JPPI Vol 10 No 2 (2020) 125 - 144

Jurnal Penelitian Pos dan Informatika
32a/E/KPT/2017

e-ISSN 2476-9266
p-ISSN: 2088-9402

Doi:10.17933/jppi.2020.100204

SLA and Network Availability Mechanism Implementation Scheme for Customer Service Provider

Skema Penerapan Mekanisme SLA Dan Network Availability Untuk Customer Service Provider

Hillman Akhyar Damanik [1] Merry Anggraeni [2]

Fakultas Teknologi Informasi Universitas Budi Luhur[12]
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, DKI Jakarta, Indonesia 1226012
hillman.akhyardamanik@budiluhur.ac.id[1]

Received: 31 October 2020 ; Received in revised from: 9 December 2020; Accepted: 9 December 2020

Abstract

Increasingly complex network heterogeneity and network monitoring tasks become the management concentration of a large distributed production infrastructure with various business services requiring a centralized control monitoring system, with increasing network size, heterogeneity and complexity. The network monitoring and management solutions available are not only expensive but also difficult to use, configure and maintain. Manually routing pins to the wrong device on a large complex network is very complicated and time-consuming for Service Provider (SP). Thus, it is necessary to have an automatic system that immediately reports to the network Service Provider (SP) monitoring system regarding the type of error or alert, Network Availability and Service Level Agreement (SLA). This research presents the modeling design and implementation of Network Availability and SLA network systems for Service Provider (SP) organizations, by being based on open-source programming tools (Zabbix System) and intelligently integrating to monitor network devices, especially to get Network Availability and SLA parameters and values on a customer or customer. Monitoring Customers devices in the network in the form of a module alert parameter that will be applied so that it is seen and can be said to be a universal Plug & Play technology concept (UPnP). Monitoring system developed will provide value and quality of service (qos) output parameters in the form of measuring and taking test value parameters Network Availability and SLA modeling, which will produce an accurate Service Level Agreement (SLA) value parameter test, and become a reference for an agreement between a service provider and a customer. As a guarantee or link availability for the services provided by Service Provide (SP) to customers. With the SLA value fulfilled at 99.9% with a 99.5% agreement, Network availability is met with a percentage of 98.89% and Down time with a percentage of only 1% of the agreement 2%, and the latency value of the terrestrial transmission media obtained is 2 ms, from the 8 ms agreement and the obtained VSAT transmission media is 500-600 ms from the agreement latency value is 700 ms.

Keywords: *Zabbix, Alert Parameter, Open Source, ICMP, Raspbian, Raspberry Pi, Availability, SLA*.

INTRODUCTION

In the last decade, communication technology has been increasingly revolutionized. The rapid emergence of new network technologies and the development of more heterogeneous equipment has resulted in a situation characterized by a high degree of heterogeneity as well as the complexity of centralized management solutions due to the heterogeneity of the underlying equipment to manage. The difficulty comes from the fact that equipment usually runs proprietary management protocols and implements a heterogeneous data management model (Renitea et al. 2017; Petruti et al. 2018; Marik et al., 2014). In this complex environment, Information Technology (IT) and telecommunications network operators face important problems in management costs. Therefore, operators are required to use multiple management platforms to manage the entire network (Mescheryakov et al., 2014; Hernantes et al., 2015).

This situation will not change in the future as operators need to purchase equipment from a manufacturer to reduce the risk of dependence on one manufacturer and also to reduce the cost of purchasing this equipment in competitive markets (Iqbal et al., 2015; Marik et al., 2014). As a result, operators are forced to use management and monitoring tools specific to each product line. Today, some surveillance tools can use expert system engines to improve management. The problem with such systems is their limitation in terms of reasoning in situations where new component types are introduced in the network. In this case, most of the time the efficiency of an expert system to find the right solution is not guaranteed. Other concepts of network management such as neuronal correlation or alarms have also been investigated in the literature but a new challenge is to be at least as effective as existing approaches and provide greater flexibility (Rezac et al., 2015; Mullins et al., 2013; Hendrawan et al., 2016; Urunov et al., 2017; He et al., 2017; Kim et al., 2014; and Manna et al., 2019).

This study focuses on the framework scheme and implementation with a focus on monitoring the complexity of the customer network using the Zabbix open-source software. Zabbix is one tool that has been widely used by the experienced industrial world. Due to its flexible modular architecture, Zabbix allows users to develop custom modules to enhance system functionality in various ways. In this study, a Zabbix integration conceptual design is proposed as the core of a new feature-rich monitoring system. Our new system is integrated with a more interactive and friendly user interface, and provides more information for SLA values and parameters and ICMP Ping: ICMP Packet Loss, ICMP Ping: ICMP Ping Time and ICMP Latency (ICMP Response Time) (Coonjah et al., 2019; and Jian et al., 2012). These values and parameters are the agreement between the service provider and a customer. The proposed research process can be seen in Figure I.1 Scheme SLA and Network Availability Mechanism for Customer Service Providers

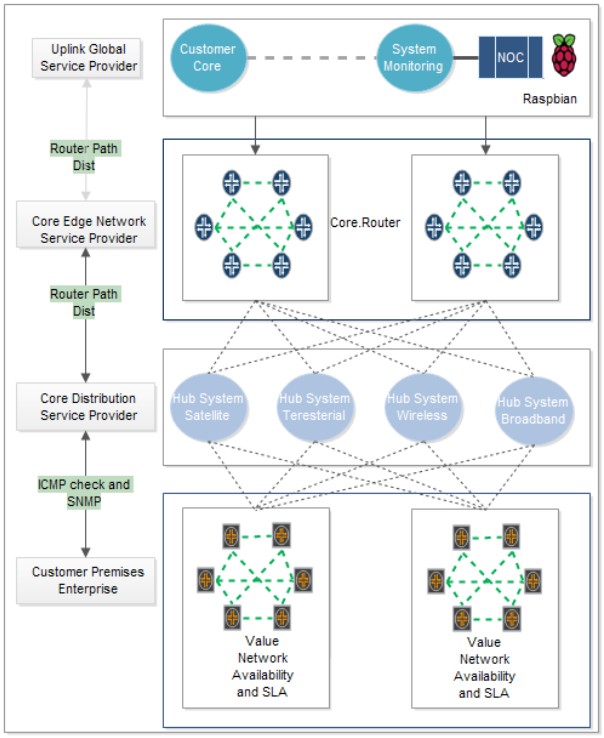


Figure.1 Scheme SLA and Network Availability Mechanism for Customer Service Provider

1. Network Availability

The literature often suggests calculating theoretical availability as a pre-study when planning networks, or before having sufficient data to calculate actual availability. To calculate the theoretical availability, the network is divided into each dependent unit, such as hardware, software, physical connection, power supply, etc. (Geng et al., 2020 and Wang, 2018). For most equipment, manufacturers will provide information on expected availability, often described as Mean Time between Failure (MTBF). For those parts of the network where this data is not available, such as resources, statistical data and estimates should be used. The time expected to repair each part of the network must be estimated. This is usually referred to as Mean Time to Repair (MTTR) (Ying-Hui Fan, 2015 and Wang, 2018). Availability for each unit is calculated by:

$$Availability = \frac{MTBF}{MTBF + MTTR}$$

To calculate the total network availability, the availability of all units must be summed up. For example, the path modeling to be implemented which consists of five units, (see Figure 2: Four-unit point-to-point availability) each has an expected availability of 99.99% having a total availability of 99.96% or three and a half hours per years (Jiang, 2015). Availability is the percentage of time, in a specified time interval, during which servers, cloud services, network connectivity can be used for the purpose for which they were designed and built. The most common formulas used to calculate uptime are as follows:

$$Network\ availability = Weight_{customer\text{-}core}\ x\ Network\ Availability_{nms\text{-}core} + Weight_{hub\text{-}system}\ x\ Network\ Availability_{customer\text{-}edge}$$

