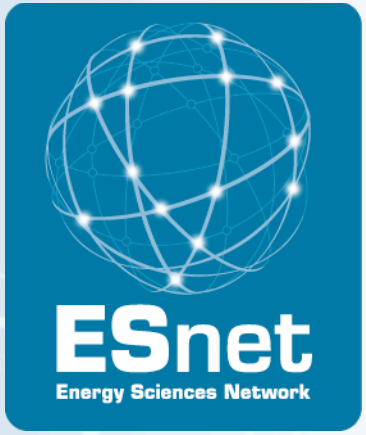


LHCONE Security Discussion

Mike O'Connor, Network Engineer

ESnet Engineering Group

LHCOPN and LHCONE Joint Meeting

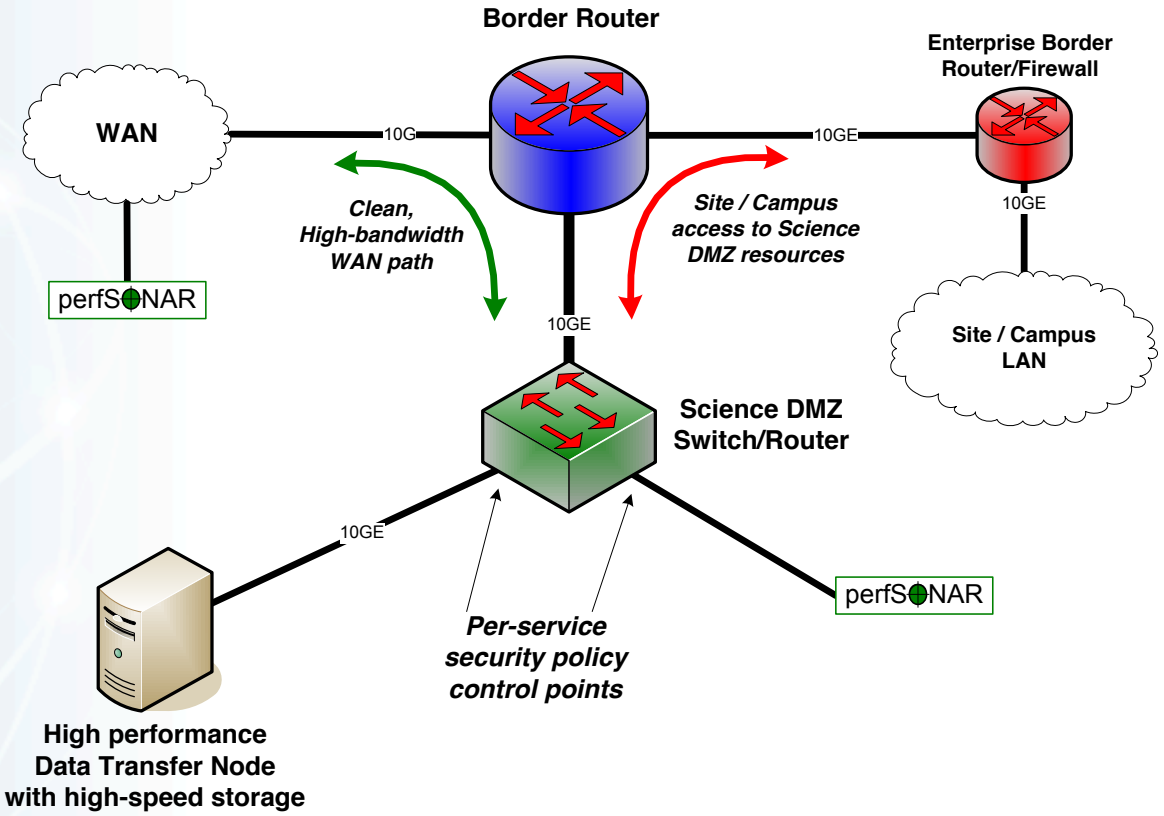
Oslo (No)

