LHCONE Edge Filtering Policy and Practice

Bruno Hoeft / KIT
Michael O'Connor / ESnet
Kars Ohrenberger / DESY

STEINBUCH CENTRE FOR COMPUTING - SCC

LHCONE Route Admission Objective

Objective: In order to maintain route symmetry and controlled access, each NSP will implement policy and packet filters to manage their connected customer address prefix ranges.

All LHCONE Traffic is subject to the following conditions:

- Traffic injected into the LHCONE can only be originated from addresses within an LHCONE route prefix
- Traffic injected into the LHCONE will be destined for an LHCONE Prefix

https://twiki.cern.ch/twiki/pub/LHCONE/LhcOneVRF/LHCONEconnectionguide-1.2.pdf

NSP BGP Import Policy

Prefix Lists will be negotiated between connecting institutions and their NSP within the constraints imposed by the LHCONE AUP.

The NSP will codify this agreement in terms of:

1. BGP import filters
2. Source address packet filters

Connecting institutions should not have the ability to add prefixes to the LHCONE routing table without direct cooperation with their NSP.

NSP Packet Filtering Requirements

NSPs will implement packet filters at their edge based on the prefixes ranges imported from customer sites.

All accepted packets will be sourced from address ranges present in the LHCONE routing table.

This serves multiple purposes:

1. Ensures that a return route exists in the LHCONE network
2. Restricts forged traffic

A connecting site should be confident that only address ranges present in the LHCONE routing table will arrive on their network connection.

The Investigation

DE-KIT Router Packet Filters

- Unsampled ingress at DE-KIT used to detect routing table misses from over 35 source locations.

ESnet

- Three months of ESnet netflow IPv4 & IPv6 sampling from Nov 2017 - Jan 2018 for the following sites and peers

aarnet	ind-gpop	slac
aglt2	internet2	tacc
anl	kreonet	uchicago
ansp	lhcone_cern	ucsb
asgc	lhcone_ornl	ucsd
bnl	mit	ufl
caltech	net2	uiuc
canet	nordunet	unl
cernlight	ou	uta
duke	pnnl	uwmadison
fnal	rnp	vanderbilt
geant	sinet	

We counted:

- Routable packets
- Unroutable packets
- Packets with bad origin ASN

* corrected for netflow sampling rate

Detailed data at:
https://twiki.cern.ch/twiki/pub/LHCONE/LhcOneVRF/LHCONE-ESnet-Address-Filtering-Detail.pdf