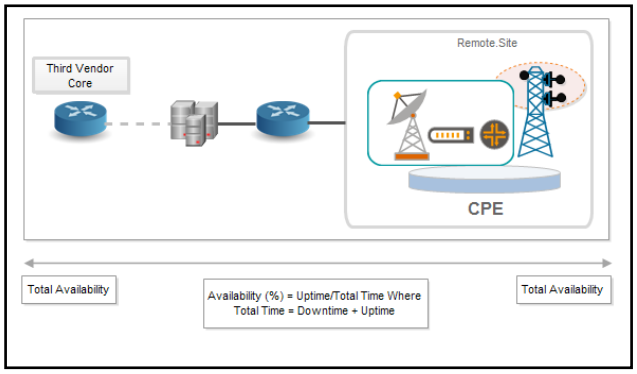


Figure 2. Network Availability

2. Service Level Agreement (SLA)

Service providers (SP) provide internet or telecommunications media services to customers using a pay-per-use model, while the quality of service provided is determined using a service level agreement also known as an SLA. To optimize the level of assurance of each service, workload in underwriting large-scale telecommunications networks is reduced. In particular, to address the diversification and change of assurance objects and services, automatization is made in decision making in network operation assurance work such as reaction requirements, reaction due dates and reaction priorities, based on the quality target value (SLA) (Takada et al., 2019).

METDHOLOGY

1. Analysis System Network Availability

The monitoring system is a model scheme and Zabbix system modeling for monitoring Customers Edge (CE) by taking several parameters of the Network Availability and SLA Service Provider (SP) to Customers. With the applied modeling system, it will be able to detect alert status (Up or down) and availability and SLA parameter values at the Customer Edge (CE) service provider endpoint. ICMP Packet Loss, ICMP Ping Time and Latency (ICMP Response Time) parameters will be taken in realtime with a flow as shown in Figure 3.1.

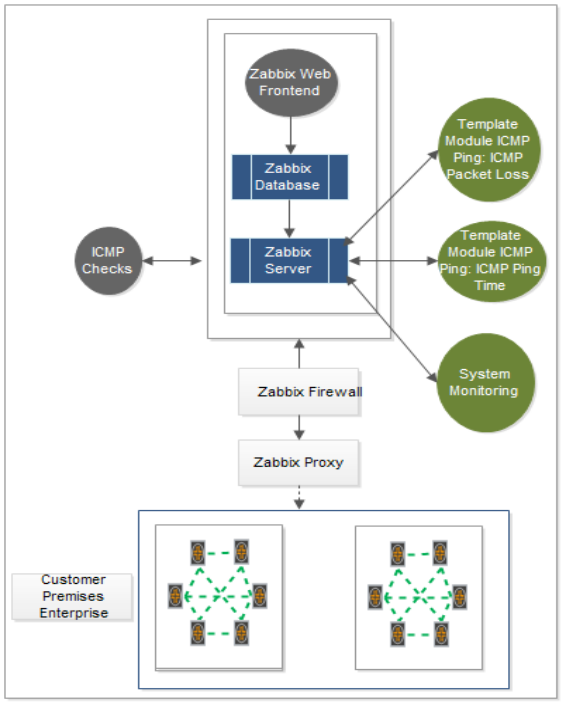


Figure 3. Flow Network Availability ICMP

2. Design System Network Availability

In the design phase, conceptualizatio of performance system planning is made on a Network Availability and alert system for flexibility, portability and dynamic scalability. Currently, Service Providers (SP) are developing and implementing a monitoring system, as a reference for the level of quality of service guaranteed by the

infrastructure to measure service quality parameters and network performance, down to the customers edge. The values and parameters measured are the availability of ICMP Packet Loss, ICMP Ping Time and Latency (ICMP Response Time) and Service Level Agreement (SLA).

- The design technique will be designed before topology scenario Modeling Network Availability and SLA Customers Service Provider on Zabbix server and remote site customer allocation.
- Installation and configuration of Ubuntu Server 18.04 and Zabbix Stable release: 4.4.6.
- Installataion and Configuration of Zabbix on the Raspbian on the Raspberry Pi.
- Installation and Configuration of the path route from CE to Zabbix Server, to verify by continuously monitoring network behavior based on predefined parameters.
- Implementation and modeling of network availability monitoring systems and alert systems with ICMP Ping Template Module: ICMP Packet Loss, ICMP Ping Template Module: ICMP Ping Time and Template Module Latency (ICMP Response Time) and SLA.
- Recording quality of service output parameters: measuring and retrieving test scenario value parameters with ICMP Ping: ICMP Packet Loss, ICMP Ping: ICMP Ping Time and Template Module Latency (ICMP Response Time) and SLA.
- Results of parameters and modeling of Network Availability and SLA Customers Service Provider.

The system will analyze monitoring technology and customer edge network alert systems, especially to obtain availability values and parameters; Identify and assess how well current technology is integrated into the entire network management operation cycle, whether on each of the distribution system hubs available to the customer end device or the customer edge. Service Providers first set up the network configuration, are given a set of requirements, then use the new design for the topology and modeling scheme to be designed and implemented, and finally verify it by continuously monitoring the network behavior. A further observation is that the efficiency of the monitoring and alert cycles can be greatly improved by automatic deployment of pre-designed configurations, in response to changes in monitored network behavior.

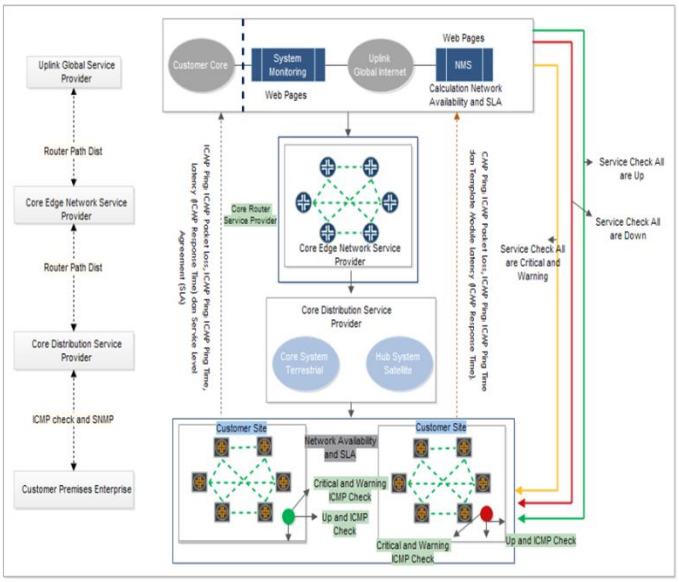


Figure 4. Topology Modeling of Network Availability Mechanisms and Alert Customers Service Provider Systems

3. Data Modeling Schemes and Network Availability

Service Level Agreement (SLA) and Network availability are placed between the client, core node, system hub node to the Zabbix server

monitoring system, at a Service Provider (SP) as shown in Figure 4, All remote sites will be monitored based on the criteria that have been mentioned, to get the value of Availability and SLA as a guarantee of quality service from SP to Customer. Figure5 shows ICMP packet loss modeling which makes ping requests via the ICMP protocol. If ICMP replies with a value of 1 or in an *up* status, the ICMP packet loss will send a status with a notification *up*. Meanwhile, if ICMP replies with a value of 0 or down, the trigger on the ICMP packet loss will be active and initiate 3 delivery checkings for 150 ms (15 seconds) x 3. If after the 3 checkings the status remains 0 or down, the ICMP packet loss will send a network down notification.

