Quality of Service EIGRP Routing Protocol on Campus Area Network

Hari Antoni Musril1*, Febria Sri Artika2, Sarwo Derta3, Gusnita Darmawati4, Riri Okra5

1,2,3,4,5Institut Agama Islam Negeri (IAIN) Bukittinggi, Bukittinggi, Indonesia
2Central Quensland University, Australia

Abstract. Quality of Service (QoS) is a method of measurement used to determine the capacity of a network to perform services. One of the QoS implementations is to manage the performance of routing protocol. The routing protocol is a method used to connect one router to another, to convey information correctly and to provide a guaranteed service. This study discusses the QoS of the Enhanced Interior Gateway Routing Protocol (EIGRP) applied to campus area network. EIGRP is a routing protocol which only available on Cisco routers and often refers to the proprietary protocol on Cisco. EIGRP can only be applied by Cisco routers and their fellow. Campus area network is an interconnection of computer networks within the campus area. Data exchange on campus network should be undertaken quickly and precisely to facilitate campus operations. The method used in this study was Network Development Life Cycle (NDLC) which consisted of several phases, namely analysis, design, simulation prototyping, implementation, monitoring, and management. The results of this study provided QoS with a throughput value of 77 bps, 0.53 percent of the packet loss value, 1.89 ms of latency, and 1.87 ms of jitter value. This indicates that the EIGRP routing protocol has a strong QoS value to be applied to campus area networks.

Keywords: Quality of Service (QoS), Enhanced Interior Gateway Routing Protocol (EIGRP), Campus Area Network, Router, Routing Protocol

1. Introduction

Computer is a programmable appliance to support human work consisting of input, process, and output devices. One of its developments is in the networking. A computer network is a series of "interconnections" between two or more autonomous computers linked to a wired or wireless communication media [1]. Using a computer network, users would be able to share data, software and different computer hardware. There will be more than one network on a wide network. The additional router is therefore needed to maintain the transmission of data between the networks. As an electronic device, the router forwards data between computer networks, where software and hardware are set up to route and forward information [2]. Routing is a mechanism for sending data packets that are transmitted from one network to another and it also selects the path which is passed by a packet. A good path depends
on the network load, the length of datagram, type of service requested, and the traffic patterns. In general, the routing scheme only considers the shortest path.

Various algorithms can be adopted in manage the routing process and these are known as the routing protocols. Addressing the path / route of data packets to be sent by this routing protocol will be regulated by forming a routing table. Each routing protocol has different way and method of performing its duties and will determine the strengths and weaknesses of each routing protocol.

Computer network technicians have used various types of routing protocols; however, the Enhanced Interior Gateway Routing Protocol (EIGRP) is currently widely used. EIGRP is an advanced routing protocol of its predecessor IGRP and can only be operated by routers produced by Cisco, Inc. EIGRP uses an autonomous system concept to describe the network routers that operate on the same protocol and share the same routing information [3].

EIGRP converges precisely to avoid loops, requiring less memory and processes. Therefore, the choice of a precise routing protocol will strengthen data traffic management. The routing protocol is not only designed to modify the backup route when the main path is ineffective, but also to decide which path is best to enter the terminal and to overcome complex routing situations quickly and precisely [4].

The performance of the routing protocol is determined by using parameters in the Quality of Service (QoS) parameters. QoS is a method of calculating the power of a network and an attempt to determine the features and characteristics of a service [5].

A good QoS routing protocol value is required in the Campus Area Network (CAN) as a group of Local Area Networks (LAN) forming a network within the campus [6]. It will connect a number of campus buildings, and computer networks in the campus area will provide convenience in learning and administration activities.

Based on the above description, this study discusses the Quality of Service (QoS) of the EIGRP routing protocol applied to the campus area network. EIGRP was measured by QoS parameters as follows: throughput, packet loss, delay, and jitter values.

