

Network Management tools

Security and observability upgrades

Compiled and presented by:

Darshan Subedi

Engineer

Network Engineering Section

Introduction

- Darshan Subedi
- Network Engineer for Bhutan Telecom (since 2025)
- Previously Assistant Lecturer for CST, Software Engineering Programme (2023-2025)
- BE in Electronics and Communications Engineering (2019-2023)
- 8th ThaiNOG
- darshan.subedi@bt.bt

Agenda

- | | | | |
|---|-------------------------|---|-----------------------------|
| 1 | Infrastructure overview | 5 | New tooling stack |
| 2 | AAA triad | 6 | Challenges and restrictions |
| 3 | Old tooling stack | 7 | Open source vs paid tools |
| 4 | Security concerns | 8 | Future implementations |

1. Infrastructure overview - the scale

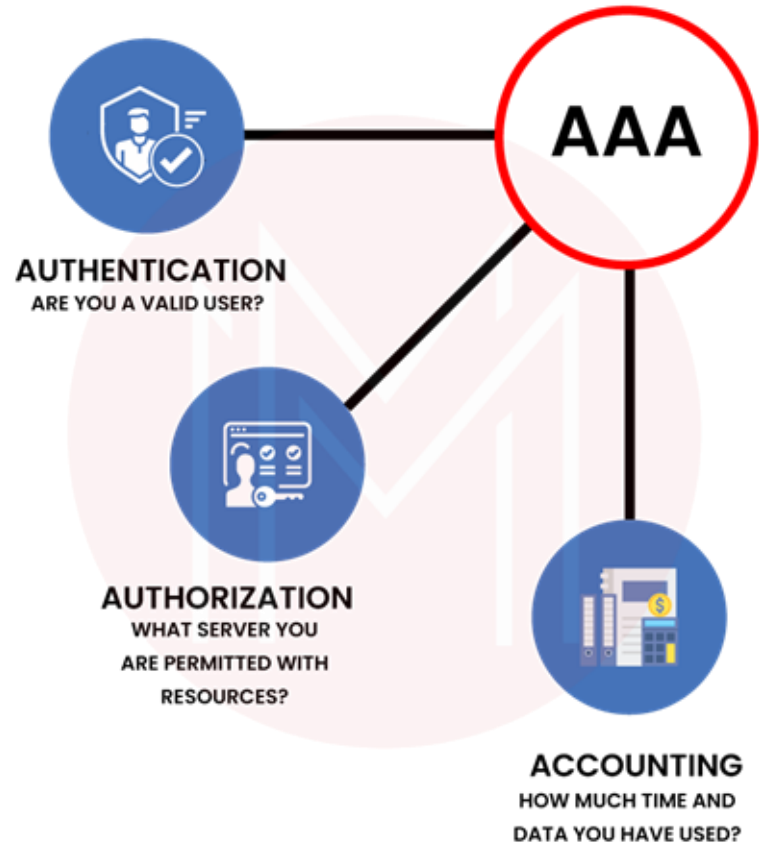
- | | | |
|---|-------------------------|---|
| 1 | Gateway routers | Customer facing routers provisioned to provide leased line internet, often configured with leased line switches. |
| 2 | Core routers | Infrastructure routers that help define access lists (ACL) policies and act as route reflectors in areas with many gateways |
| 3 | Transit routers | Routers that receive or terminate into international traffic |
| 4 | Other equipments | Firewall, RTBH trigger routers and BR routers for peering |

This totals to about 400 routers and 100 switches

2. AAA - Authentication, Authorization and Accounting

AAA (Authentication, Authorization, and Accounting) is a security framework used to control and monitor access to network devices and services.

Authentication verifies the identity of a user or device, typically through usernames, passwords, or certificates
Authorization determines what resources and commands an authenticated user is permitted to access based on assigned roles or policies
Accounting records user activities, such as login times, executed commands, and resource usage, providing an audit trail for monitoring, troubleshooting, and compliance



