International Journal of Applied Mathematics and Computing
E-ISSN: 3047-146X
P-ISSN: 3048-1988
IJAMC

Research Article

Optimizing Bandwidth Settings Using the Y.1731 Method Based on Ethernet OAM on Raisecom Devices in a Metro Ethernet Network

Dadang Iskandar Mulyana[1*], Nandang Sutisna[2], Tatinia Arda Rizqi Amalia[3], Muhamad Rafli Alfiansyah[4]

[1]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: dadang@stikomcki.ac.id
[2]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: nandangsutisna@stikomcki.ac.id
[3]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: tatiniaarda@stikomcki.ac.id
[4]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: muhamad.alfiansyah@pin.co.id
*Corresponding Author: dadang@stikomcki.ac.id

Abstract: The rapid development of network infrastructure demands high Quality of Service (QoS), especially in Metro Ethernet networks widely utilized by telecommunication service providers. A primary challenge is efficient bandwidth management to ensure network stability and performance. This research aims to optimize bandwidth management by implementing the Y.1731 method based on Ethernet Operations, Administration, and Maintenance (OAM) on Raisecom devices. The methodology employed is a quantitative experimental approach based on technical simulation within an Professional Network Emulator Tool Lab (PNET Lab), where real-time network performance measurements are conducted using the ITU-T Y.1731 protocol for key parameters such as delay, jitter, and packet loss on Raisecom devices (represented by Cisco routers). The expected outcomes include increased efficiency in bandwidth utilization through more adaptive allocation, comprehensive and accurate real-time network performance monitoring capabilities, validation of OAM functions on Raisecom devices, improved Quality of Service (QoS) and better Service Level Agreement (SLA) attainment, and the provision of technical recommendations for network management. The implementation of Y.1731 is anticipated to quickly detect and respond to service degradation, thereby providing a strong basis for decision-making in network management and contributing to the enhancement of service quality in Metro Ethernet networks through optimization based on proactive monitoring.

Keywords: Bandwidth; Ethernet OAM; Metro Ethernet; QoS; Raisecom.

Received: 15 August 2025
Revised: 11 September 2025
Accepted: 25 October 2025
Published: 30 October 2025
Curr. Ver.: 30 October 2025

1. Introduction

In the era of rapid digital transformation, network service quality (Quality of Service or QoS) has become a crucial aspect of Information and Communication Technology (ICT) infrastructure implementation, particularly in the public sector and electronic-based services. The Indonesian Government, through Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (Sistem Pemerintahan Berbasis Elektronik or SPBE), has emphasized the importance of reliable, secure, and measurable network systems. However, practical conditions indicate that network disruptions still frequently occur, especially within Metro Ethernet infrastructures that support e-government services, regional tax systems, and population data management. This condition reflects a gap between the need for high-quality network systems and the technical capabilities of

bandwidth management implemented by network operators (Government of the Republic of Indonesia, 2018).

Metro Ethernet has become a primary choice for building backbone network infrastructure due to its ability to provide high bandwidth, scalability, and cost efficiency. Global data indicate that the number of cities utilizing Metro Ethernet has increased significantly in recent years, accompanied by growing bandwidth demands from enterprise and government sectors. However, this growth has not been fully matched by improvements in network performance monitoring systems, particularly regarding precise bandwidth management (Nugroho, 2020).

One of the major challenges in Metro Ethernet network management is the suboptimal monitoring of technical performance directly associated with QoS parameters such as delay, jitter, and packet loss. These parameters greatly influence network effectiveness, particularly for real-time services such as video conferencing, online public services, and telemedicine. When bandwidth is not properly managed, service performance degradation can occur on a large scale without an accurate early detection mechanism (Credence Research, 2024).

To address these challenges, the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) developed the Y.1731 standard as part of the Ethernet Operations, Administration, and Maintenance (OAM) protocol, enabling real-time network performance monitoring. This standard integrates various measurement functions, including Delay Measurement Message (DMM), Loss Measurement Message (LMM), and Synthetic Loss Measurement (SLM). Y.1731 serves as a technical foundation for establishing data-driven Service Level Agreements (SLAs). Nevertheless, the implementation of Y.1731 in government network systems, particularly at the regional level, remains limited and is often not activated in device configurations.

Raisecom, as one of the Metro Ethernet equipment vendors widely used in network infrastructure projects in Indonesia, has equipped its products, such as the ISCOM6800, iTN2100, and RAX701, with full support for Y.1731 and Ethernet OAM features. However, in practice, these capabilities have not been fully utilized by government institutions or service providers. Limited technical training and the absence of contractual requirements mandating the use of these features are among the factors contributing to this issue (Vaez-Ghaemi, 2007).

Furthermore, existing regulations governing telecommunications network operations emphasize the importance of ensuring service quality but do not explicitly specify technical standards such as Y.1731 as tools for network performance verification. As a result, monitoring and evaluation of public network quality tend to remain administrative and subjective, lacking support from objective technical data. This situation may create difficulties in assessing service provider performance and establishing accountability in cases of network service agreement violations (Autenrieth et al., 2006).

Based on this background, this study aims to examine and optimize bandwidth management using the Y.1731 method based on Ethernet OAM on Raisecom devices within Metro Ethernet networks. The study focuses not only on technical aspects but also on governance and accountability issues related to digital service delivery. The results of network performance monitoring are expected to provide an objective basis for evaluating service provider performance, enforcing SLA-based contracts, and improving the quality of public services supported by reliable network infrastructure (Indukuri, 2011).

This study provides an original contribution to the field of network management, particularly in optimizing bandwidth allocation within Metro Ethernet infrastructures, by utilizing the ITU-T Y.1731 standard based on Ethernet Operations, Administration, and Maintenance (OAM) on Raisecom devices. The primary contribution of this research lies in the use of Y.1731 not only as a network performance monitoring mechanism but also as a foundation for decision-making processes aimed at achieving measurable and efficient bandwidth optimization.

Unlike previous studies that primarily employed Y.1731 as a tool for monitoring network performance indicators such as delay, jitter, and packet loss, this research integrates the measurement results into a more adaptive bandwidth management strategy. Consequently, the study extends beyond conventional Quality of Service (QoS) monitoring and moves toward the practical implementation of bandwidth optimization based on network performance parameters. This approach enables a more effective utilization of network resources while supporting the delivery of reliable and high-quality services in Metro Ethernet environments.