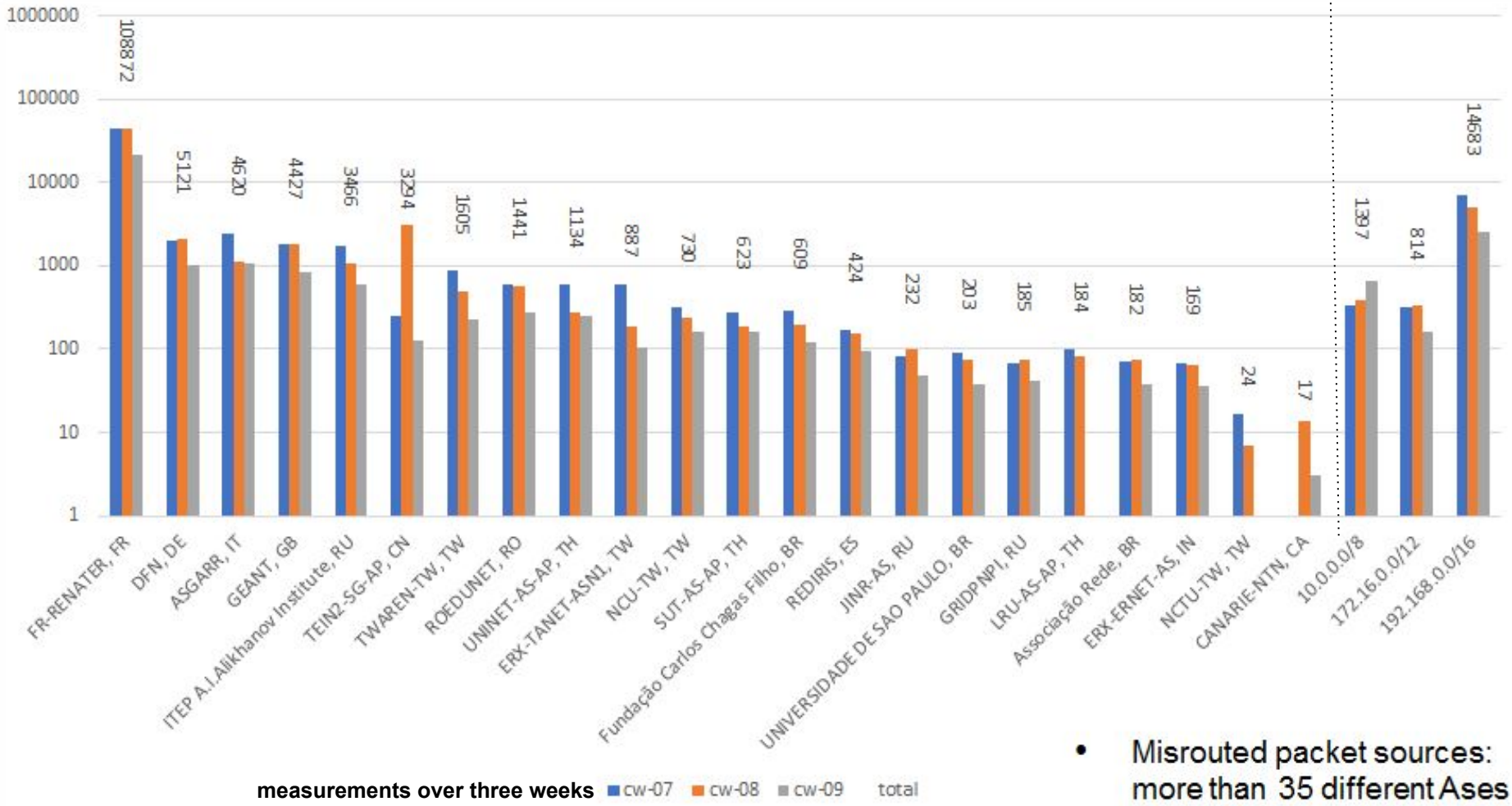
unroutable packet count @ DE-KIT

155343 approx. 0,5% of total traffic

16894

source → traceable

untraceable

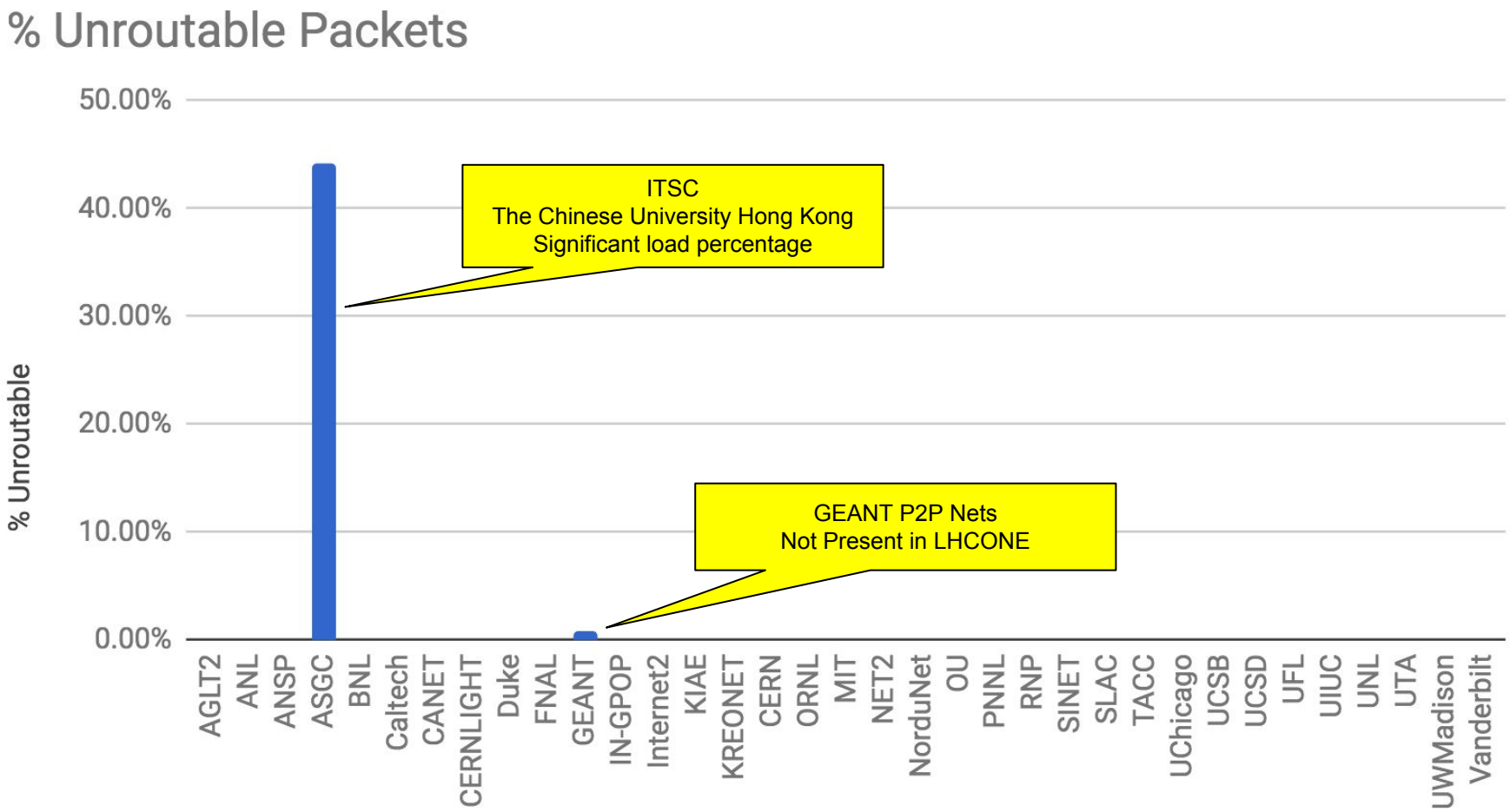


- Misrouted packet sources: more than 35 different Ases