Representation of the ICMP packet loss (Network Availability) modeling flowchart and the explanation above:

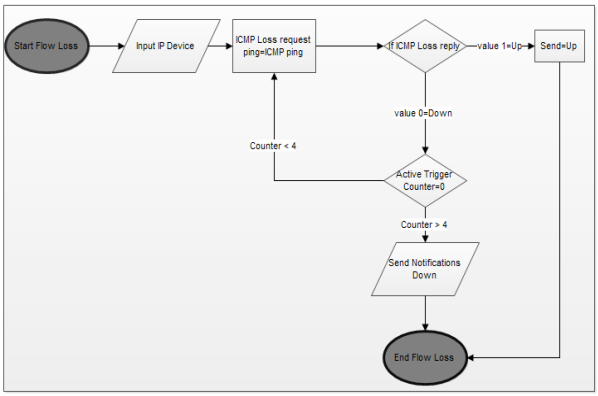


Figure 5. Flow Network Availability Ping Loss (Up and Down Packet)

Figure 5 describes the ICMP packet loss modeling for Network Availability calculations with calculations on the applied topology design. This ICMP packet loss service is based on the problem of each remote customer at the Service Provider (SP) experience, which occurs when real-time customers' networks are down. ICMP packet loss performs ping requests via the ICMP protocol. If ICMP replies with a value of 1 or in an *up* status, the ICMP packet loss will send a status with an *up* notification. Meanwhile, if ICMP replies with a value of 0 or down, the ICMP packet loss will send a status with *down* notification.

4. Schemes Service Level Agreement (SLA)

Each customer node in the remote site in the structure will have a status attribute. The SLA status is calculated according to the selected algorithm. At the lowest level of service is a trigger. The status of each customer node is affected by the trigger status. The Service Level Agreement (SLA) modeling concept as described above will explain the SLA calculation in detail as shown in table 2 Modeling SLA Service Data.

Table 1. Modeling SLA Service Data.

Parameter	Description
Service times	By default the service operates 24x7x365 with the formula: `Acceptable SLA x Number of Days in 1 Month x 24 Hours`
New service time	Service times:
	Uptime - service uptime
	Downtime - Service status (`Status State`) in this period does not affect SLA.
	One-time downtime - one-time downtime. Service status during this period does not affect SLAs.
Acceptable SLA (%)	99.5
SLA (%)	100

In SLA calculation, if sent ICMP Ping time is 1, the SLA value will be (SLA Calculation) up. Conversely, if the ICMP Ping time value is 0, it will affect the SLA value because the remote site status will experience downtime. In Figure 6, the SLA calculation process is the trigger used is ICMP ping time. If ICMP replies with value 1 or is in an *up* status, ICMP ping time will send a successful notification status (SLA Calculation). Meanwhile, if ICMP replies with a value of 0 or unsuccessful, the trigger on the ICMP packet loss will be active and initiate 4 delivery checks which equals to 150 ms (15 seconds) x 4, if there is a return after 4 checks, the value will become 1 and the status is successful (if at least one package out of four is returned, the item will return to 1). If there is no return after 4 checks, the value will remain at 0 and the status is unsuccessful (if at least no packages are returned, the item will return 0) (SLA Calculation). In Table 3, SLA modelling with calculations on the applied topology design is described. By default the service operates 24x7x365 with the formula: Acceptable SLA x Number of Days in 1 Month x 24 Hours. The acceptable SLA formulation or the agreement between Service Provide (SP) and customer is 99.5%.

SLA Service Customer	
Description Customer	**Customer Service VSAT**
Status calculation algorithm	Problem, if all device have problems
Kalkulasi SLA, Acceptable SLA (%)	99.5
Trigger	ICMP Ping Time (Unavailable Ping)
Periode	Uptime

In Figure 6 describes the ICMP ping time modelling flowchart and the explanation above:

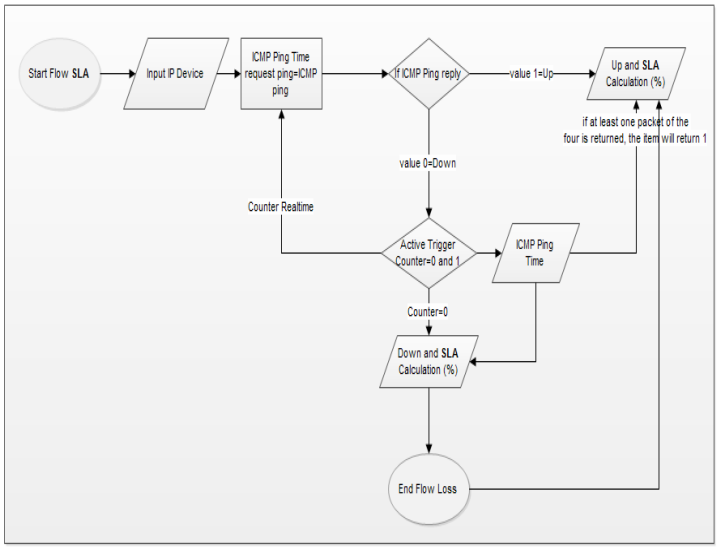


Figure 6. Service Level Agreement (SLA) Flow

RESULTS AND ANALYSIS

In this stage, the Network Availability and SLA generated from 7 days at the monitoring stage is analyzed. Output data is classified to determine the results of the Service Level Agreement (SLA) and Network availability in the modelling. The performance parameters obtained include ICMP Packet Loss, ICMP Ping: ICMP Ping Time and Latency (ICMP Response Time) and SLA Value.

1. Testing and Analyzing Service Results for ICMP Packet Loss, ICMP Ping Time and Latency (ICMP Response Time) Customer Site Satellite

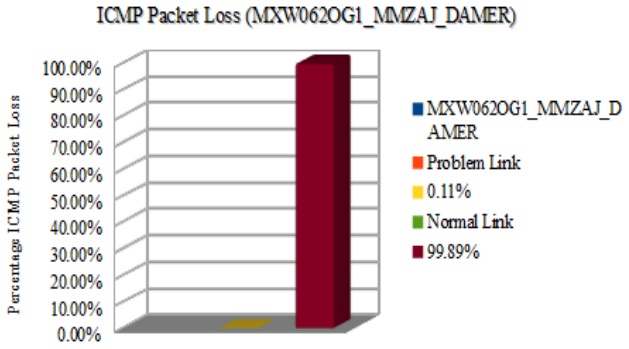
The test is carried out with a topological model with the value on the ICMP Loss packet in the specified time range.

A. ICMP Packet Loss

The ICMP packet loss data processing is carried out within a span of 7 days from 07-21-2020-17: 57 to 07-28-2020-17: 57, as shown in graph 4.6. Figure 7 shows the ICMP packet loss data collection process with the resulting trend of a problem link at 0.11% and a normal link at 99.89%, within a span of 7 days. Table 4 shows each time a remote site MXW062OG1_MMZAJ_DAMER encountered a link problem and its recovery process. Table 4.5 shows the result of the ICMP Packet loss trend occurred within the time range of 7/24/2020 14: 15-7 / 26/2020 18:35. With the ICMP Loss results, Service provider (SP) will obtain availability values with available data and identify detailed link problems occur and a detailed log of the link recovery process. Table 4 describes the results of the logs from the ICMP packet loss service status obtained from the monitoring system modeling.

The packet loss measurement is the number of packets lost during the transmission process to the remote customer. Packet loss occurs when one or more data packets passing through the media fail to reach their destination. In Figure 7, the sample trend result is the failed or down link problem

(Customer Link at remote site) with a percentage of 0.11% and a normal link of 99.89% is shown. The ICMP Loss parameter value that is tolerated between the SP and the customer has been met with a percentage of 99.89%.