2. Literature Review

Network Infrastructure

According to Cisco, "A Local Area Network (LAN) is a collection of devices connected together in a single physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with a single user to an enterprise network with thousands of users and devices in an office or school. Regardless of its size, the defining characteristic of a LAN is that it connects devices within a limited area. In contrast, a Wide Area Network (WAN) or Metropolitan Area Network (MAN) covers a larger geographical region.

Some WANs and MANs connect multiple LANs simultaneously." Based on this statement, network infrastructure can be defined as a collection of interconnected systems. When classified according to scale, network infrastructure can be divided into three categories: Local Area Network (LAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN). LAN represents the smallest scale, covering only a local area or a single ownership domain, such as internal networks within schools, universities, offices, and similar environments. MAN covers a larger area than LAN and is commonly used to connect headquarters with branch offices through wired, wireless, or virtual interface tunnel connections. WAN represents the largest scale, encompassing networks that span across the globe (Lucena et al., 2009).

OSI Model

According to the AWS website, the Open Systems Interconnection (OSI) Model is defined as "a conceptual framework that divides network communication functions into seven layers. Data transmission across networks is highly complex because various hardware and software technologies must operate cohesively across boundaries. The OSI data model provides a universal language for computer networking, enabling different technologies to communicate using standardized communication rules or protocols." Based on this explanation, the Open Systems Interconnection (OSI) Model can be understood as a standard framework for communication between network devices. The model consists of multiple layers, each with its own specific functions (Lucena et al., 2009).

Static Routing

The routing method used in tunnel infrastructure is static routing. This is because static routes are given the highest priority, have the lowest administrative distance, and are configured with specific source and destination parameters. As a result, the virtual interface in this case is selected as the primary gateway to reach the destination. This is consistent with Cisco's explanation regarding static routes, which states that "Static routes have a lower administrative distance than dynamic routes and are preferred over dynamic routes when reaching the same destination" (Lucena et al., 2009).

Bandwidth

Bandwidth management is the process of controlling data traffic within a computer network to ensure that network capacity is allocated efficiently and according to service requirements. In this context, bandwidth refers to the maximum data transfer capacity, usually measured in Mbps or Gbps, that can pass through a network link. According to Cisco (2021), bandwidth management includes techniques such as traffic shaping, rate limiting, and Quality of Service (QoS), which are intended to prioritize services, prevent congestion, and maintain network performance stability. In Metro Ethernet networks, bandwidth management is particularly important because of the dense and diverse nature of data traffic, including video, voice, and public service-based data communications (Nugroho, 2020; Credence Research, 2024). In this study, bandwidth management focuses on how the Y.1731 protocol can be utilized to monitor and optimize network performance through parameters such as delay, jitter, and packet loss, enabling bandwidth allocation to be adjusted in real time based on technical performance data (Ryoo et al., 2008).

Y.1731

Y.1731 is a protocol standard developed by the International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) as part of the Ethernet Operations, Administration, and Maintenance (OAM) framework for real-time network performance measurement. The protocol is specifically designed for Carrier Ethernet networks, including Metro Ethernet, to ensure Quality of Service (QoS) through standardized technical parameters (Ryoo et al., 2008; Minei et al., 2016).

The main advantage of Y.1731 lies in its ability to generate performance data directly at Layer 2 (Data Link Layer) without relying on external monitoring systems or IP-based mechanisms such as Simple Network Management Protocol (SNMP). Therefore, this protocol is highly suitable for Carrier Ethernet environments that require high-performance monitoring with minimal latency (Hofstede et al., 2008).

In the context of implementation on devices such as Raisecom equipment, Y.1731 can be enabled to perform these functions automatically and programmatically, allowing operators to optimize bandwidth allocation, identify bottlenecks at an early stage, and ensure that service availability remains within acceptable limits for end users and applicable regulations (Indukuri, 2011; Juniper Networks, 2025).

In practice, Y.1731 plays a vital role in ensuring Quality of Service (QoS) through a systematic measurement approach involving several key technical parameters (Ryoo et al., 2008): 1) Frame Delay (end-to-end latency). 2) Frame Delay Variation (jitter). 3) Frame Loss Ratio. 4) Availability and Service Degradation.

The strength of Y.1731 lies in its ability to provide integrated performance monitoring directly at Layer 2 (Data Link Layer), eliminating dependence on external monitoring systems or IP-based monitoring mechanisms such as SNMP. As a result, it is highly effective for Carrier Ethernet environments that require precise and low-latency performance supervision (Minei et al., 2016).

Furthermore, Y.1731 provides mechanisms for both Fault Management (FM) and Performance Monitoring (PM), which are two fundamental pillars of modern network management. FM enables rapid fault detection and isolation, while PM delivers accurate performance statistics to support capacity planning and Service Level Agreement (SLA) analysis. Through its standards-based approach, Y.1731 strengthens Ethernet's position as a technology that is not only reliable in terms of throughput but also measurable and controllable in terms of service performance (Hofstede et al., 2008; Ryoo et al., 2008).

Ethernet OAM

Ethernet OAM (Operations, Administration, and Maintenance) is a set of functions and protocols designed to enable the monitoring, management, and maintenance of Ethernet networks, particularly in Carrier Ethernet environments such as Metro Ethernet. Its primary objectives are to ensure service availability, detect network faults at an early stage, and provide accurate network performance information to administrators (Juniper Networks, 2025; Ventre et al., 2019).

Ethernet OAM operates at Layer 2 of the OSI model, meaning it does not impose additional overhead on higher-layer protocols such as IP or TCP. This characteristic makes it ideal for large and complex transport networks, such as Metro Ethernet, which support various types of data traffic including government, educational, and business services. Ethernet OAM serves as a key instrument for bandwidth optimization and ensuring the performance of network-based public services. It not only assists network operators but also functions as a legal validation tool for verifying the achievement of Service Level Agreements (SLAs) in network procurement contracts (Hofstede et al., 2008; Ventre et al., 2019).

Metro Ethernet

Metro Ethernet is a type of Carrier Ethernet network designed to provide high-speed networking services across metropolitan areas. This technology enables interconnection among government buildings, schools, hospitals, and private offices within a city or provincial region using Ethernet standards commonly employed in Local Area Networks (LANs), but extended to support Wide Area Network (WAN) environments. According to the Metro Ethernet Forum (MEF), Metro Ethernet provides scalable, flexible, and cost-effective Layer 2 connectivity services compared to traditional WAN technologies such as Frame Relay and ATM (Autenrieth et al., 2006; Rathore, 2012).

