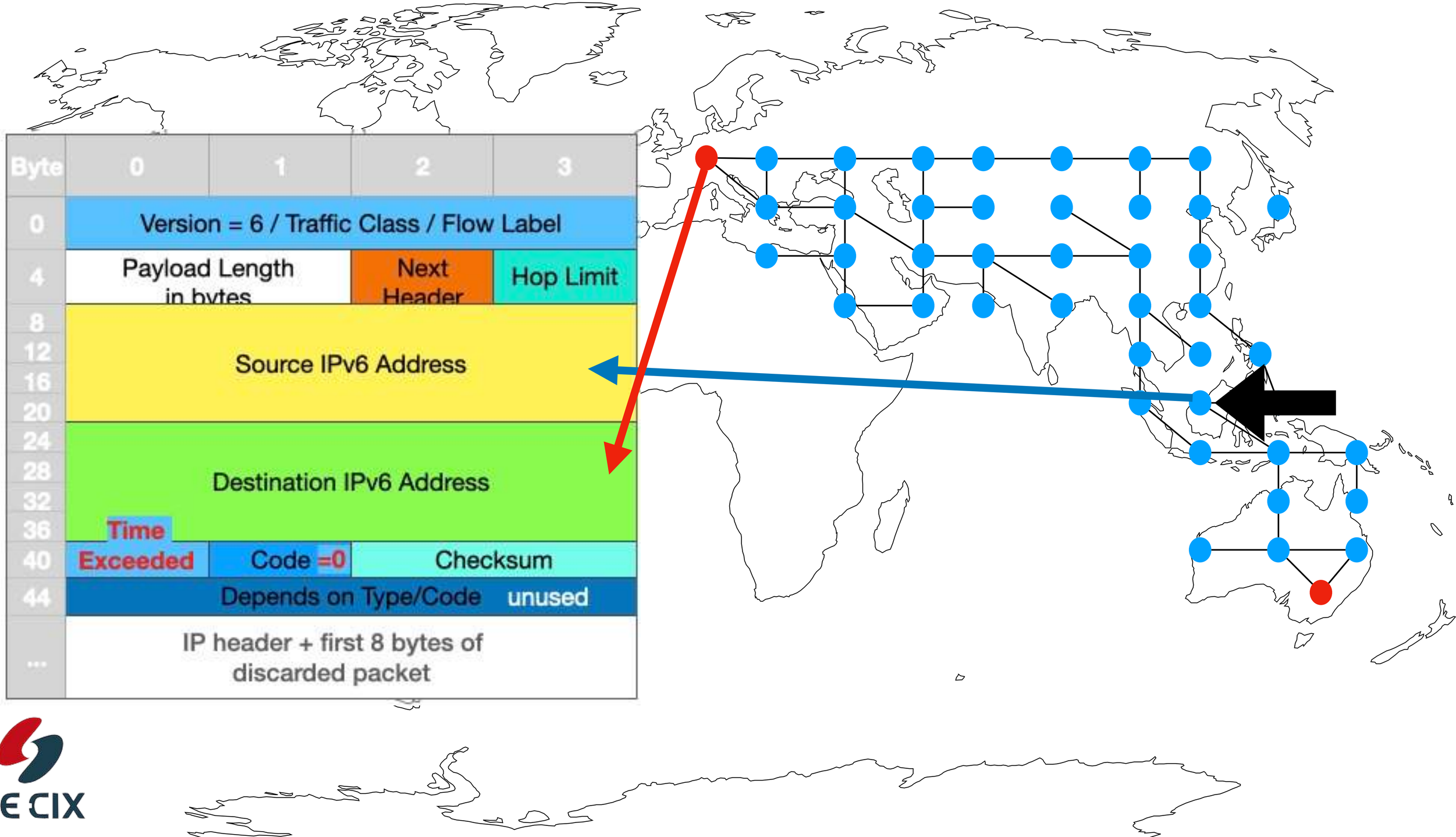
DE CIX

ICMP-Packet

Byte	0	1	2	3
0	Version = 6 / Traffic Class / Flow Label			
4	Payload Length in bytes		Next Header	Hop Limit
8	Source IPv6 Address			
12				
16				
20				
24	Destination IPv6 Address			
28				
32				
36				
40	Time Exceeded	Code =0	Checksum	
44	Depends on Type/Code		unused	
...	IP header + first 8 bytes of discarded packet			



