Technical Assistance to RNRA regarding LAIS Remote Connectivity and recommendations regarding network connectivity

David Sibley

April 2015
This report has been produced by Land Registry for Evidence on Demand with the assistance of the UK Department for International Development (DFID) contracted through the Climate, Environment, Infrastructure and Livelihoods Professional Evidence and Applied Knowledge Services (CEIL PEAKS) programme, jointly managed by DAI (which incorporates HTSPE Limited) and IMC Worldwide Limited.

The views expressed in the report are entirely those of the author and do not necessarily represent DFID’s own views or policies, or those of Evidence on Demand. Comments and discussion on items related to content and opinion should be addressed to the author, via enquiries@evidenceondemand.org

Your feedback helps us ensure the quality and usefulness of all knowledge products. Please email enquiries@evidenceondemand.org and let us know whether or not you have found this material useful; in what ways it has helped build your knowledge base and informed your work; or how it could be improved.

Disclaimer

This report was prepared by an employee of Land Registry with no prior involvement in the systems and migrations reviewed. The views and opinions expressed in the report do not necessarily correspond with the views of the Department for International Development (DFID) or the Rwanda Natural Resources Authority (RNRA).

DOI:http://dx.doi.org/10.12774/eod_cr.april2015.sibleyd

First published April 2015
© CROWN COPYRIGHT
# Contents

Abbreviations and Terminology ........................................................................................................ ii
Executive Summary .......................................................................................................................... iii
Summary of recommendations ......................................................................................................... v

SECTION 1 ......................................................................................................................................... 1
Introduction ....................................................................................................................................... 1
   1.1 Distribution List ......................................................................................................................... 1

SECTION 2 ......................................................................................................................................... 2
Assistance on LAISv2 remote connectivity ....................................................................................... 2
   2.1 High-level assessment of network infrastructure ................................................................. 2
   2.2 High level assessment of client-server interactions ............................................................. 3
   2.3 Actions taken to support LAIS connectivity ........................................................................... 4

SECTION 3 ......................................................................................................................................... 6
Recommendations on further improvement ..................................................................................... 6
   3.1 Improving security of data in transit ....................................................................................... 6
   3.2 Physical layout of network can be improved ....................................................................... 7
   3.3 Logical layout of network can be improved ....................................................................... 7
   3.4 Centralise policy enforcement ............................................................................................... 8
   3.5 Implement network monitoring / management ................................................................... 8

SECTION 4 ......................................................................................................................................... 10
Implementation of recommendations ............................................................................................... 10
   4.1 Securing Oracle Glassfish ..................................................................................................... 10
   4.2 Securing PostgreSQL ............................................................................................................ 10
   4.3 Restructuring physical layout of network ............................................................................. 10
   4.4 Restructuring logical layout of network .............................................................................. 11
   4.5 Centralising policy enforcement ............................................................................................ 12
   4.6 Adopt naming convention ..................................................................................................... 12
   4.7 Implement network monitoring solution ............................................................................. 13
   4.8 Define Acceptable Usage Policy for staff internet use ..................................................... 13

List of Appendices

Appendix A - Technical references ............................................................................................... 16
Appendix B Skills/Costs of recommendations ............................................................................... 17
### Abbreviations and Terminology

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUP</td>
<td>Acceptable Usage Policy</td>
</tr>
<tr>
<td>BSC Ltd</td>
<td>Broadband Systems Corporation Ltd</td>
</tr>
<tr>
<td>DfID</td>
<td>Department for International Development</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSEC</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>ISR</td>
<td>Integrated Services Router</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LR</td>
<td>Land Registry</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi-protocol label switching</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>Rapid PVST+</td>
<td>Rapid Per-VLAN Rapid Spanning Tree</td>
</tr>
<tr>
<td>RNRA</td>
<td>Rwandan Natural Resources Agency</td>
</tr>
<tr>
<td>SOHO</td>
<td>Small Office / Home Office</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
</tbody>
</table>
Executive Summary

This report describes the details, findings and recommendations of an assignment to support RNRA network administrators in addressing issues related to LAIS 2 remote connectivity and advise on further improvement.

Network connectivity is satisfactory

Network traffic from remotely located systems is satisfactorily transmitted from geographically dispersed sites to central servers. Of the sites observed, quality of data throughput was acceptable although bandwidth is understandably limited. There is a need to establish service level agreements with the Internet Service Provider to ensure issues with ISP-supplied equipment are solved in a timely fashion.

Security of data in transit must be improved

Network traffic from remotely located systems is not encrypted by RNRA's Internet Service Provider to prevent traffic being read, or altered, in transit. Further to this the LAIS 2 application traffic is also not encrypted. This means that any traffic intercepted in transit can be easily read or potentially altered. This should be remediated as soon as possible, both by RNRA's Internet Service Provider and by RNRA IT staff.