Raisecom

Raisecom is a Chinese networking and telecommunications solutions provider known for manufacturing Carrier Ethernet, optical transport, and access network equipment. Raisecom products are widely used by telecommunications operators, Internet Service Providers (ISPs), and government institutions because they support various networking standards and protocols, including IEEE 802.1ag, ITU-T Y.1731, and MPLS (Glamočanin, 2017; Vaez-Ghaemi, 2007).

Technical documentation regarding Raisecom in academic and regulatory environments in Indonesia remains relatively limited. This makes Raisecom equipment an important subject for further research, particularly in evaluating Y.1731-based network performance in the public sector. Raisecom was selected as the subject of this study because it is widely deployed

in local government Metro Ethernet infrastructure projects, yet its OAM features have not been comprehensively evaluated in terms of their effectiveness in ensuring SLA compliance and network performance monitoring (Glamočanin, 2017).

Quality of Service (QoS)

Quality of Service (QoS) is a network management mechanism that plays a crucial role in optimizing data service quality through the control of various network parameters, including bandwidth, latency, jitter, and packet loss. As modern networks become increasingly complex and support diverse traffic types, ranging from standard data services to real-time applications such as video streaming and Voice over IP (VoIP), the implementation of QoS becomes increasingly essential (Nugroho, 2020; Business Research Insights, 2024).

QoS was selected as a subject of study because of its ability to ensure reliable and measurable network performance, as well as its relevance in supporting increasingly critical digital communication requirements in the era of government and industrial digital transformation. By examining QoS, it is possible to understand how this technology supports innovation and responds to growing communication demands while maintaining network efficiency and effectiveness in service delivery (Government of the Republic of Indonesia, 2018).

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a dynamic routing protocol used to determine the best path within IP networks. As a link-state protocol, OSPF collects information about the status of all network links and builds a topology database. Each router distributes this information through Link State Advertisements (LSAs), enabling all routers to maintain a comprehensive understanding of the network topology. OSPF supports network segmentation into areas to reduce complexity and improve efficiency, with Area 0 (the backbone area) serving as the core. The protocol also provides fast convergence, allowing routing tables to be updated quickly when topology changes occur. OSPF uses a cost metric based on link bandwidth to determine the optimal path (Lucena et al., 2009).

The OSPF process begins with neighbor discovery through the exchange of Hello packets, which establish neighbor relationships among routers. Once adjacency is formed, routers exchange LSAs containing information about link status. Each router then builds and maintains a Link State Database (LSDB) based on the received LSAs. Using the Dijkstra algorithm, routers calculate the shortest path to every destination within the network. After determining the best routes, routers update their routing tables accordingly. OSPF is widely implemented in large and complex networks because of its ability to manage routing efficiently and rapidly (Lucena et al., 2009).

In addition, OSPF provides message authentication mechanisms to ensure that only authorized routers participate in the routing process. With its capability to manage large-scale and complex network infrastructures, OSPF has become a preferred routing protocol for many organizations. Its reliability and efficiency make it one of the most widely used routing protocols worldwide (Lucena et al., 2009).

Internet Protocol

Internet Protocol (IP) is the primary protocol used to transmit data across computer networks, including the Internet. IP is responsible for addressing and delivering data packets from a source to a destination. Two major versions of IP are currently in use: IPv4 and IPv6. IPv4 utilizes 32-bit addresses, allowing approximately 4.3 billion unique addresses, whereas IPv6 uses 128-bit addresses, providing an almost unlimited address space and overcoming the limitations of IPv4 (Lucena et al., 2009).

IP operates by dividing data into smaller packets that are transmitted through the network. Each packet contains addressing information, including source and destination IP addresses, along with additional control information. The protocol itself does not guarantee packet delivery, which is why it is commonly used in conjunction with other protocols such as the Transmission Control Protocol (TCP) to ensure reliable communication. IP also supports various addressing methods, including unicast (one-to-one), multicast (one-to-many), and broadcast (one-to-all). Its ability to interconnect devices globally makes IP the foundation of modern data communications (Lucena et al., 2009).

One important feature of IP is hierarchical addressing, which allows addresses to be grouped into subnets. This capability facilitates network management and reduces routing table sizes, thereby improving routing efficiency. In IPv4, subnet masks are used to distinguish the network portion of an address from the host portion (Lucena et al., 2009).

The protocol also supports fragmentation, enabling large packets to be divided into smaller segments for transmission across networks with maximum packet size limitations. Furthermore, IP includes mechanisms for error handling, such as the Time to Live (TTL) field, which prevents packets from circulating indefinitely within the network (Lucena et al., 2009).

Tunnel Infrastructure

The information above indicates that the term tunnel literally refers to a passageway. In networking, as described in Cisco documentation, a tunnel functions as a private communication path between devices. As a result, devices appear to be directly connected, even though they are physically connected through a WAN and multiple intermediate routers. As long as the public IP addresses of both devices are reachable, a tunnel interface can be established. Consequently, a tunnel network enables the connected devices to communicate as though they are directly linked, as illustrated in Figure 2.8, which connects an office network and a user network (Ferrari & Christen, 2010).

Maintenance Domain

A Maintenance Domain (MD) is a distinct area within a network that provides connectivity fault detection capabilities. The boundaries of an MD are defined by Maintenance End Points (MEPs) configured on network interfaces. Each MD is identified by a unique MD name (Juniper Networks, 2025).

To facilitate fault tracking, MDs are organized into hierarchical levels ranging from 0 to 7. The higher the level value, the broader the coverage of the MD. An MD may be tangential to or nested within another MD, but overlapping domains are not permitted. Lower-level MDs may exist within higher-level MDs, whereas the reverse arrangement is not allowed (Minei et al., 2016).

This level-based classification assists in fault diagnosis. For example, as illustrated in Figure 5-89, MD2 is nested within MD1. If a fault is detected in MD1, the issue can be inferred to exist between devices PE2 and PE6 or on the links connecting them. If no fault is detected in MD2, it can be concluded that PE2, PE3, and PE4 are functioning correctly, suggesting that the fault is likely located at PE5, PE6, PE7, or their associated links (Lee et al., 2018).