Source - transtutors.com/AAAnetworksecurity

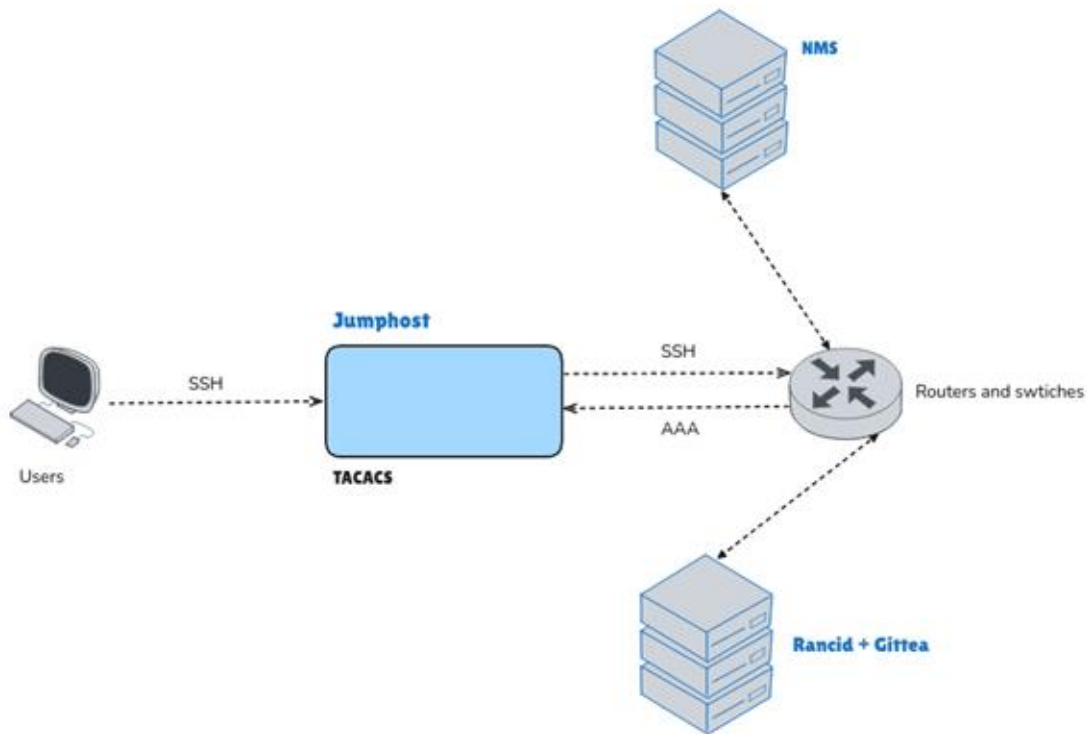
3. Old tooling stack

The old server was the primary jump host hosting these services:

- TFTP server (config backup)
- TACACS+ (router authentication)
- ssh and sshd config

This is standard ISP network architecture. Only one server being able to ssh into routers and switches reduces attack surface.

But this also means that the jump host which many users interact with, is vulnerable to privilege escalation attacks.



4. Security concerns

1 **Rogue user attempts**

Many rogue users would repeatedly try to login to the jump host as it had a public IP.

3 **Public key and password based auth**

A user would either ssh using password (unsafe) or public key. Both of which can be exploited if an employees machine is compromised.

2 **Limited ufw settings**

Limited UFW setting causes the server to be vulnerable to attacks from different IP's, ports and protocols.

4 **Documentation**

Troubleshooting becomes difficult with old tools with no proper documentation.

5.1 New tooling stack - security

To address the issues mentioned above, the following measures have been put in place:

- Installed Ubuntu 24.04 LTS
- **UFW firewall rules:** restrict ssh only from BT LAN IP.
- **Fail2ban:** a tool designed to ban IP's that make repeated ssh attempts into the server.
- **Google authenticator:** adds an extra layer of security by providing **time-based one-time passwords (TOTP)** as a second authentication factor, ensuring that even if a user's password is compromised, unauthorized access to the server is prevented without the user's registered device

.

