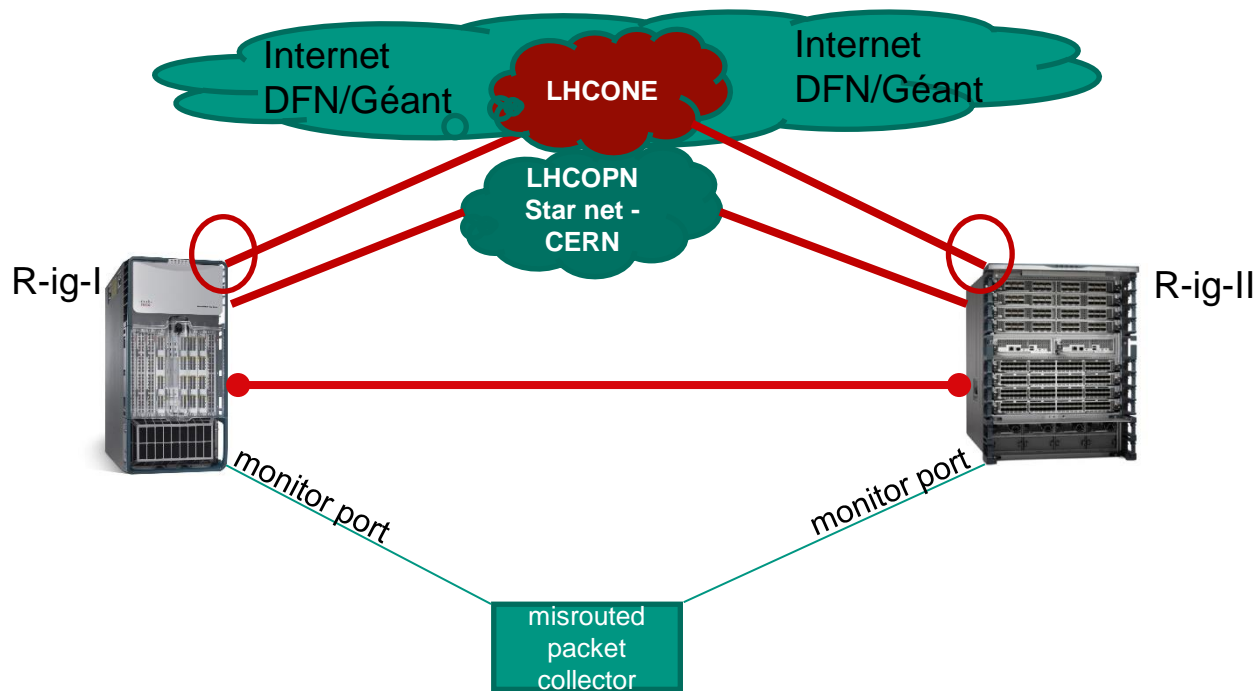# Unwanted packets at LHCONE

Bruno Hoeft – Karlsruhe Institute of Technology

WAN layout

Current deployment does allow:

- separate LHCONE virtual interface only
- allow all bgp routing table CIDRs
- Filter out: all non-routing table containing received packets

unwanted Packet finder

At KIT still Cisco Nexus 7000 Series Border Switch/Router running

- Matching against the LHCONE routing table
- Able to strip the header of not matching packts to a mirror port
- Found during 80 days **21.549.536** unwanted packets from close to 500 diffrented AS numbers and 10602 sources
(probl. hosts/router) (private sources not included)