2. Theoretical Framework

A. Quality of Service (QoS)

Quality of Service (QoS) is the network’s capacity to provide reliable services to specific network traffic by sharing bandwidth and managing jitter and latency with its parameters, including delay (latency), jitter, packet loss, and throughput [7]. QoS is largely determined by the quality of the network used and attenuation, distortion, and noise can reduce its value. The purpose of the QoS design is to assist clients be more productive by ensuring that they obtain stable performance from network-based applications.

The QoS Monitoring Model is consists of the following four components [8]:

1) Monitoring Application: It is a network administrator interface. The functions of this part are to collect data packet traffic information from the display, analyse and send the report to the user.

2) QoS Monitoring: This component provides a QoS monitoring mechanism by extracting information on the QoS parameters values from data packet traffic.

3) Monitor: It collects and records data packet traffic information, and then sends it to the monitoring programme.

4) Monitored Objects: These components are attributes and activities that are monitored on the network. In the QoS monitoring context, information is the current data packet that is monitored in real time. The type of data packet current in the IP layers can be determined from the source and the final station.
The QoS monitoring process is carried out in the transmission path segments or between intended codes through the data packet path (see Figure. 1).

![Figure. 1. Mode Monitoring QoS.](image)

The QoS parameters can be explained as follows [9]:

1) **Throughput**: It refers to the rate of effective data transfer, measured in bps (bits per second). The following table is the categories of this parameter (see Table 1.).

| Throughput Categories | Throughput (bps) | Index |
|-----------------------|------------------|-------|
| Very good             | 100              | 4     |
| Good                  | 75               | 3     |
| Fair                  | 50               | 2     |
| Bad                   | < 25             | 1     |

Throughput calculation equation:

\[
\text{Throughput} = \frac{\text{Data packed is accepted}}{\text{Duration of observation}}
\]

2) **Packet Loss**: This parameter describes the total number of packets loss due to collision (smash between packets sent by two or more users at the same time) and congestion (congested data traffic, which affects the slow connection) on the network. Packet loss groups are explicitly illustrated as follows (see Table 2.).

| Packet Loss Categories | Packet Loss (%) | Index |
|------------------------|-----------------|-------|
| Very good              | 0               | 4     |
| Good                   | 3               | 3     |
| Fair                   | 15              | 2     |
Packet loss calculation equation:

\[
\text{Packet Loss} = \frac{(\text{Sent data packet} - \text{Accepted data packet})}{\text{Sent data packet}} \times 100\%
\]

3) Delay: This represents the time required by the data to move from the starting point to the end. It can be influenced by distance, physical media, congestion or a long time phase. The following table (see Table 3) is a type of delay (latency):

| Latency Categories | Delay (ms)          | Index |
|--------------------|---------------------|-------|
| Very good          | < 150 ms            | 4     |
| Good               | 150 ms ≤ 300 ms     | 3     |
| Fair               | 300 ms ≤ 450 ms     | 2     |
| Bad                | > 450 ms            | 1     |

Delay measurement equation:

\[
\text{Delay} = \frac{\text{Packet Length}}{\text{Link Bandwidth}}
\]

4) Jitter: In electronics and telecommunications, jitter is characterised as the time variation of periodic signals; it is often related to clock reference sources. It can be observed from successive pulse frequencies, signal amplitudes, or periodic signal characteristics phases. It has certain categories (see Table 4.).

| Jitter Category | Jitter (ms)          | Index |
|-----------------|----------------------|-------|
| Very good       | 0 ms                 | 4     |
| Good            | 0 ms ≤ 75 ms         | 3     |
| Fair            | 75 ms ≤ 125 ms       | 2     |
| Bad             | 125 ms ≤ 225 ms      | 1     |

Jitter measurement equation:

\[
\text{Jitter} = \frac{\text{Total of delayed variation}}{\text{Total of accepted packet}}
\]

\[
\text{Total of delayed variation} = \text{Delay} - \text{(delay average)}
\]
B. Routing Protocol

Routing is a protocol used to receive routes or instructions from one network to the next. This is the process by which a router choose a path or route to send or forward a packet to the destination. Routers use the IP address terminal to send packets, and to know which route should be used to forward packets to their destination, the router must learn or share information between connected routers to determine the best path or route.