Dispersed points of policy enforcement present challenges

Critical infrastructure servers are protected with host-based firewalls. There is some evidence of policy control, but half of the estate appears to be managed on a per-device basis, while the remainder is managed with a one-size-fits-all policy. This has been identified as a root cause of the RNRA difficulties in testing the LAIS 2 remote application. Similarly, while stateless filtering of network traffic is possible on the equipment available, the logical structure of the network renders this unlikely until precursory changes are made.

Physical layout of network can be improved

The layout of the network infrastructure at the Kigali office has a number of opportunities for improvement. Changing the layout to follow a two-layer hierarchical model, utilising aggregated logical links between equipment, utilising available equipment to ensure a loop-free topology, and reducing the end-to-diameter of the network are goals that can be achieved with existing equipment. This will then improve the performance and resilience of the network.

Logical layout of network can be improved

The logical structure of the RNRA network offers opportunities for improvement. At present all hosts and servers share the same broadcast domain. Separation of devices into independent subnets and VLANs should be a necessary precursor to offering services to the general public in a secure manner. Separation of devices will also improve the security of the RNRA's servers.
Network monitoring is not present

There is no evidence of any monitoring of services or infrastructure devices taking place. This should be remediated. The implementation of a centrally located monitoring solution such as Cacti, or a Software-as-a-Service solution such as Monitis or Uptrends Infra would give RNRA administrators access to rich information regarding the health and performance of the RNRA network.
Summary of recommendations

The recommendations, as documented in this report, are summarized below. They are presented with relation to RNRA aspirations to present services to members of the general public. Relative priority/urgency has been presented with a simplified MoSCoW grouping: “Must Have” and “Could Have”.

Must Have:
- Utilise TLS to secure client-server interactions to ensure end-to-end encryption of traffic.
- Ensure all network devices are managed/manageable via SSH.
- Conduct restructure of logical network, segregating servers from users.
- Conduct restructure of physical network to improve resilience and scalability.
- Formalise working practices with Internet Service Provider, establishing a service level agreement (SLA) with expectations of service availability and support provision.

Should Have:
- Implement network monitoring solution (such as Cacti or Solarwinds Orion).
- Request encryption of network traffic when traversing ISP-owned infrastructure.
- An acceptable use policy (AUP) should be established for internet use, with infrastructure equipment configured in support of this policy.
- Documentation of service flows should be completed and maintained over the lifetime of the relevant service (EG, LAISv2, CORS, Flexicadastre).
- Up-to-date network documentation should be created and maintained.
- Realign cabling standards; network cabling should be organised to make use of cabinet cable runs, ensuring ease of access to equipment and improving airflow for cooling.
- Equipment should be installed in racks with rack-mounting kits.
- Equipment in racks should be racked to allow access to console ports
- RNRA should consider improving their use of Kaspersky Endpoint Security and its management via Kaspersky Security Centre to centrally manage hosts.
- Consider non-Cisco networking hardware to reduce cost of future procurement exercises, ensuring that alternatives meet business requirements.

Further assistance has been provided on a selected part of these recommendations, as documented in Section 4, Implementation of Recommendations.
SECTION 1

Introduction

In March 2015, Land Registry was approached by the Department for International Development (DfID) on behalf of the Rwandan National Resources Agency Lands & Mapping Division (RNRA) to provide technical expertise relating to their launch of the Land Administration Information System Version 2 (LAISv2).

The LAISv2 application was launched on Monday 23rd of March and improved the ability of RNRA Geospatial Information System (GIS) staff to make changes (splits, joins) to spatial data representing existing parcels of land.

To facilitate the successful launch of this application Land Registry provided two technical experts to the RNRA with the following objectives:

1. To support RNRA LAIS developer and Local ICT advisor in implementing and testing migration scripts.
2. To support RNRA network administrators in addressing issues related with LAIS 2 remote connectivity and advise on further improvement.
3. To advise on the creation of LAIS users active directory accounts and on its implementation.

It became clear in the early stages of this engagement that although ten working days had been allocated for these three objectives the relative weighting of time allotted to each objective was not equal. This report concerns itself with the second objective. As a result this report is of a notably technical nature. Considering the mixed audience of interested readers (DfID Rwanda staff, RNRA management, RNRA technical personnel) technical details will be confined where possible to Section 4, or separated into appendixes.

