Doc No. 25/EACO/BP/1/2023

East African Communications Organisation

Communications for all in East Africa

BEST PRACTICES FOR SYSTEMS/NETWORK MANAGEMENT ISSUES WITHIN THE REGION

Prepared by EACO

JUNE 2023

Table of Contents

Acronyms

AR - Augmented Reality

CAB - Change Advisory Board

EAC - East African Community

ECAB - Emergency Change Advisory Board

GDPR - General Data Protection Regulation

IoT – Internet of Things

ISI - Inter Symbol Interference

KPI - Key Performance Indicator

KYC – Know Your Customer

MNO - Mobile Network Operator

NOC - Network Operations Center

O&M - Operations & Maintenance

OPEX - Operational Expense

PDT - Performance Degradation Ticket

SLA - Service Level Agreement

SNR -Signal to Noise Ratio

TT -Trouble Ticket

VR -Virtual Reality

1.0 Background

Under the EACO strategic plan of 2018-2023 it was identified that there is a need of having recommendations on best practices for systems/network management issues within the region considering the architecture complex in Operating and Maintenance (O&M) of system / telecom network of Mobile Network Operators' (MNOs) including next generation mobile networks especially 5G, calling for protection and proper management for ensuring constant service availability.

Usage and dependencies in systems/ networks have increased in many ways other than voice and messaging and traditional data services such as Facebook, WhatsApp in Social networking, Content services like Netflix, IoT, Cloud computing, VR/AR etc. that will require automation and diversification which will introduce cyber threat and hence cyber security management will be one of the major concerns.

It was determined that there was no recommendation on the best practices for system/network management in the East African region. It was further highlighted that there is a need to come up with the recommendations on the best practices to manage system/ network issues in the Regional.

To this end, EACO WG2 on Infrastructure Development, Connectivity, Sharing and Digital Inclusion was assigned the task of developing recommendations on the best practises for system/network management issues within the East African region.

2.0 Definition of System/Networks

a) A telecommunications network is a group of nodes interconnected by telecommunications links that are used to exchange messages between the nodes. The links may use a variety of technologies based on the methodologies of circuit switching, message switching, or packet switching, to pass messages and signals. https://en.wikipedia.org/wiki/Telecommunications_network

b) It could also refer to the means of providing telecommunication services between a number of locations where equipment provides access to these services. (ITU: https://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.662-2-199304-S!!PDF-E.pdf

3.0 Operational Goals

Network availability, Operational cost and Cyber Security Management are the main goals of running a mobile telecommunication network. Failure in network equipment causes degradation in network performance, revenue loss and wrong image on brand. On the other hand, breach in cyber security can destroy brand image and even can trigger legal issues.

To keep the network running smoothly and protect from cyber-attack, there is a need to implement better operational process, tight SLA, enhance proactive monitoring, implement strong control in access, develop process in line with Authorities' policy and ensure compliance.

4.0 Key recommendations for Network Operation activities

Network operation refers to activities to monitor network's availability and performance, to manage and operate, to implement changes and to secure.

Main Network Operation activities include:

i. Network monitoring
ii. Incident response
iii. Fault handling and troubleshooting
iv. Performance monitoring and optimization
v. Corrective Maintenance
vi. Implement Network Changes – Configuration
vii. Patch management
viii. Preventive Maintenance -Backup and storage
ix. Life Cycle Management

x. Security management – Network Access, Firewall management, security tool deployment and monitoring.
xi. Cyber Security and Privacy Protection management
xii. Reporting and Communication management

The objective of Mobile Network operators to provide end to end service to end users without any disruption. Hence 24x7 fault monitoring and periodic performance monitoring are done.

Globally, it is believed that a small percentage of the network issues remains hidden even though network faults and performance are usually monitored. In order to address the hidden issues, preventive maintenance activities such as system functionality and network health checks should be done. There is also need to handle end of life management of system hardware as well as carrying out software updates and/or upgrades in line with vendors' roadmap.

There is higher concern in modern day mobile network on security and privacy protection. Mobile operators need to implement measures to protect end users' information in compliance with local Data Protection and Privacy Laws and Policies such as Data Protection and privacy Act 2019 for Uganda, Data Protection Act 2019 for Kenya, Personal Data Protection and Privacy Law 2021 for Rwanda as well as the EU GDPR that has been active since May 2018.

5.0 Recommended key processes in systems/networks operations

Different processes have been developed and adopted for carrying out key activities in Mobile Network Operation in a systematic and controlled manner as stated in section 4 above. These include;

5.1 Network Surveillance Process
5.2 Fault Management Process
5.3 Problem Management Process
5.4 Preventive Maintenance Process

5.5 Incident Management Process

5.6 Performance Management Process

5.7 Change Management Process

Relationship and Interoperability between different processes in the context of real life situation has been depicted below.

5.1 Network Surveillance Process

In the network surveillance process, active monitoring of the overall network health and initiation of appropriate follow-up actions responding to network events should be done in a timely manner.

Network Operations Center/Network Surveillance Engineers play a key role in this process. Main responsibilities for this role include;

- Detecting alarms
- Analyzing alarms
- Correlating and filtering of alarms
- Determining of impacted services
- Create trouble Tickets
- Troubleshooting where possible
- Escalate incidents
- Create and manage incident reports.

It should be noted that the main aim of the above processes is to ensure service availability through monitoring or service restoration following the appropriate Mean Time to repair (MTTR) as per agreed SLAs.

5.2 Fault Management Process

Fault management process deals with detection and identification of issues that result into service impact, outage or degradation of the network performance. Faults can be categorized as Critical, Major or Minor as per the impact level.

Poor fault management practice may cause longer network outage or degradation or other network faults.

Maintenance Engineers play the main role in the Fault management process. Main responsibilities in this process include;

- Handle Trouble Ticket
- Localize fault
- Resolve fault
- Conclude Fault
- Track and manage fault
- Report fault

Main KPI in this process is ‘Percentage of faults handled within target restoration time’.

5.3 Problem Management Process

Problem management process minimizes the impact of faults and prevents reoccurrence of those faults. Problem management differs from Fault management in the way that Problem management investigates the root cause of a fault and finds solution while Fault management finds the quickest way of restoring faults, in many cases through a work-around rather than by a permanent solution.

Problem management is categorized as Reactive and Proactive. In Reactive problem management, root cause of a fault is analyzed upon reception from Network Surveillance team and respective solution/measures are provided accordingly. Proactive problem management is concerned with identifying and solving problems before they occur.

Poor problem management practice leads to “firefighting” of problems, poor quality of service and high cost of operation.

The maintenance Engineer plays the key role in the problem management process. Main responsibilities in this process include;

- Handling problem ticket
- Track and manage problem
- Analyzing root cause
- Localizing problem
- Providing and effecting the solution
- Prepare a Root Cause Analysis (RCA) report

Main KPI in this process is 'Percentage of problems handled within the appropriate Mean Time To Repair (MTTR).

5.4 Preventive Maintenance Process

Preventive maintenance is a planned maintenance activity to avert failure of network before it happens. Lack of preventive maintenance may cause longer fault resolution time, excessive inventory requirement, more service impact time that leads to poor customer satisfaction.

The Maintenance Engineer plays a key role in this process. The main responsibilities in this process include;

- Planning and scheduling preventive maintenance
- Receiving preventive maintenance task
- Analyzing preventive maintenance task
- Informing NOC before task execution for relevant stakeholder to be updated
- Carrying out the preventive maintenance
- Preparing and submitting the preventive maintenance report

Main KPI in this process is 'the reduced number of fault tickets raised due to preventive maintenance activities'.

5.5 Incident Management Process

Incident management in networks is the process of managing service disruptions and restoring services within agreed service level agreements.

Lack of proper Incident management process causes difficulty in collecting information about incidents, identifying the impact and longer service interruptions and chaotic back and forth communication between stakeholders.

NOC and Maintenance Engineers play key roles in incident management processes. Main steps in Incident management process include;

- Incident Identification, Logging, and Categorization
- Incident Notification & Escalation
- Investigation and Diagnosis
- Resolution and Recovery
- Incident Closure

Main KPIs for Incident management process are ‘Mean Time to Acknowledge’ and ‘Percentage of Incidents Resolved within SLA.

5.6 Performance Management Process

Performance management process helps detects the abnormal KPI of network performance and triggers the need for troubleshooting. This also includes network routine health checks under the standard operating procedures.

Lack of Performance management process may cause major network outage, higher OPEX and low customer satisfaction.

Performance Engineer, Performance Analyst and Performance Management Supervisor mainly carry out the major responsibilities in the Performance management process. Main tasks in the Performance management process include;

- Monitoring network performance
- Creating performance degradation TT
- Analyzing network performance
- Controlling network performance
- Closing Performance Degradation Ticket (PDT)

- Reporting network performance
- Tracking and managing performance

Main KPI for the Performance management process is to resolve service degradation based on affected KPI as per SLA.

5.7 Change Management Process

Change management process deals with modification in the network configuration, software, capacity expansion, functionality implementation in a controlled manner so that services do not get disrupted after the change implementation. It evaluates the risk during implementation and ensures minimal or no disruption during the change implementation.

Lack of Change management process can cause bad communication between involved stakeholders, poor configuration and service disruption.

Roles and groups in Change management process include; Change requester, Change Manager, Change analyst, Change implementer and Change approver/Committee.

Main tasks in the Change management process include;

- Creating change request
- Categorizing change requests
- Assessing change requests
- Scheduling change requests
- Implementing change requests
- Review and closing change requests

Main KPI for Change management process are “Percentage of successful/failed change request”.

6.0 General Recommended best practices for Management of systems/networks

In addition to the recommended key processes discussed in section 5.0 above, EACO further recommends the following as best practices for systems/network management.

i) Outsourcing; Whereas this has been adopted by several service providers due to improved efficiency, there should be 100% liability of business to the licensee who also has to ensure compliance with license obligations.

ii) Listing in local stock exchange; This will increase the sense of ownership amongst local stakeholders due to increased local participations in the affairs of the organization.

iii) Network Security; Communication CERTs should be put in place

iv) Consider communications infrastructure as critical and develop guidelines for management of critical infrastructure

v) Ensure robust KYC through SIM card registration compliance

vi) Develop CLI and CEIR regulations

vii) Ensure system/network redundancy

viii) Developing national disaster communication plan that among other will include:

- Spectrum for emergency and disasters,
- Implementation of national Emergency operations center (EOC)
- Regional satellite as an alternative to communication services
- Sign the ITU TAMPERE Convention on emergency support
- Deployments of optimized networks (Oponets/ WSNs) for disaster situations

i. Data protection

- Put in place Data protection law
- Ratification Malabo convection on Cyber security and personal data protection and electronic transaction
- Develop regional Cross border data sharing frameworks

ii. Data hosting; International standard of data hosting.

- Recommend Local hosting of telecom nodes within local jurisdiction
- License for datacenters

iii. Conformity and interoperability (Vendor locking)

- Promoting interoperable networks systems across the region
- Participate in standardization meetings and processes eg ITU-T, IEEE
- Regulators to implement thorough type approval process.

iv. Carry out regional cross-border coordination

v. Provide guidelines on Interconnection

- Shouldn't be prohibitive
- symmetrical charging
- Approval from regulator before switching off

vi. Encourage the use of alternative sources of clean energy to power networks/ systems such as wind, solar, bio energy, geo thermal among others.

vii. Operators to connect and peer to the local IXPs and encourage interconnection of regional IXPs.

viii. Develop regulatory frameworks that encourage Infrastructure Sharing (passive and active).

- National roaming, radio access network etc
- Passive sharing (towers, fiber cable, ducts, manhole etc).

7.0 Conclusion

This paper discusses the need for best practices for systems/network management. It further highlights the key processes and best practices as detailed in section 6.0. EACO therefore encourages administrations to consider these best practices in ensuring proper systems/network management in their respective countries.