Previous slide

All counted packets (at beginning of 2019)
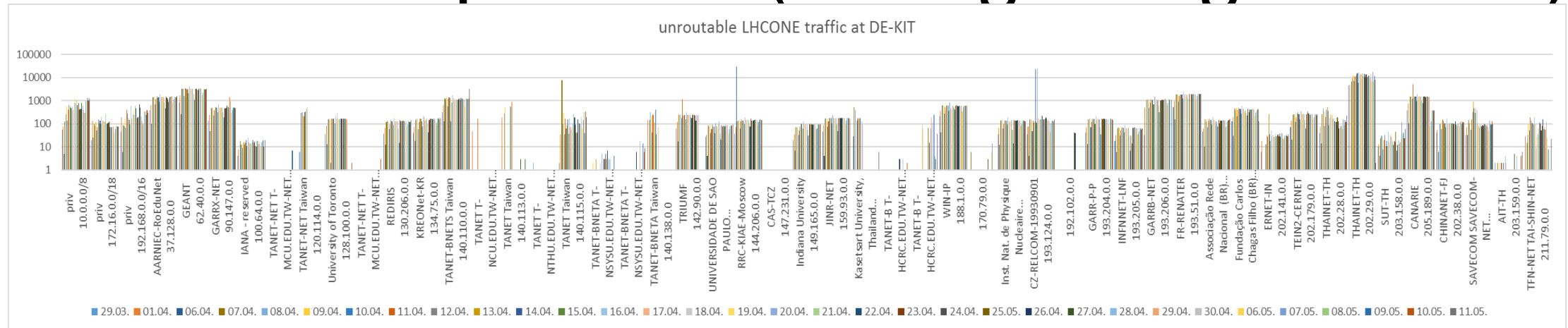
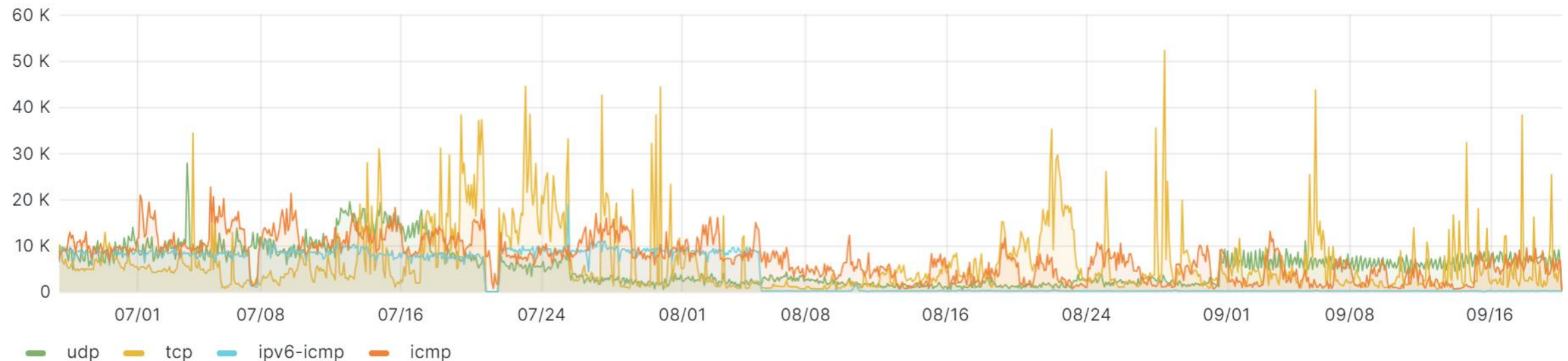Total : 1010889 + 33582 = 1044471

Packts per day: **19707**

⟶ Today: a per day packet rate above **220.000**

Splittet to diffrent AS'es/protocols

Org.-Name	AS-number	number of packets
Amazon	16509	2928540
ESnet	293	2916543
JPNIC	2907	2735478
JISC	786	2696245
APNIC (Taiwan)	7539	2582628
RoEduNet	2614	2035052
KFKI-AS (Wigner)	3314	1935188
IN2P3	789	1661567

US, CH, CA, BE, IS, UA, AE, PS, RU; FR, DE SG, AU,
PL, ID, BH, IN, JP, KR, SE, HK, GB, BR, IT, ES, ZA, NG

ICMP	IPv4	5187010
	IPv6	4044466
udp	IPv4	6046847
	IPv6	687108
tcp	IPv4	2986452
	IPv6	4260452

Protocol graph

transport

Legend: udp, tcp, ipv6-icmp, icmp

Sources:

Split into areas:

Central Europe

DFN - Hamburg

DFN - Bremen

Nikhef Network Operations Centre

Ice Communication Norge AS - Göttingen

DFN - Kassel

DFN - Cologne

Universite catholique de Louvain

Amazon Data Services Ireland

Vrije Universiteit Brussel

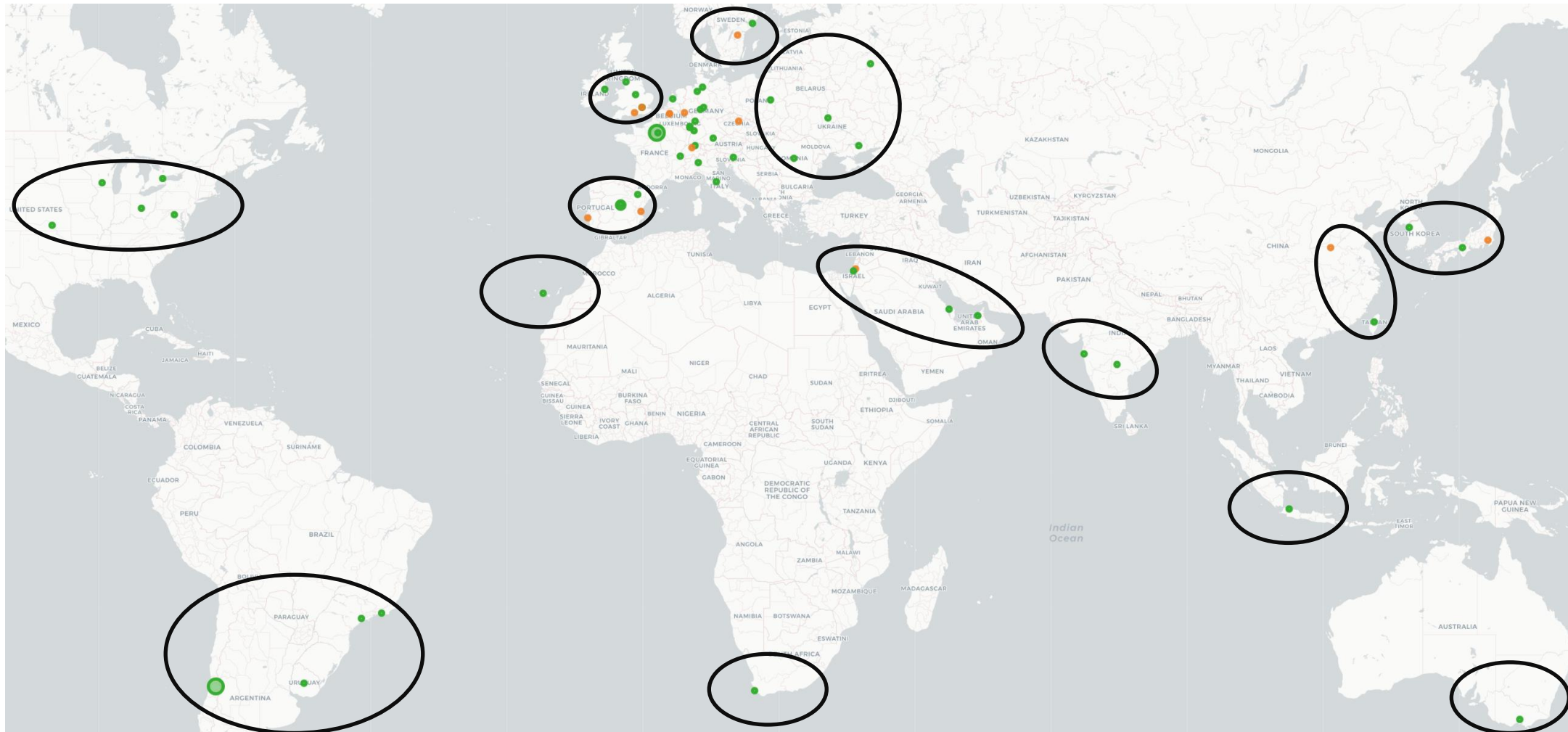DFN - Kaiserslautern

KIT

Renater

Leibniz-Rechenzentrum

Amazon Data Services Ireland

CERN
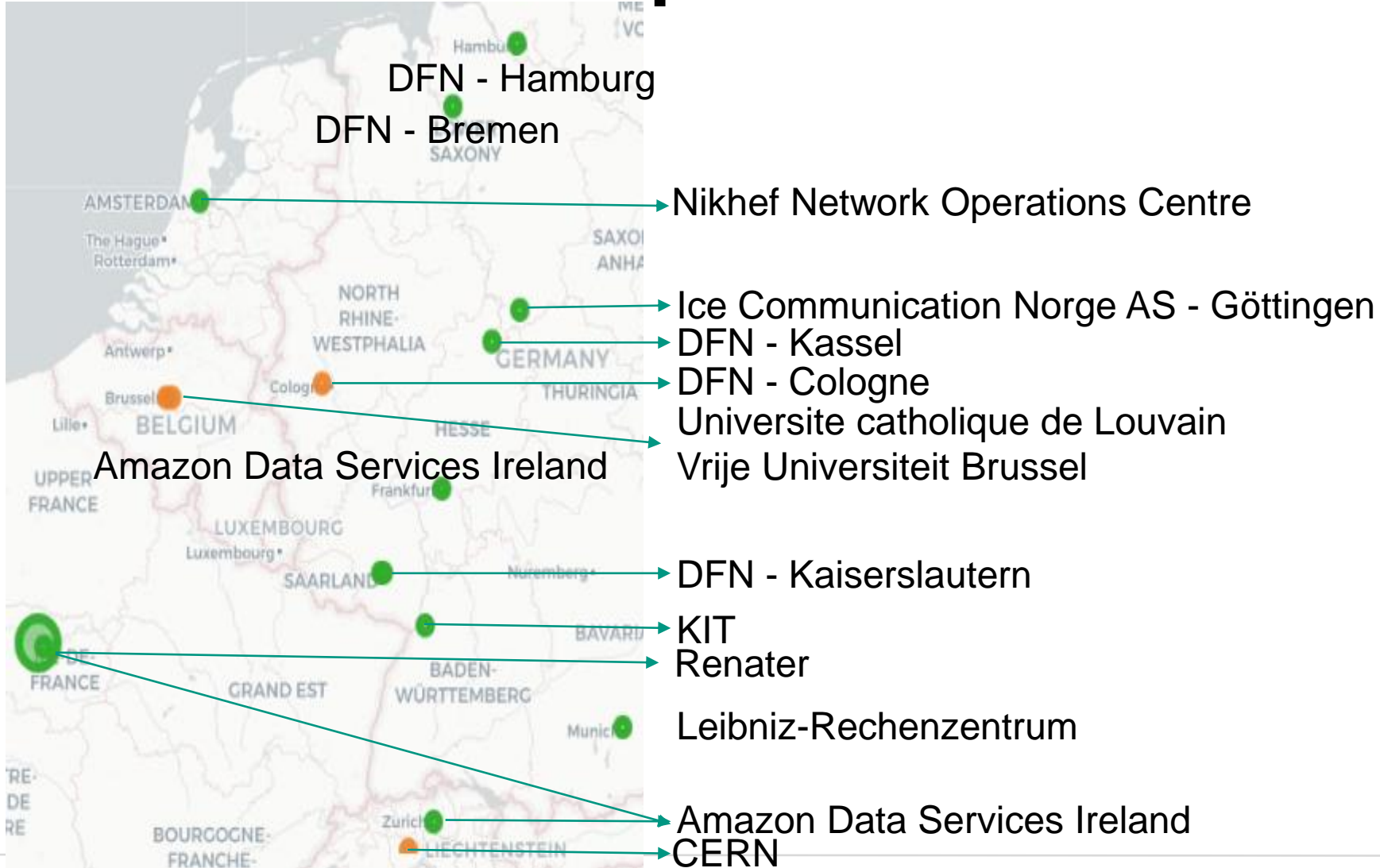
unwanted LHCONE packets project ?

or act on it

     would require a group of at least 4 people

      - beneficial would be having site and ISPs representatives

        as parts of this group

    In case there is interest i am happy to organize the working

      group with sites / ISP together

task already obvious:

How AWS (Amazon) is bridged to LHCONE

Identify other options to prevent misrouted packets

is uRPF a path to go (or is this to restrictive and will cause more trouble…)

Thanks – Questions

USA

Data taken from 2023-06-26 14:09:42 to 2023-09-08 10:55:40

2607:f388:101c:1000::119: 12

2607:f8f0:c10:70f3::60: 23