In practical network deployments, a nested MD can monitor the connectivity of a higher-level MD. Level assignments allow IEEE 802.1ag packets to traverse nested domains. In the example shown in Figure 5-89, MD2 is nested within MD1, and MD1's IEEE 802.1ag packets must be able to pass through MD2. Therefore, MD1 is configured at level 6, while MD2 is configured at level 3 (Juniper Networks, 2025).

With this configuration, IEEE 802.1ag packets used to monitor MD1 connectivity can traverse MD2, whereas packets used for monitoring MD2 remain confined within that domain. Appropriate level assignment facilitates layered fault isolation and accelerates fault localization processes (Ventre et al., 2019).

Maintenance Association End Point

In practical network implementations, a Maintenance Domain (MD) that is nested within another MD can monitor the connectivity of a higher-level MD. Level assignments allow IEEE 802.1ag packets to traverse nested MDs. In the example shown in Figure 5-89, MD2 is nested within MD1, and IEEE 802.1ag packets belonging to MD1 must be able to pass through MD2. Therefore, MD1 is configured with level 6, while MD2 is configured with level 3. With this configuration, IEEE 802.1ag packets used to monitor MD1 connectivity can pass through MD2, while IEEE 802.1ag packets used to monitor MD2 connectivity are prevented from propagating into MD1. Proper level assignment facilitates layered fault isolation and accelerates fault localization processes (Minei et al., 2016).

Maintenance Intermediate Points (MIPs) are calculated separately for each service instance (for example, a VLAN). Within a service instance, MDs with different levels may be configured together with a Maintenance Association (MA). These MAs share the same VLAN ID but differ in their assigned levels. For each service instance on an interface, the device attempts to create a MIP from the lowest-level MEP according to the rules defined in Table 5-22 and the associated configuration requirements (Juniper Networks, 2025).

Each MD on an interface is assigned a specific level and is associated with several MIP creation rules. The rule with the highest priority is applied, where explicit rules take precedence over default rules. The MIP level must always be higher than the level of any MEP configured on the same interface (Juniper Networks, 2025).

Explicit rules apply only to interfaces where MEPs have been configured. Only one MIP can be created on a single interface. If multiple eligible MIPs with different levels satisfy the requirements, the MIP with the lowest level is selected and created (Minei et al., 2016). A well-designed MIP creation policy simplifies fault detection and fault tracing processes based on hierarchy levels. This is because MEPs within lower-level MDs can be mapped to MIPs within higher-level MDs (Lee et al., 2018). For example, if a fault occurs within a level-7 MD, it can be detected using Continuity Check Messages (CCMs). Subsequently, loopback or linktrace functions can be employed to locate the fault, which may be found between two MIPs. This result suggests that the fault may exist within a level-5 MD. The process can then be repeated until the specific link or device causing the problem is identified (Lee et al., 2018; Ventre et al., 2019).

IP-layer mechanisms such as Simple Network Management Protocol (SNMP), IP ping, and IP traceroute are commonly used to manage network services, detect faults, and monitor performance in traditional Ethernet networks. However, these mechanisms are not suitable for end-to-end (E2E) operations and management at the client layer within Ethernet networks (Hofstede et al., 2008).

Networks are logically divided into Maintenance Domains (MDs). For example, network devices managed by a single Internet Service Provider (ISP) may be grouped into one MD to distinguish the ISP network from customer networks. Two Maintenance Association End Points (MEPs) are configured at both ends of the network segment being managed to define the boundaries of the MD (Juniper Networks, 2025). Maintenance Association Intermediate Points (MIPs) can be configured as needed. During testing procedures, a MEP sends a test request, and either a Remote MEP (RMEP) or a MIP responds. This process provides information about the managed network segment and facilitates fault detection (Ryoo et al., 2008).

Connectivity Fault Management (CFM) also supports level-specific management of MDs. An MD at a particular level can manage lower-level MDs but cannot manage higher-level MDs. This concept is used to maintain service flows according to MD hierarchy levels and to manage multiple service flows within a single MD (Minei et al., 2016). An MEP generates and transmits Continuity Check Messages (CCMs). In the network example shown in Figure 5-98, MEP1, MEP2, and MEP3 belong to the same Maintenance Association (MA). Once CCM transmission is enabled, MEP1 periodically multicasts CCMs to MEP2 and MEP3. Similarly, MEP2 sends CCMs to MEP1 and MEP3 at the same interval, and MEP3 sends CCMs to MEP1 and MEP2 at the same interval (Cisco Systems, 2018; Ryoo et al., 2008). Every device supporting Ethernet Connectivity Fault Management (CFM) maintains a MEP database. This database records information regarding local MEPs and Remote MEPs (RMEPs) that belong to the same MA. Local MEPs and RMEPs are manually configured, and their information is automatically stored in the MEP database (Juniper Networks, 2025).

If a MEP does not receive CCMs from its corresponding RMEP within three consecutive CCM transmission intervals, it assumes that the path between itself and the RMEP has failed. In such cases, the system generates a log report. To locate the fault, loopback or linktrace functions may be used. MEPs within the same MD can also transmit CCMs to monitor link connectivity in a multipoint-to-multipoint (MP2MP) environment (Ryoo et al., 2008; Lee et al., 2018). CCMs are generated and terminated by MEPs. If a MEP receives a CCM with a higher level than its own, it forwards the CCM. Conversely, if the received CCM has the same or lower level, it is not forwarded. This mechanism prevents CCMs originating from lower-level MDs from propagating into higher-level MDs (Minei et al., 2016).

Huawei

Huawei Technologies Co., Ltd. is a Chinese multinational technology company founded in 1987 and headquartered in Shenzhen, Guangdong Province, China. Huawei initially focused on the production and distribution of Private Branch Exchange (PBX) systems for the domestic market but later evolved into one of the world's largest providers of telecommunications infrastructure and information technology solutions (Glamočanin, 2017).

In the networking sector, Huawei offers a comprehensive portfolio that includes Metro Ethernet equipment, Optical Transport Networks (OTN), IP/MPLS routers, switching solutions, and Operations, Administration, and Maintenance (OAM) technologies, including the implementation of the ITU-T Y.1731 standard for network performance monitoring. Huawei products are frequently utilized in simulation laboratories, such as eNSP and PNetLab, as well as in real-world deployments because they support advanced network

management features, including Ethernet Connectivity Fault Management (CFM), Performance Monitoring, and Fault Management (Gomes et al., 2018; Glamočanin, 2017).

