Networking Basics

04a - User Datagram Protocol (UDP)

Wolfgang Tremmel
academy@de-cix.net

DE-CIX

Where networks meet

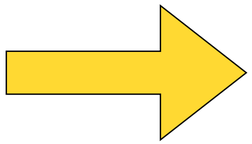
Networking Basics

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 - TCP

04c - ICMP + 04d - Traceroute

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

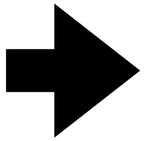
06a - Domain Name System (DNS)

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



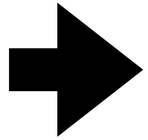
Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

DE CIX

Internet Model

Transport Layer

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



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

DE CIX

Encapsulation

Packets inside packets

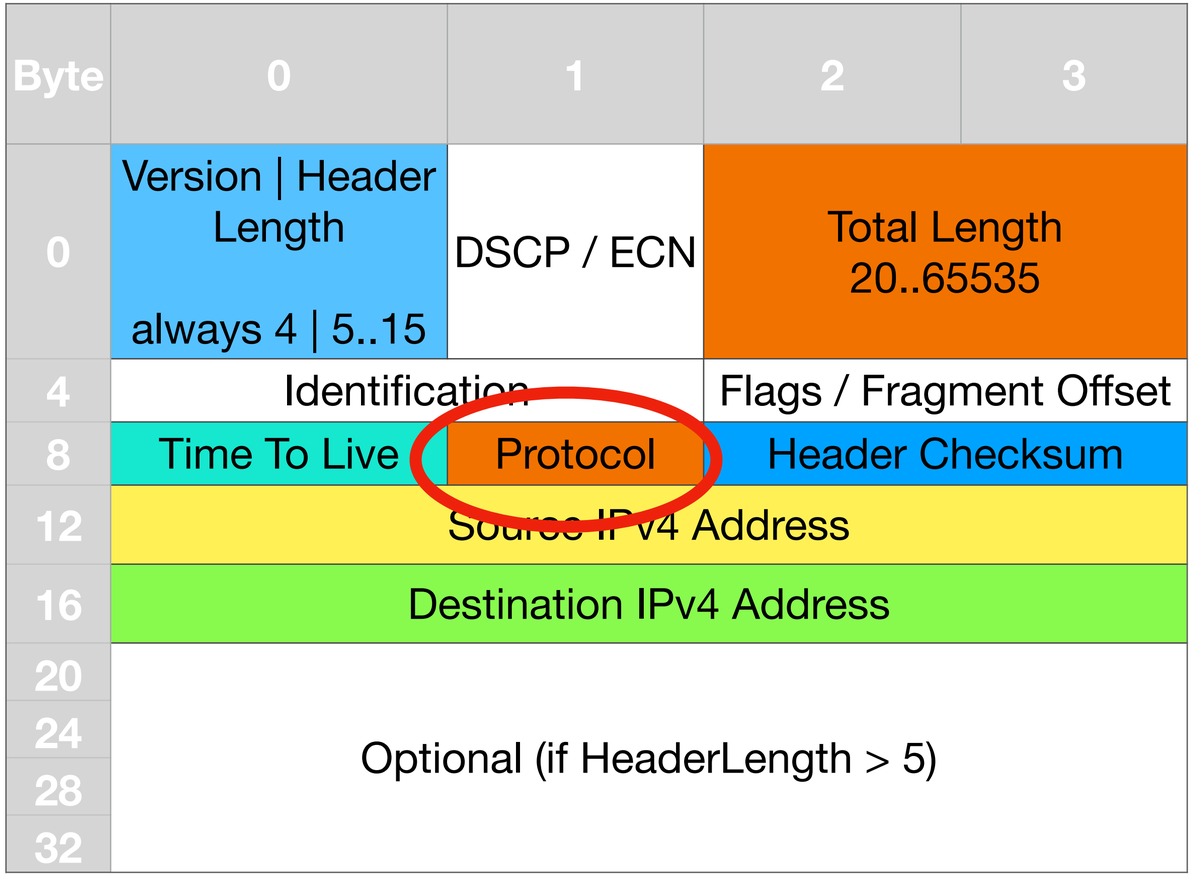
- Encapsulation is like Russian dolls
- IP Packets have a payload
- This payload is usually UDP or TCP (there are others as well)
- So we have an UDP packet inside an IP packet

