Addis Ababa University

College of Natural and Computational Sciences,

School of Information Science

Title: - Network Performance Analysis to propose optimization Framework: The case of MoR

ABDULAZIZ KELIFA

September 2021

ETHIOPIA, ADDIS ABABA

Addis Ababa University

College of Natural and Computational Sciences,

School of Information Science

Information Science Department (MSc. Program)

Network Performance Analysis to propose optimization Framework: The case of MoR

A THESIS

SUBMITTED TO THE SCHOOL OF GRADUATE STUDIES OF ADDIS ABABA UNIVERSITY IN PARTIAL FULFILMENT FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION SCIENCE and SYSTEM

By:-

Abdulaziz Kelifa

Advisor: Workishet Lamenaw (PhD)

APPROVED BY EXAMINING BOARD:

Name	Title	Signature	Date
1. Workshet Lamenew (PhD)	Advisor	----------	Sep 30 2021
2. Dereje Teferi (PhD)	Examiner	----------	Sep 30 2021
3. Michael Melese (PhD)	Examiner	----------	Sep 30 2021

Acknowledgment

First of all, I would like to thank Almighty ALLAH for blessing me with the ability and patience to finish this thesis work.

Next I would like to thank my advisor, Dr. Workishet Lamnaw for his support and guidance during this thesis work.

I also want extend my appreciation to our beloved parents & family for their heartless love, support and encouragement during the thesis work, especially my mother for her kind love and encouragement advice. Last but not least, I'm grateful to my friends for their continuous and dedicated supports, discussions, and constructive comments. Without their suggestions this work would not have been possible.

Table of Contents

List of Tables

List of Figures

List of Acronyms

CQ ---------- Custom Queuing
BFD ----------Bidirectional Forwarding Detection
FIFO---------- First in First out
FQ ----------Fair Queuing
GA ---------- Genetic Algorithm
ICMP ---------- Internet Control Message Protocol
MoR ----------Ministry of Revenue
MoR ----------Ministry of Revenue
NBE ---------- National Bank of Ethiopia
PQ ---------- Priority Queuing
PRTG---------- Paessler Router Traffic Grapher
QoS ----------Quality of Service
SFQ---------- Stochastic Fairness Queuing
SIGTAS----------Standard Integrated Government Tax Administration Sys.
SNMP ---------- Simple Network Management Protocol
TBF----------Token Bucket Filter
TIN ----------Taxpayer Identification Number
WFQ---------- Weighted Fair Queuing

Abstract

Government office service provision is being supported by networking infrastructure to connect their branch office with the central datacenter from which the service of application and database is accessed and shared. MoR is among the main government institution which is legally established to levy and collect the inland and custom taxes from the concerned bodies. MoR network dropouts is noticed and become the most discussed issues not only with management and Ethio telecom officials but also with taxpayers as clearly shown on annual reports, stakeholders meeting, and ten years strategic plan.

Currently Ethiopian tax management is being supported by systems developed to support the taxation process based on the defined laws and regulations. The Branch offices are connected to the main datacenter to share the central resources. Though MoR is continually upgrading bandwidth and replacing its devices that are assumed to cause network dropouts, the problem of network dropouts is still unresolved and become the main cause of taxpayers complains publicly. This thesis is aimed to analyze MoR network infrastructure to find the major causes for network dropouts, which leads to taxpayer dissatisfaction with the service provided by the organization. To accomplish the main objective of the thesis MoR network infrastructure is analyzed based on the primary and secondary data collected from network administrators and the monitoring tools installed in the datacenter. The collected data from the SolarWinds and PRTG is analyzed based on the metrics availability, utilization, error and discards, delay, and protocol overhead.

The simulation of the existing network infrastructure is done to further understand the network problems causing network congestion and system unavailability by using OPNET simulation tools, the simulation also help us to demonstrate and test recommended solutions. The analysis result leads us to conclude that there is underperformance caused by different factors like structural imbalance, overloads, lack of system tuning and protocol overheads, on all stages of MoR network and this leads to experiencing some problems like unhealthy link and resource utilization, packets discards and error, high device response time, ISP service availability problems. The major causes are lack of system tuning, overloads, not establishing enterprise-wide performance metrics or improvement targets and policies, not having complete visibility into the network to efficiently manage and operate the enterprise.Then optimization framework consisting 6 modules is proposed which can withstand the problem noticed in the previous stages. The building blocks of the

frameworks are tested on the OPNET network modeling tools and the result shows improvement on the configured metrics.

Finally, to overcome the network problems this thesis highly recommends toward MoR management to consider the findings of this paper and implementing the framework. MoR also needs to establish an IT policy and a network strategy to include a process that continuously monitor IT infrastructures, and develop enterprise-wide performance metrics. Additionally the organization need to establish improvement targets in coordination with the management to implement a solution, such as site wide emergency generators that is fully dedicated only for the data centre to avoid relaying only on the building power generator, this will prevent network connectivity and availability issues.

Key Words: - *MoR, network performance metrics, network dropouts, MoR VPN, Interface utilization, SolarWinds*

Chapter 1

1. Introduction

Currently there is rapid increase in the number of distributed applications which is causing shift from the era of giga byte to the era of tera byte requiring high bandwidth consumption. Besides that, the performance of any organization is being measured by the quality of the services they have given for their customer irrespective of their place and time. To satisfy customers need and implement the merit of the technology in government organization building the networking infrastructure accompanied with analysis and monitoring capability is mandatory task. Decentralizing the services given in one center to other branch offices of government organization need those branches to be connected to the central data center by using the ISP networking infrastructure. Networking is the main technological innovation that can make this communication realistic. Network is simply two (or more) connected computers. Computers can be connected with cables or telephone lines, or they can connect wirelessly with radio waves, fibre-optic lines, or even infrared signals. Today, the most widely used network is the Internet [1] [2].

It's evident that with the emergence of social Medias and other entertainment sites the need for the network bandwidth usage is increasing day after day which is creating the gap between the high user demand and limited bandwidth supply. For solving the gaps and proving the greatest possible throughput and lowest possible latency, network performance and analysis is mandatory task. Effective network management of any size needs a multifaceted approach that includes effective network monitoring, a sensible policy that defines acceptable behaviour, and a solid implementation that enforces these rules [3] [4].

The usage and demand of bandwidth may not meet specially in developing countries like Ethiopia. The speeds of connections from North America to Africa are slower than those to Europe by a factor of 50 or so. Such assessments have been made by measuring the round-trip time that it takes for a digital pulse sent over the Internet to return to the sender. The reasons for this disparity include the availability of Internet access only via slow satellite connections, and the lack of communications infrastructure in the remote parts of the world. Bandwidth and computing

equipment are expensive as a result of weak currencies, high transport costs, few or monopolized ISP small budgets, and unreasonable tariffs [5] [6].

Bandwidth can be defined as the rate or capacity of data transmission. It is measured in bits per second or hertz. Throughput describes the actual amount of information flowing through a Connection. Latency refers to the amount of time it takes for a packet to travel from one point on a network to another. A closely related concept is Round Trip Time (RTT), which is the amount of time it takes for a packet to be acknowledged from the remote end of a connection. Latency is measured as some amount of time, usually in milliseconds. Because bandwidth is a valuable and costly resource, demand usually exceeds supply. In many environments, uncontrolled access and usage of bandwidth results in degraded service for all users. This is partly a supply problem, partly a demand problem, and partly a technical problem [4] [7].

Network traffic data can be collected using active and passive techniques. In passive monitoring technique, the monitoring system captures live data from a particular point(s) within the network. SNMP (Simple network monitoring tool), Net-Flow based monitoring tools, packet sniffers, and different tools used to capture the network statistics from the given node ion the network. Active monitoring techniques provide end-to-end performance measures, unlike passive monitoring methods that measure network performance at a single point. In active monitoring test packets are injected into the network between two given end points. The test packets are used to collect metrics like route, packet loss, jitter, round trip time, availability, using Trace route, Ping etc commands. The disadvantage of active monitoring is that it generates additional network traffic [8] [9].

Having this in mind analyzing the network performance gap is mandatory to allocate the available limited bandwidth in the way that can increase the business interest and performance of the organization in delivering the services to the customers above all to be competitive enough.

MoR is among the crucial government institution that is given the legal rights and duties to collect the revenue from the concerned bodies that can serve as a main financing medium for the government. In a span of 8 years the revenue collection figure has increased from 50.8 billion birr

in 2003 E.C to 198.23 billion in 2011 E.C. The success of this organization is equivalent to achievement of the country's main development goals, since all of those grand plans need government continuous financing. With the principles of being closer to the taxpayer MoR established different branch offices that are already connected to the main data-centre.

Network monitoring and analysis has a vital role in ensuring that these goals of high performance are delivered to the end-users. This network analysis and monitoring not only ensure smooth running of the network but also provide valuable information about network performance characteristics, device performance, routing patterns, routing anomalies, bandwidth usage patterns. This information is used in planning network upgrades, developing new network models/protocols and for efficient resource management. MoR can reach the promised service quality for customers if the task of network performance tuning is aided by proper traffic data analysis of the existing network infrastructure. Those remedies taken to tackle the network performance like additional bandwidth subscription, purchasing high end servers, replacing network devices with new brands, building fancy datacentres and others should be assisted by proper analysis of the existing network environments that can show us the possible bottlenecks contributing for network performance degradation, above all it can direct us to the probable solution if dealt with that can smoothen the performance gaps being noticed in the overall network [10].

1.1 Background

1.1.1 MoR overview

Ministry of Revenue is the core government institution who is given the legal rights and duties to Levy and collects inland and customs taxes based on the ratified rules and regulations.

For the delivery of its services closer to the customers there are 19 branch offices for inland and customs revenue collection in different parts of the country. Those branch offices are connected to the main data centre by using the Ethio Telcom VPN and WAN network infrastructure. The total subscription from the Ethio Telecom for data line is 400Mbps and 500Mbps for the internet services.

1.1.1.1 MoR Network infrastructure overview

MoR built modern data centre for the consolidation of most of the services and enabling central management of system infrastructures. MoR is in a constant transformation to build a modern tax administration system which lead to ease of doing business strategies. The basic idea behind modern tax administration system is to increase the number and quality of compliant tax payers and decrease the non-compliant tax payers in the tax system. From the above fact it's evident that to accomplish those plans we need to be closer to the customer and increaser the frequency of communication. If necessary, devising new branches that are closer to the customer can contribute by saving the time and resources of the customers and contribute towards promotion of the complaint tax payers [11] [12] [13].

All of the 29 customs and Inland Revenue branch offices need to connect to the main data centre for accessing tax administering applications. The main datacentre subscribed 500Mbps for the VPN data line connection and 400Mbps for internet connections from Ethio telecom. Beside the 29 MoR branch offices there are different third-party applications that are connecting to the main data centre such as, NBE for TIN validation, Commercial Bank of Ethiopia for E-payment, Transistors for custom related information access, and cargo tracking system. Most of the applications running in this data centre in one way or the other are related to the critical custom or revenue collection component which requires continuous availability of all the network infrastructures 24/7. Continuous availability of the network can only be assured by network related data analysis and using those data to monitoring the existing problems [11] [12] [13].

For efficient provision of the services for their customers as well as to be closer to their taxpayers MoR is establishing different branch offices which are connected to the main datacenter using Ethio Telecom WAN infrastructure. Central management of those networking infrastructure is preferred from the data center to reduce the costs and ease the management. Accessing resources from central datacenter introduce low bandwidth high latency because of incoming and outgoing traffic imbalances [11] [12] [13].

1.2 Problem Statement

MoR is among the core government institution entitled by law to collect different kind of inland and customs revenues for the government. Most of MoR's tax related operation is supported by the systems and also demanding network infrastructure for instance SIGTAS for E-payment. The organization has a modern centralized datacenter which connects all branches through Ethio Telecom network infrastructure. Since tax is the main source of revenue for the government devising a way that can facilitate the tax collection is vital. Requesting additional bandwidth from Ethio Telecom is preferred to solve network delays and loses which rarely solve the problem from the root. It is evident that MoR is striving to facilitate the provision of quality services and this research aim to help achieving this objective by analyzing the problems related to the network infrastructure so that it will maximize taxpayer's satisfaction.

With the increase in the transmission distance high latency and congestion will be introduced which is the main contributing factor for application high response time and packet loss. The network availability issues like bandwidth limitation, latency, throughput, congestion and packet loss are more of an issue for enterprise WANs. As MoR is adding more branches to be closer to the tax payers, it's experiencing network and system performance problems.

MoR was conducting discussion groups with different stockholders like Ethio telecom the IT directorate itself. While the discussion is being held by the management to pave the way for future network tuning and upgrading plan they were facing difficulty to support the discussion arguments with tangible scientific findings. The group discussion held concerning the existing network problem with the network and system administrators facing the same obstacle as the previous one. This thesis is dedicated to identify the main area of performance problems for the MoR network and pay the way that can show the main area of concern for the technical staffs while dealing with the issues of network performance problems. The finding can be used to limit performance problem focus area happing currently and for the future improvement plan of the organization.

[14]Analyzed the performance effect of various WAN factors from the case target organization WAN perspective and accordingly develop an optimization model that can reduce the factors effect and improves the performance of business-critical applications. He studied WAN performance factors from UNECA WAN perspective and consequently benchmark the performance of

business-critical applications in terms of WAN conditions which he used to develop algorithm for detecting WAN conditions as optimization model. Since the performance of MoR business critical applications is slightly different when they run in internal LAN(VPN) and external environment (WAN) this research wants to benchmark the LAN network performance to detect the performance gap of the same application when they run in the WAN environment. Additionally, this research will be conducted in MoR which is running different business environment and different critical applications.

The work by [15] is also among related thesis to identify the cause of high bandwidth consumption by using proxy log analysis tools with the main target of developing bandwidth optimization framework depending on the quality of services parameters in Addis Ababa University. He identified unbalanced usage of the bandwidth from the proxy log analysis using SAWMILL tool. He then used this finding to develop an optimization framework based on the QOSs. In the target research the area is MoR which different with its operation and business critical applications.
But networking statistics that is only taken form the proxy log is not enough to show the overall network performance, which requires additional active and passive monitoring methods. Nothing is being done on the area of revenue office by considering business critical applications and their behavior on the WAN and LAN environment. Since our target want to identify factors that are causing network performance problem packet statistics behavior is not identical from one network to other network infrastructure. The network performance is basically dependent on the type of network used, type of medium, user behavior , the type of application, the end devices capacity and configuration, the path the packet follow to arrive at their destination, and the network topology adopted by the organization.

The other work by [16] is also allocating a decent amount of bandwidth to users in AAU staffs and students. The researcher identified unfair usage of the bandwidth among the users in AAU by using proxy log statistics analysis. Then he developed a dynamic bandwidth allocation algorithm based on user demand and bandwidth sharing. The main purpose of the target thesis is not bandwidth sharing among the users of the network rather resolving the performance gaps in the WAN by benchmarking the LAN performance of critical applications. Above all the network statistics is not taken from the proxy log files but from the devices that are actually running in the MoR data

centers which can show the overall network statistics of the organizations. Besides that, nothing is being done on the area of revenue office regarding bandwidth allocation problems and the leading remedies.

When we summarize the scope of the works mentioned in the related fields they are basically analyzing the given network environment to find the way to manage the bandwidth of that organization which leads to develop bandwidth allocation algorithms. Generally, Network performance analysis of existing traffic using the data collected from the networking devices in the datacenter can help to identify what is actually happening in the network, what are the bottlenecks, resource utilization the way of identifying, diagnosing and rectifying faults.

This thesis will be dedicated to answer the following questions

RQ1 -What are the suitable metrics to measure the performance of MoR network?

RQ2-What are the possible bottlenecks of the MoR networks that are hindering the performance of the overall network performance?

RQ3-What optimization framework can solve the performance bottlenecks?

1.3 Objective

1.3.1 General Objective

The general objective of this research is network performance analysis to propose possible optimization framework. The networking statistics collected from the MoR datacentre and its branches are analysed in detail in the way that can elaborate the possible cause of network problems of the organization. Then, the optimization framework is proposed based on the selected metrics.

1.3.2 Specific objectives

While accomplishing the main objective of the thesis, there are integral tasks that need to be done. The current network infrastructure is discussed to help us visualize the existing network of the organization. The other task is the suitable tools selection for data collection, analysis, and simulation of the existing network. The network problems are identified based on the data

analysis tasks. Finally the optimization framework is proposed that is assumed to lessen the identified problems.

The summery of specific objective is as follow:-

1. Understand the general network infrastructure of MoR
2. Selecting the suitable tools for the data collections and analysis stage.
3. Analysis of collected network statistics
4. MoR network simulation using modeller tools,
5. To assess the bottlenecks of MoR network based on the selected metrics , and
6. To propose possible optimization framework

1.4 Scope of the of the research

The scope of this is on the analysis of network connectivity issues of MoR network infrastructure to propose optimization framework. The data that will be collected from the networking devices, which consists the details of the network traffic, network bandwidth and network devices performance. The performance metrics selected for this work are related to network delay or latency, error and discards, availability, utilization, and protocol overhead.

1.5 Limitation of the of the research

Considering time and cost constraint, the end device and end user analysis is performed based on the MoR branches offices that are found in Addis Ababa region. Assuming all devices of MoR are connected to share resources from the main datacentre, the data collected from the SolaWinds can represent the overall communicating devices in the networks. Though the network performance can be affected by application and network problems, this thesis concentrate on network connectivity issues.

1.6 Significance of the thesis

The result of this paper can show major issues causing network dropouts, which need to be considered during replacement and upgrading plans by MoR management team and different level of system and network administrators. The organization can adopt the proposed optimization framework to optimize the performance of its network. This thesis believed to shift the usual method the organization where using to pinpoint the spots of the network problem

based on the real network environment data analysis that is taken from the communicating device, which can show their behaviour on the medium. Since any piece of network and server farm replacement is accompanied by huge investment, it needs to be supported by real network statistics and related data analysis results. Future discussion with Ethio telecom and others stakeholders can be MoRe fruitful, because the IT management teams concerns can be supported with the tangible situation of network infrastructure rather than routine assumptions which can lead to disputes.

1.7 Thesis organization

The thesis report comprises seven chapters. The first chapter introduces the general background of the thesis. The sub contents are problem statement, objective of the thesis, scope and limitation, and significance of the thesis.

The second chapter goes through the existing network performance literatures and related concepts that can capitalize the theoretical framework of the thesis. This chapter defines and discusses the concepts related to network and network performance optimization in details.

The third chapter deals with the methodology followed throughout the thesis to accomplish the main objective, which is design science. This chapter discusses the method for data collection, data analysis, tools for data analysis, sampling, the metrics, and metrics used.

The fourth chapter is about simulating and describing organizational profile of MoR, which includes the existing networking infrastructures details.

The fifth chapter deals with results and discussion based on the selected network performance metrics. The analysis is performed on the collected data from SolarWinds and other source. In addition, a simulation result from OPNET modeler tools is also incorporated for analysis and discussion.

The sixth chapter concentrates on the optimization framework proposed for the problems identified in the previous stages. The optimization framework consists of the optimization model, low level flow chart, and the algorithms.

The final chapter is about conclusion on the major findings and the leading recommendation that needs to be forwarded for MoR.

Chapter 2

2. Literature Review

The main aim of this chapter is to establish the theoretical framework of the thesis based on research dissertations, books, journal articles and other reliable source of documents. In addition, related terms and concepts are described that will be used throughout the paper.

2.1 Definitions

2.1.1 Networking

Network is computers and other devices connected in such a way that they can communicate with each other. Computers and related technological devices have gone enormous improvement ranging from a room-sized frame to smart tablet devices. Today's main challenge is diverted to connectivity and keeping the availability of the connection. A network in a simple form is a set of PCs and other devices connected using communication channels so that they can communicate to serve our purpose [2] [5].

The biggest benefit of networks is that facilitate resource sharing such as, shared data, making sharing information and working together easy for network users. Individuals and organizations can use networking infrastructures to centralize their operations and share those limited resources. Networks starting from data sharing it also let users share hardware resources, such as printers, so that you don't need a separate printer for each user, which has been a driving factor for both business and home networks. Networking infrastructure with such fascinating advantage some time may brought concerns if day to day network statistics is not analyzed and monitored based on those statistics. MoR is relaying on the network infrastructure to provide its service from centralized datacenter. The VPN connection between data center and the branch offices is handled by Ethio Telecom [2] [5] [1].

In a simple workgroup we find interconnected computers, printers, scanners, servers and so on. We can make this network availability possible by creating a networking environment that is being monitored based on the network devices and services performance analysis. What we are going to monitor for this case is the packet which is travelling across the network infrastructure of the given working environment. The packets or the data that is travelling in the network is named TCP

segment in transport layer, IP packet in network layer, Ethernet Frame in Link layer but it's commonly called packets [17]. Creating connection for every devices and services can also bring security concerns for our organization .The security concerns related to abuse of the overall network and information depicted us that network packets need to be analyzed to handle security threats [18] . Since MoR is handling taxpayers sensitive data's, analyzing the network statistics can help to minimize the security threats.

2.1.2 Bandwidth

Bandwidth can be defined as the rate or capacity of data transmission. It is measured in bits per second or hertz. Throughput describes the actual amount of information flowing through a Connection. Latency refers to the amount of time it takes for a packet to travel from one point on a network to another. A closely related concept is Round Trip Time (RTT), which is the amount of time it takes for a packet to be acknowledged from the remote end of a connection. Latency is measured as some amount of time, usually in milliseconds. Because bandwidth is a valuable and costly resource, demand usually exceeds supply. In many environments, uncontrolled access and usage of bandwidth results in degraded service for all users. This is partly a supply problem, partly a demand problem, and partly a technical problem [6] [7].

2.1.3 Network Protocols

Protocol is a recognized set of rules, conventions and data structure that oversees how computers and other network devices exchange information over a network. In other words, a protocol is a standard procedure and format that two data communication devices must understand, accept and use to enable successful communication [19].

Among the protocol suite TCP/IP is the major one for seamless communications for internetworking. IP and TCP are the main protocols that make up the TCP-IP protocol suite. The former is responsible to select the best path for the packet through the routers and the latter one is in charge of making the packets delivery reliable. LAN and WAN protocols are also critical protocols in network communications. The LAN protocols suite is for the physical and data link layers communications over various LAN media such as Ethernet wires and wireless waves. The

WAN protocol suite is for the lowest three layers and defines communication over various wide-area media, such as fiber optic and copper cable [19].

TCP

When we talk about network performance it may be characterized by its reliability, speed, fairness, and other factors. MoReover, it is not very easy to measure and determine whether or not a particular internet service is good. Despite the contribution of TCP or UDP protocols to the network performance there are limitations to network performance measurement tests today, observe how network measurement will need to adapt to a future of increasingly higher capacity links, as well as consider how to design network measurement methods for a world that requires ubiquitous network measurement. Our main discussion here is not how to measure or design the measurement but explain or point out the some of the issues. Let's discuss some of the factor by TCP to network performance [20] [5].

The TCP/IP protocol suite is the two transport protocols: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol which are responsible for a reliable a flow of data between two hosts. It is concerned with issues such as dividing the data passed to it from the application into appropriately sized segments for the network layer below, acknowledging received packets, setting timeouts to make certain the destination acknowledges packets that are sent, and so on. Because this reliable flow of data is provided by the transport layer, the application layer can ignore these details. UDP on the other hand provides a simpler service to the application layer. It sends packets of data called datagrams from one host to the other, but there is no guarantee that the datagrams reach their destination. Reliability must be added by the application layer [19] [20].

The IP protocol in the network layer is used by both TCP and UDP (User Datagram Protocol).

All TCP and UDP data that is transferred through an internet goes through the IP layer at both end systems and at every intermediate router. The ICMP (Internet Control Message Protocol) is an adjunct to IP. It is used by the IP layer to exchange error messages and other control information with the IP layer in another host or router. Although ICMP is used primarily by IP, it is possible for an application to access it. The two popular diagnostic tools, ping and traceroute use ICMP [20].

TCP is used by many of the popular applications, such as telnet, RLogin (Remote Login), FTP (File Transfer Protocol) and SMTP (Simple Mail Transfer Protocol or e{mail). The Domain Name System (DNS), the Trivial File Transfer Protocol (TFTP), the Simple Network Management Protocol (SNMP) and the Bootstrap Protocol [20].

2.1.4 Networking Architectures

Networking architecture is a guidelines and conceptual framework for designing, building and managing a communication networks. Architecture is the standard technology vendor's use while designing and building communication network whereas, protocols are the general rules used by the communicating networks. Commonly accepted networking standards are mandatory, because for any communicating devices in the internetworking there must be common governing rules that is known and obeyed by all parties regarding their definition and development. If we fail to follow the same standards the devices manufactured by one company may not communicate with the other devices manufactured some else in the world resulting incompatibility. TCP/IP network and Open Systems Interconnection (OSI) network architecture in the form of layered structure are the major ones in the communication networks. Layering is a modern network design principle which divides the communication tasks into a number of smaller parts, each part accomplishing a particular sub-task and interacting with the other parts in a small number of well-defined ways. Layering allows the parts of a communication to be designed and tested without a combinatorial explosion of cases, keeping each design relatively simple. The TCP/IP is basically the derived version of the OSI reference model which merges some layers of the OSI model, but the major operation framework is being the same [5] And [19].

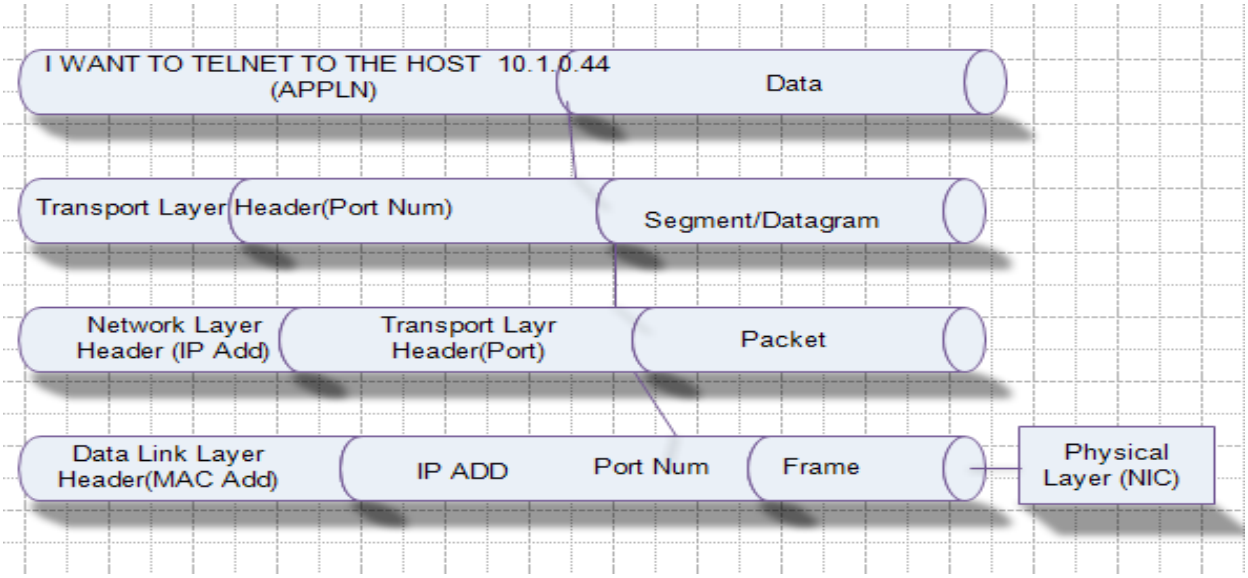


Figure 2.1.4-1 TCP/IP network architecture

2.1.5 TCP/IP Architecture

The TCP/IP network architecture open network architecture adopted by internet and it is adopted as a worldwide network standard and widely deployed in local area network (LAN), wide area network (WAN), small and large enterprises, and last but not the least, the Internet.

2.1.6 OSI Architecture

Open Systems Interconnection (OSI) network architecture, developed by International Organization for Standardization, is an open communication standards for varieties of technology vendors around the world. Though there are other standards; the OSI 7 layer architecture is the leading one. The OSI reference model uses layers to sub divide activities taken by network communication devices and assign each tasks to those layers.

Clear understanding can be achieved if we can see the layers 7 to 4 deals with end to end communication between sending and receiving devices , while the remaining layers 3 to 1 deals with deals with the communication between network devices. We can also see layers 7,6, and 5 as upper layer dealing with application which is applied in software and the 4, 3,2, and 1 as lower layers specially the physical layer and the data link layer which can be applied in software and the

hardware to handle data transporting tasks. Finally the physical medium is responsible to put the data on the destination devices [19].

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	Protocols Per Layers
5,6,7	Application, session, presentation	Application	NFS, NIS+, DNS, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP
3	Network	Internet	IP, ARP, ICMP
2	Data link	Data link	PPP, IEEE 802.2
1	Physical	Physical network	Ethernet (IEEE 802.3) Token Ring, RS-232, others

Table 2.1.6-1 protocols in TCP/IP and OSI architectures

2.2 Network Performance Analysis

Global network users can get instant news, communicate with others, use it as a super encyclopedia and find anything that they are interested in via search engines at their fingertips. Internet not only provides unprecedented convenience to our daily life, but also opens up new areas of disciplines and commercial opportunities that have boosted overall economy by creating many new jobs; above all in today's world mankind is being affected by the technological products so it's worth investigating the factors affecting the performance of the network [19] [2] [5].

Network performance analysis is also defined by Attamah as the creation and enforcement of network policies to ensure fair and satisfactory network performance. It becomes the tool used to ensure enough bandwidth is available to meet the traffic needs of those mission-critical and time-sensitive applications and prevents competition between these applications and lower priority traffic for the limited network resources. Network Performance monitoring encompasses methods, techniques, and tools for constantly monitoring the state of network, applications system and its usage, as well as for detecting, diagnosing, and resolving performance-related problems using the monitored data [8].

Network performance analysis can be better described in the five functions defined in the OSI Network Management Framework i.e., configuration management, performance management, fault management, accounting management and security management. Traffic monitoring is used in configuration management for tasks such as estimating the traffic demands between different points in the network, so that network capacity can be allocated to these demands. In performance management, traffic monitoring can be used to determine whether the measured traffic levels exceed the allocated network capacity, thus causing congestion or delays. When a fault occurs in the network, traffic monitoring is used in fault management to help locate the source of the fault, based on changes in the traffic levels through the surrounding network elements. In accounting management, traffic monitoring is needed to measure the network usage by each customer, so that costs can be charged accordingly in terms of the volume and type of traffic generated. Finally, network traffic monitoring can be used in security management to identify unusual traffic flows, which may be caused by a denial-of-service attack or other forms of misuse [3].

Timely correction of problems on a network is essential, because of the effect on user productivity and the desire for fast Service that is prevalent among users. Service level agreements also place a premium on timely resolution of network problems. Thus, the prior art techniques for monitoring of networks and identifying problems and their causes are not responsive to the requirements of the users and the business Served by the network. The prior art techniques are also not responsive to the needs of the network and/or System managers who are charged with accomplishing timely identification and resolution of problems [21] [9] [22].

Computer network is growing in an exponential speed, and one of the challenges for network designers is to provide a higher bandwidth and more reliable connection. Therefore, every component in a network needs to be optimized in order to achieve the highest performance While conventional gradient-based optimization algorithms require a smooth and uni-modal space, Genetic Algorithm (GA) does not have these limitations and is useful for solving combinatorial problems; therefore, GA has a great potential use for computer network and telecommunication applications. Although there are many variations of genetic algorithm customized for different applications, they all share certain common features that usually can be clearly recognized [23].

The book written by [2]emphasized the issues that must be addressed in order to predict application-level performance between two network end points, and thus provision enough

capacity to meet an application's performance requirements. The main issues they believed to be solved are modeling of the network traffic, network performance requirements, and models and techniques for optimal bandwidth allocation.

(1) Models of traffic demand between network end points. Models may need to be specified at both the call level (for example, users "arriving" to the network and starting up end-to-end applications) and at the packet level (for example, packets being generated by ongoing applications). Note that workload may change over time.

(2) Well defined performance requirements. For example, a performance requirement for supporting delay-sensitive traffic, such as a conversational multimedia application, might be that the probability that the end-to-end delay of the packet is greater than a maximum tolerable delay be less than some small value.