DE CIX

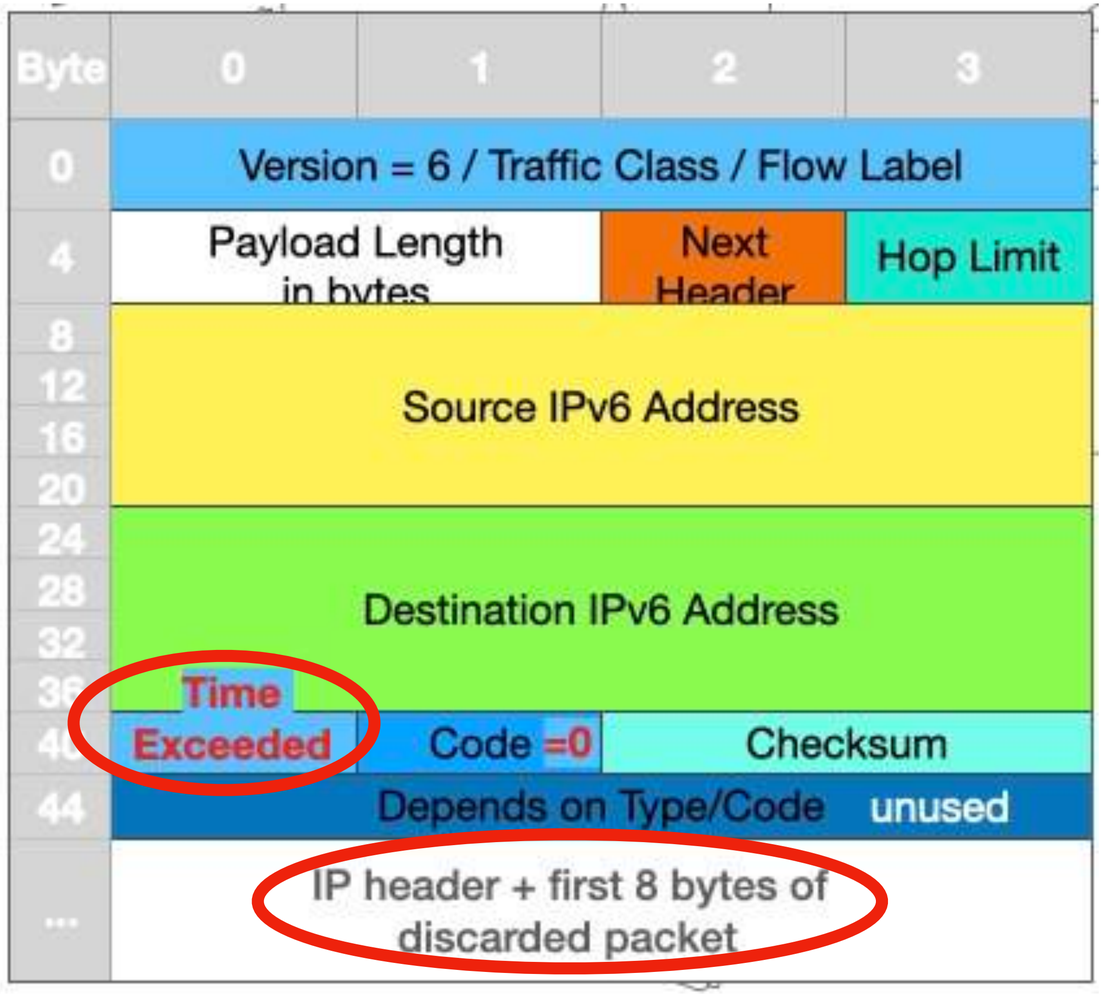

Byte
0
1
2
3
0
Version = 6 / Traffic Class / Flow Label
4
Payload Length in bytes
Next Header
Hop Limit
8
12
16
20
Source IPv6 Address
24
28
32
36
Destination IPv6 Address
40
Time Exceeded
Code =0
Checksum
44
Depends on Type/Code
unused
...
IP header + first 8 bytes of discarded packet

DE CIX

ICMP Time Exceeded

Sent by router discarding packet

- When the TTL / HopCount hits zero
  - The router discards the packet
  - The router sends an ICMP packet of type *Time Exceeded* back to the originator of the discarded packet
  - This ICMP *Time Exceeded* contains enough information for the originator to determine which packet was discarded