Attribution: Fanghong. derivative work: Greyhood
https://commons.wikimedia.org/wiki/File:Matryoshka_transparent.png

IPv4 Header

"Legacy" IP

- Starts with version and length
- Total length of packet
- Important: Time to live (TTL)
- **Protocol: Type of payload**
  - TCP = 6, UDP = 17
- Source / Destination address 32 bits
- Options (optional)

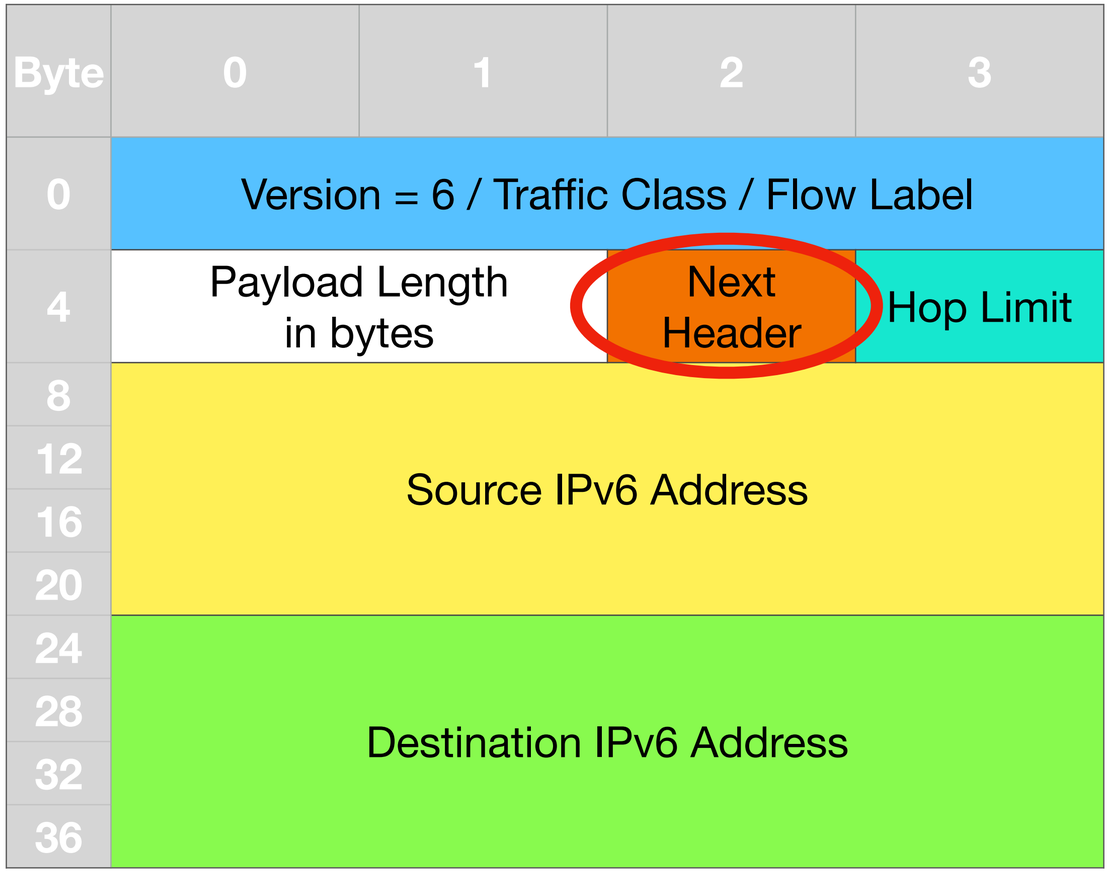


DE CIX

IPv6 Header

Looks simpler, yes?

