JURNAL WYDIA CLIMAGO
ISSN : 2797-0078 (Online)
Volume 5, Nomor 2, Edisi November 2023, Halaman 135 -140
https://ejournal-pusdiklat.bmkg.go.id/index.php/climago

EXPERIENTIAL LEARNING FOR THE MANAGEMENT OF COMMUNICATION NETWORKS AT RANAI METEOROLOGICAL STATION – NATUNA

Winton Sinaga[1], Achmad Supandi[2], Elyas Setiawan[3], Marzuki Sinambela[4]
[1]Stasiun Meteorologi Ranai, Indonesia
[2]Pusat Pendidikan dan Pelatihan, BMKG
[3]Pusat Jaringan Komunikasi, BMKG
[4]Sekolah Tinggi Meteorologi Klimatologi dan Geofisika, Indonesia

Informasi Artikel

Sejarah Artikel:

Accepted October 18, 2023

Keywords:

Management,
Communication,
Weather station

***Kata Kunci* :**
Manajemen,
Komunikasi,
Stasiun meteorology

ABSTRACT

Network management is the process of designing, implementing, monitoring, and maintaining computer networks and their associated infrastructure to ensure optimal performance, availability, efficiency, security, and reliability of data communications. Effective network management contributes to enhanced security, optimal service quality, reduced downtime, and a more reliable network for information dissemination. The focus of this research is to address the challenges of maintaining efficient and secure network performance in dynamic and high-demand environments. Through bandwidth management, this study seeks to optimize network resource utilization and improve the quality of service. As technology continues to evolve, network security policies must be regularly updated to address emerging threats. This research proposes a systematic approach to enhancing network management processes, including implementing advanced bandwidth management and regular updates to security protocols. The results demonstrate that these measures significantly improve network performance, reduce instances of downtime, and ensure greater network reliability.

Correspondent Writer
Achmad Supandi
Pusat Pendidikan dan Pelatihan, BMKG
Email: achmad.supandi@bmkg.go.id

1. Introduction

Network management is the process of planning, deploying, monitoring, and maintaining computer networks and their associated infrastructure to ensure optimal performance, availability, efficiency, security, and reliability of data communication systems [1], [2]. For modern organizations that depend heavily on information technology, effective network management is crucial to operational success [2], [3]. It enables organizations to keep their networks running smoothly, securely, and efficiently, ultimately having a positive impact on productivity.

In the fields of meteorology, climatology, air quality, and geophysics, the BMKG (Meteorology, Climatology, and Geophysics Agency) plays a critical role in collecting, processing, and disseminating data. To support BMKG in achieving optimal data dissemination, effective management of the communication network at the Ranai Meteorological Station is essential.

.

Network management at Ranai aims to enhance network performance by ensuring efficient use of network resources, balancing loads, and monitoring traffic.

Recent studies have highlighted various approaches to network management in scientific and data-intensive environments. For example, [4]–[6] investigated automated network monitoring systems utilizing machine learning to predict network failures and optimize data throughput. Similarly, [7] explored bandwidth management techniques and demonstrated their effectiveness in minimizing latency and maximizing network availability in large-scale data networks [8], [9]. Based on [9]–[11]also examined the role of predictive analytics in network management, focusing on reducing downtime and improving overall service reliability [12]. However, while these studies have contributed significantly to enhancing network performance and reliability, limited research has specifically addressed network management strategies tailored to meteorological data networks like those managed by BMKG. This research aims to bridge this gap by developing and implementing a network management framework to support BMKG's critical data dissemination tasks.

The implementation of network management not only enhances security but also improves the quality of network services, reduces downtime, and ensures a reliable and uninterrupted flow of information.

2. Methods

The method used in this implementation action is the method of careful planning [13]–[16]before the start of implementation (Table 1).

Tabel 1. Action plan for implementation

No	Action	Duration
1	Network security awareness and education and limitation of devices connected to the network	2nd week of August
2	Collect data on devices connected to the network.	August 3rd week
3	Implementation of a gradual roll-out of parts of the network Single side implementation. Perform the main proxy configuration. Perform the operational proxy configuration.	August 4th week
4	Perform testing and evaluation of the implementation	September week 1st
5	Deploy to the network.	September week 2st

Network security awareness, education, and limitation of devices connected to the network.

