# Performance Evaluation Between Network Communications Switches in a Substation

A Thesis
Presented in Partial Fulfillment of the Requirements for the
Degree of Master of Science
with a
Major in Computer Engineering
in the
College of Graduate Studies
University of Idaho
By
Rayan A. Alghamdi

Approved by
Major Professor: Brian K. Johnson, Ph.D.
Committee Members: Hangtian Lei, Ph.D.; Yacine Chakhchoukh, Ph.D.
Department Administrator: Joseph D. Law, Ph.D.

December 2021

# Abstract

Improving substation performance can be achieved by selecting a network design that enhances network reliability. Different network topologies can be executed for communication networks inside and outside of the substation based on standard power industry protocols, such as distributed network protocol version 3 (DNP3), Generic Object-Oriented Substation Event (GOOSE) messages, and Sampled Values (SV). Possible network topologies include star, ring bus, and others.

Each of these substation topologies contains multiple Ethernet switches to transmit a variety of traffic such as measurement data, commands, and engineering access between intelligent electronic device (IED) nodes and the central station. Field installations in substations use a mix of different topologies and a mix of different capabilities of switches such as managed switch, unmanaged switch, hub, and software defined network (SDN) switches. The various network topologies have different levels of performance, stability, and reliability. Similarly, the different types of switches each contribute different levels of performance, stability, and reliability for the substation networks.

GOOSE and SV messages are usually transferred via Ethernet frames, which contain measurement information or commands such as signaling a trip operation. In addition, both protocols pass through multiple Ethernet switches in normal operation. The Ethernet switch is an essential part of a network and plays a vital role in ensuring the connectivity of various devices. In addition, Ethernet switches often are designed according to the general requirements of various industries. Some of them are also customized depending on the environment and other factors.

This thesis will present a comparative analysis of the various types of Ethernet switches and their reliability and response times in transmitting GOOSE messages. This will help industrial facilities and students in university courses to understand the differences between the switches and make the right preparations for future substation network plans.

This thesis will observe and evaluate the performance of the substation networks with series and star topologies implemented with different types of Ethernet switches using network emulation software. It will compare the reliability of these topologies and switches inside a simulated substation with IED devices by transferring GOOSE messages to measure network speed, reliability, and performance. The simulation tool emulates a substation network that consists of six IEDs broadcasting GOOSE messages which are transmitted through two or three switches connected to a remote terminal unit, with different numbers of switches depending on the topology. This thesis demonstrates a communication network of substations for use in assignments or labs for classes and possibly for research projects.

# Acknowledgements

I would like to express my very great appreciation to Dr. Brian K. Johnson for his valuable guidance, constructive suggestions, wide knowledge, and gracious insight; he provided invaluable guidance, encouragement, and useful critiques during the planning and development of this research work. Dr. Johnson's commitment to education is admirable and his willingness to give his time so generously has been very much appreciated. I cannot really thank him enough for all the help and attention he provided me with during my studies at the University of Idaho.

Appreciation and acknowledgment are also due to the College of Engineering faculty members. Their assistance, vision, and illuminating discussions significantly improved this work. Thank you very much, I really appreciate it.

I would like to express my deep and extreme gratitude to my parents for their love, prayers, caring, and sacrifices for educating and preparing me for my future. To my mother, may Allah have mercy on you; thank you for everything and for your love, support, and caring. I cannot really thank you enough for all your help, sacrifice, and care that you provided me, and I am praying to Allah that we meet you in heaven. To my father, may Allah keep you safe and healthy. I cannot thank you enough for your prayers, love, and support during these rough times. I would not be here without your encouragement, advice, and backup.

Finally, to my special person, I would really like to thank my beautiful wife for all of her encouragement and for her love and constant support; I would have never gotten to this point without you. Thank you for being on my side during this hard time. I cannot thank you enough for your patience with all the trouble I made for you. You are my love, my rock, my muse, and my everything. I love you.

# Dedication

*Dedicated to my mother, have mercy on her soul, and my father, bless him. Dedicated especially to my beautiful wife Amal and my son Tayem; you are my heart, my soul, and everything. May Allah keep you safe and healthy. Let us enjoy the rest of our lives together.*

# Table of Contents

# List of Figures

# List of Tables

# List of Abbreviations

| | |
|---|---|
| ACL | Access Control List |
| API | Application Programming Interface |
| ARP | Address Resolution Protocol |
| BPF | Berkeley packet filter |
| CCNA | Cisco Certified Network Associate |
| Cisco | Computer Information System Company |
| CPU | Central Processing Unit |
| DoS/DDoS | Denial of Service/Distributed Denial of Service |
| DPI | Deep Packet Inspection |
| DHCP | Dynamic Host Configuration Protocol |
| DNP3 | Distributed Network Protocol 3 |
| DNS | Domain Name System |
| EMI | Electromagnetic Interference |
| EPS | Enhanced Polar System |
| ForCES | Forwarding and Control Element Separation |
| FTP | File Transfer Protocol |
| GW | Gateway |
| GARP | Generic Attribute Registration Protocol |
| GMRP | Generic Multicast Registration Protocol |
| GNS3 | Graphical Network Simulator 3 |
| gocbRef | GOOSE Object Reference |

| | |
|---|---|
| goID | GOOSE Identity |
| GOOSE | Generic Object-Oriented Substation Event |
| GUI | Graphical User Interface |
| GCKS | Group Control/Key Server |
| GSSE | Generic Substation State Events |
| HSR | High-availability Seamless Redundancy |
| HMAC | Hash Message Authentication Code |
| HMIs | Human-Machine Interfaces |
| HSRP | Hot Standby Router Protocol |
| VRRP | Virtual Router Redundancy Protocol |
| HTTP | Hypertext Transfer Protocol |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IED | Intelligent Electronic Device |
| IEEE | Institute of Electrical and Electronics Engineers |
| IHMI | Integrated Human Machine Interface |
| I&C | Instrumentation and Control |
| IOS | Cisco Internetwork Operating System |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| LANs | Local Access Networks |
| MAC | Media Access Control |

| | |
|---|---|
| MMS | Manufacturing Message Specification |
| Mbps | Megabits Per Second |
| MiM | Man In the Middle |
| MTBF | Mean Time Between Failures |
| MTTR | Mean Time To Repair |
| MU | Merging Unit |
| NCC | Network Control Center |
| NIDS | Network Intrusion Detection System |
| NIPS | Network Intrusion Prevention System |
| NOX | Network Operating System |
| OPNET | Optimized Network Engineering Tools |
| OSI | Open Systems Interconnection |
| P&C | Protection and Control |
| PRP | Parallel Redundancy Protocol |
| PC | Personal Computer |
| PDU | Protocol Data Unit |
| POF | Protocol Oblivious Forwarding |
| Q VLAN | Quality Virtual Local Access Controls |
| RSTP | Rapid Spanning Tree Protocol |
| REST | Representational State Transfer |
| RS232/RS485 | Recommended Standard 232/485 |
| RTU | Remote Terminal Unit |

| | |
|---|---|
| SCADA | Supervisory Control and Data Acquisition |
| SDN | Software-Defined Network |
| SEL | Schweitzer Engineering Laboratories |
| SNMP | Simple Network Management Protocol |
| sqNum | Sequence Number |
| stNum | State Number |
| STP | Spanning Tree Protocol |
| SAS | Substation Automation System |
| SCN | Substation Communication Network |
| SCL | Substation Configuration Language |
| SV | Sampled Value |
| SYN | Synchronize |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| UI | User Interface |
| VIRL | Virtual internet Routing Lab |
| VLANs | Virtual Local Access Network |
| VM | Virtual Machine |
| WAN | Wide Area Network |

# Chapter 1: Introduction and Objective

## 1.1 Background of the Communications Inside the Substation

Substations are high-voltage electric system facilities that transfer electric power between power generators, transmission lines, and distribution systems that supply loads. The reliability and performance of the power grid is enhanced through the use of communication within substations and between substations and the utility control center. The communications for electrical substation instrumentation and control (I & C) systems have configurable nodes that communicate over networks are constructed by using different network topologies, types of switches, communication protocols, and security schemes. Some of these configurable nodes are Intelligent Electronic Devices (IED) that communicate based on internet protocol (IP) models. An IED is a device that can take measurements, take control actions, or perform electrical protection tasks to isolate faults. IED functionality allows engineers to build substation networks with various topologies, switches, and links so that unexpected dynamic performance failures can be solved to maintain high degrees of reliability.

The common communications architecture goal for engineers in a substation network is to make reliability as high as possible. Improvement of the substation performance can be achieved by selecting a proper network design that enhances network reliability. The substation networks can communicate based on standard commercial protocols like Generic Object-Oriented Substation Event (GOOSE) messages [1], Distributed Network Protocol 3 (DNP3) [1], and Sampled Values (SV) [2] over network topologies such as star, ring, bus, etc. Each of these substation topologies contains Ethernet switches to transmit traffic flows with data from IED nodes to the central station and commands from local IEDs or from the control center. To increase reliability, performance, and stability of the substation network, network designers can evaluate the impact of using different types of switches such as hubs, unmanaged switches, managed switches, and Software-Defined Network (SDN) switches for performance comparison by analyzing the security effectiveness, packet droopiness, and message delivery timeliness [1].

Electric substations contain multiple pieces of equipment that are part of the supervision and control system; some examples are actuators such as circuit breakers, disconnect switches, grounding switches, tap changers, and IEDs such as meters, protective relays, and digital fault recorders. The list serves as a representation of the equipment inside a substation where timely information transfer is very important to its operation. Communication plays a crucial role in the operation of this electrical equipment. In the context of a power substation, getting the information transfer accurately and on time is critical.

An early system device that collected measurement data from devices in a substation to communicate them to the control center was a Remote Technical Unit (RTU). This device was typically connected to a utility's main supervisory control and data acquisition (SCADA) network and contained input and output physical hardware. These inputs and outputs were collected by RTUs to monitor and control various devices in the substation. RTUs also reported the status of the measured variables they monitored to system operators over a communication network. This functionality allows remote monitoring and control of electrical substations. This was an immense benefit to the industry, as it eliminated much of the need for manned electrical substations. The communication between the electric substation and the control room was more relevant for operator situational awareness. Thereby, the data collected by the various relays and instruments was reported to the station RTU at the time they asked for it.

In the early days of communication networks, the use of communication media in substations based on RS232 and RS485 was widespread. Today, most microprocessor relays still support these two media. However, industry field projects have started adopting Ethernet as their network technology based on standard network protocols. This transition had largely driven by the additional bandwidth and standardization that the network provided [2].

Communication schemes for industrial control systems applications, including those in substations, started with each vendor developing their own protocols specific to their equipment. The practice allowed individual vendors to lock customers into their products since they had limited interoperability with their competitor's products.

Modbus and DNP3 are presently the main communication protocols used in substations in North America. The Modbus protocol is a communication system that enables multiple entities to communicate with each other over a serial interface. It is commonly used for monitoring and controlling industrial machines. Modbus became a defacto standard due to its widespread use, and the eventually became a partially open standard to allow interoperability. However, many vendors added extensions to favor their equipment.

The DNP3 protocol is an open standard that enables serial communication lines to easily port to other devices. It evolved out of the development of the IEC 160870-5 but was released before the standard was completed. It has its own complex protocol stack that can be easily assembled [1].

Both Modbus and DNP3 can also be implemented over Ethernet. However, both protocols are complex to implement. This issue is solved by having a list of data from two devices connected to the same network that are different from one another and perform the same function. The complexity of integrating various devices into a monitoring and controlling system requires an experienced and skilled integrator with deep knowledge of both the hardware and the software devices. The speed and performance limitations of these protocols continued to leave room for vendors to implement their own proprietary protocols optimized to perform faster and more reliably on their hardware [1].

The desire for standardization in the protocols used in electrical substations to enable interoperability led to the emergence of the family of international standards under the umbrella of IEC 61850 [2]. IEC 61850 addresses the concerns of system operators when it comes to communicating between devices inside a substation at different levels and data rates, covering different operational niches. Its scope includes the addition of new protocols that allow real-time data exchange. Adoption of IEC 61850 is proceeding at different rates in different parts of the world.

The purpose of exchanging the data using real-time protocols over Ethernet is to improve data throughput and flexibility compared to using analog and serial connections between control devices and instruments. One of the real-time protocols under IEC 61850 is GOOSE messages broadcast over an Ethernet network. GOOSE messages are implemented by introducing an interface that allow the exchange of processed measurements, status indicators and commands in a high-speed fashion. For example, a GOOSE message can be sent to a circuit that initiates a trip operation. This method of signaling a trip operation is very similar to what was done using relay output contacts with added flexibility while being almost as fast. Another Ethernet-based protocol introduced in IEC 61850 is Sample Values (SV). This protocol allows the simultaneous multicast of current and voltage measurement values in the form of data frames. This multicast data can be used by multiple microprocessor relays, thus enabling different zones in the substation to execute their primary and backup protection functions without the need to connect physically to an instrument transformer.

GOOSE and SV messages can be transferred via Ethernet frames. The data packets for these protocols are transferred between protection and control devices within a substation via one or more Ethernet switches as shown in Figure 1. The GOOSE messages can also be transferred between different substations, sometimes hundreds of kilometers apart.

The Ethernet switch is an essential part of a network and plays a vital role in ensuring the connectivity of various devices. In addition, Ethernet switches often designed according to the requirements of various industries. Some of them are also customized depending on the substation environment and other operational factors. There are many types of Ethernet switches, and they all work in different ways. As will be shown in this thesis, analysis of the various types of Ethernet switches and the response times of their various functions in transmitting GOOSE messages would help students learn about industrial facilities in their classes and labs, understand their differences, and to learn what is coming in the development of future substation networks.

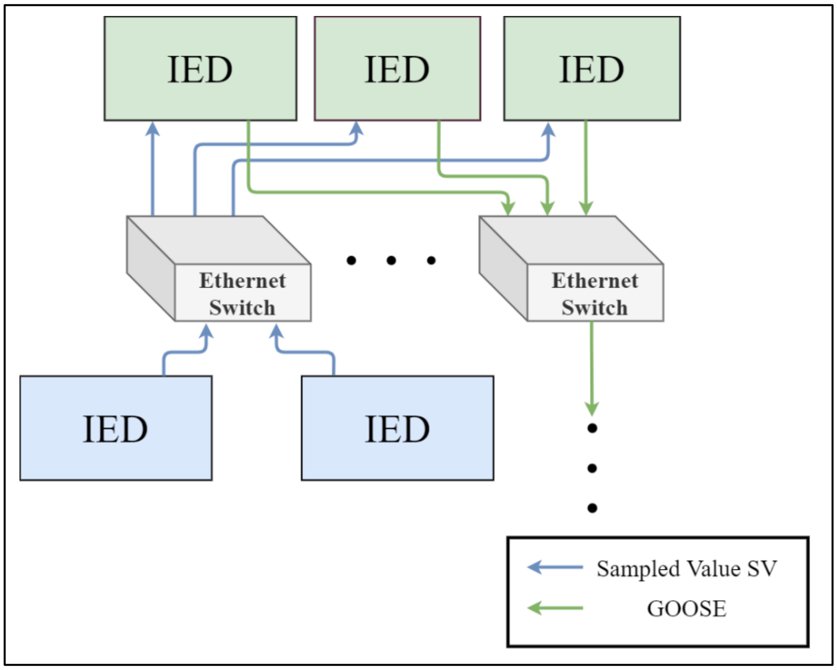


Figure 1. Simplified View of Substation Communication Connectivity

## 1.2 Thesis Objective

The objective of this thesis is to observe and document the performance of a substation network by using a variety of Ethernet switches in two topology illustrations (serial and star).

This work compares the reliability of Ethernet topologies and switches inside a substation that connect IEDs. The thesis analyzes a variety of switch types and network topologies by assessing their performance transferring GOOSE messages through the Ethernet switch in terms of the network speed, reliability, and performance. Networks based on these topologies and switches are used to meet the instrumentation and control (I&C) needs of a substation.

For this thesis, the author has simulated a substation network consisting of six IEDs that broadcast GOOSE messages through two or three switches connected to an RTU. Different network topologies and switch types are compared.

In this thesis, an advanced communication network of a substation to be used as a first step in classes will be designed in a network emulator. It is necessary to understand and document the process generating IEC 61850 GOOSE messages before determining and evaluating the expected network load performance metrics such as latency, average delivery time and the number of lost packets that could expected in such different network configurations. In addition, performance tests and analysis of results for transfer of GOOSE messages in each Ethernet switch type are recorded separately using network emulation software. The author hopes this work will serve as a valuable reference for study material for universities and labs to help students determine the reliability and performance of substation networks based on the topology and type of switch.