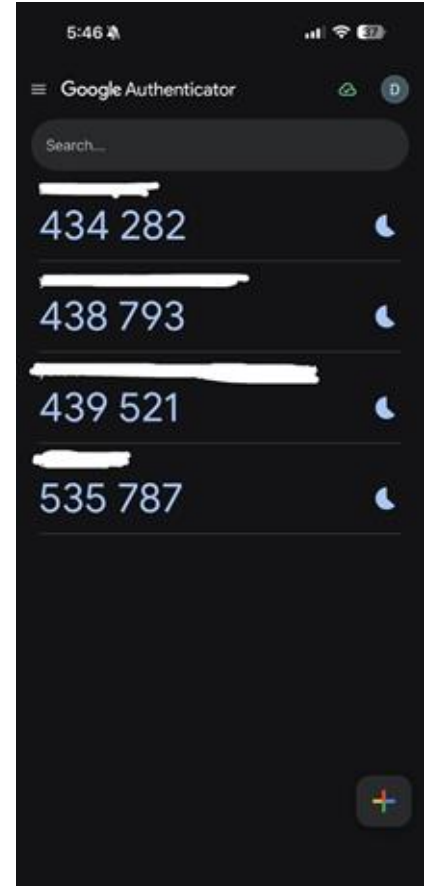
Google authenticator setup

Google authenticator setup with the pam.d file in `/etc/pam.d/sshd`

You can set pre-requisites in sequence, for example:

1. First require user pubkey to match
2. Then require user password
3. Then require TOTP 6 digit code from the authenticator app

Abort connection if any method fails.



5.2 New tooling stack - observability

Tools have been configured to observe interactions with our equipments and services

Logs

Well documented TACACS+NG logs that records who did what and when on the routers, set up in year/month/date format.

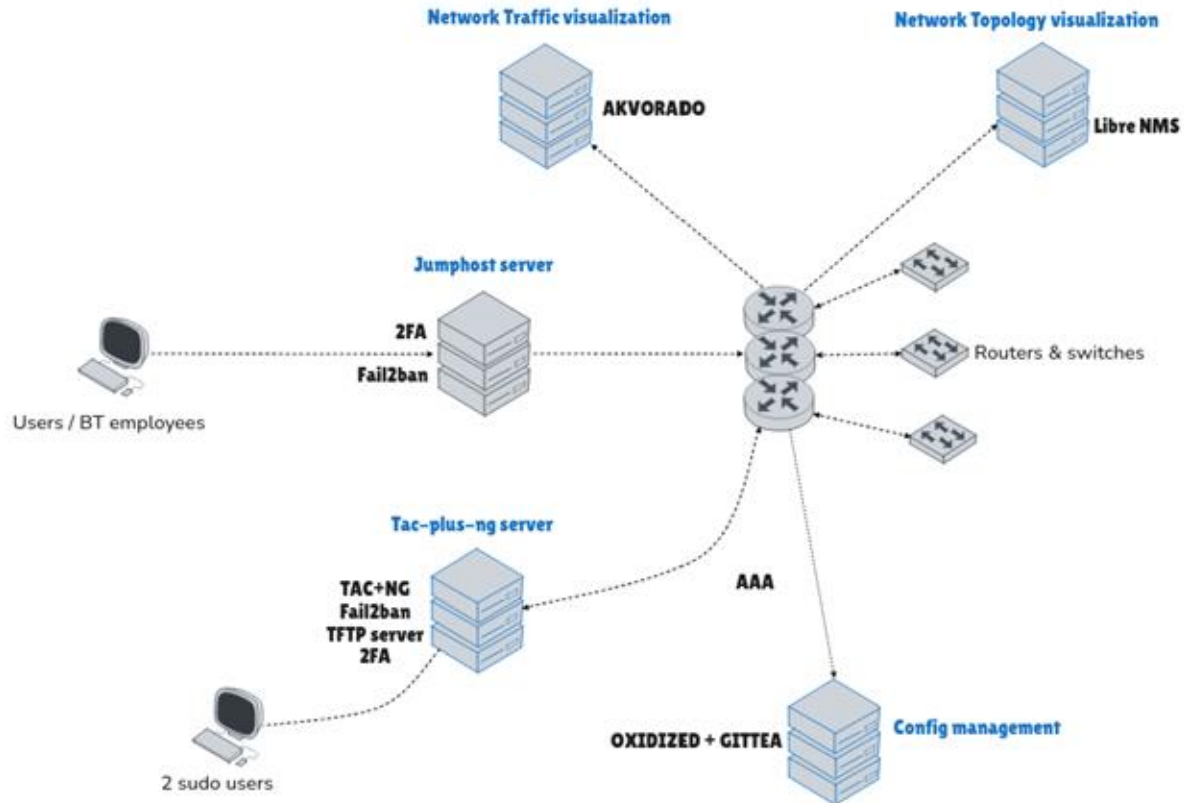
Config backup

In the event a router gets flushed or inactive, backups are in place to replicate the exact config on the new router as soon as possible