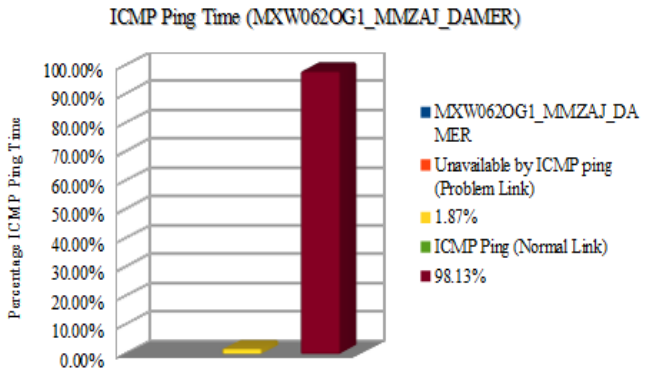
Time	Recovery Time	Customer Name	Problem	Duration
7/26/2020 18:35	7/26/2020 18:38	MXW062OG1_MMZAJ_DAMER	High ICMP ping loss	3m
7/24/2020 15:45	7/24/2020 15:46	MXW062OG1_MMZAJ_DAMER	High ICMP ping loss	1m 1s
7/24/2020 15:27	7/24/2020 15:29	MXW062OG1_MMZAJ_DAMER	High ICMP ping loss	2m 1s
7/24/2020 15:26	7/24/2020 15:29	MXW062OG1_MMZAJ_DAMER	High ICMP ping loss	3m 1s
7/24/2020 14:17	7/24/2020 14:18	MXW062OG1_MMZAJ_DAMER	High ICMP ping loss	1m 1s

Figure 6. Percentage of Value of Availability (ICMP Packet Loss) Customer MXW062OG1_MMZAJ_Damer

B. ICMP Ping Time

The ICMP ping time data processing is carried out in a span of 7 days from 07-21-2020-17: 57 to 07-28-2020-17: 57, as shown in Figure 4.7. In Figure 7, it is seen that the ICMP ping time collection data process resulting in a trend of a problem link of 1.87% and normal link of 98.13%, within a span of 7 days. Table 5 shows the respective times when the remote site MXW062OG1_MMZAJ_DAMER experienced link problems (Unavailable by ICMP ping) and the recovery process. The detailed recovery process can be seen in table 5. Table 5 shows the results of the ICMP Ping time trend that occurred from 7/24/2020 14: 15-7 / 26/2020 18:35, along with realtime ICMP packet loss sent to remote sites. With the results of this ICMP Ping time, Service Provider (SP) will obtain the availability value with available data to determine the status of the customer's device, as well as to identify occurring link problems in detail and a detailed log of the link recovery process. This ping time is the implication of packet loss that occurs, the time span of packet loss during the transmission process through the media to the remote customer. When the ICMP Packet loss sending process occurs, ICMP Ping will calculate the time duration and also calculate the recovery time that occurs from the hub or core hub to the remote customer. This occurs due to the instability of the transmission media, the propagation of data packets sent through the media, the occurrence of

delays and also interference with the signaling frequency.



Time	Recovery time	Status	Age	Duration
7/27/2020 19:40	7/27/2020 19:42	Resolved	23h 36m 20s	2m
7/27/2020 16:41	7/27/2020 16:43	Resolved	1d 2h 35m	2m
7/26/2020 18:36	7/26/2020 18:38	Resolved	2d 40m	2m
7/26/2020 17:50	7/26/2020 17:52	Resolved	2d 1h 26m	1m 58s
7/26/2020 17:46	7/26/2020 17:47	Resolved	2d 1h 30m	1m
7/26/2020 17:27	7/26/2020 17:31	Resolved	2d 1h 49m	4m 1s
7/25/2020 20:08	7/25/2020 20:09	Resolved	2d 23h 8m	1m 1s
7/25/2020 17:56	7/25/2020 17:57	Resolved	3d 1h 20m	1m
7/24/2020 20:21	7/24/2020 20:24	Resolved	3d 22h 55m	2m 58s
7/24/2020 19:40	7/24/2020 19:41	Resolved	3d 23h 36m	1m
7/24/2020 19:36	7/24/2020 19:37	Resolved	3d 23h 40m	1m
7/24/2020 17:07	7/24/2020 17:11	Resolved	4d 2h 9m	4m 1s

Figure 7 Percentage Value Link Availability (ICMP Ping Time) Customer MXW062OG1_MMZAJ_Damer

C. ICMP Ping Latency

ICMP ping response time (latency) data processing is carried out within 7 days from 07-21-2020-17: 57 to 07-28-2020-17: 57, as shown in Figure 8. Graph 8 shows the process of data retrieval of ICMP ping response time (latency) with an average trend result at 562 -ms. Table 6, describes the respective times when the MXW062OG1_MMZAJ_DAMER remote site experiences high latency and normal latency. The detailed recovery process can be seen in table 6. Table 6 is the result of the ICMP Ping Response (Latency) trend that occurred from 7/24/2020 14: 15-7 / 26/2020 18:35, along with realtime ICMP packet loss sent to remote sites. With the results of this ICMP Ping Response (Latency), the value of availability with available data will be obtained by the Service Provider (SP) to determine the status of delay (latency), as well as to identify the occurring details and the detailed log of operational customer

link processes. Following, table 2 describes the results of the logs from the ICMP ping response time (latency) service status from the monitoring system modeling.

Table 2 Results of the Logs from the ICMP

Timestamp		ICMP Latency
7/28/2020 21:03	0.5805	580.5
7/28/2020 21:03	0.5924	592.4
7/28/2020 21:03	0.588	588
7/28/2020 21:03	0.5963	596.3
7/28/2020 21:03	0.5765	576.5
7/28/2020 21:03	0.5728	572.8
7/28/2020 21:03	0.5844	584.4
7/28/2020 21:02	0.6004	600.4
7/28/2020 21:02	0.5787	578.7
7/28/2020 21:02	0.5682	568.2

The ICMP latency value occurs due to the instability of the transmission media, the propagation of the transmission of data packets through the media, the occurrence of delays and also disturbances in the frequency or signaling of the transmission media. In the application of this study, the resulted ICMP latency value is normal, which is an average of 500 ms. Average range of latency values on satellite media by default is 450-900 ms.

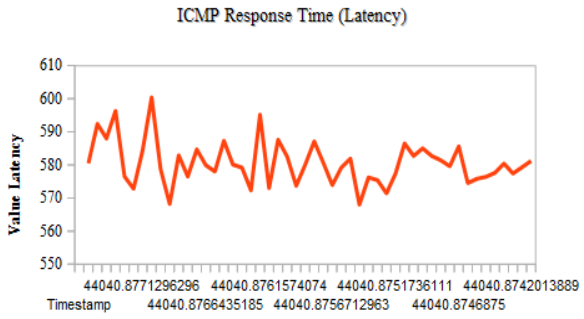


Figure 8 Percentage value link Availability (icmp ping response time (latency) customer MXW062OG1_MMZAJ_Damer

D. Network Availability Testing (ICMP Packet Loss, ICMP Ping Time and ICMP Ping Latency)

2. Data Service Level Agreement (SLA) Test Results

Service Level Agreement (SLA) data processing is carried out within a span of 1 month and within a period of 7 days from 7/6/2020 12:00:00 AM to 7/27/2020 12:00:00 AM, as shown in chart 4.9. Service Level Agreement data collection process (SLA with an average acceptable SLA result trend is 99.9% of 100% SLA, within 1 month. The SLA calculation value is related to ICMP packet loss. When a remote site experiences packet loss, the level will be calculated. Customer link loss is equal to the total amount of traffic lost divided by the total amount of input traffic over a given period of time.