Huawei also plays an active role in the development of international standards through its participation in standardization organizations such as ITU-T, 3GPP, and IEEE. As a result, many Huawei products adopt protocols and methodologies that are fully compatible with global standards (Gomes et al., 2018).

3. Materials and Method

Research Data

In this study, the required data were obtained through a series of tests conducted in a virtual laboratory environment. The researcher built a simulation laboratory using the Professional Network Emulator Tool Lab (PNET Lab). The type of research applied was quantitative experimental research with a technical simulation-based approach. This approach was selected to enable controlled testing and realistic replication of Metro Ethernet network conditions.

This research was specifically designed to evaluate the effectiveness of bandwidth management using the ITU-T Y.1731 protocol based on Ethernet OAM (Operations, Administration, and Maintenance) on Raisecom devices. Within the PNET-Lab simulation environment, Raisecom devices were represented by virtual devices with similar capabilities, such as Cisco routers, which support Ethernet OAM features and the Y.1731 protocol.

Methodology Implementation

The methodology in this study was implemented through a network simulation experiment using an Emulated Virtual Environment (PNET Lab). Systematic, measurable, and repeatable procedures were designed to ensure the validity of the collected data and testing results.

The implementation of this methodology enabled direct measurement of the impact of the Y.1731 protocol on service quality and bandwidth optimization in Metro Ethernet networks. It also validated the capability of Raisecom devices to effectively implement Ethernet OAM and Y.1731 features. The data and findings obtained serve as a strong foundation for technical and contractual recommendations aimed at strengthening regulations for public digital infrastructure management and ensuring objective verification of service quality standards.

Problem Statement

The primary issue addressed in this research is the limited implementation of network performance monitoring standards in Metro Ethernet infrastructures, particularly on devices used by public service providers such as Raisecom. Although these devices support the ITU-T Y.1731 protocol as part of Ethernet OAM, in practice, these features are often not activated or optimally utilized. As a result, there is a lack of objective data for performance evaluation and Service Level Agreement (SLA) enforcement.

Topology Analysis

The network topology used in this study was designed to represent the operational conditions of Metro Ethernet networks in government institutions or public service providers, with the primary objective of evaluating the effectiveness of the ITU-T Y.1731 protocol in monitoring and optimizing network performance.

The topology consists of four Layer 3 router devices (CE1 Router and CE2 Router) that function as network endpoints. These routers are configured with Ethernet OAM features and support the Y.1731 protocol for performance measurement.

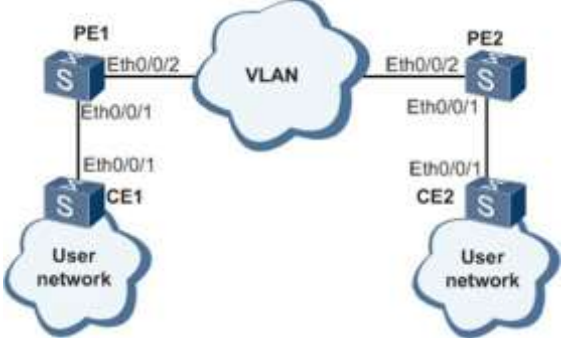

Figure 1. Test Design.

This topology illustrates the basic structure of a computer network in which devices are interconnected using dynamic routing, enabling CE1 Router and CE2 Router to efficiently send and receive data to and from routers and computers within the network.

Underlay Configuration

At this stage, the researcher performed the Underlay Configuration, which represents the initial phase in building a Metro Ethernet network and serves as the communication foundation among network devices. This stage involved configuring basic Layer 2 and Layer 3 connectivity to ensure that all devices within the topology could communicate reliably before the implementation of the Y.1731 protocol.

In the underlay configuration, the researcher utilized OSPF (Open Shortest Path First) dynamic routing, a widely used and open-standard routing protocol. The VLAN protocol was selected due to its capability to support rapid network convergence as well as multi-area and large-scale topologies, which are commonly deployed in Metro Ethernet networks.

VLAN configuration was implemented on each router (Router A and Router B) to interconnect devices through Internet Protocol Version 4 (IPv4) paths. OSPF was used to automatically establish routing tables and serve as the primary communication path between network nodes before activating OAM (Operations, Administration, and Maintenance) features.

In this study, the Y.1731 protocol operates over IPv4 paths configured through VLANs. Therefore, validating the success of the underlay configuration is critical because OAM features such as ETH-DM and ETH-LM cannot function optimally if the underlay network is not operational. Once all verification procedures are successfully completed, the underlay network is considered stable and ready for the activation and configuration of the ITU-T Y.1731 protocol as part of the network performance monitoring system.

Y.1731 Protocol Configuration

After successfully implementing the underlay configuration using the OSPF protocol, the next stage involved implementing the ITU-T Y.1731 protocol as part of the Ethernet OAM (Operations, Administration, and Maintenance) mechanism. This protocol plays a crucial role in monitoring and measuring network performance in real time, particularly in terms of delay, jitter, packet loss, and availability.

In this study, the protocol configuration was performed on Huawei simulation devices using the Command Line Interface (CLI) within the PNET-Lab platform. These devices were selected based on their support for Ethernet OAM and compliance with industry standards such as IEEE 802.1ag for Connectivity Fault Management and ITU-T Y.1731 for Performance Monitoring. All testing was conducted within a virtual network environment while simulating realistic conditions of Metro Ethernet infrastructures commonly used by public service providers.

4. Results and Discussion

Implementation and Testing

Referring to Chapter III, the implementation and testing stage falls within the Underlay Configuration phase. As discussed in Chapter III, the topology used in this study requires VLAN configuration between Router 1 and Router 2 as Provider Edge (PE) routers, and Router 3 and Router 4 as Customer Edge (CE) routers. Each router is interconnected through VLAN trunk links to ensure connectivity and communication among devices.

The following topology design is used in this study. The initial step involves establishing the underlay network using VLANs. Therefore, the configuration process focuses on the connectivity between PE routers and CE routers.