(3) **Models to predict end-to-end performance workload model, and techniques to find a minimal cost bandwidth allocation that will result in all user requirements being met**. Here, researchers are busy developing performance models that can quantify performance for a given workload, and optimization techniques to find minimal-cost bandwidth allocations meeting performance requirements [2].

The book by [2] described the time scale to which the packet flow is important while managing the traffic. He categorized the time scale to describe the time where network monitoring is critically important. The time scale are average rate , peak rate ,and burst size when he traffic reaches to the level it cannot be handled by the existing setup. The concept of network optimization is important mainly to handle the situation at the peak rate and burst size which can cause network congestion, delay, and loss of packet leading to network performance degrading; above all failure to provide the service we have promised for the customers demanding high quality service.

The Average rate is the time the network may limit the long-term average rate at which a flow's packets can be sent into the network. The main idea here is that knowing the time interval to monitor the average rate.

While the average-rate constraint limits the amount of traffic that can be sent into the network over a relatively long period of time, a peak-rate constraint limits the maximum number of packets that can be sent over a shorter period of time. The network may also wish to limit the maximum number of packets (the "burst" of packets) that can be sent into the network over an

extremely short interval of time. In the limit, as the interval length approaches zero, the burst size limits the number of packets that can be instantaneously sent into the network. Even though it is physically impossible to instantaneously send multiple packets into the network (after all, every link has a physical transmission rate that cannot be exceeded!), the abstraction of a maximum burst size is a useful one Fundamentally, the difficulty in supporting multimedia applications arises from their stringent performance requirements:- low end-to-end packet delay, delay **,** jitter, and loss and the fact that packet delay, delay jitter, and loss occur whenever the network becomes congested [2].

2.3 Network Performance Metrics

The existing network performance is affected by available bandwidth, network congestion delay, server performance, and the protocol as a whole. Network exact Performance analysis and prediction of performance patterns can be better achieved by looking at the operational network usage status. To enable us detecting, diagnosing, and resolving performance-related problems using the monitored data network performance metrics are required. The existing network performance is affected by available bandwidth, network congestion, delay, server performance, and the protocol as a whole [2] [24].

The Doctoral thesis by [25] on Performance monitoring in communication networks aimed at developing the most significant performance measurement for IP networks. The paper used both active and passive methods of network block data analysis. The Passive methods include sniffers, and well known traffic meters, also active methods, where dedicated probe packets are generated. The idea behind passive methods is to capture packets in order to collect and store information from various fields within the packet header. Traditional sniffers, protocol analyzers and traffic meters are all based on this principle. Well-known tools such as PRTG, solarWinds , Net-flow, are based on the passive methods of analysis. The parameters he used for his work are packet loss, Packet Delays and Delay Variations, and Throughput. Those parameters are employed to identify possible point of measurement of the mentioned metrics. Measurement data carried by the monitoring packets may be processed and stored by the originating entry node, the exit node, or by a dedicated stand-alone server. The difference between Number-Of-Sent-Packets in monitoring packet n and monitoring packet n-1 gives the number of packets sent in an monitoring block and

correspondingly for Number-Of-Received-Packets. Thus, the number of lost packets in a monitoring block is the difference between the number of packets sent and received. A sample of the transfer delay between a sending and a receiving node is given by the difference between Time-At-Receiver and Time-At-Sender in a monitoring packet. Lost monitoring packets are detected through missing sequence numbers.

Though it may not important to consider all network performance metrics for all network analysis purpose but there are common metrics that can be used for most of the network performance analysis purpose. Metrics which mostly affect the performance of both the LAN and WAN network performance are Latency, Jitter, packet loss, packet duplication, packer reordering, and throughput [26].

on his work bandwidth management in the era of bring your device recommend that using quality of service(QOS) and bandwidth management policies will enable network administrators to control network traffic flow so that appropriate users and applications get priority during the allocation of network resources. Then visibility, optimization, and control will be done [27].

Bandwidth, packet loss, latency and delay, congestion and response time are also used as the basic metric that can be used to measure the given network performance. The paper categorized the metrics in to availability, loss & error, delay, and bandwidth [28].

On his research automated System to Debug Under-performing Network Flows in Wide Area Networks which basically focus on effect TCP on the overall network performance. The paper want to show as delay or latency, TCP window size, and packet loss are the basic performance issues caused by the nature of TCP protocol. Transmission delay: It is the time taken to transmit all the bits in a packet on to the physical link. It depends on the link speed and packet size. For low speed links transmission delay is limiting factor while at high speeds propagation delay can be the limiting factor. The delay imposed by the speed of light in fiber. The TCP window size gives the maximum number of bytes that a receiver can buffer at a time [17].

The following sub topics will discuss the common metrics adopted by scholars worked on the thesis related to network performance analysis [6] [5] [27] [28] [9] [25] [3] [29].

The TCP window size

This window size means the maximum number of bytes that a receiver node can buffer at a time interval. The sender can send a maximum of window size bytes before waiting for acknowledgement from the receiver. The window size can be between 2 to 65,535bytes.

Packet loss

Packet loss examines how many data packets are dropped during data transmissions on your network. The MoRe data packets that are lost, the longer it takes for a data request to be fulfilled. A networks Transmission Control Protocol (TCP) interprets when packets are dropped and takes steps to ensure that data packets can still be transmitted. When users from branch office are requesting services of MoR datacentre the distance and the network instability contributes to packet loss. Packet loss refers to the number of data packets that were successfully sent out from one point in a network, but were dropped during data transmission and never reached their destination. Packet loss is taken us the performance metrics for a given network by comparing the rate of packet loss in the transmission medium for specific period of time. It is usually expressed as a percentage of the total number of sent packets. Often, MoRe than 3% packet loss indicates the service given is being compromised by different factors, but even just 1% packet loss might not be tolerated in a critical environment like MoR.

Bandwidth usage

Bandwidth is the maximum data transmission rate possible on a network. For optimal network operations, you want to get as close to your maximum bandwidth as possible without reaching critical levels. Randomly adding bandwidth without considering other factor that can cause network problem is just investing on something that cannot provide equivalent performance improvements. This indicates that your network is sending as much data as it can within a period of time, but isn‟t being overloaded. There are network monitoring tools that can monitor how much bandwidth is currently being used on a network, in addition the amount of bandwidth typically used during daily operations. The solution can also alert you when your network is using too much bandwidth.

Throughput

Throughput measures networks actual data transmission rate passing through the network from point sender to receiver on specific period of time. Throughput can be different on different point of the network considering the bandwidth, type of medium used, and the type of nodes participating in the communication system. The bandwidth is the amount of data size subscribed from ISP which may not indicate the actual data transfer rate in the working environment. Throughput shows the actual shows the amount of data size that moving in the communication channel. Definitely, throughput can represent the percentage of the data packet sent over that medium. If the amount of throughput is decreased its means the success rate of packet delivery is decreased or there are packets dropped or lost in the channel before being delivered to their destination. When referring to communication networks, throughput is the rate of data that was successfully delivered over a communication channel. Throughput is usually measured in bits per second (bps). The term "Internet Connection Speed" or "Internet Connection Bandwidth" is a common term used by ISP companies while bandwidth is subscribed.

Latency

Latency is the time delay that experienced between a sender and receiver devices requesting data and when that data is delivered. This delay can happen for a variety of reasons, but whatever the cause like network device problem, configuration problem, over utilization of the given medium, faulty software‟s and devices, et al. Consistent delays or odd spikes in delay time indicate a major performance issue; however, because delays can often be unnoticeable easily, we need monitoring tools to keep truck of those events between nodes.

There are several contributing factors for the delay encountered in transmitting a packet. The major delay problem that can happen in the LAN is bandwidth delay. It’s the time needed for a sender node to put the packet onto the wire. This is simply the packet size divided by the bandwidth, after everything has been converted to common units. For a 1500-byte packet on 100 Mbps Ethernet, the bandwidth delay is 12,000 bits / (100 bits/μsec) = 120 μsec. There is also propagation delay, relating to the propagation of the bits at the speed of light (for the transmission medium in question). This delay is the distance divided by the speed of light; for

1,000 m of Ethernet cable, with a signal propagation speed of about 230 m/μsec, the propagation delay is about 4.3 μsec.

Jitter

Jitter can be caused by network congestion. Network congestion occurs when network devices are unable to send the equivalent amount of traffic they receive, so their packet buffer fills up and they start dropping packets. In simple terms jitter is the variation of latency caused by the network. If there is no disturbance on the network at an endpoint, every packet arrives. When the buffer size arriving at the edge device gets full enough the packets arriving later may not delivery within expected time interval. The jitter problem can be noticed at the time of a video and audio communication. If the channel is experiencing jitter problem audio and video communications lacks quality problem on both ends of the users. The medium type we are using can be possible cause of jitter; especially the one that is shared.

Packet Reordering

The reordering problem happen when the packets following multiple paths are arrived out of order. Packet reordering happen for numerous reasons, such as multipath routing, route fluttering and wrong QoS queue configuration. It can be identified easily. Packet reordering problem in a given communication of audio and video may cause all of a sudden words in their sentences sound scrabbled and out of order. Packet reordering is dealt with by avoiding parallelism while sending the packets belonging to the same end-to-end flow.

Retransmission

When packets are lost, the network needs to retransmit it to complete a data request. This retransmission rate lets your enterprise know how often packets are being dropped, which is an indication of congestion on your network. You can analyze retransmission delay, or the time it takes for a dropped packet to be retransmitted, to understand how long it takes your network to recover from packet loss.

Availability

Network availability, also known as uptime, simply measures whether or not the network is currently operational. You can never guarantee 100% availability, but you want to be aware of any downtime that happens on your network that you weren't expecting. It's important to be alerted when the network goes down, which network monitoring tools will provide for you. However, you should also be able to discover your actual uptime percentage and how often your network goes down.

Connectivity

Connectivity refers to whether or not the connections between the nodes on your network are working properly. If there is an improper or malfunctioning connection on your network, it can be a major hurdle for your company. Ideally, every connection should be operating at peak levels at all times. However, performance issues like malware can target specific nodes or connections to affect performance in that specific area of the network.

2.4 Network traffic analysis and optimization Techniques

Network traffic analysis and management must be applied in a way that can address the end to end network communication bottlenecks and achieve increased network availability and minimized response time. Literatures related to network performance analysis and optimization framework followed techniques resembling the pattern of packet traffic classification to be used as input for the queuing and scheduling algorithms to decide the next packet for transmission without causing network congestion, then the output of this module is taken by the traffic shaping algorithms like lucky bucket and token bucket which can control the traffic rate on the given network infrastructure. There are also different modeling techniques to model the existing network which can help to propose optimization frameworks. The following paragraphs discuss those techniques followed by different scholars [9] [27] [2] [15]

The collaborative paper by [29] summarized the network performance optimization models and framework dealt with most of the scholars in the current complex network environment which they call it internet of things consisting of the communication of billions of devices and their medium as a whole. Optimization problem is made up of input factors, outputs, constraints and different objective function. Network optimization problem in IoT (Internet of things) comprises many parts

which will be combined using different combination and methods which address a particular type of network problem.
They found out two important methods for network related optimization:-

- Applying known optimization framework for addressing the problem.
- Scheming novel work based on a heuristic method for the problem., and
- Combination of the two methods for complex environments.

Experiential and for problems that are novel or new the scholars mentioned two kind of which are implement by using the power of the algorithm to find new pattern in the complex datasets of the network traffics. Approach consists of:-

- Algorithm which provides a faster approximation solution for more complex problem example, convex optimization
- Greedy approach which provides optimal solution by making assumptions.

They remarked that both approaches can provide optimal solution for complex problems and achieve performance near to optimal. Hence there won't be a single algorithm which provides optimal solution to network optimization problem in that complex network [29].

Both scholars [9] and [30]worked on the thesis that starts with managing the performance issues related to the protocols mainly TCP. Network Management and Traffic control deals with TCP congestion control avoidance and follow control of TCP. The next task is bandwidth Usage optimization which constitutes traffic management, Cashing, and Compression methods to smooth the flow of traffic. The other is bandwidth management techniques including Class Based Queuing weighted Fair Queuing, Fair Queuing, Priority Queuing, FIFO. Admission control and traffic shaping enable proper queuing and shaping of the traffic.

Among the toughest thesis I have reviewed the bandwidth Management and Monitoring for IP Network Traffic by [31] and ([8] introduced different techniques for optimizing the performance of the network to recover from the network bottlenecks. The paper mentioned ying-yang for congestion avoidance. He also mentioned traffic accounting strategies including network and host

accounting that can identify the statistics of the host and network in the way that can identify the abuse area. Another method of optimization is the Quota systems that assign a fixed amount of traffic for given user in a given period of usage. Finally he mentioned traffic shaping methods which includes Traffic queues and Quality of Service, Active Content Control, Limitation of Services, and Threshold management. Under traffic queues and Quality of Service the paper discussed First in First out, Weighted Fair Queuing, Fair Queuing Stochastic Fairness Queuing Token Bucket Filter Custom Queuing Priority Queuing

[9] On his paper which focuses on internet bandwidth management of institutions he identified different bandwidth management techniques. Among the techniques queuing and scheduling techniques, and admission control and traffic shaping techniques are the two broad categories for optimization techniques on the paper. For the queuing and scheduling techniques the FIFO(First in firs out) , priority queuing, Fair queuing, weighted fair queuing , and class based queuing are discussed. In the case of admission control and traffic shaping leaky bucket and token bucket algorithms are discussed.

The paper by [32] is also among the papers that want to answer the basic question behind network performance monitoring and the possible optimization techniques. He then outlined the network resource and budget, intrusion and virus detection, simplification of troubleshooting network services, enhance network performance, above all to enhance proper network usage are the basic reasons why we need to monitor our network. The researcher used cache optimization, Traffic shaping, Protocol tuning (TCP window size), DNS optimization, and Bandwidth accounting. Finally he recommends policy formation and the creation of awareness or the users.

There is also a paper done by group of scholars [30] to survey the bandwidth management techniques. In their way to survey the management techniques they have identified the main purpose of network management and analysis as reducing bandwidth requirements, tracking bandwidth uses, ensuring security, protecting business by disabling access of blacklisted sites, ensuring suitable allocation of resources among all workstations above all to optimize the quality of service. The paper mentioned scheduling and traffic shaping algorithms as the techniques that can be used to optimize the traffic in any kind of network environment. Besides this techniques

they have also depicted buffer management can be used to ensure the fairness connection while the queuing is performed. Among the protocol optimization methods the TCP optimization methods for window size mss-shrinking are also discussed.

Scheduling

When the packets arrive at network segment the need to be queued in the way that can facilitate they are transmitted to their specific destination. Queening can be handled by FIFO if we want the arriving packets to be exactly based on the order they are received on that node. The problem with FIFO is no distinction is made between network traffics, so the critical and the non-critical packets are treated equally.

The other methods is priority queuing which requires the packets to be classified in their priority queue , then the packets in the high priory class are transmitted first followed by the lowest priority class packets. The main drawbacks with this method are that the highest priority class may engulf the network inhibiting other class of packets from transmitting to their destination causing starvation.

In weighted fair queuing technique, the packets are still assigned to different classes and admitted to different queues. The queues, however, are weighted based on priority of the queues; higher priority means a higher Wight. The weight is given for the packets in each queue in a round –robin fashion with the number of packets selected from each queue based on the corresponding weight. Selecting weights 6, 4, and 2 means we can process six packets are processed from the first queue, four from the second queue, and two from the third queue. With these methods we can achieve fair queuing of the packets relative to the above methods. CBQ arranged in hierarchical manner. A top of hierarchical is the root queue which defines the total amount of bandwidth available. Child queues are created under the root queue, each of which can be assigned some portion of the root queues bandwidth [30] [32].

Bandwidth usage optimization

[9] And [8] proposed traffic management, cashing, and compression as bandwidth usage optimization techniques.

Traffic management is the ability of a network to ensure fairness in a network by guaranteeing that all users in the network receive at least a given amount for the inbound and outbound bandwidth.

Caching is the way of creating a temporary local storage for the frequently accessed user data's. The basic idea behind cache implementation is to accelerate the delivery of content as well as optimize the use of LAN bandwidth. There are different ways of implementing cache including local cache for browsers, proxy cache, datacenter cache et el.

Compression is a bandwidth management technique that is used to reduce the size of a file data to be transmitted through a network. In particular compression can make the network perform as if bandwidth has been increased

	Traffic management	caching	compression
Protect mission critical applications	Yes	No	No
Reduce bandwidth	No	Yes	Yes
Optimize bandwidth	Yes	No	No
Core or edge deployment	Core or edge	Edge	Core and edge
Cost of deploying	Variable	High	High

Table 2.4-1 Bandwidth usage optimization

Traffic shaping

Network performance optimization may not end up by only applying efficient scheduling algorithms, rather traffic shaping is also mandatory to control the amount and the rate of the traffic sent to the network. The two well-known leaky bucket and token bucket techniques are discussed as follow. Network performance analysis goal is to increase the efficiency and availability of the network while the congestion happens on the network [24] [30] [33].

Leaky-Bucket

This algorithm can be better understood by mirroring it with real world water container or bucket full of water. Creating a hole in a container full of water can brought the leakage of the water from the container irrespective of the amount of the water in the container. The input rate can vary, but

the output rate remains constant. Likewise, in networking, a technique called **leaky bucket** can smooth out burst traffic. Traffic chunks are queued in the bucket to be dropped in a constant fashion which may cause overall network congestion if not dropped. The leaky bucket is working on the assumption that host are authorized a given part of the bandwidth, so the algorithm strive to shape the coming traffic to enforced bandwidth policy in the specific network environment. We can also see that the leaky bucket may prevent congestion. The packets can be queued by using one of the scheduling algorithms we have discussed earlier to remove those burst packets at a constant rate. When the traffic consists of variable-length packets, the fixed output based on the number of bytes or bits.

The algorithm for this variable length packets scenario is shown below:-

- Initialize a counter to n at the tick of the clock.
- If n is greater that the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
- Reset the counter and go to step 1

Token-Bucket

The leaky bucket is very restrictive. It does not credit an idle host. For example, if a host is not sending for a while, its bucket becomes empty. Now if the host has burst data, the leaky bucket allows only an average rate. The time when the host was idle is not taken into account. On the other hand, the token bucket algorithm allows idle host to accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) 0f data sent. For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens

Now the host can consume all these tokens in one tick with 10,000 cells, or the host takes 1000 ticks with 10 cells per tick. In other words, the host can send burst data as long as the bucket is not empty.

The token bucket can easily be implemented with a counter. The token is initialized to zero. Each time a token is added, the counter is incremented by 1. Each time a unit of data is send, the counter is decremented by 1. When the counter is zero, the host cannot send data.

The-TCP-optimization

TCP provides a reliable end to end connection for traffic transmission irrespective of the status of the medium used in a network. This makes TCP connection oriented. TCP is also a reliable protocol since any data transmitted over the TCP is delivered accurately in the correct sequence and error free. The sequencing of packets is achieved by assigning a sequence number to each packet. These sequence number enables the destination node to accurately re-order any packets that arrive out of sequence. TCP features called flow control and congestion control that can be used to shape the network traffic.

Window size indicates the size of the devices receive buffer for the particular connection. In the window size represent how much data a device can handle from its peer at one time. For example serves window size was 360. This means the serves is willing to take to home than 360 bytes at a time from a client. Miss-Shrinking TCP sender always chooses the largest possible packet size. Max segment size, MSS typically ranging from 1000 to 1500 bytes such large packet require a along transmission time to be completely put on to the wire. When the WAN link bandwidth is narrow the long transmission time can block mission. Critical real time traffic such as VOIP, hence significantly degrade the quality of transmission [24] [30] [33].

2.5 Related works

Researchers have contributed different literatures regarding the optimization of performance optimization. The next topics will summarize the global and local scholar works on the network performance analysis and the leading optimization framework proposed.

2.5.1 Network Optimization Frameworks

The IEEE communication surveys and tutorials paper focusing on the wide area network optimization identified optimization method adopted by scholars. The paper listed compression, data de-duplication, caching, prefetching, and protocol optimization as the techniques and methods

for WAN optimization which mitigate the problems of latency, packet loss, and minimize bandwidth consumption [7].

The work of [28] to accomplish the objective of AAU bandwidth optimization is among the related work for the target thesis. The researcher collected the packet data using network performance monitor NPM tool from the AAU datacenter that helped him to identify the possible bottlenecks of the AAU network. The used the metrics availability, response time, and packet loss to analysis the data and finally proposed an optimization framework based on the traffic data analysis result. The researcher recommended the application performance measurement from the user side. The research is conducted in different network environment and organization. This paper is dedicated to analyze the network performance of the MoR datacenter specifically in Addis Ababa region to propose possible optimization framework.

The thesis by [15]is also performed in AAU with the same objective with that of [28] to optimize the network performance issues in the AAU datacenter. The difference is he used the log data collected by SAWMILL tool which he believed showed the resource usage in the campus network users. The result showed him the bandwidth is consumed by only 10% users. The then used the finding to develop the optimization framework based on the principles of quality of services. The gala of the target thesis is to analysis the network performance issues from the MoR datacenter using the network packet statistics exchanged between the network nodes which is collected using the SolarWinds and PRTG monitoring tools.

AAU network traffic usage statistics is collected using SARAG tools and analyzed by [34] to propose a quota based model that recommend for each user <256kbps in the university in order to make the bandwidth available for all users and to utilize efficiently and effectively.

[14] In the UNECA is also concerned on developing WAN optimization framework for the performance issues faced by the regional countries while accessing the resource from the head office. The researcher uses Net flow analyzer from the UNECA head quarter datacenter. His intention is to figure out the performance bottlenecks of the applications performance while they are accessed over the WAN specifically by the regional branches offices. The collected data is modeled by using the OPENT modular which is used to develop WAN optimization models that

can smooth the application performance gaps while used on the WAN. The target thesis is c conducted in different area concerning the network users, application types, and the organization business. The network performance analysis of MoR is mainly concerned on identifying the connectivity issues which are causing the network congestion, high response time, and packet loss.

2.5.2 Tools for Network modeling simulation and analysis

The Network Simulator provides an integrated, versatile, easy-to-use GUI-based network designer tool to design and simulate a network with working network protocols and the data collected from the active devices in the MoR datacenter specifically solarwinds network statistics.

Network simulator allows the researchers to test the scenarios that are difficult or expensive to simulate in real world. It particularly useful to test new networking protocols or to changes the existing protocols in a controlled and reproducible environment. Simulation can assist us to represent in a model the current working network topology including the devices connected end to end [35] [4]. Including OPNET which will be used by the target work will as main simulation tool to model the existing network in the MoR datacenter other simulation tools are discussed in the following paragraphs.

OPNET: It is extensive and powerful simulation software with wide variety of possibilities to simulate entire heterogeneous networks with various protocols. It is an application that simulates Cisco Systems networking hardware and software and is designed to aid the user in learning the Cisco IOS command structure.

NS2: NS2 is a discrete event simulator targeted at networking research. It provides support for simulation of TCP, routing, and multicast protocols over all networks (wired and wireless).

NS3: NS3 is also an open sourced discrete-event network simulator which targets primarily for research and educational use. NS3 is licensed under the GNU GPLv2 license, and is available for research and development.

OMNET++: It is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators.

JSIM It is a Java-based simulation system for building quantitative numeric models and analyzing them with respect to experimental reference data. JSim is an application development environment based on the component-based software architecture.
QUALNET: It is a commercial version of GloMoSim used by Scalable Network Technologies for their defense projects.

REAL: It is a network simulator originally for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks. It provides users with a way of specifying such networks and to simulate their behavior

we observed that before an enterprise network is constructed, during the design phase of an enterprise network, creating enterprise network scenarios using a reliable simulation tool, like OPNET, and designing the enterprise network in the virtual environment, simulating the use of network applications and different network traffics, and verifying designs provide cost and time savings. The target thesis will use the OPENET tool to simulate the MoR network traffic and build a network model. OPENET has rich and comprehensive development features to build and design the real world network traffics. OPNET provides a environment which is scalable enough for development of communication network and distributed systems by performing discrete event simulation, performance and behavior of the network is calculated. It works in the three main modules: modeling, simulation, analysis of network. For modeling of a network OPNET uses GUI(Graphical User Interface) as it provides a network with its all the components in graphical format. This simulator constitutes features that can support different vendors and network platforms. We can model communication network and results visualization and interpretation is easier than other tools.

Chapter 3

3. Methodology

The methodology is the how of the thesis. It consists of the procedures and methods we may follow to accomplish our objectives. It can also be "a system of principles, practices, and procedures applied to a specific branch of knowledge. Design science creates and evaluates IT artifacts intended to solve identified organizational problems Generally it consists of the process of motivating, developing, and designing, demonstrating, evaluating, and communicating the artifact [36].

The most important of design science methodology is that the research must produce an artifact created to address a problem. Such artifacts may include constructs, models, methods, and instantiations (representation) in short; this definition includes any designed object with an embedded solution to an understood research problem.

The research by [36]done on the design science research methodology which aim to form a standardized process model used by different researchers. Finally they devised a commonly accepted framework for carrying out research based on design science research principles. The framework consists of process model consisting of six activities as shown in the following figure.

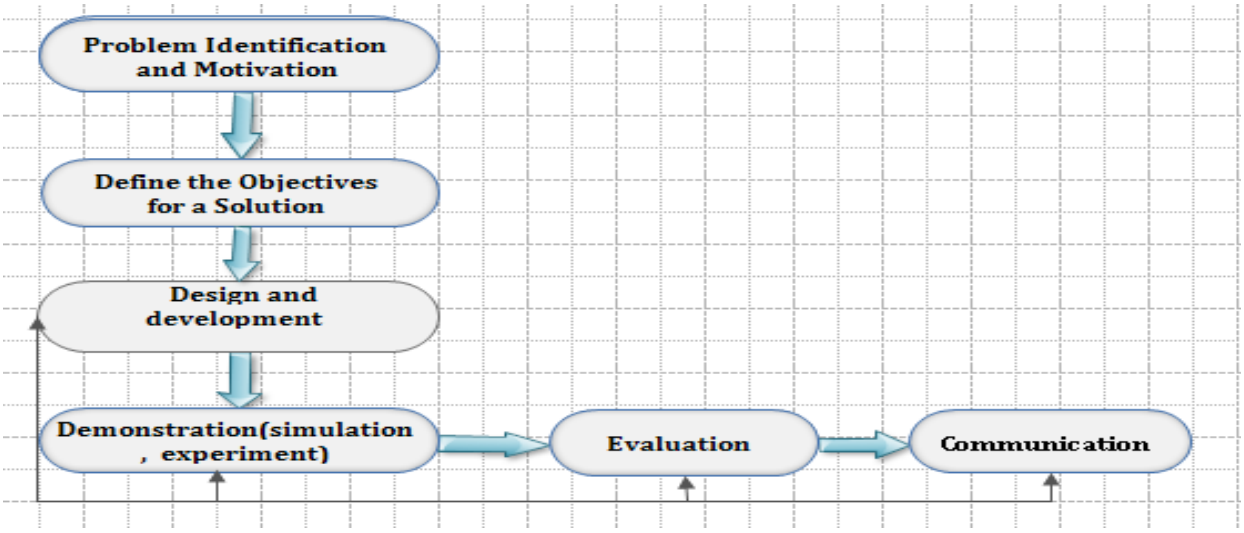


Figure 3-1 Design science process model [36]

Problem Identification and motivation (problem statement and data collection):- It deals with clearly stating the problem and justifies the value of a solution. Clearly specifying the problem statement is mandatory, which can assist during the artifact construction. The other point here is justifying the value of a solution to motivate the researcher and the audience of the research to pursue the solution and to accept the results and it helps to understand the reasoning associated with the researcher's understanding of the problem.

Define the objectives for a solution: - This phase of design scene methodology is concerned with deducing the objectives of a solution from the problem statement and possible solutions that can be archived. The objective can be quantitative and qualitative. The quantitative objective can be used to compare the existing solutions with target inventions. The qualitative objective can be description of how a new artifact is expected to support solutions to problems not previously addressed. The objectives need to align with the problem statement or the questions raised in the problems statement need to be solved.

Design and development (Analysis, Synthesis, or Development):- The goal of this phase is to create the artifact. The artifacts can be potentially constructs, models, methods, or instantiations or "new properties of technical, social, and/or informational resources. Conceptually, a design research artifact can be any designed object in which a research contribution is embedded in the design. The artifact development activities includes: identifying the major functionality and the leading architecture to create the artifact. The development of the artifact means giving the real meaning for the defined objective in the previous stages of the design science methodology.

Demonstration (simulation, experiment):- It's about describing the use of the artifact to solve one or more instances of the problem. This might encompass its use in experimentation, simulation, case study, proof, or other appropriate activity. To demonstrate the artifact effectively, having the knowledge of the artifact for solving the given problem is mandatory.

Evaluation (Observe how effective, efficient Iterate back to design):- This phase wants to check the concurrency of the artifact with the defined objective. This activity involves comparing the objectives of a solution to actual observed results as shown in the demonstration. This phase

requires defined metrics and data analysis ability. The artifact evaluation may be performed in different ways depending on the problem types. It comprises of as assessment of the artifact functionality against the solution objectives, the customer satisfaction collected from survey or simulations done, and system performance like response time and availability

Communication: - Informing the practicing professionals on the importance, of the artifact, its utility and novelty, the rigor of its design, and its effectiveness. In scholarly research publications, researchers might use the structure of this process to structure the paper, just as the nominal structure of an empirical research.

3.1 Data Collection

The data is collected from the devices found in the MoR datacentre mainly from switches, core switches, routers, firewalls, end devices, and other management software's for 6-month periods of 2020/21.

The tools used for network data collection are PRTG and SolarWinds. The data collection and analysis procedure are aided by PRTG and SolarWinds, which are network monitoring tools chosen for this work.

The collected data is selected for analysis by purposive sampling methods to choose suitable time and nodes that believed to represent the overall network behaviour. Purposive sampling is a kind of non-probabilistic sampling methods. It is mostly used for the type of data that requires the judgment of the researcher to select the valuable sample point. Since the collected data at different point of the network represent different behaviours of the communicating devices, selecting the data that can resemble the overall communicating device behaviour based on the purposive sampling is preferred. Additional data's is collected from the network administrators department by using interviews and holding discussion groups.

3.2 Tools for data collection

For the purpose of data collection SolarWinds and PRTG tools are used. Though they are not using it for network monitoring, solarwinds is already installed in one of the MoR datacentre server. In addition to the SolarWinds PRTG tool report from Ethio Telecom and Addis Ababa Revenue offices will be used to collect the network statistics in more details format.

Attributes that are related to the MAC address and IP address are removed from the report assuming the security concerns and to align with the company data usage norms. In addition to Excel the network dataset is analysed using SolarWinds and Excel. . SolarWinds is configured with the capability to compare the network nodes and devices based on defined parameters. The reporting the tool is also arranged in the way that can show the basic metrics, which are used to measure the performance of the network such as: - availability, response time, utilization, error and discards, and device alerts.

Some of the generated reports consist of graphs and percentage of utilization to help the administrators to view the general performance of the device installed in the datacenter. Those reports are analyzed using Mss Excel by forming graphs, average, and other statistical tools supported by excel.

3.3 Tools for data analysis

After those data are collected and the data understanding for common pattern is finished, the analysis is will be performed by using the SolarWinds and PRTG tools which can be used for simulation and modeling are inducted by using OPENT tool. After the data is collected and analyzed for possible gaps then the modeler tools will be used to model the network. The data we collected from the tools are expected to show different statistics like the heaviest interfaces, the most popular, available bandwidth, and packet loss, latency, and overall availability, amount of inbound or outbound traffic close to our available.

3.4 Network Performance metrics

It's desirable to identify network bottlenecks, determine the basic causes for the problems, before customers' service delivery is affected. These monitoring and diagnostic capabilities are critical to today's computer networks, since their effectiveness determines the quality of the network service delivered to customers. The most important performance metrics that are monitored include connectivity, delay, packet loss rate, and available bandwidth [1].