Sep 20-21, 2012

LHCONE Characteristics

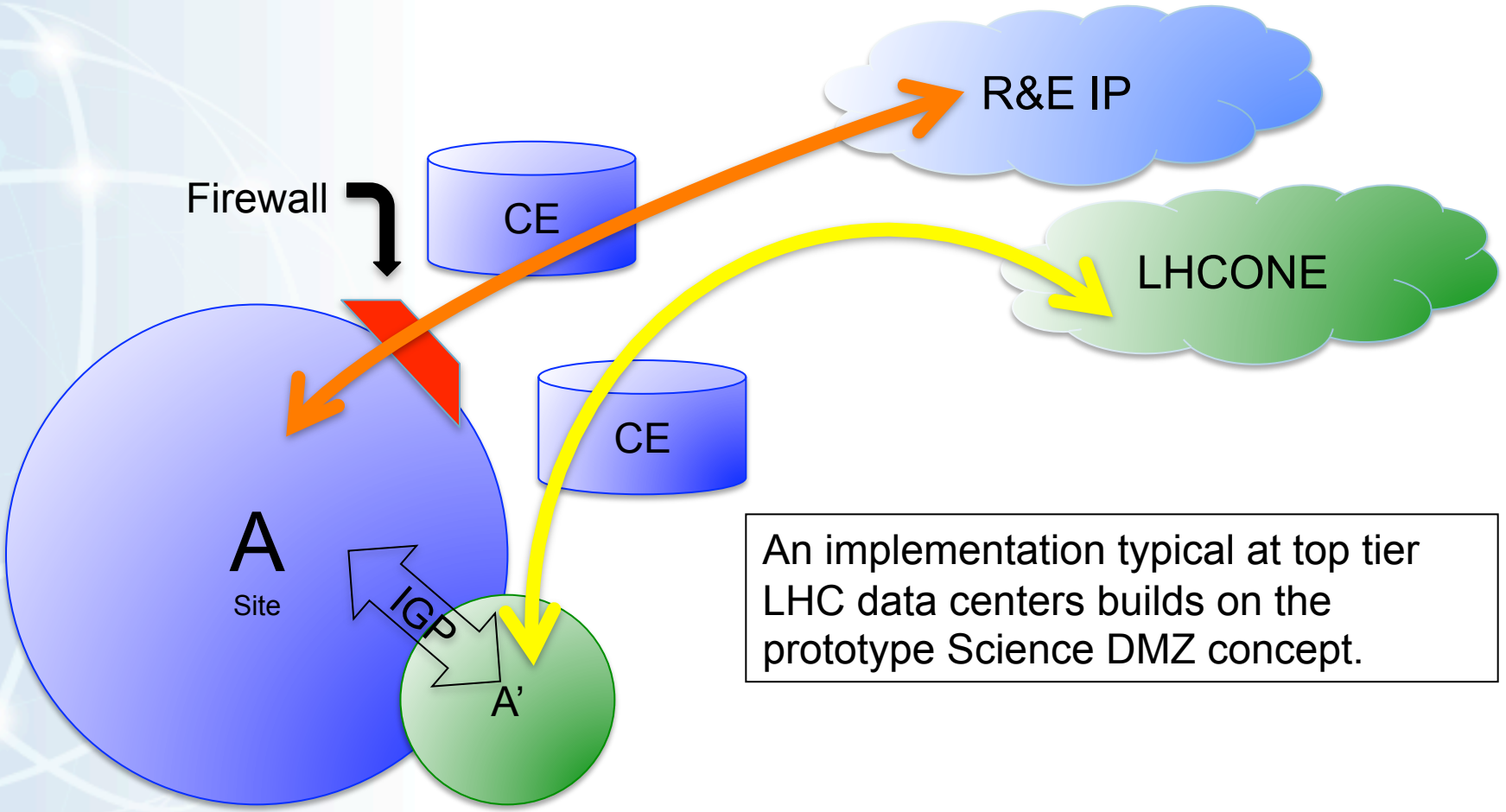
- A global collaboration of research institutions and R&E networks.
- Wide area purpose built bounded and collaborative Internet.
- Dedicated network resources, achieving high TCP performance, through low loss over potentially high latency wide-area paths.
- Typically implemented as a layer three overlay network with a limited routing table.
- Well instrumented, NOC services, PerfSonar etc.
- Builds on an integration with the Science DMZ model.
- No commercial or residential networks.
- No expectation of privacy among collaborating institutions or NSPs.

Prototype Science DMZ



LHCONE Science DMZ

Provides a high performance path alternative to a common perimeter chokepoint



An implementation typical at top tier LHC data centers builds on the prototype Science DMZ concept.

LHCONE Connection Types

Tightly integrated – Enterprise network is architected specifically for science DMZ scoped services. Larger compute centers well matched to WAN services, primarily Tier1 and Tier2 institutions and collaborations. Strong case for eliminating a FW.

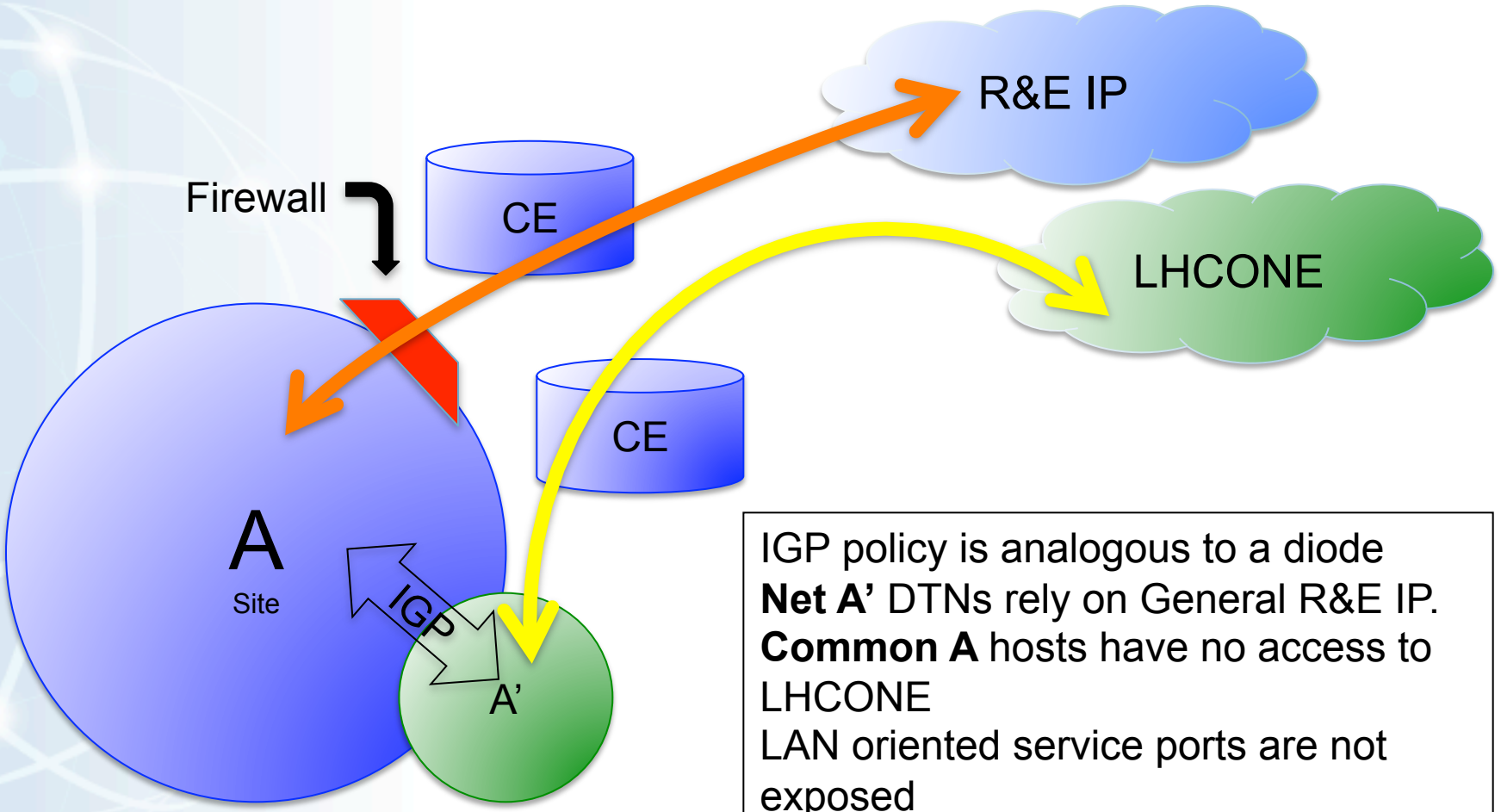
Loosely integrated – Lack significant alignment of the network architecture with science DMZ. Routing implementation where campus prefixes are all advertised to LHCONE. (A = A'). . Implemented in a similar fashion to their General R&E Internet connection, IDS recommended. Weaker case for eliminating a FW.