1.1 Distribution List

<table>
<thead>
<tr>
<th>Land Registry</th>
<th>DfID Rwanda</th>
<th>RNRA Management</th>
<th>RNRA Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kevin Rowley</td>
<td>Sarah Love</td>
<td>Didier G. Sagashya</td>
<td>Jean de Dieu Uwumukiza</td>
</tr>
<tr>
<td>Emma Vincent</td>
<td>Justus Turyatembe</td>
<td>Rhona Nkayulama</td>
<td>Jacqueline Uwimbabazi</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Land Registry Delivery Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deputy Director General</td>
<td>RNRA Network Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Department of Lands and Mapping</td>
<td>RNRA Active Directory Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ICT Liaison</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Land Registry Head of Global Business Development</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DFID Economic/Climate Change &amp; Low Carbon Development Adviser</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DFID Project Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Deputy Director General</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Department of Lands and Mapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Project Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ICT Liaison</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following sections describe assistance rendered during the period from March 16th to March 20th inclusive. The original scope anticipated that this assistance would cover connectivity from RNRA GIS processing officers at remote offices to network-connected servers at the RNRA Lands & Mapping Division office in central Kigali.

Rendering this assistance required a high-level assessment of the network infrastructure over which remote connectivity was to be established. Further to this an assessment of detailed client-to-server interactions was also required. The findings of this assessment were collated across the duration of the engagement and are presented here.

2.1 High-level assessment of network infrastructure

The network infrastructure connecting remote offices to servers located in Kigali falls into two areas of responsibility. WAN connectivity is the responsibility of the RNRA’s chosen ISP, BSC Ltd. BSC Ltd.’s responsibility covers the transit of data across networking infrastructure wholly owned by BSC Ltd, and on equipment co-located on premises occupied by RNRA staff. For the purposes of this report the demarcation point at which BSC Ltd holds responsibility for the transit of data is at the switchport interface into which a cable is connected from an RNRA device. The definition of demarcation points should be defined in an SLA if an agreement has not already been reached. LAN connectivity is the responsibility of the RNRA and its employees, covering the transit of data across networking infrastructure wholly owned by the RNRA, and on equipment located on premises occupied by RNRA staff. For the purposes of this report the responsibility of RNRA staff and equipment for the transit of data ends at the switchport interfaces of BSC Ltd equipment. Network cables connecting RNRA equipment to BSC Ltd equipment are considered within the RNRA’s area of responsibility.

BSC Ltd utilise a diverse estate of networking equipment to provide service to the RNRA. BSC Ltd equipment located on RNRA premises includes both Cisco ISR 891 SOHO routers and Cisco Catalyst 3560 8-port Layer 3 switches. This equipment can be considered appropriate for the needs of the RNRA, and comment about the selection of equipment or configuration of such remains outside the scope of this report.

RNRA likewise utilise a diverse estate of networking equipment relative to this report. At remote sites this includes a range of SOHO equipment such as Linksys WRT45G routers to provide WLAN access, with D-Link 1024D and 1026G Ethernet switches to provide LAN access. Cyberoam 50ai hardware firewalls are located at some remote offices to secure connectivity to the internet but for the purposes of this report they are considered outside of scope. At the RNRA Kigali office equipment relative to this report consists of Cisco hardware: a Cisco ISR 1941 and Cisco Catalyst 3750G L3 switches.

Network traffic from RNRA remote offices is securely transmitted to the RNRA central office over MPLS VPN tunnels. This networking protocol allows the transmission of data in such a fashion as to assure confidentiality, integrity, and authentication. Standards for encryption
and secure hashing should be defined in RNRA's SLA with BSC Ltd. At present this capability is not being utilised.

Both BSC Ltd.’s co-located networking equipment and RNRA networking equipment appears minimally configured. Recommendations will later be made in Chapter 4 to improve this situation with regard to RNRA networking equipment.

Key observations are as follows:

- Reliance on static routing by both parties.
- Confusion over usage and purpose of VLAN segregation.
- Little / no evidence of packet-filtering access-lists to control traffic.
- Confusion over routing between remote office network addressing and central office network addressing.
- Physical layout of central office networking equipment does not provide resilience / fault tolerance.
- Good relationship between RNRA IT administrators and BSC Ltd support staff.
- No evidence of network traffic encryption taking place.

2.2 High level assessment of client-server interactions

RNRA GIS processing staff interact with LAISv2 using Microsoft Windows-based applications. The primary application is Esri ArcGIS. This application is used to administer information on registered plots of land, leveraging a ‘dockable window’ that represents a core requirement of the LAISv2 rollout. This application communicates with four centrally-located servers.

Server one is the LAIS Admin textual server. This server holds information on parcels, rights, and rights holders. This server listens to client requests on a proxy port for standard HTTP traffic.

Server two is the GIS PostgreSQL database server. This server holds geospatial information and listens to client requests on standard SQL ports.

Server three is the Active Directory server. This server holds client credentials for GIS processing staff and uses pass-through authentication to enable functionality of the dockable window in ArcGIS. Traffic to this server goes over a number of ports related to Active Directory logon and Active Directory Web Services.

Server four is the ArcGIS Licensing server. This server holds software license 'tokens' for the ArcGIS applications installed at remote sites and utilised by GIS processing staff. This server listens for licensing calls from remote workstations.