Through the SLA, Service Provider obtain quality assurance value of customer link availability from the available data, the detailed SLA data within the required timeframe will also be obtained. This SLA value is the guarantee or quality assurance value of link availability for customers as agreed with the Service Provider (SP). SLA is agreed upon between the Service Provider (SP) and the customer, as a guarantee or availability link for the services provided by the Service Provide (SP) to the customer. In business, in the telecommunication and ICT SLA sector, the Service Provider (SP) will have it reported within a period of 1 month to the customer. In this study, the SLA value applied to remote customers is 99.5%. Table 4.9 shows that within a period of 1 month, the SLA value to the

customer is fulfilled with an average SLA of 99.9%. By knowing the parameters of this SLA value, it is expected that the level of service and also the minimum level is identified and customers can use the maximum service from the Service Provider (SP).

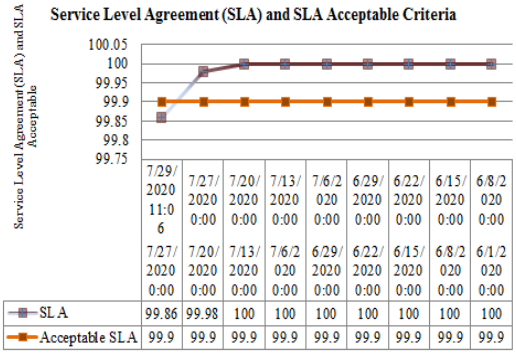


Figure 9 Percentage value of SLA and SLA links Acceptable customer MXW062OG1_MMZAJ_Romean

3. Testing and Analysis of ICMP Packet Loss Results, ICMP Ping Time and Latency (ICMP Response Time) Customer site Terrestrial

In the above discussion, testing and analysis of network topology has been done by modeling the customer site using satellite transmission media. Furthermore, the network availability will be tested and analyzed by comparing the customer site with terrestrial media with the same parameters, namely the ICMP Packet Loss, ICMP Ping Time and Latency (ICMP Response Time) and Service Level Agreement (SLA) values.

A. ICMP Ping Packet Loss

The data parameter results from ICMP packet loss are obtained from a span of 7 days from 2020-07-22 16:29:19 to 2020-07-28 17:17:11, as shown in Figure 10. Figure 10 map the process of ICMP packet loss data collection which resulted in 1.3142% of problem link and 98.6858% of normal link within a span of 7 days.

From the ICMP Loss data results, the value of network availability from the available data will be obtained by the Service Provider (SP), along with the detailed problem links occured and a detailed log of the link recovery process. In the following table 4.9, the logs of ICMP packet loss service status obtained from the monitoring system modelling is described.

The mapping of changes occurred in each trend is shown in Figure 10. Figure 4.10 shows the sample trend where links (Customer Link on remote site) experiencing failure or down constitute a percentage of 1.31% and the normal links conctitute 98.68%. The ICMP Loss parameter value that is tolerated between SP and customer has been met with a percentage of 98.68%.

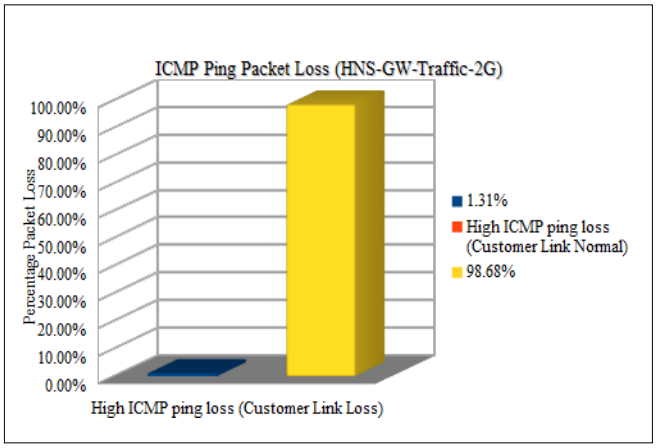


Figure10. Percentage of value Link Availability (ICMP Packet Loss) customer Hub-System-HNS-GW-Traffic-2G

When the ICMP Packet loss sending process occurs, ICMP Ping will calculate the delivery time and recovery time from the hub or

core hub to the remote customer. Packet loss occurs because of instability of the transmission media, propagation of data packet delivery through the media, occurrence of delay or packet delay when passing through the transmission line.

B. ICMP Ping Time

The ICMP ping time data collection is carried out within a period of 7 days from 2020-07-22 16:29:19 to 2020-07-28 17:17:11, as shown in Figure 11. Figure 11 shows that from the ICMP ping time data collection process, a trend resulted is a problem link of 0.3203% and normal link of 99.6797%, within a span of 7 days.

From the ICMP Ping time, the value of availability from the available data will be obtained by the Service Provider (SP) to determine the status of the customer's device, the status of the service link, and to find out in detail the problematic link occurred and a detailed log of the link recovery process. This ping time is the implication of occurring packet loss, the time span of packet loss during the transmission process through the media to the remote customer. When the ICMP Packet loss sending process occurs from the hub or core hub to the remote customer, ICMP Ping will calculate the duration and recovery time . Packet loss occurs because of instability of transmission media, propagation of data packets sent through the path, the occurrence of delay and also interference with the signaling frequency.

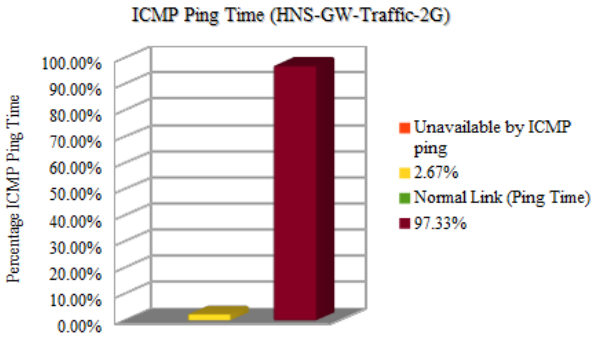


Figure 11. Percentage of Value of Link Availability (ICMP Ping Time) for HNS-GW-Traffic-2G customers

C. ICMP Ping Latency

The ICMP ping response time (latency) data collection is carried out within a period of 7 days from 2020-07-22 16:29:19 to 2020-07-28 17:17:11, as shown in Figure 12. The ICMP ping response time (latency) data shows an average trend result of 3 ms. Figure 12 shows the respective times when the Hub-JKTDR3SJ01 remote site experienced high latency and normal latency. High latency occurs because of decrease of transmission quality and propagation of packet delivery, creating delays on the transmission path.

ICMP latency has a mean yield trend of 3 ms. The ICMP latency value occurs due to the instability of the transmission media, the propagation of the transmission of data packets through the media, the occurrence of delays and also disturbances in the frequency or signaling of the transmission media. In the application of this study, the resulting ICMP latency value is normal, which is an average of 3 ms. Default range of latency values for terrestrial media is 2-10 ms.

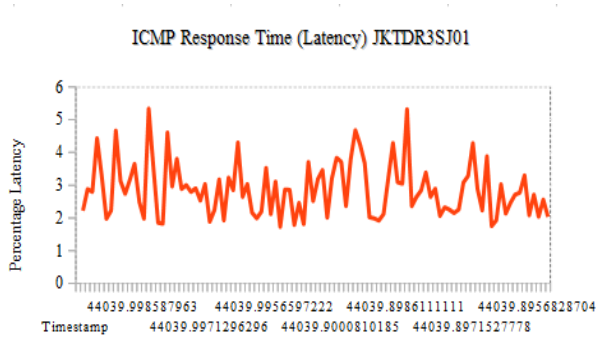


Figure 12. Percentage of value link Availability (icmp ping response time (latency) customer JKTDR3SJ01

D. Service Level Agreement (SLA) Test Results

The value of the Service Level Agreement (SLA) is tested over a period of 1 month and within a period of 7 days from 2/3/2020 12:00:00 AM to 12/08/2020 12:00:00 AM, as shown in Figure 13 Image retrieval of Service Level Agreement (SLA with the trend of acceptable SLA average results at 99.9% of 100% SLA, within 1 month). From the results of this SLA, the quality assurance value of customer link availability from the available data will be obtained by the Service Provider (SP), as well as identification of detail SLA data within the time needed.