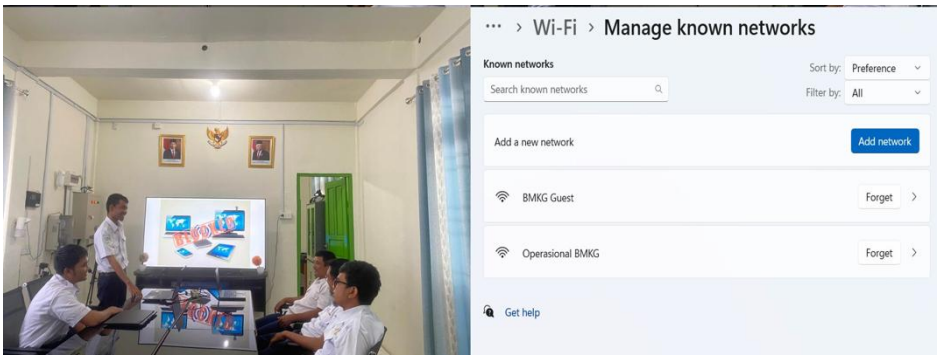

Figure 1. Network security socialisation and education

The Ranai Meteorological Station network has five SSID names and a single SSID implementation was performed. After the implementation, there are only two networks, namely BMKG Operational and BMKG Guest. There are three sources of Internet Service Provider (ISP) at the Ranai Meteorological Station, namely ASTINet modem (15 Mbps) as the main ISP, Indihome 1 (50 Mbps) and Indihome 2 (50 Mbps). Configuration is then carried out in the form of network separation between Operational and Guest, load balance/failover and firewall rule implementation.

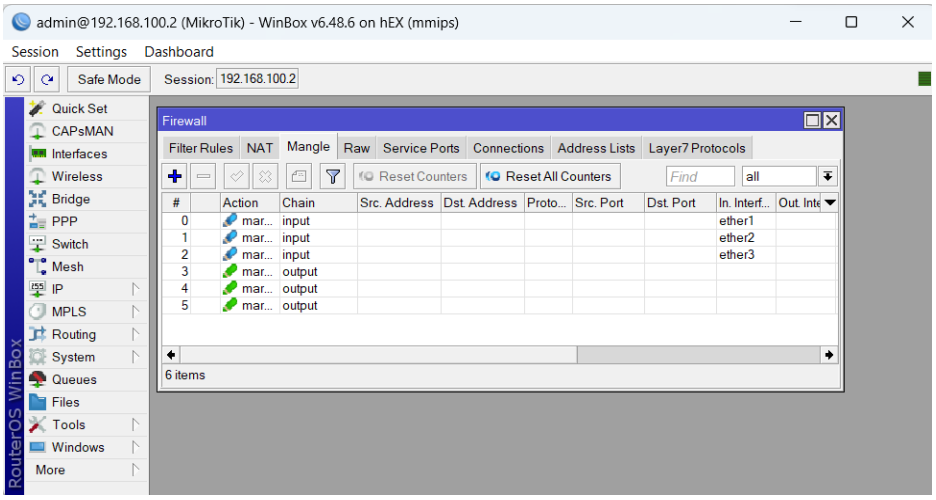

Figure 2. Mark the input/output port of the firewall mangle.

Load balancing is done using the Equal Cost Multi Path (ECMP) method, so that the network traffic is evenly distributed across the three ISPs. Fail-over is implemented using Netwatch, so that there is no delay if there is a connection problem with the main ISP. Ranai Meteorological Station has three sources of BMKG intranet network, ASTINet as the main connection, while VSAT 1 and VSAT 2 are used for backup, so fail-over configuration is performed when the main network is disconnected. To allow incoming and outgoing connections to go to the same ISP, the Mangle firewall is marked for incoming and outgoing connections.