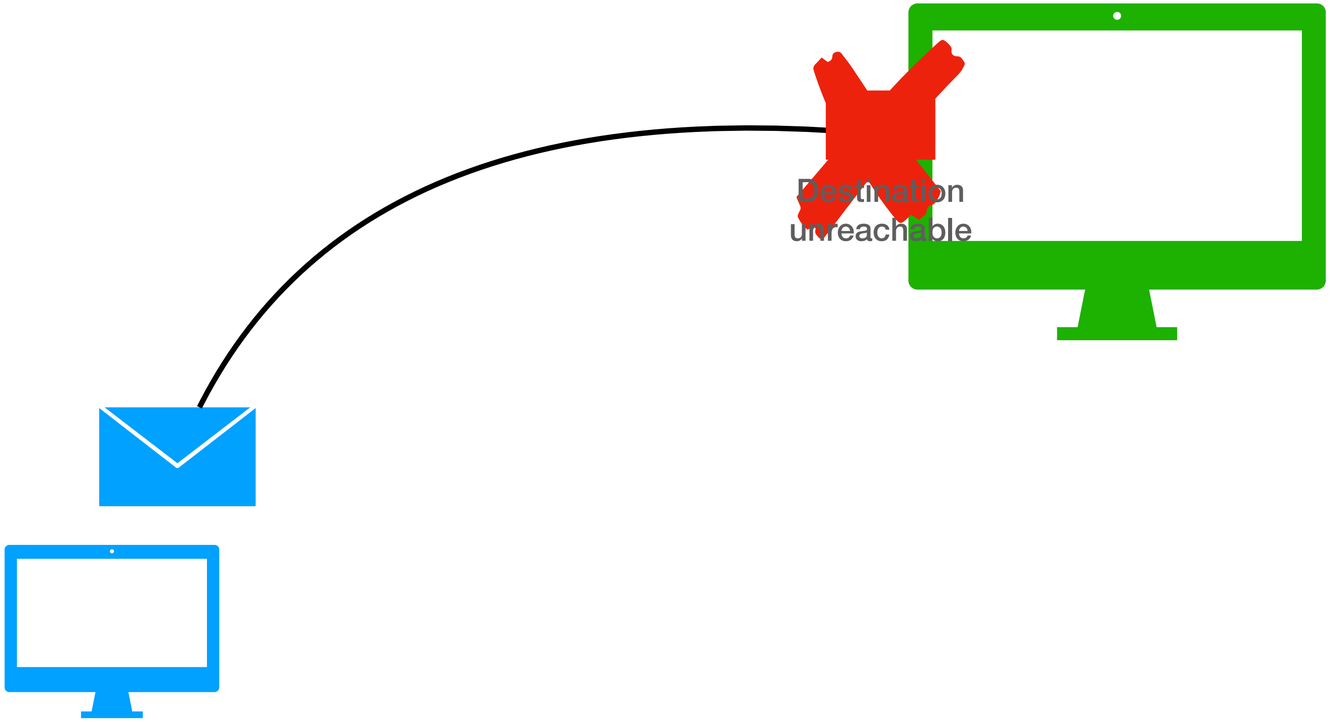


ICMP Types

ICMP Types

Destination unreachable

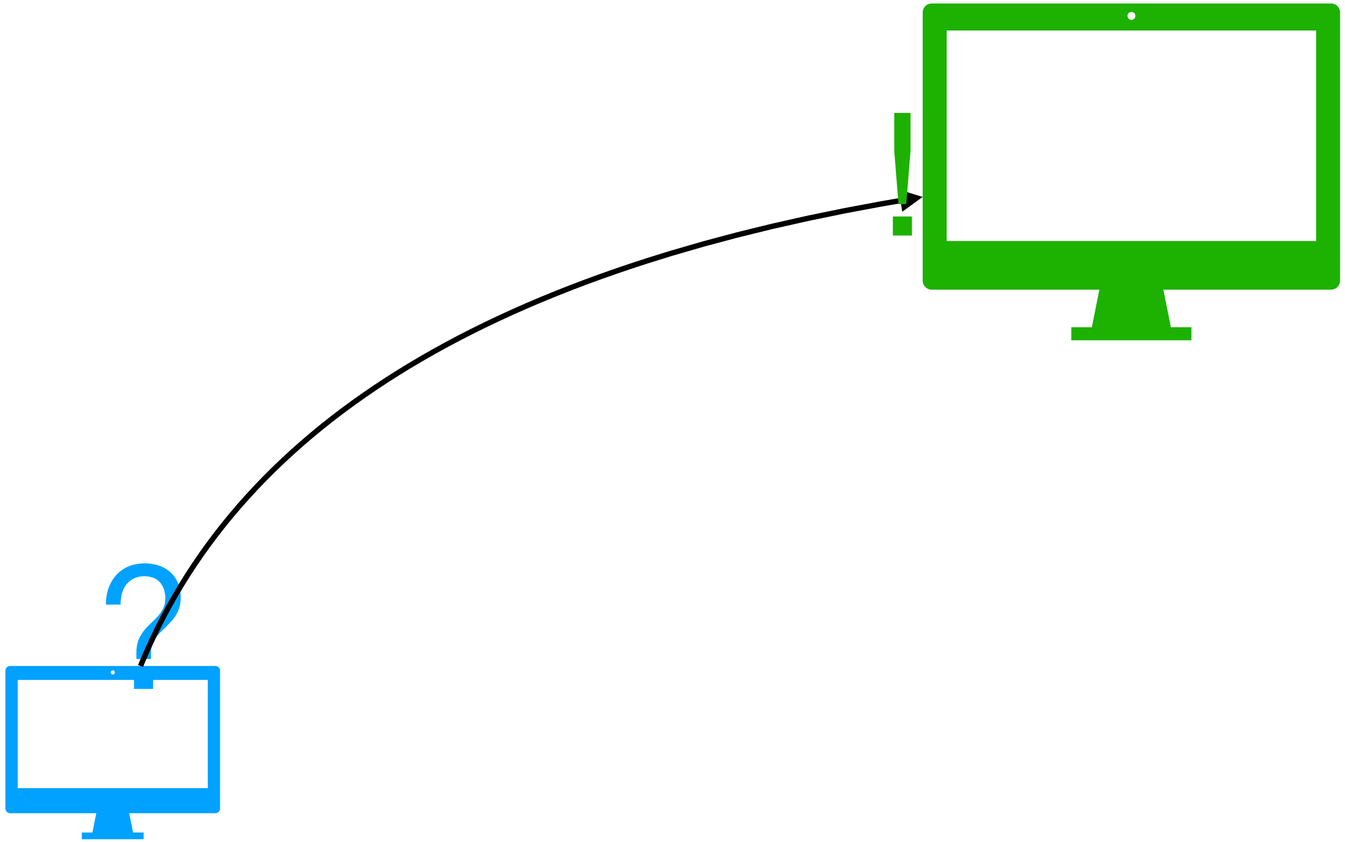
- Ever got a "destination unreachable" error?
- This is also an ICMP message
- ICMP Type = 1
- Code gives reason
  - no route
  - administratively prohibited
  - address unreachable
  - port unreachable
  - ... more



ICMP Types

Echo request / echo reply

- Do you know "ping"?
- This is one of the few user-originated ICMPs
- Ping sends an "echo request" ICMP packet
- And expects an "echo reply" packet back
- Here we have some difference in IPv4 and IPv6



ICMP Types

Differences in IPv4 and IPv6

- In IPv4, "type" values were assigned as they were defined
  - with some of them kept unassigned for future use
  - starting with "0" for echo reply, ending with "43" for extended echo reply
- In IPv6, there is some structure to "type" numbers
  - error messages are 0-127
  - informational messages are 128-255

ICMP Type	IPv4	IPv6
Echo Request	8	128
Echo Reply	0	129
Destination unreachable	3	1
Time exceeded	11	3

DE CIX

Conclusion

DE CIX

Conclusion

ICMP - Internet Control Message Protocol

Layer	Name
4	ICMP
3	Internet
2	Link
1	Physical

- ICMP plays an important role for signalling in the Internet
- Devices send ICMP messages to indicate error states or for informational purposes
- ICMP messages are often not user-initiated but triggered by packet forwarding or delivery events
- ICMP exists both in IPv4 and IPv6, but the values for its fields differ.

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

DE-CIX

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

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