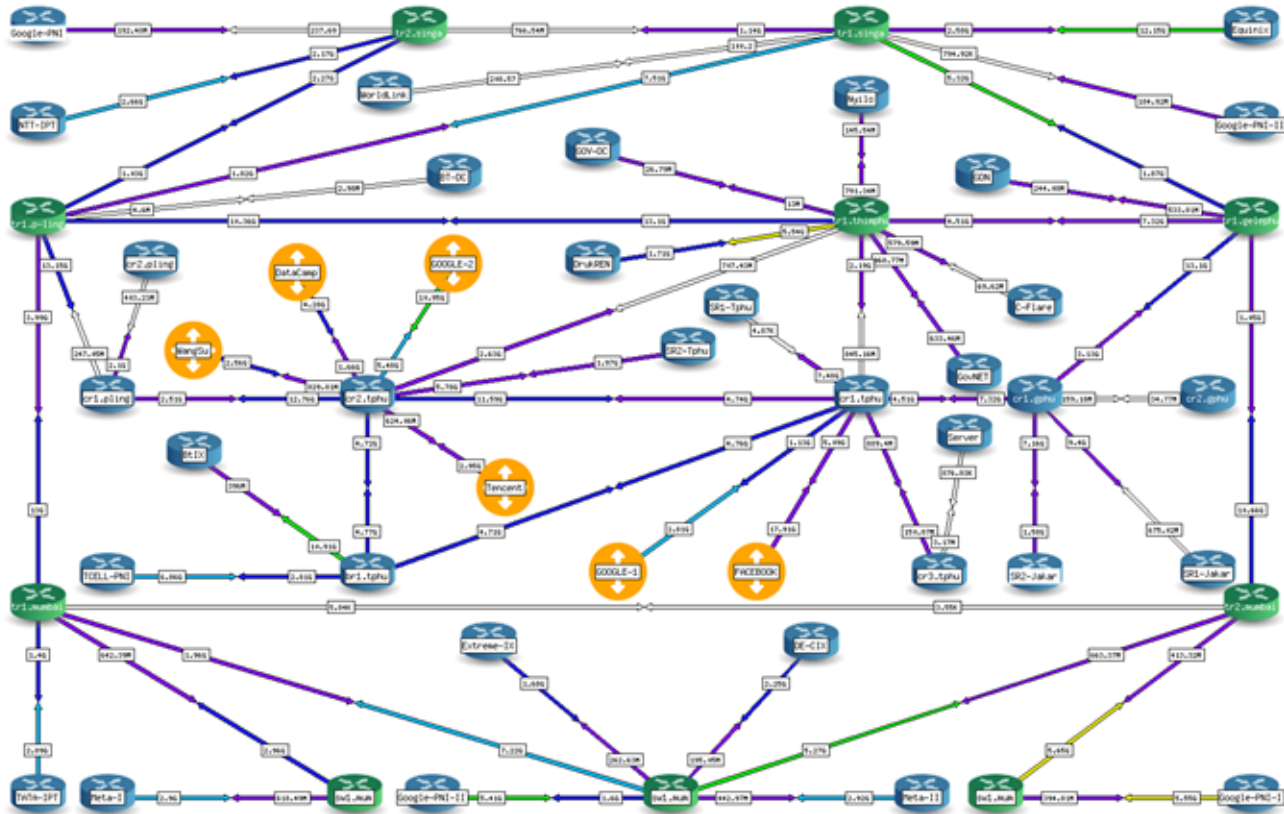
Traffic visualization

Visualize transit traffic based on ASN, IP addresses and CDNs.

5.3 New tools and infra overview



Libre NMS - Network map and visualization



Created: May 19 2026 04:20:00

Oxidized + GITEA - config backup stack

The screenshot displays the Gitea web interface for the repository 'teawithsugar / network-config-logs'. The interface is in dark mode and includes a top navigation bar with links for Issues, Pull Requests, Milestones, and Explore. Below the repository name, there are icons for Code, Issues, Pull Requests, Actions, Packages, Projects, Releases, Wiki, and Activity. The main content area shows a list of commits, with the first commit 'Oxidized' (c38b6532f9) selected. The commit message is 'update /gw1.khitshang'. The right sidebar contains a search bar, a description of the repository, and a languages section showing 'ColdFusion 100%'.