The routing protocol facilitates the exchange of information between routers. Routers will exchange information about the routing table, that is, information about other linked networks, using the routing protocol [10]. In general, the routing protocol is consists of static routing and dynamic routing.

Dynamic routing protocol, or also known as dynamic routing, is a form of routing where the router may recognise the path / best route to transfer data packets from one network to another. Dynamic routing creates a dynamic routing table (changes automatically) when the network topology changes. The EIGRP is a dynamic routing protocol (see Fig. 2).

![Dynamic Routing Protocols](image.png)

**Figure. 2.** Classification of Dynamic Routing Protocol.

C. Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is an advanced version of IGRP, offering superior operating efficiency. Only the Cisco routers or the Cisco proprietary distance vector routing protocol have approved this routing protocol. EIGRP is a remote vector protocol which controls a complex collection of metrics for the mileage of other networks. EIGRP also embodies the connection state protocol principle. Broadcasts are updated every 90 seconds to all adjacent EIGRP routers [1]. Each update only includes the changing of network, therefore EIGRP is sufficient for large networks.

EIGRP also uses the Diffusing Update Algorithm (DUAL) concept to generate the best way to reach the terminal address. DUAL uses two techniques that enable EIGRP to converge quickly. First, every EIGRP router saves its neighbour's routing table. This enables the router to use the new route directly to the terminal if the route is known. If no route is known based on previous router information from a neighboring router, the EIGRP router will actively go to the destination address and send a message to each neighboring router to get an alternative route to that destination. The message will still be sent until an alternative route has been found. Routers that are not affected by the change in topology will not respond to the messages sent.

EIGRP will update the routing table when changes are made. This change in information is addressed only to routers that are directly affected by changes to the topology. EIGRP is therefore very efficient in the use of bandwidth. EIGRP uses additional bandwidth for the HELLO protocol, which is used to monitor the status of the connection to the neighbouring routers.
EIGRP conducts a routing process to find the best route by producing three information tables, namely a neighbouring table containing information on all routers connected to it or forming a neighbour relationship, then a topology table that stores all route information created from neighbouring routers and finally a routing table containing information on all neighbouring routers that are still connected and the best route to reach the router. The first time a network topology is built, EIGRP will recognise a neighbour router where the interface that is directly connected to a neighbour router has zero distance and will increase by one if it has moved to the next neighbour router. All information is stored in the routing table.

After the routing table has been formed, the next step is for EIGRP to send a hello packet to find out the on or off condition of all its neighbouring routers. Hello packet messages are sent simultaneously; there will be a hold time in the message that is the maximum time to wait for a reply message from a neighbour router. If the neighbor router does not reply to the Hello packet message within the specified period, the next router will be declared off. This situation will require EIGRP to update the routing table.

Next, EIGRP and DUAL (Diffusing Update Algorithm) will determine the best path to reach the target. DUAL calculates which router will be designated as a successor and a feasible successor.

D. Campus Area Network

Campus Area Network (CAN) based on university or campus networking can link different campus buildings, such as departments / faculties, libraries, laboratories, and others [11]. Connecting different locations in the campus area will facilitate the transfer of information and.

CAN is designed to provide various facilities to support academic activities in the university environment. With the implementation of CAN, a number of inside and outside information can be obtained and disseminated quickly and precisely.

CAN generally uses devices such as routers, switches, hubs, network cards or wired or wireless connections and LAN as the backbone networks. Based on the breadth of coverage, CAN is larger than LAN but smaller than MAN and WAN.

3. Methodology

This study used Network Development Life Cycle (NDLC) method. In the NDLC design process, each stage will largely determine the results in the next phases. The beginning of the stage will be started with analysis, then the result of analysis will be used to design the network. Next, the design process will be simulated in a prototype form. Furthermore, the simulation results will be performed on the device and then monitored. Management is the last stage in the development of management policies for the sustainability of the system [12].