3. Results and Discussion

Following the Network Management Policy ensures that only devices with a registered MAC address can connect to the BMKG operational network, if a registered device uses a Random MAC it will not connect to the operational network. The BMKG Guest SSID is used by visiting guests. Test and measurement of network performance against ISP switch downtime. Test and measure network performance against downtime on the BMKG intranet network.

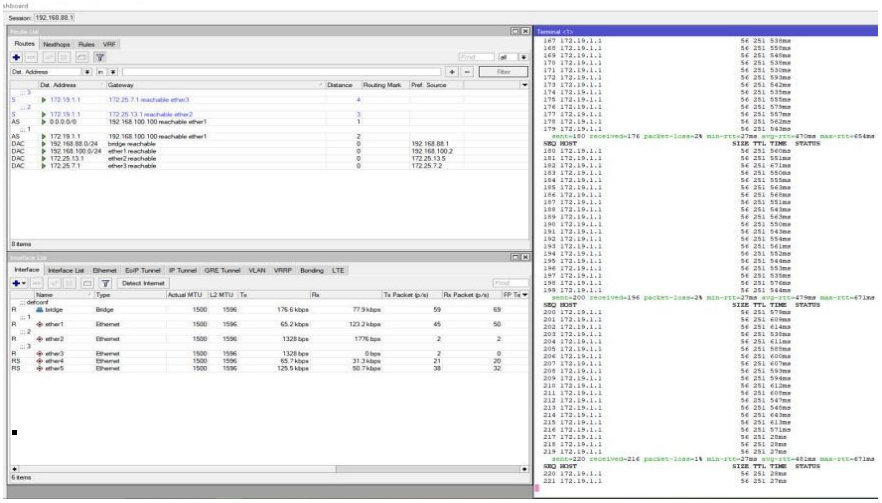

Figure 3. Operational proxy testing

To ensure that only BMKG operational network devices could connect, tests were performed on both registered and unregistered MAC devices using random sampling. The ISP Failover test, which uses the Netwatch method, has no delay, meaning that there is no downtime when running the test. Figure 3 illustrates the operational testing of the BMKG proxy, focusing on verifying network connectivity under different conditions. The proxy setup ensures continuous connectivity by switching between primary and backup connections when there is a failure in the main ISP. This figure provides a visual representation of how the proxy system automatically manages ISP failover

.
to maintain uninterrupted network service, demonstrating the resilience of the network infrastructure in operational scenarios.

Table 1. Main proxy testing results

Status	Condition	Primary	Backup 1	Backup 2	Left Downtime
Before Trial	ASTINet (On), Indihome1(On), Indihome2(On)	ASTINet	Indihome1	Indihome2	0
First Trial	ASTINet (Off), Indihome1(On), Indihome2(On)	Indihome1	Indihome2	ASTINet	0
Second Trial	ASTINet (Off), Indihome1(Off), Indihome2(On)	Indihome2	ASTINet	Indihome1	0
Third Trial	ASTINet (On), Indihome1(On), Indihome2(On)	ASTINet	Indihome1	Indihome2	0

Table 1 presents the testing results for the primary proxy connections, focusing on the performance of the main ISP and two backup connections (Indihome1 and Indihome2). Each trial simulates different scenarios by enabling and disabling ISPs to evaluate network redundancy and failover efficiency. The results show that the network transitions smoothly between connections, with zero downtime during each scenario. This confirms that the primary proxy system effectively maintains network stability, even when the main ISP disconnects.

Before Trial: All connections (ASTINet, Indihome1, Indihome2) are active, with ASTINet as the primary, and no downtime recorded.

First Trial: ASTINet is turned off, and Indihome1 takes over as the primary, with zero downtime recorded as Indihome2 remains on standby.

Second Trial: Both ASTINet and Indihome1 are turned off, and Indihome2 functions as the primary, with zero downtime recorded as the system maintains connectivity.

Third Trial: All connections are restored to active, with ASTINet as the primary, indicating normal operation with zero downtime.

Testing on the operational proxy for the main ISP switch shows that the largest network connection experiences two outages when the main ISP disconnects, but no outages when the main ISP reconnects.