Below is a Figure 13 which shows the percentage of the log of the service level agreement status obtained from the monitoring system modeling.

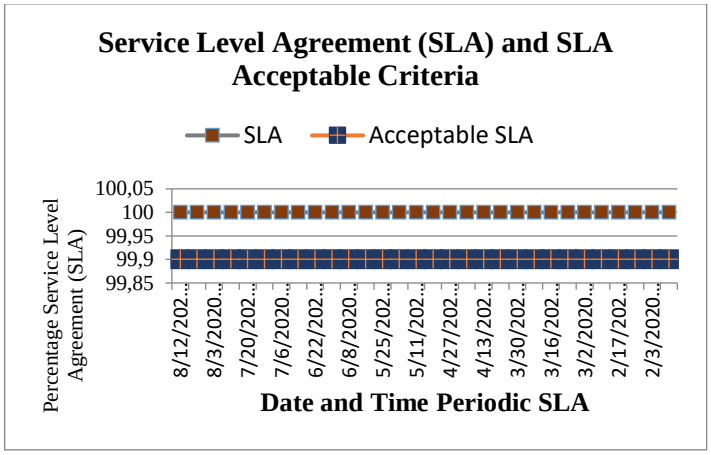


Figure 13. Percentage value of SLA and SLA Acceptable customer links JKTDR3SJ01

This SLA value is the guarantee or the quality assurance value of link availability for the customer as agreed with the Service Provider (SP). SLA is agreed upon between the Service Provider (SP) and the customer, as a guarantee or availability link for the services provided by the Service Provide (SP) to the customer. In business, in the telecommunication and ICT SLA sector, the Service Provider (SP) will report it within a period of 1 month to the customer. In this study, the applied SLA or acceptable SLA for remote customers was 99.5%. Table 4.12 shows that within 1 month, the SLA value to the customer is fulfilled with the average SLA of 100%. Recognising the parameters of this SLA value, it is expected that the level of service and also the minimum level are identified, and customers can use the maximum service from the Service Provider (SP).

Testing Network Availability (ICMP Packet Loss, ICMP Ping: ICMP Ping Time and Latency (ICMP Response Time) and Service Level Agreement

A. Network Availability generated from 7 days customer site VSAT

Figure 14 shows a dashboard view of a zabbix monitoring system designed to monitor service providers' customers. Of the several parameters designed in the zabbix monitoring system, there are customer taffic graph parameters and alarm systems, but the focus of testing in this study is how to obtain Network availability and Service Level Agreement (SLA) values, as a quality assurance of the availability of customer links with available data obtained by the Service Provider (SP), as well as identified detail SLA data within the required timeframe. So that in the future, service provider can report the data in accordance with their agreement with the customers.

Figure 14 dashboard display of the zabbix monitoring

Figure 15, shows failed links trend graph (Customer Link at remote site). With the ICMP Ping time results, Service provider will obtain availability value from available data to determine the status of the customer's device, as well as to identify links of problems occurred in detail and obtain a detailed log of the link recovery process. This ping time is the implication of packet loss that occurs, the duration of packet loss during the transmission process through the media to the remote customer VSAT.

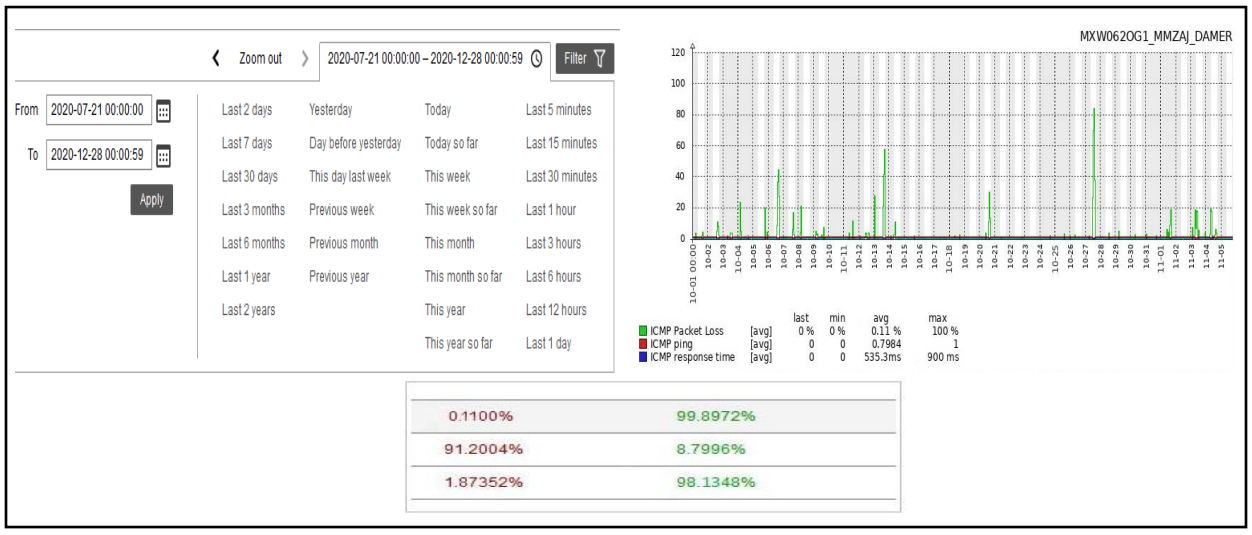


Figure 15 Network Availability generated from 7 days (ICMP Packet Loss, ICMP Ping Time and ICMP Latency) customer site VSAT

With the results of the ICMP Ping Response (Latency), Service Provider (SP) will obtain availability value from available data to determine the status of delay (latency), as well as to identify links of problem occurred and a detailed log of the operational customer link process. The real-time data collection which is accessible anytime and anywhere allows customer service providers to easily conduct periodical update on Network Availability status to customers. In the Graph, the Network Availability is presented in a percentage, for easier monitoring by Service Providers to and reporting to customers.