This method has a number of stages [13]:

1) Analysis: Needs analysis, problem analysis, user desires analysis, and current network topologies analysis are carried out at this initial stage.

2) Design: This stage will outline the design of the interconnection network topology that will be constructed from the previous data.

3) Simulation Prototyping: At this stage, a small-scale system or a prototype simulation test phase is carried out. The results of this stage will be used to design a larger scale of the actual system.

4) Implementation: The previous plan and design will be implemented at this stage. Fixing systems from the simulation stage will be implemented under actual conditions.

5) Monitoring: This stage is a significant stage in order to ensure that the computer and communication network can operate in accordance with the user’s initial objectives. Monitoring can be carried out by observing traffic on the network, monitoring active network connections and monitoring the results of bandwidth measurements across the network.

6) Management: The policy is going to be a concern at this regulatory level. It is necessary to initiate the organisation of the system and to maintain its reliability and sustainability.
4. Result and Discussion

E. Network Topology

The network topology scheme used in this study illustrates the interconnection between several buildings in the campus area network (see Fig. 3). Each building has a router that is connected to each other by cable media. The link between these buildings becomes a backbone for the campus area network. Routers in each building use the EIGRP routing protocol for data communication processes.

![Network Topology Scheme](image)

**Figure 3.** Network Topology Scheme.

In this study, the network topology (see Fig. 3) consists of six routers. Each building has a router, and each outer will be reconnected to other network devices such as switches, hubs, and access points. In each building, equipment such as computers, laptops and smartphones is connected to staff, lecturers and students. In this campus area network, each user in each building can communicate with each other.

F. Measurement of Quality of Service

The Campus Area Network designed to implement the EIGRP routing protocol could probably know the quality of service by measuring the value of the following parameters:

1) Throughput: The results obtained from the average throughput measurements was 77 bps (see Table 5.). This value indicates that the EIGRP routing protocol has good throughput results on the campus area network.

| Router | Throughput (bps) |
|--------|------------------|
| Building A | 78 |
| Building B | 77 |
| Building C | 75 |
| Building D | 76 |
| Building E | 77 |
| Building F | 79 |

2) Packet Loss: The results obtained from the average packet loss measurement was 0.53 % (see Table 6.). It points out that the EIGRP routing protocol has a very good packet loss result on the campus area network, which means that the packet loss number is very small.

| Router | Packet Loss (%) |
|--------|-----------------|
| Building A | 0.5 |
| Building B | 0.7 |
| Building C | 0.4 |
Building D 0.6
Building E 0.3
Building F 0.7

3) **Delay:** The result gained from the average of delay measurement was 1.89 ms (see Table 7.). The value shows that the EIGRP routing protocol has very good delay results on the campus area network.

| Router | Delay (ms) |
|--------|------------|
| Building A | 2.1 |
| Building B | 1.6 |
| Building C | 1.9 |
| Building D | 1.8 |
| Building E | 2.2 |
| Building F | 1.7 |

**Table 7. Results Of Delay Measurement**

4) **Jitter:** The result of the average jitter measurement was 1.87 ms (see Table 8.). It indicates the EIGRP routing protocol has good jitter results on the campus area network.

| Router | Jitter (ms) |
|--------|-------------|
| Building A | 2.2 |
| Building B | 1.7 |
| Building C | 1.8 |
| Building D | 1.9 |
| Building E | 2.1 |
| Building F | 1.5 |