- Starts with version and some labels
- Payload length in bytes (0-65535)
- **Next Header** - you can chain more headers
  - replaces protocol field, same values
- Hop Limit replaces TTL
- Addresses are now 128bits

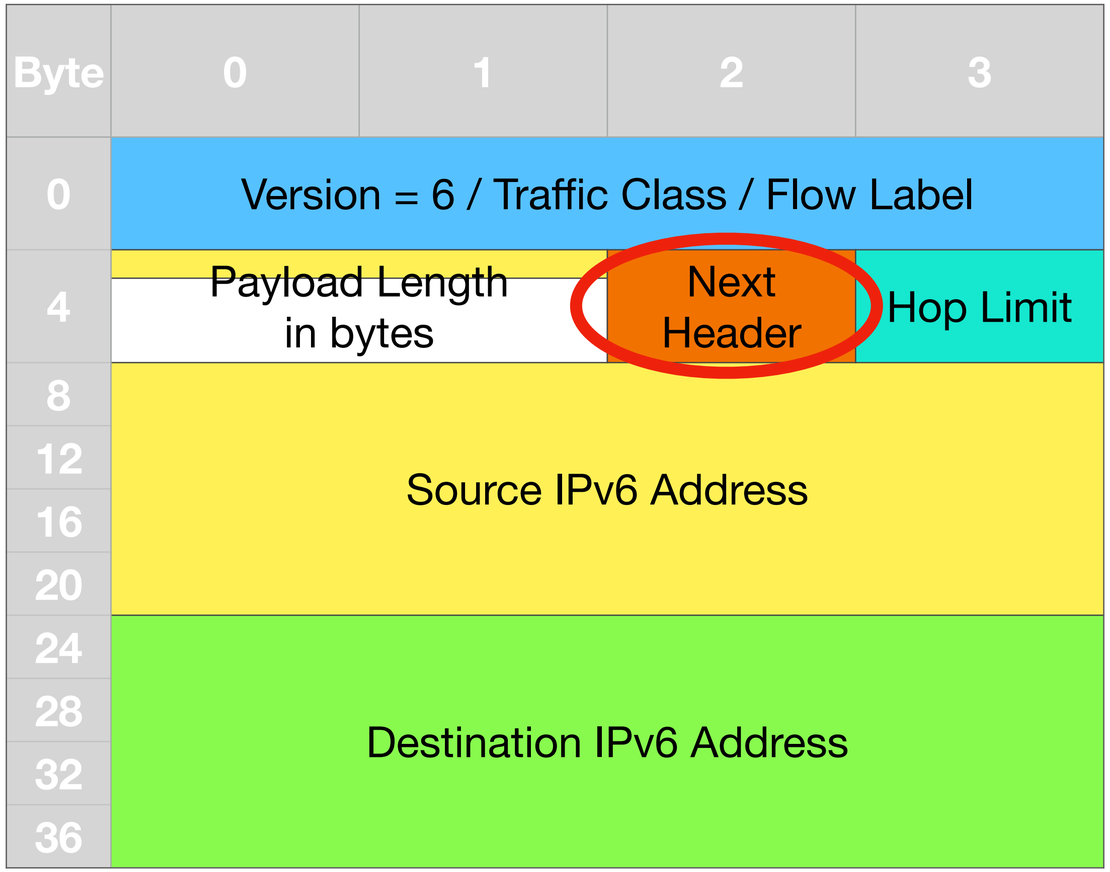


DE CIX

Next header: Transport layer header

TCP, UDP, and more

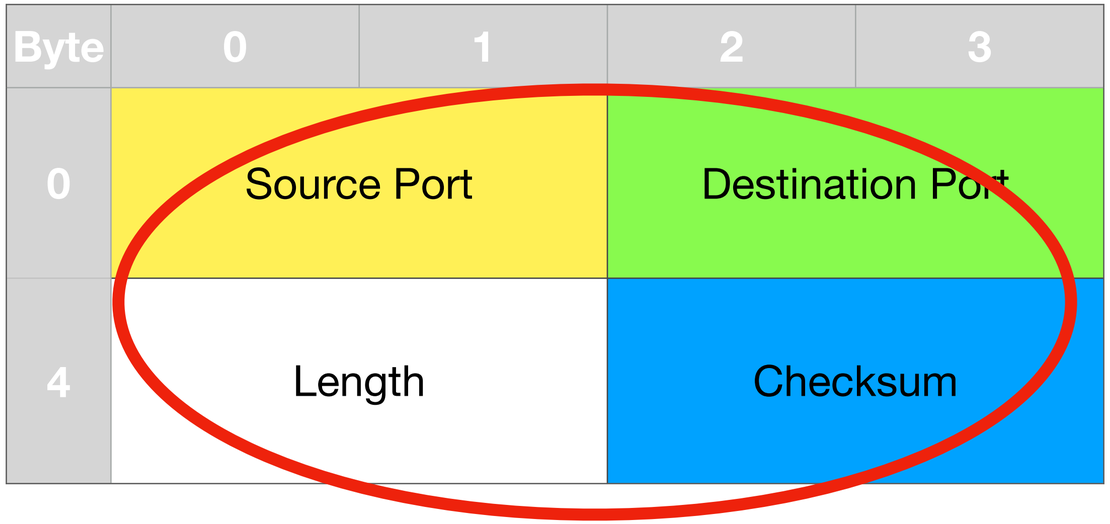
- We start with the "easiest" protocol
- UDP
  - User Datagram Protocol
  - Protocol ID is **17**
  - Introduced in 1980
- Lets have a look at the header



DE CIX

UDP Header

- 4 fields, each of them 16 bits
- Length: UDP header + UDP payload
- Checksum
  - Optional for IPv4, required for IPv6
  - IP header + UDP header are covered
- Source Port
  - Optional, zero if not used
- Destination Port number
  - required