Implementation of One-Way Frame Delay Measurement in a VLAN

```
<Quidway> system-view
[Quidway] sysname CE1
[CE1] vlan 2
[CE1-vlan2] quit
[CE1] interface ethernet 0/0/1
[CE1-Ethernet0/0/1] port link-type trunk
[CE1-Ethernet0/0/1] port trunk allow-pass vlan 2
[CE1-Ethernet0/0/1] quit
```

Figure 2. CE1 VLAN Configuration.

The VLAN configuration on CE1 begins by entering system-view mode and changing the device name to CE1. Next, VLAN 2 is created, and the configuration exits VLAN mode. Subsequently, Ethernet interface 0/0/1 is configured as a trunk port and permitted to carry VLAN 2 traffic before returning to the previous configuration mode.

```
<Quidway> system-view
[Quidway] sysname CE2
[CE2] vlan 2
[CE2-vlan2] quit
[CE2] interface ethernet 0/0/1
[CE2-Ethernet0/0/1]port link-type trunk
[CE2-Ethernet0/0/1]port trunk allow-pass vlan 2
[CE2-Ethernet0/0/1]quit
```

Figure 3. CE2 VLAN Configuration.

The VLAN configuration on CE2 starts by entering system-view mode and changing the device name to CE2. Afterward, VLAN 2 is created and the configuration exits VLAN mode. Then, Ethernet interface 0/0/1 is configured as a trunk port and allowed to pass VLAN 2 traffic before returning to the previous configuration mode.

```
<Quidway> system-view
[Quidway] sysname PE1
[PE1] vlan 2
[PE1-vlan2] quit
[PE1] interface ethernet 0/0/1
[PE1-Ethernet0/0/1] port link-type trunk
[PE1-Ethernet0/0/1] port trunk allow-pass vlan 2
[PE1-Ethernet0/0/1] quit
[PE1] interface ethernet 0/0/2
[PE1-Ethernet0/0/2] port link-type trunk
[PE1-Ethernet0/0/2] port trunk allow-pass vlan 2
[PE1-Ethernet0/0/2] quit
```

Figure 4. PE1 VLAN Configuration.

The VLAN configuration on PE1 is performed by entering system-view mode and renaming the device to PE1. After creating VLAN 2 and exiting VLAN configuration mode, Ethernet interface 0/0/1 is configured as a trunk port and permitted to carry VLAN 2 traffic. The same procedure is applied to Ethernet interface 0/0/2 by setting the link type to trunk and allowing VLAN 2 traffic before returning to the previous configuration mode.

```
<Quidway> system-view
[Quidway] sysname PE2
[PE2] vlan 2
[PE2-vlan2] quit
[PE2] interface ethernet 0/0/1
[PE2-Ethernet0/0/1] port link-type trunk
[PE2-Ethernet0/0/1] port trunk allow-pass vlan 2
[PE2-Ethernet0/0/1] quit
[PE2] interface ethernet 0/0/2
[PE2-Ethernet0/0/2] port link-type trunk
[PE2-Ethernet0/0/2] port trunk allow-pass vlan 2
[PE2-Ethernet0/0/2] quit
```

Figure 5. PE2 VLAN Configuration.

The VLAN configuration on PE2 begins by entering system-view mode and renaming the device to PE2. After creating VLAN 2 and exiting VLAN configuration mode, Ethernet interface 0/0/1 is configured as a trunk port with permission to carry VLAN 2 traffic. The same procedure is performed on Ethernet interface 0/0/2 by changing the link type to trunk and allowing VLAN 2 traffic before returning to the previous configuration mode.

```
[CE1] cfm enable
[CE1] cfm version standard
[CE1] cfm md md3
[CE1-md-md3] ma ma3
[CE1-md-md3-ma-ma3] map vlan 2
[CE1-md-md3-ma-ma3] mep mep-id 3 interface ethernet 0/0/1 outward
[CE1-md-md3-ma-ma3] mep ccm-send mep-id 3 enable
[CE1-md-md3-ma-ma3] remote-mep mep-id 4
[CE1-md-md3-ma-ma3] remote-mep ccm-receive mep-id 4 enable
[CE1-md-md3-ma-ma3] quit
[CE1-md-md3] quit
```

Figure 6. CE1 CFM Configuration.

The basic Ethernet CFM function configuration on CE1 begins by enabling CFM and specifying its version according to the IEEE 802.1ag-2007 standard. Next, a Maintenance Domain (MD) named md3 is created, followed by the creation of a Maintenance Association (MA) named ma3 mapped to VLAN 2. Subsequently, a Maintenance End Point (MEP) with ID 3 is configured on Ethernet interface 0/0/1 with an outward direction. CCM transmission is enabled for this MEP, and a remote MEP with ID 4 is configured with CCM reception enabled.

```
[CE2] cfm enable
[CE2] cfm version standard
[CE2] cfm md md3
[CE2-md-md3] ma ma3
[CE2-md-md3-ma-ma3] map vlan 2
[CE2-md-md3-ma-ma3] mep mep-id 4 interface ethernet 0/0/1 outward
[CE2-md-md3-ma-ma3] mep ccm-send mep-id 4 enable
[CE2-md-md3-ma-ma3] remote-mep mep-id 3
[CE2-md-md3-ma-ma3] remote-mep ccm-receive mep-id 3 enable
[CE2-md-md3-ma-ma3] quit
[CE2-md-md3] quit
```

Figure 7. CE2 CFM Configuration.

The Ethernet CFM basic function configuration on CE2 is performed by enabling CFM and setting its version according to the IEEE 802.1ag-2007 standard. Afterward, a Maintenance Domain (MD) named md3 is created, within which a Maintenance Association (MA) named ma3 is established and mapped to VLAN 2. A MEP with ID 4 is then configured on Ethernet interface 0/0/1 with an outward direction. CCM transmission is enabled for this MEP, and a remote MEP with ID 3 is configured with CCM reception enabled. After completing the configuration, the system exits MA and MD configuration modes.

```
[CE2] cfm md md3
[CE2-md-md3] ma ma3
[CE2-md-md3-ma-ma3] delay-measure one-way receive
[CE2-md-md3-ma-ma3] quit
[CE2-md-md3] quit
```

Figure 8. CE2 One-Way DM Configuration.

On CE2, the configuration is performed to enable the device to receive Delay Measurement (DM) frames. This process begins by entering the Maintenance Domain md3, accessing Maintenance Association ma3, and enabling the one-way delay measurement reception function. Afterward, the system exits both the MA and MD configuration modes.

```
[CE1] cfm md md3
[CE1-md-md3] ma ma3
[CE1-md-md3-ma-ma3] delay-measure one-way remote-mep mep-id 4 interval 10000 count 20
[CE1-md-md3-ma-ma3] quit
[CE1-md-md3] quit
```

Figure 9. CE1 One-Way DM Configuration.

On CE1, this configuration aims to enable one-way frame delay measurement. The process begins by entering Maintenance Domain md3, followed by Maintenance Association ma3. A one-way delay measurement toward the remote MEP with ID 4 is then configured

using an interval of 10,000 microseconds and a total of 20 measurement iterations. After completing the configuration, the system exits the MA and MD configuration modes.

```
<CE2> display y1731 statistic-type oneway-delay md md3 ma ma3
Latest one-way delay statistics:
--------------------------------------------------------------------------------
Index    Delay(usec)    Delay variation(usec)
--------------------------------------------------------------------------------
    1          10000                      -
    2          10000                      0
    3          10000                      0
    4          10000                      0
    5          10000                      0
    6          10000                      0
    7          10000                      0
    8          10000                      0
    9          10000                      0
   10          10000                      0
   11          10000                      0
   12          40000                  30000
   13          10000                  30000
   14          10000                      0
   15          10000                      0
   16          10000                      0
   17          10000                      0
--------------------------------------------------------------------------------
Average delay(usec) :      11764    Average delay variation(usec) :       3750
Maximum delay(usec) :      40000    Maximum delay variation(usec) :      30000
Minimum delay(usec) :      10000    Minimum delay variation(usec) :          0
```

Figure 10. One-Way Delay Statistics Results.

This command displays one-way delay measurement statistics between connected MEPs. The results present a list of measurement indexes, delay values in microseconds, and delay variations for each test. Based on the collected data, the average delay was recorded at 11,764 μs with an average variation of 3,750 μs. The maximum delay reached 40,000 μs with a maximum variation of 30,000 μs, while the minimum delay was 10,000 μs with a variation of 0 μs, indicating stable connectivity in most measurements but revealing one anomaly with significantly higher delay.

Implementation of Two-Way Frame Delay Measurement in a VLAN

In the next stage of this laboratory session, the focus shifts to testing and implementing a Two-Way Frame Delay Measurement configuration within a VLAN environment. This step aims to provide a deeper understanding of bidirectional traffic delay measurement methods, enabling more accurate network performance monitoring and service quality evaluation.

The configuration plan followed in this stage involves establishing an on-demand two-way frame delay measurement on the end-to-end connection path between the two CE devices. This configuration is intended to periodically collect statistical data regarding frame transmission delays, providing a clearer representation of network transmission performance.

Enter system-view mode on the Huawei device and change the system name to CE1. Next, create VLAN 2 and exit VLAN configuration mode. Access Ethernet interface 0/0/1, configure the link type as trunk, and allow VLAN 2 traffic to pass through the link. Finally, exit interface configuration mode.

Enter system-view mode on the Huawei device and assign the system name CE2. Then, create VLAN 2 and exit VLAN configuration mode. Access Ethernet interface 0/0/1, change the link type to trunk, and permit VLAN 2 traffic on the link. Finally, exit interface configuration mode.

Access system-view mode on the Quidway device and change the system name to PE1. Then, create VLAN 2 and exit VLAN configuration mode. Enter Ethernet interface 0/0/1, configure the link type as trunk, and allow VLAN 2 traffic on the link before exiting interface configuration mode. Repeat the same process on Ethernet interface 0/0/2 by configuring it as a trunk port and allowing VLAN 2 traffic, then exit interface configuration mode.

Enter system-view mode on the Quidway device and change the system name to PE2. Then, create VLAN 2 and exit VLAN configuration mode. Access Ethernet interface 0/0/1, configure the link type as trunk, and allow VLAN 2 traffic before exiting interface configuration mode. Repeat the same procedure on Ethernet interface 0/0/2 by configuring it as a trunk port and allowing VLAN 2 traffic, then exit interface configuration mode.

Enable the CFM feature on CE1 and specify its version according to the IEEE 802.1ag-2007 standard. Create a Maintenance Domain (MD) named md3, and within it create a Maintenance Association (MA) named ma3. Bind the MA to VLAN 2. Then, configure a MEP with ID 3 on Ethernet interface 0/0/1 in the outward direction and enable CCM transmission for this MEP. Add a remote MEP with ID 4 and enable CCM reception from that remote MEP. After all steps are completed, exit the MA and MD configuration modes.

Enable the CFM function on CE2 and set its version according to the IEEE 802.1ag-2007 standard. Create a Maintenance Domain (MD) named md3, and within it create a Maintenance Association (MA) named ma3. Associate the MA with VLAN 2. Then, configure a MEP with ID 4 on Ethernet interface 0/0/1 in the outward direction and enable CCM transmission from this MEP. Next, configure a remote MEP with ID 3 and enable CCM reception from that remote MEP. Finally, exit the MA and MD configuration modes after completing all settings.

On CE2, enter Maintenance Domain (md3) and Maintenance Association (ma3). Configure the device to receive two-way delay measurement frames (DMM) for bidirectional delay measurement. Afterward, exit the MA and MD configuration modes.

On CE1, enter Maintenance Domain (md3) and Maintenance Association (ma3). Configure a two-way frame delay measurement targeting the remote MEP with ID 4, using a measurement interval of 10,000 ms and a total of 20 repetitions. After completing the configuration, exit the MA mode and return to the MD mode.

After completing all configurations, execute the command display y1731 statistic-type twoway-delay md md3 ma ma3 on CE1 to display the bidirectional frame delay measurement results. The generated output presents a table containing measurement indexes, delay values in microseconds, and delay variations for each measurement. Additionally, statistical information including average, maximum, and minimum values for both delay and delay variation is displayed, facilitating a comprehensive analysis of transmission quality along the tested path.

5. Conclusion and Suggestion

Conclusion

Based on the series of research stages conducted, including the design of testing scenarios, device configuration, data collection, and result analysis, it can be concluded that the implementation of the ITU-T Y.1731 method based on Ethernet Operations, Administration, and Maintenance (OAM) on Raisecom devices within a Metro Ethernet network significantly improves bandwidth management by minimizing delay variation, controlling jitter, and reducing frame loss rates along transmission paths. Through One-Way Frame Delay Measurement and Two-Way Delay Measurement testing, empirical evidence was obtained demonstrating that the system provides precise measurement performance. The observation results indicate stable average delay values and jitter fluctuations that remain within the acceptable tolerance limits of Carrier Ethernet service standards.

The measurement data indicate that the Y.1731 method is not only effective as a network performance monitoring tool but also plays a strategic role in fine-tuning bandwidth allocation according to service requirements and Service Level Agreements (SLAs). This study further demonstrates that the implementation of Y.1731 on Raisecom devices can be efficiently integrated into complex Metro Ethernet network topologies without disrupting primary network operations, while also providing real-time monitoring capabilities that assist network operators in the early detection of potential service quality degradation.

From a practical perspective, these findings reinforce the relevance of implementing the Y.1731 standard in supporting service quality sustainability within carrier-grade network infrastructures, particularly amid the increasing demand for Quality of Service (QoS) in today's data-intensive digital era. This research also opens opportunities for further studies related to the optimization of other OAM methods, testing on larger-scale network environments, and integration with Software-Defined Networking (SDN)-based network management mechanisms to develop more adaptive and automated performance management systems.

Therefore, it can be firmly concluded that the Y.1731 method based on Ethernet OAM represents a feasible and effective technical solution for improving bandwidth utilization efficiency while maintaining consistent service quality in modern Metro Ethernet networks.

Suggestion

Based on the research findings and analysis conducted, the author proposes several recommendations that may serve as considerations for network practitioners, future researchers, and service providers: a) For network operators, it is recommended to continuously integrate the Y.1731 method into Metro Ethernet infrastructures, particularly on high-traffic transmission paths, to enable proactive performance monitoring and responsive bandwidth management according to changing network conditions. b) Further testing should be conducted over longer observation periods and with a wider variety of traffic scenarios, including peak-hour conditions and synthetic fault injection, to obtain a more comprehensive understanding of network performance characteristics. c) To maximize the potential of Y.1731, it is recommended to combine its implementation with Software-Defined Networking (SDN) or Network Function Virtualization (NFV)-based network management systems, enabling automated and dynamic bandwidth allocation and optimization. d) Future researchers are encouraged to expand the scope of study to include different network devices and vendors, as well as interoperability testing among heterogeneous devices, in order to strengthen the validity and generalizability of the research findings. By implementing these recommendations, it is expected that Quality of Service (QoS) management in Metro Ethernet networks can become more efficient, adaptive, and capable of addressing the continuously growing demands for high-quality data communication services.

References

Autenrieth, A., Kirstädter, A., & Edmaier, B. (2006). Carrier grade metro Ethernet networks.

Bidkar, S., Gumaste, A., Ghodasara, P., & Kushwaha, A. (2015). Scalable segment routing: A new paradigm for efficient service provider networking using carrier Ethernet advances. https://doi.org/10.1364/JOCN.7.000445

Bidkar, S., Gumaste, A., Ghodasara, P., & Kushwaha, A. (2017). Field trial of a software defined network (SDN) using carrier Ethernet and segment routing in a tier-1 provider. https://doi.org/10.1364/JOCN.9.000711

Bidkar, S., Gumaste, A., Ghodasara, P., et al. (2008). Field trial SDN with carrier Ethernet & segment routing. https://doi.org/10.1109/ANTS.2008.4937766

Business Research Insights. (2024). Metro Ethernet services market size, share, trends, and growth forecast. https://www.businessresearchinsights.com/market-reports/metro-ethernet-services-market-105345

Cisco Systems. (2018). Performance monitoring with CCM in Ethernet.

Credence Research. (2024). Metro Ethernet market size, share, trends analysis report 2024–2032. https://www.credenceresearch.com/report/metro-ethernet-market

Ferrari, G., & Christen, K. O. (2010). Carrier Ethernet for mobile backhaul. https://doi.org/10.1109/MCOM.2010.5594682

Glamočanin, D. (2017). Migration to next gen optical carrier Ethernet. https://doi.org/10.1088/1757-899X/200/1/012028

Gomes, N. J., Jäntti, R., Kämäräinen, J., & Perälä, P. (2018). Boosting 5G through Ethernet: How evolved fronthaul can take next-generation mobile to the next level. https://doi.org/10.1109/MVEH.2018.8200834

Hofstede, A., Drago, M., Moura, G., & Pras, A. (2008). Carrier Ethernet OAM: An overview and comparison to IP OAM. https://doi.org/10.1109/ANTS.2008.4937766

Indukuri, N. (2011). Pseudowire VCCV-BFD vs Ethernet OAM. https://doi.org/10.1007/978-3-642-21484-4_14

Jahanshahi, M., & Bistouni, F. (2019). Reliability-aware ring protection link selection in Ethernet ring mesh networks. https://doi.org/10.1016/j.ress.2019.106575

Juniper Networks. (2025). Ethernet OAM overview. https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/oam-service-overview.html

Lee, K. K., Ryoo, J. D., & Joo, B. S. (2018). Faultless protection methods in self-healing Ethernet ring networks. https://doi.org/10.4218/etrij.12.1812.0102

Lucena, A. A. B., Lindgren, A., & Nucciello, A. (2009). A survey of advanced Ethernet forwarding approaches. https://doi.org/10.1109/SURV.2009.090108

Minei, I., Strassner, J., & Pyda, A. (2016). Packet transport OAM. https://doi.org/10.1109/COMST.2016.2602412

Nugroho, A. (2020). Analisis quality of service (QoS) jaringan Metro Ethernet di Kota Samarinda. https://etd.repository.ugm.ac.id/penelitian/detail/181834

Pemerintah Republik Indonesia. (2018). Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). https://peraturan.bpk.go.id/Details/97880/perpres-no-95-tahun-2018

Rathore, V. (2012). The evolution of carrier Ethernet.

Ryoo, J. D., Song, J., & Park, J. H. (2008). OAM and its performance monitoring mechanisms for carrier Ethernet transport networks. https://doi.org/10.1109/MCOM.2008.4463778

Vaez-Ghaemi, R. (2007). Wireless backhaul for LTE: OAM considerations.

Ventre, P. L., Salsano, S., Polverini, M., & Cianfrani, A. (2019). OAM and segment routing for resilience. arXiv. https://arxiv.org/abs/1904.03471