- Network connectivity is probably the most important metric for a network monitoring and diagnosis system, since the top priority of a network service is to guarantee that any pair of end nodes can communicate with each other. Due to its importance, all network

layers, starting from the physical layer, provide mechanisms to automatically monitor network connectivity.

- Network delay is perhaps the most widely used performance metric in today's network applications. It is monitored mainly at the end-to-end level using ping. Network delay can be used to directly evaluate network path performance, especially for small data transmissions.
- Packet loss rate refers to the probability that a packet gets dropped on a network path. It is mainly monitored at router interfaces using SNMP packet statistics. For ISPs (Internet Service Providers), since packet loss rate is a key marketing metric, a lot of monitoring and diagnostic effort is devoted to reducing packet loss. For applications, however, packet loss rate does not always significantly affect the performance of data transmissions. For example, single packet loss has a very limited impact on bulk data transmissions that use state-of-art TCP protocols.
- Available bandwidth is another important performance metric, which directly captures data transmission speed. Although network delay can be used to evaluate the performance of a network path for small data transmissions, the available bandwidth metric is needed for larger data transmissions. However, available bandwidth is much less popular than the delay metric due to its high measurement overhead. People instead use the link load metric, which can be more easily measured (e.g., using SNMP), to capture available bandwidth information.

Chapter 4

Experimentation and Business Understanding

This chapter will cover overview of MoR network infrastructure and the procedures and the basic content of the experimentation environment on the network data collected from the target devices.

4.1 MoR

MoR is a government organization entitled by federal income tax proclamation NO.286/2002 to levy and collect inland and custom taxes from different services and sales. Custom and Domestic tax collection was administered in one management framework named ERCA before its substituted by MoR which brought domestic tax collection for MoR and establishment of custom commission to administer the custom related tax collection. It is established with a Vision to be a leading, fair and modern Tax and Customs Administration in Africa by 2020 that will finance Government expenditure through domestic tax revenue collection. MoR mission is to contribute to economic development and social welfare by developing a modern Tax and Customs Administration that employs professional and highly skilled staff who promote voluntary compliance amongst individuals and businesses, and take swift action against those who do not comply [13].

MoR is striving to implement modern tax administration. Modern tax administration is dedicated to promote compliance tax payers and discourage non-compliant tax payers. MoR is using different technological outputs to automate collection of tax. Among those systems implemented to Inland Revenue management SIGTAS is the critical application besides those supportive sub-systems for receipt management, third party data management, report management, sales and cash register machine management. SIGTAS constitutes Tax roll, Doc/Files, Remittance, payment, ---8---modules with distinct functions. Tax roll is the main module to register the taxpayer and deliver different certificate according to the customer request. The document/file module is responsible to register the taxpayer self-declarations according to the tax period. The declaration is captured according to their line for further assessment using capture remittance module. Finally the payment is made using the capture payment module to collect the payment form the tax payers. The main tasks handled by SIGTAS are:-

- Registration of student , employees , Individual and non-individual taxpayers
- TIN generation to uniquely identify tax payers.
- VAT, Clearance, Excise Tax, TIN certificate generation.
- Tax account creation for VAT, TOT, Sch-C , Etc.
- Presumptive tax management
- Remittance capturing for grade A and Grade B tax payers.
- Tax assessment and Assessment notice creation
- Refund management
- Payment collection
- Audit and objection case management.

MoR is in a continuous transformation to bring the changes that deserves the tax payers for saving their time and cost. MoR is establishing different branches nearest to tax payers. There are 12 main federal and Addis Ababa branch offices of MoR dedicated for domestic revenue collection which are:- LTO ,MTO, East , West , North West, Jimma, Adama, Diredawa, Hawasa, Gambella ,Bahidar, and Mekele by excluding the 9 regional branch offices dedicated for individual tax collection. The number of active domestic taxpayers throughout the country whose grade is labeled A and B are exceeding 500,000 based on MoR warehouse and SIGTAS reports. Since our scope is on MoR branches for domestic revenue collection residing in Addis Ababa region, the focus of the thesis will be on those 6 branch offices. The six branches are LTO for large tax payers, MTO for medium tax payers, North West, East, West, and Addis Ababa Revenue Bureau. These branch offices are scattered in different corner of the city to provide those services closer to the customer [13] [12].

4.2 MoR network Infrastructure

MoR datacenter is serving as a central point of link for database and network connection for all domestic, custom, and regional revenue branch offices. Those links coming to the datacenter can be subdivided as MoR VPN links, third party links, and DMZ links for internet related connections.

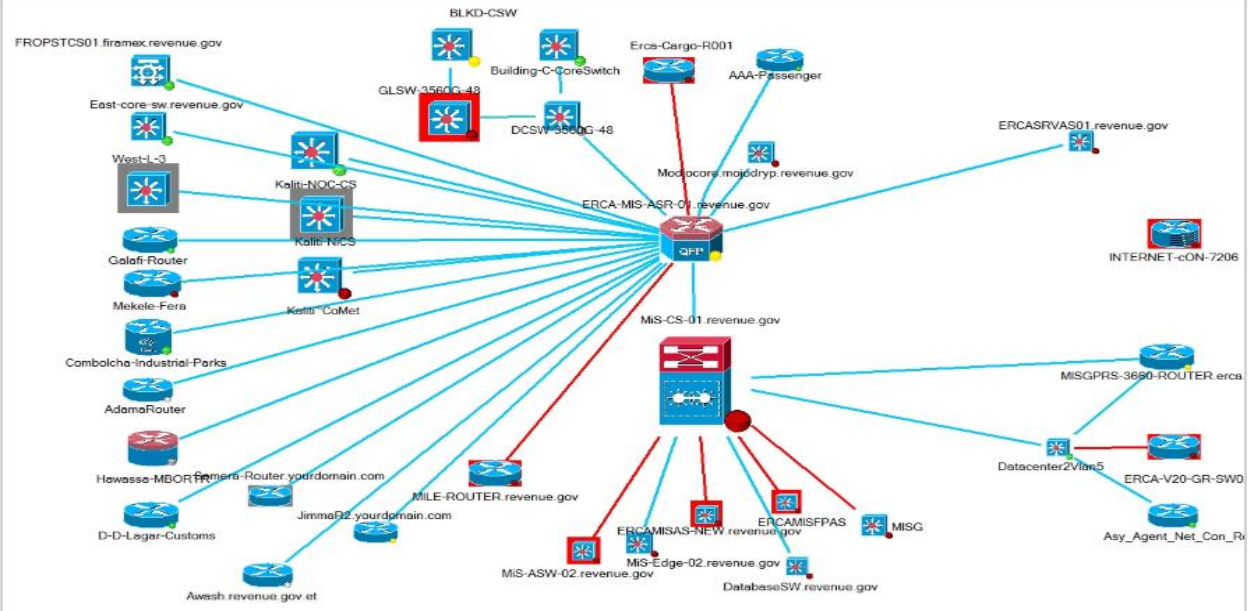


Figure 4.2-1 Current network design of entire MoR branches

MoR VPN Links (Data links)	Third party links	DMZ (Internet)
-All links coming from domestic and custom branches. • Main branch and sub-branch offices are exceeding 60 links	-NBE(National bank of Ethiopia), cargo tracking, MOFED , Commercial Bank of Ethiopia for DERASH service Ministry of Trade, DTI(transitory data), Single window	-Internet services , E-filing and E-payment platforms

Table 4.2-1 MoR network links types

The above table shows almost all Federal government tax and customs revenue collection is dependent on this datacenter. The 24/7 availability of database and network services in this datacenter is mandatory. As mentioned above all those 542,260 taxpayers need to access the resources from MoR datacenter to accomplish their tax duty through SIGTAS. Robust and fault tolerant network and system infrastructure is required to handle those customers. Continuous availability of the network services can be assured by monitoring the network traffic of those branch offices in the data center that enable us to identify the day to day network status and locate the major bottlenecks before it gets worsen.

The network connection between MoR datacenter and branch office is handled by Ethio Telecom. MoR subscribed Ethio Telecom broadband of speed 400 mbps for data connection and 300 mbps for internet connections. The 6 target branch offices also subscribed broadband VPN of speed 60

mbps to access resources from the main datacenter through their edge router. The network communication between the main datacenter and those branch offices is established once both parties configured with the parameters placed in Ethio Telecom ERCA-Net VRF. The data center is using LAN IP of 10.1.0.0 for domestic related services and 172.17.0.0 for custom related services.

As shown in the Figure_1 Ethio telecom subscribed VPN broadband data line is connected to the layer_3 switch using the WAN IP which serves as a bridge. Then interface of layer_3 switch is configured with short IP which enables links with the two redundant ISA routers for and the core switchers for load balancing. The routers are redundantly connected with the cisco core switches where all the VLANs and distribution layers information is configured. The third party and DMZ connections are established through the core switches. Finally the core switches are connected with other distribution layer switches based on their access privilege from different VLANs. After the connection is finalized more than 50 high end server farms exists with brands of Dell, HP, NEC, Sun, etc.

Branch	**Specific location**	**Num. of net.**	**Net. devices used**	**Subscribed Speed Mbps**	**Win. platforms**	**Num. of A,B tax payers**
LTO	Saris round Yoseph Mulege Building	340	Cisco L2 for distribution and L3 as router	60	Win 7/10	652
MTO	Round Kazanchis Manahariya	360	Cisco L2 for distribution and L3 as router	60	Win 10	3,613
EAST	Megenanya near to Lem Hotel	375	Cisco L2 for distribution and L3 as router	60	Win 7/10	9,775
WEST	Lancha round Global Hotel	350	Cisco L2 for distribution and L3 as router	60	Win 7/10	9,556
North WEST	Lideta round Lideta court	370	Cisco L2 for distribution and L3 as router	60	Win 7/10	5,842
AA Rev. Bureau	Mexico In front of AU	220	Huawei and Cisco L3 as a router and Cisco L2 as distribution	50	Win10	257,225
All Regional state Revenue Offices			Mixed use	10-20mbps	Win7/8	210,047
Total	1,795 computer and network users (AA and Federal only)				~ 527,260 Domestic-tax payers	

Table 4.2-2 MoR branch offices in Addis Ababa

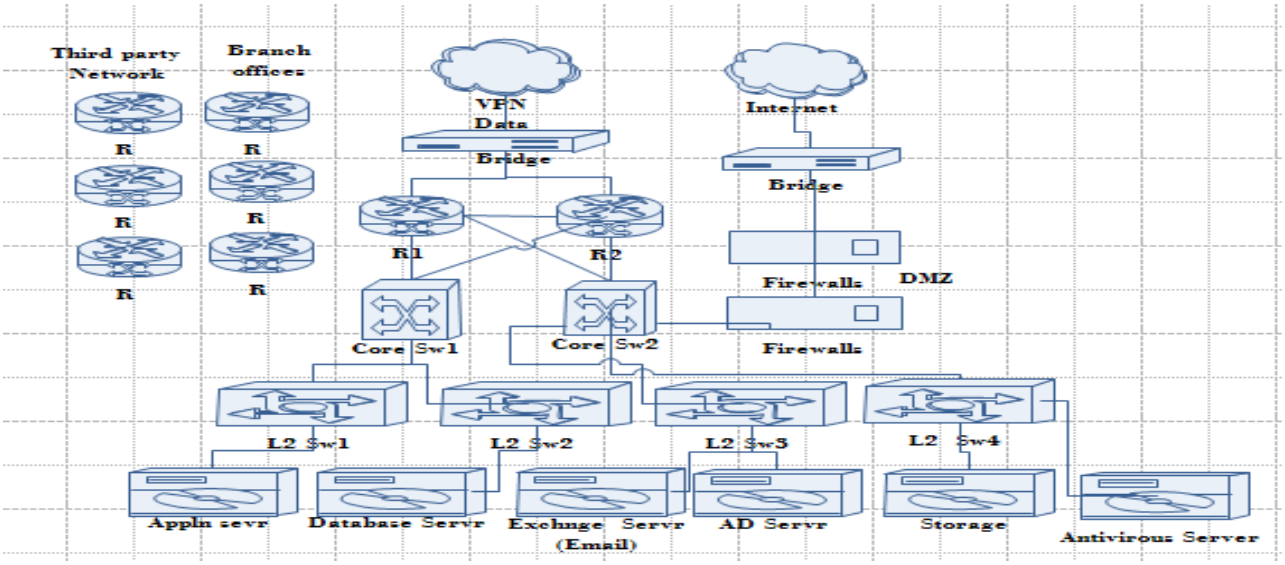


Figure 4.2-2 Summery of MoR network Architecture

4.3 Critical application performance

From the overview section we have mentioned SIGTAS and other supportive systems as critical applications which are being accessed using the data and internet line. The critical applications are identified by interviewing the network and system administrator department of MoR. The commonly mentioned application performance issues especially at the end of each tax period by the branch office SGTAS users and customers are: - continuous system dropouts, unable to generate reports, system too busy to perform a given operation, difficulty login to the system, TIN validation is awaiting long time, carry forwarding and other transaction balancing problems, and etc. MoR IT directorate is taking different actions to handle the specified problems. Following gaps and increased complains from the customers, they have upgraded the capacity of their server and other datacenter hardware infrastructures accordingly. In addition, the broadband subscription from Ethio telecom is also upgraded to 400mbps which they assumed can ease the performance issues. The missing point behind the existence of those gaps after the mention mitigation task is that network and application performance gaps need to be analyzed based on the network traffic passing the datacenter. The network traffic performance analysis can help us predict the network bottlenecks which may bring the performance degradations [11].

4.3 Data collection and understanding

To achieve the objective of this paper network statistics data is collected from different sources using passive monitoring techniques. Solar winds monitoring tools is installed in MoR datacenter. Solar wind collects the traffic of edge, core, and distribution layer of selected devices using configured sensors of the network interfaces. SolarWinds collect and generate the report for the CPU usage, memory usage, average response time, top 20 interfaces by current traffic, top 20 interfaces by CPU load, traffic from interfaces, top errors and discards and other related statistics for configured devices. Even if, it's possible to collect all related data's from the monitoring tools only some of the data's from the selected interfaces is selected for this paper. In addition to solar winds data also collected from the simulation tools and PRTG monitoring tools report from Ethio telecom and Addis Ababa city revenue bureau for selected branch offices is collected and used as well. Besides the traffic data from network monitoring tools, interview with the network and system administrator department is conducted.

The responsibility of connecting entire network segments to the MoR datacenter is handled by Ethio Telecom. Those branch offices are already subscribed broadband data line to their specific location which enables them to connect to MoR datacenter through Ethio Telecom network infrastructure. After VPN data client is configured for specific branches on Ephon bridges by Ethio Telecom technicians using WAN IP and LAN IP , the remaining configuration that enables internal LAN to access the MoR datacenter infrastructure is done by MoR Network Administrators on the routers using that branch specific LAN IP. Finally to enable resource accessing from MOR datacenter the distribution layer 2 switches which are connected to the routers through their up links are used to connect those end nodes.

The VPN line from Ethio telecom is connected to the L3 Bridge using the short IP on the Interfaces G/0/51 and 52. Then the G/0/52 is connected to the ASR1 router on port G0/0/2 and the 51 is connected with the ASR2 on G0/0/0/2 for redundancy. The ASR routers are then connected to the core switches named CS1 and CS2. ASR1 on port G0/0/0 is connected to CS1 on port G2/15 and ASR2 on port G5/17. MoR_DC_local is the MoR head office local network connection including its floor.

4.5 The Active Core Switch (CS1) ports connection details

- Ports G2/23 and 24 on CS1 are connected to CS2 for redundancy.

- Port G2/1 of CS1 is connected with the DMZ router G0/1
- Port G2/19 and 20 are connected to server farm with SW2on port G0/45 and 46
- Port G2/12 and 13 are connected to server farm with SW3 on port G0/45 and 46
- Port G2/21 and 22 user switch SW1 G0/1 and 2
- Port G2/10 and 11 to Temp SW1 G0/1 and 2
- Port G2/17 to management SW on port G0/48
- Port SW3 GPRS (Gi0/8) , DTI(Gi0/42) , Cargo(Gi0/41)

Network device descriptions

Nodes	IP VERSION	VENDOR	MACHINE TYPE
aa#1-core-sw	IPv4	Cisco	Cisco Catalyst 3560-G24PS
blkd-csw	IPv4	Cisco	Catalyst 37xx Stack
building-c-coreswitch	IPv4	Cisco	Catalyst 37xx Stack
cc-awash-r.revenue.gov.et	IPv4	Cisco	Cisco 1941K9
cc-jjga-r.yourdomain.com	IPv4	Cisco	Cisco 1941K9
cc-kaliti-cs	IPv4	Cisco	Cisco Catalyst 3650-48PS-E
cc-mil-r.revenue.gov	IPv4	Cisco	Cisco 1941K9
CC-Mojo-CS.mojodryp.revenue.gov	IPv4	Cisco	Catalyst 37xx Stack
CivilS-Erca.yourdomain.com	IPv4	Cisco	Cisco 1941K9
Comb-ZXR10-R	IPv4	Shenzhen Zhongxing Telecom Co.,ltd.	Shenzhen Zhongxing Telecom Co.,ltd.
CS-DC2950-24	IPv4	Cisco	Cisco Catalyst 2950t 24
DatabaseSW.revenue.gov	IPv4	Cisco	Cisco Catalyst 2960-24TC
ERCAMISAS-NEW.revenue.gov	IPv4	Cisco	Cisco Catalyst 2960-24TC
ERCA-MIS-ASR-01.revenue.gov	IPv4	Cisco	Cisco ASR 1001-X Router
ERCAMISFPAS	IPv4	Cisco	Catalyst 355024 PWR
ERCASRVAS01.revenue.gov	IPv4	Cisco	Cisco Catalyst 3560-G48PS
FROPSTCS01.firamex.revenue.gov	IPv4	Cisco	Cisco WS-C4506
GelanRW.yourdomain.com	IPv4	Cisco	Cisco 1941K9
GLSW-3560G-48	IPv4	Cisco	Cisco Catalyst 3560-G48PS
Gprs-R.erca.gov	IPv4	Cisco	Cisco 3662 Ac
INTERNET-cON-7206	IPv4	Cisco	Cisco 7206 VXR
JimmaR2.yourdomain.com	IPv4	Cisco	Cisco 1941K9
Kaliti~CoMet	IPv4	Cisco	Cisco Catalyst 3560-G48PS
localhost	IPv4	VMware Inc.	VMware ESX Server
MiS-ASW-02.revenue.gov	IPv4	Cisco	Cisco Catalyst 2960-Plus 24TC-L Switch

MiS-CS-01.revenue.gov	Cisco	Cisco WS-C4506	
MiS-Edge-03	IPv4	Cisco	Cisco Catalyst 3560-G48PS
MISG	IPv4	Cisco	Cisco Catalyst 2960-48
MoR-ADMA-R	IPv4	Cisco	Cisco 1941K9
MoR-DS2.MoR.local	IPv4	Cisco	Cisco
MoR-EAST-CS.revenue.gov	IPv4	Cisco	Catalyst 37xx Stack
MoR-HWSA-R	IPv4	Cisco	Cisco 1751
PostofficeRW.yourdomain.com	IPv4	Cisco	Cisco 1941K9
ZTE Router	IPv4	Shenzhen Zhongxing Telecom	Shenzhen Zhongxing Telecom Co.,ltd.

Table 4.5-1 Device details

The reports generated for average response time, top traffic utilization, and top errors and discards are selected that are believed to describe the existing network traffic status.

4.6 Tools and metrics

To investigate the existing bottlenecks on the datacenter and the overall branches network simulation of the network traffic is done using the OPENET modeler tool. The basic configurations, interface statistics, network topology, device details, and other selected information from solarwinds report are used to build the model. The metrics response time, delay, throughput, and reliability are selected to be tested on the model. Response time can be used to identify the time of specific nodes to answer a given request from a remote client and vice versa. The higher the response time, there will exist network dropouts and delay of the requested packets to the destination node. Throughput is the actual traffic transfer rate in the network. Throughput measures the actual data being sent over the network. The capacity of the network medium to transfer the network traffic data and the theoretical subscribed broadband speed need to be balanced. The other metrics that will be tested is reliability of the target network to check if the network is consistently operating when facing different scenarios.

4.7 Introduction to OPNET

It is originally developed at MIT, OPNET [11] is a network simulator allowing researchers to design and study communication networks, devices, protocols, and applications. An OPNET simulation package includes three main graphic editors – network editor, node

editor, and process editor. The network editor manages network topologies; the node editor controls network devices' performance; the process editor implements protocols, resources, applications, algorithms, and queuing policies. These three editors work together to provide various simulation environments

The simulator can be used for traffic modeling of telecommunication networks, protocol modeling, modeling queuing networks, modeling multiprocessors and other distributed hardware systems, validating hardware architectures, evaluating performance aspects of complex software systems modeling any other system where the discrete event approach is suitable.

4.8 Simulation Setup

MoR network architecture on the simulation have 30 subnets for each branches of network. Subnets assigned based on the current network infrastructure and all the network equipment exactly matched from the real environment.

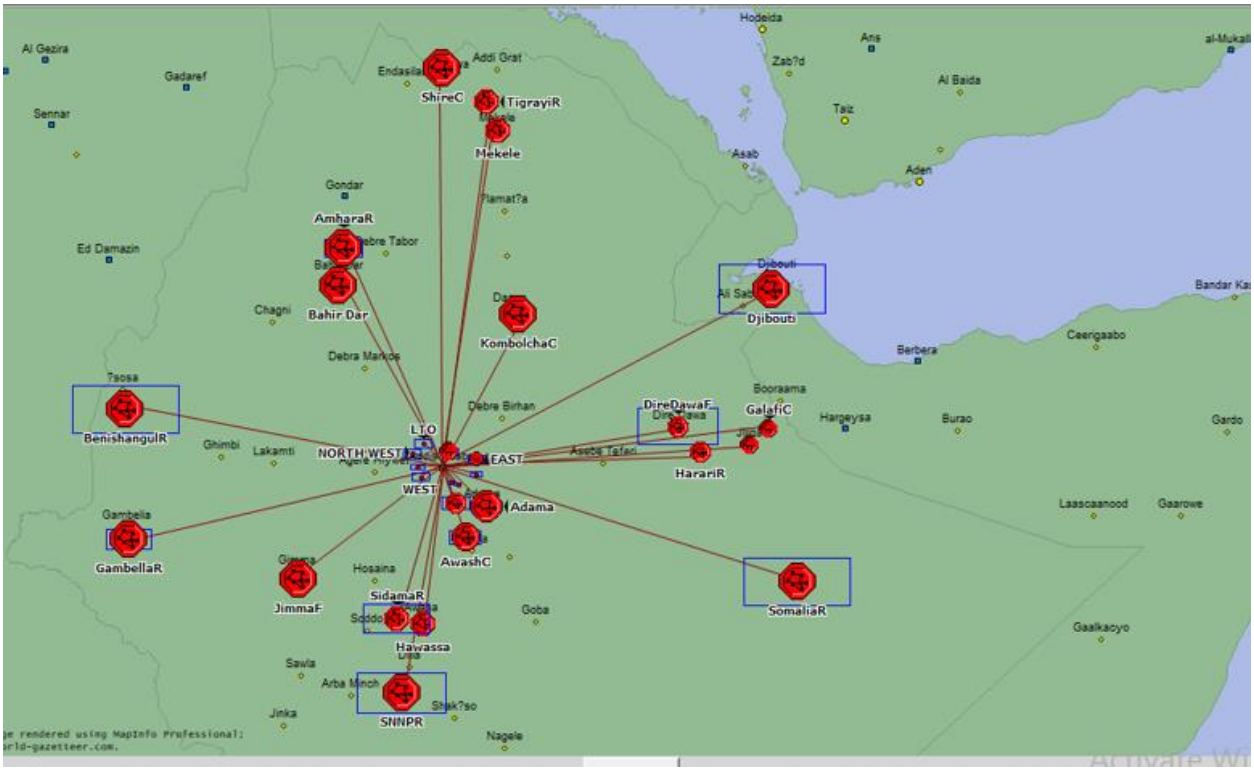


Figure 4.8-1 MoR Network Architecture on Simulation Environment [Parent Subnet]

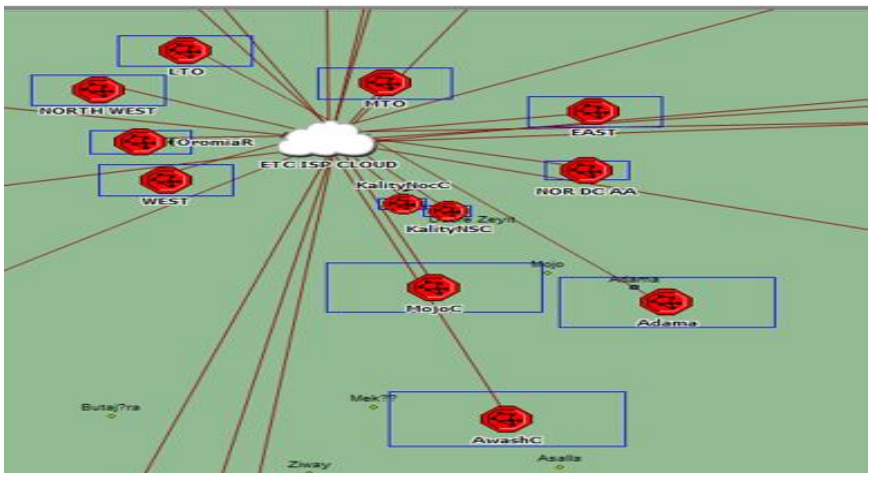


Figure 4.8-2 MoR Network Architecture on Simulation Environment [Central Subnet]

4.8.1 Network Components

This section discusses about the network components and models used on the simulation environment to represent the actual network.

- Ethernet2_slip8_ler(Label Edge Router) and ethernet2_slip8_lsr(Label Switched Router) node models are used to represent an IP-based gateway running MPLS and supporting up to two Ethernet interfaces and up to 8 serial line interfaces at a selectable data rate. IP packets arriving on any interface are routed to the appropriate output interface based on their destination IP address.
- Ethernet16_switch node model is used to represent a switch supporting up to 16 Ethernet interfaces. The switch implements the Spanning Tree algorithm in order to ensure a loop free network topology. Switches communicate with each other by sending Bridge Protocol Data Units (BPDU's). Packets are received and processed by the switch based on the current configuration of the spanning tree.
- Ethernet_wkstn_adv node model is used to represent a workstation with client-server applications running over TCP/IP and UDP/IP.
- 10BaseTand 100BaseTduplex links are used to represent the Ethernet connections operating at 10 Mbps and 100Mbps, respectively. These links can connect any combination of the nodes such as Station, Hub, Bridge, Switch and LAN nodes (except Hub-to-Hub, which cannot be connected).

- ppp_adv, point-to-point link is used to connect two nodes with serial interfaces (e.g., routers with PPP ports)) at a selectable data rate.
- Application_Config includes a name and a description table that specifies various parameters for the different applications (i.e. video conferencing and voice applications). The specified application name is used while creating user profiles on "Profile_Config" object.
- Profile_Config is used to create user profiles. These user profiles can then be specified on different nodes in the network to generate application layer traffic. The applications defined in the Application_Config are used by this object to configure profiles. Traffic patterns can be specified followed by the configured profiles and the applications.
- QoS_Config is used to define the QoS configuration details for protocols supported at the IP layer. These specifications are referenced by the individual nodes using symbolic names as FIFO, CBWFQ and Priority Queuing.
- MPLS_Config is used to configure Forwarding Equivalence Class (FEC) and Traffic Trunk specifications. These specifications are associated with different flows at the ingress LERs, to differentiate the flows into various classes and different QoS agreements [37].
- MPLS_E-LSP_Static is a model of static Label Switched Path (LSP). This is used to create the static forwarding tables at each node whereby the LSP can traverse.

In OPNET Modeller devises will not be functional without configuring application. Various nodes which are defined in the network for the various applications these are Application configuration or “Application Config” node is used to specify different tier names used in the network model. The tier name and the corresponding ports at which the tier listens to incoming traffic is cross-referenced by different nodes in the network. Also it specifies applications using available application types.

Application configuration is totally dependent on profile configuration. Profile configuration node is used to create user profiles. These user profiles can then be specified on different nodes in the network to generate application layer traffic. The application defined in the “application config” object is used by this object to configure profiles. This specifies the traffic patterns followed by the applications as well as the configured profiles on this object.

After configuring application and profile configuration we have to set tasks using task configuration. Task configuration node is used to define/create tasks used to characterize custom applications. These applications are then used to create profiles, which are applied across different

nodes to generate desired traffic. Finally IP attribute defines attribute configuration details for protocols supported at the IP layer.

The following environments are defined for OPNET simulations:

Movement Space: Areas which branches located

Number of Nodes: 5030 nodes

Simulation Time: 6 Months

more or less 6 months can able to show all the possible behaviour of Mo network we decide to also use 6 months simulation time for all scenarios

Communication Model: packet sources are the udp_gen process models defined in the OLSR node model. In each simulation, there are 20 communication pairs. Each source sends 64-byte packets at a rate of 4 packets/second. So in total, 80 packets are sent each second.

Routing Protocol: 4 routing protocols

- Ethernet Delay – this represents the end-to-end delay of all packets received by all the stations.
- Traffic Received (in packets/sec) by the traffic sinks across all nodes
- Traffic Sent (in packets/sec) by the traffic sources across all nodes
- Collision count is the total number of collisions encountered by the hub during packet transmissions.
- Object Response Time
- Page Response Time
- Traffic Received

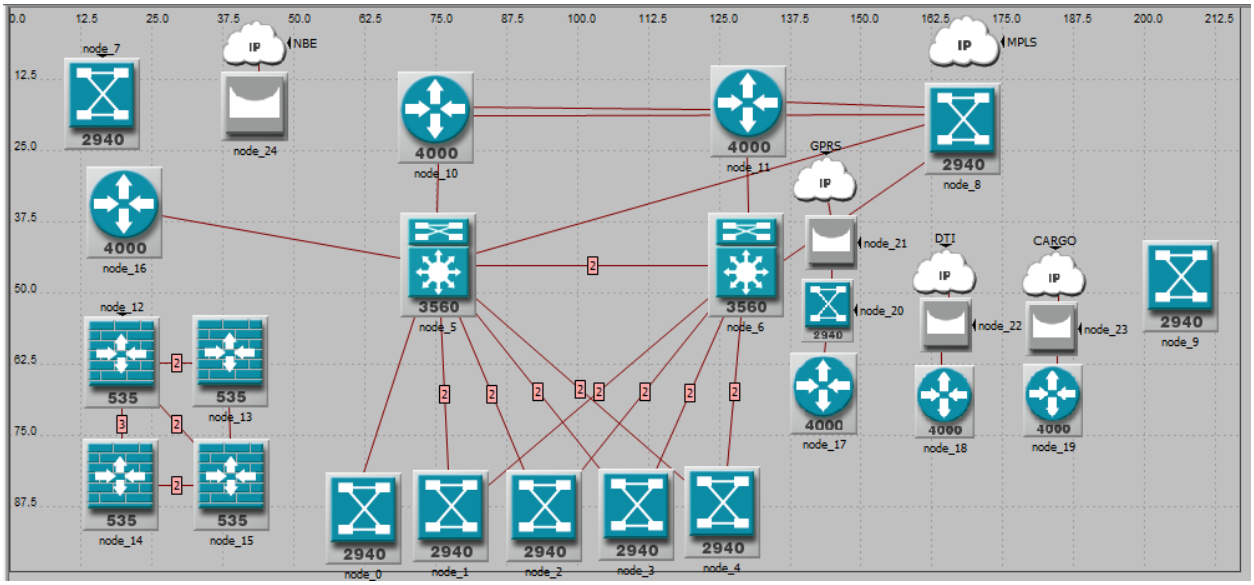


Figure 4.8.1-1 MoR Data Centre Network Architecture on Simulation Environment

Chapter 5

4. Results and discussion

This part discusses the results and findings that we discover by collecting and analysing network statistics that collected from management, simulation and modelling tools such as SolaWinds, PRTG and also OPNET. The major data showing the overall network performance and behaviour is summarized in tables and charts to describe the existing network status of MoR network infrastructure. For comprehensive representation, broad understanding and better problems identification of MoR network infrastructure, more or less inclusive statistics collected or simulated and also analysed that can express the network infrastructure, this is based on the selected metrics plus data sets. The selected metrics are utilization, traffic received and sent, error and discards, availability, response time, and delay.