Delegated – NSP injects a site's prefixes into it's LHCONE VRF. VRF peers with NSP core. Minimal if any Science DMZ. NSP policy routing could potentially affect performance of the core and or VRF.

Discussion: Have any NSPs either implemented or considered a Delegated type connection?

Tight Integration

Architecture Is designed for DTN integration with LHCONE



IGP policy is analogous to a diode
Net A' DTNs rely on General R&E IP.
Common A hosts have no access to LHCONE
LAN oriented service ports are not exposed

Data Transfer Nodes and the Science DMZ

LHC compute facilities have moved toward scalable host management solutions and virtualization in DTN deployments.

Only the required and carefully provisioned WAN service ports are provisioned on their **A'** network blocks. This obviates the need for the kind of "blanket" perimeter protection required for LAN oriented service ports typically provided by a perimeter firewall or router ACLs.

Scalable host management tools (ie: puppet) are used to enforce strict service port provisioning on externally exposed DTN network interfaces.

This type of scalable host management is a core component of a tightly integrated Science DMZ.

> An accept source ANY firewall ACL is equivalent to a no-op.
> John Hover - US ATLAS

LHCONE & More Specific Prefixes

LHCONE contains many “more specific” BGP prefixes, particularly from the tightly integrated collaborators.

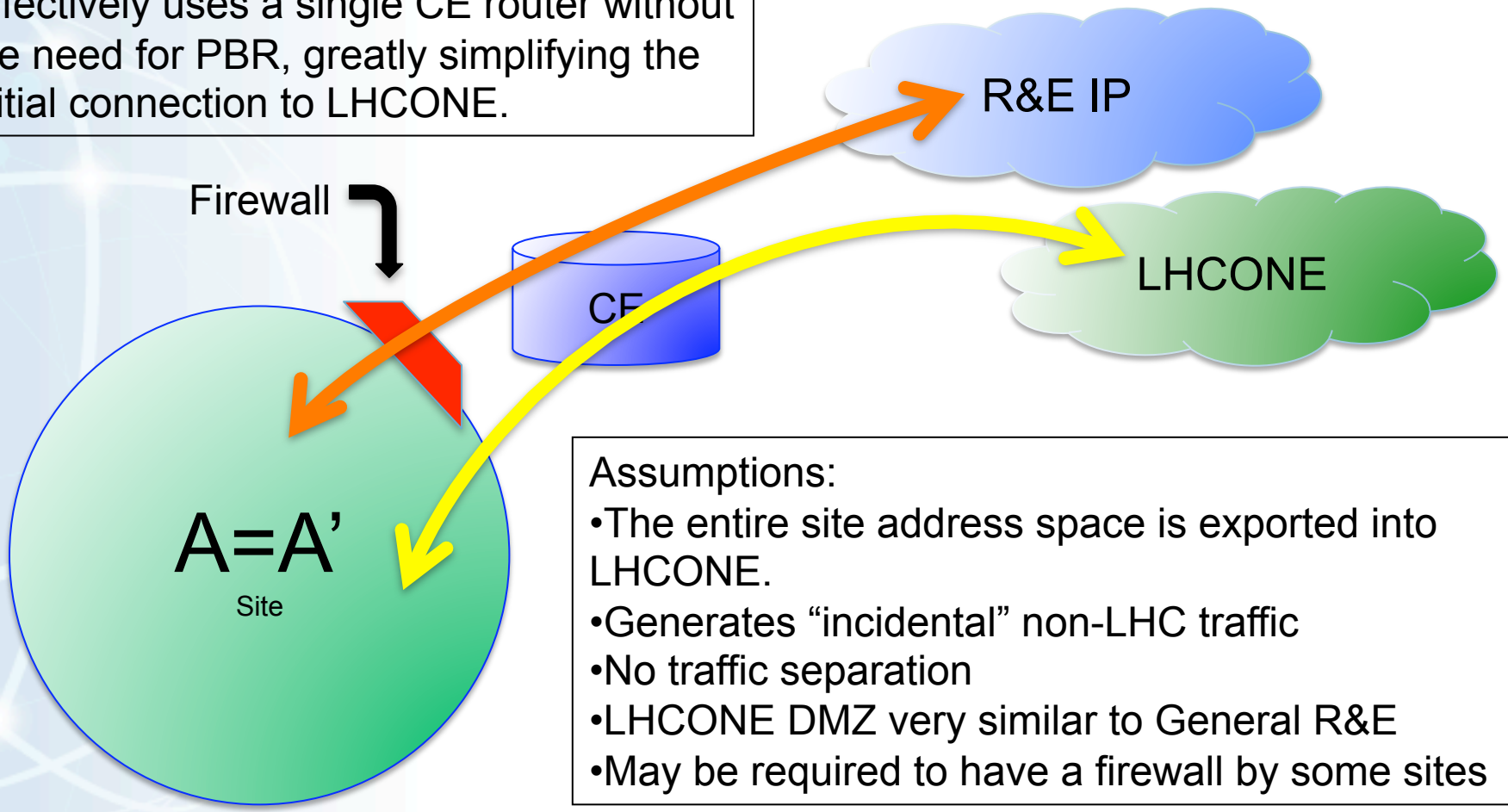
If present in the general campus routing table, these LHCONE more specific routes will be preferred over their covering prefix.