It is important for students to understand how to bring about the most effective design utilizing a given set of resources, such as links, switches, and devices that could apply to substations in the future to build a reliable, cyber-secure network architecture that will provide system stability for power system protection and control.

### 1.3 Summary

Electric substations have been using Ethernet networks for communications within substations and for SCADA communication with the control center to allow operators to monitor power and control voltage with better system awareness. To fully utilize the emerging IEC 61850 standard, network and communication engineers need specific knowledge about Ethernet networks such as switches, hops, and links in the context of real time operational technology networking. Knowledge of specific requirements involving availability, speed, and reliability is also crucial. It is useful for students to understand the latencies of GOOSE messages through different kinds of switches and network topologies. This thesis seeks to address these questions by simulating, deploying, and testing a sample substation communication network in a computer-based network emulator in order to compare topologies and switch types to enhance the reliability, availability, resilience, and security and, additionally, to contribute to developing designs that reduce the unavailability of the network along with reducing the cost of the components, installation, and maintenance.

### 1.4 Thesis Layout

This thesis captures research performed during the 2020-2021 academic year. Chapter 2 presents a literature review describing three main topics plus a brief detail of cyber threats to the security of substation networks. Chapter 3 offers an overview of the communications inside a substation. It includes a summary of different Ethernet network topologies in substations as well a traffic load and performance of each topology. In addition, Chapter 3 describes various switch types, including a comparison in terms of reliability, price, and challenges that need to be taken into consideration when applying to for designing and setting up a network inside the substation. Chapter 4 records benchmark testing performed in an emulator for measuring the response time of GOOSE messages, their latency, and the relationship between latency and network load. In addition, Chapter 4 provides test results for the different Ethernet switches and topologies. Finally, Chapter 5 concludes with a summary of the test results, analysis, conclusions, and suggestions for future work.

# Chapter 2: Literature Review

## 2.1 Introduction

A modern electrical substation is a power network facility that uses a communication network-based Ethernet switches to distribute and transmit processed measurements of electrical power signals. Configurable switches are typically used in industrial control systems to facilitate communication between network enabled IEDs. IEDs are devices that can perform electrical monitoring, control, and protection tasks. They can be combined through communication using analog connections, RS-232 and RS-485 based series works, and Ethernet network of switches. Modern substations use Ethernet communication. Engineers create a substation network with multiple topologies and switches to interconnect IEDs.

Some network and communication research areas depend on knowing the networks' behavior and traffic patterns; therefore, it is important that detailed characterizations are performed regularly. These characterizations can offer insight on how to run a more efficient and reliable network when adding network communications in a substation. Unfortunately, there has been little research published about the different switch models and products in power system networks and industrial control system traffic. Some authors have discussed the network topology in a power substation environment in many forms and shapes [1] [2]. In addition, many design factors like redundancy, efficiency, scalability, management, latency, price, reliability, substation size, and more may influence the decision to choose one topology over the other [3]. Therefore, the same design factors could affect the network performance in substation if the designer chooses a specific switch model.

This literature review performs comparisons between switches, including network topology, data traffic load, and security, using different managed switches such as the SEL 2730M or software defined network (SDN) switches such as the Cisco 2900.

The purpose of this research is to test, develop, evaluate, and design topologies for substation communication networks and combinations of switch types that would enhance the reliability, availability, and security of the substation network. In addition, the options will be compared with respect to the unavailability of the network and the cost of the product, installation, and maintenance. It is crucial to select most effective design utilizing the given set of resources such as links, switches, and devices that could applied to substations in the future, which may bring a reliable network architecture, system stability, and financial benefits for communications for power system protection and control.

## 2.2 Methods to Analyze Performance of Network Topologies and Ethernet Switch

Electrical substation communication network systems use multiple types of topologies, such as bus or star, between substation nodes for communications. Choosing a suitable topology may be guided by multiple factors, including redundancy, reliability, scalability, efficiency, diagnostics, cost, management, latency, substation size, etc.

Skendzic et al. [4] offered a comparison between several redundant Ethernet network topologies to examine their suitability, analyze performance, and summarize reliability, unavailability, and availability of the topologies. The comparison calculations of the topologies in [4] are based on 22 local station relays. They summarized the unavailability of the Ethernet network for each of the topologies based on normalizing numbers using an availability calculation based on statistical mean time between failures (MTBF) numbers for each device. However, the authors of [4] did not use any other types of switches in order to understand the differences and get the complete result of the performance between the switch types in each topology. They only examined eight topologies with the same Ethernet switch and router of many possible switch networks configuration types. Another issue is the absence of cost and resilience calculations.

Scheer et al. [5] calculated and compared reliability, unavailability, and availability of a substation network by using different components, such as Ethernet switches, hubs, and redundant switches, in each topology. Although the authors of [5] calculate the reliability and compare between different devices in five LAN networks, the paper does not assess topology schemes such as ring and star topologies. The cost provided in the paper for each device and the average equipment prices for the IED interfaces, fiber optic, cables, hubs, switches, routers, and servers are included in the costs result at the time the paper was written. In addition, the statistical MBTF and MTTR numbers were obtained to determine the unavailability and availability. However, both [4] and [5] used different MTBFs for Ethernet switches. One has been in use for 60 years and the other one has for 11.5 years, reflecting improvements in switches in the years that passed between publication of the papers. Therefore, the actual MTBF for each switch must be obtained from switch device manufacturer’s manual.

Alexander et al. [3] propose a Software-Defined Networking-based solution for loop-based topologies by using linear programming in the proposed network topology, which would be technically unfeasible using traditional network protocols. The author employed a SDN switch to solve problems associated with the broadcast traffic restraint and the diffusion and reliability of the multicast traffic.

Topological examination by using different switch types in a network is critical to figure which one is more suitable and reliable than the others. This examination indicates that more topological design would help engineers to build a proper network for a substation to increase network reliability. In addition, it is crucial to identify and characterize all the devices in a network and their connections to analyze the reliability of the network. Calculating different components in various topologies mathematically could achieve a more accurate outcome for the network in substation.

### 2.3 Data Transmission Analysis

The network messages communicated between intelligent electronic devices (IEDs) in a substation carry data packets containing DNP3 messages, GOOSE messages, and sampled values transmitted through Ethernet switches typically transferred over twisted pair copper cables or fiber optic cables within any substation topology. While communication response time for commands over Ethernet is slower that older schemes using direct analog or digital signals, it is possible to configure communication networks with redundant connections to improve reliability. The speed and reliability of substation communications can be used as a measure of substation performance. The overall performance and extensibility of substation communication networks between different switch types can be rated using measures of traffic load such as speed and packets lost.

The authors of [6] described the performance and requirements of applying Ethernet in a substation. They used a managed Ethernet switch with advanced layer 2 and 3 qualities to support real-time control and automation, such as full-duplex operation on all ports, priority queuing, IEEE 802.1Q VLAN, Rapid Spanning Tree Protocol, and Generic Multicast Registration Protocol (GMRP). Full duplex operation on all ports means the Ethernet communication will have no collisions in the data buses, thus making the communication more deterministic. Priority queuing sets a different priority level tag for each frame to ensure that real-time critical traffic frames go through the network even when the network has congestion.

Q VLAN functionality groups IEDs into virtual LANs that will separate real-time IEDs from less time critical data functions. Rapid Spanning Tree Protocol is used for ring topologies to prevent the frame from going in a loop and instead breaks the ring by blocking one of the links. However, if a link fails the link blocked by the protocol is immediately activated to restore data flow. A Generic Attribute Registration Protocol (GARP) is a multicast application that filters and assigns multicast data frames to IEDs, for example Generic Substation State Event (GSSE) and GOOSE frames.

The authors of [6] studied a few network architectures, such as bus, ring and star, to observe the different levels of redundancy, availability, performance, and cost. In addition, they list the pros and cons of each topology scheme. One of the topologies is a bus topology also called a cascading architecture. It is a typical topology where switch is connected to the next switch. They calculated the frame transmission and total delay from all switches by equations (1) and (2):

*The Frame Transmission time = Message frame size * 8 Bits/Byte * 1/100 Mbps (if the speed of uplink ports = 100Mbps)* (1)

*The Total Delay from Switch 1 to Switch N = (Frame Transmission Time + Internal Switch Latency (5us typical for 100 Mbps ports) * (# of 'Hops' or number of switches)* (2)

Although the authors of [6] explain multiple topologies in a comprehensive way, the paper did not make conclusions comparing different kinds of switches such as unmanaged switches, managed switches, or hubs for each topology. These performance differences with different switch types could allow the engineers to easily build a network with different topology schemes for substations so that the dominant performance issues could solved. Switch technologies have continued to evolve since [6] was written.

Evaluation of a traffic load flow in a substation by modeling and simulating a network could be considered to determine the total rates of the network. Sidhu et al. [7] demonstrate three IED models (breaker IED, merging MU and protection & control [P&C] IED) connected using the three topologies of bus, star, and ring to gauge the performance in each message delay type, such as raw data message, intrabay trip message, and interbay trip message. Raw data samples are time-critical and directly mapped to a low–level Ethernet layer so the Ethernet frame path will be short, with reduced latency. The paper found that in the worst-case scenario using 10

Mbps switches with no priority messages will see an increase the delay time of more than 5 ms, which was the standard time for direct digital messages in the power system industry. A comparison between the messages for those three IED types in a ring topology implies that the best choice is to upgrade the link to 100 Mb/s and ensure that the Local Access Network (LAN) speed in the subnets is kept to at least 10 Mb/s to keep the End-To-End delays are in the specified standard range.

Papers [6] and [7] use the OPNET modeler platform to analyze the information network characteristics in substations. Some results indicate that LAN speed of at least 10 Mbps link is more beneficial and able to transmit the data at as small a delay as possible (note that these papers were written at a time when 10 Mbps links were not common in substations). Since the papers are outdated and did not consider modern technologies, they did not examine of the static optimization of network structure with key factors that could influence the network performance. One of the factors is using different switch types that could affect the evaluate transmission performance of traffic flow and data load traffic along with speed and length of the links. Modern Ethernet switches can manage the data rate in the range of gigabits per second and collisions can prevented. Furthermore, Ethernet switches can also support Priority Queuing, Q VLAN, Rapid Spanning Tree Protocol, and GMRP. These technical features can be helpful in increasing the performance of the substation network. However, changing the switch type could affect the traffic transmission abilities through the substation networks, including delay, speed, and lost packets. A study of data transfer delay and data traffic lost for different Ethernet switches in substations will be useful to determine the reliability, availability, and performance of communication networks in substations.

## 2.4 Cybersecurity and Reliability

Cybersecurity has become one of the key factors to consider in substation performance evaluation in modern substations. Using Ethernet communication between and within substations opens vulnerabilities that did not exist in older designs. Potential crossover points between the operational and enterprise networks within utilities open bridges for potential attacks. Network security in the power system is designed to provide integrity, authentication, and confidentiality of messages exchanged between devices in substations, possibly using some of the security tools developed for enterprise communication networks like digital signature, cryptographic algorithms, keyed-hash message authentication codes (HMAC), and Transport

Layer Security (TLS). Some of the methods developed for enterprise networks are not suitable for substation environments where real-time delivery of data is a priority and lost or delayed packets through the security tools are not acceptable. In addition, the legacy IEDs in substations have limited computing resources and can offer only a slight part of their resources for overhead for security processing.

The following discussion of potential cyberattacks starts from the assumption that attackers have already penetrated the utility network and are striving to perform an attack within a substation.

According to Rashid et al. [8], the lack of encryption between field devices in the substation creates security vulnerabilities for GOOSE and SV messages, and the authors noted the absence of security measures in the version of the standards at the time the paper was written. One type of attack is a DoS attack. There are several types of DoS attacks, such as SYN flood attack and buffer overflow. A DoS attack can be implemented on the connection between IEDs by sending a spoofed SYN request multiple times until the server will no longer be able respond. Another DoS attack targets the IEDs by sending malicious packets with oversized data payloads, causing a buffer overflow. Both attacks will affect the availability of the Ethernet switch that in turn will affect the performance of the network. The use of managed switches can block some forms of DoS attacks but not all types.

Another avenue to attack a substation is a password cracking attack, which can be implemented in several ways, including brute force attacks and dictionary attack. A brute force attack assembles all possible combinations of passwords until the right one is found; however, it may take a long time to get the right one, especially if the password is complicated. Since many legacies substation IEDs do not support complex passwords, this can simplify the attack. A dictionary attack uses constructed words from commonly language words or number combinations to crack weak passwords. Once attackers can break into a device through a stolen password, they can do further attacks on a network, including further password cracking attacks on further devices or DoS attacks. Another attack that can be used to enable further attacks is a packet sniffing attack, which is an attack where a compromised device on a network captures packets transmitted through the network by a host configuration. This act gives the attacker the ability to steal data and perform further attacks, such as a man-in-the-middle attack to Address Resolution Protocol (ARP) and switch port.

The authors of [8] and [9] did their research connected through a fast Ethernet network to a Cisco 2950T managed network switch SDN switches are more advanced than conventional managed Ethernet switches and can reduce the possibility of some forms of attacks. However, they are in some ways more vulnerable to the attacker since they more complicated to configure, and configuration errors could create vulnerabilities. Therefore, the design of a network based on SDN switches has possible attack points that could defeat its system. Attackers can be concentrated on the switches' table since it has information related to network management, switching routing, and access control [9]. The attacker also could concentrate on the controller because the controller is the central place to manage and control the whole SDN network. It is possible to attack the link between the controller and the switch since there are discreet messages between them. Such an interface could be attacked by tricking the controller to add a suspicious application that could join the network and a compromised network. The SDN controller performs many jobs such as network information collection, network configuration, and routing calculation, making it the perfect target for major attacks. If the attacker takes over the controller, they can cause damage to operation of the physical power network.

Cybersecurity becomes a crucial feature of any new network design seeking to improve the performance of the substation network. Researchers have shown cyberattacks on substations can disrupt the operation of the power system. Cybersecurity threats are so numerous as to be uncountable; there are many research papers in this field as well as a limited number of papers documenting successful attacks. Cybersecurity professionals must know how to secure the data, the network devices, and the communication network transporting data across the network to reduce the risk of malicious attacks. When choosing between managed switches, hubs, and SDN networks in a substation, network security must assessed [10].

## 2.5 Summary

Communication networks in modern power substations network have increased in both size and complexity at the same time as the need for higher levels of reliability, availability, and security. The examination of topologies and switches is critical to figure which are more suitable and reliable. In addition, the transmission speed of packets and traffic flow in a substation are important criteria for performance evaluation in substations. Cybersecurity has become a crucial feature of any new network design that will increase the performance of the substation network.

The research question for this project is how the application of different switch types when combined with different network topologies could affect the network performance in a substation.  This question will be answered by gathering comparative data between switch types in different topologies by using network simulations. Each topology will be compared using different Ethernet switches such as hubs, unmanaged switches, managed switches, and SDN switches. The comparisons will be based on tests relating to speed, congestion, and packets lost.

# Chapter 3: Overview of Communications Inside the Substation

## 3.1 Substation communication Architectures (Topologies)

Communication inside a substation plays an important role in the operation of the power system. Modern substations can have communications for a variety of power system applications, starting from internal communications between local devices in part of substation up to communication between stations in high voltage transmission systems, resulting in multiple levels of communication networks [4]. This thesis will concentrate on substations with one or more internal Ethernet networks.

A substation communication system uses a selection of topologies, networks and subnetworks, and protocols to communicate between multiple nodes. Most new substations use Ethernet communication. These nodes are intelligent electronic devices (IEDs). Each IED device is connected to the Ethernet and therefore has one or more Ethernet interfaces that include transceiver technology to match the network speed and size [5]. There can be many types of IEDs in a substation; one class of the IED is protective relays, which implement functions to detect faults in lines, transformers, and other equipment. Another example of a class of IEDs is made of up metering devices used to monitor current and voltages to be communicated to the control center. Control signals can be carried over another communication network to actuate devices such as circuit breakers, which break the current flow and isolate the circuit either in response to a short circuit or for routine maintenance. Protective relays detect faults and send trip and reclose commands to the breakers over one of the networks in the substation.