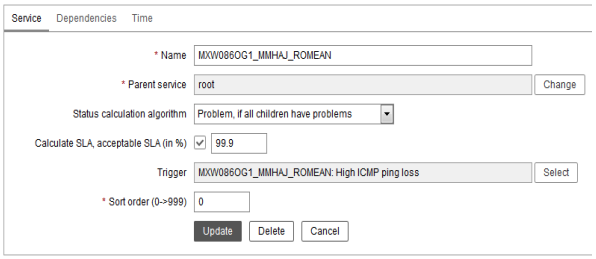


Figure 16 Test Service Level Agreement customers MXW062OG1_MMZAJ_Romean

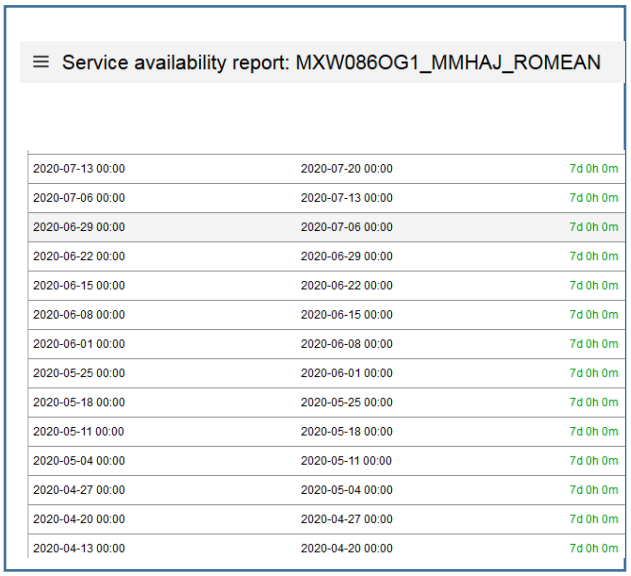


Figure 17 Result Test Service Level Agreement customers MXW062OG1_MMZAJ_Romean

B. Network Availability generated from 7 days) customer site Terrestrial

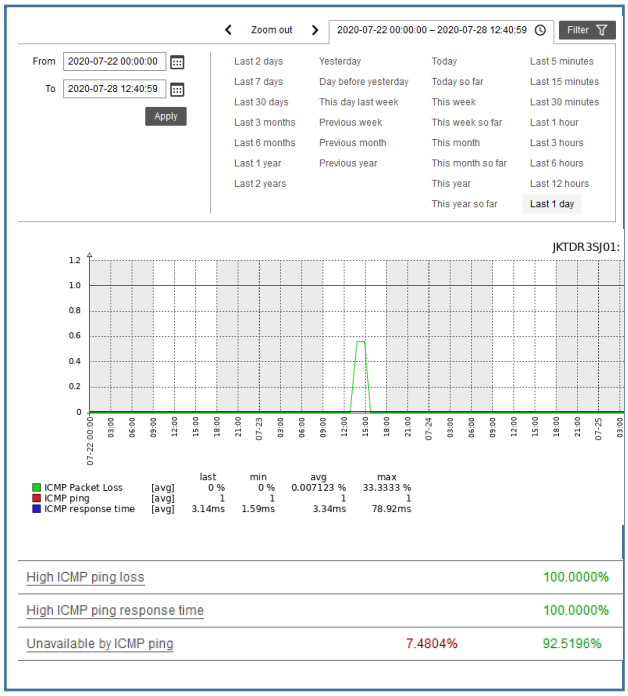
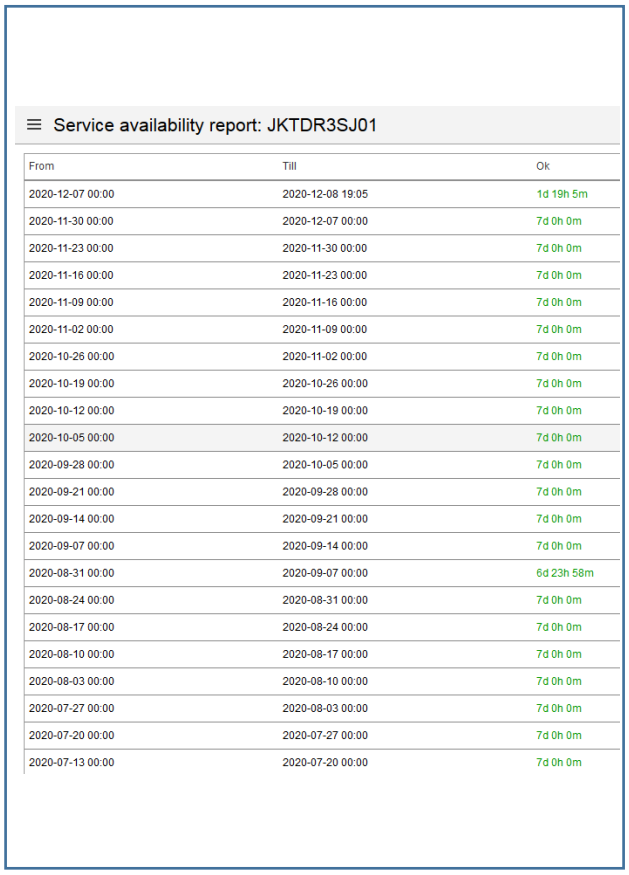


Figure 18 Network Availability generated from 7 days (ICMP Packet Loss, ICMP Ping Time and ICMP Latency) customer site Terrestrial

In Figure 18, the availability value will be obtained from the data available by the Service Provider (SP) to determine the status of the customer's device, as well as to find out in detail the problem links that occur and a detailed log of the link recovery process. This ping time is the implication of packet loss that occurs, the time span of packet loss during the transmission process through the media to the remote customer Terrestrial.

Figure 14 shows a dashboard view of the zabbix monitoring system which is designed to monitor customers from customer Service Level Agreement (SLA) service providers. The focus of testing in this study is how to obtain Network availability value

and display the Service Level Agreement (SLA), as a guarantee of quality of the availability of customer links with available data that will be obtained by Service Providers (SP), as well as identifying SLA data detail within the required time. The data allows service providers to report in accordance with their agreement with customers.

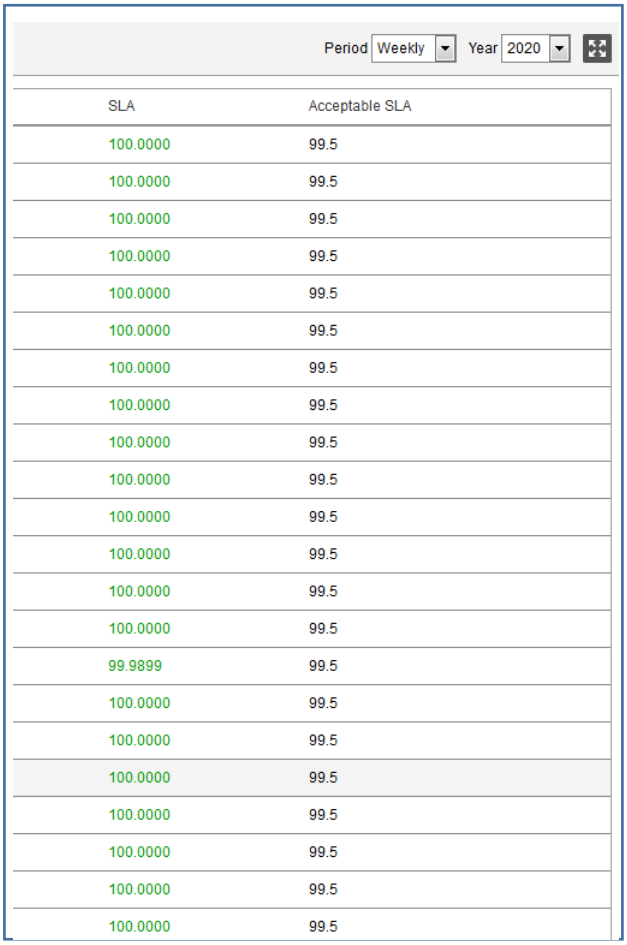


Service availability report: JKTDR3SJ01

From	Till	Ok
2020-12-07 00:00	2020-12-08 19:05	1d 19h 5m
2020-11-30 00:00	2020-12-07 00:00	7d 0h 0m
2020-11-23 00:00	2020-11-30 00:00	7d 0h 0m
2020-11-16 00:00	2020-11-23 00:00	7d 0h 0m
2020-11-09 00:00	2020-11-16 00:00	7d 0h 0m
2020-11-02 00:00	2020-11-09 00:00	7d 0h 0m
2020-10-26 00:00	2020-11-02 00:00	7d 0h 0m
2020-10-19 00:00	2020-10-26 00:00	7d 0h 0m
2020-10-12 00:00	2020-10-19 00:00	7d 0h 0m
2020-10-05 00:00	2020-10-12 00:00	7d 0h 0m
2020-09-28 00:00	2020-10-05 00:00	7d 0h 0m
2020-09-21 00:00	2020-09-28 00:00	7d 0h 0m
2020-09-14 00:00	2020-09-21 00:00	7d 0h 0m
2020-09-07 00:00	2020-09-14 00:00	7d 0h 0m
2020-08-31 00:00	2020-09-07 00:00	6d 23h 58m
2020-08-24 00:00	2020-08-31 00:00	7d 0h 0m
2020-08-17 00:00	2020-08-24 00:00	7d 0h 0m
2020-08-10 00:00	2020-08-17 00:00	7d 0h 0m
2020-08-03 00:00	2020-08-10 00:00	7d 0h 0m
2020-07-27 00:00	2020-08-03 00:00	7d 0h 0m
2020-07-20 00:00	2020-07-27 00:00	7d 0h 0m
2020-07-13 00:00	2020-07-20 00:00	7d 0h 0m

Figure 19 Service Level Agreement customers JKTDR3SJ01 (Terrestrial) test results

The Service Level Agreement (SLA) applied and agreed upon with remote customer is 99.5%. In the zabbix monitoring system that is designed, samples are collected within 1 week and daily average for the SLA value to customers is met with an average SLA of 100%. By knowing the parameters of this SLA value, it is hoped that the service level and also the minimum level will be identified and allow customers to use the maximum service from the Service Provider (SP).