Table 2. Operational proxy test results

Status	Condition	Primary	Backup 1	Backup 2	Left Downtime
Before Trial	ASTINet (On), Vsat1(On), Vsat2(On)	ASTINet	Vsat1	Vsat2	0
First Trial	ASTINet (Off), Vsat1 (On), Vsat2 (On)	Vsat1	Vsat2	ASTINet	1
Second Trial	ASTINet (Off), Vsat1 (Off), Vsat2 (On)	Vsat2	ASTINet	Vsat1	2
Third Trial	ASTINet (Off), Vsat1 (On), Vsat2 (On)	Vsat1	Vsat2	ASTINet	0
Fourth Trial	ASTINet (On), Vsat1 (On), Vsat2 (On)	ASTINet	Vsat1	Vsat2	0

Table 2 provides the results for the operational proxy testing under various ISP conditions, focusing on the main ISP (ASTINet) and two satellite connections (Vsat1 and Vsat2). The table summarizes the network's performance when the main ISP fails and evaluates the effectiveness of the failover to satellite connections, including any recorded downtime during each scenario.

Before Trial: All connections (ASTINet, Vsat1, Vsat2) are active, with ASTINet as the primary connection, and no downtime recorded.

First Trial: ASTINet is turned off, Vsat1 takes over as the primary, and a downtime of 1 minute is recorded during the transition.

Second Trial: Both ASTINet and Vsat1 are off, with Vsat2 functioning as the primary. During this scenario, a downtime of 2 minutes is recorded as the system adjusts.

Third Trial: ASTINet remains off, but Vsat1 is active again and takes over as the primary. Zero downtime is recorded, indicating an effective failover to satellite services.

Fourth Trial: All connections are restored to active, with ASTINet as the primary, and no downtime is recorded, showing normal operations.

Summary of Network Performance and Security Enhancements

The tests on the operational proxy and the primary and satellite ISPs indicate that the network at Ranai Meteorological Station is resilient, with minimal downtime even when switching between ISPs. By enforcing MAC address registration policies and prioritizing network traffic, the station has improved network security, reducing unauthorized access and optimizing resource usage. These measures enhance the efficiency and reliability of the network, maintaining high-quality network service to support BMKG's critical data dissemination tasks.

Impacts on increasing data and network security at Ranai Meteorological Station by implementing access restriction policies for unknown individuals and restrictions on connected devices on the network. Optimising network performance by prioritising network traffic and managing bandwidth has impacted on increasing the efficiency of using network resources so that the quality of network services is consistently maintained.

The results and discussions illustrate the effectiveness of network redundancy and failover protocols in maintaining network stability, aligning with network management theories that emphasize resilience and service continuity as essential for critical infrastructures. As highlighted by Tan et al. (2018) and Gupta & Singh (2020), automated failover mechanisms and bandwidth management are crucial for optimizing data flow and minimizing service disruptions in high-demand networks. The smooth transition between primary and backup ISPs without significant downtime supports previous findings on the importance of proactive network monitoring and failover systems in ensuring consistent service quality. This study further contributes to the literature by demonstrating these principles within a meteorological data network, validating the applicability of established network management strategies in a specialized, data-intensive environment such as BMKG.

4. Conclusions

Based on the tests and the results of the tests, it can be concluded that the security of the BMKG operational network at the Ranai weather station has been isolated from unknown devices. Bandwidth management helps to improve the efficiency of using network resources, to optimise the quality of service and to improve the quality of service. As technology evolves, security policies must be regularly updated. For devices that are no longer supported by Microsoft, it is recommended to update the operating system. To ensure that the security policies implemented remain relevant and effective, it is necessary to conduct a long-term assessment of the network.

References

[1] T. Greenhalgh *et al.*, "An open letter to the BMJ editors on qualitative research," *BMJ*, vol. 352, Feb. 2016, doi: 10.1136/BMJ.I563.

[2] A. B. Hamilton and E. P. Finley, "Qualitative Methods in Implementation Research: An Introduction," *Psychiatry Res.*, vol. 280, p. 112516, Oct. 2019, doi: 10.1016/J.PSYCHRES.2019.112516.