A merging unit is an IED device for gathering multiple digital signals like currents and voltages from instrument transformers and transmit them to other IED devices such as relays and meters through a dedicated network over Ethernet switches. Using merging units means that a single communication cable can carry many digital signals to replace many individual copper cables that carry analog signals between the instrument transformers and the relays or meters. However, each digital stream of SV (sampled values) messages from different merging units should be time-synchronized; consequently, the protection relay can utilize many digital signals from individual merging units making it easier to implement back up schemes to improve protection reliability. The list of types of devices above is not exhaustive, but it illustrates the variety of equipment inside the substation. Furthermore, communications perform an important role in information distribution. This information is crucial for some system operations. There is a monitoring device inside the substation called a “Remote Technical Unit” or RTU. The RTU is a physical device that monitors and controls some of the IEDs described above. RTUs are used to communicate the status of the substation to the control center over a communications and control network referred to as a Supervisory Control and Data Acquisition (SCADA) system [2]. This makes it easy to monitor and control substations remotely to improve overall system operation and reliability. In a substation, in addition to the IEDs connected to different networks through Ethernet switches, there may also be programmable automation controllers that provide data concentration and automatic control with the Substation Automation System (SAS). [4]. In addition, there may be a Human-Machine Interface (HMIs) allowing a local snapshot of the substation. The substation may be connected to one or more connections to external private communication networks such SCADA for system operations or other wide-area network (WAN) links for remote maintenance engineering access and disturbance analysis. All these devices are connected via Ethernet switches, forming multiple networks to transmit measurement data and commands within a substation, between substations, or from substation to control center.

Generally, there are three levels in a modern IEC 61850-based substation automation system, called the station, bay, and process levels, as shown in Figure 2. The station level is located at the top level, which has a user interface (UI) computer, a Network Control Center (NCC), and gateways (GW) to each of the external networks the substation connects to. In addition, the station level bus may have a human-machine interface (HMI) , the RTU that interfaces to the SCADA network, and a group control/key server (GCKS) [5].

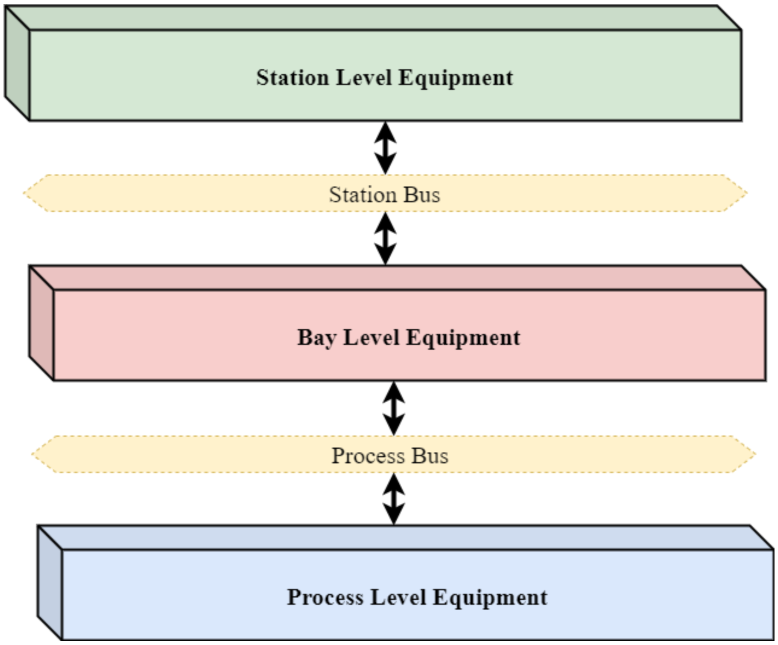


Figure 2. Substation Levels

The purpose of this station level is to monitor and control substation devices and interface them to the control center. In IEC 61850-based substation designs, station-level devices communicate with bay level devices using a Manufacturing Message Specification (MMS) protocol with devices at the station and bay level. Other substations may use different communication protocols at this level, such as DNP3 or MODBUS, or they may even have hardwired connections.

The second level is the bay level, which is the middle level that is involved with coordinated measurement and control inside a substation. The bay level has units for protection and control. A bay level controller controls IEDs to perform fault isolation, load management, voltage and frequency control, and power quality control functions. As noted above, the bay level is tied to the station bus communication network. The bay can also be connected to process bus networks, allowing IEDs to subscribe to measurements from merging units (MU) and other monitoring IEDs to acquire necessary data values that are needed to make protection decisions as well as send commands to actuators, such as circuit breakers.

The last level is the process level, which interfaces to the actual power apparatus. The process level can include actuators for switchgear like circuit breakers and circuit switches, which controlled opening or closing based on commands from IEDs at the bay level or commands from the control center received at the station level. The process level can use IEC

61850 Generic Object-Oriented Substation Event (GOOSE) message communications, which are specific protocols to communicate critical messages between IEDs at the bay level. Older substations have direct connections at this level.

The process level can also carry data broadcast by measurement devices such as merging units that collect analog signals from current transformers and voltage transformers and convert them to processed digital signals. In a complete IEC 61850 digital substation the merging units support the sampled value (SV) multicast communication protocol and transmit measurement to IEDs at the bay level for further processing or transmission to the station level. Several equipment vendors have proprietary protocols that are similar to SV. Devices support a key-hash message authentication code (HMAC) for integrity protection plus authentication that uses Transport Level Security (TLS) protection. The process level is most likely an interface to the primary equipment, which directly connects with the switchyard equipment [11].

From a communication protocol perspective, as shown in Figure 3, GOOSE and SV are mostly used in substations between the bay and process levels. GOOSE is a connection-less Ethernet-based protocol that broadcasts a binary high-speed fashion connection between protection and control IEDs, although some utilities use GOOSE messages for commands between substations. GOOSE provides a flexible implementation for engineers that permits them to design a complex yet independent network. In addition, GOOSE messages make the connection in P&C design less costly to install in new substations and easily editable in a way that allows the engineers to update protection and control schemes [2]. GOOSE messages transfer via Ethernet frames, which can include data payloads such a breaker open/close commands, breaker status information, or processed measurement data from IEDs. This will capture the data frames for analyzing network performance. The other Ethernet-based IEC 61850 processes bus level protocol sampled values and broadcasts measurement signals from merging units to any subscribing device at the bay level. The subscriber device, such as a relay, can receive these sample messages and make use of them to execute their metering and protection functions.

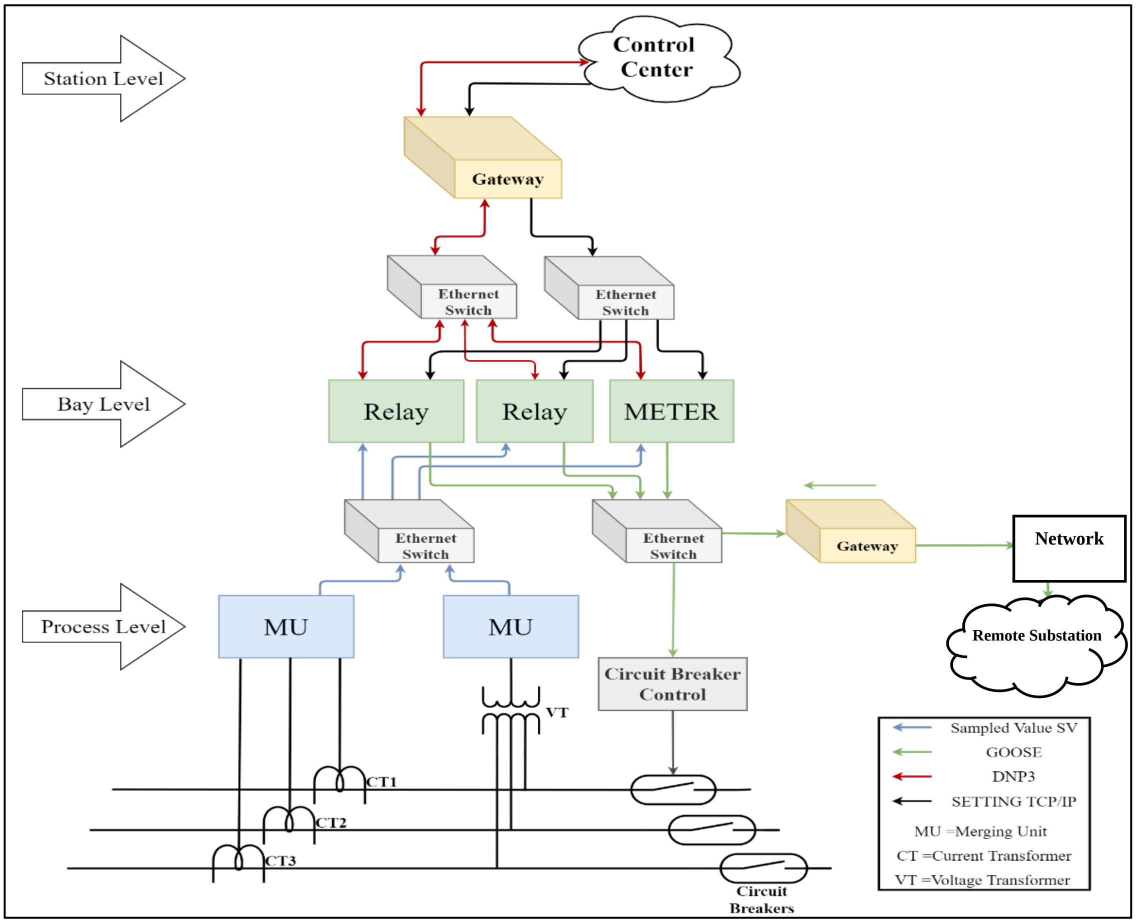


Figure 3. Architecture for the Substation Communication

In the Substation Communication Network (SCN) architecture shown in Figure 3, each IED is connected to Ethernet switches. The Ethernet network topologies used in substations diverge widely with no established standard industry practice [4]. In the next section, more detail is provided on possible substation network topologies schemes.

### 3.1.1 Network Topologies in a Substation

An Ethernet communication switch is a central focus in any topology's structure. The star topology is most commonly used topology but not the only one. However, the implementation of a topology can be customized depending on applications, system sizes, and the number of levels. Several network topologies comprised of Ethernet switches, such as bus, star, tree, ring, or a combination between star and ring, can be applied. These topologies are designed based on the suitability, size, and complexity of the networks in the bus levels in Figure 2. The following topologies summarized are used in substations.

### 3.1.1.1 Serial (Cascading) Topology

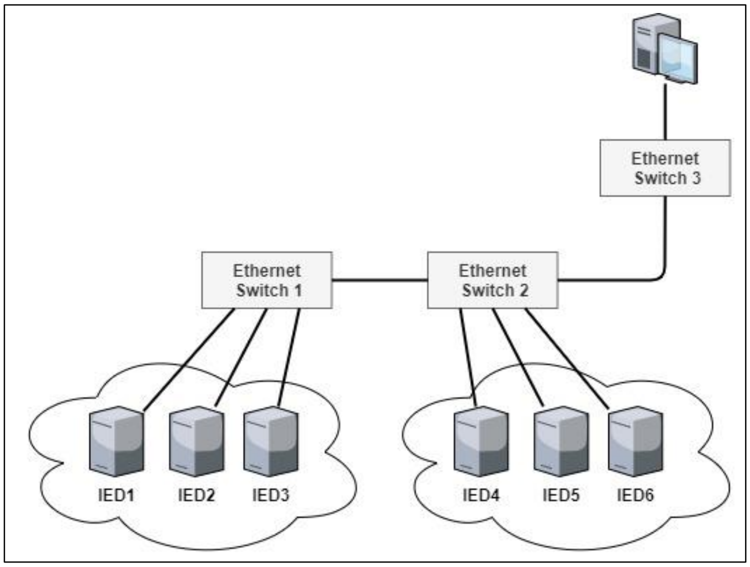


Figure 4. Serial (Cascading) Topology

The serial or cascading architecture is shown in Figure 4. Each switch is connected to the next switch in the cascade like a series of switches and connected via one of its ports. The switch contains two types of ports: a high uplink port, which is specifically customized to connect a switch to another switch, and a downlink port that is connected to IEDs. The number of switches could be increased and further cascaded depending on the size of the network. The system operation must be able to  tolerate the worst latency scenario. For instance, if an IED1 sends a packet to the control center, the packet will pass through switch 1 to switch 2 to switch 3, which results in delay because each switch will take time to process the frame [6]. In testing in this thesis, the packet is a GOOSE message, which can go from any IED. The size of the packet is 350 bytes in the GOOSE message that is transmitted through a switch. To be more specific, the 350 bytes is a combination of 336 bytes of data, and 14 bytes of header. In that case, the typical speed of uplink port network used in electric substation applications is 100 Mbps, which means that the internal switch latency will be 5µs. So, the calculation for transmission time and total delay for GOOSE messages in each switch in a serial topology will be the following:

$$\textit{The frame (350 bytes) transmission time} = \frac{350\ x\ 8}{100000000} = \textit{28 microseconds} \qquad (3)$$

Therefore, the total delay for one switch and several switches will be the total delay in one switch = (the frame transmission time + switch latency) x number of switches or hops:

*The Total delay in one switch with frame size (350 bytes) = 28 + 5 x 1 =33 microseconds* (4)

However, here in the test, the number of used switches will be 3, so
*The Total delay from three switches with frame size (350 bytes) = (28 + 5) x 3 = 99 microseconds* (5)

The serial topology features are simple, and they cost less when they need only short wires run. However, redundancy is absent in this topology [12]. When one of the switches fails, the IED connection will be lost and the whole system will be unreliable. Moreover, the time delay or latency of this topology is high.

#### 3.1.1.2 Star Topology

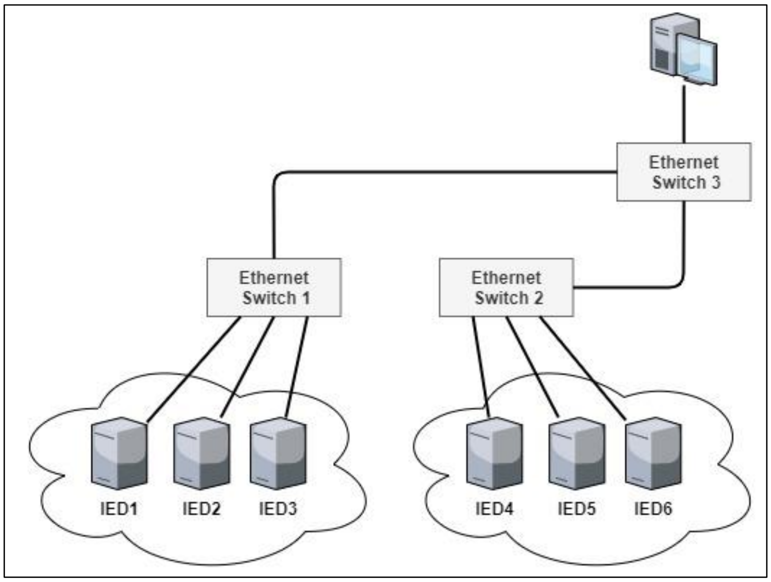


Figure 5. Star Topology

The communication network architecture of a star connected substation automation system may include a single central switch in which all the IEDs, Ethernet switches, and gateways may be connected, thus creating a look of star network topology is shown in Figure 5. Switch 3 is referred to as the ‘central’ or master switch since all the other switches connected to switch 3, creating a star form. This topology offers the least amount of delay because an IED is connected to any two switches; for example, in Figure 5, switch 1 is connected to switch 3, which only requires the message frames to send in two hops. The same is the case with switch 2. The time delay uses the same equation of (4) however, instead of using 3 hops it will be 2 hops:

*The Total delay from in three switches with frame (350 bytes) = (28 + 5) x 2 = 66 microseconds* (6)

This topology is easy to configure, monitor, maintain, and troubleshoot. In addition, if a link is lost, the recovery will be cause fewer disruptions to the network. The equipment installation and removal will be more efficient. However, the redundancy in this topology is zero since there is a single point of failure. In other words, if the master switch has failed, the whole network will be lost, and then the network will have reduced reliability due to having a single central Ethernet switch. In addition, the cost of the links and communications is expensive since there is no direct communication between nodes.