**Table 8. Results Of Jitter Measurement**

5. **Conclusion**

Based on the results of the research, the EIGRP routing protocol is very appropriate for use in campus area networks. This is supported by the results of the measurements of the average value of the service quality criteria, which show satisfactory results. The result of the throughput measurement is 77 bps, which means that the EIGRP routing protocol has a good throughput. The result of the packet loss measurement is then 0.53 percent, which is in very good criteria. Moreover, the delay measurement has a value of 1.89 ms, which means that it is very good. Finally, the jitter measurement is 1.87 ms with good criteria. The EIGRP routing protocol that is implemented on campus area networks can work effectively as it has a good algorithm. The EIGRP routing protocol is a type of routing that has a speed to determine the best path and speed when sending data packets. Quality of service measurement can be used as an analysis of the level of reliability of the computer network. QoS parameters, i.e. availability and performance, consist of throughput, delay, packet loss, and jitter for measuring EIGRP routing protocol on campus area networks affecting traffic for each device or end user. Factors that could affect QoS campus area networks are attenuation, distortion, noise, and available bandwidth capacity.

**REFERENCES**

[1] H. A. Musril, “Analisis Unjuk Kerja RIPv2 Dan EIGRP Dalam Dynamic Routing Protocol,” *J. Elektro Telekomun. Terap.*, vol. 2, no. 2, hal. 116–124, 2015, doi: 10.25124/jett.v2i2.99.

[2] Wahana Komputer, *Cara Mudah Membangun Jaringan Komputer & Internet*. Jakarta: Mediakita, 2010.

[3] T. Lammle, *CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120*. New Jersey: Sybex, 2013.

[4] D. Abdullah, *Jaringan Komputer: Data Link, Network & Issue*. Lhokseumaweh: Unimal Press,
2015.

[5] R. Wulandari, “Analisis QoS (Quality of Service) Pada Jaringan Internet (Studi Kasus: UPT Loka Uji Teknik Penambangan Jampang Kulon – LIPI),” *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. 2, hal. 162–172, 2016, doi: 10.28932/jutisi.v2i2.454.

[6] O. K. Sulaiman dan A. Widarma, “Sistem Internet of Things (IoT) Berbasis Cloud Computing Dalam Campus Area Network,” in *Seminar Nasional Fakultas Teknik UISU*, 2017, hal. 9–12.

[7] Rasudin, “Quality of Services (QoS) Pada Jaringan Internet Dengan Metode Hierarchy Token Bucket,” *J. Penelit. Tek. Inform. Univ. Malikussaleh*, vol. 4, no. 1, hal. 210–223, 2014.

[8] Yoanes, “Metoda Real Time Flow Measurement (RTFM) untuk Monitoring QoS di Jaringan NGN,” in *Prosiding 14 Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia 3-6 Mei 2006 Institut Teknologi Bandung*, 2006.

[9] T. Pratama, M. A. Irwansyah, dan Yulianti, “Perbandingan Metode PCQ, SFQ, RED Dan FIFO Pada Mikrotik Sebagai Upaya Optimalisasi Layanan Jaringan Pada Fakultas Teknik Universitas Tanjungpura,” *J. Tek. Inform. Univ. Tanjungpura*, vol. 3, no. 3, hal. 298–303, 2015.

[10] S. Budiyanto dan A. S. Prasetyo, “Studi Analisis Performansi Protokol Routing IS-IS Dan OSPFv3 Pada IPv6 Untuk Layanan Video Streaming,” *J. Tek. Elektro*, vol. 5, no. 1, hal. 18–32, 2014.

[11] J. Sinaga, “Practice Managing Internet Connection Campus Area Network (CAN) With Firewall And Address List Mikrotik Router OS,” *Techno Nusa Mandiri*, vol. 10, no. 1, hal. 132–142, 2013.

[12] P. L. Maheswara, T. I. Bayu, dan Y. A. Susetyo, “Perancangan Global Positioning System (GPS) Pada Sensor Curah Hujan Menggunakan Raspberry Pi,” *Indones. J. Model. Comput.*, vol. 2, no. 2, hal. 9–16, 2019.

[13] Y. Afrianto dan A. H. Hendrawan, “Implementasi Data Center Untuk Penempatan Host Server Berbasis Private Cloud Computing,” *Krea-Tif J. Tek. Inform.*, vol. 7, no. 1, hal. 50–59, 2019.