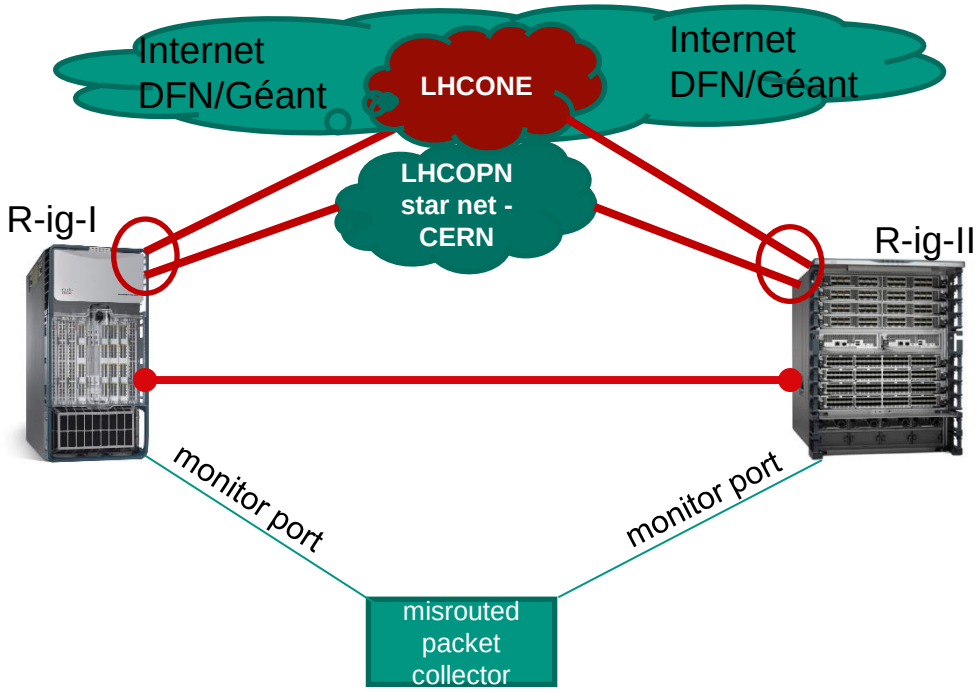
Karlsruhe Institute of Technology

GridKa

LHCONE unrouteable packets

Bruno Hoeft (KIT)

WAN layout



Current deployment does allow:

- Monitoring 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
- duplicate the header of not matching packts to a mirror port
- **107.162.478** unwanted packets found during **90 days**
  - **from 12 diffrented AS numbers**
  - **1560 sources (incl. some packets from private addresses)**
  - **approx. 5x as in 2023 and**
  - **no Cloud (AWS, Asure, GCP, …)**