2600:1f18:5b75:b804:6916:bab7:8df8:bb72: 117
2600:1f18:5b75:b803:ffd8:fce2:44b7:8f43: 100
2600:1f18:5b75:b800:983f:45d6:41e5:5925: 99
2600:1f18:3120:f505:1ca7:178b:2529:6588: 123
2600:1f18:3120:f504:b7cb:dd12:d475:9c2f: 142
2600:1f18:3120:f503:eafb:7d00:3e6f:693: 163
2600:1f18:3120:f502:e26d:b047:40e5:d050: 197
2600:1f18:3120:f501:8557:d9f2:3e83:b6ee: 182
2600:1f18:3120:f500:7f9e:112c:57bc:29f5: 128

2620:83:8000:4d07::b: 22 2620:83:8000:4d02::15: 113
2620:83:8000:4d01::15: 56 2607:ff10:c8:594::6: 6
2607:ff10:c8:594::5: 3 2607:f720:1700:1b30::82: 10
2605:d9c0:1:61::11:20: 12 2605:d9c0:1:5::1:2: 6
2605:9a00:10:200a:e643:4bff:fe1b:2608: 16
2602:fd0f:0:1001::20: 24 2602:fd0f:0:1001::19: 22
2602:fd0f:0:1001::18: 36 2602:fd0f:0:1001::2: 5
2600:900:6:1102:2eea:7fff:fef5:d140: 12
2001:48a8:68f7:1:7efe:90ff:fe64:d579: 10
2001:18e8:c02:5:b27b:25ff:feb9:d30e: 10

2600:1f16:668:2002:9904:b34a:7a85:8a4f: 82
2600:1f16:668:2001:910f:1a2c:9327:db3c: 187

Unwanted packets at LHCONE, LHC[OPN/ONE] Meeting, Victoria (BC), October 18, 2023