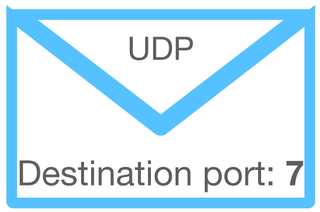


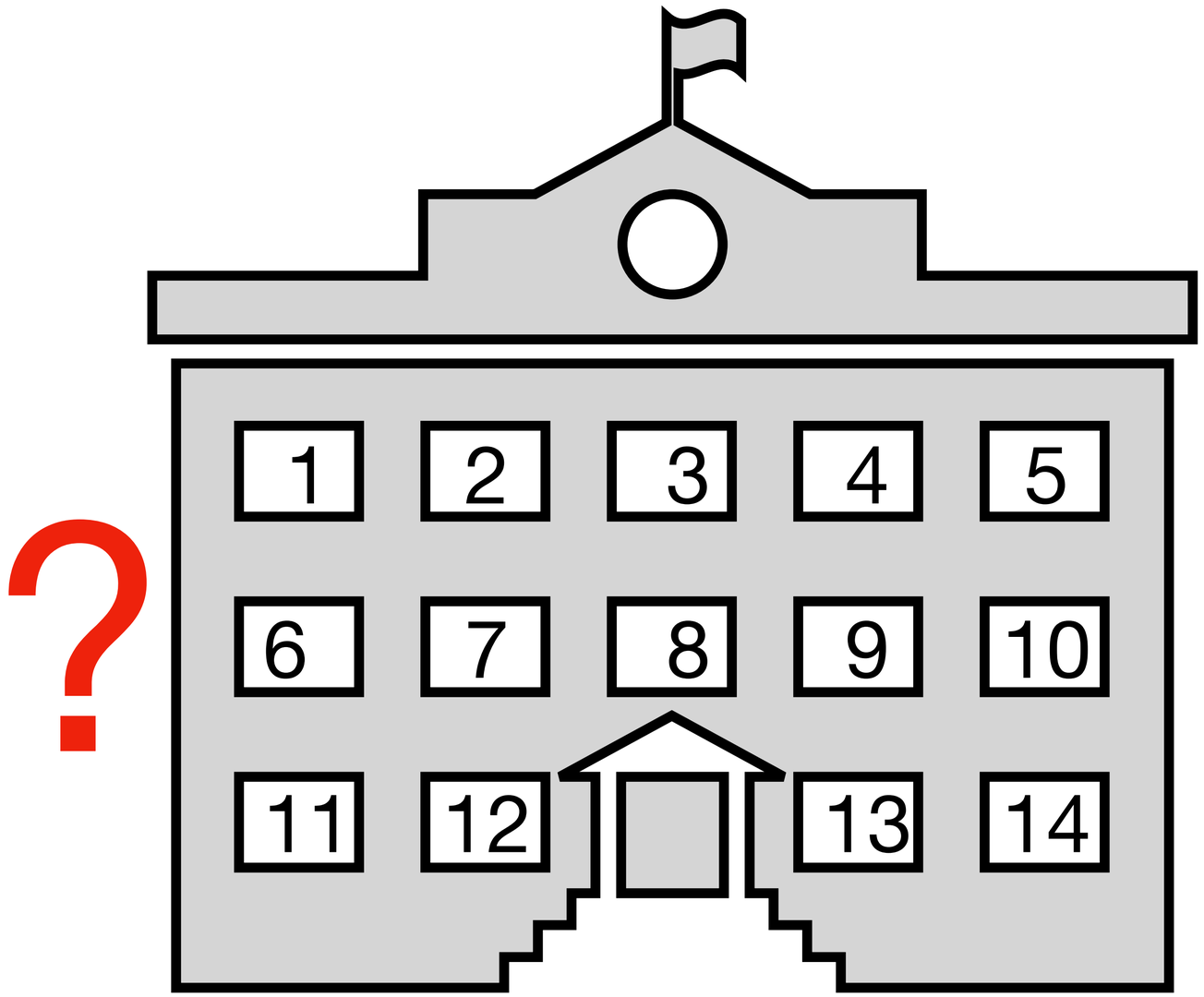
DE CIX

Port number

DE CIX

Port number



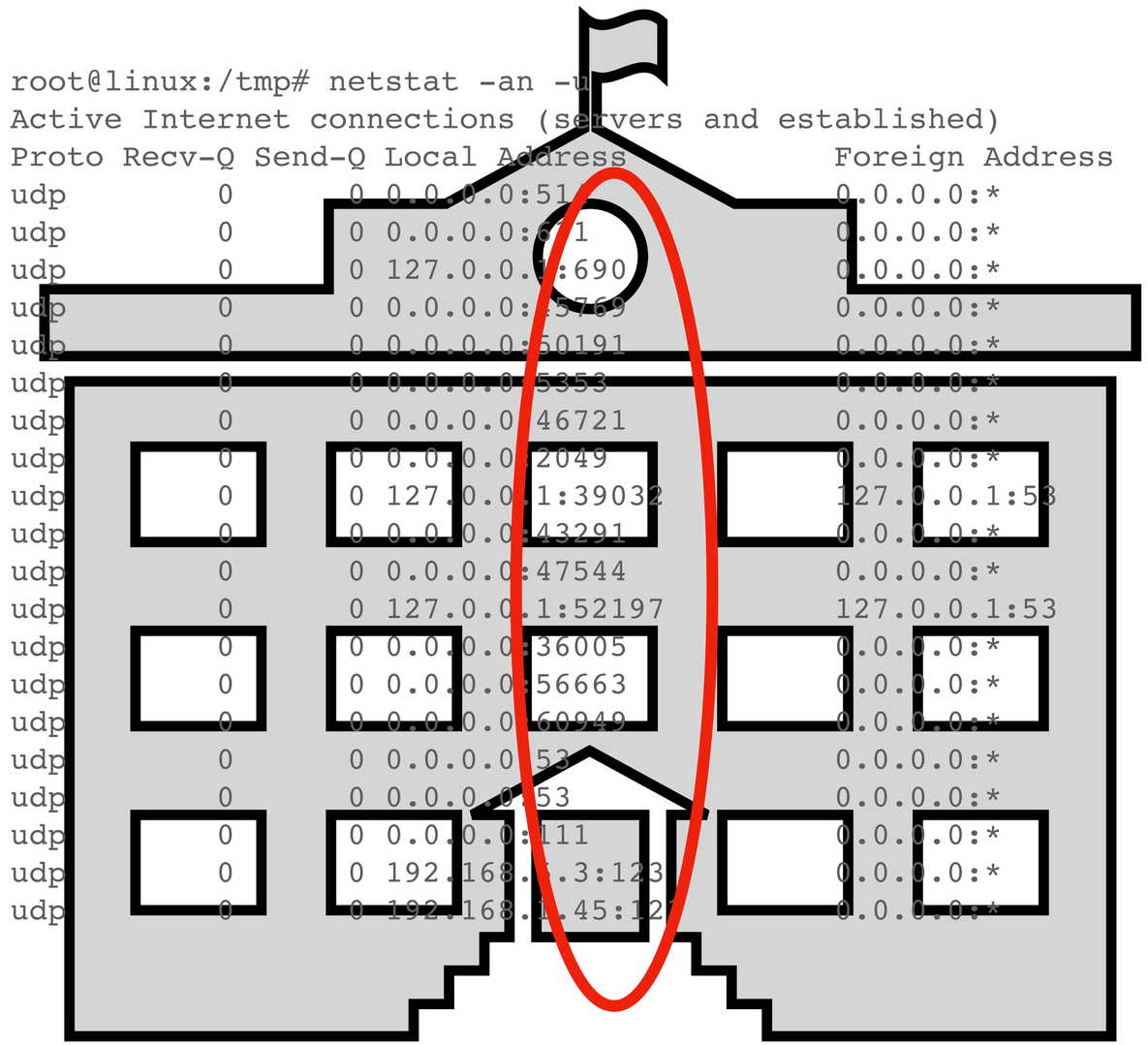


DE CIX

Port numbers

In reality...

- Of course we have not a building
- We have a computer system
- But we have port numbers
- Behind each port sits a piece of software
  - On some systems this software is called a "daemon"



UDP - Connectionless communication

Why is it called connectionless?

- The sender does not know if and when the packet has been received
- There may be an answer, but there also may be not
- If there is an answer, the sender knows the packet got through
- If there is no answer