**3.1.1.3 Ring Topology**

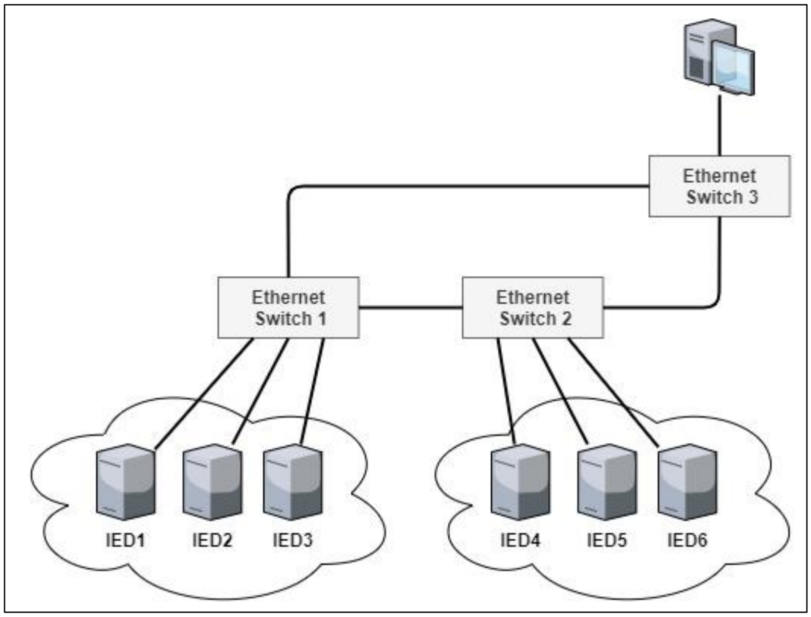


Figure 6. Ring Topology

As shown in Figure 6, ring topology is very similar to the serial topology except that the loop has closed from the last switch to the first switch. However, Ethernet Switches do not support loops. To put it differently, messages that go in a loop will be circulated and the availability of the bandwidth will be reduced. Therefore, it is necessary to employ managed switches that contain a protocol called rapid spanning tree protocol (RSTP) [6]. Messages that are circulating in the loop will be stopped by the spanning tree protocol to block them from circulating in the loop. To put it another way, managed switches with spanning tree will break the ring by blocking messages if there is a loop detected. This protocol in a managed switch and SDN switch allows them to reconfigure the network by themselves during communication network faults to span out into two paths within a fraction of a second.

Consider that switches 1, 2, and 3 have connected to a ring as shown in Figure 6, and all the switches are managed switch with RSTP protocol. Network traffic will be streaming in path 1 and path 2, right or left. Switch 3 will break the loop and prevent any messages in full circle from getting looped. In case a link fails, the switch with RSTP will reconfigure itself and redirect communication to another path and isolate the network segments into two paths, as shown in Figure 7. This action offers high reliability due to its redundancy, as all IEDs are still connected even if one of the links or switches fails. Although this topology offers immunity from breaking the network and reducing the redundancy, it increases latency due to the complexity of the topology, which takes some time to reconfigure the network. Moreover, this topology only works with a managed switch since it is needed to run the RTSP. In addition, it is hard to remove or add nodes, troubleshoot a link, and detect a fault in a node since the modification needs to be programmed in the switch. Furthermore, the cost of the network in cabling, configuring, and wiring is expensive [12].

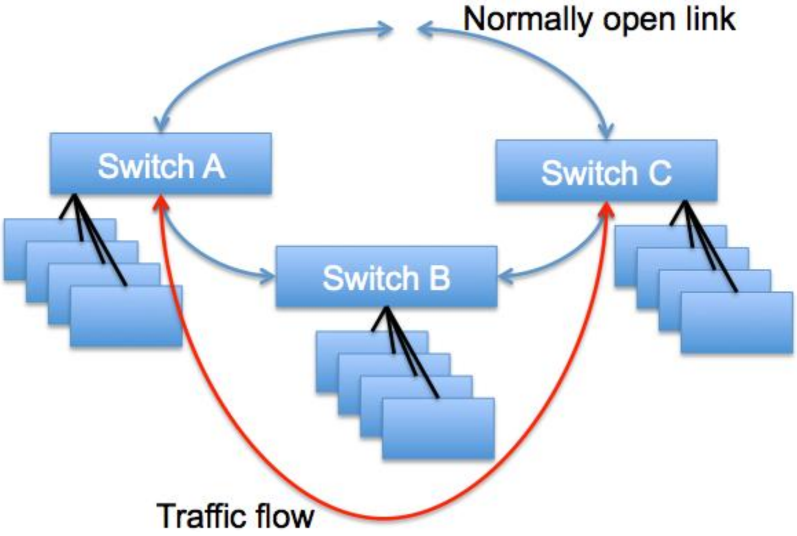


Figure 7. Rapid Spanning Tree Protocol RSTP Description [2]

#### 3.1.1.4 Hybrid Topology

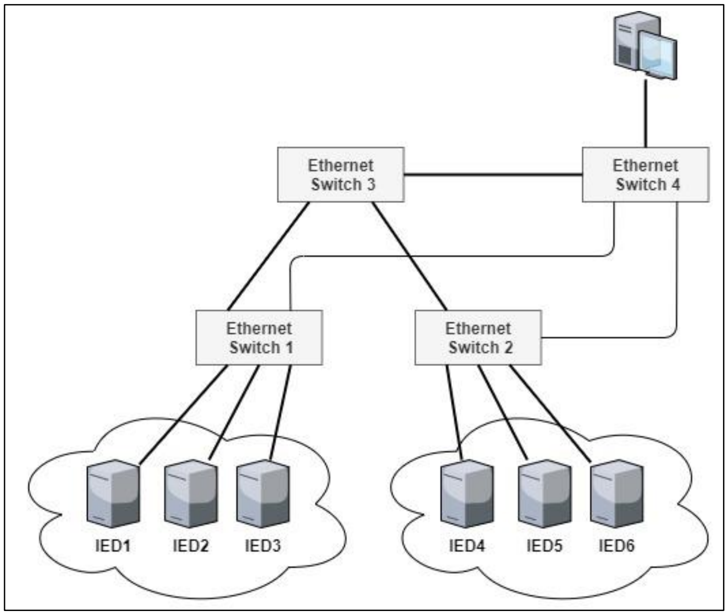


Figure 8. Hybrid Topology

A hybrid topology is a combination of star and ring topologies in which each Ethernet switch is connected directly to two main Ethernet switches, as shown in Figure 8. Both main Ethernet switches are connected in a ring topology. As shown in Figure 8, two rings operate in parallel; both ring topologies provide a higher level of redundancy and zero recovery time in case any link fails as well as low latency [11]. This approach will minimize collisions, latency, and unavailability and maximize the availability, reliability, and redundancy. However, this topology requires additional cables and switches to assemble the network in a star-ring configuration, which leads to an increase in the cost [12].

### 3.1.2 Ethernet Switch Characteristics

The broadest communication standard used in substations is Ethernet (IEEE 802.3 [29]). The Ethernet switch is fundamental due to its bandwidth. In addition, it has a full-duplex probability, which means it can send and simultaneously receive packets. Other fundamental Ethernet switch factors involve the absence of collisions and store and forward capability. As mentioned above, a rapid spanning tree protocol  is a motivation for engineers to use managed Ethernet switches, especially in a ring topology for blocking loops in circulated messages. The Ethernet switches also support two independent protocols that can are used by most industrial substations: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy

(HSR). Both protocols provide  redundant transmission of packets in ring topology, and they will stand against any failure of any single network component. HSR arranges two ports into a ring topology without dedicated switches. On the other hand, PRP will merge ports for redundancy in a substation by using a duplicate switch. Nevertheless, these protocols apply protection against collapse due to a single point of failure. The most reliable and best available protocol in a real-time control network is the parallel redundancy protocol because it will accomplish a zero-link failure of switch and zero data loss and delays. However, this approach comes at a price since all links and network infrastructure must be doubled [11].

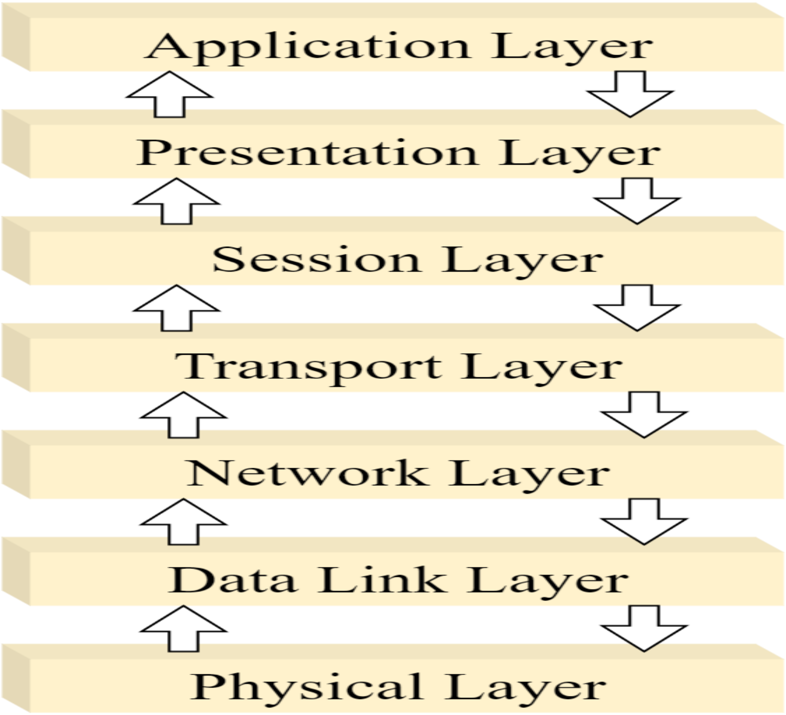


Figure 9. 7 Layers OSI Model

Characteristics and standards of the communications of the telecommunications process are in a structure of a 7-layer network model called the Open Systems Interconnection (OSI) model, as shown in Figure [9]. The IEEE Ethernet switch standard sits at layer 2 or 3 since it has a communications protocol. The data sent from devices such as an IED goes through several stages. The first one will go through an application layer to the transport layer. The transport layer puts the data into small blocks called segments. The segment will be encapsulated to get ready to transmit through the network. After that, the segment will transmit into a lower level called the network layer and the network layer will put the segments into packets to communicate with nodes into different networks. The content of the packets is the address of the destination node. Each node has an address that based on the internet protocol. To deliver the packets to the destination it will need a router, so the packets will go through intermediate nodes. The layer before the physical layer is called the data link layer. The data link layer is responsible for transferring the data between network nodes by detecting the error first before transmitting it to the upper layers. In addition, the data link layer will put the packets into frames, as shown in Figure 10.

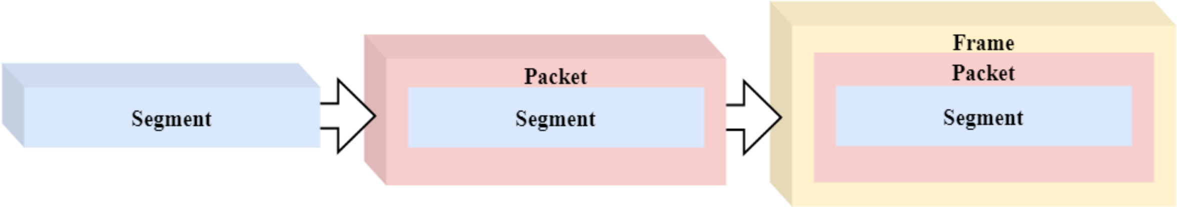


Figure 10. Data Passing Through Stages.

A frame consists of a header, the carries data, and a Cyclic Redundancy Check (CRC). The cyclic redundancy check software checks the frame against an integer value and generates an alarm if the frame contains an error in the data. Figure 11 illustrates the content of an Ethernet frame and the data length of each part of a frame. The header will have 14 bytes. These 14 bytes are divided into multiple aspects, such as source mac address and destination mac address. Each one will have a 4-byte description combined with 2 bytes describing the size of the frame tag. The next part of the frame will be the main payload, which is the data. The data will have a range from 46 to 1500 bytes depending on the transmission data size. As shown above, the data of GOOSE messages used here had 336 bytes of data and 14 bytes in the header. All GOOSE frames coming from IEDs are broadcast to all stations, which allows the station receiving the frame to choose messages it needs based on the context.

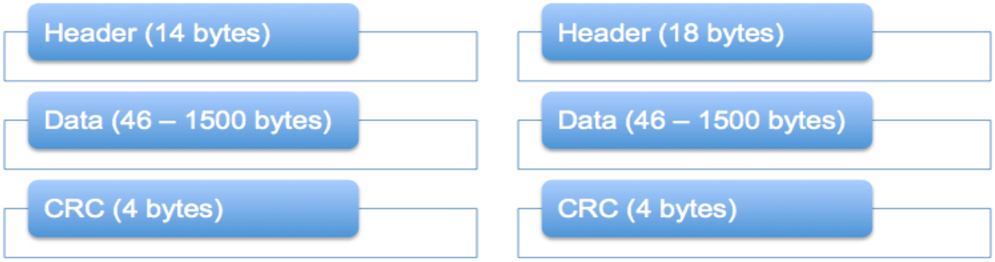


Figure 11. Ethernet Frame [6]

## 3.2 Types of Switches

An Ethernet switch is a network hardware device that connects multiple devices such as IEDs, computers, and servers to exchange data, commands, and information. The standard Ethernet switch is the IEEE 802 Ethernet switch, which was defined by working group 802.1 [13]. However, many Ethernet switches are available in many models and categories, including unmanaged switches, managed switches, hubs, and software-defined network switches.

### 3.2.1 Unmanaged Switch

An unmanaged switch is simple, as it is a plug-and-play device with no configuration interface or options needed. In addition, it has an in-built quality of service to make sure it works completely. Most unmanaged switches are used in small environments due to their low cost, and they can work in environments with high-frequency electromagnetic interference (EMI). They are very secure and can be used with any type of network device. One example of an unmanaged switch is the SEL-2730U 24-Port Unmanaged Ethernet Switch [14] shown in Figure 12. It is a reliable Ethernet switch that is designed for a small substation. An unmanaged switch model is often chosen for IED applications due to its ease of setting. In addition, since they are simpler that are more likely to have higher highest Mean Time between Failures (MTBF) numbers.

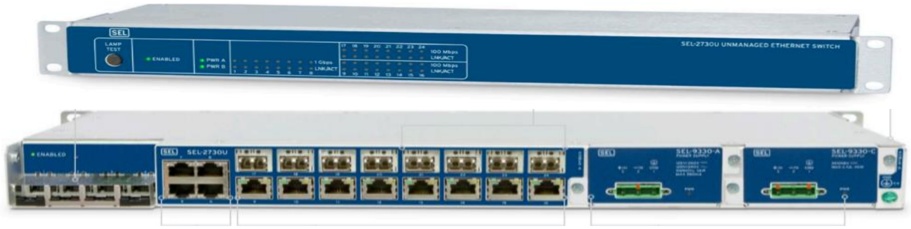


Figure 12 SEL 2730U Unmanaged Switch Model [14]

The cost of unmanaged switches could range from $50 to $2000. The difference is usually due to the number of ports and enhancements in some models. Unmanaged switches are typically the lowest cost options for network management. They do not require an IP address or advanced features such as web page and Simple Network Management Protocol (SNMP) management. Although a managed switch has the same mechanism as an unmanaged switch of routing messages to specific devices, a managed switch is an extra bonus of security and configuration to a network that can do it manually.

### 3.2.2 Managed Switches

A managed switch has one or more methods for users to modify its operation. Common management methods include a command-line interface or a web interface. These can be used to modify the configuration of the switch. In addition, some of the features that can programmed fora managed switch include spanning tree protocols and port mirroring, and there are others as well. A managed switch is a tool that allows one to manage and monitor the settings of LAN. It can also create virtual LANs to keep tight control over their traffic. A managed switch can prioritize the channels that it supports, ensuring the best possible performance. It can also detect and prevent issues before they affect the network. The Simple Network Management Protocol (SNMP) feature is beneficial for monitoring and controlling network traffic. In addition, in the event of a device or network failure, the managed switch can present a feature that repeats and recovers data called redundancy.

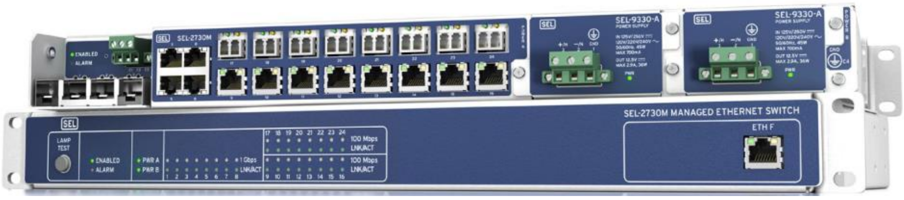


Figure 13. SEL-2730M Managed Switch Model [30]

An example of a managed switch is the SEL-2730M [30]. The SEL-2730M is a 24 Port managed switch that can handle harsh conditions in a substation shown in Figure 13. It features a built-in vibration and electrical surge barrier. An industrial grade managed switch should have RSTP performance is fast enough to minimize downtime. In addition, another robust feature of the IEC 61850 network is a security system that helps to minimize network complexity and provide a secure environment for organizations.