5.1 Utilization

Utilization is a way to measure the performance of the network. Utilization percentage describes how much of the total network bandwidth, network capacity, is in use at a certain point of time.

The best way to detect over utilization in the network is to monitor it constantly. Measurements can be taken for instance from 8 working hours, the busiest hour of the day and from the busiest 15 minutes of the day. Charles Spurgeon in [38] gives an example for these reference values: for the 8-hour working day utilization should be 20% or less and for the busiest hour the average utilization should not exceed 30%. In addition the 15 minute average should be less than 50%. In [39]Bartlett, Sevcik and Moore state that overall utilization should be most of the timeless than 35%. It is hard to define when the performance is good - these reference values might change based on the network and how it is used. One important factor in defining whether the network is over utilized is to get the opinions of end users. In general the reference values are based on the examinations of the statistical properties of the traffic. In this thesis these statistical properties and end users opinions are not discussed in detail.

This thesis presents important utilization such as CPU, Link and memory statistics collected from MoR networks

Generally we can able to say that Measure of the usage of a link, port, or network resources. Nominal is best because high utilization is accompanied by high delays and low utilization is seen as a poor use of resources.

5.1.1 CPU Utilization

NO	NODE NAME	CPU UTILIZATION		NODE NAME	CPU UTILIZATION
1	MoR-EAST-CS.revenue.gov	74 %	14	MoR-HWSA-R	10 %
2	BLKD-CSW	43 %	15	addmis024.revenue.gov	6 %
3	Building-C-CoreSwitch	38 %	16	MiS-ASW-02.revenue.gov	6 %
4	CC-Mojo-CS.mojodryp.revenue.gov	29 %	17	CC-Kaliti-CS	6 %
5	MISG	28 %	18	ERCAMISAS-NEW.revenue.gov	5 %
6	Kaliti~CoMet	25 %	19	DatabaseSW.revenue.gov	5 %
7	GLSW-3560G-48	24 %	20	INTERNET-cON-7206	3 %
8	ERCASRVAS01.revenue.gov	23 %	21	MoR-DS2.MoR.local	2 %
9	AA#1-core-sw	23 %	22	ERCA-MIS-ASR-01.revenue.gov	2 %
10	MiS-CS-01.revenue.gov	18 %	23	CS-DC2950-24	2 %
11	addmis040.revenue.gov	17 %	24	MoR-ADMA-R	2 %
12	MiS-Edge-02.revenue.gov	10 %	25	CC-AWASH-R.revenue.gov.et	1 %
13	MiS-Edge-03	10 %			

Table 5.1.1-1 summery of top interfaces by the percent utilization

Both very high and very low CPU utilization is not advised in any given network, because very high utilization leads to Congestion, Delay, Poor performance and slow services, very low utilization of CPU is unwise use of network resources, regards to MoR we observe that the average CPU utilization of selected device is 16.48% this is a very low utilization of CPU resource, from 255 selected core network device only 11 of them uses more than 17% of their CPU capacity. So almost all services of MoR executed or processed by only very few devices. This is the result of mismanagement or poor allocation of resources.

The main reason of high CPU utilization is that Email service and access list, both has huge demands not only on CPU but also disk utilization

5.1.2 Link Utilization

It became apparent that we needed to do fairly high-resolution monitoring of network utilization and performance, regards to the MoR network there are 964 ports available and at the time of capturing the statistics 592 ports or 61% is used and 372 ports or 39% is idle.

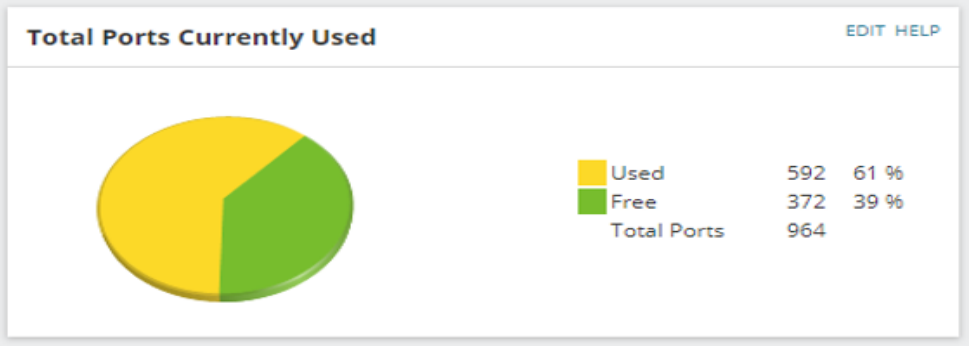


Figure 5.1.2-1 Port Usage chart

The following graph shows top interfaces based on their link utilization that generated from the monitoring tool that currently deployed on MoR datacenter. The result shows utilization of the major interfaces which is transmitting highest traffic in the data center and branch offices. Based on this result the highest interface utilizing the bandwidth that connected to the datacenter is the interface which is connecting to the server farm sw3. Though there are different distribution switches in the datacenter connected to the core switch1, the highest load is noticed on the interfaces of G2/12 connected to the serve farm sw3. The single interface utilization is even beyond 400mbps, the total data line subscribed from Ethio telecom. This can possibly cause network congestion, packet loss, and high network, or application response time.

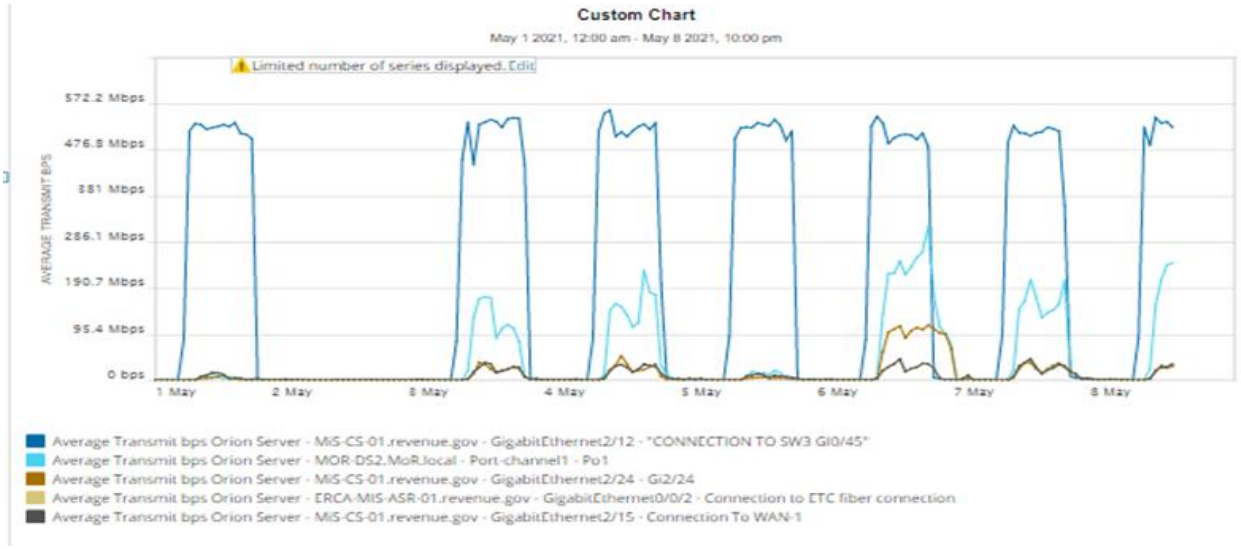


Figure 5.1.2-2 Interfaces by traffic utilization From (May1-May8) peak days

Table 5.1.2 is the summery of top interfaces by the percent utilization for overall received and transmitted packets. This shows the interface's transmitted and receives utilization as a percent based on total interface speed. The table shows CS1 exhibits high percent imbalance of received and transmitted packets ports G2/12 and G2/19. Port G2/19 is transmitting only 3% while receiving 56% of the traffic which depicts possible packet drop or loss. The leading Interfaces are also behaving relatively in the same way. Though there imbalance between receiving and transmitting percent utilization, the utilization rate is in a normal and green state.

NODE	INTERFACES	RECEIVE	TRANSMIT
core_sw1	GigabitEthernet2/19 · "CONNECTION TO SW2 GI0/45"	56 %	3 %
core_sw1	GigabitEthernet2/12 · "CONNECTION TO SW3 GI0/45"	0 %	55 %
MoR_hq_sw	Port-channel1 - Po1	15 %	14 %
MoR_hq_sw	Vlan100 · ServerFarm Vlan	27 %	2 %
MoR_hq_sw	GigabitEthernet0/47 · Connection to BLKC_L3-24 Switch	1 %	18 %
MoR-hwsa-r	Ethernet0/0 · connection to ISP-WAN	16 %	3 %
core_sw1	GigabitEthernet2/1 - Gi2/1	8 %	1 %
isa_r1	GigabitEthernet0/51 - Gi0/51	7 %	1 %
MoR_hq_sw	GigabitEthernet0/22 - Gi0/22	7 %	1 %
core_sw1	GigabitEthernet2/24 - Gi2/24	4 %	3 %

Table 5.1.2-1 Top interfaces by precent utilization

The links between layers should be designed to carry the amount of traffic load handled by the distribution devices, at a minimum. The links between two devices should be of sufficient size to

carry the aggregate amount of traffic coming into one of the devices. Consider the average link utilization, but allow for future growth.

The traffic imbalance can be clearly shown by the following figure which is the traffic share of selected branches in ascending order. The share of the traffic with the number of client is not proportional based on the next diagram that comprises of the number of client per selected branch offices.

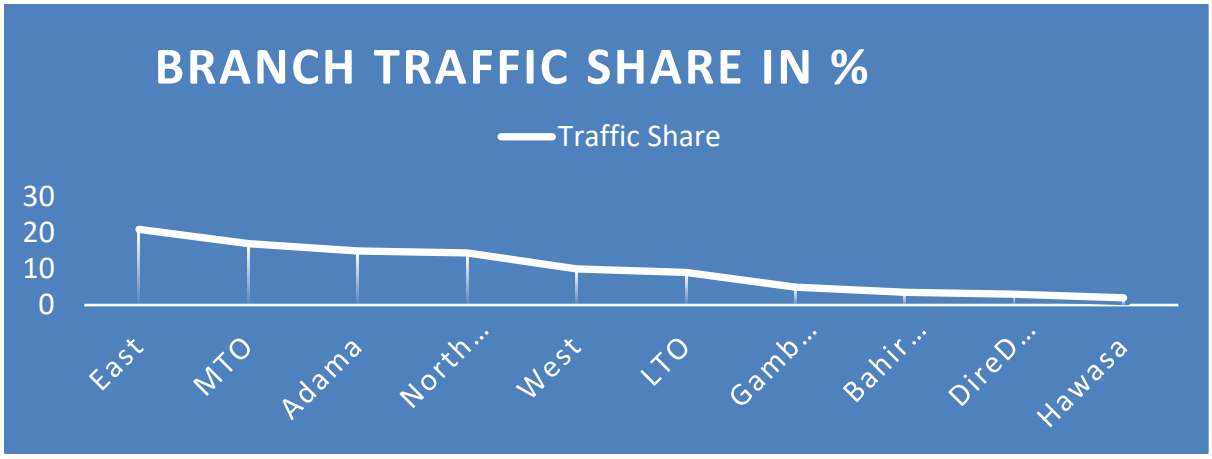
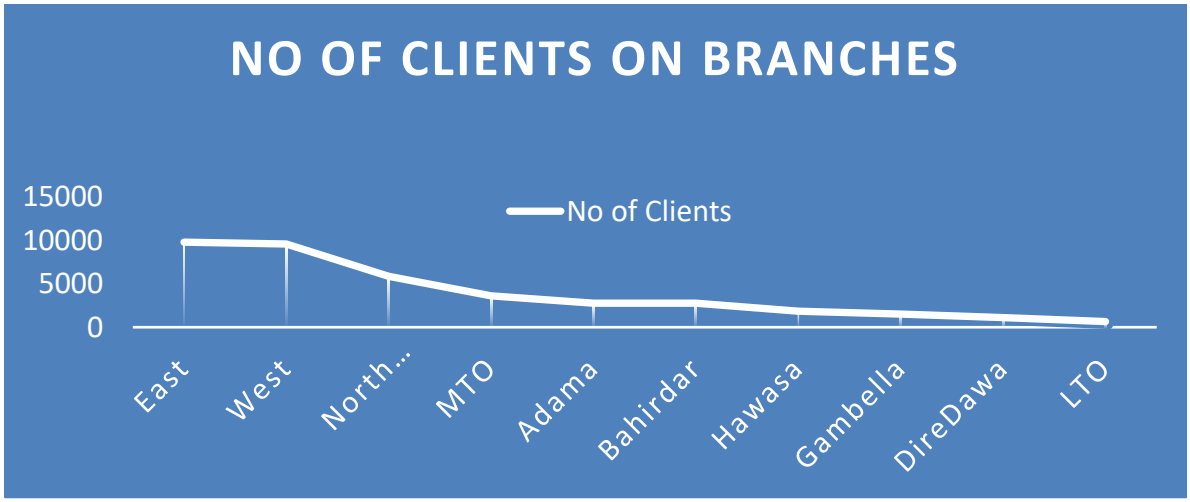


Figure 5.1.2-3 Traffic per selected branch offices

The branch offices serving large number of the clients need to have the greater traffic share compared to the other branch offices which are serving less number of customers. This can brought about the fair distribution of the resources among the users of the network.



5.1.3 Memory Utilization

Monitoring memory usage is essential in guaranteeing maximum performance. High rates of memory utilization can results in decreased performance for the associated processes. In MoR network 77.45% of the total memory used out of all critical devices, but in high memory utilization is only showed only on few devices, this is because of not employing load balance between devices on MoR network. Regards to the memory consumption it is the result of using outdated routing algorithms/protocols like RIP and also by deploying a configuration that puts enormous burden on memory.

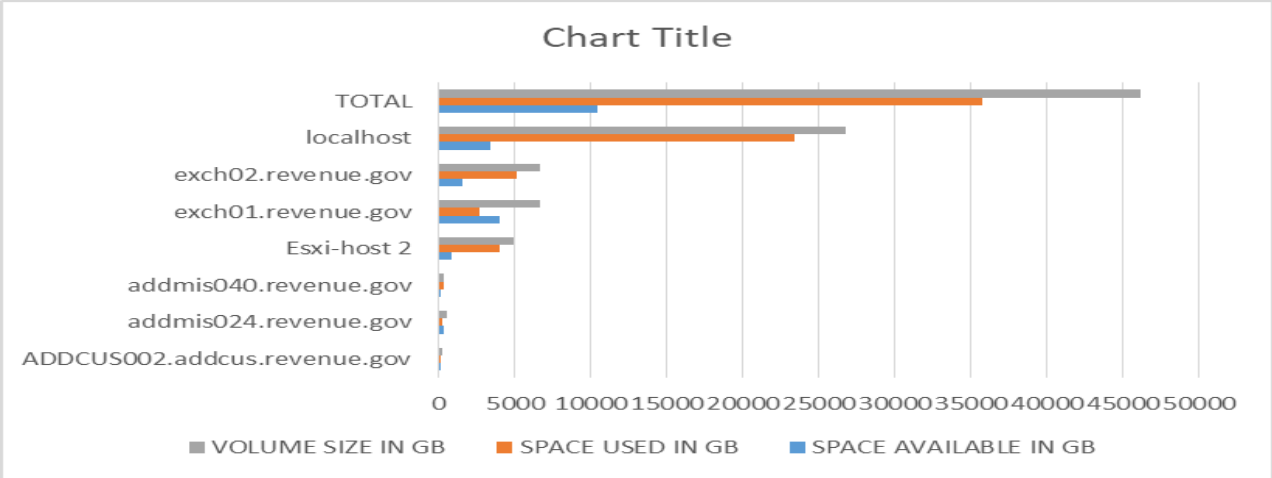


Figure 5.1.3-1 memory utilization

One of the most common mistakes that we make is that whenever a device isn't performing up to its potential, more memory is added. Adding more memory is not going to do you any good if your device isn't optimized and thus, it will just keep on with its sagging performance [40]. Instead we have to optimize the memory utilization by using updated protocols, light memory configurations and detail monitoring tools.

5.2 Traffic

The overall traffic received and the transmitted for the top interfaces listed on Table 4.2, this shows the overall traffic sent and received between the branches and datacenter. The data is gathered from the links that connects the data center with the branches, we can see that the CS1interface connected with the server farm sw2 is receiving the traffic which is beyond the subscribed

bandwidth from the Ethio Telecom which may cause packet loss and discards. The traffic imbalance between the receiving and the transmitting node is higher.

NODE	INTERFACE	RECEIVE	TRANSMIT
CS1	GigabitEthernet2/19 · "connection to sw2 gi0/45"	562.293 Mbps	25.996 Mbps
MoR_Local	Port-channel1 - Po1	305.375 Mbps	272.028 Mbps
CS1	GigabitEthernet2/12 · "connection to sw3 gi0/45"	3.161 Mbps	547.153 Mbps
MoR_Local	Vlan100 · ServerFarm Vlan	273.653 Mbps	18.453 Mbps
CS1	GigabitEthernet2/1 - Gi2/1	75.175 Mbps	13.815 Mbps
MoR_Local	GigabitEthernet0/22 - Gi0/22	74.826 Mbps	5.868 Mbps
ASR1	GigabitEthernet0/51 - Gi0/51	69.847 Mbps	10.183 Mbps
CS1	GigabitEthernet2/24 - Gi2/24	44.675 Mbps	26.353 Mbps
MoR_Local	GigabitEthernet0/50· connection to ethio telecom	5.628 Mbps	38.766 Mbps
CS1	GigabitEthernet2/20 · "connection to sw2 gi0/46"	8.165 Mbps	27.113 Mbps

Table 5.2-1 Top Interfaces by received and transmitted Traffic

5.3 Errors & Discards

Error report describes a packet that was received but could not be processed, because there was a problem with the packet. On the other hand discard packet is a packet that was received without errors but was dropped, usually because interface utilization is near 100%. Another reason of errors and discards is hardware problem such as cables, firewall, router and switches can weaken signals because of unable to update those devices and when they are faulty, software and protocol bucks are also the reasons.

The report clearly shows that the CS1 is exhibiting receive errors and transmit discards on different interfaces that connect to the server farm. The highest received error is exhibited on the CS interfaces connected to the server farm switches which can possible cause packet loss and discards.

NODE	INTERFACES	RECEIVE ERRORS	RECEIVE DISCARDS	TRANSMIT ERRORS	TRANSMIT DISCARDS
MIS-CS-01.REVENUE.GOV	GIGABITETHERNET2/19 · "CONNECTION TO SW2 GI0/45"	289,491	0	0	2,203
MIS-CS-01.REVENUE.GOV	GIGABITETHERNET2/20 · "CONNECTION TO SW2 GI0/46"	3,963	0	0	5,299
MIS-CS-01.REVENUE.GOV	GIGABITETHERNET2/12 · "CONNECTION TO SW3 GI0/45"	0	0	0	8,078
MIS-CS-01.REVENUE.GOV	GIGABITETHERNET2/13 · "CONNECTION TO SW3 GI0/46"	2,997	0	0	0

CC-MOJO-CS.MOJODRYP.REVENUE.GOV	GIGABITETHERNET1/0/20 - GI1/0/20	0	0	0	2,079
CC-MOJO-CS.MOJODRYP.REVENUE.GOV	GIGABITETHERNET1/0/6 - GI1/0/6	0	0	0	903
MIS-CS-01.REVENUE.GOV	GIGABITETHERNET2/24 - GI2/24	0	0	0	169
MOR-DS2.MOR.LOCAL	PORT-CHANNEL1 - PO1	0	0	0	89
MIS-CS-01.REVENUE.GOV	GIGABITETHERNET2/23 - GI2/23	0	0	0	25
CC-MOJO-CS.MOJODRYP.REVENUE.GOV	GIGABITETHERNET1/0/17 - GI1/0/17	0	0	0	12

Table 5.3-1 Top errors and discards

Even if we get the rate of errors and discards, we can't able to get the root-cause since MoR didn't deploy a seamless network monitoring and troubleshooting that can view the entire system from a single window. In a nutshell comprehensive network monitoring solution can also provide packet loos fix.

5.4 Availability

Analyzing availability is very vital since MoR is more dependent on network communications than it were only a few years ago. Network availability is the amount of uptime in a network system over a specific time interval. Uptime refers to the amount of time a network is fully operational, it is measured as a percentage and is monitored to ensure the service being provided is consistently kept running for end- users

Network availability is often confused with network reliability. Reliability is the ability of a device or system to perform its function without failure when called upon to do so. Availability means the system is ready for immediate use.

Report from PRTG monitoring of branch offices shows that the average availability of 131 network segment up and down percentage calculated to be 49% vs 51% which means the network is 49% up and 51% down. This is basically the problem with the ISP frequent network infrastructure failure. The detailed report will be attached to the annex part of the paper.

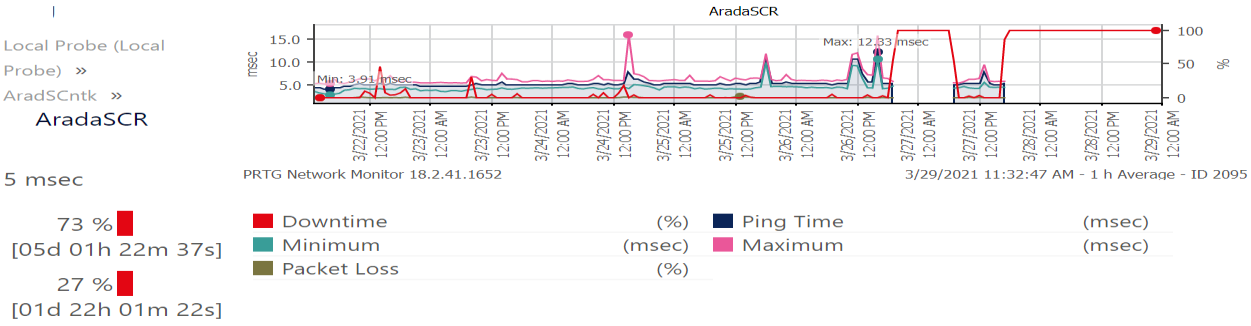


Figure 5.4-1PRTG Monitoring report of AA Arada branch

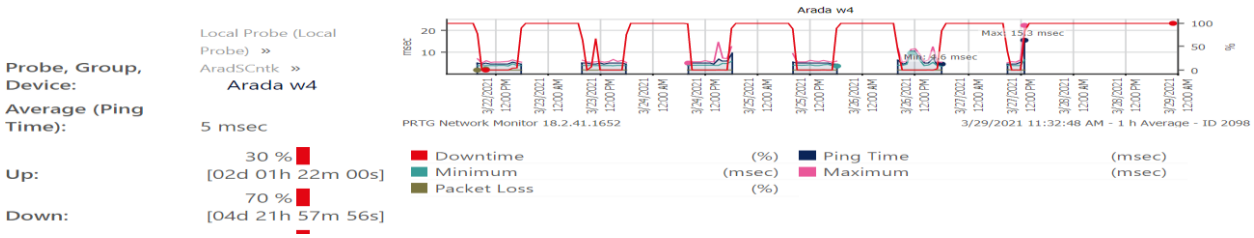


Figure 5.4-2 PRTG Monitoring report of Arada W4

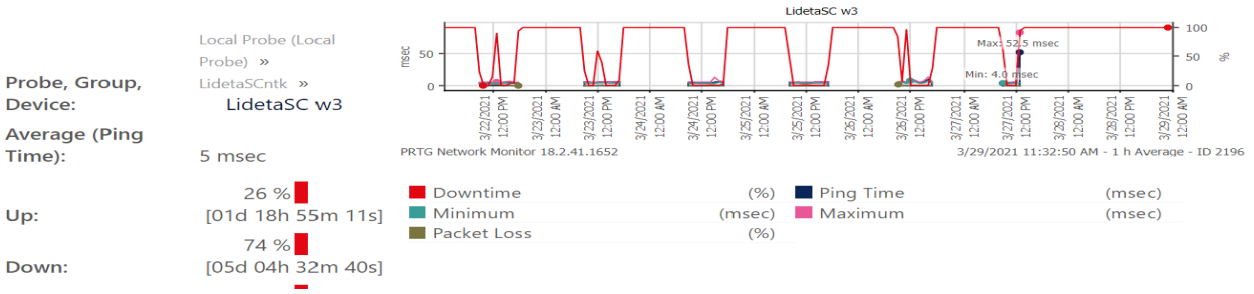


Figure 5.4-3 PRTG Monitoring report of Lideta W3

High network availability results from attention to three key points. Choice of high-availability network elements, hardware and software, Creation and maintenance of a high- availability environment including security and use of network design and operations practices that emphasize high availability [37].

MoR management should consider employing efforts in all three of these areas on entire network, including LAN and branch networks, data centers and specially on WAN services provided by Ethio Telecom because most of the availability issues is raised by their poor services.

5.5 Response Time

Network Response Time is a measure of the amount of time required for a packet to travel across a network path from a sender to a receiver. This metrics gives insight whether the network is performing as expected.

Response Time describe a website speed, it is a term used in Uptime reports. For an uptime check (http check) the response time is calculated as the time it taks to perform a HTTP GET to the specified URL, so the response time is calculated in three parts, Time to first byte, Time to receive headers and Time to load HTML of the site so z [41]

The network response time issues occur when network packets fail to reach their destinations or experience delays on the journey. Such issues can be caused by many different factors, but it helps to get a working definition of network latency issues.

On the measurement and analysis of Response Time on MoR network measured from 231 active devices and 48 devices measured zero in both average and peak response time this means they are inactive so we eradicate those devices from the calculation, plus measurement of response time not available within 24 devices, so accordingly the average Response Time is 0.35msc and the Pear Response Time is 115.8msc.

The top response time for different devices is also summarized using graph. Surprisingly among the highest response time exhibited the report most of the devices are found in the datacenter itself. The name of the devices and the response time of Top 20 devices which have very slow response time in MoR data center and branches offices showed on the above figure will help us to answer where the major problem existed on the all network situated, 70% of top 20 devices which scores very slow response time located on MoR Data Center.

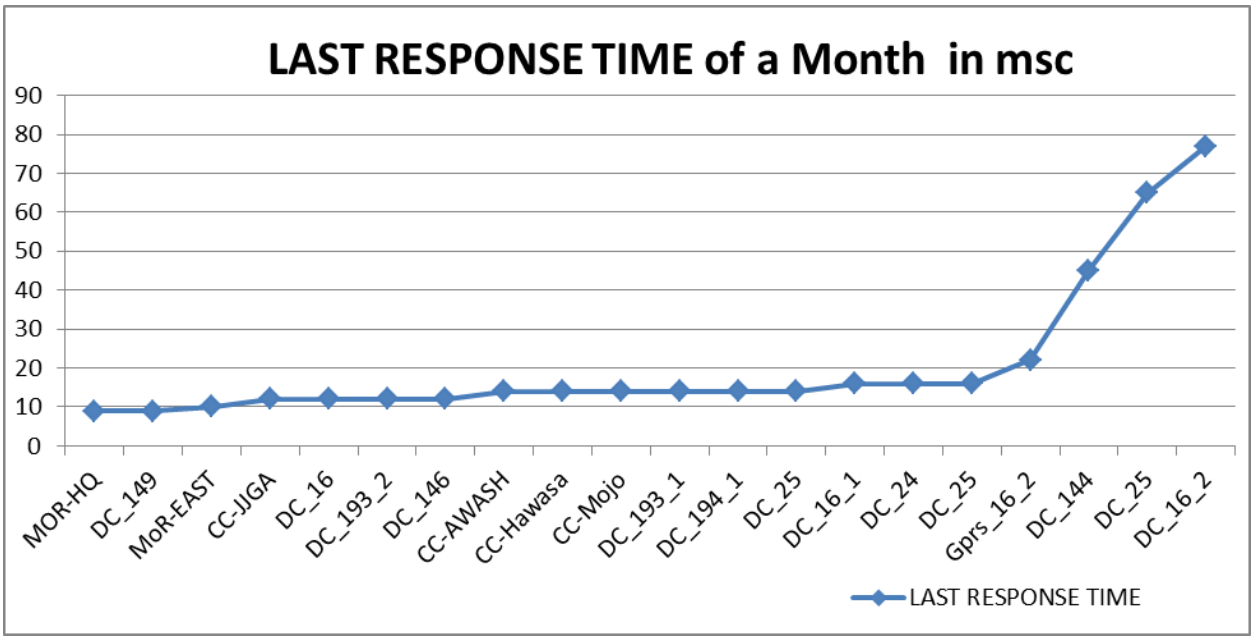
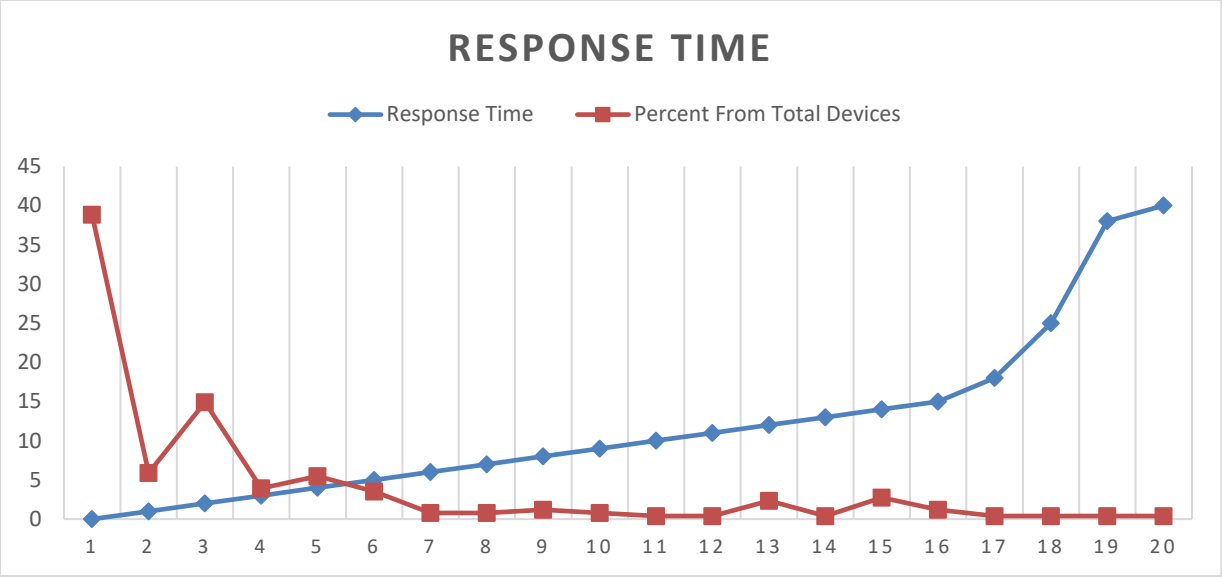


Figure 5.5-1 Response Time (Sec) of top 20 devices in both at MoR data center and branch offices.



Issues with network high response time might look like websites not loading, data taking too long to send and slow applications. The common cause of latency is propagation or the time to takes a packet to travel from source to destination, overutilization of routers and layer 4 switches, type of transmission WAN/LAN/Fiber and Storage delay [37].

Regards to MoR the major reason for high response time is using too few routers, even if there are some routers available because of not using load balance only few of them are used

OPENET simulation designed with the aim to know the overall network behavior when exposed to different situations and traffic loads. The response time, TCP delay, and other network parameters are observed under different network traffic loads.

The simulation shows how the result varies on the simulation environment when the network bandwidth has been taken by different levels of background traffic. The response time shows augmented from 3.36 Sec to 19.56 Sec, in addition Page Response Time it incremented from 4.57 Sec to 36.2 Sec when the background traffic taken 90% of the bandwidth, this response time not only decrease the performance of the network and applications who used the network, but it may stop some network services to stop. When we come to Traffic Received and Sent both shows a major decrement as the background traffic increases to be more specific the number of Packet Received per second sent when the background traffic is 90% is only 3.35% of the traffic that has

been sent when the background traffic was 25%, this will have clear negative impact on the network infrastructure.

Statistic	Average			
	25%	50%	75%	90%
Object Response Time (Sec)	3.360	7.392	12.2304	19.56864
Page Response Time (Sec)	4.579	10.90246	20.18016	36.20198
Traffic Received (Packet/Sec)	655.36	174.284	21.48471	22.34696
Traffic Sent (Packet/Sec)	891.29	1585.604	1515.192	1454.585

Table 5.5-1 Average Comparison result of Object Response Time (Sec), Page Response Time (Sec), Traffic Received (Packet/Sec) and Traffic Sent (Packet/Sec) When Background traffic takes 25%, 50%, 75% and 90% of the total bandwidth respectively

Figure 5.5-2 Average Comparison result of Object Response Time (Sec), Page Response Time (Sec), Traffic Received (Packet/Sec) and Traffic Sent (Packet/Sec) When Background traffic takes 25%, 50%, 75% and 90% of the total bandwidth respectively

As we describe on chapter three, the analysis on the above figure is made by using the using the metrics Object Response Time of Object and Page plus Packet Received and Sent.

Both table 4. And figure 4. Shows how the result of metrics changes on the simulation environment when the network bandwidth has been taken by different levels of background traffic. The response time shows augmented from 3.36 Sec to 19.56 Sec, in addition Page Response Time it incremented from 4.57 Sec to 36.2 Sec when the background traffic taken 90% of the bandwidth, this response time not only decrease the performance of the network and applications who used the network, but it may stop some network services to stop. When we come to Traffic Received and Sent both shows a major decrement as the background traffic increases to be more specific the number of Packet Received per second sent when the background traffic is 90% is only 3.35% of the traffic

that has been sent when the background traffic was 25%, this will have clear negative impact on the network infrastructure.

5.6 DELAY

Statistic	Average			
	25%	50%	75%	90%
TCP Delay (sec)	0.34073	0.81536	0.17563	0.14197
TCP Retransmission Count	840	924	770	733.333
TCP Segment Delay (sec)	0.04746	0.05979	0.415	0.55195

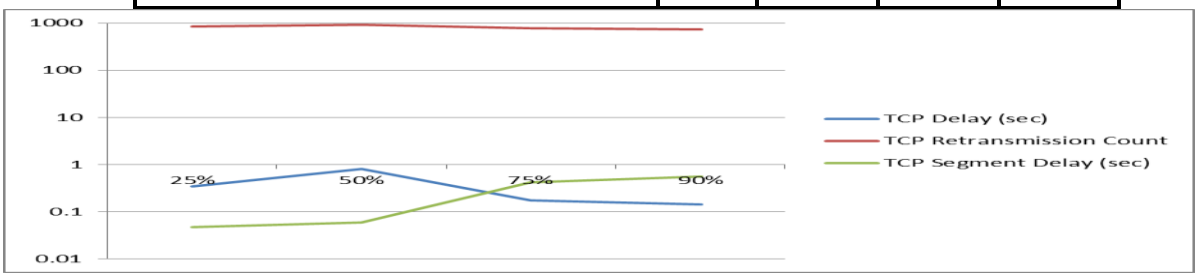


Figure 5.6-1 TCP Delay, Retransmission Count and Segment Delay of HTTP applications when there is 25%, 50%, 75% and 90% background traffic usage of the bandwidth of the links

We can quantity the behaviour of the network infrastructure and the application performance using the metrics TCP Delay, Retransmission Count and Segment Delay. It shows very slight variation On Retransmission Count even if the background traffic increases, but the Segment Delay keeps increasing as the background traffic increases. When we come to the TCP Delay it turns from 0.34 to 0.815 second when the background traffic curved from 25% to 50%, after that amazingly it shows significant decrement, the reason is because both the amount of traffic sent and received decreased. We also observe that some of the critical application on MoR had some difficulties on giving much of their services.

Chapter 6

5.1. Optimization Framework

After the network data is analyzed optimization framework is proposed which can identify the possible network bottlenecks to improve network performance. The framework basically deals with the network connectivity issues and the associated bottlenecks identification.

As described above, the WAN factors that primarily caused the network bottlenecks are network devices processing delay, link latency, inefficiencies of existing transport and application protocols, link propagation delay, link bandwidth, duplicate or lost packets, link congestion. Thus, when the experimental result is narrowed down, protocol bottleneck, congestion bottleneck, bandwidth bottleneck and latency bottleneck is taken as a major performance bottlenecks.

The collected traffic data analysis and, network statistics modeling shows that MoR network is experiencing high latency, high packet loss, and application performance problems. The optimization framework includes incoming network traffic analysis, identification of the network bottlenecks, selection of appropriate bottleneck solutions, and a reporting.

The optimization framework consists of different components for traffic statistics collections, network bottleneck identification, and selection of suitable optimization methods to solve the identified problems. The proposed framework incorporate network Data Acquisition, Data Identifier based on Ssource and destination address, Network Problem Identifier, Optimizer, Notify and Record, Monitor as main modules. The leading topics discuss the description of those main modules along with high level and low level prototype.

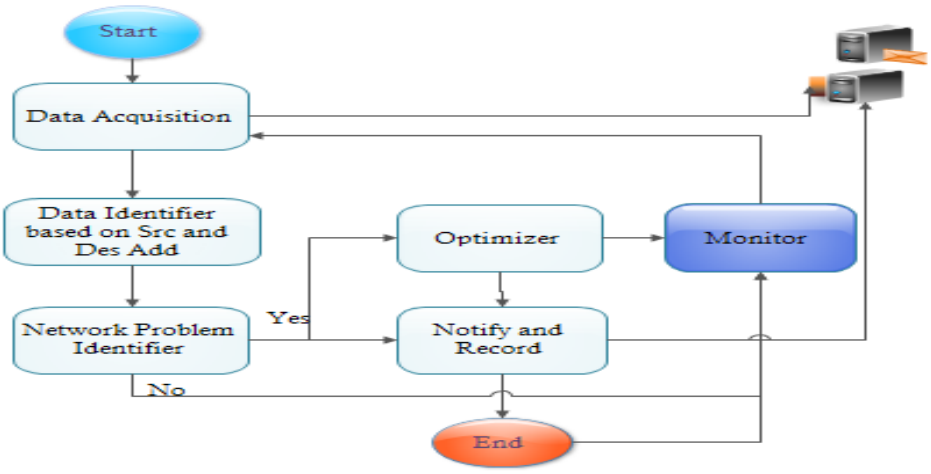


Figure 5.1-1 Proposed Optimization model

Data Acquisition

This module is responsible for the collection of the network device statistics by the monitoring tools. The traffic is then forwarded from the devices that can generate network statistics and BFD protocol heads from those interfaces that are connected to the gateway router by using the monitoring tool. The traffic data collected in this stage will be used for the next stage traffic data identifier based on their source and destination address.

Data Identifier based on Source and Destination Address

After the traffic data is collected from the receiving and sending nodes the network traffic data is identified or tagged based on the source IP address, destination IP address, and the destination port number. In addition, the associated application and protocols are also identified which can be used for the bottlenecks identification phase. The given packet can be encouraged and other can be discouraged based on the source and destination address when the network is at its peak hours.

Network Problem Identifier

This is the main module that is dedicated to identify the network related bottlenecks which possibly cause the network & application performance degradation. From the analysis phase we have noticed problems with utilization, Delay, Errors & Discard, response time, protocol overhead, and Availability , which need to be identified on early stage to take appropriate measure before the company experience network congestion that cause degradation service quality of the taxpayers. In the very beginning of this paper identification of the major point of network failure and droops was mentioned as among the target to be achieved. The modules are basically implemented by using features of the enhanced BFD. Enhanced BFD packets are capable of carrying the packet loss and latency in addition to short duration failure detection which is supported by the former BFD. BFD protocol provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. Therefore, in order for a BFD session to be created, you must configure BFD on both systems (and BFD peers). Once BFD has been enabled on the interfaces and at the router level for the appropriate routing protocols, a BFD session is created, BFD timers are negotiated, and the BFD peers will begin to send BFD control packets to each other at the negotiated interval. BFD provides fast BFD

peer failure detection times independently of all media types, encapsulations, topologies, and routing protocols BGP, EIGRP, IS-IS, and OSPF.

Optimizer

Other main part of the framework dedicated to ease the negative effect of the bottlenecks identified in the previous identifier. The network related problems used for the this thesis are related to response time, delay, availability, discards and error, protocol overhead, link utilization, and bandwidth.

Notify and Record

The responsibility of this module is to report some problems based on the defined notification level for the network administrators and other in need. Network administrators need to have the proper understanding of their real network environment prior to propose any solution for the management. Those short and long terms solution taken based on the existing problem analysis maximize our effort to tackle the root cause of the network service instability.

Monitoring

Network monitoring phase is the continuous task which needs to be performed to assure the availability of the network in the way that can fulfill the need of the customers.

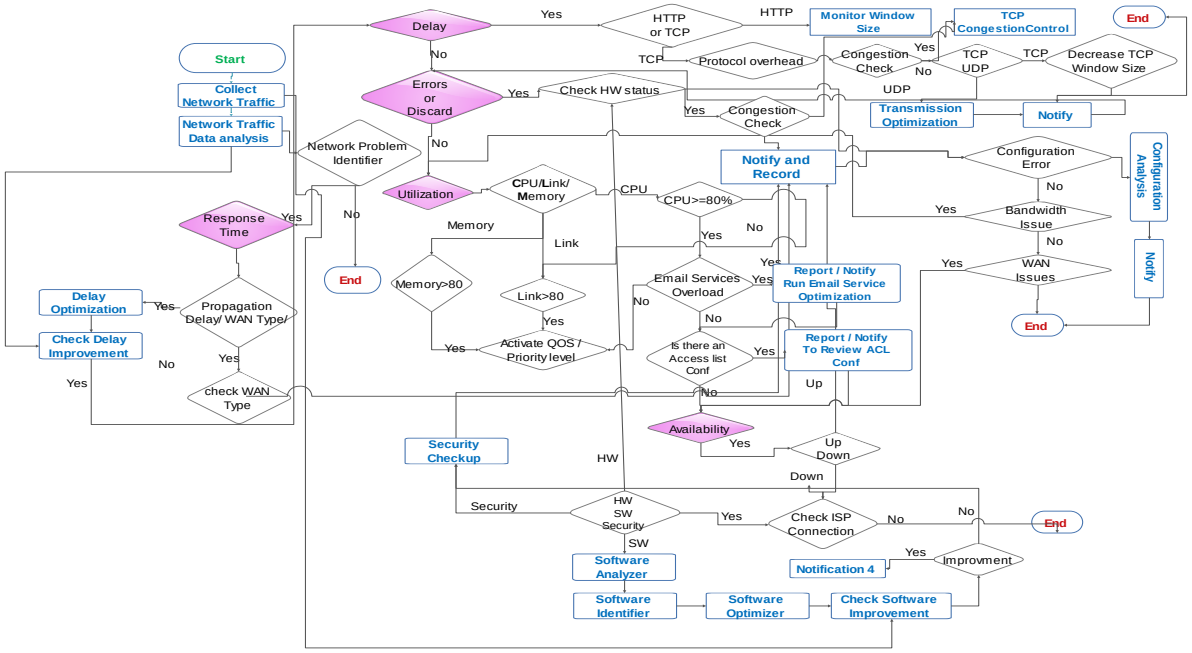


Figure 5.1-2 MoR Network Optimization Framework

OPTIMIZED DELAY THRESHOLD SCHEDULER

```
1.  Initalize DThreshold to Zero
2.  DThreshold = 110MS
3.  For every TTI
4.       Calculate DThreshold
5.              for every node
6.                     calculate the Node packets delay
7.              if the Node packets delay > DThreshold then the node and packet is selected
8.                     if packet = TCP
9.                            Run protocol overhead checker
10.                                  if protocol overhead result = no protocol overhead
11.                                         Run window size monitoring
12.                                  End if
13.                    End if
14.                    else start again
15.                    End if
16.             End if
17.      end
18. end
```

Algorithm 5.1: optimized delay threshold scheduler

Algorithm 5.1 starts by comparing a packet delay with the given threshold, then Protocol Overhead Checker algorithm will be launched if the delay is greater than 110 millisecond and also the protocol is TCP, sometimes the reason for high delay may not be protocol overhead if it is not the algorithm checks for window size.

```
 CONGESTION AVOIDANCE ALGORITHM USING SLOW START
1.       Initial: cwnd = 1:
2.       For (each packet Acked)
3.       Cwnd++;
4.       Until (congestion evnent, or, cwnd > ssthresh)
5.
6.  Enhanced Congestion Avoidance
7.       /* slow start is over and cwnd > sstresh */
8.       Every Ack:
9.                TR = TRc - TRp
10.               calculate increment value;
11.               cwnd = cwnd + increment
12.               Until (timeout or 3 DUPACKs)
13.
14. FAST RETRANSMIT ALGORITHM:
15.      After receive 3 DUPACKs
16.      Resend lost packet;
17.      Invoke Enhanced Fast Revcovery algorithm
18.
19. ENHANCED FAST RECOVERY ALGORITHM:
20.      I-With 3 DUPACKs:
21.               cwndn = MAX {2, (cwndn};
22.               ssthresh = MAX {2, (cwndn};
23.               cwndn = ssthresh +3;
```

Algorithm 6.2: Congestion avoidance

Algorithm 6.2 contains three algorithms which is Enhanced Congestion Avoidance, Fast Retransmit Algorithm and Enhanced Fast Recovery Algorithm. Enhanced Congestion Avoidance used to calculate the increment value, this value keeps incrementing until it finds either three duplicated packets or reaches timeout. When we face either of this Fast Retransmit Algorithm will be executed to resend lost packets by invoking Enhanced Fast Recovery Algorithm which is used to overcome packet drop problem when there is congestion.

```
 CPU UTILIZATION Algorithm
1.  CPU Utilization(device i)
2.       if CPU current utilization(device i) > 80%
3.                call CPU utilization function(device i)
4.                if port_no = 15 or 21 or DB app
5.                         notify 15/21/DB_overload
6.                else-if ACL conf == TRUE
7.                         notify ACL_conf_issue
8.                end if
9.       end if
```

Algorithm 6.3: CPU utilization avoidance

The following algorithm used to identify and switch the primary with secondary backup device based on CPU and memory utilization by comparing there serving with available resources, if the serving resource is greater than the available resource and if it's not true for the secondary device, then the secondary device will take over the primary position.

```
 RESPONSE TIME
1.  RESPONSE_TIME(device i)
2.      if CPU current response time(device i) >= 120ms
3.              call utilization function(device i)
4.              check WAN type
5.              notify response_time_issue
6.      end if
```

Algorithm 6.4: Response Time

If there is a response time delay the first thing we have to do to find the root cause is checking the utilization of the device which means CPU, link and memory utilization because all of this has the potential to cause a network delay so to impose that we call the utilization function in the above algorithm. The utilization algorithm is responsible to identify which device resource is currently used beyond the predefined threshold level.

```
 Response Time Minimization and Device Utilization Algorithm
1.  BackupData(A is a backup of B, B is a backup of A)
2.      device(1,2), device(3,5), device(4,6), device(9,10)
3.              for each(device)
4.                      A=device(x,)
5.                      B=device(.y)
6.                      if(device number == A)
7.                              return B
8.                      End if
9.              End
10. LoadBalanceData(A load balance with B, B load balance with A)
11.     device(1,2), device(3,5), device(4,6), device(9,10)
12.             for each(device)
13.                     A=device(x,)
14.                     B=device(.y)
15.                     if(device number == A)
16.                             return B
17.                     End if
18.             end
19. For Each(device i in datacenter)
20. Calcualte_remaining_memory_capacity(device i )
21.             If(remaining memory capacity>serving memory capacity)
22.                     call backup function
23.                     y = backup(device i)
24.                     If(remaining memory capacity of device i>serving memory capacity of
    device i)
25.                             use device i as a primary device
26.                     else(do nothing)
27.                     End If
28.             End If
29. Calcualte_remaining_ memory _capacity(device i )
30.             If(remaining memory capacity>serving memory capacity)
31.                     call backup function
32.                     y = backup(device i)
33.                     If(remaining cpu capacity of device i>serving cpu capacity of device i)
34.                             use device i as a primary device
35.                     End If
36.             End If
37.
```

Algorithm 6.5: Response Time Minimization and Device Utilization Algorithm

To identify the resource utilization of a specific node and then to replace it with another device or to do load balancing, first we have to identify which device is accountable to substitute the other

device or to be in-charge and also which device is to be considered if a load balance is imposed, to do that first we have to establish a relationships dataset between the device on both backup and load balance relationship, this algorithm not only helps to identify which device replace or work together with another device, but also help us to compare and identify the given devices so if the other device is no better than with the primary device that we are currently using, we have to look for another solution instead of swapping between the device.

According to the investigation that we make on MoR network, it is better to overcome link load problem by using bandwidth management, redundancy, configuration and also administration policy, instead of using some sort of algorithm because of the following reason. First based on the very nature of MoR network infrastructure it's very hard to deploy a dynamic link management. Second the old protocols make it very hard to pass fast instruction to the devices at a real time. So our frame work only notifies and suggests link utilization and issues to the admins.

5.2. Framework Demonstration

Practical use of our framework using algorithms depends critically on the use of suitable parameter configuration and settings on selected devices. End users often have little or no knowledge about the impact of an algorithm's parameter settings on its performance, and thus simply use default settings, instead the algorithm will be totally deployed only on core and distribution devices. Default configuration may not perform well on the particular problem instances encountered by the devices so the algorithm will apply a given solution or configuration according to the situation. Automatic algorithm configuration methods can be used to improve performance in a principled and convenient way.

The proposed framework modules are demonstrated using the pfSense operating system. pfSense is the most power full router operating system, mostly used as a router and firewall software, and could be configured as DHCP server, DNS server, WiFi access point, VPN server, all running on the same hardware device. pfSense also allows for installation of third party open source packages such as Snort or Squid through a built in Package Manager, making it the default choice of many network administrators. pfSense is flexible by design. It can be used on a small home router as well as run the entire network of a large corporation. Nowadays, pfSense is often replacing CISCO and other expensive name brands in large corporate environments, not because it's free, but

because it is feature rich and are regularly updated and are known to patch security issues promptly. pfSense puts you in control of your networking.

  - It allows you to sort traffic by many criteria (for example, IP address, port, and protocol even by application (eg. YouTube, Facebook))
  - It allows you to identify top talkers and listeners.
  - It stores persistent traffic statistics.
- Traffic shaper: this a pfsense feature that we can use future after monitoring and analysing the traffic using ntop monitoring tool to increase the performance of our organization.

So some parts of the optimization frameworks can be configured on the pfSense as a script to manage the existing network conditions. the network traffic and analysing the bottlenecks for the performance excluding other reason like packet loose, high RTT with the help the above packages will help to improve the performance

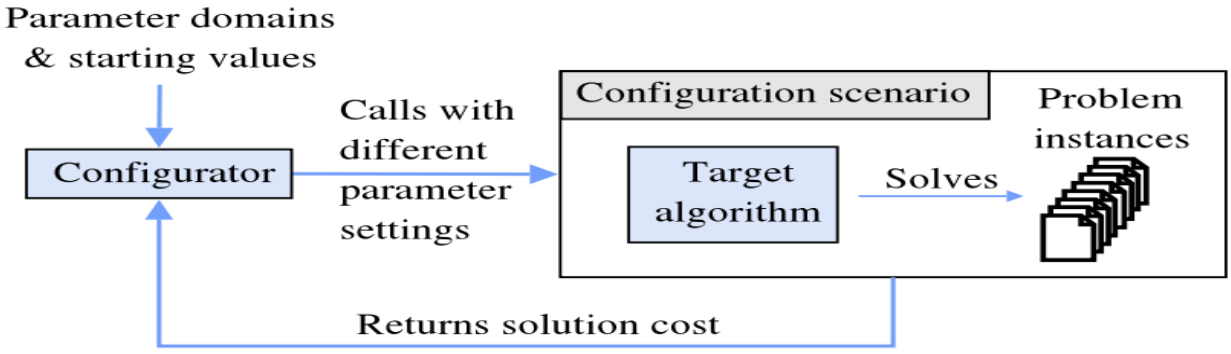


Figure 5.2-1 Figure MoR Network Optimization Framework Configuration Scenario

A configuration scenario includes an algorithm or framework solution to be configured, and a collection of problem instances. A configuration procedure implements the target algorithm with specified parameter settings on some or all of the algorithm instances, receives information about the performance of these runs, and uses this information to decide which subsequent parameter configurations to evaluate. The execution time of the algorithms varies based on the problem and algorithm type.

5.3. **Evaluation of the formwork**

Based on the survey and Observation that we make on the

- Data center,
- Simulation environment and also
- By interviewing the system and network administration we learned that the following improvement achieved by implementing the algorithm

No	Metrics		Improvement Level			
			High	Medium	Low	No
1	Utilization	CPU	5	2	2	
2		Memory	4	3	2	
3		Link	1	5	3	
4	Traffic(R/S)		2	3	3	1
5	Errors		3	3	2	1
6	Discards		6	2	1	
7	Availability		2	4	1	2
8	Response Time		7	1	1	
9	Delay		3	2	3	1

Figure 5.2-2 Optimization framework evaluation

Chapter 7

6. Conclusion and Recommendation

7.1 Conclusion

The analysis and simulations are obviously guiding us the spot of the problem, which is mainly in the main datacentre. With the entire selected performance metrics one can notice performance problem on the edge devices, core devices, and distribution devices; which can cause network dropouts.

Based on the investigation and analyses that we made so far, we can conclude that there is a performance degrade caused by different factors like structural imbalance, overloads, lack of system tuning and protocol overheads, even if its a fact that all those factors affects the performance on MoR network a lot, but the magnitude of their impact is different or they don't have an equal share.

On MoR network performance degrade caused by structural imbalance is like a Gigabit line attached to low-end machines on both data center and branches where CPU can't process packets fast enough which leads to packets being lost and more retransmissions count. Performance degrade also caused on MoR network by overloads which triggered synchronously by protocols and broadcasts.

Poor performance also occurred on MoR network due to lack of system tuning. Even if there is plenty of CPU, memory or buffer space and bandwidth available on the network and on the devices, but there is no proper configuration, allocation which considers the current situations in MoR Or if the CPU scheduling algorithm does not give high enough priority to the process which is processing incoming segments, some of the segments can be lost.

While the MoR network handles huge in and out traffic and gives a service that requires reliable connectivity but, it is not fully optimized as it's expected. Specifically, we found that MoR did not establish enterprise-wide performance metrics or improvement targets for network devices and did not proactively monitor and resolve reoccurring network connectivity issues. Ensuring efficient, this may result in additional manual work to do with additional processing costs when the system does not work as intended and also this makes it very difficult to even recognize network

performance problems. Plus the network infrastructure doesn't have an improvement targets, and a methodology to evaluate the health of the network.

MoR did not upgrade the bandwidth operating above recommended capacity as defined in the internal best practice. The organization used a threshold of 80 percent as their internal best practice for when circuit bandwidth should be upgraded. Bandwidth utilization represents the percentage of a network's maximum available capacity that is currently being consumed by network traffic. Monitoring bandwidth utilization allows IT to easily identify when a circuit in the network is overloaded. Consistently high bandwidth utilization is an indicator of possible network stress, slowdown, or failure and it highlights a need for changes or upgrades in a network infrastructure.

We assessed 17 custom and 12 federal MoR sites from September 2020 through January 2021 most of the devices on the sites including the Data Centre exceeded the 80 percent threshold for five months. This facility experienced increased network traffic for five months and should consider upgrading the network circuits to continue to operate efficiently.
Visibility is gained from having detailed network diagrams and an accurate inventory of network devices. The IT directorate does not have complete visibility into the network to efficiently manage and operate the enterprise. This paper found that the MoR IT network diagrams and inventory system do not contain sufficient information for a complete representation of its IT network. As a result, it does not have complete awareness and visibility of its network architecture to support the systems and IT services.

While MoR has a very poor method to collect network inventory data, this process has not resulted in an accurate inventory of network devices connected to its IT network. Additionally, we identified the following inaccurate, incomplete, or duplicate data within their inventory records: duplicate IP addresses and duplicate hostnames; missing device capacity and models.

7.2 Recommendation

The main objective of this thesis is to know the overall network performance of MoR network infrastructure and also to identify the major problems of the network.

First of all we highly recommend to MoR management consider the findings of this paper and to implement the framework and the solutions, to overcome those problems we mention on the previous chapters.

We recommend for the IT team to establish an IT policy and a network strategy to include a process that continuously monitor the information technology infrastructure, and develop enterprise-wide performance metrics and improvement targets.

We recommend the IT team, in coordination with the management, to implement a solution, such as sitewide emergency generators that is fully dedicated only for the datacenter to avoid relaying only on the building power generator, this will prevent network connectivity and availability issues.

To adjust the configuration settings issues, protocol overhead and protocol instability problems on network devices at MoR datacenter and Distribution Centre to prevent issues regards to performance degrade

Once the network is congested, both the network and the application performance are degraded causing the service availability inefficient for the taxpayers. Except Addis Ababa City Revenue branch offices, the other MoR branch office network established in Addis Ababa are not facing difficulties in their local network connectivity. As we can infer the previous section the major problem of the network and application latency, which can result in packet loss is noticed in the MoR datacenter. The datacenter traffic load is not properly managed to be shared by different distribution switches that are connected to the main server farms. The traffic analysis and the traffic modeling results depict that only few interfaces connected to the server farm switches are handling the major traffic in the datacenter. There are enormous distribution switches installed on the datacenter rack mount believed to boost the network and application performance problems raised by different stockholders. With all those expensive server farm and network devices highest packet discard rate and highest response time is noticed in the main datacenter, which necessitates proper understanding of the network traffic patterns before any network upgrading plan is being done.

This thesis highly focuses on the general performance of MoR network infrastructure but we highly recommend future researchers to study on how the network performance affects business critical applications.

Additional research is also needed to develop methods for security of the infrastructure, users and networked applications to ease the problem of reliable connection and allowing secure communication.

8 References

[1] B. Sandberg, Networking The Complete Reference, New York: ISBN:, 2015.

[2] J. F. Kurose and K. W. Ross, Computer Networking Top-Down Approach Six Edition, Massachusetts: Addison-Wesley, 2013.

[3] A. N. Mahmood and C. Leckie, Network Traffic Analysis and SCADA Security, Springer, 2010.

[4] N. Hu, "Network Monitoring and Diagnosis Based on Available Bandwidth Measurement," Carnegie , 2006.

[5] P. L. Dordal, An Introduction to Computer Networks, Chicago: Illinois, 2020.

[6] T. Bujlow, "Classification and Analysis of Computer Network Traffic," 2014.

[7] Y. Zhang, N. Ansari, M. Wu and H. Yu, "IEEE Survey On Wide Area Network Optimization," *EEE COMMUNICATIONS SURVEYS & TUTORIALS,* pp. 1090-1113, 2012.

[8] M. K. Attamah, "Bandwidth management: the public policy Approach," European Union, Nigeria , 2010.

[9] K. Joseph, "INTERNET BANDWIDTH MANAGEMENT FOR TERTIARY INSTITUTIONS," *Computer Applications Technology and Research,* p. 2319–8656, 2016.

[10] D.-I. A. V. H. /. S. SIEGL, Application Performance Management: Measuring and Optimizing the Digital, Troisdorf, 2010.

[11] MOR, "Ministry of Revenue Ten Years Propsperity Plan(2012-2022 E.C)," MoR, Addis Ababa, 2020.

[12] M. N, "Report Warehouse," MoR, Feb 2021. [Online]. Available: http://10.1.0.122:8080/apex/f?p=100. [Accessed March 2021].

[13] M. o. Revenue, "Federal Ministry Of Revenue," January 2021. [Online]. Available: http://www.mor.gov.et/. [Accessed Monday Feb 2021].

[14] Y. Gobena, "Performance benchmarking of critical applications is done to determine the impact level of Various WAN factors (bottlenecks), which is used for developing WAN Optimization Model to alleviate the impact of this factors accordingly," AAU, Addus Ababa, 2018.

[15] M. Assefa, "BANDWIDTH OPTIMIZATION FRAMEWORK FOR WIDE AREA NETWORK: THE CASE OF ADDIS ABABA UNIVERSITY," AAU, Addis Ababa, 2016.

[16] F. Mekonen, "DESIGNING DYNAMIC BANDWIDTH ALLOCATION ALGORITHM:AAU," AAU, Addis Ababa , 2018.

[17] H. Tandra, "Automated System to Debug Network Flows in Wide Area Networks," Knoxville, 2009.

[18] B. Li, "Network Security Monitoring and Analysis based on Big Data Technologies," Bingdong Li, Reno, 2013.

[19] Javvin, Network Protocol Handbook, Saratoga: Javvin Technologies Inc, 2005.

[20] W. R. Stevens, TCP/IP Illustrated, USA: Addison Wesley Reading, 1994.

[21] L. Chitanana, "Bandwidth management in universities in Zimbabwe," *Education and Development using Information and Communication Technology,* pp. 62-76, 2012.

[22] A.-W. Longman, "Network Performance analysis," Boston, 1994.

[23] H.-Y. Kevin-Lai, "Genetic Algorithm Based Optimization in Computer Network Applications," 2015.

[24] A. Hanemann1, A. Liakopoulos2, M. Molina3 and D. M. Swany, "A study on network performance metrics and their composition," 2018.

[25] T. Lindh, "PERFORMANCE MONITORING IN COMMUNICATION NETWORKS," Stockholm, 2004.

[26] D. Hein, "Solutions Review," June 2019. [Online]. Available: https://solutionsreview.com/network-monitoring/network-performance-metrics-7-essential-network-metrics-to-monitor/. [Accessed Feb 2021].

[27] L. Chitanana, "Bandwidth Managment In The Era of Bring your Own Device," *The Electronic Journal of Information Systems in Developing Countries,* pp. 1-14, 2015.

[28] T. Birhanu, "PERFORMANCE ANALYSIS FOR WIDE AREA NETWORK OPTIMIZATION," Addis Ababa, 2014.

[29] N. Srinidhi, S. D. Kumar and K. Venugopal, "Network optimizations in the Internet of Things," *Engineering Science and Technology,* pp. 1-21, 2019.

[30] N.Snehalatha, S. Julia and P. Rodrigues, "Survey of Bandwidth Management Techniques," *International Journal of Science and Modern Engineering (IJISME),* pp. 2319-6386, 2013.

[31] B. V. William, "Bandwidth Management and Monitoring for IP Network Traffic: An Investigation," 2001.

[32] Flickenger R., How To Accelerate Your Internet, New York : INASP/ICTP, 2006.

[33] M. Mehari, "Performance Optimization and Modelling of Complex Wireless Networks Using Surrogate Models," Ghent, 2018.

[34] K. Sinshaw, "DEVELOPING OPTIMIZATION MODEL FOR BANDWIDTH UTILIZATION BASED ON NETWORK TRAFFIC ANALYSIS THE CASE OF ADDIS ABABA UNIVERSITY," Addis Ababa , 2016.

[35] M. S. Siraj1, M. A. K. Gupta2 and M. Rinku-Badgujar, "Network Simulation Tools Survey," *International Journal of Advanced Research in Computer and Communication Engineering,* vol. 1, no. 4, pp. 201-210, June 2012.

[36] K. Peffers, T. Tuure and R. M. A., "A Design Science Research Methodology for IS," *Management Information Systems,* vol. 24, no. 3, pp. 45-78, 2007-8.

[37] cisco inc, "CISCO," CISCO, 2021. [Online]. Available: www.cisco.com.

[38] C. Spurgeon, Ethernet: The definite guide, O'Reilly, Ed., Sebastopol: ISBN 1-56592-660-9, 2000, p. 498.

[39] Bartlett, J. S. P. and S. Moore, "Economics of QOS on WAN Access Lines," *Business Communications Review,* vol. 34, no. 10, 2014.

[40] K. A., "How to analyze and monitor memory utilization in realtime on network devices," 2021.

[41] S. Winds, " Solar Winds Documentation," 2021.

[42] S. Sobolevsky, "Recurrent Graph Neural Network Algorithm for Unsupervised Network Community Detection," Brooklyn NY, New York, 2021.

[43] K. Sambanis, "Quality of service for IP-based networks," California, 2001.

[44] C. F. F. A. D. PATRICK CICCARELLI, D. GROTH and T. SKANDIER, Networking Basics, New York: Don Fowley, 2013.

[45] B. L. Madegwa*, E. N. Makokha and P. G. Namusonge, "Effects of Automation of Revenue Collection on the Performance od Country Government," *European Journal of Business and Management,* pp. 118-124, 2018.

[46] Flickenger R ; Editors: Belcher M.; Canessa E.; Zennaro M, "How To Accelerate Your Internet," INASP/ICTP, 2006.

9. ANNEX

A

Availability - This Year

NODE	IP ADDRESS	AVAILABILITY
January 2021		
V1	V1	100.00 %
V0	V0	100.00 %
V120	V120	100.00 %
V121	V121	100.00 %
V166	V166	100.00 %
V167	V167	0.00 %

B

C

Current Traffic - All Interfaces

INTERFACE	INTERFACE TYPE	TRANSMIT TRAFFIC	RECEIVE TRAFFIC	TRANSMIT % UTILIZATION	RECEIVE % UTILIZATION
AA#1-core-sw					
GINT0/23 · CONNECTION TO ETC		48.07 kbps	113.547 kbps	0 %	0 %
GINT0/24 · IN-LAN		228.023 kbps	5.078 Mbps	0 %	5 %
Vlan1 - Vl1		0.0 bps	7.69 bps	0 %	0 %
ADDCUS002.addcus.revenue.gov					
Broadcom BCM5708C NetXtreme II GigE (NDIS VBD Client) #2 · Local Area Connection 2		2.065 kbps	1.686 kbps	0 %	0 %

Broadcom BCM5708C NetXtreme II GigE (NDIS VBD Client) #2-QoS Packet Scheduler-0000 · Local Area Connection 2-QoS Packet Scheduler-0000	1.867 kbps	1.717 kbps	0 %	0 %
Broadcom BCM5708C NetXtreme II GigE (NDIS VBD Client) #2-WFP LightWeight Filter-0000 · Local Area Connection 2-WFP LightWeight Filter-0000	1.867 kbps	1.717 kbps	0 %	0 %
RAS Async Adapter · Local Area Connection* 10	0.0 bps	0.0 bps	0 %	0 %
Software Loopback Interface 1 · Loopback Pseudo-Interface 1	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP) · Local Area Connection* 8	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP)-QoS Packet Scheduler-0000 · Local Area Connection* 8-QoS Packet Scheduler-0000	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IPv6) · Local Area Connection* 6	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IPv6)-QoS Packet Scheduler-0000 · Local Area Connection* 6-QoS Packet Scheduler-0000	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (L2TP) · Local Area Connection* 3	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor) · Local Area Connection* 7	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000 · Local Area Connection* 7-QoS Packet Scheduler-0000	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (PPPOE) · Local Area Connection* 5	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (PPTP) · Local Area Connection* 4	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (SSTP) · Local Area Connection*	0.0 bps	0.0 bps	0 %	0 %
HstA024.revenue.gov				
HP NC373i Multifunction Gigabit Server Adapter #10 · Local Area Connection	0.0 bps	0.0 bps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #10-QoS Packet Scheduler-0000 · Local Area Connection-QoS Packet Scheduler-0000	947.91 kbps	608.678 kbps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #10-WFP LightWeight Filter-0000 · Local Area Connection-WFP LightWeight Filter-0000	947.91 kbps	608.678 kbps	0 %	0 %
RAS Async Adapter · Local Area Connection* 10	0.0 bps	0.0 bps	0 %	0 %

Software Loopback Interface 1 · Loopback Pseudo-Interface 1		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP) · Local Area Connection* 8		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP)-QoS Packet Scheduler-0000 · Local Area Connection* 8-QoS Packet Scheduler-0000		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP)-QoS Packet Scheduler-0000 · Local Area Connection* 8-QoS Packet Scheduler-0000		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IPv6) · Local Area Connection* 6		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (L2TP) · Local Area Connection* 3		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor) · Local Area Connection* 7		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000 · Local Area Connection* 7-QoS Packet Scheduler-0000		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (PPPOE) · Local Area Connection* 5		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (PPTP) · Local Area Connection* 4		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (SSTP) · Local Area Connection*		0.0 bps	0.0 bps	0 %	0 %
HstA040.revenue.gov					
HP NC373i Multifunction Gigabit Server Adapter #56 · Local Area Connection		0.0 bps	0.0 bps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #57 · Local Area Connection 2		0.0 bps	0.0 bps	0 %	0 %
Intel(R) PRO/1000 MT Network Connection #2 · Local Area Connection 4		0.0 bps	0.0 bps	0 %	0 %
Intel(R) PRO/1000 MT Network Connection #2-Kaspersky Lab NDIS 6 Filter-0000 · Local Area Connection 4-Kaspersky Lab NDIS 6 Filter-0000		0.0 bps	0.0 bps	0 %	0 %
Intel(R) PRO/1000 MT Network Connection #2-QoS Packet Scheduler-0000 · Local Area Connection 4-QoS Packet Scheduler-0000		0.0 bps	0.0 bps	0 %	0 %
Intel(R) PRO/1000 MT Network Connection · Local Area Connection 3		8.816 kbps	19.088 kbps	0 %	0 %
Intel(R) PRO/1000 MT Network Connection-Kaspersky Lab NDIS 6 Filter-0000 · Local Area Connection 3-Kaspersky Lab NDIS 6 Filter-0000		8.816 kbps	19.087 kbps	0 %	0 %

Intel(R) PRO/1000 MT Network Connection-QoS Packet Scheduler-0000 · Local Area Connection 3-QoS Packet Scheduler-0000	8.816 kbps	19.087 kbps	0 %	0 %
isatap.{95ED87AB-B358-4835-A4E0-9B233CF7F91F} · Local Area Connection* 11	0.0 bps	0.0 bps	0 %	0 %
isatap.{F2C281B6-6F2E-4219-99A0-233D62F2A24C} · Local Area Connection* 8	0.0 bps	0.0 bps	0 %	0 %
RAS Async Adapter · Local Area Connection* 10	0.0 bps	0.0 bps	0 %	0 %
Software Loopback Interface 1 · Loopback Pseudo-Interface 1	0.0 bps	0.0 bps	0 %	0 %
Teredo Tunneling Pseudo-Interface · Local Area Connection* 9	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP) · Local Area Connection* 7	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP)-Kaspersky Lab NDIS 6 Filter-0000 · Local Area Connection* 7-Kaspersky Lab NDIS 6 Filter-0000	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP)-QoS Packet Scheduler-0000 · Local Area Connection* 7-QoS Packet Scheduler-0000	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IPv6) · Local Area Connection* 5	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IPv6)-Kaspersky Lab NDIS 6 Filter-0000 · Local Area Connection* 5-Kaspersky Lab NDIS 6 Filter-0000	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IPv6)-QoS Packet Scheduler-0000 · Local Area Connection* 5-QoS Packet Scheduler-0000	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (L2TP) · Local Area Connection* 2	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor) · Local Area Connection* 6	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor)-Kaspersky Lab NDIS 6 Filter-0000 · Local Area Connection* 6-Kaspersky Lab NDIS 6 Filter-0000	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000 · Local Area Connection* 6-QoS Packet Scheduler-0000	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (PPPOE) · Local Area Connection* 4	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (PPTP) · Local Area Connection* 3	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (SSTP) · Local Area Connection*	0.0 bps	0.0 bps	0 %	0 %

BLKD-CSW					
GINT1/0/23 · "Connection To EAST Core Switch "	660.289 kbps	502.802 kbps	0 %	0 %	
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %	
BCC					
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %	
ARV					
Embedded-Service-Engine0/0 - Em0/0	0.0 bps	0.0 bps	0 %	0 %	
GINT0/0 · connection to ISP	134.234 kbps	1.659 Mbps	0 %	0 %	
GINT0/1 · connection to Internal-LAN	1.663 Mbps	147.807 kbps	0 %	0 %	
GINT0/3 - Gi0/3	0.0 bps	0.0 bps	0 %	0 %	
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %	
JRRD					
Embedded-Service-Engine0/0 - Em0/0	0.0 bps	0.0 bps	0 %	0 %	
GINT0/0 · connection to ISP-WAN	152.247 kbps	195.613 kbps	0 %	0 %	
GINT0/1 · NLAN	195.939 kbps	155.82 kbps	0 %	0 %	
GINT0/3 - Gi0/3	0.0 bps	0.0 bps	0 %	0 %	
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %	
CC-CustK-CS					
GINT1/0/1 · "To Ethio-Telecom Side"	6.092 Mbps	2.484 Mbps	1 %	0 %	
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %	
CC-MIL-R.revenue.gov					
Backplane-GINT0/3 - Ba0/3	0.0 bps	0.0 bps	0 %	0 %	
GINT0/0 · "connection to ISP"	50.018 kbps	5.867 kbps	0 %	0 %	
GINT0/1 · IN-LAN	4.263 kbps	50.858 kbps	0 %	0 %	
CC-Mojo-CS.mojodryp.revenue.gov					
FSTETH - Fa0	0.0 bps	0.0 bps	0 %	0 %	
GINT1/0/1 - Gi1/0/1	0.0 bps	0.0 bps	0 %	0 %	

GINT1/0/10 - Gi1/0/10	10.442 kbps	1.262 kbps	0 %	0 %
GINT1/0/11 - Gi1/0/11	0.0 bps	0.0 bps	0 %	0 %
GINT1/0/12 - Gi1/0/12	0.0 bps	0.0 bps	0 %	0 %
GINT1/0/13 - Gi1/0/13	0.0 bps	0.0 bps	0 %	0 %
GINT1/0/14 - Gi1/0/14	3.27 Mbps	7.41 Mbps	0 %	1 %
GINT1/0/15 - Gi1/0/15	1.699 Mbps	503.213 kbps	0 %	0 %
GINT1/0/16 - Gi1/0/16	1.546 Mbps	887.756 kbps	0 %	0 %
GINT1/0/17 - Gi1/0/17	1.117 Mbps	144.564 kbps	1 %	0 %
GINT1/0/18 - Gi1/0/18	5.651 Mbps	1.129 Mbps	1 %	0 %
GINT1/0/19 - Gi1/0/19	0.0 bps	0.0 bps	0 %	0 %
GINT1/0/2 - Gi1/0/2	705.343 kbps	14.71 kbps	0 %	0 %
GINT1/0/20 - Gi1/0/20	1.316 Mbps	293.656 kbps	1 %	0 %
GINT1/0/21 - Gi1/0/21	1.659 Mbps	613.127 kbps	0 %	0 %
GINT1/0/22 - Gi1/0/22	5.842 Mbps	1.323 Mbps	1 %	0 %
GINT1/0/23 · connection-to-UTM-Internal	56.923 kbps	43.071 kbps	0 %	0 %
GINT1/0/24 · LINK-DATA-ETC-AGG	0.0 bps	0.0 bps	0 %	0 %
GINT1/0/3 - Gi1/0/3	25.672 kbps	5.627 kbps	0 %	0 %
GINT1/0/4 - Gi1/0/4	136.553 kbps	177.339 kbps	0 %	0 %
GINT1/0/5 - Gi1/0/5	0.0 bps	0.0 bps	0 %	0 %
GINT1/0/6 - Gi1/0/6	17.849 kbps	8.049 kbps	0 %	0 %
GINT1/0/7 - Gi1/0/7	0.0 bps	0.0 bps	0 %	0 %
GINT1/0/8 - Gi1/0/8	94.944 kbps	17.768 kbps	0 %	0 %
GINT1/0/9 - Gi1/0/9	17.685 kbps	173.323 kbps	0 %	0 %
GINT1/1/1 · "connection to ISP"	0.0 bps	0.0 bps	0 %	0 %

GINT1/1/2 · "CONNECTION TO ISP"	3.501 Mbps	9.015 Mbps	0 %	1 %
GINT1/1/3 - Gi1/1/3	0.0 bps	0.0 bps	0 %	0 %
GINT1/1/4 - Gi1/1/4	0.0 bps	0.0 bps	0 %	0 %
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %
StackPort1	0.0 bps	0.0 bps	0 %	0 %
StackSub-St1-1	0.0 bps	0.0 bps	0 %	0 %
StackSub-St1-2	0.0 bps	0.0 bps	0 %	0 %
TenGINT1/1/1 - Te1/1/1	0.0 bps	0.0 bps	0 %	0 %
TenGINT1/1/2 - Te1/1/2	0.0 bps	0.0 bps	0 %	0 %
Vlan1 - Vl1	0.0 bps	0.0 bps	0 %	0 %
Vlan10 - Vl10	2.468 kbps	12.78 kbps	0 %	0 %
Vlan20 - Vl20	2.681 kbps	22.18 kbps	0 %	0 %
Vlan30 - Vl30	8.577 kbps	18.231 kbps	0 %	0 %
Vlan40 - Vl40	10.77 kbps	32.779 kbps	0 %	0 %
Vlan5 - Vl5	585.38 bps	4.204 kbps	0 %	0 %
CivilS-Erca.AD				
GINT0/0 · Connection to Ethiotelcom	10.721 kbps	138.833 kbps	0 %	0 %
GINT0/1 · Connection to Civil_S L3 switch	36.434 kbps	3.753 kbps	0 %	0 %
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %
CS-DC2950-24				
FSTETH/1 - Fa0/1	0.0 bps	0.0 bps	0 %	0 %
FSTETH/10 - Fa0/10	10.394 kbps	35.44 bps	0 %	0 %
FSTETH/11 - Fa0/11	13.13 kbps	2.186 kbps	0 %	0 %
FSTETH/12 - Fa0/12	233.443 kbps	47.696 kbps	0 %	0 %
FSTETH/13 - Fa0/13	12.857 kbps	97.99 bps	0 %	0 %

FSTETH/14 - Fa0/14		25.642 kbps	509.33 bps	0 %	0 %
FSTETH/15 - Fa0/15		0.0 bps	0.0 bps	0 %	0 %
FSTETH/16 - Fa0/16		0.0 bps	0.0 bps	0 %	0 %
FSTETH/17 - Fa0/17		0.0 bps	0.0 bps	0 %	0 %
FSTETH/18 - Fa0/18		0.0 bps	0.0 bps	0 %	0 %
FSTETH/19 - Fa0/19		0.0 bps	0.0 bps	0 %	0 %
FSTETH/2 - Fa0/2		0.0 bps	0.0 bps	0 %	0 %
FSTETH/20 - Fa0/20		552.811 kbps	1.006 Mbps	1 %	1 %
FSTETH/21 - Fa0/21		228.859 kbps	5.97 kbps	0 %	0 %
FSTETH/22 - Fa0/22		0.0 bps	0.0 bps	0 %	0 %
FSTETH/23 - Fa0/23		0.0 bps	0.0 bps	0 %	0 %
FSTETH/24 - Fa0/24		0.0 bps	0.0 bps	0 %	0 %
FSTETH/3 - Fa0/3		10.633 kbps	565.93 bps	0 %	0 %
FSTETH/4 - Fa0/4		100.886 kbps	2.016 Mbps	0 %	2 %
FSTETH/5 - Fa0/5		0.0 bps	0.0 bps	0 %	0 %
FSTETH/6 - Fa0/6		11.516 kbps	1.786 kbps	0 %	0 %
FSTETH/7 - Fa0/7		52.19 kbps	91.912 kbps	0 %	0 %
FSTETH/8 - Fa0/8		1.964 Mbps	12.964 kbps	2 %	0 %
FSTETH/9 - Fa0/9		24.216 kbps	320.024 kbps	0 %	0 %
GINT0/1 - Gi0/1		8.971 kbps	3.646 kbps	0 %	0 %
GINT0/2 - Gi0/2		2.286 Mbps	1.372 Mbps	0 %	0 %
Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
Vlan1 - Vl1		12.03 kbps	48.974 kbps	0 %	0 %
DatabaseSW.revenue.gov					
FSTETH/18 - Fa0/18		0.0 bps	0.0 bps	0 %	0 %

FSTETH/19 - Fa0/19	0.0 bps	0.0 bps	0 %	0 %	
FSTETH/21 - Fa0/21	6.254 kbps	0.0 bps	0 %	0 %	
GINT0/2 - Gi0/2	0.0 bps	0.0 bps	0 %	0 %	
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %	
ERCAMISAS-NEW.revenue.gov					
FSTETH/4 - Fa0/4	0.0 bps	0.0 bps	0 %	0 %	
FSTETH/5 - Fa0/5	12.568 kbps	590.39 bps	0 %	0 %	
FSTETH/6 - Fa0/6	0.0 bps	0.0 bps	0 %	0 %	
GINT0/1 - Gi0/1	11.162 kbps	73.313 kbps	0 %	0 %	
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %	
Vlan1 - Vl1	351.45 bps	851.58 bps	0 %	0 %	
ERCA-MIS-ASR-01.revenue.gov					
Crypto-Engine0/0/8 - Cr0/0/8	0.0 bps	0.0 bps	0 %	0 %	
GINT0/0/0 · Connection to MIS core switch	11.414 Mbps	21.3 Mbps	1 %	2 %	
GINT0/0/1 · Connection to redundancy	515.66 bps	0.0 bps	0 %	0 %	
GINT0/0/2 · Connection to ETC fiber connection	21.394 Mbps	11.553 Mbps	2 %	1 %	
Loopback0 - Lo0	443.25 bps	0.0 bps	0 %	0 %	
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %	
ERCAMISFPAS					
FSTETH/1 - Fa0/1	0.0 bps	0.0 bps	0 %	0 %	
FSTETH/10 - Fa0/10	0.0 bps	0.0 bps	0 %	0 %	
FSTETH/11 - Fa0/11	0.0 bps	0.0 bps	0 %	0 %	
FSTETH/12 - Fa0/12	0.0 bps	0.0 bps	0 %	0 %	
FSTETH/13 - Fa0/13	0.0 bps	0.0 bps	0 %	0 %	
FSTETH/14 - Fa0/14	0.0 bps	0.0 bps	0 %	0 %	
FSTETH/15 - Fa0/15	24.233 kbps	230.66 bps	0 %	0 %	
FSTETH/16 - Fa0/16	0.0 bps	0.0 bps	0 %	0 %	

FSTETH/17 - Fa0/17	24.233 kbps	230.66 bps	0 %	0 %
FSTETH/18 - Fa0/18	24.233 kbps	230.66 bps	0 %	0 %
FSTETH/19 - Fa0/19	24.068 kbps	164.02 bps	0 %	0 %
FSTETH/2 - Fa0/2	0.0 bps	0.0 bps	0 %	0 %
FSTETH/20 - Fa0/20	24.233 kbps	230.66 bps	0 %	0 %
FSTETH/21 - Fa0/21	0.0 bps	0.0 bps	0 %	0 %
FSTETH/22 - Fa0/22	2.441 kbps	62.629 kbps	0 %	0 %
FSTETH/23 - Fa0/23	0.0 bps	0.0 bps	0 %	0 %
FSTETH/24 - Fa0/24	0.0 bps	0.0 bps	0 %	0 %
FSTETH/3 - Fa0/3	0.0 bps	0.0 bps	0 %	0 %
FSTETH/4 - Fa0/4	0.0 bps	0.0 bps	0 %	0 %
FSTETH/5 - Fa0/5	0.0 bps	0.0 bps	0 %	0 %
FSTETH/6 - Fa0/6	0.0 bps	0.0 bps	0 %	0 %
FSTETH/7 - Fa0/7	24.113 kbps	127.97 bps	0 %	0 %
FSTETH/8 - Fa0/8	0.0 bps	0.0 bps	0 %	0 %
FSTETH/9 - Fa0/9	0.0 bps	0.0 bps	0 %	0 %
GINT0/1 - Gi0/1	0.0 bps	0.0 bps	0 %	0 %
GINT0/2 - Gi0/2	0.0 bps	0.0 bps	0 %	0 %
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %
Vlan1 - Vl1	661.88 bps	967.51 bps	0 %	0 %
ERCA-SLB-02				
net0	15.18 kbps	3.742 kbps	0 %	0 %
utp ethernet (10/100) - Port 3	927.124 kbps	1.531 Mbps	0 %	0 %
utp ethernet (10/100) - Port 6	70.871 kbps	15.353 kbps	0 %	0 %
utp ethernet (10/100) - Port 7	1.3 Mbps	846.346 kbps	0 %	0 %

	utp ethernet (10/100) - Port 8		64.537 kbps	38.27 kbps	0 %	0 %
ERCASRVAS01.revenue.gov						
	GINT0/14 - Gi0/14		0.0 bps	0.0 bps	0 %	0 %
	GINT0/16 - Gi0/16		0.0 bps	0.0 bps	0 %	0 %
	GINT0/17 - Gi0/17		0.0 bps	0.0 bps	0 %	0 %
	GINT0/18 - Gi0/18		0.0 bps	0.0 bps	0 %	0 %
	GINT0/2 - Gi0/2		0.0 bps	0.0 bps	0 %	0 %
	GINT0/3 - Gi0/3		0.0 bps	0.0 bps	0 %	0 %
	GINT0/36 - Gi0/36		0.0 bps	0.0 bps	0 %	0 %
	GINT0/39 - Gi0/39		0.0 bps	0.0 bps	0 %	0 %
	GINT0/46 · Connection to FRMISCS01		4.868 kbps	302.926 kbps	0 %	0 %
	GINT0/47 · Connection to FRMISCS02		0.0 bps	0.0 bps	0 %	0 %
	GINT0/48 · Connection to FRMISCS02		298.038 kbps	17.07 bps	0 %	0 %
	GINT0/49 - Gi0/49		0.0 bps	0.0 bps	0 %	0 %
	GINT0/51 - Gi0/51		7.079 Mbps	123.155 Mbps	1 %	12 %
	GINT0/52 - Gi0/52		12.811 Mbps	23.843 Mbps	1 %	2 %
	Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
	Port-channel1 · Connection to FRMISCS02		298.252 kbps	17.07 bps	0 %	0 %
	Port-channel2 · Connection to FRMISCS01		4.92 kbps	303.189 kbps	0 %	0 %
	Vlan1 - Vl1		1.475 kbps	1.437 kbps	0 %	0 %
	Vlan180 - Vl180		0.0 bps	2.186 kbps	0 %	0 %
	Vlan6 - Vl6		0.0 bps	0.0 bps	0 %	0 %
ERCA-STR-DC-CTR1.revenue.gov						
	e0a		2.39 kbps	51.814 kbps	0 %	0 %
	e0M		41.964 kbps	55.359 kbps	0 %	0 %

	ERCA-VPIP1		2.39 kbps	51.814 kbps	0 %	0 %
	lo		0.0 bps	0.0 bps	0 %	0 %
	losk		261.76 bps	0.0 bps	0 %	0 %
ERCA-STR-DC-CTR2						
	e0a		0.0 bps	0.0 bps	0 %	0 %
	e0b		0.0 bps	0.0 bps	0 %	0 %
	e0M		2.577 kbps	47.838 kbps	0 %	0 %
	lo		0.0 bps	0.0 bps	0 %	0 %
	losk		165.38 bps	0.0 bps	0 %	0 %
	vh		0.0 bps	0.0 bps	0 %	0 %
Esxi-host 2						
	Device vmnic0 at 04:00.0 nx_nic · 04:00.0		0.0 bps	0.0 bps	0 %	0 %
	Device vmnic1 at 04:00.1 nx_nic · 04:00.1		90.506 kbps	315.469 kbps	0 %	0 %
	Device vmnic2 at 04:00.2 nx_nic · 04:00.2		0.0 bps	0.0 bps	0 %	0 %
	Device vmnic3 at 04:00.3 nx_nic · 04:00.3		7.291 Mbps	3.369 Mbps	1 %	0 %
	LIA 10 G VM Network on switch: vSwitch1, load balancing algorithm: source port id hash · vSwitch1		7.292 Mbps	3.369 Mbps	0 %	0 %
	LIA Management Network on switch: vSwitch0, load balancing algorithm: source port id hash · vSwitch0		2.944 Mbps	7.295 Mbps	0 %	1 %
	LIA VLAN 172 Vswitch 2 on switch: vSwitch1, load balancing algorithm: source port id hash · vSwitch1		38.386 kbps	469.483 kbps	0 %	0 %
	LIA VLAN 50 Vswitch on switch: vSwitch1, load balancing algorithm: source port id hash · vSwitch1		38.386 kbps	469.483 kbps	0 %	0 %
	LIA VM Network 2 on switch: vSwitch1, load balancing algorithm: source port id hash · vSwitch1		267.392 kbps	372.729 kbps	0 %	0 %
	LIA VM Network on switch: vSwitch0, load balancing algorithm: source port id hash · vSwitch0		2.944 Mbps	7.295 Mbps	0 %	1 %
	LIA vMotion1 on switch: vSwitch1, load balancing algorithm: source port id hash · vSwitch1		7.291 Mbps	3.369 Mbps	0 %	0 %

Traditional Virtual VMware switch: vSwitch0 · vSwitch0	?	0.0 bps	0.0 bps	0 %	0 %
Traditional Virtual VMware switch: vSwitch1 · vSwitch1	?	0.0 bps	0.0 bps	0 %	0 %
VI: vmk0 on vswitch vSwitch0 portgroup: Management Network · vmk0-vSwitch0		0.0 bps	32.223 kbps	0 %	0 %
exch01.revenue.gov					
HP NC373i Multifunction Gigabit Server Adapter #5 · Local Area Connection		15.836 kbps	45.677 kbps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #5-QoS Packet Scheduler-0000 · Local Area Connection-QoS Packet Scheduler-0000		15.836 kbps	45.677 kbps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #5-WFP LightWeight Filter-0000 · Local Area Connection-WFP LightWeight Filter-0000		15.836 kbps	45.677 kbps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #60 · Private		0.0 bps	399.65 bps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #60-QoS Packet Scheduler-0000 · Private-QoS Packet Scheduler-0000		0.0 bps	399.65 bps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #60-WFP LightWeight Filter-0000 · Private-WFP LightWeight Filter-0000		0.0 bps	399.65 bps	0 %	0 %
Microsoft Failover Cluster Virtual Adapter · Local Area Connection* 9		0.0 bps	0.0 bps	0 %	0 %
Microsoft Failover Cluster Virtual Adapter-QoS Packet Scheduler-0000 · Local Area Connection* 9-QoS Packet Scheduler-0000		0.0 bps	0.0 bps	0 %	0 %
Microsoft Failover Cluster Virtual Adapter-WFP LightWeight Filter-0000 · Local Area Connection* 9-WFP LightWeight Filter-0000		0.0 bps	0.0 bps	0 %	0 %
RAS Async Adapter · Local Area Connection* 10		0.0 bps	0.0 bps	0 %	0 %
Software Loopback Interface 1 · Loopback Pseudo-Interface 1		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP) · Local Area Connection* 8		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP)-QoS Packet Scheduler-0000 · Local Area Connection* 8-QoS Packet Scheduler-0000		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IPv6) · Local Area Connection* 6		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IPv6)-QoS Packet Scheduler-0000 · Local Area Connection* 6-QoS Packet Scheduler-0000		0.0 bps	0.0 bps	0 %	0 %

WAN Miniport (L2TP) · Local Area Connection* 3	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor) · Local Area Connection* 7	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000 · Local Area Connection* 7-QoS Packet Scheduler-0000	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (PPPOE) · Local Area Connection* 5	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (PPTP) · Local Area Connection* 4	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (SSTP) · Local Area Connection*	0.0 bps	0.0 bps	0 %	0 %
exch02.revenue.gov				
HP NC373i Multifunction Gigabit Server Adapter #59 · Private	0.0 bps	0.0 bps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #59-QoS Packet Scheduler-0000 · Private-QoS Packet Scheduler-0000	0.0 bps	0.0 bps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #59-WFP LightWeight Filter-0000 · Private-WFP LightWeight Filter-0000	0.0 bps	0.0 bps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #60 · Local Area Connection	8.848 kbps	55.012 kbps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #60-QoS Packet Scheduler-0000 · Local Area Connection-QoS Packet Scheduler-0000	4.925 kbps	43.73 kbps	0 %	0 %
HP NC373i Multifunction Gigabit Server Adapter #60-WFP LightWeight Filter-0000 · Local Area Connection-WFP LightWeight Filter-0000	4.925 kbps	43.73 kbps	0 %	0 %
Microsoft Failover Cluster Virtual Adapter · Local Area Connection* 9	0.0 bps	0.0 bps	0 %	0 %
Microsoft Failover Cluster Virtual Adapter-QoS Packet Scheduler-0000 · Local Area Connection* 9-QoS Packet Scheduler-0000	0.0 bps	0.0 bps	0 %	0 %
Microsoft Failover Cluster Virtual Adapter-WFP LightWeight Filter-0000 · Local Area Connection* 9-WFP LightWeight Filter-0000	0.0 bps	0.0 bps	0 %	0 %
RAS Async Adapter · Local Area Connection* 10	0.0 bps	0.0 bps	0 %	0 %
Software Loopback Interface 1 · Loopback Pseudo-Interface 1	0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IP) · Local Area Connection* 8	0.0 bps	0.0 bps	0 %	0 %

WAN Miniport (IP)-QoS Packet Scheduler-0000 · Local Area Connection* 8-QoS Packet Scheduler-0000		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IPv6) · Local Area Connection* 6		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (IPv6)-QoS Packet Scheduler-0000 · Local Area Connection* 6-QoS Packet Scheduler-0000		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (L2TP) · Local Area Connection* 3		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor) · Local Area Connection* 7		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000 · Local Area Connection* 7-QoS Packet Scheduler-0000		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (PPPOE) · Local Area Connection* 5		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (PPTP) · Local Area Connection* 4		0.0 bps	0.0 bps	0 %	0 %
WAN Miniport (SSTP) · Local Area Connection*		0.0 bps	0.0 bps	0 %	0 %
GAD					
Embedded-Service-Engine0/0 - Em0/0		0.0 bps	0.0 bps	0 %	0 %
GINT0/0 · Connection To ISP		188.657 kbps	186.975 kbps	0 %	0 %
GINT0/1 · Connection To Internal Network		195.15 kbps	201.695 kbps	0 %	0 %
GINT0/3 - Gi0/3		0.0 bps	0.0 bps	0 %	0 %
Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
GLSW-3560G-48					
GINT0/47 · Link to BLKD_L3-24 Switch		0.0 bps	0.0 bps	0 %	0 %
GINT0/49 · "Connection with DCSW-3560G-48"		0.0 bps	0.0 bps	0 %	0 %
Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
Gprs-R.erca.gov					
FSTETH/0 · Connection to MIS core switch		1.003 kbps	572.79 bps	0 %	0 %
FSTETH/1 · Connection to GPRS ADSL		177.42 bps	60.28 bps	0 %	0 %
Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
INTERNET-cON-7206					

	GINT0/1 - Gi0/1		28.262 Mbps	4.793 Mbps	3 %	0 %
	GINT0/2 - Gi0/2		6.125 Mbps	28.611 Mbps	1 %	3 %
	GINT0/3 - Gi0/3		348.501 kbps	1.33 Mbps	0 %	0 %
	Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
JAD						
	Embedded-Service-Engine0/0 - Em0/0		0.0 bps	0.0 bps	0 %	0 %
	GINT0/0 · Connection to Ethio~Telecom		55.424 kbps	61.671 kbps	0 %	0 %
	GINT0/1 · IN-LAN		14.014 kbps	9.73 kbps	0 %	0 %
	GINT0/3 - Gi0/3		0.0 bps	0.0 bps	0 %	0 %
	Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
CustK~CoMet						
	GINT0/6 · "Connection to 10.18.1.55 (ZTE Switch) with VLAN55"		0.0 bps	0.0 bps	0 %	0 %
	Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
localhost						
	Device vmnic0 at 04:00.0 nx_nic · 04:00.0		2.536 kbps	248.584 kbps	0 %	0 %
	Device vmnic0 at 04:00.0 nx_nic · 04:00.0		20.862 kbps	55.325 kbps	0 %	0 %
	Device vmnic0 at 04:00.0 nx_nic · 04:00.0		2.355 Mbps	2.804 Mbps	0 %	0 %
	Device vmnic1 at 04:00.1 nx_nic · 04:00.1		1.499 Mbps	2.814 Mbps	0 %	0 %
	Device vmnic1 at 04:00.1 nx_nic · 04:00.1		33.16 kbps	178.564 kbps	0 %	0 %
	Device vmnic1 at 04:00.1 nx_nic · 04:00.1		559.931 kbps	11.305 Mbps	0 %	1 %
	Device vmnic2 at 04:00.2 nx_nic · 04:00.2		0.0 bps	0.0 bps	0 %	0 %
	Device vmnic2 at 04:00.2 nx_nic · 04:00.2		692.111 kbps	1.307 Mbps	0 %	0 %
	Device vmnic3 at 04:00.3 nx_nic · 04:00.3		589.944 kbps	5.646 Mbps	0 %	1 %
	Device vmnic3 at 04:00.3 nx_nic · 04:00.3		0.0 bps	0.0 bps	0 %	0 %

	LIA 10 G Network on switch: vSwitch1, load balancing algorithm: source port id hash · vSwitch1		1.282 Mbps	6.953 Mbps	0 %	1 %
	LIA Management Network on switch: vSwitch0, load balancing algorithm: source port id hash · vSwitch0		3.854 Mbps	5.618 Mbps	0 %	1 %
	LIA Management Network on switch: vSwitch0, load balancing algorithm: source port id hash · vSwitch0		0.0 bps	0.0 bps	0 %	0 %
	LIA NBE on switch: vSwitch0, load balancing algorithm: source port id hash · vSwitch0		0.0 bps	0.0 bps	0 %	0 %
	LIA VLAN 10 vswitch 2 on switch: vSwitch1, load balancing algorithm: source port id hash · vSwitch1		4.692 Mbps	6.839 Mbps	0 %	1 %
	LIA vlan 172 vSwitch0 on switch: vSwitch0, load balancing algorithm: source port id hash · vSwitch0		2.442 Mbps	3.035 Mbps	0 %	0 %
	LIA VLAN 50 on switch: vSwitch0, load balancing algorithm: source port id hash · vSwitch0		3.854 Mbps	5.618 Mbps	0 %	1 %
	LIA VM Network 2 on switch: vSwitch1, load balancing algorithm: source port id hash · vSwitch1		1.282 Mbps	6.953 Mbps	0 %	1 %
	LIA VM Network on switch: vSwitch0, load balancing algorithm: source port id hash · vSwitch0		3.854 Mbps	5.618 Mbps	0 %	1 %
	LIA VM Network on switch: vSwitch0, load balancing algorithm: source port id hash · vSwitch0		54.023 kbps	233.889 kbps	0 %	0 %
	LIA VM Network on switch: vSwitch0, load balancing algorithm: source port id hash · vSwitch0		0.0 bps	0.0 bps	0 %	0 %
	LIA vMnetwork vSwitch1 on switch: vSwitch1, load balancing algorithm: source port id hash · vSwitch1		0.0 bps	0.0 bps	0 %	0 %
	LIA Vswitch 2 VLAN 50 on switch: vSwitch1, load balancing algorithm: source port id hash · vSwitch1		1.282 Mbps	6.953 Mbps	0 %	1 %
	Traditional Virtual VMware switch: vSwitch0 · vSwitch0	?	0.0 bps	0.0 bps	0 %	0 %
	Traditional Virtual VMware switch: vSwitch0 · vSwitch0	?	0.0 bps	0.0 bps	0 %	0 %
	Traditional Virtual VMware switch: vSwitch0 · vSwitch0	?	0.0 bps	0.0 bps	0 %	0 %
	Traditional Virtual VMware switch: vSwitch1 · vSwitch1	?	0.0 bps	0.0 bps	0 %	0 %
	Traditional Virtual VMware switch: vSwitch1 · vSwitch1	?	0.0 bps	0.0 bps	0 %	0 %

VI: vmk0 on vswitch vSwitch0 portgroup: Management Network · vmk0-vSwitch0	0.0 bps	25.836 kbps	0 %	0 %
VI: vmk0 on vswitch vSwitch0 portgroup: Management Network · vmk0-vSwitch0	0.0 bps	12.887 kbps	0 %	0 %
VI: vmk0 on vswitch vSwitch0 portgroup: Management Network · vmk0-vSwitch0	0.0 bps	28.157 kbps	0 %	0 %
VI: vmk2 on vswitch vSwitch0 portgroup: vlan 172 vSwitch0 · vmk2-vSwitch0	0.0 bps	87.11 bps	0 %	0 %
MiS-ASW-02.revenue.gov				
GINT0/10 - Gi0/10	0.0 bps	0.0 bps	0 %	0 %
GINT0/17 - Gi0/17	0.0 bps	0.0 bps	0 %	0 %
GINT0/18 - Gi0/18	0.0 bps	0.0 bps	0 %	0 %
GINT0/2 · connection to CS1	0.0 bps	0.0 bps	0 %	0 %
GINT0/21 - Gi0/21	0.0 bps	0.0 bps	0 %	0 %
GINT0/23 - Gi0/23	0.0 bps	0.0 bps	0 %	0 %
GINT0/24 - Gi0/24	0.0 bps	0.0 bps	0 %	0 %
GINT0/25 - Gi0/25	0.0 bps	0.0 bps	0 %	0 %
GINT0/28 - Gi0/28	0.0 bps	0.0 bps	0 %	0 %
GINT0/3 - Gi0/3	0.0 bps	0.0 bps	0 %	0 %
GINT0/45 · Connection to FRMISCS01	1.327 kbps	111.069 kbps	0 %	0 %
GINT0/46 · Connection to FRMISCS01	116.77 bps	25.694 kbps	0 %	0 %
GINT0/47 · Connection to FRMISCS02	4.708 kbps	89.157 kbps	0 %	0 %
GINT0/48 · Connection to FRMISCS02	762.4 bps	60.621 kbps	0 %	0 %
GINT0/5 - Gi0/5	0.0 bps	0.0 bps	0 %	0 %
GINT0/9 - Gi0/9	0.0 bps	0.0 bps	0 %	0 %
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %
Port-channel1 · Connection to FRMISCS02	0.0 bps	0.0 bps	0 %	0 %
Port-channel2 · Connection to FRMISCS01	0.0 bps	0.0 bps	0 %	0 %
Vlan1 - Vl1	900.41 bps	769.36 bps	0 %	0 %
MiS-CS-01.revenue.gov				

GINT2/1 - Gi2/1	6.98 Mbps	49.157 Mbps	1 %	5 %
GINT2/10 · "CONNECTION TO TEMP-SW01"	18.408 Mbps	4.917 Mbps	2 %	0 %
GINT2/11 · "CONNECTION TO TEMP-SW01"	2.533 Mbps	78.015 Mbps	0 %	8 %
GINT2/12 · "CONNECTION TO SW3 GI0/45"	5.175 Mbps	217.262 kbps	1 %	0 %
GINT2/13 · "CONNECTION TO SW3 GI0/46"	3.908 Mbps	2.598 Mbps	0 %	0 %
GINT2/15 · Connection To WAN-1	23.697 Mbps	12.568 Mbps	2 %	1 %
GINT2/19 · "CONNECTION TO SW2 GI0/45"	13.485 Mbps	14.764 Mbps	1 %	1 %
GINT2/2 - Gi2/2	0.0 bps	0.0 bps	0 %	0 %
GINT2/20 · "CONNECTION TO SW2 GI0/46"	12.168 Mbps	2.731 Mbps	1 %	0 %
GINT2/22 · "CONNECTION TO USER SW1 GI0/2"	17.07 bps	17.07 bps	0 %	0 %
GINT2/23 - Gi2/23	25.943 Mbps	16.527 Mbps	3 %	2 %
GINT2/24 - Gi2/24	102.832 Mbps	33.668 Mbps	10 %	3 %
GINT2/4 · "CONNECTION TO ZTE THEN TO NBE"	44.516 kbps	161.897 kbps	0 %	0 %
GINT2/5 · "Connection to eSW-Router"	17.754 kbps	492.294 kbps	0 %	0 %
GINT2/6 · "CONNECTION TO TEMP-SW02"	312.108 kbps	413.835 kbps	0 %	0 %
GINT2/8 - Gi2/8	296.599 kbps	4.891 kbps	0 %	0 %
GINT2/9 · "CONNECTION TO SINGLE WINDOW SWITCH"	0.0 bps	0.0 bps	0 %	0 %
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %
Vlan1 · Network Management Stations and Devices	27.573 kbps	1.947 Mbps	0 %	0 %
Vlan198 · Connection to GPRS	1.836 Mbps	655.671 kbps	0 %	0 %
Vlan199 · Connection to WAN	2.521 Mbps	3.47 bps	0 %	0 %
MiS-Edge-02.revenue.gov				
GINT0/1 · "Domestic Server Farm"	197.792 kbps	1.346 kbps	0 %	0 %

GINT0/2 · "Domestic Server Farm"	0.0 bps	0.0 bps	0 %	0 %
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %
MiS-Edge-03				
GINT0/10 · "CONNECTION TO ACS2"	6.276 kbps	1.93 bps	0 %	0 %
GINT0/26 · "CONNECTION TO MOF SERVER"	59.887 kbps	3.054 kbps	0 %	0 %
GINT0/29 · "CONNECTION TO EFW-MGMT"	58.138 kbps	1.103 kbps	0 %	0 %
GINT0/30 · "CONNECTION TO IFW-MGMT"	1.976 Mbps	34.527 kbps	0 %	0 %
GINT0/4 · 1G connection to ESXiHost1	17.041 kbps	2.16 kbps	0 %	0 %
GINT0/41 · "CONNECTION TO CARGO ROUTER ON INTERFACE Fei1/2"	13.51 kbps	116.23 bps	0 %	0 %
GINT0/42 · "CONNECTION TO DTI ROUTER ON INTERFACE Fei1/2"	109.721 kbps	6.848 kbps	0 %	0 %
GINT0/5 · 1G connection to ESXiHost1	1.112 kbps	184.53 bps	0 %	0 %
GINT0/7 · 10G connection to ESXiHost1	113.538 kbps	0.0 bps	0 %	0 %
GINT0/8 · "CONNECTION TO GPRS ROUTER"	1.289 kbps	1.007 kbps	0 %	0 %
GINT0/9 · "CONNECTION TO ACS1"	6.274 kbps	4.27 bps	0 %	0 %
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %
MISG				
FSTETH/15 - Fa0/15	0.0 bps	0.0 bps	0 %	0 %
FSTETH/16 - Fa0/16	0.0 bps	0.0 bps	0 %	0 %
FSTETH/18 - Fa0/18	0.0 bps	0.0 bps	0 %	0 %
FSTETH/30 - Fa0/30	0.0 bps	0.0 bps	0 %	0 %
FSTETH/31 - Fa0/31	0.0 bps	0.0 bps	0 %	0 %
FSTETH/37 - Fa0/37	0.0 bps	0.0 bps	0 %	0 %
FSTETH/38 - Fa0/38	0.0 bps	0.0 bps	0 %	0 %
GINT0/1 - Gi0/1	117.243 kbps	15.602 kbps	0 %	0 %
GINT0/2 - Gi0/2	0.0 bps	0.0 bps	0 %	0 %
Null0 - Nu0	0.0 bps	0.0 bps	0 %	0 %

MOR-ADMA-R						
	Backplane-GINT0/3 - Ba0/3		0.0 bps	0.0 bps	0 %	0 %
	Embedded-Service-Engine0/0 - Em0/0		0.0 bps	0.0 bps	0 %	0 %
	GINT0/0 · connection to ISP-WAN		893.334 kbps	1.825 Mbps	0 %	0 %
	GINT0/1 · IN-LAN		1.864 Mbps	959.735 kbps	2 %	1 %
	Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
MLAN						
	GINT0/10 · "Connection to 3RSW-2950-24"		566.7 kbps	27.804 kbps	1 %	0 %
	GINT0/11 · "Connection to 5LSW-2950-24"		428.545 kbps	8.724 kbps	0 %	0 %
	GINT0/13 · CONNECTION TO SERVERFARM SWITCH		860.833 kbps	18.326 kbps	0 %	0 %
	GINT0/15 - Gi0/15		456.151 kbps	12.435 kbps	0 %	0 %
	GINT0/16 · "Connection to 4LSW-2950-24"		243.37 bps	0.0 bps	0 %	0 %
	GINT0/17 - Gi0/17		0.0 bps	0.0 bps	0 %	0 %
	GINT0/18 - Gi0/18		0.0 bps	0.0 bps	0 %	0 %
	GINT0/19 - Gi0/19		0.0 bps	0.0 bps	0 %	0 %
	GINT0/2 · "Connection to 6RSW-2950-24"		416.98 kbps	10.947 kbps	0 %	0 %
	GINT0/22 - Gi0/22		5.868 Mbps	74.826 Mbps	1 %	7 %
	GINT0/23 - Gi0/23		136.93 kbps	116.383 kbps	0 %	0 %
	GINT0/24 - Gi0/24		0.0 bps	0.0 bps	0 %	0 %
	GINT0/26 - Gi0/26		425.68 kbps	0.0 bps	0 %	0 %
	GINT0/3 · "Connection to 3LSW-2950-24"		425.785 kbps	463.58 bps	0 %	0 %
	GINT0/31 · "Connection to CCTV Cameras"		0.0 bps	0.0 bps	0 %	0 %
	GINT0/34 - Gi0/34		4.449 kbps	0.0 bps	0 %	0 %
	GINT0/35 - Gi0/35		0.0 bps	0.0 bps	0 %	0 %
	GINT0/37 · "Connection to server"		25.891 kbps	73.613 kbps	0 %	0 %

	GINT0/39 - Gi0/39		0.0 bps	0.0 bps	0 %	0 %
	GINT0/4 · "Connection to 5RSW-2950-24"		673.042 kbps	61.42 kbps	1 %	0 %
	GINT0/41 - Gi0/41		0.0 bps	0.0 bps	0 %	0 %
	GINT0/42 - Gi0/42		4.43 kbps	92.36 bps	0 %	0 %
	GINT0/43 - Gi0/43		0.0 bps	0.0 bps	0 %	0 %
	GINT0/45 · "Connection with MOFED"		27.484 kbps	104.232 kbps	0 %	0 %
	GINT0/47 · Connection to BLKC_L3-24 Switch		17.951 Mbps	622.197 kbps	18 %	1 %
	GINT0/49 · "Connection with GLSW-3560G-48"		24.621 Mbps	850.022 kbps	2 %	0 %
	GINT0/5 - Gi0/5		1.49 Mbps	96.227 kbps	0 %	0 %
	GINT0/50 · CONNECTION TO ISP		38.766 Mbps	5.628 Mbps	4 %	1 %
	GINT0/7 · "Connection to 1RSW-2950-24"		1.388 Mbps	180.467 kbps	1 %	0 %
	GINT0/9 · "Connection to 2LSW-2950-24"		425.782 kbps	1.505 kbps	0 %	0 %
	Loopback1 - Lo1		0.0 bps	0.0 bps	0 %	0 %
	Loopback10 - Lo10		0.0 bps	0.0 bps	0 %	0 %
	Loopback122 - Lo122		0.0 bps	0.0 bps	0 %	0 %
	Loopback172 - Lo172		0.0 bps	0.0 bps	0 %	0 %
	Loopback198 - Lo198		0.0 bps	0.0 bps	0 %	0 %
	Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
	Port-channel1 - Po1		130.843 Mbps	304.854 Mbps	7 %	15 %
	Vlan1 - Vl1		0.0 bps	10.501 kbps	0 %	0 %
	Vlan10 · BLCK-A Ground Floor		7.84 Mbps	231.369 kbps	1 %	0 %
	Vlan100 · ServerFarm Vlan		9.009 Mbps	217.592 Mbps	1 %	22 %
	Vlan110 - Vl110		30.34 bps	0.0 bps	0 %	0 %
	Vlan125 · APC UPS VLAN		0.95 bps	0.0 bps	0 %	0 %
	Vlan130 · "Connection to CCTV Camera"		0.0 bps	0.0 bps	0 %	0 %

Vlan140 · "Next Room Connection"	0.0 bps	0.0 bps	0 %	0 %
Vlan15 · BLCK-A Fifth Floor	22.047 Mbps	601.202 kbps	2 %	0 %
Vlan151 · to INT-FW	251.2 bps	0.0 bps	0 %	0 %
Vlan158 - Vl158	251.2 bps	0.0 bps	0 %	0 %
Vlan2 - Vl2	0.0 bps	0.0 bps	0 %	0 %
Vlan20 · BLCK-B Ground Floor	1.303 Mbps	80.853 kbps	0 %	0 %
Vlan25 · BLCK-B Fifth Floor	7.972 Mbps	234.132 kbps	1 %	0 %
Vlan30 - Vl30	93.86 bps	126.06 bps	0 %	0 %
Vlan40 - Vl40	113.36 bps	1.681 kbps	0 %	0 %
Vlan45 - Vl45	129.89 bps	661.06 bps	0 %	0 %
Vlan5 · users on datacenter switch	0.0 bps	0.0 bps	0 %	0 %
Vlan50 - Vl50	24.65 bps	0.0 bps	0 %	0 %
Vlan55 - Vl55	80.41 bps	258.48 bps	0 %	0 %
Vlan60 - Vl60	287.27 bps	0.0 bps	0 %	0 %
Vlan65 - Vl65	350.09 bps	284.93 bps	0 %	0 %
Vlan70 - Vl70	0.95 bps	0.0 bps	0 %	0 %
Vlan75 - Vl75	0.95 bps	0.0 bps	0 %	0 %
Vlan8 - Vl8	0.0 bps	0.0 bps	0 %	0 %
Vlan80 · Voice vlan	144.89 bps	236.08 bps	0 %	0 %
Vlan85 - Vl85	2.84 bps	0.0 bps	0 %	0 %
Vlan90 - Vl90	1.9 bps	0.0 bps	0 %	0 %
Vlan95 - Vl95	0.0 bps	0.0 bps	0 %	0 %
MoR-EAST-CS.revenue.gov				
GINT1/0/23 · connection to ISP	1.363 Mbps	7.654 Mbps	0 %	1 %
GINT1/0/24 · CONNECTION TO ETC LINE	127.11 kbps	20.172 kbps	0 %	0 %

	Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
MHW						
	Ethernet0/0 · connection to ISP-WAN		263.077 kbps	1.608 Mbps	3 %	16 %
	FSTETH/0 · IN-LAN		1.612 Mbps	271.543 kbps	2 %	0 %
	Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
NOC-SRV01						
	Broadcom NetXtreme Gigabit Ethernet #2 · NIC1		94.598 kbps	101.03 kbps	0 %	0 %
PostofficeRW.AD						
	Embedded-Service-Engine0/0 - Em0/0		0.0 bps	0.0 bps	0 %	0 %
	GINT0/0 - Gi0/0		5.569 kbps	25.202 kbps	0 %	0 %
	GINT0/1 - Gi0/1		24.749 kbps	5.181 kbps	0 %	0 %
	GINT0/3 - Gi0/3		0.0 bps	0.0 bps	0 %	0 %
	Null0 - Nu0		0.0 bps	0.0 bps	0 %	0 %
WIB 8000 SNMP Interface						
	eth0		246.93 bps	13.89 kbps	0 %	0 %
	LOOPBACK		0.0 bps	0.0 bps	0 %	0 %

D

Downtime

FULL NAME	STATUS	TOTAL DURATION IN MINUTES
AAC- GINT0/24 · IN-LAN	Up	4070
AAC- GINT0/24 · IN-LAN	Down	2

AAC- Vlan1 - Vl1	Warning	4
AAC- Vlan1 - Vl1	Shutdown	4074
BLKD-CSW - GINT1/0/23 · "Connection To EAST Core Switch "	Unknown	5875
BLKD-CSW - GINT1/0/23 · "Connection To EAST Core Switch "	Unreachable	32
BLKD-CSW - Null0 - Nu0	Unknown	5875
BLKD-CSW - Null0 - Nu0	Unreachable	32
BCC - Null0 - Nu0	Unknown	10
BCC - Null0 - Nu0	Up	5871
BCC - Null0 - Nu0	Warning	11
BCC - Null0 - Nu0	Unreachable	20
ARV - Embedded-Service-Engine0/0 - Em0/0	Unknown	4
ARV - Embedded-Service-Engine0/0 - Em0/0	Warning	2
ARV - Embedded-Service-Engine0/0 - Em0/0	Warning	29
ARV - Embedded-Service-Engine0/0 - Em0/0	Shutdown	965
ARV - Embedded-Service-Engine0/0 - Em0/0	Shutdown	5232
ARV - Embedded-Service-Engine0/0 - Em0/0	Unreachable	19
ARV - Embedded-Service-Engine0/0 - Em0/0	Unreachable	2049
ARV - GINT0/0 · connection to ISP	Unknown	4
ARV - GINT0/0 · connection to ISP	Up	967
ARV - GINT0/0 · connection to ISP	Up	5234
ARV - GINT0/0 · connection to ISP	Warning	2
ARV - GINT0/0 · connection to ISP	Warning	27
ARV - GINT0/0 · connection to ISP	Unreachable	17
ARV - GINT0/0 · connection to ISP	Unreachable	2049
ARV - GINT0/1 · connection to Internal-LAN	Unknown	4
ARV - GINT0/1 · connection to Internal-LAN	Up	967
ARV - GINT0/1 · connection to Internal-LAN	Up	5236
ARV - GINT0/1 · connection to Internal-LAN	Warning	2
ARV - GINT0/1 · connection to Internal-LAN	Warning	26
ARV - GINT0/1 · connection to Internal-LAN	Unreachable	17
ARV - GINT0/1 · connection to Internal-LAN	Unreachable	2048
ARV - GINT0/3 - Gi0/3	Unknown	4
ARV - GINT0/3 - Gi0/3	Up	967
ARV - GINT0/3 - Gi0/3	Up	5236
ARV - GINT0/3 - Gi0/3	Warning	2
ARV - GINT0/3 - Gi0/3	Warning	26
ARV - GINT0/3 - Gi0/3	Unreachable	17
ARV - GINT0/3 - Gi0/3	Unreachable	2048
ARV - Null0 - Nu0	Unknown	4
ARV - Null0 - Nu0	Up	967

ARV - Null0 - Nu0	Up	5239
ARV - Null0 - Nu0	Warning	2
ARV - Null0 - Nu0	Warning	25
ARV - Null0 - Nu0	Unreachable	17
ARV - Null0 - Nu0	Unreachable	2046
JRRD - Embedded-Service-Engine0/0 - Em0/0	Unknown	2
JRRD - Embedded-Service-Engine0/0 - Em0/0	Unknown	10
JRRD - Embedded-Service-Engine0/0 - Em0/0	Warning	18
JRRD - Embedded-Service-Engine0/0 - Em0/0	Warning	71
JRRD - Embedded-Service-Engine0/0 - Em0/0	Shutdown	2291
JRRD - Embedded-Service-Engine0/0 - Em0/0	Shutdown	7235
JRRD - Embedded-Service-Engine0/0 - Em0/0	Unreachable	230
JRRD - Embedded-Service-Engine0/0 - Em0/0	Unreachable	575
JRRD - GINT0/0 · connection to ISP-WAN	Unknown	2
JRRD - GINT0/0 · connection to ISP-WAN	Unknown	8
JRRD - GINT0/0 · connection to ISP-WAN	Up	2291
JRRD - GINT0/0 · connection to ISP-WAN	Up	7241
JRRD - GINT0/0 · connection to ISP-WAN	Warning	18
JRRD - GINT0/0 · connection to ISP-WAN	Warning	70
JRRD - GINT0/0 · connection to ISP-WAN	Unreachable	228
JRRD - GINT0/0 · connection to ISP-WAN	Unreachable	574
JRRD - GINT0/1 · NLAN	Unknown	2
JRRD - GINT0/1 · NLAN	Unknown	8
JRRD - GINT0/1 · NLAN	Up	2291
JRRD - GINT0/1 · NLAN	Up	7246
JRRD - GINT0/1 · NLAN	Warning	18
JRRD - GINT0/1 · NLAN	Warning	68
JRRD - GINT0/1 · NLAN	Unreachable	228
JRRD - GINT0/1 · NLAN	Unreachable	571
JRRD - GINT0/3 - Gi0/3	Unknown	2
JRRD - GINT0/3 - Gi0/3	Unknown	8
JRRD - GINT0/3 - Gi0/3	Up	2291
JRRD - GINT0/3 - Gi0/3	Up	7257
JRRD - GINT0/3 - Gi0/3	Warning	18
JRRD - GINT0/3 - Gi0/3	Warning	68
JRRD - GINT0/3 - Gi0/3	Unreachable	228
JRRD - GINT0/3 - Gi0/3	Unreachable	560
JRRD - Null0 - Nu0	Unknown	1
JRRD - Null0 - Nu0	Unknown	4
JRRD - Null0 - Nu0	Up	2292
JRRD - Null0 - Nu0	Up	7268

JRRD - Null0 - Nu0	Warning	18
JRRD - Null0 - Nu0	Warning	69
JRRD - Null0 - Nu0	Unreachable	228
JRRD - Null0 - Nu0	Unreachable	552
CC-CustK-CS - GINT1/0/1 · "To Ethio-Telecom Side"	Unknown	2
CC-CustK-CS - GINT1/0/1 · "To Ethio-Telecom Side"	Unknown	2
CC-CustK-CS - GINT1/0/1 · "To Ethio-Telecom Side"	Up	2223
CC-CustK-CS - GINT1/0/1 · "To Ethio-Telecom Side"	Up	5939
CC-CustK-CS - GINT1/0/1 · "To Ethio-Telecom Side"	Warning	2
CC-CustK-CS - GINT1/0/1 · "To Ethio-Telecom Side"	Warning	6
CC-CustK-CS - GINT1/0/1 · "To Ethio-Telecom Side"	Unreachable	7
CC-CustK-CS - GINT1/0/1 · "To Ethio-Telecom Side"	Unreachable	1066
CC-CustK-CS - Null0 - Nu0	Unknown	2
CC-CustK-CS - Null0 - Nu0	Unknown	2
CC-CustK-CS - Null0 - Nu0	Up	2223
CC-CustK-CS - Null0 - Nu0	Up	5939
CC-CustK-CS - Null0 - Nu0	Warning	2
CC-CustK-CS - Null0 - Nu0	Warning	6
CC-CustK-CS - Null0 - Nu0	Unreachable	7
CC-CustK-CS - Null0 - Nu0	Unreachable	1066
CC-MIL-R.RG- Backplane-GINT0/3 - Ba0/3	Unknown	12
CC-MIL-R.RG- Backplane-GINT0/3 - Ba0/3	Unknown	18
CC-MIL-R.RG- Backplane-GINT0/3 - Ba0/3	Up	3352
CC-MIL-R.RG- Backplane-GINT0/3 - Ba0/3	Up	6732
CC-MIL-R.RG- Backplane-GINT0/3 - Ba0/3	Warning	5
CC-MIL-R.RG- Backplane-GINT0/3 - Ba0/3	Warning	13
CC-MIL-R.RG- Backplane-GINT0/3 - Ba0/3	Unreachable	70
CC-MIL-R.RG- Backplane-GINT0/3 - Ba0/3	Unreachable	152
CC-MIL-R.RG- GINT0/0 · "connection to ISP"	Unknown	12
CC-MIL-R.RG- GINT0/0 · "connection to ISP"	Unknown	20
CC-MIL-R.RG- GINT0/0 · "connection to ISP"	Up	3352
CC-MIL-R.RG- GINT0/0 · "connection to ISP"	Up	6729
CC-MIL-R.RG- GINT0/0 · "connection to ISP"	Warning	5
CC-MIL-R.RG- GINT0/0 · "connection to ISP"	Warning	15
CC-MIL-R.RG- GINT0/0 · "connection to ISP"	Unreachable	70
CC-MIL-R.RG- GINT0/0 · "connection to ISP"	Unreachable	151
CC-MIL-R.RG- GINT0/1 · IN-LAN	Unknown	12
CC-MIL-R.RG- GINT0/1 · IN-LAN	Unknown	19
CC-MIL-R.RG- GINT0/1 · IN-LAN	Up	3352
CC-MIL-R.RG- GINT0/1 · IN-LAN	Up	6732
CC-MIL-R.RG- GINT0/1 · IN-LAN	Warning	5

CC-MIL-R.RG- GINT0/1 · IN-LAN	Warning	12
CC-MIL-R.RG- GINT0/1 · IN-LAN	Unreachable	70
CC-MIL-R.RG- GINT0/1 · IN-LAN	Unreachable	152
CC-MJR- FSTETH - Fa0	Unknown	5
CC-MJR- FSTETH - Fa0	Down	6821
CC-MJR- FSTETH - Fa0	Warning	18
CC-MJR- FSTETH - Fa0	Unreachable	641
CC-MJR- GINT1/0/1 - Gi1/0/1	Down	6840
CC-MJR- GINT1/0/1 - Gi1/0/1	Warning	12
CC-MJR- GINT1/0/1 - Gi1/0/1	Unreachable	632
CC-MJR- GINT1/0/10 - Gi1/0/10	Up	2781
CC-MJR- GINT1/0/10 - Gi1/0/10	Up	6747
CC-MJR- GINT1/0/10 - Gi1/0/10	Down	78
CC-MJR- GINT1/0/10 - Gi1/0/10	Down	125
CC-MJR- GINT1/0/10 - Gi1/0/10	Warning	12
CC-MJR- GINT1/0/10 - Gi1/0/10	Unreachable	630
CC-MJR- GINT1/0/11 - Gi1/0/11	Down	6842
CC-MJR- GINT1/0/11 - Gi1/0/11	Warning	12
CC-MJR- GINT1/0/11 - Gi1/0/11	Unreachable	630
CC-MJR- GINT1/0/12 - Gi1/0/12	Unknown	2
CC-MJR- GINT1/0/12 - Gi1/0/12	Down	6834
CC-MJR- GINT1/0/12 - Gi1/0/12	Warning	8
CC-MJR- GINT1/0/12 - Gi1/0/12	Unreachable	640
CC-MJR- GINT1/0/13 - Gi1/0/13	Unknown	1
CC-MJR- GINT1/0/13 - Gi1/0/13	Down	6835
CC-MJR- GINT1/0/13 - Gi1/0/13	Warning	8
CC-MJR- GINT1/0/13 - Gi1/0/13	Unreachable	640
CC-MJR- GINT1/0/14 - Gi1/0/14	Up	6838
CC-MJR- GINT1/0/14 - Gi1/0/14	Warning	6
CC-MJR- GINT1/0/14 - Gi1/0/14	Unreachable	640
CC-MJR- GINT1/0/15 - Gi1/0/15	Up	6829
CC-MJR- GINT1/0/15 - Gi1/0/15	Down	16
CC-MJR- GINT1/0/15 - Gi1/0/15	Warning	6
CC-MJR- GINT1/0/15 - Gi1/0/15	Unreachable	640
CC-MJR- GINT1/0/16 - Gi1/0/16	Up	6839
CC-MJR- GINT1/0/16 - Gi1/0/16	Warning	5
CC-MJR- GINT1/0/16 - Gi1/0/16	Unreachable	640
CC-MJR- GINT1/0/17 - Gi1/0/17	Up	6831
CC-MJR- GINT1/0/17 - Gi1/0/17	Down	16
CC-MJR- GINT1/0/17 - Gi1/0/17	Warning	4
CC-MJR- GINT1/0/17 - Gi1/0/17	Unreachable	640

CC-MJR- GINT1/0/18 - Gi1/0/18	Up	6840
CC-MJR- GINT1/0/18 - Gi1/0/18	Warning	4
CC-MJR- GINT1/0/18 - Gi1/0/18	Unreachable	640
CC-MJR- GINT1/0/19 - Gi1/0/19	Down	6840
CC-MJR- GINT1/0/19 - Gi1/0/19	Warning	4
CC-MJR- GINT1/0/19 - Gi1/0/19	Unreachable	640
CC-MJR- GINT1/0/2 - Gi1/0/2	Unknown	6
CC-MJR- GINT1/0/2 - Gi1/0/2	Up	760
CC-MJR- GINT1/0/2 - Gi1/0/2	Up	650
CC-MJR- GINT1/0/2 - Gi1/0/2	Down	2052
CC-MJR- GINT1/0/2 - Gi1/0/2	Down	6180
CC-MJR- GINT1/0/2 - Gi1/0/2	Warning	16
CC-MJR- GINT1/0/2 - Gi1/0/2	Unreachable	632
CC-MJR- GINT1/0/20 - Gi1/0/20	Up	6840
CC-MJR- GINT1/0/20 - Gi1/0/20	Warning	4
CC-MJR- GINT1/0/20 - Gi1/0/20	Unreachable	640
CC-MJR- GINT1/0/21 - Gi1/0/21	Up	6831
CC-MJR- GINT1/0/21 - Gi1/0/21	Down	16
CC-MJR- GINT1/0/21 - Gi1/0/21	Warning	4
CC-MJR- GINT1/0/21 - Gi1/0/21	Unreachable	640
CC-MJR- GINT1/0/22 - Gi1/0/22	Unknown	6
CC-MJR- GINT1/0/22 - Gi1/0/22	Up	6830
CC-MJR- GINT1/0/22 - Gi1/0/22	Down	2
CC-MJR- GINT1/0/22 - Gi1/0/22	Warning	10
CC-MJR- GINT1/0/22 - Gi1/0/22	Unreachable	636
CC-MJR- GINT1/0/23 · connection-to-UTM-Internal	Unknown	4
CC-MJR- GINT1/0/23 · connection-to-UTM-Internal	Up	6836
CC-MJR- GINT1/0/23 · connection-to-UTM-Internal	Warning	8
CC-MJR- GINT1/0/23 · connection-to-UTM-Internal	Unreachable	636
CC-MJR- GINT1/0/24 · LINK-DATA-ETC-AGG	Unknown	4
CC-MJR- GINT1/0/24 · LINK-DATA-ETC-AGG	Down	6836
CC-MJR- GINT1/0/24 · LINK-DATA-ETC-AGG	Warning	8
CC-MJR- GINT1/0/24 · LINK-DATA-ETC-AGG	Unreachable	636
CC-MJR- GINT1/0/3 - Gi1/0/3	Unknown	6
CC-MJR- GINT1/0/3 - Gi1/0/3	Up	772
CC-MJR- GINT1/0/3 - Gi1/0/3	Up	2250
CC-MJR- GINT1/0/3 - Gi1/0/3	Down	2044
CC-MJR- GINT1/0/3 - Gi1/0/3	Down	4582
CC-MJR- GINT1/0/3 - Gi1/0/3	Warning	14
CC-MJR- GINT1/0/3 - Gi1/0/3	Unreachable	632
CC-MJR- GINT1/0/4 - Gi1/0/4	Unknown	4

CC-MJR- GINT1/0/4 - Gi1/0/4	Up	5261
CC-MJR- GINT1/0/4 - Gi1/0/4	Down	1575
CC-MJR- GINT1/0/4 - Gi1/0/4	Warning	12
CC-MJR- GINT1/0/4 - Gi1/0/4	Unreachable	632
CC-MJR- GINT1/0/5 - Gi1/0/5	Unknown	3
CC-MJR- GINT1/0/5 - Gi1/0/5	Down	6839
CC-MJR- GINT1/0/5 - Gi1/0/5	Warning	12
CC-MJR- GINT1/0/5 - Gi1/0/5	Unreachable	630
CC-MJR- GINT1/0/6 - Gi1/0/6	Unknown	3
CC-MJR- GINT1/0/6 - Gi1/0/6	Up	2774
CC-MJR- GINT1/0/6 - Gi1/0/6	Up	6831
CC-MJR- GINT1/0/6 - Gi1/0/6	Down	4
CC-MJR- GINT1/0/6 - Gi1/0/6	Down	8
CC-MJR- GINT1/0/6 - Gi1/0/6	Warning	12
CC-MJR- GINT1/0/6 - Gi1/0/6	Unreachable	630
CC-MJR- GINT1/0/7 - Gi1/0/7	Unknown	3
CC-MJR- GINT1/0/7 - Gi1/0/7	Up	4108
CC-MJR- GINT1/0/7 - Gi1/0/7	Down	2733
CC-MJR- GINT1/0/7 - Gi1/0/7	Warning	14
CC-MJR- GINT1/0/7 - Gi1/0/7	Unreachable	630
CC-MJR- GINT1/0/8 - Gi1/0/8	Unknown	1
CC-MJR- GINT1/0/8 - Gi1/0/8	Up	2790
CC-MJR- GINT1/0/8 - Gi1/0/8	Up	3961
CC-MJR- GINT1/0/8 - Gi1/0/8	Down	2880
CC-MJR- GINT1/0/8 - Gi1/0/8	Warning	12
CC-MJR- GINT1/0/8 - Gi1/0/8	Unreachable	630
CC-MJR- GINT1/0/9 - Gi1/0/9	Unknown	1
CC-MJR- GINT1/0/9 - Gi1/0/9	Up	6841
CC-MJR- GINT1/0/9 - Gi1/0/9	Warning	12
CC-MJR- GINT1/0/9 - Gi1/0/9	Unreachable	630
CC-MJR- GINT1/1/1 · "connection to ISP"	Unknown	3
CC-MJR- GINT1/1/1 · "connection to ISP"	Warning	8
CC-MJR- GINT1/1/1 · "connection to ISP"	Shutdown	6839
CC-MJR- GINT1/1/1 · "connection to ISP"	Unreachable	634
CC-MJR- GINT1/1/2 · "CONNECTION TO ISP"	Unknown	3
CC-MJR- GINT1/1/2 · "CONNECTION TO ISP"	Up	6839
CC-MJR- GINT1/1/2 · "CONNECTION TO ISP"	Warning	8
CC-MJR- GINT1/1/2 · "CONNECTION TO ISP"	Unreachable	634
CC-MJR- GINT1/1/3 - Gi1/1/3	Unknown	1
CC-MJR- GINT1/1/3 - Gi1/1/3	Down	6841
CC-MJR- GINT1/1/3 - Gi1/1/3	Warning	8

CC-MJR- GINT1/1/3 - Gi1/1/3	Unreachable	634
CC-MJR- GINT1/1/4 - Gi1/1/4	Unknown	1
CC-MJR- GINT1/1/4 - Gi1/1/4	Down	6841
CC-MJR- GINT1/1/4 - Gi1/1/4	Warning	8
CC-MJR- GINT1/1/4 - Gi1/1/4	Unreachable	634
CC-MJR- Null0 - Nu0	Up	6842
CC-MJR- Null0 - Nu0	Warning	8
CC-MJR- Null0 - Nu0	Unreachable	634
CC-MJR- StackPort1	Unknown	2
CC-MJR- StackPort1	Down	6838
CC-MJR- StackPort1	Warning	12
CC-MJR- StackPort1	Unreachable	632
CC-MJR- StackSub-St1-1	Unknown	1
CC-MJR- StackSub-St1-1	Warning	12
CC-MJR- StackSub-St1-1	Shutdown	6839
CC-MJR- StackSub-St1-1	Unreachable	632
CC-MJR- StackSub-St1-2	Unknown	1
CC-MJR- StackSub-St1-2	Warning	12
CC-MJR- StackSub-St1-2	Shutdown	6839
CC-MJR- StackSub-St1-2	Unreachable	632
CC-MJR- TenGINT1/1/1 - Te1/1/1	Down	6842
CC-MJR- TenGINT1/1/1 - Te1/1/1	Warning	8
CC-MJR- TenGINT1/1/1 - Te1/1/1	Unreachable	634
CC-MJR- TenGINT1/1/2 - Te1/1/2	Down	6840
CC-MJR- TenGINT1/1/2 - Te1/1/2	Warning	10
CC-MJR- TenGINT1/1/2 - Te1/1/2	Unreachable	634
CC-MJR- Vlan1 - Vl1	Unknown	5
CC-MJR- Vlan1 - Vl1	Up	6824
CC-MJR- Vlan1 - Vl1	Warning	21
CC-MJR- Vlan1 - Vl1	Unreachable	634
CC-MJR- Vlan10 - Vl10	Unknown	5
CC-MJR- Vlan10 - Vl10	Up	6831
CC-MJR- Vlan10 - Vl10	Warning	14
CC-MJR- Vlan10 - Vl10	Unreachable	634
CC-MJR- Vlan20 - Vl20	Unknown	3
CC-MJR- Vlan20 - Vl20	Up	6835
CC-MJR- Vlan20 - Vl20	Warning	12
CC-MJR- Vlan20 - Vl20	Unreachable	634
CC-MJR- Vlan30 - Vl30	Unknown	2
CC-MJR- Vlan30 - Vl30	Up	6838
CC-MJR- Vlan30 - Vl30	Warning	12

CC-MJR- Vlan30 - Vl30	Unreachable	632
CC-MJR- Vlan40 - Vl40	Unknown	2
CC-MJR- Vlan40 - Vl40	Up	6838
CC-MJR- Vlan40 - Vl40	Warning	12
CC-MJR- Vlan40 - Vl40	Unreachable	632
CC-MJR- Vlan5 - Vl5	Unknown	5
CC-MJR- Vlan5 - Vl5	Up	2655
CC-MJR- Vlan5 - Vl5	Up	6830
CC-MJR- Vlan5 - Vl5	Warning	1
CC-MJR- Vlan5 - Vl5	Warning	15
CC-MJR- Vlan5 - Vl5	Unreachable	634
DSW- FSTETH/18 - Fa0/18	Unknown	2
DSW- FSTETH/18 - Fa0/18	Unknown	1
DSW- FSTETH/18 - Fa0/18	Down	4297
DSW- FSTETH/18 - Fa0/18	Down	4413
DSW- FSTETH/18 - Fa0/18	Warning	2
DSW- FSTETH/18 - Fa0/18	Warning	20
DSW- FSTETH/18 - Fa0/18	Unreachable	3
DSW- FSTETH/18 - Fa0/18	Unreachable	26
DSW- FSTETH/19 - Fa0/19	Unknown	2
DSW- FSTETH/19 - Fa0/19	Unknown	1
DSW- FSTETH/19 - Fa0/19	Down	4297
DSW- FSTETH/19 - Fa0/19	Down	4413
DSW- FSTETH/19 - Fa0/19	Warning	2
DSW- FSTETH/19 - Fa0/19	Warning	20
DSW- FSTETH/19 - Fa0/19	Unreachable	3
DSW- FSTETH/19 - Fa0/19	Unreachable	26
DSW- FSTETH/21 - Fa0/21	Unknown	2
DSW- FSTETH/21 - Fa0/21	Up	5620
DSW- FSTETH/21 - Fa0/21	Up	4414
DSW- FSTETH/21 - Fa0/21	Warning	2
DSW- FSTETH/21 - Fa0/21	Warning	20
DSW- FSTETH/21 - Fa0/21	Unreachable	3
DSW- FSTETH/21 - Fa0/21	Unreachable	26
DSW- GINT0/2 - Gi0/2	Unknown	2
DSW- GINT0/2 - Gi0/2	Down	4297
DSW- GINT0/2 - Gi0/2	Down	4414
DSW- GINT0/2 - Gi0/2	Warning	2
DSW- GINT0/2 - Gi0/2	Warning	20
DSW- GINT0/2 - Gi0/2	Unreachable	3
DSW- GINT0/2 - Gi0/2	Unreachable	26

DSW- Null0 - Nu0	Unknown	2
DSW- Null0 - Nu0	Up	4297
DSW- Null0 - Nu0	Up	4416
DSW- Null0 - Nu0	Warning	2
DSW- Null0 - Nu0	Warning	20
DSW- Null0 - Nu0	Unreachable	3
DSW- Null0 - Nu0	Unreachable	24
ERCA-SLB-02 - utp ethernet (10/100) - Port 8	Up	2863
ERCA-SLB-02 - utp ethernet (10/100) - Port 8	Down	2
exch01.RG- HP NC373i Multifunction Gigabit Server Adapter #60 · Private	Up	3643
exch01.RG- HP NC373i Multifunction Gigabit Server Adapter #60 · Private	Up	6154
exch01.RG- HP NC373i Multifunction Gigabit Server Adapter #60 · Private	Down	4
exch01.RG- HP NC373i Multifunction Gigabit Server Adapter #60 · Private	Warning	3
exch01.RG- HP NC373i Multifunction Gigabit Server Adapter #60 · Private	Warning	2
exch01.RG- HP NC373i Multifunction Gigabit Server Adapter #60-QoS Packet Scheduler-0000 · Private-QoS Packet Scheduler-0000	Up	6156
exch01.RG- HP NC373i Multifunction Gigabit Server Adapter #60-QoS Packet Scheduler-0000 · Private-QoS Packet Scheduler-0000	Down	4
exch01.RG- HP NC373i Multifunction Gigabit Server Adapter #60-WFP LightWeight Filter-0000 · Private-WFP LightWeight Filter-0000	Up	6156
exch01.RG- HP NC373i Multifunction Gigabit Server Adapter #60-WFP LightWeight Filter-0000 · Private-WFP LightWeight Filter-0000	Down	4
exch01.RG- Microsoft Failover Cluster Virtual Adapter-WFP LightWeight Filter-0000 · Local Area Connection* 9-WFP LightWeight Filter-0000	Down	7198
exch01.RG- Microsoft Failover Cluster Virtual Adapter-WFP LightWeight Filter-0000 · Local Area Connection* 9-WFP LightWeight Filter-0000	Down	2604
exch01.RG- Microsoft Failover Cluster Virtual Adapter-WFP LightWeight Filter-0000 · Local Area Connection* 9-WFP LightWeight Filter-0000	Warning	2
exch01.RG- Microsoft Failover Cluster Virtual Adapter-WFP LightWeight Filter-0000 · Local Area Connection* 9-WFP LightWeight Filter-0000	Warning	2
GAD - Embedded-Service-Engine0/0 - Em0/0	Unknown	2
GAD - Embedded-Service-Engine0/0 - Em0/0	Unknown	2
GAD - Embedded-Service-Engine0/0 - Em0/0	Warning	2
GAD - Embedded-Service-Engine0/0 - Em0/0	Warning	13
GAD - Embedded-Service-Engine0/0 - Em0/0	Shutdown	3509
GAD - Embedded-Service-Engine0/0 - Em0/0	Shutdown	6825
GAD - Embedded-Service-Engine0/0 - Em0/0	Unreachable	1
GAD - Embedded-Service-Engine0/0 - Em0/0	Unreachable	5
GAD - GINT0/0 · Connection To ISP	Unknown	2
GAD - GINT0/0 · Connection To ISP	Unknown	2
GAD - GINT0/0 · Connection To ISP	Up	3509
GAD - GINT0/0 · Connection To ISP	Up	6829
GAD - GINT0/0 · Connection To ISP	Warning	2
GAD - GINT0/0 · Connection To ISP	Warning	9

GAD - GINT0/0 · Connection To ISP	Unreachable	1
GAD - GINT0/0 · Connection To ISP	Unreachable	5
GAD - GINT0/1 · Connection To Internal Network	Unknown	2
GAD - GINT0/1 · Connection To Internal Network	Unknown	1
GAD - GINT0/1 · Connection To Internal Network	Up	3509
GAD - GINT0/1 · Connection To Internal Network	Up	6832
GAD - GINT0/1 · Connection To Internal Network	Warning	2
GAD - GINT0/1 · Connection To Internal Network	Warning	11
GAD - GINT0/1 · Connection To Internal Network	Unreachable	1
GAD - GINT0/1 · Connection To Internal Network	Unreachable	1
GAD - GINT0/3 - Gi0/3	Unknown	1
GAD - GINT0/3 - Gi0/3	Up	3511
GAD - GINT0/3 - Gi0/3	Up	6834
GAD - GINT0/3 - Gi0/3	Warning	2
GAD - GINT0/3 - Gi0/3	Warning	9
GAD - GINT0/3 - Gi0/3	Unreachable	1
GAD - GINT0/3 - Gi0/3	Unreachable	1
GAD - Null0 - Nu0	Unknown	1
GAD - Null0 - Nu0	Up	3511
GAD - Null0 - Nu0	Up	6835
GAD - Null0 - Nu0	Warning	2
GAD - Null0 - Nu0	Warning	9
GAD - Null0 - Nu0	Unreachable	1
JAD - Embedded-Service-Engine0/0 - Em0/0	Unknown	476
JAD - Embedded-Service-Engine0/0 - Em0/0	Unknown	2416
JAD - Embedded-Service-Engine0/0 - Em0/0	Unreachable	3941
JAD - Embedded-Service-Engine0/0 - Em0/0	Unreachable	3479
JAD - GINT0/0 · Connection to Ethio~Telecom	Unknown	476
JAD - GINT0/0 · Connection to Ethio~Telecom	Unknown	2416
JAD - GINT0/0 · Connection to Ethio~Telecom	Unreachable	3941
JAD - GINT0/0 · Connection to Ethio~Telecom	Unreachable	3479
JAD - GINT0/1 · IN-LAN	Unknown	476
JAD - GINT0/1 · IN-LAN	Unknown	2416
JAD - GINT0/1 · IN-LAN	Unreachable	3941
JAD - GINT0/1 · IN-LAN	Unreachable	3479
JAD - GINT0/3 - Gi0/3	Unknown	476
JAD - GINT0/3 - Gi0/3	Unknown	2416
JAD - GINT0/3 - Gi0/3	Unreachable	3941
JAD - GINT0/3 - Gi0/3	Unreachable	3479
JAD - Null0 - Nu0	Unknown	476
JAD - Null0 - Nu0	Unknown	2416

JAD - Null0 - Nu0	Unreachable	3941
JAD - Null0 - Nu0	Unreachable	3479
CustK~CoMet - GINT0/6 · "Connection to 10.18.1.55 (ZTE Switch) with VLAN55"	Unknown	4
CustK~CoMet - GINT0/6 · "Connection to 10.18.1.55 (ZTE Switch) with VLAN55"	Down	1434
CustK~CoMet - GINT0/6 · "Connection to 10.18.1.55 (ZTE Switch) with VLAN55"	Down	5187
CustK~CoMet - GINT0/6 · "Connection to 10.18.1.55 (ZTE Switch) with VLAN55"	Warning	4
CustK~CoMet - GINT0/6 · "Connection to 10.18.1.55 (ZTE Switch) with VLAN55"	Warning	18
CustK~CoMet - GINT0/6 · "Connection to 10.18.1.55 (ZTE Switch) with VLAN55"	Unreachable	2
CustK~CoMet - GINT0/6 · "Connection to 10.18.1.55 (ZTE Switch) with VLAN55"	Unreachable	1814
CustK~CoMet - Null0 - Nu0	Unknown	3
CustK~CoMet - Null0 - Nu0	Up	1434
CustK~CoMet - Null0 - Nu0	Up	5192
CustK~CoMet - Null0 - Nu0	Warning	4
CustK~CoMet - Null0 - Nu0	Warning	14
CustK~CoMet - Null0 - Nu0	Unreachable	2
CustK~CoMet - Null0 - Nu0	Unreachable	1814
MiS-Edge-03 - GINT0/26 · "CONNECTION TO MOF SERVER"	Up	5731
MiS-Edge-03 - GINT0/26 · "CONNECTION TO MOF SERVER"	Up	3015
MiS-Edge-03 - GINT0/26 · "CONNECTION TO MOF SERVER"	Down	5
MiS-Edge-03 - GINT0/26 · "CONNECTION TO MOF SERVER"	Down	14
MOR-ADMA-R - Backplane-GINT0/3 - Ba0/3	Unknown	2
MOR-ADMA-R - Backplane-GINT0/3 - Ba0/3	Up	4538
MOR-ADMA-R - Backplane-GINT0/3 - Ba0/3	Warning	6
MOR-ADMA-R - Backplane-GINT0/3 - Ba0/3	Unreachable	919
MOR-ADMA-R - Embedded-Service-Engine0/0 - Em0/0	Unknown	2
MOR-ADMA-R - Embedded-Service-Engine0/0 - Em0/0	Warning	10
MOR-ADMA-R - Embedded-Service-Engine0/0 - Em0/0	Shutdown	4534
MOR-ADMA-R - Embedded-Service-Engine0/0 - Em0/0	Unreachable	919
MOR-ADMA-R - GINT0/0 · connection to ISP-WAN	Unknown	2
MOR-ADMA-R - GINT0/0 · connection to ISP-WAN	Up	4538
MOR-ADMA-R - GINT0/0 · connection to ISP-WAN	Warning	6
MOR-ADMA-R - GINT0/0 · connection to ISP-WAN	Unreachable	919
MOR-ADMA-R - GINT0/1 · IN-LAN	Unknown	2
MOR-ADMA-R - GINT0/1 · IN-LAN	Up	4538
MOR-ADMA-R - GINT0/1 · IN-LAN	Warning	6
MOR-ADMA-R - GINT0/1 · IN-LAN	Unreachable	919
MOR-ADMA-R - Null0 - Nu0	Unknown	2
MOR-ADMA-R - Null0 - Nu0	Up	4539
MOR-ADMA-R - Null0 - Nu0	Warning	6
MOR-ADMA-R - Null0 - Nu0	Unreachable	918
MLAN - Null0 - Nu0	Up	4331

MLAN - Null0 - Nu0	Warning	4
MLAN - Vlan1 - Vl1	Unknown	1
MLAN - Vlan1 - Vl1	Warning	2
MLAN - Vlan1 - Vl1	Shutdown	4374
MLAN - Vlan10 · BLCK-A Ground Floor	Up	4372
MLAN - Vlan10 · BLCK-A Ground Floor	Warning	0
MLAN - Vlan100 · ServerFarm Vlan	Up	4096
MLAN - Vlan15 · BLCK-A Fifth Floor	Up	4372
MLAN - Vlan20 · BLCK-B Ground Floor	Up	4372
MLAN - Vlan80 · Voice vlan	Up	4077
MECS- GINT1/0/23 · connection to ISP	Unknown	9
MECS- GINT1/0/23 · connection to ISP	Up	3076
MECS- GINT1/0/23 · connection to ISP	Up	6647
MECS- GINT1/0/23 · connection to ISP	Warning	10
MECS- GINT1/0/23 · connection to ISP	Warning	41
MECS- GINT1/0/23 · connection to ISP	Unreachable	3
MECS- GINT1/0/23 · connection to ISP	Unreachable	382
MECS- GINT1/0/24 · CONNECTION TO ETC LINE	Unknown	7
MECS- GINT1/0/24 · CONNECTION TO ETC LINE	Up	3062
MECS- GINT1/0/24 · CONNECTION TO ETC LINE	Up	6653
MECS- GINT1/0/24 · CONNECTION TO ETC LINE	Warning	20
MECS- GINT1/0/24 · CONNECTION TO ETC LINE	Warning	37
MECS- GINT1/0/24 · CONNECTION TO ETC LINE	Unreachable	1
MECS- GINT1/0/24 · CONNECTION TO ETC LINE	Unreachable	382
MECS- Null0 - Nu0	Unknown	7
MECS- Null0 - Nu0	Up	3074
MECS- Null0 - Nu0	Up	6649
MECS- Null0 - Nu0	Warning	14
MECS- Null0 - Nu0	Warning	41
MECS- Null0 - Nu0	Unreachable	1
MECS- Null0 - Nu0	Unreachable	382
MHW - Ethernet0/0 · connection to ISP-WAN	Unknown	6703
MHW - Ethernet0/0 · connection to ISP-WAN	Unreachable	91
MHW - FSTETH/0 · IN-LAN	Unknown	6703
MHW - FSTETH/0 · IN-LAN	Unreachable	91
MHW - Null0 - Nu0	Unknown	6703
MHW - Null0 - Nu0	Unreachable	91

EFGHIJKLMN

O

Project: Final ERCA Network With Scenarionw2 | Report: User Selected
Scenario: scenario30 | **Title: Global Statistics Summary**

Simulated from 16:10:10 Sun Jun 27 2021 to 16:10:10 Fri Jul 02 2021.

Ethernet

Statistic	Average	Maximum	Minimum
Ethernet Delay (sec)	0.00079422	0.00080464	0.00078507

HTTP

Statistic	Average	Maximum	Minimum
HTTP Object Response Time (seconds)	0.0041937	0.0042514	0.0041428
HTTP Page Response Time (seconds)	0.012555	0.012727	0.012405
HTTP Traffic Received (bytes/sec)	7,602.2	8,565.9	7,373.8
HTTP Traffic Received (packets/sec)	25.165	28.333	24.418
HTTP Traffic Sent (bytes/sec)	7,602.2	8,565.9	7,374.0
HTTP Traffic Sent (packets/sec)	25.165	28.333	24.419

IP

Statistic	Average	Maximum	Minimum
IP Network Convergence Activity	0.00002	1.00000	0.00000
IP Network Convergence Duration (sec)	8.5471	8.5471	8.5471
IP Number of Hops	1.9993	2.0000	1.9988
IP Traffic Dropped (packets/sec)	0	0	0

Client Http Downloaded Objects

Statistic sampling period is 72 minutes.

Sort By Node	Sorted By Average	Sort By Peak
BenishangulR.BenishangulR node_3	1,817.4	2,118
DireDawaF.DireDawaF node_3	1,794.0	2,124
DireDawaF.DireDawaFnode_2	1,786.4	1,974
KalityNocC.KalityNocC node_2	915.7	1,140
KombolchaC.KombolchaC node_3	912.9	1,122

Client Http Downloaded Pages

Statistic sampling period is 72 minutes.

Sort By Node	Sorted By Average	Sort By Peak
BenishangulR.BenishangulR node_3	302.90	353
DireDawaF.DireDawaF node_3	299.00	354
DireDawaF.DireDawaFnode_2	297.73	329
KalityNocC.KalityNocC node_2	152.61	190
KombolchaC.KombolchaC node_3	152.15	187

Client Http Object Response Time (seconds)

Statistic sampling period is 72 minutes.

Sort By Node	Sorted By Average	Sort By Peak
ShireC.ShireC node_2	0.0077621	0.0077697
ShireC.ShireC node_3	0.0077610	0.0077675
TigrayiR.TigrayiR node_2	0.0072369	0.0072519
TigrayiR.TigrayiR node_3	0.0072357	0.0072460
Djibouti.Djibouti node_2	0.0069689	0.0069767

Client Http Page Response Time (seconds)

Statistic sampling period is 72 minutes.

Sort By Node	Sorted By Average	Sort By Peak
ShireC.ShireC node_3	0.023219	0.023316
ShireC.ShireC node_2	0.023210	0.023317
TigrayiR.TigrayiR node_2	0.021633	0.021752
TigrayiR.TigrayiR node_3	0.021630	0.021742
Djibouti.Djibouti node_3	0.020848	0.020937

Client Http Traffic Received (bytes/sec)

Statistic sampling period is 72 minutes.

Sort By Node	Sorted By Average	Sort By Peak
BenishangulR.BenishangulR node_3	107.06	123.35
DireDawaF.DireDawaF node_3	105.73	124.73
DireDawaF.DireDawaFnode_2	105.23	116.07
KombolchaC.KombolchaC node_3	53.71	66.47
ShireC.ShireC node_3	53.68	65.26

Client Http Traffic Sent (bytes/sec)

Statistic sampling period is 72 minutes.

Sort By Node	Sorted By Average	Sort By Peak
BenishangulR.BenishangulR node_3	147.25	171.60
DireDawaF.DireDawaF node_3	145.35	172.08
DireDawaF.DireDawaFnode_2	144.74	159.93
KalityNocC.KalityNocC node_2	74.19	92.36
KombolchaC.KombolchaC node_3	73.96	90.90

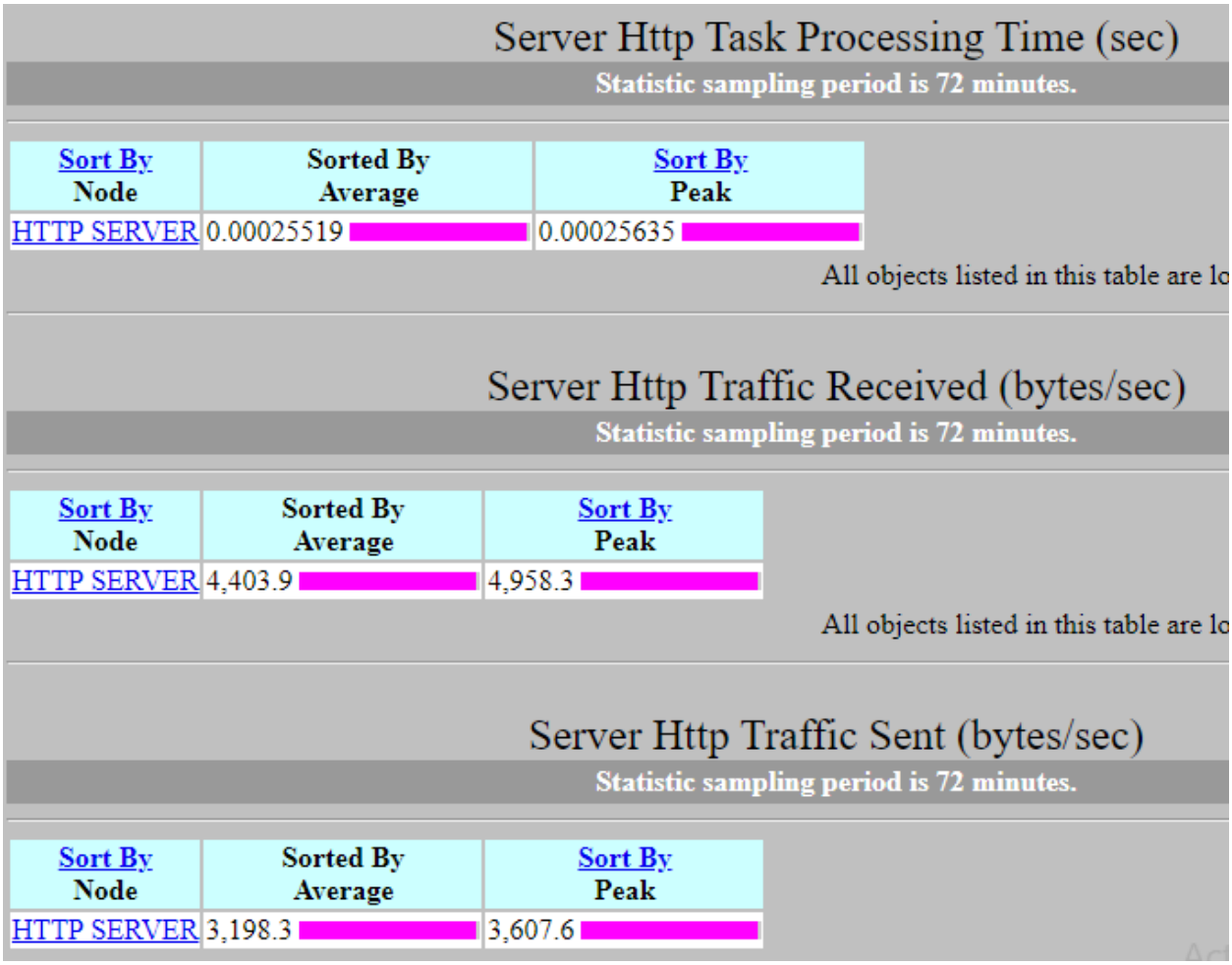
Client Http User Cancelled Connections

Statistic sampling period is 72 minutes.

Sort By Node	Sorted By Average	Sort By Peak
Bahir Dar.Bahir Dar node_2	1	1
BenishangulR.BenishangulR node_3	1	1
EAST.EAST node_2	1	1
GambellaR.GambellaR node_2	1	1
Mekele.Mekele node_2	1	1

PQR

S



Server Http Task Processing Time (sec)

Statistic sampling period is 72 minutes.

Sort By Node	Sorted By Average	Sort By Peak
HTTP SERVER	0.00025519	0.00025635

All objects listed in this table are lo

Server Http Traffic Received (bytes/sec)

Statistic sampling period is 72 minutes.

Sort By Node	Sorted By Average	Sort By Peak
HTTP SERVER	4,403.9	4,958.3

All objects listed in this table are lo

Server Http Traffic Sent (bytes/sec)

Statistic sampling period is 72 minutes.

Sort By Node	Sorted By Average	Sort By Peak
HTTP SERVER	3,198.3	3,607.6

TUVWXYZ