  - Either the packet did not get through
  - Or the answer did not get through

DE CIX

UDP packet processing

Security issues ahead!

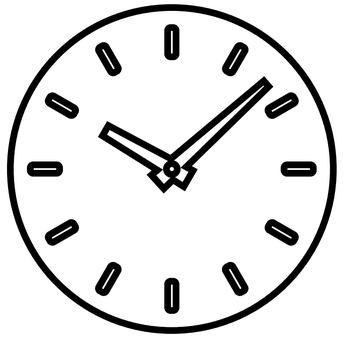
- A UDP packet is received by a system
- It is delivered to the software matching the destination port number
- If a response has to be sent, it is sent to back to sender
  - Using the source IP as destination of the response
  - The source-port becomes the destination port of the response
- Can you see a security problem in that?

DE CIX

UDP - what it is used for

NTP - Network Time Protocol

Synchronizing clocks over the Internet



- NTP is a protocol to synchronize computer clocks using the Internet
- Systems send and receive UDP packets on port 123
  - Packets contain a 32-Bit number for seconds and a 32-bit number for fractional seconds
  - Epoch (start) is 1st of January, 1900
  - Rollover will be on 7th of February, 2036
- Newest version of NTP now uses 64 bits for seconds

DE CIX

DNS - Domain Name Service

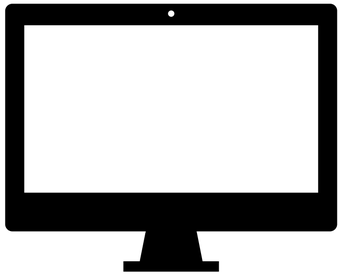
The phonebook of the Internet

- DNS translates names (like "www.de-cix.net") to IP addresses
- DNS is so complex and widely used, it deserves a webinar on its own
- Roughly explained
  - A system sends a name to a name server via UDP
  - The name server sends an UDP packet back containing the IP address where the name is hosted