teawithsugar / network-config-logs

1,542 Commits 1 Branch 0 Tags

master -

Go to file T Add File + Code -

Oxidized c38b6532f9 update /gw1.khitshang 3 minutes ago

cr1.gelephu.druknet.bt	update /cr1.gelephu.druknet.bt	2 days ago
cr1.jakar.druknet.bt	update /cr1.jakar.druknet.bt	2 weeks ago
cr1.kanglung.druknet.bt	update /cr1.kanglung.druknet.bt	2 weeks ago
cr1.mongar.druknet.bt	update /cr1.mongar.druknet.bt	2 weeks ago
cr1.p-ling.druknet.bt	update /cr1.p-ling.druknet.bt	5 days ago
cr1.paro.druknet.bt	update /cr1.paro.druknet.bt	yesterday
cr1.samtse.druknet.bt	update /cr1.samtse.druknet.bt	2 weeks ago
cr1.semtokha.druknet.bt	update /cr1.semtokha.druknet.bt	yesterday
cr1.sjk.druknet.bt	update /cr1.sjk.druknet.bt	4 days ago
cr1.thimphu.druknet.bt	update /cr1.thimphu.druknet.bt	5 days ago
cr1.trongsa.druknet.bt	update /cr1.trongsa.druknet.bt	last week
cr1.tsirang.druknet.bt	update /cr1.tsirang.druknet.bt	2 weeks ago
cr1.wangdue.druknet.bt	update /cr1.wangdue.druknet.bt	3 days ago
cr2.gelephu.druknet.bt	update /cr2.gelephu.druknet.bt	last week
cr2.p-ling.druknet.bt	update /cr2.p-ling.druknet.bt	2 weeks ago
cr2.thimphu.druknet.bt	update /cr2.thimphu.druknet.bt	5 days ago
gw1.autsho	update /gw1.autsho	4 hours ago

Search code...

Description

Network config logs for all routers/switches pulled every 30 mins.

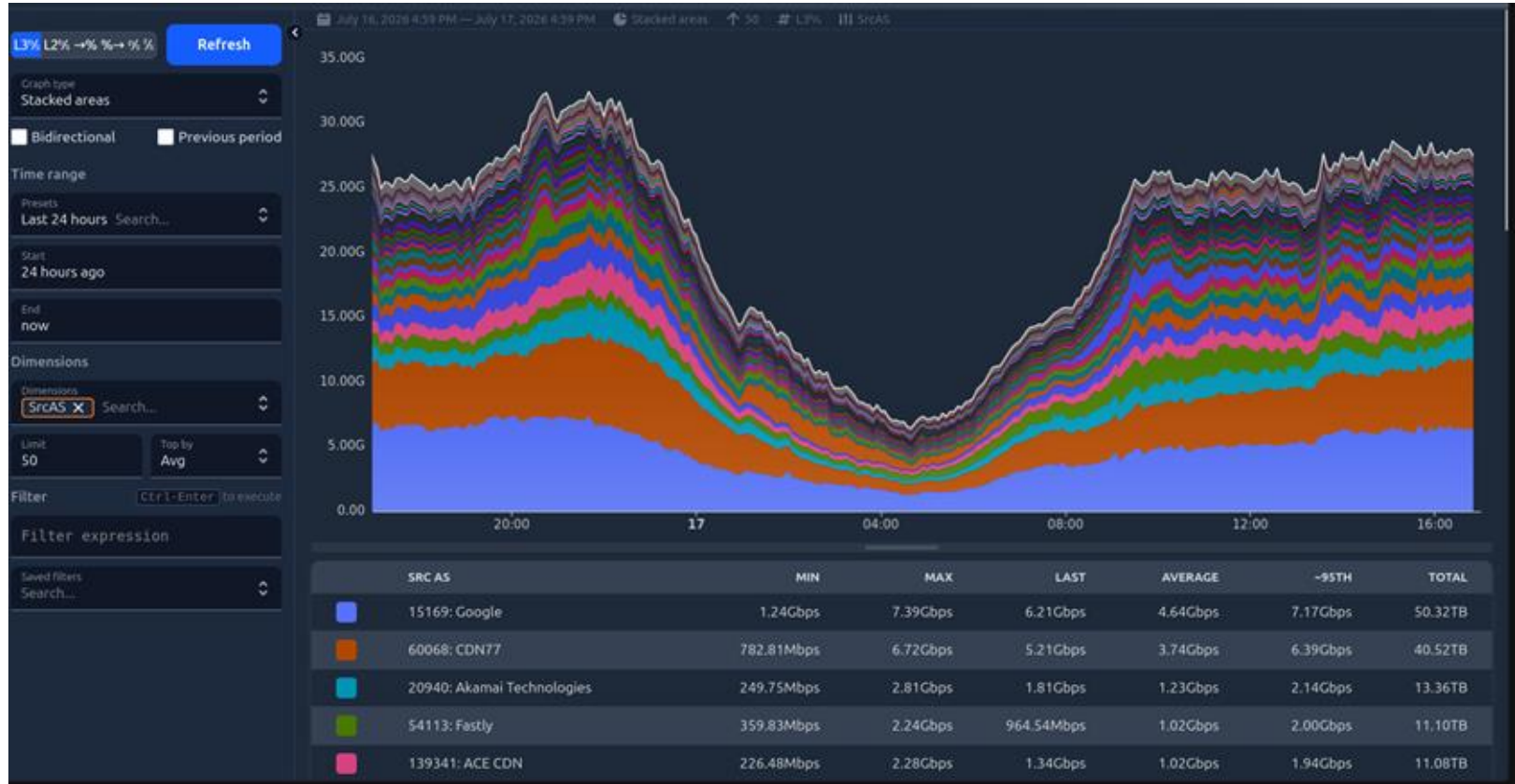
Manage Topics

34 MiB

Languages

ColdFusion 100%

Akvorado - flow collector and visualizer



Akvorado - Top CDNs



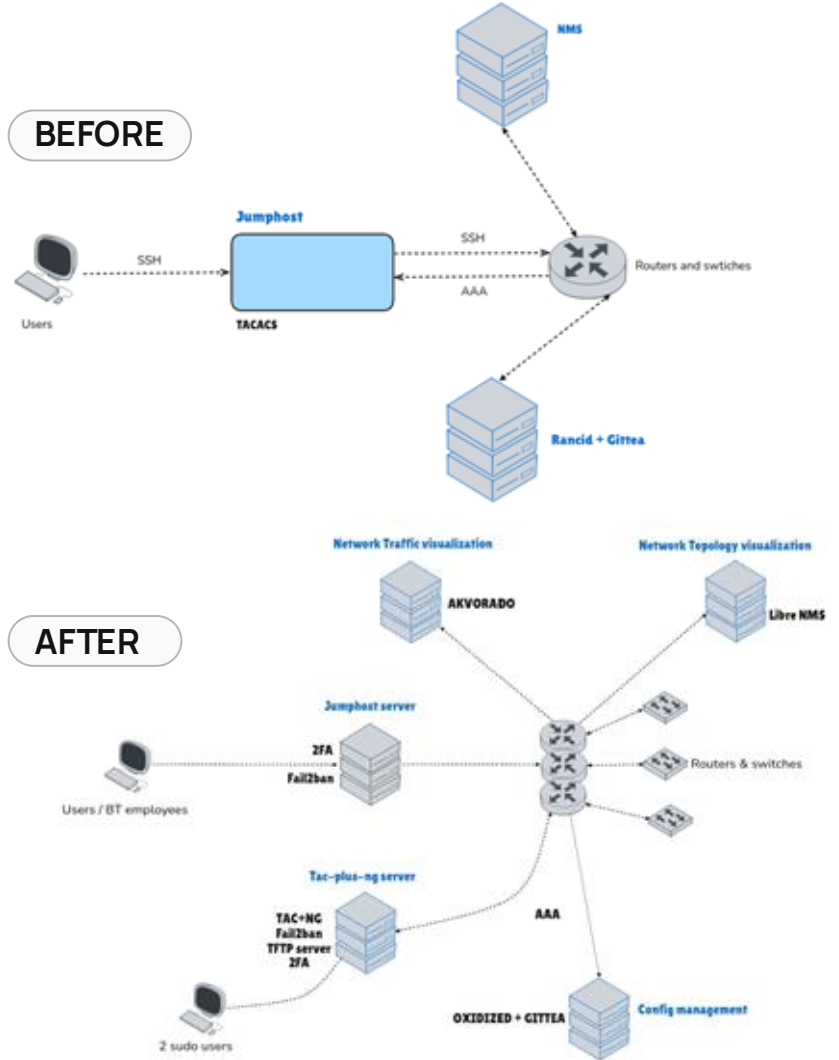
Flow exporter config in IOS-XR

```
flow exporter-map exporter1
  transport udp 9005
  source Loopback1
  destination *serverIP*
!
flow monitor-map FLOW-MONITOR
  record ipv4
  exporter exporter1
  cache timeout active 300
  cache timeout inactive 60
!
sampler-map FLOW-MONITOR
  random 1 out-of 2000
```

```
interface TenGigE0/0/0/1
  description Link to |TransitLink1|
  ipv4 address 192.168.144.127 255.255.252.0
  flow ipv4 monitor FLOW-MONITOR sampler FLOW-MONITOR ingress
```

Migration

On **6th May, 2026** we migrated from our old tools to the new setup. The migration was successful with only one issue with an external automation project which was resolved in under an hour.



5.4 Documentation

The screenshot displays the BookStack web application interface. The top navigation bar is dark blue with the BookStack logo, a search bar, and links for Shelves, Books, Settings, and a user profile (Darshan). Below this, a breadcrumb trail shows the path: Books > IT Division > Network Engineering Section > NES Tools. The main content area is divided into three sections: Page Navigation, Book Navigation, and Details. The Page Navigation section on the left lists links like Welcome, Introduction, About ANTS, and Who Should Use This Doc... The Book Navigation section on the left shows a tree view of the IT Division, with the Network Engineering Section expanded to show the NES Tools page. The main content area features the NES Tools title with a globe icon, a welcome message, an introduction paragraph, and an 'About ANTS' section with a bulleted list of items. The Details section on the right shows revision information and action buttons like Edit, Copy, Move, Revisions, Permissions, Delete, Watch, Favourite, and Export.

BookStack Search Shelves Books Settings Darshan

Books > IT Division > Network Engineering Section > NES Tools

Page Navigation

- Welcome 🙌
- Introduction
- About ANTS
- Who Should Use This Doc...

Book Navigation

- IT Division
 - Cyber Security Section
 - 1 Page
 - Network Engineering Section
 - 6 Pages
 - NES Tools**
 - Inventory
 - Getting Started
 - Server setup
 - Creating accounts and setting credentials
 - Tac_plus-ng
 - IT System and Servers

NES Tools

Welcome 🙌

This documentation is dedicated towards addition, development and maintenance of tools that are used by the Network Engineering Section, Bhutan Telecom Ltd. This document is for reference of BT employees only and hence is restricted to certain email addresses. If you need help adding another employee or editing its contents, please contact: darshan.subedi@bt.bt

Introduction

Welcome to the All NES Tech Stack (ANTS) Documentation!

About ANTS

ANTS is an all encompassing tech stack that ensure secure implementation and daily upkeep guides for different tools we currently have in place. This documentation also serves as a guide for:

- What we had (Old)
- What we have (Current) and
- What we need (Future)

to keep our network infrastructure secure and robust. ANTS also ensures that we have a log of changes, design decisions and choice of tools based on what is needed.

Who Should Use This Documentation

Details

- Revision #16
- ★ Created 2 weeks ago by Darshan Subedi
- ✓ Updated 2 weeks ago by Darshan Subedi

Actions

- Edit
- Copy
- Move
- Revisions
- Permissions
- Delete
- Watch
- Favourite
- Export

6. Challenges and restrictions

External Automation

Some external vendor based automation projects interact with our infrastructure daily which made the migration difficult. For future implementation, we are looking to expose an intermediary server that interacts with their API's

