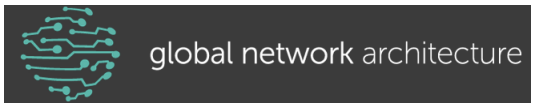

Document name:	Operations in the GNA-Compliant Network Infrastructure
Author(s):	Alexander van den Hil, Siju Mammen, Warrick Mitchell, and Migiel de Vos
Contributor(s):	GNA Technical Working Group
Date:	January 2017
Version:	v1.0

Operations in the GNA-Compliant Network Infrastructure

Table of Contents

Executive Summary

This document outlines a set of services and mechanisms that various NOCs agree follow to participate in the GNA. It defines how network providers that are compliant to the GNA are expected to communicate about operational activities such as data sharing, change management, and incident management.

Introduction

As a global network based on the Global Network Architecture (GNA) aspirations evolves, the NOCs of the participating organizations will collaborate to deliver the quality of service required.

Due to the heterogeneous, open, and inter-organizational character of the GNA, the bulk of traditional operations functions will remain distributed.

Distributed Global Operational Functions

Distributed Global Operational Functions are the functions that are organized globally and executed jointly though locally.

The following distributed global functions are required for the operation of a compliant infrastructure:

Function	Description
Change Management	Procedures and systems, either manual or automated, required for: - provisioning or decommissioning services; and - planned maintenance of services and/or infrastructure.
Capacity Management and Planning	Systems and processes enabling identification and anticipation of capacity or congestion issues and procedures to deal with these.
Incident Management	Ticketing systems, troubleshooting procedures, communication and escalation protocols required for managing unplanned incidents that may have an impact on performance.

Change Management

Link initialization

Typically, a link is procured by a contracting party, but operationally provided by a commercial supplier.

When a link is connected between two Global Research and Education Exchange Points (GXPs) the supplier will need to be provided with the contact information of the NOCs at each of the GXPs. This will be the responsibility of the contracting party for the circuit. When the contract is put in place the supplier must be provided with, and agree to use, all the contacts that the Contractual Owner provides.

There is a set of information that needs to be kept by every GXP for each circuit.

Information to be provided to the GXP by the Contractual Owner:

a) Circuit ID's from the carrier.
b) Contractual Owner contact information.
c) NOC contacts at both ends of the circuit.
d) Port information on the connecting ends.
e) Opt-in contact lists for notifications.

Information to be provided by the GXP to each participant:

a) Letter of Authorization

This information will be shared between both connecting NOCs. Any time this information is updated all participating parties will need to be notified.

For all the links and resources (such as the GXP) there will be SLAs. It is important that the contracting party documents and advises the other GNA participant (GXP or NREN) of the SLA which the contracting party has agreed to with the supplier.

Each GXP NOC should be able to request the state, as noted at both ends, of any circuit landing on that GXP, to confirm that any changes have been completed.

Service Change

Provisioning, modifying and decommissioning.
Documentation on procedures for provisioning services will be made available. This does not need to be different from standard participant provisioning methods. Useful information would include:

- Standard provision request addresses
- Standard provisioning times
- Service description: describes the services that can be requested and the required parameters, e.g., bandwidth, VLAN tags, MTU, etc.
- A link to the AUP documentation.
- Any other information required to provision a service

Maintenance Management

For all maintenance issues the participating NOCs will need to agree on requirements. These would include:

- Notification of standard maintenance windows for any scheduled event.
- General agreement on preferred windows for maintenance need to be documented.
    - Where maintenance windows are scheduled which impact services over multiple time zones, a degree of flexibility in scheduling the maintenance window is desirable.
- Impact assessments for any planned maintenance need to be prepared and made available.

There will also be times where emergency maintenance will be required. There needs to be a clear understanding of what situations justify emergency maintenance.

- Thresholds for soft failures need to be documented.
- This may in part depend on the user requirements in any given case.
- Some minimum levels should be set, with the understanding that some lesser levels may generate a maintenance.

In all cases, planned or emergency, notification will be sent to all NOCs so they can proceed to notify their user base.

When GXP is going to perform scheduled maintenance, the GXP NOC will schedule the maintenance, notifying the other NOC, the supplier and the contractual owners of the link. It is the responsibility of each NOC to notify their own clients of the scheduled maintenance.

When maintenance is carried out and completed all parties receive a notification that the action has finished.

When the supplier of the link is performing the maintenance they will schedule and notify both NOCs associated with the link. The NOCs will notify their users with a local ticket ID. After the maintenance, has been completed, the supplier of the link is to notify the NOCs that all work was successful and/or what changes did/did not take place. Information on standard provider windows for maintenance events should be made available to each NOC. This process could also be used for other connectors to the open exchanges.

Capacity Management and Planning

Identification of ongoing usage will be carried out and anticipated requirements will be monitored and assessed.

Incident Management

Service Disruption Reported to, or Identified by a NOC

Example: An end user reports a problem to their local NOC with a service that uses the GNA links for connectivity. This might for example be a user reporting perceived substandard end-to-end performance of a data transfer.

In any multi-domain system, there are multiple points where a problem can occur and not every NOC will have access to every location for testing. In order for incidents to be successfully managed and resolved, all test points and related information must be shared and available to every NOC.

A service disruption report is generally directed to the NOC of the organization that provides services to that user. An example is a reported problem between a site connected to Internet2 in the USA and a site connected to HEAnet in Ireland. A user at one of the two end nodes, in the USA or in Ireland, will report this to the NOC of Internet2 or HEAnet, respectively.

When an incident occurs, the following process should be followed:

1) The originating NOC opens a ticket.
    a. If the initial investigation shows that the issue is a local problem, then the originating NOC will fix the issue and update and close the ticket.
2) A Global ID and alias is assigned to the ticket.
3) The originating NOC contacts their upstream or parallel NOC with the ticket.
    a. That upstream NOC also opens a ticket for the issue.
    b. This process will continue as needed in order to involve all of the relevant NOCs.
4) The NOCs will jointly develop a test plan to isolate the problem, with the Originating NOC coordinating the plan.
5) Once the problem is understood and resolved, all tickets regarding this problem will be closed.

In these cases, the participating NOCs will make sure that any issues around fault isolation do not hinder solving the problems. The most efficient way around this is to have sufficient test points in place to minimize the danger of incorrect diagnosis.

It is possible that a service level report turns out to be an integrity issue on the circuit itself in which case the procedure described above will be initiated. Tickets related to the service level should remain open until the circuit issues are resolved and there is verification that the service is operating normally once again.

As a part of the monitoring service, performance measurement tests should occur at regular intervals. Where possible these should be done at the service level. These measurements should be made available for use as a baseline for determining if a reported issue is within the normal service parameters or not between participants.

Link Disruption Identified by a NOC

Disruption of a carrier service identified by a NOC will trigger this procedure to find out if this is a partner problem, carrier problem, or something else.

The NOC that first notices a performance impacting issue will take ownership of the incident and contact the NOC on the other side. If one of them is able to identify the problem within their own domain it is to be resolved by that entity, and the fix or maintenance required for resolving the issue is to be communicated back to the other NOC.

In case both NOCs cannot find problems in their own domain, then the supplier is contacted by the problem-owning NOC. The supplier checks their link and reports back. If the supplier is able to resolve the problem immediately, it may do so and report back to the requesting NOC.

The NOCs at either end of a circuit will need to share information on the equipment types where the circuit lands. Tools for testing for circuit integrity should be shared between the participating NOCs.

When each domain reports that no issues are seen, then a more detailed investigation is started, or the problem is escalated.

There may also be situations where internal (internal to the GNA) escalation needs to occur as well. In the RACI matrix there should be sufficient information to allow this to happen. Should a GNA participant wish to provide additional details for escalation beyond the respective NOCs, then they can do so, however they are not required to.