DE CIX

DHCP - Dynamic Host Configuration Protocol

This is how your PC gets an IP address at home



- If you connect a computer to a network it needs an IP address
- DHCP takes care it gets one, and more
  - Your computer sends out a *DHCP request* via UDP **broadcast** to port 67
  - A DHCP server *replies* via UDP and assigns
    - an IP address
    - the default gateway
    - a nameserver (where to send DNS requests to)

DE CIX

UDP and network security

UDP normal communication

Request and answer

Payload: Request

Payload: Answer

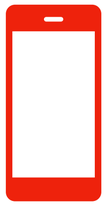
DE CIX

UDP as attack tool

Faked request and misdirected answer

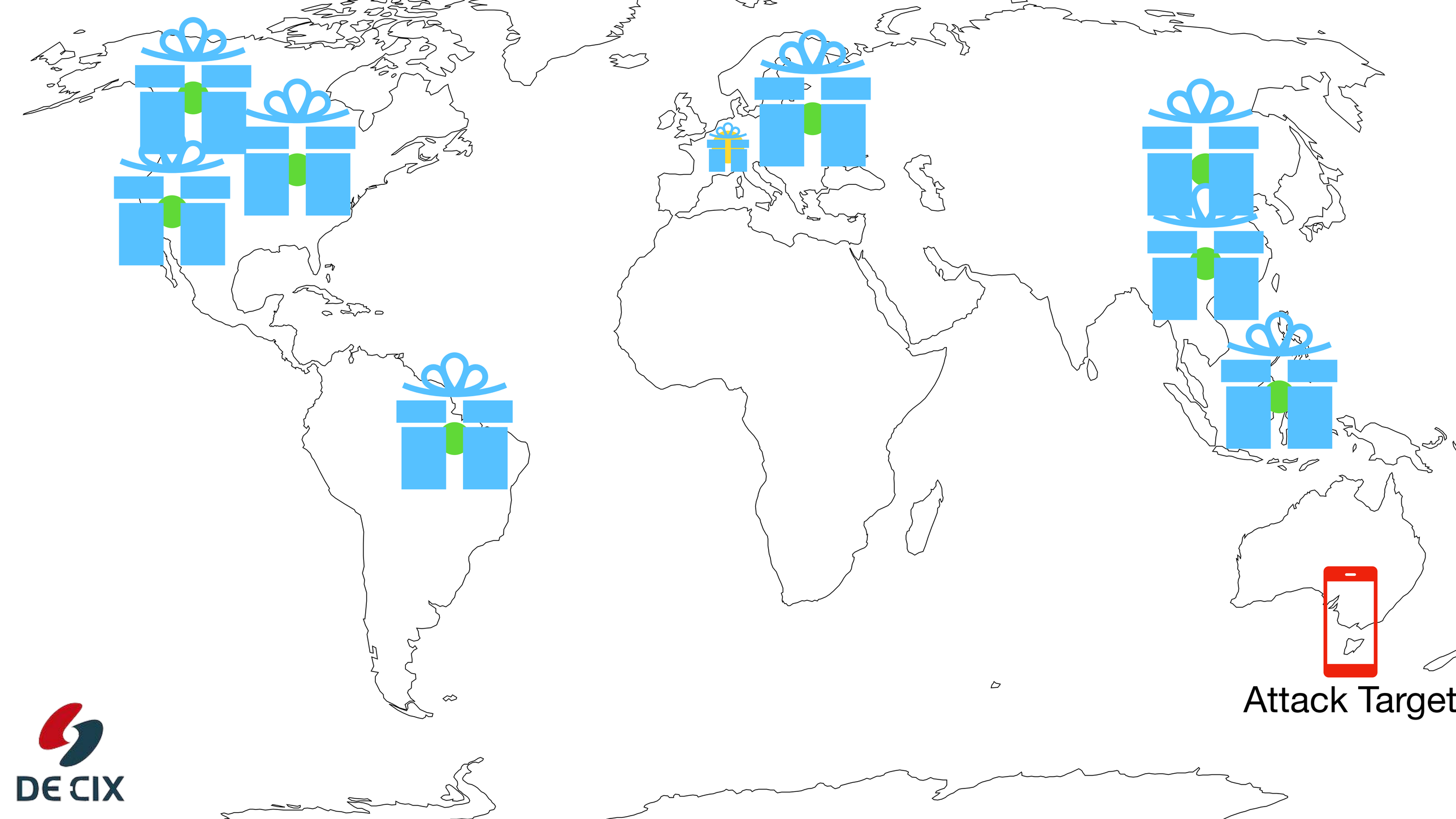
Payload: Request

Payload: Answer

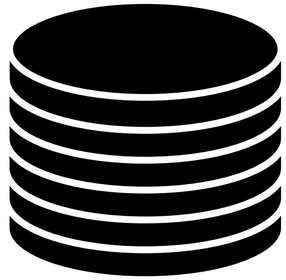


Attack Target

DE CIX


Attack Target

A real world example
Memcached

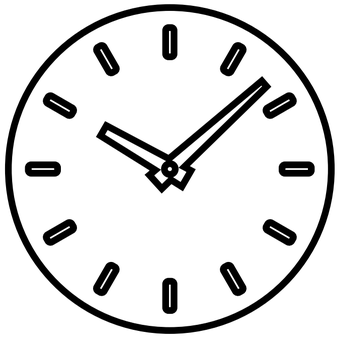


- memcached is a software to cache objects in RAM for fast retrieval
- Attack method:
  - tell an unsecured installation of *memcached* to store an object
  - send an UDP packet to that installation with a **faked source IP** to retrieve that object
  - this gives you an amplification factor of up to 51000
- Solution: Remove UDP from memcached

DE CIX

A real world example

NTP - Network Time Protocol (2010)



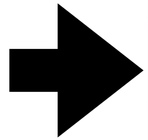
- NTP is a protocol to synchronize computer clocks using the Internet
- The "*monlist*" command, sent via UDP to an NTP server returns the list of the last 600 hosts who have connected to that server
  - If sent from a faked IP source address, this list is sent via UDP to the faked source
- Solution: "*monlist*" command was removed from the software

DE CIX

Conclusion