Storage and compute

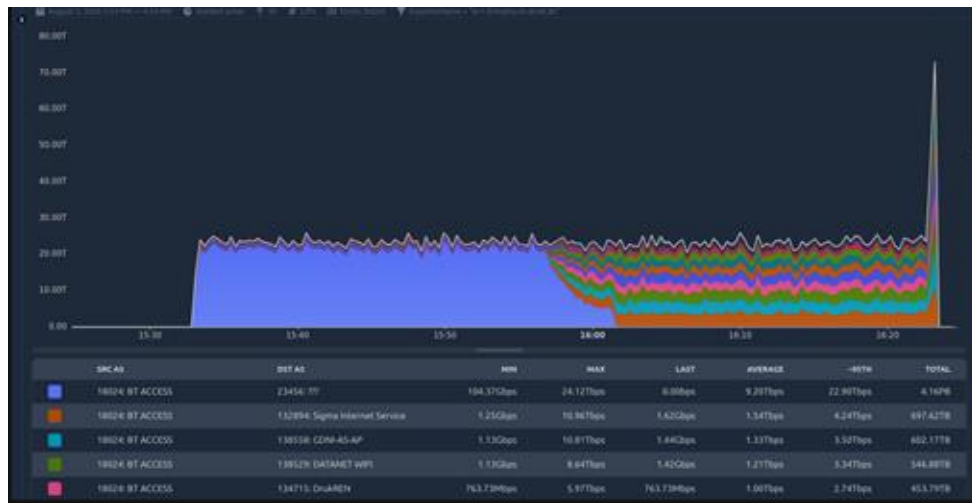
Modern applications for network analysis may require large amount of storage and compute. Procuring new devices is expensive, we are looking to reuse old or unused servers for future deployments.

Documentation and upkeep

Modern software application requires proper full fledged documentation for troubleshooting and periodic upkeep in the event of vulnerabilities and updates. Moving forward, the book stack implementation will help us stay on track with upgrades.

Lessons learned

- For tacacs:
 - Logging and log file destination
 - Passwords are **ALWAYS** saved encrypted
- For Akvorado:
 - Sampling rates
 - Ingress v/s egress traffic
 - Configuration on the bundled v/s individual ports
- Oxidized + Gitea:
 - Gitea is situational, oxidized is necessary
 - Backup frequency and revolving logs
 - Threads - defining concurrent logins for backup



7. Open source v/s paid tools

Open Source tools

Pros

- Low install and maintenance costs
- Self hosted infrastructure

Cons

- Difficult to maintain
- Self assess vulnerabilities
- Infrastructure cost

Paid Software

Pros

- Consumer support
- Reliable and kept up to date by the vendor

Cons

- Very little to no flexibility
- Data exposed to a third party company

8. Whats next?

Security

Completed:

- SSH hardening
- UFW settings
- 2FA using google-authenticator



60%

100%

Where we are
now

Where we
want to be

To Do:

Log ingestion - Deploy a tool to ingest tacplusNG logs and report suspicious activity via email alerts.

Building redundant Jump host and tacplusNG is next on the list and we are exploring servers to deploy the same across different regions for redundancy.

Limit incoming ssh on routers to jump host only - Currently the logs are cluttered due with rogue attempts with external IP's for which we have to limit the incoming ssh settings to only the jump host via line VTY configs on all routers.

Deploy varying **authorization** privileges for different user groups on tacplusNG

8. Whats next?

Observability

Completed:

- Akvorado deployment and flow exporter on all edge routers for ingress traffic
- Gitea+oxidized for device log management



70%

100%

Where we are
now

Where we
want to be

To Do:

The current LibreNMS has been having issues with polling rates (once every 5 minutes) and with the graph, showing false results. This is affecting the NOC reports as well as an external automation that depends on the NMS. We are Looking to replace the existing LibreNMS stack with a newer implementation with Zabbix and Netbox (for inventory).

Currently akvorado is deployed at edge routers (transit and peering) to assess ingress traffic, we are also looking to deploy it at routers that serve cache traffic that we host internally as well.

8. Whats next?

Maintenance and upkeep

Completed:

- Book stack complete documentation on tools deployed and their SOPs.



60%

100%

Where we are
now

Where we
want to be

To Do:

Making global changes to the entire infrastructure becomes difficult especially when dealing with hundreds of switches and routers. We are looking to have an ansible implementation that helps compare existing configurations against pre-made templates to ensure uniformity in configuration across all devices.

Conclusion

Device

Device health, interface traffic and device reachability - **LibreNMS**

Network topology and visualization - **NMS Weathermap**

Network Traffic

Flow monitor, and traffic analysis - **Akvorado**

Logs

AAA (authentication, authorization and accounting) - **Tacplus-ng logs**

Config changes and audit trail - **Oxidized + gittea and Tacplus-ng logs**

Configuration backup - **Oxidized and TFTP server**



Thank you
Any questions?