LHCONE can be viewed as “sucking up” all traffic to these more specifics.

Loose Integration

Minimal Integration with LAN architecture

Effectively uses a single CE router without the need for PBR, greatly simplifying the initial connection to LHCONE.



Assumptions:

- The entire site address space is exported into LHCONE.
- Generates "incidental" non-LHC traffic
- No traffic separation
- LHCONE DMZ very similar to General R&E
- May be required to have a firewall by some sites

Incidental Flows

Loose network integration as defined by the A = A' nomenclature will induce the side effect of directing non-LHC related incidental flows, ie: email, DNS, HTTP, etc. across the LHCONE toward other loosely integrated collaborators.

Tightly integrated Science DMZs that are scoped exclusively for **A'** prefixes will not attract incidental flows because these enterprise services are deployed out of necessity in the general enterprise or **A** LAN and not on the science DMZ.

Discussion Point:

Are Incidental Flows acceptable on the LHCONE network?

Loosely Integrated
A=A’

- Eliminates the need to dramatically re-architect the enterprise network for a science DMZ.
- Policy Based Routing is not a potential requirement since no traffic separation is performed.
- The probability of routing asymmetrically is greatly reduced.
- LAN oriented service ports are exposed to the collaborative WAN and may require access control mechanisms depending on local security policies.
- Incidental flows.

Discussion: Is A=A’ an acceptable approach for certain collaborating institutions?

The loosely integrated institutions pose the most risk to themselves collectively.

Site Perspective
Sites Trust Site Security (.)

- In general, security policy is generated internally, even if it is in response to external compliance requirements.
- There is little that the WAN can do or should do to change that.
- Host security is essential, network security is viewed with skepticism.
- Firewalls can be described in terms of the network providing security. By extension, implementing security within LHCONE can be viewed as just another attempt at this futile approach.

Discussion: How can the LHCONE community assist collaborating institutions with their internal security policy, generation or compliance?

LHCONE Site Recommendations

- Define local LAN address ranges that will participate in LHCONE. Advertise these address range prefixes to LHCONE using BGP.
- Agree to accept all BGP route prefixes advertised by the LHCONE community.
- Ensure that only hosts in your locally defined LHCONE ranges have the ability to forward packets into the LHCONE network.
- Ensure that the LHCONE paths are preferred over general R&E IP paths.
- End sites should avoid static configuration of packet filters, BGP prefix lists and policy based routing, where possible. RPF filtering is suggested as a dynamic access control method for sites.

Discussion: Are the site recommendations reasonable and complete?

NSP Filtering Recommendations

- Prefix Lists – negotiated between LHCONE connecting institutions and the NSP.
- Packet filtering – RPF filtering, analogous to spoofing filters.

Objective – NSP's will block and count packets from sources not in the LHCONE routing table.

Benefits – NSP's may assist sites by alerting sites that are attempting to send none LHCONE traffic into LHCONE. Clear NSP visible indicator of asymmetric routing.

Discussion: Are the NSP filtering recommendations reasonable and complete?

Discussion Review

- Delegated connections?
- Are Incidental Flows acceptable on the LHCONE network?
- Is A=A' an acceptable approach for certain collaborating institutions?
- How can the LHCONE community assist collaborating institutions with their internal security policy, generation or compliance?
- Are the site recommendations reasonable and complete?
- Are the NSP filtering recommendations reasonable and complete?

Questions?

Michael O'Connor

ESnet Network Engineer

moc@es.net

631 344-7410