Misrouted packets @ DESY

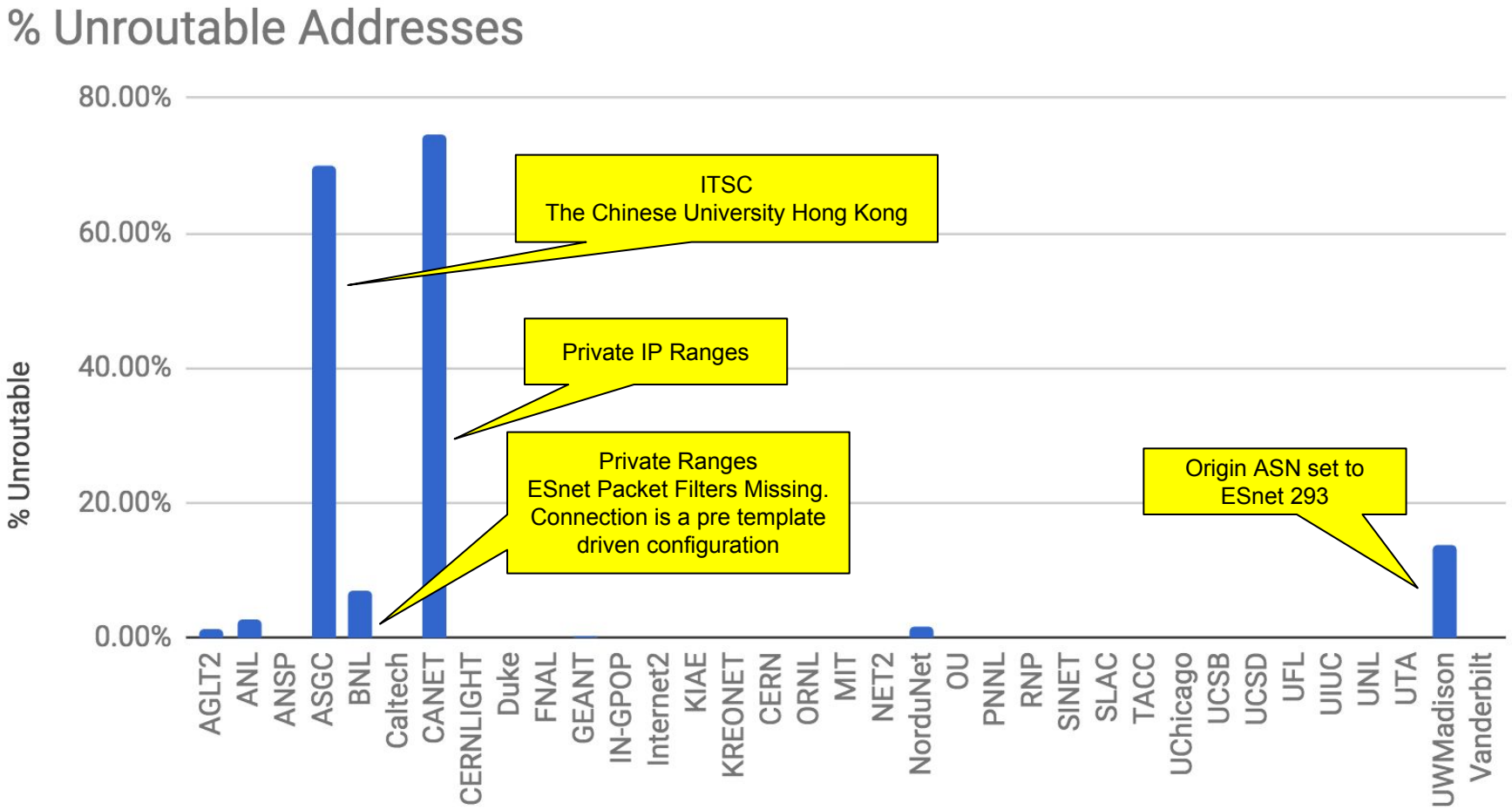
- Data capture periode: Jan. 1 - Feb. 5 2018
- Total: 335.478.209 packets
  9.318.840/Day
- Misrouted packet sources: 44 different ASes
  - Hostnames seems LHC project related

ESnet monitoring



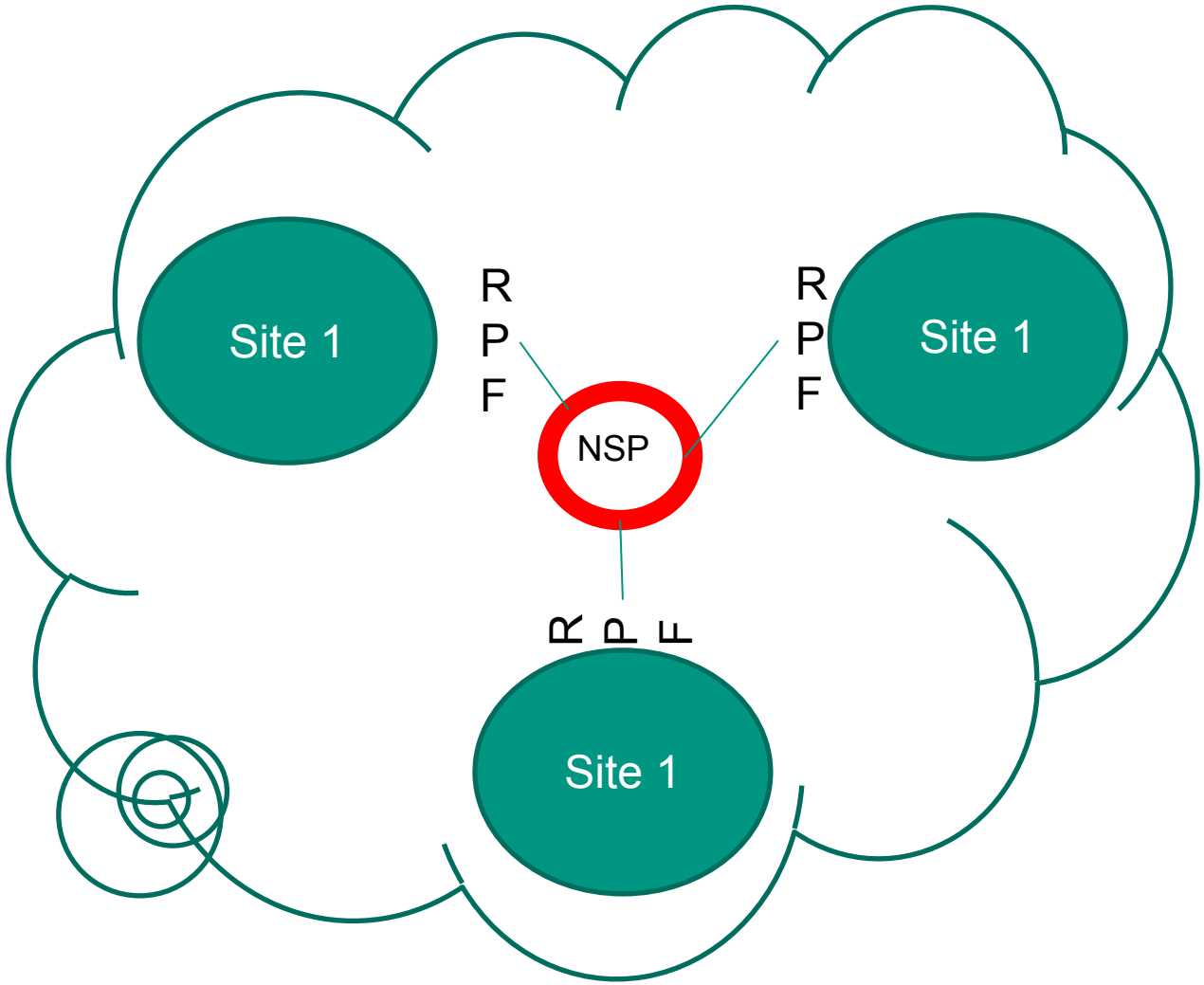
The Geant IPv6 P2P network addresses have not been exported, they are unroutable in LHCONE

ESnet monitoring



Template driven LHCONE configuration has eliminated leaked packets from our sites.
We are retrofitting the early hand configured connections.

Within the NREN domain



- RPF filter at connected sites
  - Is only half of the solution?
  - Verify that their content is AUP compliant
  - Educate the connected site
  - Workout a AUP comliant configuration with the connected site

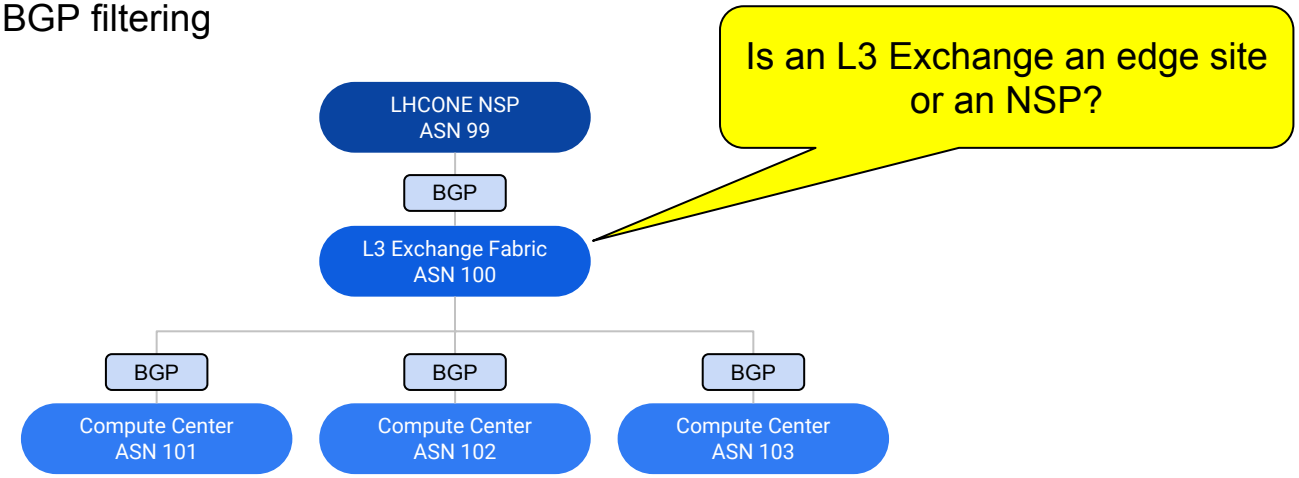
Edge Filtering Special Case

L3 Network Exchange Fabrics

Where should the following be implemented:

- BGP import filtering
- Packet filtering
- Community based BGP filtering

What is the trust model?



- Will L3 Exchange Fabrics implement and maintain LHCONE specific services?
- Should there be an LHCONE defined role for these network organizations?

Potential Courses of Action

To eliminate unroutable traffic:

Detection

- Regularly scheduled monitoring?
- Periodic NSP self run audits?

Prevention

- Edge Site filter configuration
  - RPF
  - Templated policy & filter configuration

Information

- Regular AUP updates to address special cases
- Sharing configuration best practices

Conclusion / actions

Unroutable packets are a regular occurance in LHCONE

- Violates the community trust relationship
- Damages LHCONE operational integrity and effectiveness

action plan:

- monitor
- filter
- educate connected sites
- define procedure
  - everyone finding issues talks to
    - his connecting NREN
    - to the NREN of the misrouted AS

Questions

Suggestions

Discussion