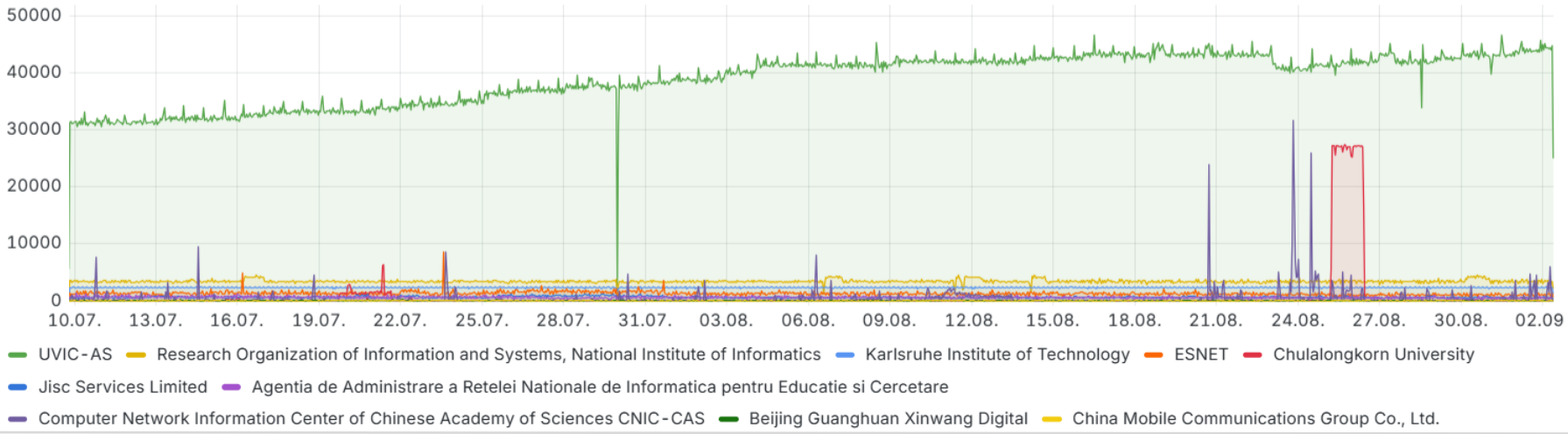
Distribution over a worldmap

Traffic pattern

Increase of UVIC-AS

More precise:
The latency + bandwidth perfsonar server
ps-latency.hepnetcanada.ca.
ps-bandwidth.hepnetcanada.ca.

traffic by source.asn_org



UVIC

increase over time

90 Days:

Name	Country	AS	IP	Count
UVIC-AS	CA	16462	2607:f8f0:c11:7000:b696:91ff:fe26:5620	10
UVIC-AS	CA	16462	2607:f8f0:c11:7000:b696:91ff:fe26:55dc	10
UVIC-AS	CA	16462	2607:f8f0:c11:700b::59	5525025
UVIC-AS	CA	16462	2607:f8f0:c11:700b::60	58465575

30 Days:

UVIC-AS	CA	16462	2607:f8f0:c11:700b::59	1838403
UVIC-AS	CA	16462	2607:f8f0:c11:700b::60	24261344

1 Day:

UVIC-AS	CA	16462	2607:f8f0:c11:700b::59	64861
UVIC-AS	CA	16462	2607:f8f0:c11:700b::60	940417

	2607:f8f0:c11:700b::59 ps-latency.hepnetcanada.ca	2607:f8f0:c11:700b::60 ps-bandwidth.hepnetcanada.ca
2025-03-09	64754	242019
2025-04-09	57578	390095
2025-05-09	60097	514498
2025-06-09	62800	591503
2025-07-09	60470	694212
2025-08-09	62928	948457
2025-09-09	63020	1044397

The 12 ASes are:

	Packets (periode of 90 days)
UVIC-AS CA 16462	**78166714**
Computer Network Information Center of Chinese Academy of Sciences CNIC-CAS CN 7497	**8644319**
Research Organization of Information and Systems, National Institute of Informatics JP 2907	**7410760**
ESNET US 293	**2847094**
CESNET z.s.p.o. CZ 2852	**2372893**
Agentia de Administrare a Retelei Nationale de Informatica pentru Educatie si Cercetare RO 2614	**1413160**
Jisc Services Limited GB 786	**1380526**
Chulalongkorn University TH 4621	**933378**
Beijing Guanghuan Xinwang Digital CN 55960	**38928**
China Mobile Communications Group Co., Ltd. CN 9808	**26188**
NSC KIPT UA 35296	**21959**
CHINA UNICOM China169 Backbone CN 4837	**8089**

Hosts injecting traffic

Order by looking at 1 day / 30 days the same (exept the the last two lines)

Source		count/24 hours	%
ps-latency.hepnetcanada.ca.	-- 2607:f8f0:c11:700b::60	934783	65,39
KEK → no dns-name	-- 2001:2f8:3e:cc26::4:39	94126	
lhcopn-cnaf-dci-r1-v6.ipv6.cern.ch.	-- 2001:1458:302:4c::2	82974	
ps-bandwidth.hepnetcanada.ca.	-- 2607:f8f0:c11:700b::59	58378	
Canari → no dns-name	-- 205.189.32.55	26504	
Canari → no dns-name	-- 2001:410:101:f01::2	23775	
Stfc → no dns-name	-- 2001:630:58:1080:2::b	12976	
Romanian Education Network→ no dns-name	… -- 2001:b30:0:18d::2	5617	
newy32aoa-cr6--wash-bb-e.igp.es.net.	… -- 2001:400:0:668::	3884	

Additional worldmap dots

traceroute:

Y 47.45.19.254 syn-047-045-019-254.biz.spectrum.com CyberOne Data, Port Edwards (WI)
Y 103.104.168.38 APNIC Brisbane, Australia
N 80.81.195.138 de-cix-rnd-measurement.fra.de-cix.net.
Y 163.171.132.[378] CDNetworks – South Korea
Y 2607:f8f0:16c0:1::3 / 209.87.0.3 (name.forward.heitbc.ca (ipv4 only)) BCNET Vancouver (🡐 now included in LHCONE)
N 100.64.255.158 / 100.64.251.226 IANA reserved (shared address space)
N 170.79.215.[389] fcbk-fna-cpe1. /dnsnic-mxam. /csc1-dnsnic.bkb.rnp.br Rede Nacional de Ensino e Pesquisa -- Brasil

Private,… Addresses (period of 30 days)

IPv4:

10.0.0.0/8 + 172.32.0.0/12 + 192.160.0.0/16
: **83064** packets

IPv6:

ULA
: **7,021M** packets
LLA
: **154610** packets

Conclusion

Currently all unrouteable packet sources are within the NRENs/LHC-sites (or somehow trusted entities)

ca. 13,78pps compared to 1.3Mpps
Yes, → small #

→ does not look alarming (sources RNE)

- but crucial if malware
- to identify you would need ESnet High Touch or something similar
- automated update of LHCONE bgp table filter
- people engaging in it

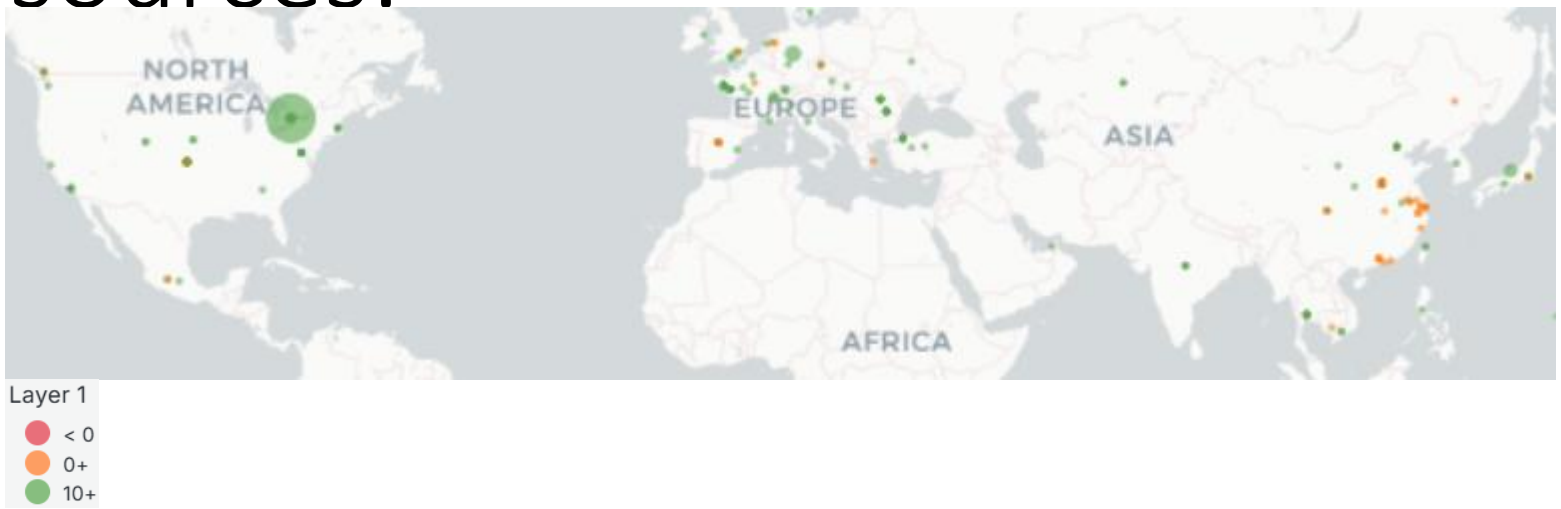
Karlsruhe Institute of Technology

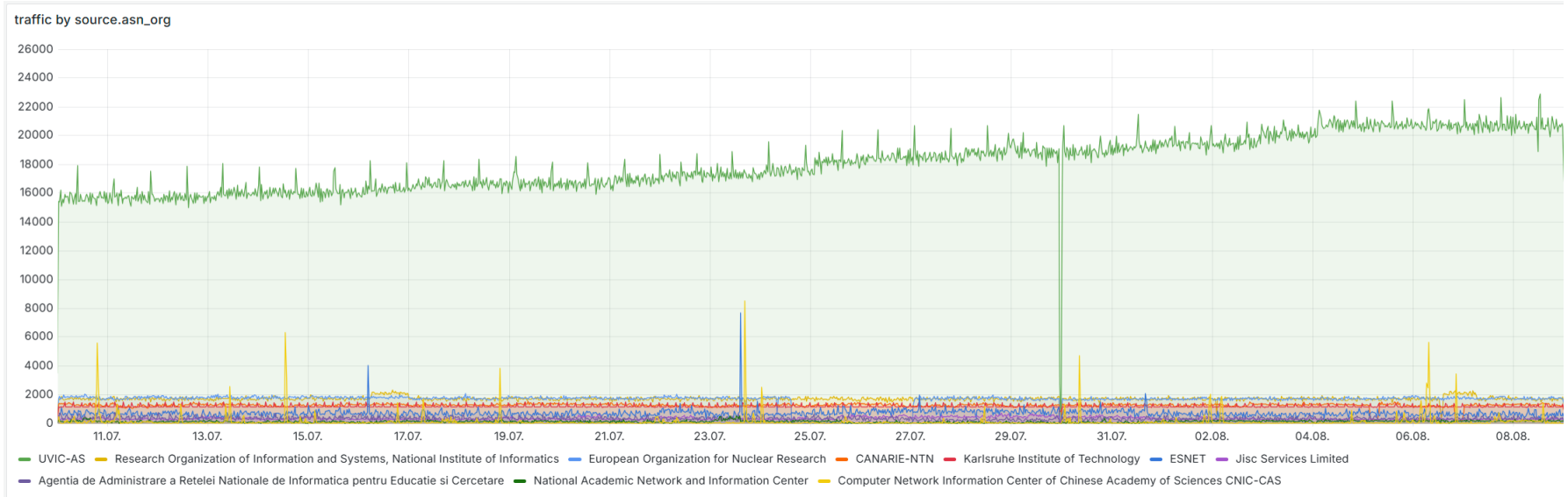
GridKa

Questions ?

Source		count/24 hours	%
ps-latency.hepnetcanada.ca.	-- 2607:f8f0:c11:700b::60	934783	65,39
KEK → no dns-name	-- 2001:2f8:3e:cc26::4:39	94126	
lhcopn-cnaf-dci-r1-v6.ipv6.cern.ch.	-- 2001:1458:302:4c::2	82974	
ps-bandwidth.hepnetcanada.ca.	-- 2607:f8f0:c11:700b::59	58378	
Canari → no dns-name	-- 205.189.32.55	26504	
Canari → no dns-name	-- 2001:410:101:f01::2	23775	
Stfc → no dns-name	-- 2001:630:58:1080:2::b	12976	
Romanian Education Network→ no dns-name	-- 2001:b30:0:18d::2	5617	
newy32aoa-cr6--wash-bb-e.igp.es.net.	-- 2001:400:0:668::	3884	

sources:


NORTH AMERICA
EUROPE
ASIA
AFRICA
Layer 1
< 0
0+
10+


traffic by source.asn_org
26000
24000
22000
20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
11.07.
13.07.
15.07.
17.07.
19.07.
21.07.
23.07.
25.07.
27.07.
29.07.
31.07.
02.08.
04.08.
06.08.
08.08.
UVIC-AS
Research Organization of Information and Systems, National Institute of Informatics
European Organization for Nuclear Research
CANARIE-NTN
Karlsruhe Institute of Technology
ESNET
Jisc Services Limited
Agentia de Administrare a Retelei Nationale de Informatica pentru Educatie si Cercetare
National Academic Network and Information Center
Computer Network Information Center of Chinese Academy of Sciences CNIC-CAS

- The first 7 sources are the major part (85%)
- 99 ip sources / 24h
- 407 ip sources / 30 days – 204 host names resolved
- the first sources are equal → comparing one and 30 days periode
- all ip sources are somehow located at NRENs or wlcg site domain
- # of LHCONE incoming packets:
  the 1,4M misrouted packets are 0,33% of the total ~419G packets of one day