Conclusion

UDP - User Datagram Protocol



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

- UDP is a connectionless protocol on the transport layer
- UDP packets are also called "datagrams"
  - the UDP header contains a source and a destination port number
- If misconfigured, UDP services can be used for network attacks
- More and more services which relied on UDP are moved to TCP
  - But TCP is the topic of the next episode

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

- List of IP protocol numbers
  - https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers
  - https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
- UDP - User Datagram Protocol
  - https://en.wikipedia.org/wiki/User_Datagram_Protocol
- UDP and Internet Security
  - IP address spoofing https://en.wikipedia.org/wiki/IP_address_spoofing
  - Anti-Spoofing https://www.manrs.org/isps/guide/antispoofing/
  - Denial of service attack
    - https://en.wikipedia.org/wiki/Denial-of-service_attack
    - https://en.wikipedia.org/wiki/UDP_flood_attack
    - Memcached
      - https://en.wikipedia.org/wiki/Memcached
      - https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/
    - NTP
      - https://en.wikipedia.org/wiki/NTP_server_misuse_and_abuse
      - https://arstechnica.com/information-technology/2014/01/new-dos-attacks-taking-down-game-sites-deliver-crippling-100-gbps-floods/

Internet RFCs (Standards)

- Applications of UDP
  - NTP - RFC5905
  - DNS - many RFCs, start here: https://en.wikipedia.org/wiki/Domain_Name_System
  - DHCP - start with RFC2131

- RFCs about UDP:
  - UDP is first introduced in RFC768
  - UDP usage guidelines in RFC8085

- 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