Period Weekly Year 2020

SLA	Acceptable SLA
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
99.9899	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5
100.0000	99.5

CONCLUSIONS

Based on problems, literature studies, research reviews, research object reviews and research methodologies in the SLA Network Availability Mechanism Modeling and the Customer Service Provider Alert System, it can be concluded that these are network monitoring systems that provide many ways to monitor various aspects of network infrastructure down to end devices point. It can be characterized as a

distributed monitoring system with centralized management. While many installations have a single central system, it is possible to use distributed monitoring. The monitoring system has requirements and criteria with the following categories, configuration interfaces can be used to accommodate and define host definitions, service definitions, and command definitions. Service Providers (SP) are facing a critical situation today where they are expected to reduce the operational costs of their infrastructure. This has forced Service Providers to strive and make efforts to configure cheap and efficient management of their increasingly complex infrastructure. Almost all existing open sources only provide monitoring features without configuration functions.

In this study, modeling and identify knowing the performance and management of business service infrastructure that requires a centralized control monitoring system. Identify the advantages and disadvantages of the Network Availability Modeling method applied. Obtain accurate Service Level Agreement (SLA) value parameter test results, and become a reference for an agreement between a service provider and a customer. As a guarantee or link availability for the services provided by Service Provide (SP) to customers. With fulfilled SLA value of 100% from the agreed 99.5%, Network availability is fulfilled with a percentage of 98.89% and down time with a percentage of only 1% from the agreed 2%, and the latency value on terrestrial transmission media at 2 ms, from the agreed 8 ms and VSAT transmission media obtained is 500-600 ms from the latency agreement value of 700 ms. Accurate availability value parameter test results are obtained, and serves as a reference for agreement between a service provider and a customer, with the SLA and Network availability agreement has been fulfilled between Service Providers and Customers.

REFERENCES

Renitea, J., & Elizabeth, N. E. (2017). Network's server monitoring and analysis using Nagios. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).

C. Petruti, B. Puiu, I. Ivanciu and V. Dobrota, "Automatic Management Solution in Cloud Using NtopNG and Zabbix," 2018 17th RoEduNet Conference: Networking in Education and Research (Ro Edu Net), Cluj-Napoca, 2018, pp. 1-6.

O. Marik and S. Zitta, "Comparative analysis of monitoring system for data networks," 2014 International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, 2014, pp. 563-568.

S. Mescheryakov, D. Shchemelinin and V. Efimov, "Adaptive control of cloud computing resources in the Internet telecommunication multiservice system," 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, 2014, pp. 287-293.

J. Hernantes, G. Gallardo and N. Serrano, "IT Infrastructure-Monitoring Tools," in IEEE Software, vol. 32, no. 4, pp. 88-93, July-Aug. 2015.

A. Iqbal, C. Pattinson and A. Kor, "Performance monitoring of Virtual Machines (VMs) of type I and II hypervisors with SNMPv3," 2015 World Congress on Sustainable Technologies (WCST), London, 2015, pp. 98-99.

O. Marik and S. Zitta, "Comparative analysis of monitoring system for data networks," 2014 International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, 2014, pp. 563-568.

F. Rezac, J. Rozhon, M. Voznak, J. Slachta and J. Safarik, "Multi-agent system for monitoring the quality of speech in computer networks," 2015 38th International Conference on Telecommunications and Signal Processing (TSP), Prague, 2015.

T. Mullins and A. Bagula, "Monitoring Community Clouds: The Lightweight Network Management Protocol," 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, Vietri sul Mere, 2013, pp. 678-684.

Hendrawan, N. Rachmana and Iskandar, "Network Management System (NMS) using local collector mediation devices," 2016 10th International Conference on Telecommunication Systems Services and Applications (TSSA), Denpasar, 2016, pp. 1-4.

K. Urunov, S. Shin and S. Park, "The unique reliable identity system of enabling lightweight device management in NMS mechanism for the U-IoT," 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS), Seoul, 2017, pp. 411-414.

J. He, Y. Zhang and X. Yuan, "MDNS based automatic discovery method in optical NMS," 2017 16th International Conference on Optical Communications and Networks (ICOCN), Wuzhen, 2017, pp. 1-3.

H. Kim, D. Kwon and H. Ju, "Analysis of ICMP policy for edge firewalls using active probing," The 16th Asia-Pacific Network Operations and Management Symposium, Hsinchu, 2014, pp. 1-4.

P. Arote and K. V. Arya, "Detection and Prevention against ARP Poisoning Attack Using Modified ICMP and Voting," 2015 International Conference on Computational Intelligence and Networks, Bhubaneshwar, 2015, pp. 136-141.

A. Manna and M. Alkasassbeh, "Detecting network anomalies using machine learning and SNMP-MIB dataset with IP group," 2019 2nd International Conference on new Trends in Computing Sciences (ICTCS), Amman, Jordan, 2019, pp. 1-5.

I. Coonjah, P. C. Catherine and K. M. S. Soyjaudah, "Design and Implementation of UDP Tunneling-based on OpenSSH VPN," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida (UP), India, 2018, pp. 640-645.

Z. Jian, W. Dinggang, H. Kun and Y. Jin, "An Approach for Storage and Search of UDP Packet Data," 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, 2012, pp. 603-607.

H. Geng et al., "A hybrid link protection scheme for ensuring network service availability in link-state routing networks," in Journal of Communications and Networks, vol. 22, no. 1, pp. 46-60, Feb. 2020.

W. Wang and J. Doucette, "Availability optimization in shared-backup path protected networks," in IEEE/OSA Journal of Optical Communications and Networking, vol. 10, no. 5, pp. 451-460, May 2018.

Ying-Hui Fan, Jie Zhang, W. Nai and Y. Yu, "Study on working status evaluation of track circuits in Shanghai Metro Line 2," 2015 12th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, 2015, pp. 408-411.

Y. Wang, G. Yang, S. Huang, M. Chang and W. C. Kwong, "Multi-MTTR Asynchronous-Asymmetric Channel-Hopping Sequences for Scalable Cognitive Radio Networks," in IEEE Transactions on Cognitive Communications and Networking, vol. 4, no. 4, pp. 692-703, Dec. 2018.

H. Jiang, Y. Wang, L. Gong and Z. Zhu, "Availability-aware survivable virtual network embedding in optical datacenter networks," in IEEE/OSA Journal of Optical Communications and Networking, vol. 7, no. 12, pp. 1160-1171, Dec. 2015.

Hernantes, J., Gallardo, G., & Serrano, N. (2015). IT Infrastructure-Monitoring Tools. IEEE Software, 32(4), 88–93.

Takada, A., Tanji, N., Seki, T., Yamagoe, K., Soejima, Y., & Tahara, M. (2019). SLA Driven Operation - optimizing telecom operation based on SLA -. 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS).