LHCONE Operational Framework

Part 1 : principles and ideas for the operational model
Part 2 : LHCONE VRF operational handbook
Part 3 : Next step

Xavier Jeannin
RENATER
2013/01/28

LHCONE VRF nature

- In standard a L3 VRF/VPN,
  - Users manage
    - Site operation
      - changes (new peering/site withdraw/prefixes)
      - maintenance
      - Information: relevant, location, maintaining up-to-date, publication
    - Security policy: firewall / filtering / science DMZ
    - Monitoring policy: tools, information and test available
  - NSP manage
    - routing policy
    - network monitoring : tools, statistics
    - network operation:
      - Relevant information (NOC email, tel., …)
      - Troubleshooting process: basic trouble (connectivity issue, …), asymmetric traffic, performance

- LHCONE VRF is a specific L3 VPN
  - Multi user entities
  - Multi NSPs

→ collaboration is required

operational handbook

- Create a light documentation :
  - https://twiki.cern.ch/twiki/pub/LHCONE/LhcOneVRF/LHCONE_VRF_Operational_Handbook-v0.2.pptx
  - Avoid a 100 pages, static document, never updated
  - Living document : the strict minimum … but be accurate enough to
  - Summarize all operation specification in one document
    - Collect the result of different sub-groups (routing, security, monitoring sub group
    - Point to all relevant documents

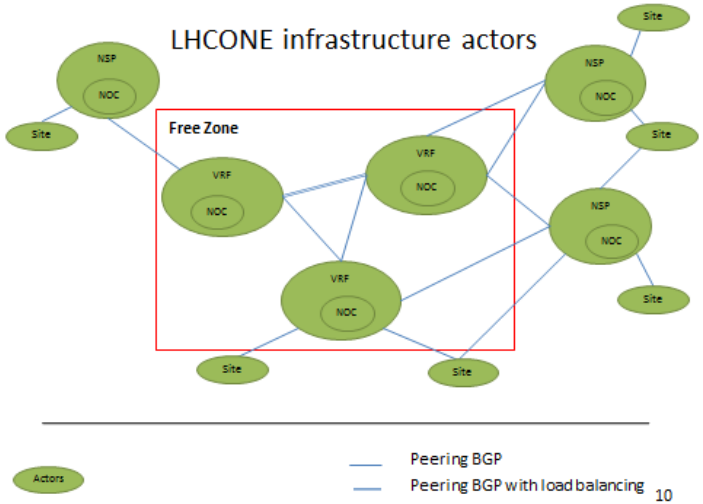
- Goals
  - help a new site for its connection to the LHCONE and to provide the appropriate information /tools
  - Help a new NSP NOC to manage the LHCONE and to provide the appropriate information /tools
  - Help experiment to interact with LHCONE

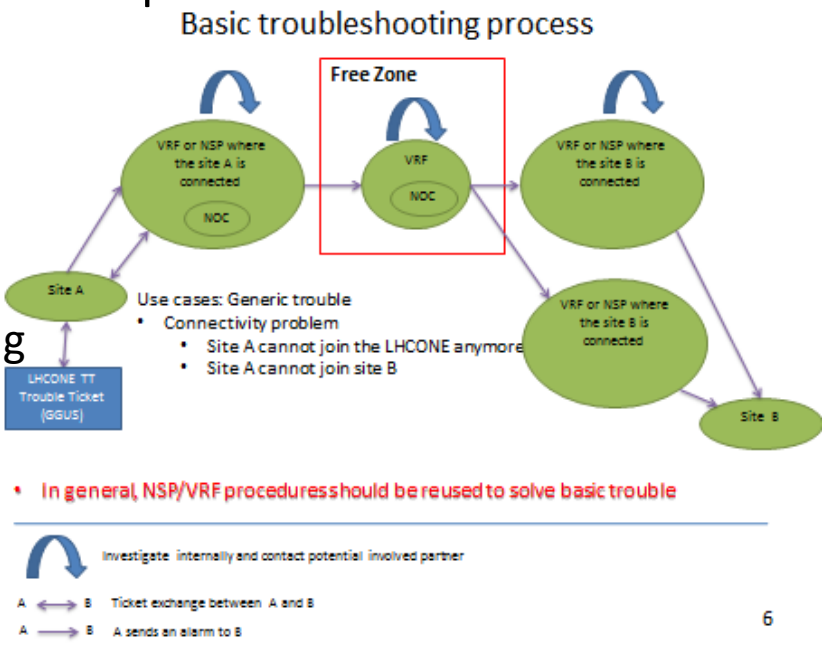
- Topics covered
  - Specify routing policy: protocol BGP / community / load balancing …
  - Specify security policy: firewall / filtering / science DMZ …?
  - Specify monitoring policy: tools, information and test available?
  - Site operation (connection, withdraw, maintenance …)
  - Network operation and troubleshooting process :
    - *Most of network entities (VRF/NSP) have their own operational procedure already defined*
    - basic trouble (connectivity issue, …), asymmetric traffic, performance
  - Information management: relevant, location, maintaining up-to-date, publication (who can access to what ?)

Approach

- Define actors, roles & responsibilities
  - Separate roles from implementation
  - Identify relationship of the actors
- Identify
  - Relevant use cases
  - Relevant information and their location
  - who is responsible to keep the information up to date
  - Tools that can help network operation
- Operational model manufacturing
  - An iterative approach

  → validation during LHCOPN/LHCONE meeting
  - Be careful as it is hard to have « agreement » from all entities





Operational Framework

- Not enough involvement of users and NSP in operational framework design

- In order to make progress, sub-groups have been proposed
  - Routing (NSP, Liaison sponsor)
    - Specify routing policy: protocol BGP / community / load balancing …
  - Security (Users)
    - Specify security policy: firewall / filtering / science DMZ …
  - Monitoring (Users/NSP)
    - Tool to be deployed both in sites en in NSP domain …

- Appeal for “author” or “reviewer” for the document → no answer

- These others topics have to be handled too
  - Site operation (connection, withdraw, maintenance …) (Users)
  - Network operation and troubleshooting process (NSP)
  - Information management (Users/NSP)
    - a reliable mechanism to broadcast information

LHCONE VRF operational handbook version 0.5

Contributor :

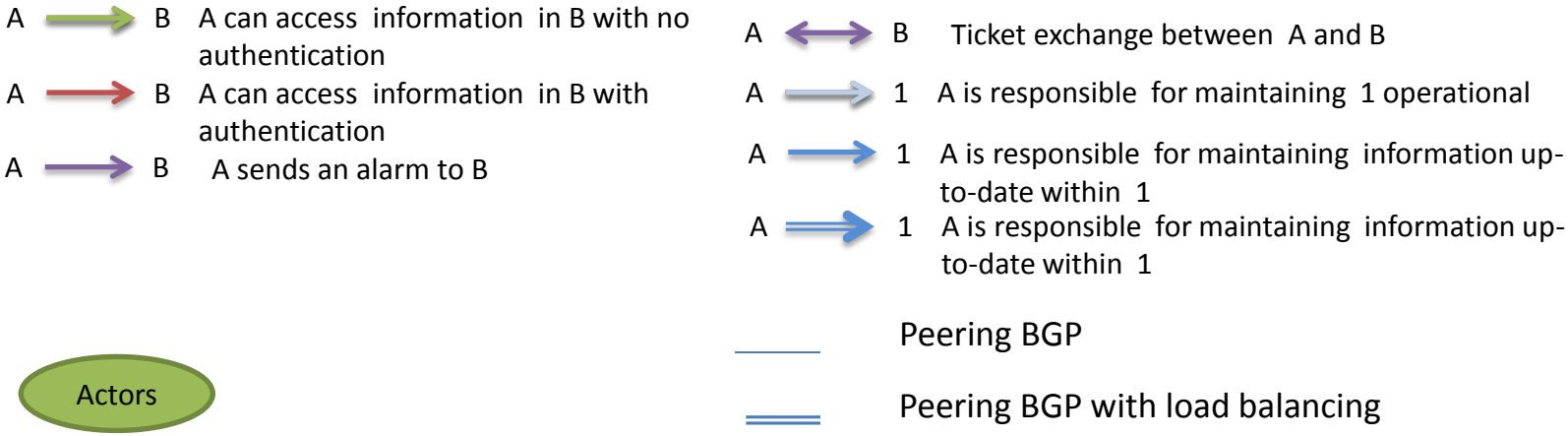
- Xavier Jeannin 2012/11/28
- ???

Inspired from G. cessieux work on LHCOPN operational model

Table of contents

- Drawing convention
- Actors
- Information management: relevant, location, maintaining up-to-date, publication (who can access to what ?)
- Site operation (connection, withdraw, maintenance …)
- Network operation and troubleshooting process :
  - basic trouble (connectivity issue, …)
  - asymmetric traffic, performance
  - maintenance process
- Routing policy (simple pointer)
- Security policy (simple pointer)
- Specify monitoring policy (simple pointer)

Drawing convention

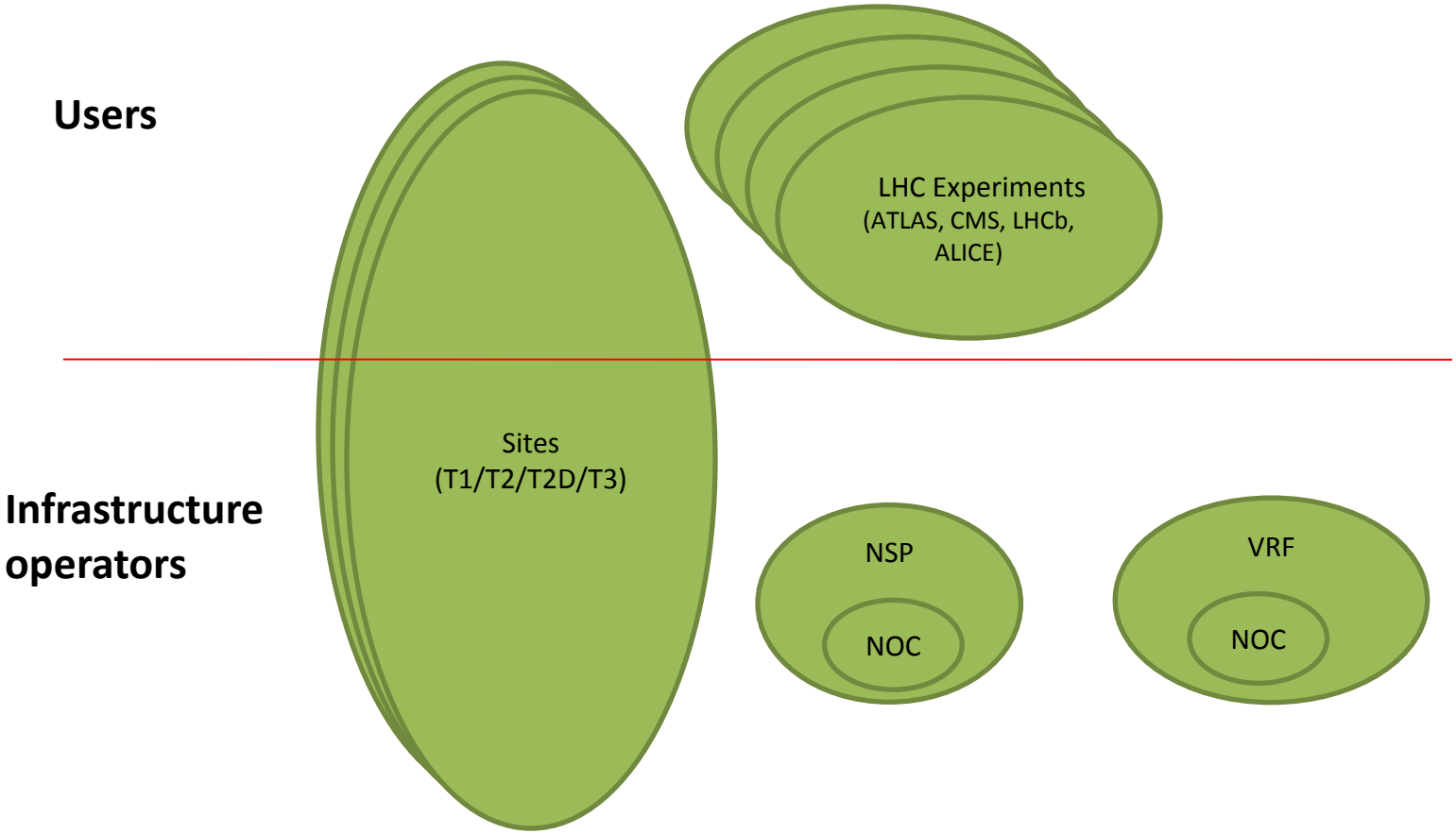


LHCONE Actors

- VRF
  - Provides a connection to other VRF for NSP's and sites/tiers
  - VRF is a specific NSP and VRF interconnection defines the "free zone"
  - NOC
- NSP
  - Provides a connection to sites/tiers
  - NOC

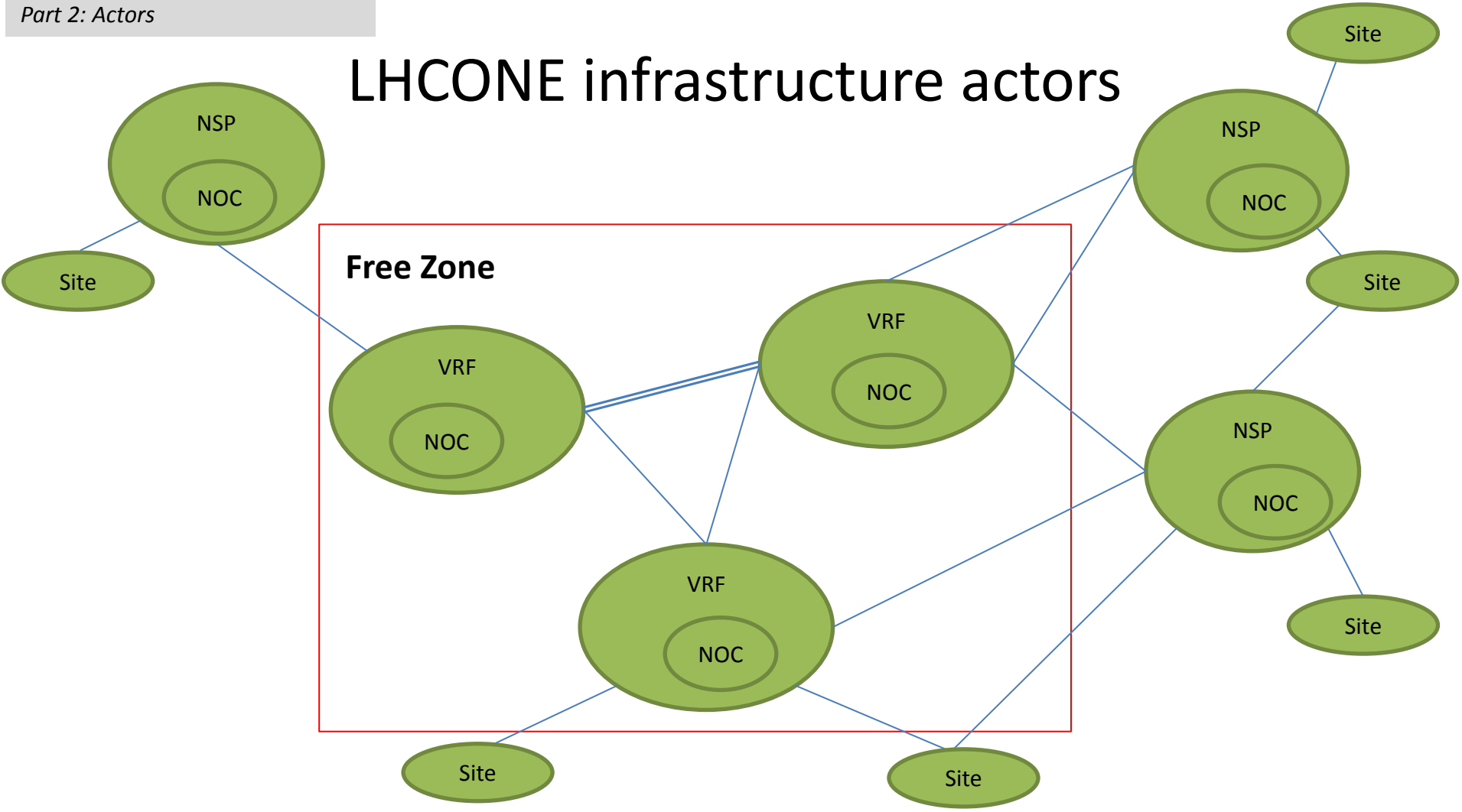
- Users
  - Sites/tiers
    - T1
    - T2/T3 (should T2D be clearly identify by others actors ?)
  - LHC experiments
    - Atlas, CMS, LHCb, Alice
    - Use the infrastructure
    - Define data flow model
    - Interact at operational level: down time (agenda), site ranking

LHCONE Actors



Actor

LHCONE infrastructure actors



Actors

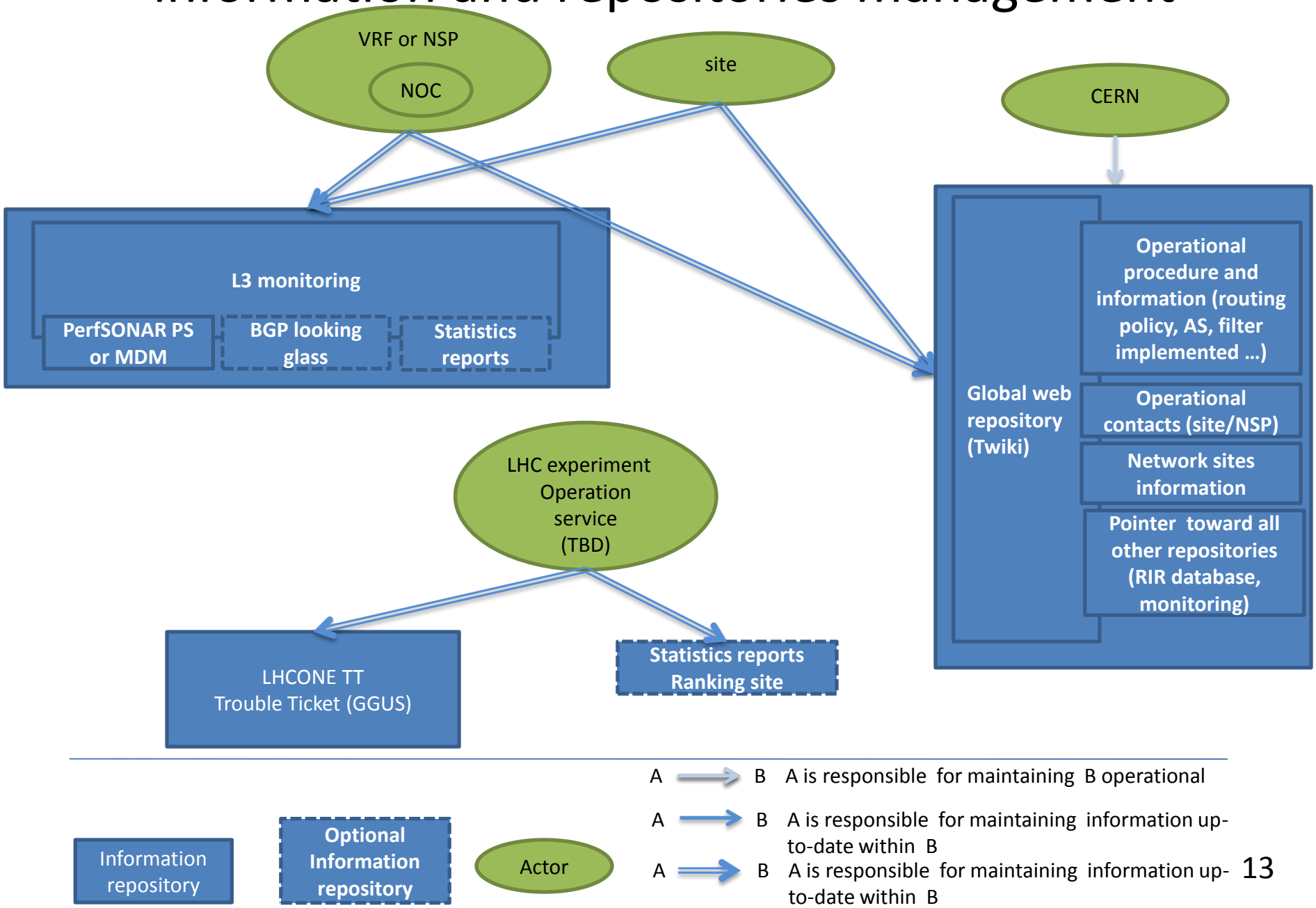
Peering BGP

Peering BGP with load balancing

Network operation information organization

- A unique information access point known by every one:
  - A central portal (wiki CERN) should allow to find where to find the information
    - Provide an exhaustive list of pointers to other repositories: for instance RIR database, monitoring tools, VRF NOC site …
    - Information could/should be distributed
  - Each information should be put under the responsibility of one identified actor
    - For instance: One site is responsible to maintain the list announced prefixes / a NSP is responsible to maintain the list sites connected to him.
  - Critical information should be mirrored ?
    - For instance, a mirror of the central portal could be implemented on other continent (America, Asia, Europe) ?

information and repositories management



List of information maintained up-to-date by NSP/VRF

Required | Optional

* Authentication required

Network Operators' Contact information

HTML link on twiki table

Operators	Served region	POPs	Contact information	VRF/NSP connected	Site connected	phone
CERNlight	Europe/any	Geneve (CH)	extip@cernSPAMNOT.ch	GEANT, …	CERN	
ESnet	US	MANLAN, WIX, …	trouble@esSPAMNOT.net	I2,	BNL,FNAL, SLAC, …	
Geant	Europe		Roberto.Sabatino@	I2, Esnet, CernLight, RedIRIS ..	?	
RedIRIS	Spain	Madrid?	?		PIC	

Monitoring information*

HTML link on twiki table

Operators	BWCTL	One Way Delay	BGP announce / received route	Looking glass *	Statistic
CERNlight	@server	@server	@server	@server	@server
Geant	@server	@server	@server	@server	@server

List of information maintained up-to-date by sites

Required | Optional

* Authentication required

Site Operators' Contact information

HTML link on twiki table

Site Name	Country	Tier	Technical Contact	VRF/NSP connected	Phone
AGLT2 (UM)	US	Tier-2D	Shawn McKee smckee@umichSPAMNOT.edu	?	
DESY-HH	DE	Tier-2D	Kars Ohrenberg Kars.Ohrenberg@ …de	DFN	

Sites network related information published

HTML link on twiki table

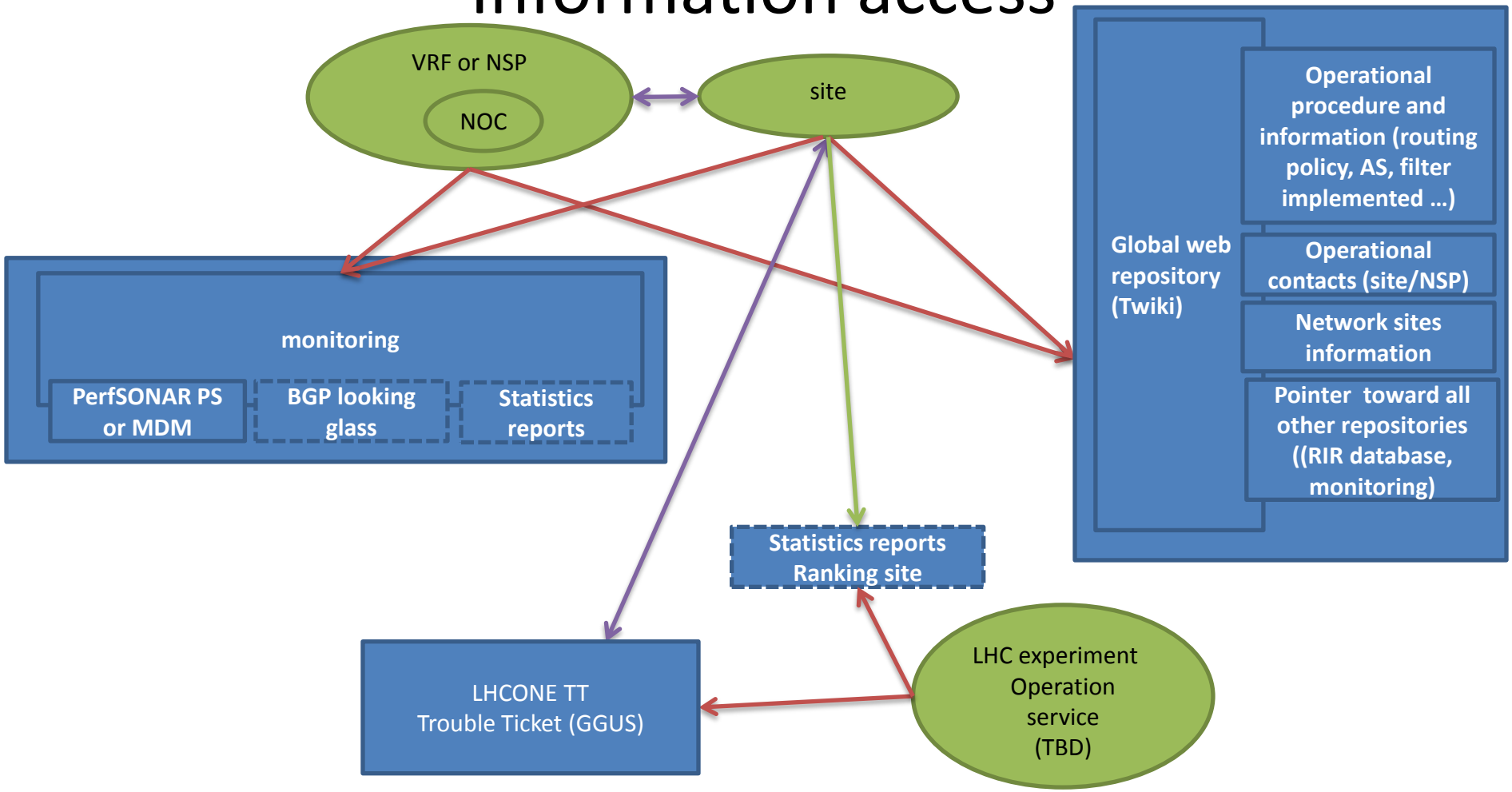
Site Name	NSP/VRF connected	Prefixes	MTU	firewall	comment
AGLT2 (UM)		published either on LHCONE or RIR Database			

Monitoring information *

HTML link on twiki table

Operators	BWCTL	One Way Delay	BGP announce / received route	Looking glass
DESY	@server	@server	Routes announced Routes received	@server
Geant	@server	@server	@server	@server

Information access



A → B A can access information in B with no authentication

A → B A can access information in B with authentication

A ↔ B Ticket exchange between A and B

Information repository

Optional Information repository

Actor

Information pending question

- An authorization framework is needed for the access to some information:
  - Looking glass
  - Monitoring tools
  - Data

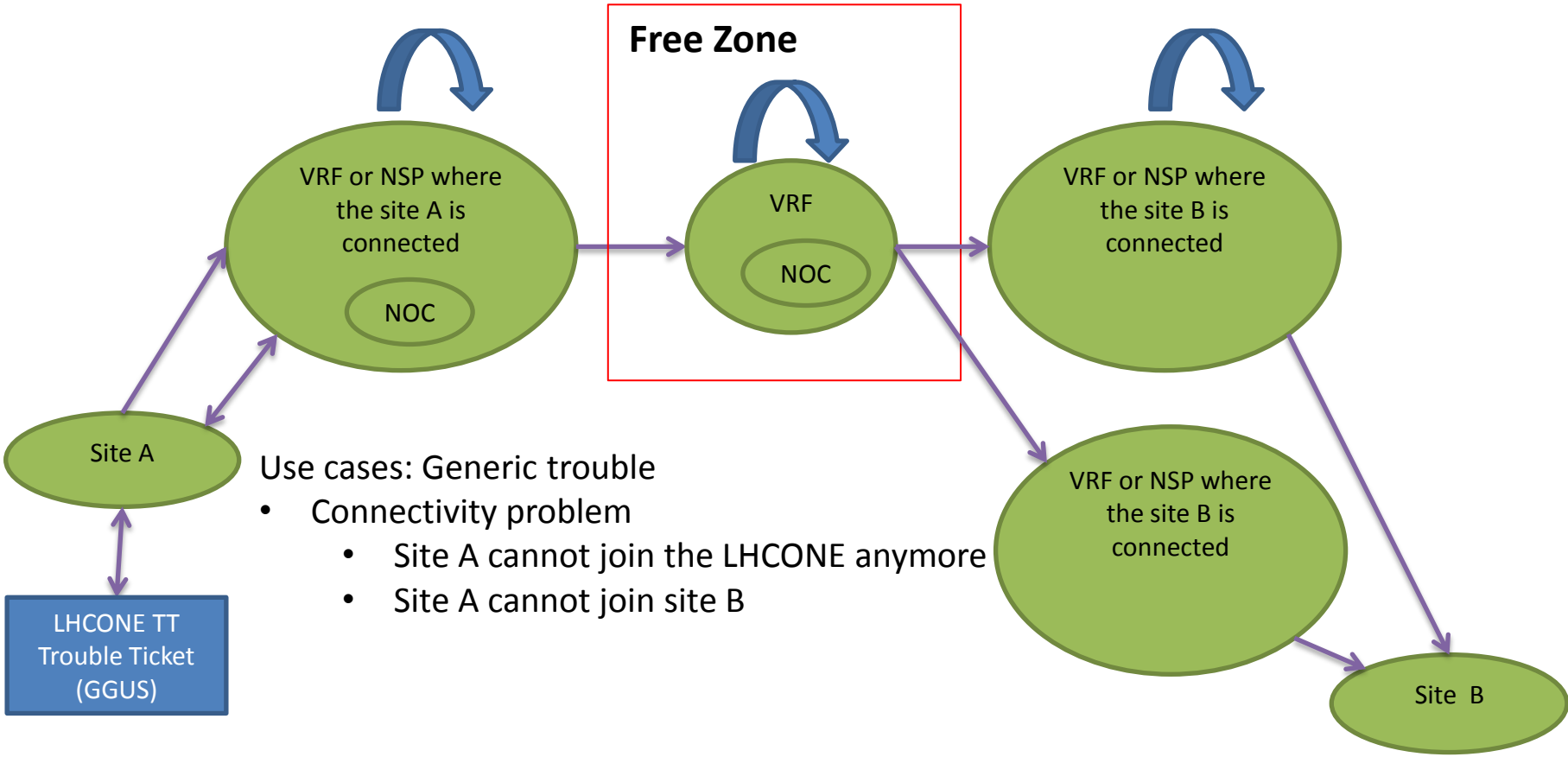
- Should prefix being published in RIR database or in the CERN twiki?
  - With RIR database, one can easily built automatic tools to check if prefixes sent by a site is appropriately declared
  - Twiki: easy in first place but less robust in long term

Information broadcast channels

- How to inform of a maintenance / a trouble?
  - Operational email list

- Which other tools should we set-up for more interactive activity?
  - Instant messenger
    - Skype, …
  - Possibility to set-up audio and video conference quickly
    - EVO, skype, ….
    - An always open conference on a MCU bridge or in EVO?

Basic troubleshooting process



Use cases: Generic trouble

- Connectivity problem
  - Site A cannot join the LHCONE anymore
  - Site A cannot join site B

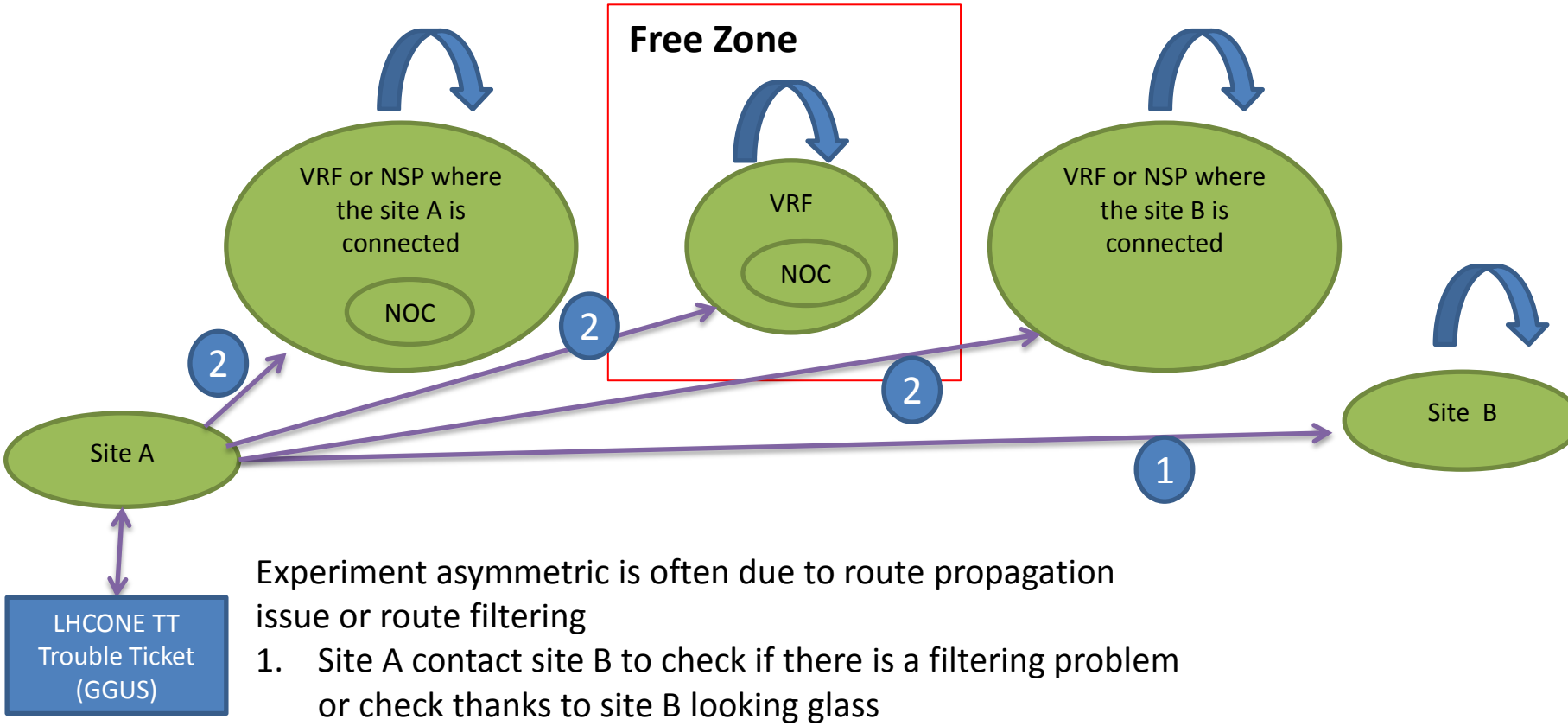
- In general, NSP/VRF procedures should be reused to solve basic trouble

Investigate internally and contact potential involved partner

Entity X ⟷ Entity Y Ticket exchange between entity X and Y

Entity X ⟶ Entity Y Entity X sends an alarm to Entity Y

Asymmetric troubleshooting process



Experiment asymmetric is often due to route propagation issue or route filtering

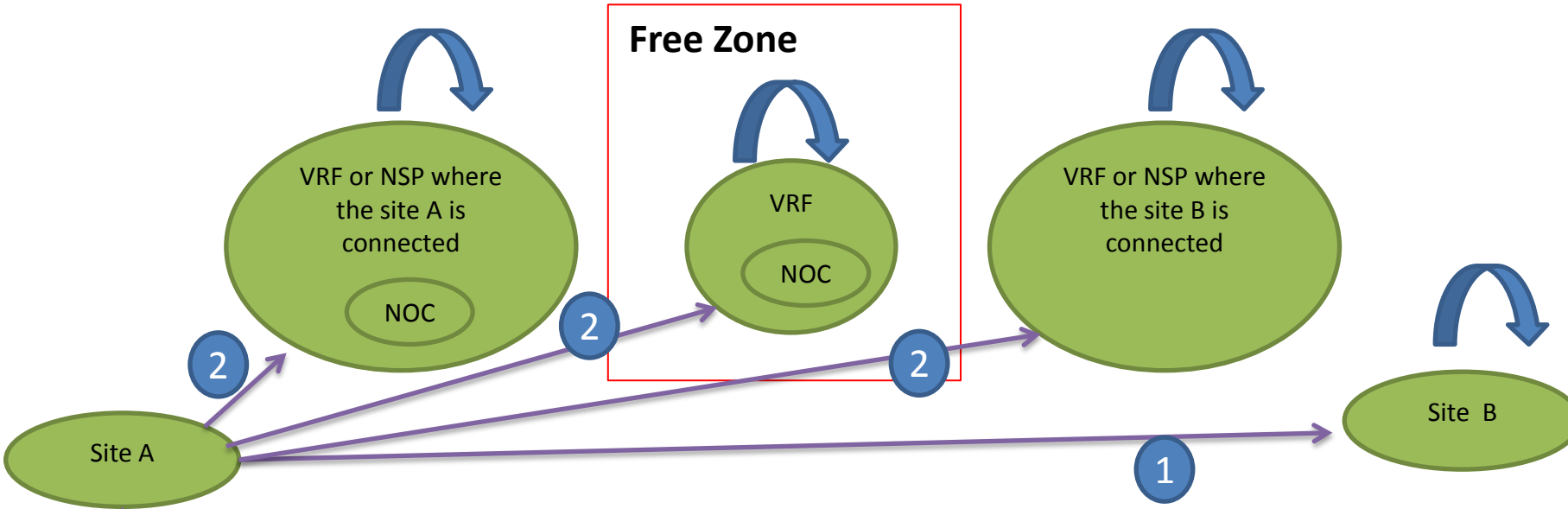
1. Site A contact site B to check if there is a filtering problem or check thanks to site B looking glass
2. Check route distribution along the path on NSP looking glass. If looking glass is not available site A will send an alarm to NSP that has to be checked.

Investigate internally and contact potential involved partner

Entity X ⟷ Entity Y Ticket exchange between entity X and Y

Entity X → Entity Y Entity X sends an alarm to Entity Y

Performance troubleshooting process



1. Site A make end to end test between site A and B thanks to remote monitoring tools : Perfsonar PS / MDM
2. Identify the faulty span
   A. Launch test between site A and every NSP crossed toward site B
   B. If the entity responsible of the faulty span is identified then contact the entity or contact suspected entities for investigation

---

Investigate internally and contact potential involved partner

Entity X ⟷ Entity Y Ticket exchange between entity X and Y

Entity X → Entity Y Entity X sends an alarm to Entity Y

Maintenance management

- Use case
  - A link will be have a maintenance
  - Routers will have a maintenance

Question

- List of entities to inform about this event? → broadcast channel
- How much time before an service interruption a NSP has to warn?

To be discussed with experiment and sites

Site operation

- connection, withdraw, maintenance
  - A new site connects the LHCONE
  - New prefixes announced
  - New link
  - Site maintenance ...

To be defined by sites if necessary

Routing policy

We can insert the of Routing policy group within operational handbook

General Rule

- BGP protocol must be used to connect LHCONE VRF
- Public ASN must be use ; Do not allow private AS ; VRF operator can announce the site address as belonging to the VRF's AS if necessary.
- Public IP addresses must be use …..

Or simply put a pointer to the relevant document

https://twiki.cern.ch/twiki/pub/LHCONE/LhcOneVRF/LHCONE_routing_policy-v2.1.pdf

Security policy

See Michael O'Connors presentation
Simply put a pointer to the relevant document provided by the sub-group

https://twiki.cern.ch/twiki/pub/LHCONE/LhcOneVRF/LHCONE_security_policy-v2.1.pdf

Monitoring policy

Simply put a pointer to the relevant document provided by the sub-group

https://twiki.cern.ch/twiki/pub/LHCONE/LhcOneVRF/LHCONE_monitoring_policy-v2.1.pdf

Next step

1. If there is an agreement on this approach
   - This document needed to be reviewed especially by users: experiment end site

1. Implement now the information repository (almost done on CERN Twiki)
2. Implement information broadcast channels
3. Network maintenance management well defined
4. Review and improve troubleshooting use case
5. Users must define site operation

6. Validation of the new specification during the next LHCOPN/LHCONE meeting

- Appeal to volunteers as a “author” or “reviewer” and contributor especially for
  - Routing policy
  - Site operation
  - Security policy