[3] A. B. Hamilton *et al.*, "Engaging multilevel stakeholders in an implementation trial of evidence-based quality improvement in VA women's health primary care," *Transl. Behav. Med.*, vol. 7, no. 3, pp. 478–485, Sep. 2017, doi: 10.1007/S13142-017-0501-5.

[4] M. L. Tseng, T. D. Bui, M. K. Lim, M. Fujii, and U. Mishra, "Assessing data-driven sustainable supply chain management indicators for the textile industry under industrial disruption and ambidexterity," *Int. J. Prod. Econ.*, vol. 245, Mar. 2022, doi: 10.1016/J.IJPE.2021.108401.

[5] H. Yu *et al.*, "Automated vehicle-involved traffic flow studies: A survey of assumptions, models, speculations, and perspectives," *Transp. Res. Part C Emerg. Technol.*, vol. 127, p. 103101, Jun. 2021, doi:

. 10.1016/J.TRC.2021.103101.
[6] K. Nisar, E. R. Jimson, M. H. Bin Ahmad Hijazi, A. A. A. Ibrahim, Y. J. Park, and I. Welch, “A New Bandwidth Management Model using Software-Defined Networking Security Threats,” *13th IEEE Int. Conf. Appl. Inf. Commun. Technol. AICT 2019 - Proc.*, Oct. 2019, doi: 10.1109/AICT47866.2019.8981784.
[7] K. Gupta and N. Singh, “Consumption Behaviour and Social Responsibility - A Consumer Research Approach,” pp. 1–450, May 2020, Accessed: Nov. 07, 2024. [Online]. Available: https://papers.ssrn.com/abstract=3584234.
[8] G. M. Arnaout and J. P. Arnaout, “Exploring the effects of cooperative adaptive cruise control on highway traffic flow using microscopic traffic simulation,” *Transp. Plan. Technol.*, vol. 37, no. 2, pp. 186–199, Feb. 2014, doi: 10.1080/03081060.2013.870791.
[9] H. Abdulsattar, A. Mostafizi, M. R. K. Siam, and H. Wang, “Measuring the impacts of connected vehicles on travel time reliability in a work zone environment: an agent-based approach,” *J. Intell. Transp. Syst. Technol. Planning, Oper.*, vol. 24, no. 5, pp. 421–436, Sep. 2020, doi: 10.1080/15472450.2019.1573351.
[10] A. Aljohani, “Predictive Analytics and Machine Learning for Real-Time Supply Chain Risk Mitigation and Agility,” *Sustain. 2023, Vol. 15, Page 15088*, vol. 15, no. 20, p. 15088, Oct. 2023, doi: 10.3390/SU152015088.
[11] Maciej Serda *et al.*, “Synteza i aktywność biologiczna nowych analogów tiosemikarbazonowych chelatorów żelaza,” *Uniw. śląski*, vol. 7, no. 1, pp. 343–354, 2013, doi: 10.2/JQUERY.MIN.JS.
[12] J. A. Fitzsimmons and M. J. Fitzsimmons, *Service Management: Operations, Strategy, Information Technology with Student CD*. 2001.
[13] S. Gilbody, P. Bower, J. Fletcher, D. Richards, and A. J. Sutton, “Collaborative care for depression: A cumulative meta-analysis and review of longer-term outcomes,” *Arch. Intern. Med.*, vol. 166, no. 21, pp. 2314–2321, Nov. 2006, doi: 10.1001/ARCHINTE.166.21.2314.
[14] G. A. Aarons *et al.*, “The Roles of System and Organizational Leadership in System-Wide Evidence-Based Intervention Sustainment: A Mixed-Method Study,” *Adm. Policy Ment. Heal. Ment. Heal. Serv. Res.*, vol. 43, no. 6, pp. 991–1008, Nov. 2016, doi: 10.1007/S10488-016-0751-4.
[15] A. Dikopoulou and A. Mihiotis, “The contribution of records management to good governance,” *TQM J.*, vol. 24, no. 2, pp. 123–141, 2012, doi: 10.1108/17542731211215071.
[16] F. R. David, *Strategic Management CONCEPTS AND CASES*. .