Server four also contains the Kaspersky Security Manager software. Although this software does not relate directly to LAISv2 its configuration was revealed to be the source of some difficulties in testing of the LAISv2 dockable window component.

No documented service flows were available at the commencement of this engagement. Documentation of service flows as a collaborative act between RNRA developers and RNRA network administrators should take place during the development of services to expedite implementation and troubleshooting.

At the commencement of the engagement the ArcGIS and LAIS Admin servers had been configured with secondary network cards in the 172.20.19.0/24 range. These network cards had been provisioned to allow traffic in from remote office users. Configuration to allow the
intended of use of these network cards had not been fully completed: specifically routing
table entries had not been made on these servers to utilise the 172.20.19.0/24 interfaces in
order to return traffic to remote users. Without these routes being present asymmetric traffic
routing took place. While this would not have halted the successful deployment of LAISv2 it
made troubleshooting more complicated for RNRA developers and network administrators.

Servers two, three, and four were configured with Kaspersky Endpoint Security 10, a host-
based antivirus and firewall application. This software is relevant to the actions taken in
support of the LAISv2 rollout as it was discovered that the firewall component was interfering
with the flow of traffic from remote office clients to central office servers.

Key observations are as follows:

- No service flow documentation was available to assist in troubleshooting.
- Confusion over requirement for dual network cards in servers.
- No traffic encryption configured for client-server flows.
- Strong relationship between IT administrators and software developers.
- Limited understanding of installed firewall software and its implications for LAISv2 service.

2.3 Actions taken to support LAIS connectivity

In order to address the issues with remote connectivity to LAISv2 the following actions were
undertaken in concert with RNRA IT staff. These actions were underpinned by an iterative
process of troubleshooting following a top-down approach\(^1\). This troubleshooting occurred
alongside the high-level assessment of the network, and of the client-server interactions.

The first action undertaken resolved an issue with bi-directional traffic from remote office
clients to the central LAIS and GIS servers. It was determined that although these servers
had secondary network cards with addresses in the 172.16.19.0/24 network they lacked
sufficient configuration to make correct use of these network cards to respond to remote
clients. Amending these servers by adding routing table entries to use these network cards
for return traffic to the remote offices resolved this initial issue.

The secondary network cards had been installed under the belief that uninterrupted
communication with remote offices required network cards in the same overall network.
Removing these cards and working with the LAISv2 developers to point application requests
at the 10.10.8.0/21 addresses of the central servers provided a more coherent routing and
addressing strategy.

Remote offices were proven capable of reaching centrally located servers on their primary
network cards using standard network troubleshooting tools as follows:

- ICMP ping echo request / echo response to establish reachability
- Traceroute application using incrementing TTL values to establish network devices in
  patch between source and destination.

These actions ensured that routing between remote offices and central servers now takes
place on the Cisco ISR 1941 located at RNRA central office in Kigali.

At the conclusion of my involvement these network cards were still installed in the relevant
servers but were deactivated and no longer configured for use.

\(^1\) http://www.ciscopress.com/articles/article.asp?p=2273070&seqNum=2
Once reachability had been confirmed between remote and central offices further problems were identified. Remote office users were unable to connect to central Active Directory and GIS license servers. Using network packet capture and analysis tools it was determined that traffic was reaching the Active Directory and ArcGIS license servers but being dropped on arrival. This was determined to be due to the firewall rules in place on the Kaspersky Endpoint Security firewall component present on both servers.

Through further packet capture and analysis the required flows for the Active Directory server were defined and permitted through the firewall. The same methodology was followed for the GIS license server along with an investigation into vendor-supplied documentation for ArcGIS License Manager to determine the required firewall rules.

These actions permitted remote office GIS Processing staff to sign-on to their computers via RNRA Active Directory accounts. This was defined as a key dependency of the LAISv2 application. Without the ability to sign on to RNRA Active Directory the dockable window component of LAISv2 could not function.

These actions permitted remote office GIS Processing staff to utilise the ArcGIS application that leverages RNRA’s dockable window component, back-end GIS and LAIS data, and perform tasks related to administration of land. Without access to the ArcGIS license server this software could not be remotely activated, requiring the presence of a hardware key to be maintained at each remote office.

At the conclusion of the engagement RNRA IT staff had been exposed to troubleshooting methodology and shown how to apply these methods to investigate problems with routing of network traffic. RNRA IT staff had also been exposed to troubleshooting techniques relevant to the firewall software installed on central Windows servers. Remote office GIS Processing staff had been engaged to trial the application with a successful outcome.
SECTION 3

Recommendations on further improvement

The following sections describe identified areas where the RNRA network can be improved. The executive summary of this report contains the most pressing concerns where the RNRA network should be improved. This section will expand upon them, laying out the justification for each. A selection of items from the simplified MoSCow grouping ‘Should Have’ list are also included and will be described in further detail.

3.1 Improving security of data in transit

At present there is no sign of any encryption taking place to prevent electronic eavesdropping, unauthorised data alteration, or assurance of participants involved in transferring data. Data encryption can and should take place on multiple levels.

There are two layers of data encryption that can be implemented to secure RNRA data in transit. The first layer relates application traffic between remote office GIS Processing staff and central office application servers.

The LAIS server runs Oracle Glassfish to serve content to remote office users. This application, by default, uses HTTP. This protocol is used to transfer web-based content across the internet in an insecure manner. Oracle Glassfish is capable of using the secure version of HTTP, HTTPS. This protocol uses TLS to ensure that electronic eavesdropping and data alteration cannot take place. Should HTTPS traffic be intercepted it is effectively unreadable without an attacker having access to the TLS keys stored on the relevant HTTPS server. Further to this should encrypted traffic be intercepted it cannot then be altered and transmitted to the LAIS server. Unencrypted traffic does not offer this protection against fraudulent alteration of data in transit.

The GIS server runs PostgreSQL as the RNRA database of choice. The PostgreSQL database listens to requests from remote office users and responds to them in an insecure manner by default. PostgreSQL has support for TLS to ensure that electronic eavesdropping and data alteration cannot take place. In the same manner as HTTPS, configuring and utilising this will ensure that should traffic be intercepted it is effectively unreadable and unalterable to an attacker.

Both of these improvements will require the creation or purchase of secure certificates, and the installation of these certificates on the GIS and LAIS servers. RNRA developers may have to assess the configuration of the LAISv2 application to direct traffic to servers on correct ports for secure connectivity.

The second layer of data encryption relates to network traffic belonging to RNRA crossing infrastructure owned by BSC Ltd. This distinction between RNRA and BSC Ltd is important. RNRA equipment at remote sites does not support the establishment or termination of IPSEC VPN tunnels. This can only be provided by equipment managed by BSC Ltd.

BSC Ltd equipment handles the transfer of RNRA network traffic using a transfer protocol called MPLS. By default no encryption is applied to traffic being transferred over MPLS. It is possible to configure MPLS to use a suite of protocols called IPSEC to ensure that network
traffic is encrypted to avoid eavesdropping, authenticated to prevent unauthorised endpoints from communicating, and securely signed to prevent unauthorised alteration of traffic.

BSC Ltd must be trusted to a certain extent to carry RNRA network traffic between remote offices and the RNRA central office. Requesting that BSC Ltd configure IPSEC tunnels to encrypt RNRA network traffic allows RNRA the confidence that even if network traffic were to be redirected, by accident or maliciously, there would be no exposure of sensitive data.

### 3.2 Physical layout of network can be improved

This recommendation covers only the RNRA central office in Kigali. The layout of the RNRA network at present places IT operations using equipment sited at the Kigali office at risk. Further to this the layout at the Kigali office offers limited opportunities for expansion without exacerbating the risk of disruption. Restructuring the physical layout of the network now will allow RNRA to reduce the risk of serious disruption as well as provide a platform for future expansion.

Using existing equipment the network can be reconfigured along the lines of a two-layer hierarchical model. The specifics of this will be discussed in Section 4. A hierarchical model divides the network into a 'core' layer of fast, feature-rich switches, and an 'access' layer to provide connectivity to hosts. By correctly connecting 'access' switches into the 'core' switches the network can survive the loss of a core switch without major interruption to the network as a whole.

At present the layout of the network means that should either of the two Cisco Catalyst 3750G switches suffer a failure then a significant proportion of connected switches will also be affected, potentially leading to a situation where all internet connectivity is lost from the Kigali central office.

Restructuring the physical layout of the network should also be accompanied by the implementation of configuration for Rapid PVST+. At present the addition of an extra switch to the network will cause a temporary outage to service for all users of the network. Correctly implementing Rapid PVST+ will ensure that no outage is experienced. Correctly implementing Rapid PVST+ with a new physical layout will also minimise any interruption to network traffic that could be caused by the failure of a switch.

Finally, as part of a physical restructuring of the network layout time should be taken to ensure cabling standards are adhered to. By using available cable runs and bundling cables to use one side of the cabinet both airflow and accessibility can be improved. At present the physical layout of equipment presents some challenges to RNRA network administrators who wish to install new network cabling or connect to on-device console ports to administer devices locally.

### 3.3 Logical layout of network can be improved

At present the RNRA network offers opportunities for improvement that will prepare the RNRA to offer services directly to the general public. This recommendation relates to the RNRA central office.

At present RNRA users, servers, and infrastructure devices all exist in the same IP network: 10.10.8.0/21. This network includes all addresses from 10.10.8.1 to 10.10.14.254 inclusive, a potential total of 2046 devices all capable of communicating without any clear point for policy enforcement.
To prepare the logical layout of the network to provide services to the general public desktop users should be segregated from servers. This would then allow the later implementation of policy enforcement at centralised points. As a side benefit this would reduce the amount of spurious network traffic being sent to hosts such as IP broadcasts requests.

The fastest way for the RNRA to improve the logical layout of their network would be to move desktop users into a different network. 10.10.16.0/21 would be an obvious choice. This would prevent any need to readdress applications to send traffic to new application server addresses. This would also be easier to action than the alternative option of readdressing servers as hosts presently receive their IP addresses from central a DHCP pool. Reconfiguring the DHCP servers would require planning, but deliver a result overnight.

This logical restructuring would open up the possibility to move to an internal / external / DMZ layout in future when RNRA are prepared to offer services directly to the general public.

### 3.4 Centralise policy enforcement

Firewall capability for RNRA servers is provided by Kaspersky Endpoint Security software installed on each server and managed either via Kaspersky Security Centre or locally. This division between locally managed / policy managed is an area for improvement.

Correct configuration of the Kaspersky Security Centre software will allow centralised management of all servers with Kaspersky Endpoint Security installed. Prior to conducting this action and enforcing central firewall policy enforcement RNRA IT staff should conduct an audit of firewall rules in place on locally managed Kaspersky installations.

Kaspersky Security Centre allows the creation of numerous firewall policies. RNRA would be well advised to create role-specific policies such as one for Active Directory servers, rather than attempting to create a one-size-fits-all generic policy or reverting to locally managed policies. This recommendation would ensure consistency across the RNRA server estate and improve time taken to troubleshoot issues by enforcing the same policy on all servers in a policy group.

In future RNRA should investigate the implementation of a feature-rich hardware firewall to provide features such as policy enforcement, traffic inspection, network address translation for publically available services, and intrusion prevention.

### 3.5 Implement network monitoring / management

This recommendation covers the proactive monitoring and management of RNRA network infrastructure. At present only a portion of RNRA network infrastructure is capable of being managed remotely, with the majority requiring an RNRA network administrator to connect directly to the switch to be managed. Further to this RNRA does not possess a centralised point of network monitoring or central log repository.

The first step to implementing this recommendation would be to ensure that all central network infrastructure devices are configured with an IP address and remote login credentials. This will allow RNRA network administrators to connect directly to devices to conduct configuration and troubleshooting activities.

The second step would be to install and configure a monitoring service. There are numerous open-source options available. The installation and configuration of a monitoring solution will allow RNRA network administrators the ability to view historical and real-time utilisation statistics of monitored devices. Some solutions will also allow RNRA network administrators
to set alert thresholds to warn of abnormal or unexpected situations, improving the time taken to identify and problem and find a resolution.

Many network monitoring tools also offer the capability to take scheduled backups of device configuration. Such a capability is highly useful in recovering from a change with an unexpected outcome or from a device failure allowing a replacement to be swiftly reprovisioned.

When RNRA move to supply services to the general public an externally-hosted solution to monitor services should be explored. This will allow RNRA to monitor their services from an external viewpoint and test service availability and performance to ensure problems are identified quickly.
This section of the report will cover methods to implement recommendations and is geared toward a technical audience. Some of the implementation recommendations made in this section are related to observations of the RNRA network not referenced elsewhere in this report. The technical methods in this section should not be implemented as-is, but viewed as guide on how to implement the recommendations on RNRA equipment and treated with caution.

4.1 Securing Oracle Glassfish

Guidance on implementing TLS/SSL can be found in the appendix to this report. The relevant pages are 191-194. An example of the required command would be as follows:

```
create-ssl
--type http-listener
--certname sampleCert http-listener-1
--tlsenabled true
--sslenabled false
```

4.2 Securing PostgreSQL

Guidance on securing PostgreSQL with TLS/SSL can be found in the appendix to this report. The relevant sections are 17.9 and 18.3.2. An example of the required command would be as follows:

```
SHOW config_file;  // this will display the location of the postgres.conf file to be edited  
ssl on
ssl_ca_file root.crt
ssl_cert_file server.crt
ssl_key_file server.crt
ssl_ciphers HIGH:+3DES
```

4.3 Restructuring physical layout of network

Guidance on the framework which informs these suggestions can be found in the appendix to this report. This recommendation is made in line with a simplified implementation of the Cisco Campus Network for High Availability Design Guide.
Describing the entirety of a proposed layout for the RNRA central office would expand beyond recommendation and into proposal. With that in mind, this should serve as a summary of a full proposal.

The purpose of this hierarchical layout, as discussed previously, is to provide a switching infrastructure that can continue to function should a device be lost with minimal impact to the rest of the network. A hierarchical layout also allows expansion of the network with minimal disruption.

RNRA possess a number of switches at the Kigali central office. These include Cisco Catalyst 2960 and Cisco Catalyst 3750G switches. The Catalyst 3750G switches should be considered RNRA’s ‘core’ switches with the following characteristics:

- Two physical cables, arranged in a single LACP bundle, should connect the two switches.
- All interfaces connecting to other switches should be configured as VLAN trunk links.
- Use of access ports on the core switches should be kept to a minimum.
  - If constraints on available ports require connection of hosts to the core switches, recommend these are servers, rather than desktop hosts.
- Both switches should be configured to use Rapid PVST+.
  - One switch should be configured as the spanning-tree primary root bridge with a suitably low priority value.
  - One switch should be configured as the spanning-tree secondary root bridge with a priority value above that of the primary.
- VLAN IP interfaces should exist only on the core switches.
  - These IP interfaces should be configured to use HSRP to provide resilience for traffic directed towards these IP interfaces.
  - These IP interfaces should occupy the last addresses in their respective subnets, with the HSRP address occupying the last host address in the subnet.
  - One VLAN should be maintained purely for switch management.

RNRA’s Cisco Catalyst 2960 switches should be considered ‘access’ switches with following characteristics:

- ‘Access’ switches should not be connected to each other.
- Each switch should maintain a link to each ‘core’ switch.
  - These links should be configured as VLAN trunk links
- Each switch should hold a VLAN IP address for remote management only
- Each switch should be configured to use Rapid PVST+
- Switchports configured for host connectivity should be configured to use portfast
  - The macro command ‘switchport host’ should be used on access ports to ensure consistency

Configuration guides for these recommendations can be found through links supplied in Appendix A, and through Cisco’s website.

### 4.4 Restructuring logical layout of network

Guidance on the framework which informs these suggestions can be found in the appendix to this report. This recommendation is made in line with a simplified implementation of the Cisco Campus Network for High Availability Design Guide.
Describing the entirety of a proposed layout for the RNRA central office would expand beyond recommendation and into proposal. With that in mind, this should serve as a summary of a full proposal.

The purpose of this hierarchical layout, as discussed previously, is to provide a logical structure that allows RNRA to segregate hosts from servers, enforce policy of traffic moving between IP subnets, and improve performance of hosts by limiting the quantity of broadcast traffic received.

With the core devices at the centre, three major subnets would be available for use:

- 10.10.8.0/21 – server network.
  - Use of this range would allow later expansion to 10.10.0.0/20
  - Use of this range would also allow subdivision to 10.10.0.0/22, 10.10.4.0/22, 10.10.8.0/22 and 10.10.12.0/22
- 10.10.16.0/21 – host network.
- 172.16.0.0/16 – remote office network range
  - This range would be subdivided into /24 networks, with one assigned to each remote office.

With this addressing structure access lists on the core switches, or later a hardware firewall, could be provisioned to control traffic and ensure security of servers providing services to public customers.

### 4.5 Centralising policy enforcement

Preferably control of traffic to servers would be conducted via a hardware firewall platform capable of application inspect. However, with the Kaspersky Security Centre software and Kaspersky Endpoint Security software installed at present the following actions are recommended:

- For each server conduct logging of ‘typical’ traffic.
- For each server use netstat or equivalent to determine listening ports.
- Compare these lists to define rule for security policy creation
- Create policies on Kaspersky Security Centre for typical server roles and assign servers into these policy groups.

Should RNRA move to use a hardware firewall platform this pattern of assessing, documenting, then implementing should still be followed.

Moving from Kaspersky Security Centre to a hardware firewall would be a recommended medium-to-long term recommendation. Compared to software solutions a hardware firewall offers dependable performance. Hardware firewalls are also easier to manage, monitor, and maintain with a wider availability of third-party support from vendors and accredited contractors.

### 4.6 Adopt naming convention

At present the nomenclature used to name servers and infrastructure devices does not help to define their purpose. Utilising a standard format for names will assist new and existing staff to understand the role or purpose of a device or server at a glance. At present the distinction between, for example MAIN_SWITCH and MAINSWITCH is unclear.
A suggested strategy would be as follows:

LOCATION-TYPE-NUMBER.domain

This would result in the following example mapping:

**MAINSWITCH** = KIGALI-C3750G-01.rnra.rw
**MAIN_SWITCH** = KIGALI-C3750G-02.rnra.rw
**MAINROUTER** = KIGALI-R1941-01.rnra.rw
**AD Primary** = KIGALI-AD-01.rnra.rw
**AD Secondary** = KIGALI-AD-02.rnra.rw
**LAIS** = KIGALI-LAIS-01.rnra.rw
**GIS Server** = KIGALI-GIS-01.rnra.rw

Amendments to this are possible, but should be logical and consistent. An example would to insert a field for production and test servers to distinguish servers with similar names but different roles:

**LAIS Production** = KIGALI-PROD-LAIS-01.rnra.rw
**LAIS Test** = KIGALI-TEST-LAIS-01.rnra.rw
**GIS Production** = KIGALI-PROD-GIS-01.rnra.rw
**GIS Test** = KIGALI-TEST-GIS-01.rnra.rw

### 4.7 Implement network monitoring solution

There are many available network monitoring solutions. The primary open-source solution available is Cacti. Cacti offers built-in monitoring tools leveraging SNMP to retrieve statistics for disk utilisation, CPU use, and interface utilisation among others. This information is graphed and can be stored for later investigation.

Cacti also offers enhance functionality through plugins. These plugins can conduct activities such as retrieving and storing configuration for network devices, and sending alert messages to network administrators when thresholds have been breached.

A full guide to installing and configuring Cacti is beyond the scope of this implementation guide but is referenced in appendix A.

### 4.8 Define Acceptable Usage Policy for staff internet use

At present there is evidence of limited filtering of internet use. The equipment used for this is limited to inspecting outbound traffic for pre-determined website addresses and does not offer scope for expansion.

The URLs that are listed appear to be related to the use of file download, bit torrent, and streaming video websites. What appears to be the common relationship between these blocked categories is that they are all bandwidth-intensive uses of the RNRA internet connection.

An Acceptable Usage Policy for staff internet use can be defined as a starting point from which to control use of internet traffic on a point of central policy enforcement such as a router, proxy server, or firewall. Logically restructure the RNRA network as suggested in 4.4 would allow the use of bandwidth policing QoS mapping to be conducted on the RNRA router between the internet and the RNRA network. An example configuration would look like the following:

In this example, Network1 represents the RNRA desktop hosts, while Network2 represents the RNRA servers. This example should not be deployed into production without properly
assessing the CIR values assigned for each network, or without assessing the impact on the RNRA ISR1941 that connects the RNRA network to BSC Ltd.'s equipment for internet and remote office access.

class-map match-all Network2
match access-group name network2
class-map match-all Network1
match access-group name network1
!
!
policy-map Upload_Limit
class Network1
police cir 512000
conform-action transmit
exceed-action drop
class Network2
police cir 512000
conform-action transmit
exceed-action drop
!
!
class-map match-all To_Network1
match access-group name To_Network1
class-map match-all To_Network2
match access-group name To_Network2
!
!
policy-map Download_Limit
class To_Network1
police cir 1024000
conform-action transmit
exceed-action drop
class To_Network2
police cir 1024000
conform-action transmit
exceed-action drop
!
ip access-list standard network1
permit 10.10.16.0 0.0.7.255
ip access-list standard network2
permit 10.10.8.0 0.0.0.7.255
ip access-list extended To_Network1
permit ip any 10.10.16.0 0.0.7.255
ip access-list extended To_Network2
permit ip any 10.10.8.0 0.0.0.7.255
!
!
interface GigabitEthernet0/0
service-policy input Download_Limit
service-policy output Upload_Limit
Appendix A - Technical references


### Appendix B Skills/Costs of recommendations

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Skills / Qualifications required</th>
<th>Estimated cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securing Oracle Glassfish</td>
<td>Experience in administering Oracle Glassfish server.</td>
<td>1 day. Supplementary cost of signed X509 certificate.</td>
</tr>
<tr>
<td>Securing PostgreSQL</td>
<td>Experience in administering PostgreSQL databases.</td>
<td>1 day. Supplementary cost of signed X509 certificate.</td>
</tr>
<tr>
<td>Restructuring physical layout of network</td>
<td>Experience with small-scale data centre racking &amp; cabling. Cisco Certified Network Professional (eg. CCNP (Routing &amp; Switching)).</td>
<td>4 days for assessment / candidate configuration / implementation. 1 day supplementary resource to assist with implementation.</td>
</tr>
<tr>
<td>Restructuring logical layout of network</td>
<td>Experience with designing and implementing IPv4 networks. Cisco Certified Network Professional (eg. CCNP (Routing &amp; Switching)).</td>
<td>3 days for assessment / candidate configuration / implementation. 1 day supplementary resource to assist with implementation.</td>
</tr>
<tr>
<td>Centralising policy enforcement</td>
<td>Experience with Kaspersky Endpoint Security. Experience / Certification with implementing / administering RNRA-chosen successor product. (eg Cisco Certified Network Professional (Security)).</td>
<td>1 day. Alternatively 3 days for assessment / candidate configuration / implementation of successor product. Supplementary cost of successor product.</td>
</tr>
<tr>
<td>Adopt naming convention</td>
<td>Familiarity with RNRA IT environment / medium-scale corporate network environment.</td>
<td>1 day for proposal / implementation.</td>
</tr>
</tbody>
</table>

---

**Evidence On Demand**

Climate & Environment Infrastructure: Livelihoods