Security considerations vary depending on the type of managed switch. Some of these include the ability to monitor and control network activities and protect against active threats. Moreover, the security features of managed switches vary depending on the platform and the complexity of the network. Some of these include network encryption, access control lists, and VLANs. While managed switches can provide a great deal of control over a network, they should not be used as a threat-fighting tool. They should only be monitored and controlled by a network technician with the highest level of privileges. An Ethernet switch uses the data link layer 2 of the OSI model to establish a collision domain for each of its ports. Each device connected to the same port can then transfer data to any other port without interference and the network domain of a switch still being used for broadcasting data. However, since devices connected to the network are still receiving and forwarding broadcasts, the new domain remains a broadcast domain.

With managed switches, costs are typically higher that for unmanaged switches. Some of these can range from $1500 to $2800. The configurations and features of these switches, such as security and access control, have been affected also by the prices. Managed switches have higher associated costs than unmanaged ones and require more expertise to manage and maintain the network. A managed switch is typically used for businesses that have a larger network footprint or need more control over their network traffic [30].

A switch is more intelligent than a standard Ethernet hub, which typically sends and receives packets out of every port of its hub. It can also identify different recipients and improve network efficiency. A hub is effectively an extension cord that is used to connect various devices on the network. It carries all the incoming messages from the ports to every device that is connected to the hub. On the other hand, switches are typically an interface to the network.

### 3.2.3 Hub Switch

A hub is a network hardware device that can connect multiple Ethernet devices. It has multiple input and output ports, and it acts as a single network segment. A hub operates at the lower layer (physical layer) of the OSI model. It can also participate in collision detection and jam signals if it detects a collision. The hub acts as a repeater that sends the same signal to all the stations. To clarify, when a single station sends a signal, the hub repeats the signal to each station. It typically does so by using the unshielded twisted pair of copper wire. In addition, an optical fiber link may use to carry a star-shaped transmission with a length of a maximum of 500 meters. The hub works with shared bandwidth and broadcasting, has broadcast and collision domains, and can be created using a hub with just a single broadcast domain and a single collision domain. In addition, the hub provides shared internet scalability, network monitoring, and backward compatibility. However, the hub usually has a half-Duplex link and does not provide dedicated bandwidth. In addition, it cannot select the network’s best path because there is no mechanism of any kind to transfer the traffic into a specific path and reduce network traffic. In addition, there is a possibility of the device tradeoff and network size capability.

### 3.2.4 Software-Defined Network Switches

A Software-Defined Network (SDN) is based on a network architecture framework that separates the network control from the main network forwarding and transporting actions so that switch programmers could program the network control in a straightforward manner without any obstacles [15]. In other words, the main SDN program that separates the data plane from a control plane is called the controller, which used for dynamic synchronization of network mechanisms. The control plane is responsible for handling the network traffic, and the data plane is in charge of forwarding the traffic based on the orders made by the control plane. Moreover, the control and data planes exist inside the network devices to reduce flexibility and prevent innovation in the network substructure [18]. In general, a SDN has three layers to deal with: the data forwarding layer, the control layer, and the application layer as shown in Figure 14 [16].

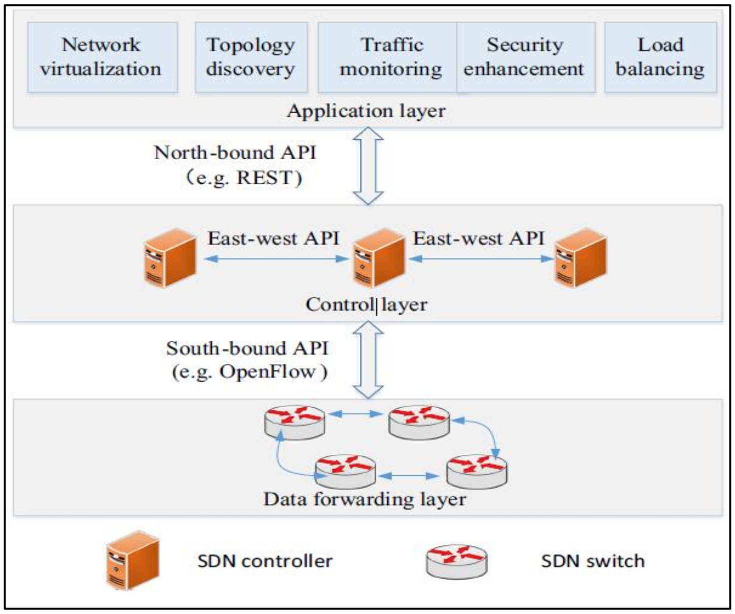


Figure 14. SDN Layers [16]

As SDN switches are one of the most developed technologies available in network schemes they have multiple advantages over the traditional network organization. First, the separation of forwarding and control layers permits the application layer to program individuality, which could lead to creating and developing new network applications. Second, SDN makes it easier for network management programmers to manage a network in a secure, proper way [16]. Third, the center logic providing the overall view of the network is at the center, which processes enough information for the programmers to adjust the network equipment and to improve network performance [16]. The SDN architecture network has three main sections, as shown in Figure 15.

1) Southbound Section: This section is responsible for the interaction and forwarding of devices between the controller and its switches [17]. In addition, the southbound interface shows the communication protocol between forwarding devices and control plane elements. Forwarding devices or the data forwarding layer contain many switches connected through wired or wireless communication. Each switch receives packets and, before dealing with them and forwarding them, the switch checks  its flow table looking for a rule made up by the controller. When the switch finds such a rule action on the packets will be performed based on that rule. Otherwise, the switch will inform the controller to take some action, such as change the flow table or discard the packets [16]. Shaping the interaction between the data plane and the control plane is done by this flow control [18]. This protocol is called Open Flow, which is in charge of communication between the switches at the data-forwarding layer [18]. There are instructions beside Open Flow that define the southbound section of an SDN such as ForCES and protocol oblivious forwarding (POF), and they are installed in the forwarding devices by the SDN controllers [18].

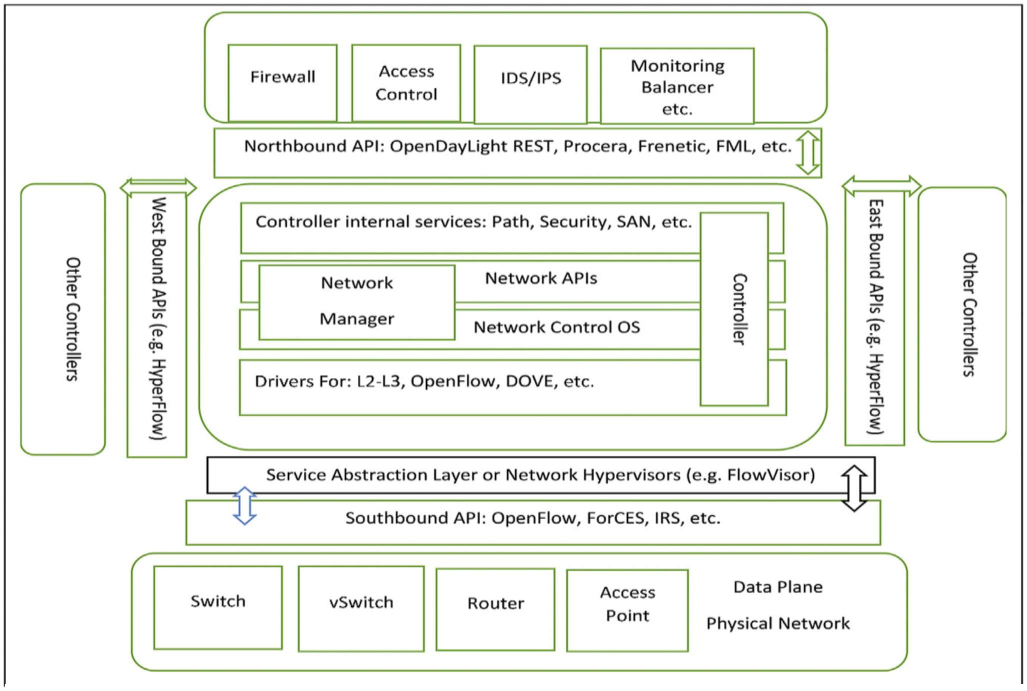

Firewall
Access Control
IDS/IPS
Monitoring Balancer etc.
Northbound API: OpenDayLight REST, Procera, Frenetic, FML, etc.
Other Controllers
West Bound APIs (e.g. HyperFlow)
Controller internal services: Path, Security, SAN, etc.
Network Manager
Network APIs
Network Control OS
Drivers For: L2-L3, OpenFlow, DOVE, etc.
Controller
East Bound APIs (e.g. HyperFlow)
Other Controllers
Service Abstraction Layer or Network Hypervisors (e.g. FlowVisor)
Southbound API: OpenFlow, ForCES, IRS, etc.
Switch
vSwitch
Router
Access Point
Data Plane
Physical Network

Figure 15. SDN Architecture. [9]

2) Northbound Section: The northbound interface (also called middle boxes [9]) has several applications through the application layer that interface with the controller such as REST API.

This section has the application layer that allows network operators to implement network control and operation logic [18]. In addition, the northbound section also has applications such as network virtualization, topology discovery, traffic monitoring, security enhancement, load balancing, routing, firewalls, and others for operation the network [16] [18]. A management application specifies a policy programming language such as Pyretic and Frenetic and communicates with the controller through the northbound section. It is highly desirable that all the security applications such as firewall, access control, and IDS/IPS use a common API for communications with the controller [9].

3) East and West Sections: some researchers call this section the brain of an SDN that controls and manages the entire network. In addition, east and westbound interfaces are required by distributed controllers such as Floodlight, NOX, and Open Daylight whose purpose is to manage, pass, and control the SDN information entirely. This architecture could use vertical or horizontal control. In other words, the application layer (top layer) controller may have several data layer (low level) controllers. An application layer controller has many functionalities, including control, management, monitoring, and tasks distribution for the different and separate SDN data layer instances. Further, each controller is responsible only for a portion of a given switch. For the network to work effectively, each individual controller must communicate with each other through the east westbound API [16].

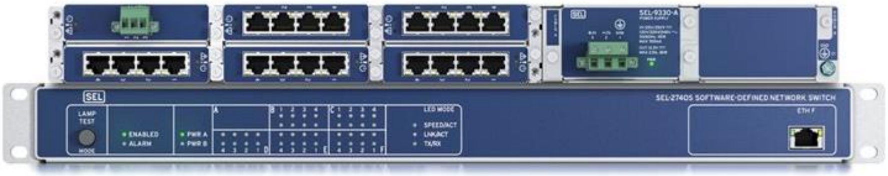


Figure 16. SEL-2740S SDN Model [31]

One example of a SDN switch is SEL-2740S, as shown in Figure 16 [31]. The SEL-2740S is a field-hardened SDN, enabling high-performance, secure, and reliable operation. The SEL-2740S requires use of SEL-5056 software-defined network flow controller.

### 3.3 Network Security and Threats.

Security problems for energy enterprises have been evident in an increasing number of publicized attacks in the past ten years. For more than two decades, nearly all conversation among gadgets outside and inside of energy substations has regarded the use of copper wires and standard communication protocols that assumed that users with access to the network could be trusted [19]. An attack could create to exploit the weaknesses in the OSI network model implementation that is used in substations protocols. Furthermore, the attack could use various techniques to gain access to the upper layers of the model. Attacks against the Ethernet layer often are carried out for various reasons. Some of these include gaining access to sensitive information or preventing legitimate users from accessing it. There are several attack techniques that can be used to target Ethernet layers since the underlying network in the substation is using an Ethernet. Some of these include MAC flooding attacks, ARP attacks, brute force password guessing attacks, spanning-tree protocol attacks, VLAN trunking protocol attacks, social engineering to steal credentials, private VLAN attacks, VLAN hopping attacks, and more.

The IEC 61850 family of standards developed a model that simplifies the management of data in an electronic environment. It provides a set of rules and procedures that are consistent across various types of electronic devices such as Intelligent Electronics Device (IEDs). Generic Object-Oriented Substation Events (GOOSE) messages are a part of the IEC 61850 family of protocol, which provides a standard method for the transmission of electrical data in a wide variety of configurations. GOOSE events are inserted in the control that transmitted in Ethernet packets such as circuit breakers [19].

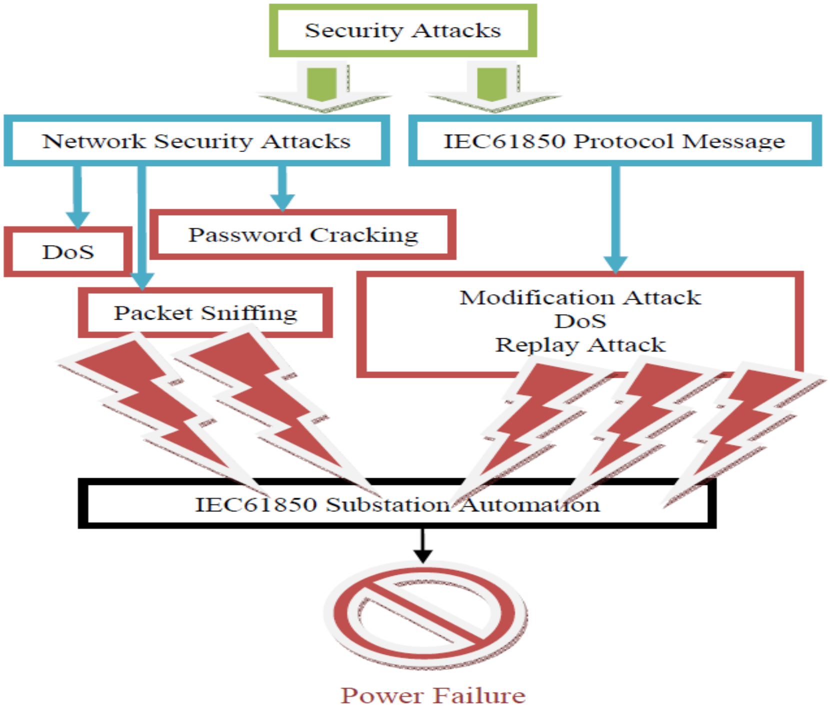


Figure 17. Security Attacks on IEC61850 Substation [8]

### 3.3.1 Ethernet Network Threats

An attack can capture and modify GOOSE messages by exploiting existing security holes in the protocol. This method could potentially allow a hacker to disrupt the power grid and cause it to malfunction. Electric substations are prime targets for malicious activities since they are critical to the function of the power grid. The next section presents some threats and vulnerabilities of the substation Ethernet. In addition, existing security mechanisms that are implemented to bring countermeasures for common threats and secure an industrial network are explained below.

#### 3.3.1.1 DoS/DDoS Threat

DoS/DDoS (Denial of Service/Distributed Denial of Service) are among the most well-known threats among security professionals and attackers because they could affect network performance, increase latency, result in the drop of genuine packets, or temporarily disable the whole network [9]. DOS/DDoS attacks try to overwhelm the network by producing an enormous flood traffic to keep the Ethernet switch busy and unavailable for some signals and stop its functionality. The traffic will be a mix of large number of spurious packets together with a smaller number of legitimate packets and it will be hard to differentiate between them. In any Ethernet switch, the DoS attack will make it stop working due to the traffic volume. The availability of a network in a substation is affected by a DoS attack. This attack causes the network to deactivate and shut down as shown in Figure 18 [8]. There are two types of DoS attacks to distract the substations. The first attack can cause a spoofed SYN request to an IED, which can affect the connection between the IED and its users. The SYN flood attack can be performed by keeping the TCP connection half-open, which is possible because some of the IEDs can simultaneously run multiple protocol services such as HTTP, FTP, and telnet for management purposes [21]. The second attack can execute a malicious code to the target IED that randomly sends oversized data to cause a buffer overflow and can also cause an IED to display unauthorized data modifications [8]. This attack works by overrunning the buffer’s boundary, which can overwrite while writing data to them. It can be exploited to execute code by sending malicious code to an IED [21].

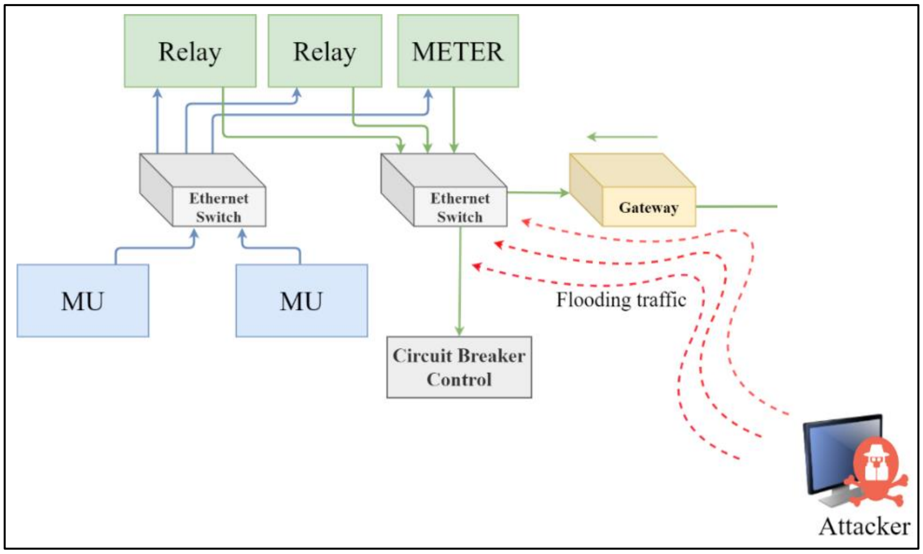


Figure 18. DoS Attack Scenario

In the case of an SDN switch, when an OpenFlow switch receives the new packet and does not know how to handle it first, it will store it into the Flow Buffer and send an instructions request. Furthermore, in a DoS attack, the control will have to deal with massive instructions messages caused by the flooding traffic in a short time, which could affect processing normal traffic into the system. Meanwhile, the link between the controller and the switch could be fully busy due to the attacking traffic, leading to a reduction in the performance of the whole system [16].

### 3.3.1.2 Spoofing

Spoofing is defined as a process in which the network information such as IP, MAC, ARP, etc., is faked to hide the actual information and identity of the traffic source or attacker [9]. For example, when users employ IP spoofing it leads them to access the network resources such as SYN flooding, DNS amplification, and Smurf [9]. Spoofing in Ethernet switch is dedicated in ARP (Address Resolution Protocol) and IP (Internet Protocol). The original goal of ARP was to resolve IP to MAC addresses. A successful attack can use an ARP spoofing scheme to trick a network traffic source into believing that its traffic is originating from the intended recipient. Therefore, ARP spoofing is linking to attacker's MAC address to a valid IP. The ARP spoofing attack may cause a miss in the network by replacing the legitimate user or host available from the list with the attacker host. IP spoofing, meanwhile, is a type of security attack that tries to trick a server into transferring traffic to an illegitimate website. Spoofing methods are very common and can be used to infiltrate legitimate websites. Also, spoofing methods can be used to launch Man in the Middle attacks. A proper authentication scheme can prevent spoofing: Strong passwords and encryption methods can help prevent unauthorized access.

#### 3.3.1.3 Tampering, Eavesdropping, Packets Sniffing and Man in the Middle

Data tampering occurs when unauthorized modifications are made to destroy network information. This is a result when an attacker has gained unauthorized use of network through network intrusion tools or techniques [9]. Once in the network an intruder may try to modify or tamper with the flow table or firewall rules to deny legitimate hosts and allow illegitimate hosts.

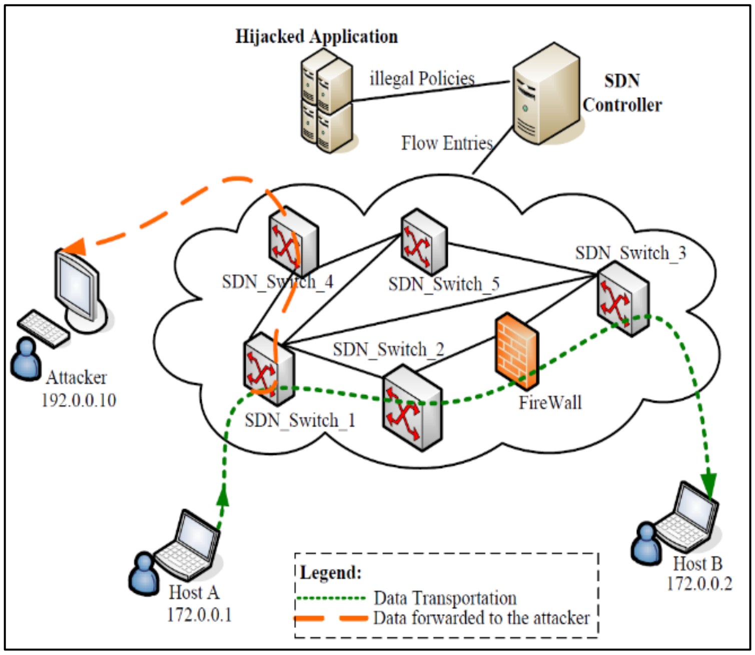


Figure 19. Data Eavesdropping Attack [15]

Eavesdropping is a listening technique where data is collected through electromagnetic coupling to the signal. Wireless communication systems are most vulnerable to this type of attack. However, magnetic field or electric field sensors in very close proximity to wired connections can capture network traffic. Another form of eavesdropping attack can be conducted if an attacker has compromised a device on the network and is able to observe the network traffic through packet sniffing, especially broadcast traffic. Through these eavesdropping methods, traffic in the network can be collected [13]. Furthermore, a message that has been previously eavesdropped on can be potentially sent again through injecting a signal. Since the packet header is not modified, it still can be authenticated or encrypted without affecting the attack. This method works even if the attacker has already modified the content of the message. Within the Ethernet domain, many types of messages can send to resend. Some of these are stateless control messages that can be used to target an attack. Hu et al. [15] demonstrate an eavesdropping attack in an SDN switch where the controller inserts a rule into the switch and the data packet that contains these rules may be made fraudulent by an attacker through eavesdropping on the link between the control and the switch. In Figure 19 the attacker hacked an application server to update policy and copy the packets and forward them with its IP address from host A to host B. Therefore, the new policy will insert into the SDN switch, and an attacker could easily intercept packets from these two hosts.

Packet sniffing is a technique used to steal packets that have been sent over the network. It is usually done through a network interface that is configured to run in promiscuous mode. Like the DoS attacks, a sniffing attack targets HTTP and FTP services because these protocol messages are not encrypted and easy to read after capture [9]. When an attacker launches a packet sniffing attack against an IEC 61850 network, they will be able to steal data from a transmitted link and execute certain attacks. With the use of multi-speed Ethernet switches, a packet sniffing attack can be prevented. However, it is still very difficult to prevent a direct packet sniffing attack in a broadcast packet. According to Premaratne et al. [22], there are three possible methods of attacks in packet sniffing. They are ARP cache poisoning, Content Addressable Memory (CAM) table flooding, and switch port stealing. To launch a packet sniffing attack, an attacker would have to compromise a machine within the IEC 61850 network or have physical access to it. A packet sniffing attack takes advantage of GOOSE and SV messages when the attacker would capture copies of GOOSE messages used to send a tripping signal to a circuit breaker and keep them in their possession. They can send copies of those messages at a later time. This act will cause the circuit breaker to open when its controller received the same GOOSE message commands at an improper time, causing a power disruption. In the case of an SV message, which contains voltage and current values, an attacker can capture a stream of SV packets and then replay and rebroadcast these packets to other IEDs in the substation in a loop, potentially causing measuring equipment to miss disruptions on the system, especially if combined with a physical attack that causes a real disruption. Similar, to incorrect GOOSE message action, stale SV messages circulating inside the substation can lead to unwanted operation [9].

A Man in the middle (MiM) attack is an information disclosure attack that targets information in transit [9]. In a MiM attack a compromised device is inserted between source and destination nodes for measurement or control traffic, allowing data to be manipulated in transit without being detected if the compromised device has sufficient computing power to modify or replace data without significant latency [16]. If an attacker can modify the traffic flow of a network without an integrity verification mechanism in place by directing it through the compromised node, they can easily execute their attack. Compromising a device IP address is typically the most common target of an attack. Attacks can be deployed to modify or eavesdrop on the traffic going through the attacker's host. A MiM attack against an Ethernet layer network is, however, an attack against a host that executed against the STP. If a host has two switches, it can create a tree topology that carries traffic between the two hosts. This attack can be executed by obtaining a connection to two or more switches. The attacker can also execute code by connecting to multiple hosts. In addition, the router redundancy protocols such as (HSRP or VRRP) typically are used to disguise as a network router or gain access to traffic [13]. In a SDN switch, the MiM attack shown in Figure 20 utilize three threats: One targets the line between the control and the switch, and its method includes session hijacking, spoofing, port monitoring. The other two threats are two DoS attacks: one is used to overflow the flow table and the other is to overflow the flow buffer. Overrunning the buffer's boundary can cause memory space to overwrite while writing data to them. This attack can be performed by sending malicious code to an IED that takes advantage of vulnerabilities in IEDs and inadequate security measures for identifying malignant code.

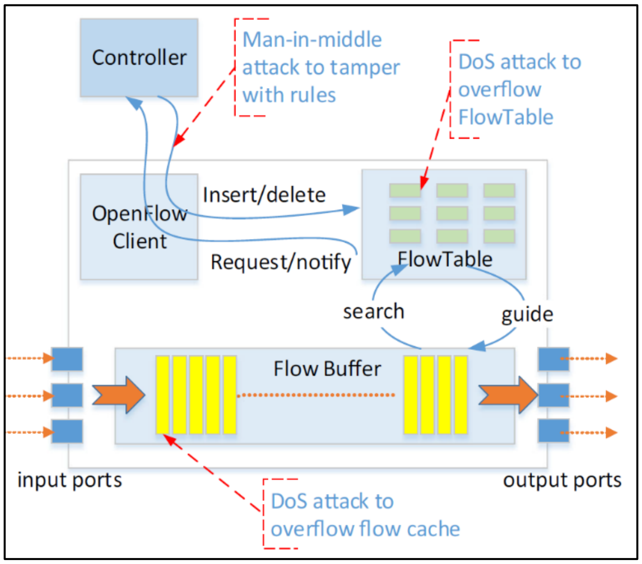

Controller
Man-in-middle attack to tamper with rules
DoS attack to overflow FlowTable
OpenFlow Client
Insert/delete
Request/notify
FlowTable
search
guide
Flow Buffer
input ports
output ports
DoS attack to overflow flow cache

Figure 20. Man-in-the-Middle Attack Scenario [16]

### 3.3.1.4 Device Password Crack

Almost all of the attacks described in this section start with an attacker gaining control of a device in the network to initiate their attack. If IEDs use older unencrypted FTP and telnet protocols they are vulnerable to a password crack attack. A successful attack use either a brute force attack or a dictionary attack. The brute force attack is an attack that tries to arrange all the possible passwords in order until the desired one is found. It can take a long time to find the correct password, especially in a complex password, however older IEDs limited the complexity of passwords by not differentiating upper- and lower-case letters and not allowing non-alphanumeric characters. Dictionary attacks are very similar to brute force attacks, except they use dictionary words instead of guessing random numbers to crack passwords and take advantage of users choosing weak passwords [8]. When IEDs use ordinary FTP or telnet the packets contain direct ASCII mappings, and an attacker can simply send user names and passwords until they get into the IED. Older IEDs do not have unique accounts for each user, and only have simple usernames for gaining different levels of access. If the attacker can determine the make and model of an IED they can determine those usernames from a user's manual, which used to publicly available on the internet, and then would only have to determine passwords. As a first step, they might try the factory default passwords, which can be also found in the manuals for older devices [22]. Older IEDs from some vendors did have functions where they would freeze login attempted for a period of time following three bad password attempts, which serves to slow down brute force or dictionary attacks but does not prevent them. Another approach to defeat passwords is social engineering to steal user's passwords.

### 3.3.2 Security Solutions (Countermeasures)

The most important assets to secure communication in networking are confidentiality, integrity, availability of information, authentication, and non-repudiation. Security professionals must secure the data, the network devices, and the communication transported across the network to reduce the threats for malicious attacks that could cause the network severe damage. The status and logs of Ethernet switches must be assessed to ensure that network security is relentless [10]. However, attackers use several techniques to discover vulnerable targets in the network. Therefore, to further protect against the threats above and emerging threats, defense-in-depth security mechanisms are initiated to bring countermeasures to reduce the vulnerability to the threat issues discussed in the previous section. However, it is challenging to completely remove all vulnerabilities.

#### 3.3.2.1 Firewalls

A firewall is a system of network access control that prevents traffic from entering or exiting a network segment. It can be considered more complex than an access control list. Also, firewalls can be used for inspection purposes such as Deep Packet Inspection DPI and the application layer. DPI is used for the analysis of the content of the packets at the application layer. In addition, DPI can be used to protect various protocols related to Ethernet such as ARP and DHCP. The concept of an Ethernet firewall is different from that of a packet inspection system. Instead of being able to inspect all network layers, an Ethernet firewall can only operate on one layer. Access Control List or ACLs switches are useful for controlling traffic on the Ethernet layer and they can be used to restrict traffic on the higher layers.

Practically, the controller in the SDN performs some of the tasks that are considered accomplished by a traditional network. For example, the SDN controller is making the decisions based on the flow situation and is writing flow rules in the switches flow table. Firewall application creates flow rules in order to enforce an access control list (ACL) to deny malicious trails as illustrated in Figure 21. To explain further, the security administrator may lay down a firewall policy as Figure 21. When host A tries to send Host C, the Open Flow checks its flow table and decides to send to the control or not that the firewall should deal with it later. After that, the firewall analyzes the packet and checks if any rule matches with this packet. Firewall application forces the network of any packets that come from Host A to C are blocked.

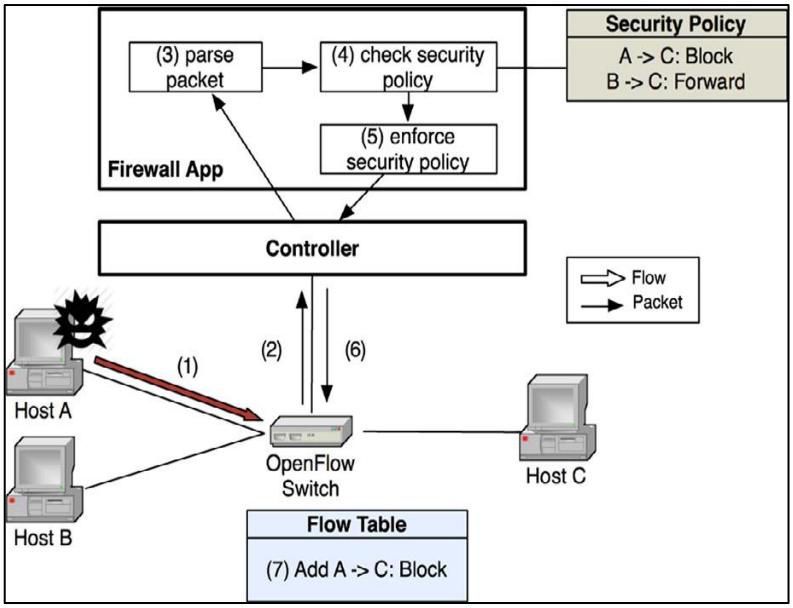


Figure 21. Firewall Function Implementation [23]

Packet data scan detection is to detect and prevent some attacks from going through. Hu et al. [15] write about making the Open Flow protocol extended to support packet data scan detection in some ways, by adding two more additional features into the flow entry format. The controller and switches must be reflected by these updates.

### 3.3.2.2 Intrusion Detection and Prevention Systems (IDS/IPS)

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) use Deep Packet inspection (DPI) to identify and prevent network attacks based on the investigation of packets use, pattern recognition, data mining, and matching with the current inventory of threats [1]. These devices are typically deployed as part of an IDS/IPS device or as part of a firewall and they can gain access to the network traffic that they monitor from a switch. Port mirroring is a technique that enables a network to copy traffic from a specific port to another port, where the monitoring device can be located. This feature can be used to prevent unauthorized access to a protected network through a monitoring device. Some of the features that are included in the switches, such as the ability to send an SNMP trap message including a MAC address when a host is moving in the network, can help detect malicious behavior.

In SDN, IDS can be distributed among switches in the network. Therefore, IDS needs to monitor all traffic, which could be exhausting and time-consuming. However, Network

Intrusion Detection/Prevention Systems (NIDS/NIPS) are a system that allows the network administrator to construct string patterns for use by Deep Packet inspection (DPI). NIPS is a function that detects and blocks any intrusion on the network. Even though the separation of the data and control plane has multiple pros, it also has its cons. If the packet goes by it will not get fully detected but instead only the header. However, NIPS is implemented to perform full packet inspection on every packet going through the network [23]. NIDS function is not that different from the NIPS function. One difference between them is that NIDS does not need to be in line with the network traffic to monitor the traffic. The NIDS wants to monitor, but it got mirrored and then forwarded a packet to the original destination and a copy to the NIDS as well [23].

#### 3.3.2.3 Planning, Configuration, and Administration.

Good network and proper planning administration practices can help minimize network complexity and provide a smooth transition from one network topology to another. This act can greatly influence the overall performance of an Ethernet network. Administrators must enable the separation of trunk networks from leaf nodes by setting up the proper connections to the switches because there is no automatically reliable mechanism. A dedicated VLAN, limiting and data flow and control plane are components of separating management information, which leads to an increase in the network security level. These features help prevent the exploitation of network resources and provide a secure environment for applications. A dedicated VLAN technique can be used to prevent the exploitation of GOOSE messages in Ethernet layer 2. These include setting a dedicated VLAN for all trunk ports, creating access or prefix-list based on the credentials of the users, disconnecting unused ports, and putting them in an unused VLAN, and avoiding the use of shared Ethernet such as hubs [19].

Network management systems help in simplifying the work of network administrators by keeping the network’s configuration in order. In addition, they can also reduce errors and make the network more secure. They can also work with multiple switches by creating a network configuration where the switches work together seamlessly. However, they must be able to do this with the management software. Network administration duties can include monitoring and troubleshooting network activities, as well as performing active network scanning and probing. In addition, network administration duty also includes testing to detect vulnerabilities in the network [13].

Although physical security can be used to reduce certain attack vectors, it is often not powerful enough to prevent others. Therefore, additional security measures must be implemented to prevent insider attacks due to the nature of IEDs and their low capability. Encryption is a security algorithm that end devices should have that can secure their packets and prevent spoofing. In addition, it should encrypt packets or add a digital signature so that packets cannot monitored by an attacker and can be authenticated. Cryptography can solve the integrity and confidentiality requirements of various industries. Encrypted packets transmit between hosts and switches, protecting the confidentiality and integrity of the content in the frames. The research community has mainly focused on cryptography-based solutions that add an authentication field to an ARP message. S-ARP is an example of a cryptography-based solution that adds an authentication field to an ARP message. Another example is the S-MACsec, which provides a secure key management structure. S-MACsec is an intrusion-resistant network security product that prevents unauthorized access to the network. It can also prevent the modification of data frames. These solutions can be used for protecting network traffic from unauthorized access [20].

GOOSE message content inspection used to identify inconsistent messages by detecting GOOSE message content and discarding or generating alarms. when the inspection detects inconsistent messages such as packets with the same MAC address coming from multiple ports on a switch or messages not coherent with the IEC 61850 configuration [19]. Also, there are a different approach to protect network traffic from unauthorized access such as turning off FTP and telnet, having IEDs send alarms to sec team if there are three failed logins, misusing default passwords, and not allowing simple passwords.

#### 3.3.2.4 Detection of DoS

DoS attacks produce many floods (volume of traffic) that at any time will keep changing the flow attributes [9]. Furthermore, the Ethernet switch will assume that every flow is new from the switch’s perspective. In the case of an SDN switch, the unknown packets will be sent to the controller for a decision to make. The attribute’s value per flow is changed by an attacker using generator traffic. Every attribute will be in the range of valid and invalid inputs IP. For example, IP will be from 0.0.0.0 to 255.255.255.255. Therefore, the number of flows can be uncountable. The purpose of this attack is as follows: first, it will flood the switch flow table and soak it with illegal rules. This act could lead to that flow table disability from accepting legal rules. The second purpose is that when hackers keep sending a large number of flows, it will keep the controller busy from responding to valid flows from other switches and may cause the switch to failure [9]. Therefore, the hardest part is distinguishing the normal packets from DoS flooding packets.

However, a simple method could solve the problem of detecting flooding: monitoring the size of traffic flows. Shu et al. [16] propose a framework solution and protocol independent which is a Flood Guard. Flood Guard contains two software modules, the Active Flow Analyzer and Packet Migration [16]. The Active Flow Analyzer is acting as a real-time running controller, so when DoS attacks cause traffic flows, it can detect them. When Packet Migration received the packet, it was buffered and transported to the controller for processing in time ratio because this act prevents the controller from taking many times in processing. Therefore, the Packet Migration module will redirect a table-miss message to the data forwarding layer if there is a DoS discovered. The current network flow is determined by the Active Flow Analyzer monitoring that a variety of sensitive variables will generate, forward, and install flow rules by the controller to the switch in a very active way [16].

#### 3.3.2.5 Man-in-the-Middle Attack Countermeasure.

Securing the channel between the controller and switches in the SDN switch is the most effective solution against the MiM attack. Transport Layer Security (TLS) is used in Open Flow specification v1.0 to secure controller-switch communication [16]. However, TLS configuration is very complicated, and it is difficult to support the TLS in Open Flow switches. There are some alternative countermeasures analyzers proposed, such as Flow Checker, Fort NOX, Veri Flow, etc. Distinguishing between normal and fake rules is our priority insecurity challenge and eliminating them before these become worse and affect the network.

Redundant links or fast link recovery mechanisms are two ways of solving the controller connectivity, which could moderate the effects of man-in-the-middle attacks between the controller and the switches. However, the connection stability testing mechanisms are already in the Open Flow protocol. In more detail, if the switch does not receive an acknowledgment from the controller from a specific time, the switch will assume that the controller has failed, and it will quickly establish a connection with another controller directly, allowing the network to work continuously [16].

## 3.4 Summary

A substation communication system consists of various topologies and networks for communicating with each other. Most new substations use Ethernet communication to communicate between multiple nodes. These nodes are intelligent electronic devices (IEDs), each IED device is connected to the Ethernet switch. An Ethernet communication switch is an essential focus in any topology's structure implementation. The implementation of a topology can be customized depending on applications, system sizes, and the number of levels. These topologies are designed based on the suitability, size, and complexity of the networks such as the serial or cascading architecture, star topology, ring topology, and hybrid topology. In addition, these topology designs use many models and categories of Ethernet switches including unmanaged switches, managed switches, hubs, and software-defined network switches based on the size, cost, and suitability of the network.

Attacks targeting energy organizations have been on the rise in the past decade. Many of these attacks are focused on attacking the network layers that are used to transport data with an Ethernet cable. Some of these threats and attacks are MAC flooding attacks, DoS/DDoS threat, spoofing, Man in the Middle attack, ARP attacks, brute force password guessing attacks, tampering, spanning-tree protocol attacks, eavesdropping, packets sniffing, and device password crack. Attacks usually exploit various techniques to find and discover vulnerable targets in the network. To minimize the vulnerability of the threats, various security mechanisms are implemented such as firewalls; intrusion detection and prevention systems (IDS/IPS); planning, configuration, and administration; detection of DoS; and Man-in-the-Middle attack countermeasure. These mechanisms use defensive measures and techniques to prevent the exploitation of cyberattacks and threats.

# Chapter 4: Benchmark Testing on Emulating a Substation with Multiple Different Switch and Topology Combinations

This chapter evaluates the viability of different Ethernet switches and network topologies to transport frames for real-time applications via simulation testing. As discussed in Chapter 3, several topology schemes and Ethernet switch types can be combined together to transport a GOOSE message. The tests performed in this chapter validate the integrity of GOOSE messages (packet loss) and the speed of their transmission. In addition, this chapter includes a description of the test methodology, results, and analysis.

## 4.1 Testing Method

The objective of the emulation-based testing is to:

- Determine the speed of GOOSE message communication.
- Assess the reliability of the GOOSE message in four switch types.
- Assess the reliability of the GOOSE message in two topologies.

The testing outcomes mentioned above serve as the basis for validating the reliability of different option for transferring GOOSE messages in a substation network. Evaluating the reliability of a GOOSE message involves several steps that can be very complex. The objective of these tests was to verify the performance of the substation network using GOOSE messages in multiple topologies and switch types under normal and abnormal conditions. To accomplish this, several tests were set up where the style of network topology, communication network load, and the type of Ethernet switch were varied to obtain a good scale of results that could analyzed. To validate the performance, the speed of the messages was measured while varying the parameters mentioned above.

This requires validation of whether the Ethernet switch type and multiple topology schemes are good enough and not too difficult to implement and maintain for transmitting GOOSE or SV messages in the substation. For such validation, the equipment to use must be the same as or have characteristics equal to that found in electrical substations network. However, this equipment is hard to get, especially the variations of Ethernet switches that can be used in this test, because of the high cost and space and implementation limitations. Therefore, a real-time network simulation for pre-deployment testing is assumed to be close enough to act as a real substation network without the need for network hardware. The emulation systems are easy to use and has multiple options and variations to design and built network communications of any size. One of the simulation tools is the GNS3 network simulator, which was used in the testing [24]. The GNS3 simulator models the substation architecture by simulating IED nodes according to IEC 61850, as shown in Figure 22.

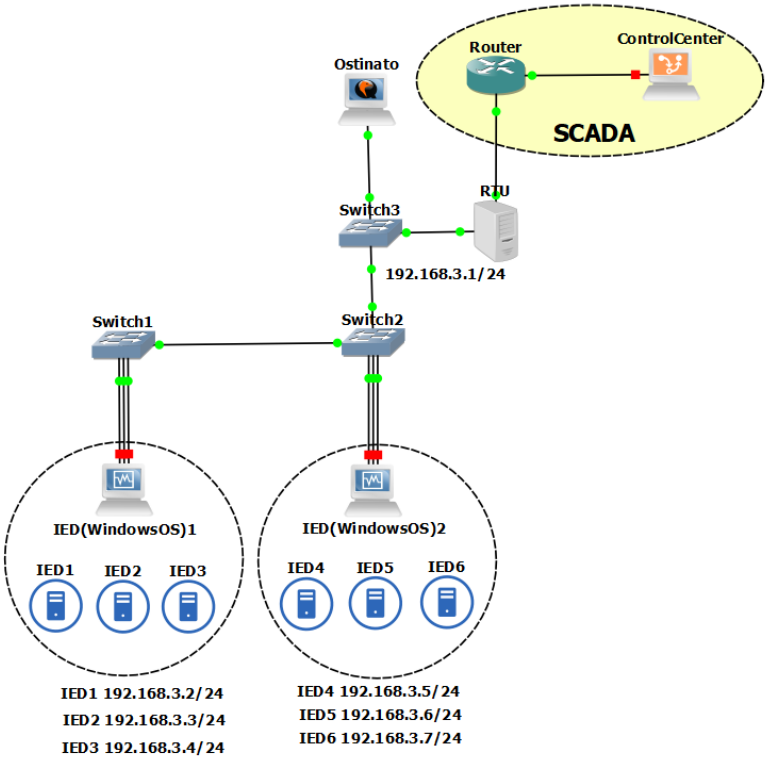


Figure 22. GNS3 Substation Communications Network

There are two IED nodes; each IED node is a simulator itself which ran a Windows XP environment, where each Windows OS contains an “IEDScout” simulator [25]. The IED Scout software is a tool for protection and substation automation and can simulate an IED and enable users to test IED performance. Each IED Scout instance will simulate three IEDs, where each one of them will have an IP address. So, the total IEDs that are simulated will be 6 IEDs in this designed substation. Each IED in the IED Scout simulator is connected into a subnet that transmits GOOSE messages on separate adapter links (each having multiple ports). All IEDs are connected to three emulated Ethernet switches, as shown in Figure 22.

## 4.2 Equipment Utilized.

There were several specialized pieces of software used to conduct the tests presented in this chapter. Figure 23 displays an overview of the setup used. In total, there was 1 computer, 2 simulators, 6 IEDs, 2 applications, and wiring.

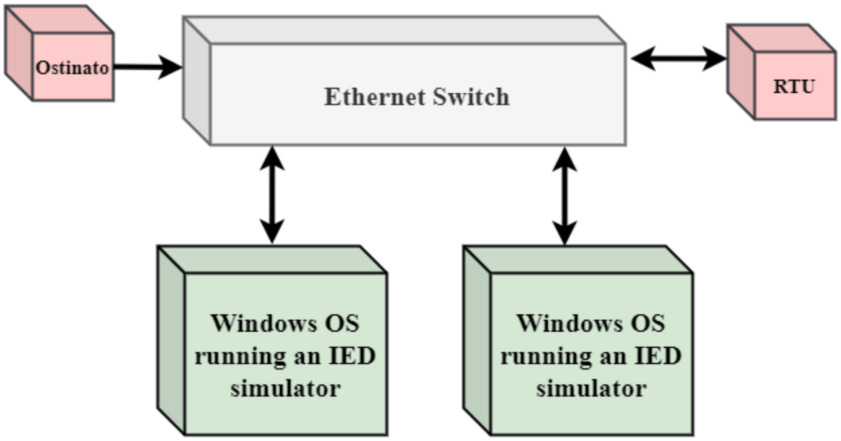

Ostinato
Ethernet Switch
RTU
Windows OS running an IED simulator
Windows OS running an IED simulator

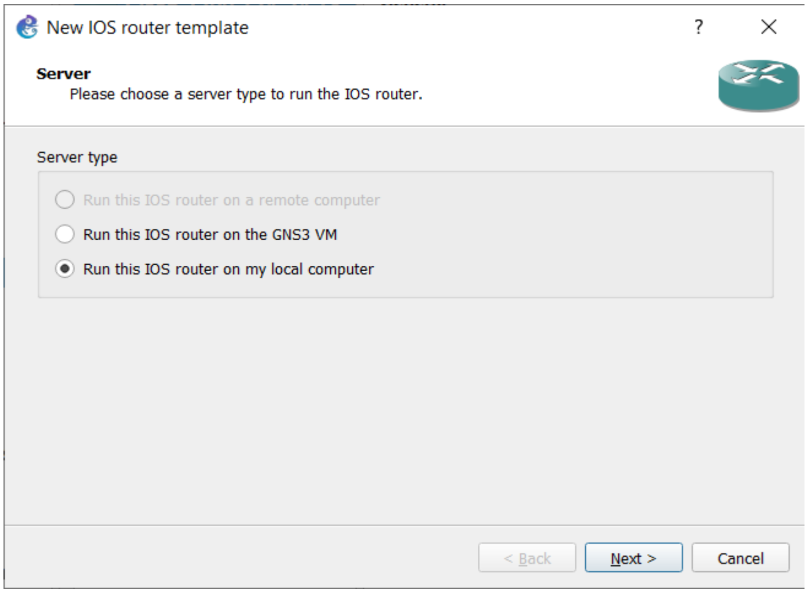
Figure 23. Simulated Test Equipment

### 4.2.1 GNS3

GNS3 [24] is an open-source network configuration tool that enables network engineers to create and test virtual and real networks. It works seamlessly with various configurations and hardware and allows running of a small number of devices in multiple topologies and configurations in a single window. GNS3 consists of two software components: The GNS3-all-in-one software (GUI) and the GNS3 virtual machine (VM). GNS3-all-in-one is the client part of GNS3 and is a graphical user interface (GUI). It can be installed as all-in-one software on a local PC (Windows, Mac, Linux) and some system topologies can be created using this software. When creating topologies in GNS3 using the GUI client, the devices that have been created need to be hosted and run by a server process. There are a few choices for the server part of the software:

1. Local GNS3 server
2. Local GNS3 VM
3. Remote GNS3 VM

The local GNS3 server runs locally on the same PC where the GNS3 is installed as all-in-one software. Both the GNS3 GUI and the local GNS3 server run as processes using the Windows operating system. Additional processes such as Dynamips will be running on the same PC. Dynamips is an older version of the Cisco hardware emulation technology. It uses actual Cisco IOS images, which is an excellent choice for basic CCNA topologies, but it has several limitations, such as supporting older versions of the Cisco IOS only. Choosing the GNS3 VM (recommended), as shown in Figure 24, means it can either run the GNS3 VM locally on a PC using virtualization software such as Virtual box, VMware Workstation; or it can be running the GNS3 VM remotely on a server using VMware such as ESXi [24].



New IOS router template

**Server**

Please choose a server type to run the IOS router.

Server type

○ Run this IOS router on a remote computer

○ Run this IOS router on the GNS3 VM

● Run this IOS router on my local computer

Figure 24. GNS3 VM

The GNS3 tool supports both emulated and simulated devices. The emulation device in GNS3 emulates a hardware device and runs actual images on the virtual device. For instance, a copy of the Cisco IOS from a real physical Cisco switch can be run on a simulator and emulates a Cisco switch using images in GNS3. A simulation device simulates the characteristics and functionality of an Ethernet switch that can be running an actual operating system (such as Cisco IOS). In addition, a simulated device developed by GNS3 can act like built-in layer 2 and layer 3 Ethernet switches. As mentioned, GNS3 is open-source software that can be downloaded and used free with no monthly or yearly license fees. In addition, there is no limitation on number of devices supported, other than limitations in the CPU and memory size for the computer running the software.

GNS3 supports multiple switching options in VIRL images [26] such as IOU/IOL Layer 2, IOSv, IOS-XRv, IOSvL2, etc. It can support a hypervisor such as a VMware workstation and Virtual box. However, the Cisco images need to be supplied and downloaded by users, but some images can be downloaded for a price. The GNS3 is not a self-contained package but needs a local installation of software (GUI). In addition, GNS3 can be affected and limited by the PC’s setup local installation, such as firewall and security settings.

### 4.2.2 IEDScout

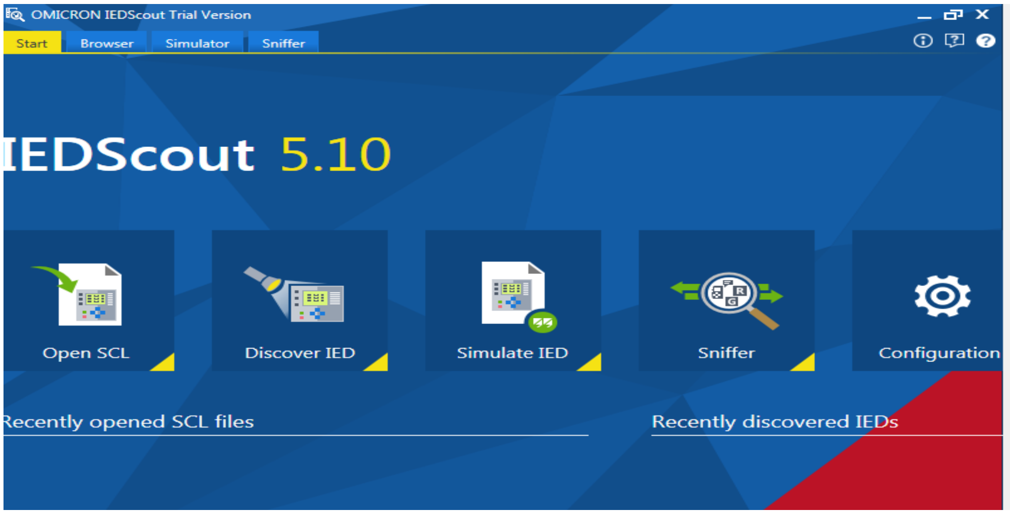
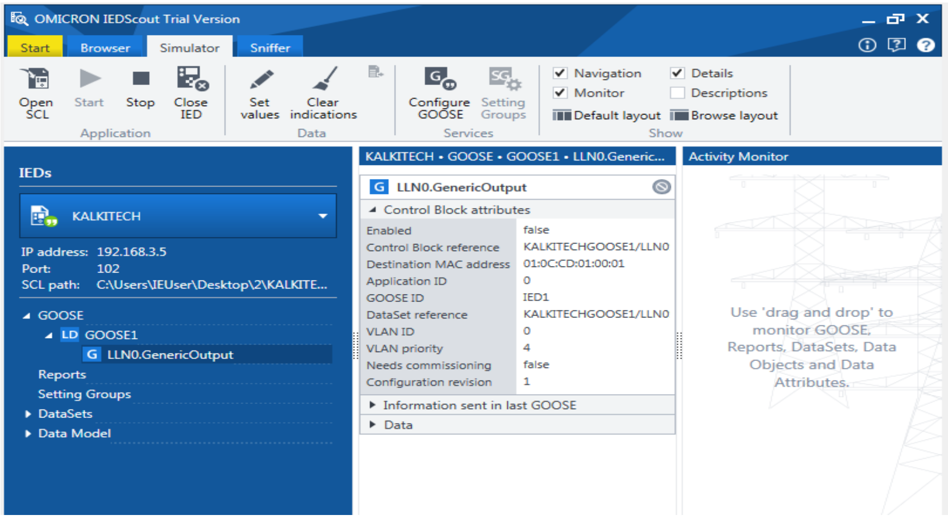


Figure 25. IEDScout Simulator User Interface

IED Scout [26] is a software tool for simulating protection and substation automation that works with IEC61850 capable devices. It offers access to IEDs and performs typical operational tasks when working with them. A user interface supports finding all relevant information of all IEDs. The software allows the engineer to look inside the simulated IED and its communication both physically and digitally. Whole IEDs, including their server and GOOSE message, can be simulated based on their Substation Configuration Language (SCL) file. SCL is a language and representation format that is used for the representation of characteristics of electrical transformers and other electrical devices used in a substation. The data values can be changed and device configurations can set also. In addition, both test mode and simulation signals are supported. An IED can be represented based on its SCL file. The IED can send a GOOSE message with a “test/simulation” indication and can shift between different modes/behaviors. It can import an SCL file and IED Scout will automatically configure IP and port settings as shown in Figure 26. In addition, it can import more than one SCL file at the same time; therefore, in the case at hand, three SCL files are imported.



☑ Navigation ☑ Details
☑ Monitor □ Descriptions
Default layout Browse layout

IEDs

KALKITECH

IP address: 192.168.3.5
Port: 102
SCL path: C:\Users\IEUser\Desktop\2\KALKITE...

- GOOSE
  - LD GOOSE1
    - G LLN0.GenericOutput
- Reports
- Setting Groups
- DataSets
- Data Model

KALKITECH • GOOSE • GOOSE1 • LLN0.Generic...

G LLN0.GenericOutput

Control Block attributes

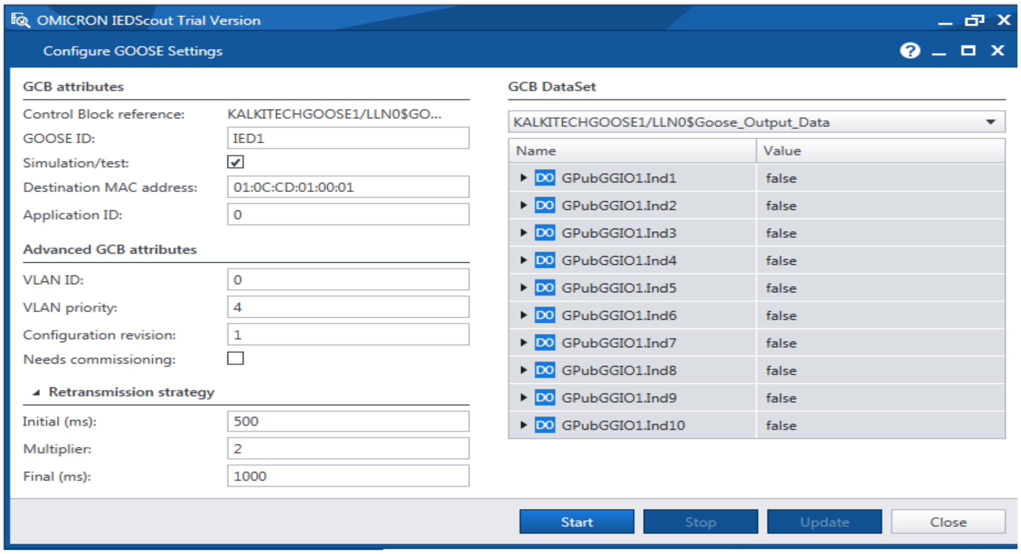
| | |
|---|---|
| Enabled | false |
| Control Block reference | KALKITECHGOOSE1/LLN0 |
| Destination MAC address | 01:0C:CD:01:00:01 |
| Application ID | 0 |
| GOOSE ID | IED1 |
| DataSet reference | KALKITECHGOOSE1/LLN0 |
| VLAN ID | 0 |
| VLAN priority | 4 |
| Needs commissioning | false |
| Configuration revision | 1 |

Information sent in last GOOSE

Data

Figure 26. IEDScout Imports a SCL File

As shown in Figure 27, IED Scout allows the user to configure the GOOSE settings manually. As shown in Figure 27, “GOOSE ID” is the name of the IED. It has a destination MAC address. The retransmission strategy defined in the standard has three elements: initial, multiplayer, and final. The "initial" is the first frame that will be transmitted or broadcasted in the network at 500 x 4 ms. The same frame will be retransmitted, but with a time doubling because there is 2 in a "multiplayer" square. However, the “final” box means the last time that the tool will keep sending frames at the final time period until it receives a command to stop transmitting from another IED or it is stopped manually. In this test setup, the final time will be doubled, and the tool will keep sending frames in each 2000 ms until the user presses stop button. After setting up the GOOSE configurations, each IED will transmit through an adapter using their IP addresses and ports as shown in the server settings in Figure 28. By pressing start, the simulated IED will immediately broadcast the GOOSE messages at the time of the initial frame transmission strategy.



GCB attributes

| | |
|---|---|
| Control Block reference: | KALKITECHGOOSE1/LLN0$GO... |
| GOOSE ID: | IED1 |
| Simulation/test: | ☑ |
| Destination MAC address: | 01:0C:CD:01:00:01 |
| Application ID: | 0 |

Advanced GCB attributes

| | |
|---|---|
| VLAN ID: | 0 |
| VLAN priority: | 4 |
| Configuration revision: | 1 |
| Needs commissioning: | ☐ |

Retransmission strategy

| | |
|---|---|
| Initial (ms): | 500 |
| Multiplier: | 2 |
| Final (ms): | 1000 |

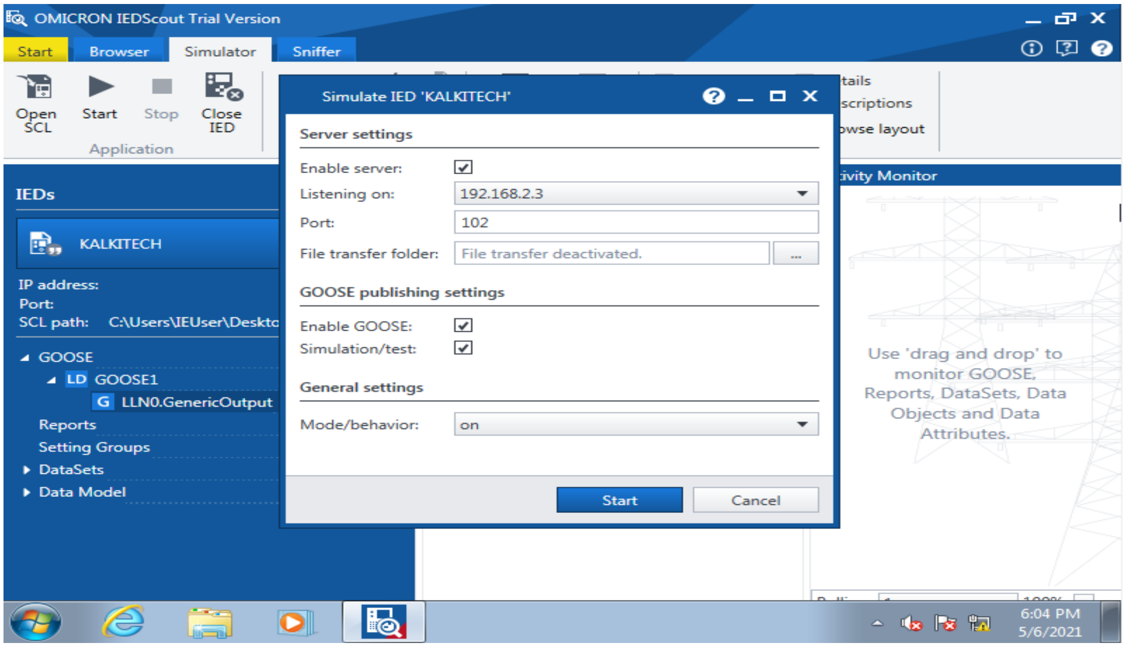
GCB DataSet

KALKITECHGOOSE1/LLN0$Goose_Output_Data

| Name | Value |
|---|---|
| DO GPubGGIO1.Ind1 | false |
| DO GPubGGIO1.Ind2 | false |
| DO GPubGGIO1.Ind3 | false |
| DO GPubGGIO1.Ind4 | false |
| DO GPubGGIO1.Ind5 | false |
| DO GPubGGIO1.Ind6 | false |
| DO GPubGGIO1.Ind7 | false |
| DO GPubGGIO1.Ind8 | false |
| DO GPubGGIO1.Ind9 | false |
| DO GPubGGIO1.Ind10 | false |

Figure 27. GOOSE Configuration Settings

The benefits of using IED Scout are that it can be an extremely cyber-secure and powerful environment and can be installed in a Windows PC operating in isolation from a substation network for testing and development purposes. In addition, it can simulate a dozen or more IEDs with their real IP addresses. However, it is not free software, a user can run on a free trial for 30 days; after that they need to purchase a license.



IEDs

KALKITECH

IP address:
Port:
SCL path: C:\Users\IEUser\Deskto

- GOOSE
  - LD GOOSE1
    - G LLN0.GenericOutput
- Reports
- Setting Groups
- DataSets
- Data Model

Server settings

| | |
|---|---|
| Enable server: | ☑ |
| Listening on: | 192.168.2.3 |
| Port: | 102 |
| File transfer folder: | File transfer deactivated. |

GOOSE publishing settings

| | |
|---|---|
| Enable GOOSE: | ☑ |
| Simulation/test: | ☑ |

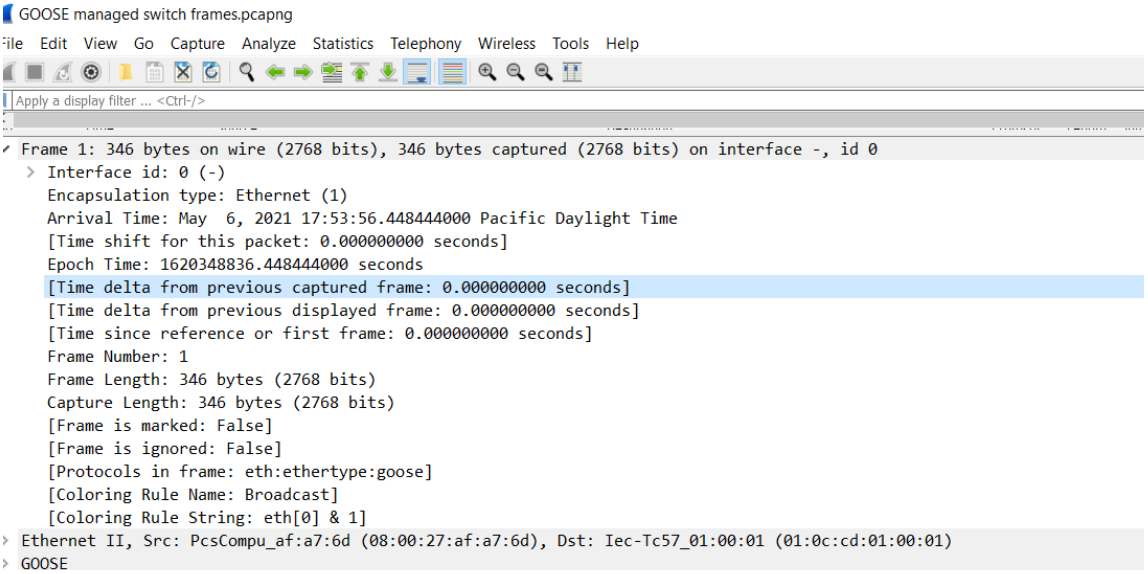
General settings

| | |
|---|---|
| Mode/behavior: | on |

Figure 28. Server Settings

### 4.3 Test Overview

After explaining the simulation tools and their mechanisms, this section will dive deep into the procedures for the tests. The first objective of this testing is to examine the different Ethernet switches and network topologies that could increase the performance of the substation network. All speed data, numbers of packets, and average time for each Ethernet switch are measured and compared. The second objective is to measure the performance of the IEDs in networks with different topologies and numbers of Ethernet switch in substation systems. For this testing, an additional tool was used. Wireshark [27] is an open-source network analyzer tool that can measure the bandwidth utilization by recording the number of frames captured per second and present the information.


GOOSE managed switch frames.pcapng
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
Frame 1: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface -, id 0
  Interface id: 0 (-)
  Encapsulation type: Ethernet (1)
  Arrival Time: May  6, 2021 17:53:56.448444000 Pacific Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1620348836.448444000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 346 bytes (2768 bits)
  Capture Length: 346 bytes (2768 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:goose]
  [Coloring Rule Name: Broadcast]
  [Coloring Rule String: eth[0] & 1]
Ethernet II, Src: PcsCompu_af:a7:6d (08:00:27:af:a7:6d), Dst: Iec-Tc57_01:00:01 (01:0c:cd:01:00:01)
GOOSE
```

Figure 29. GOOSE Message Protocol Sample Capture

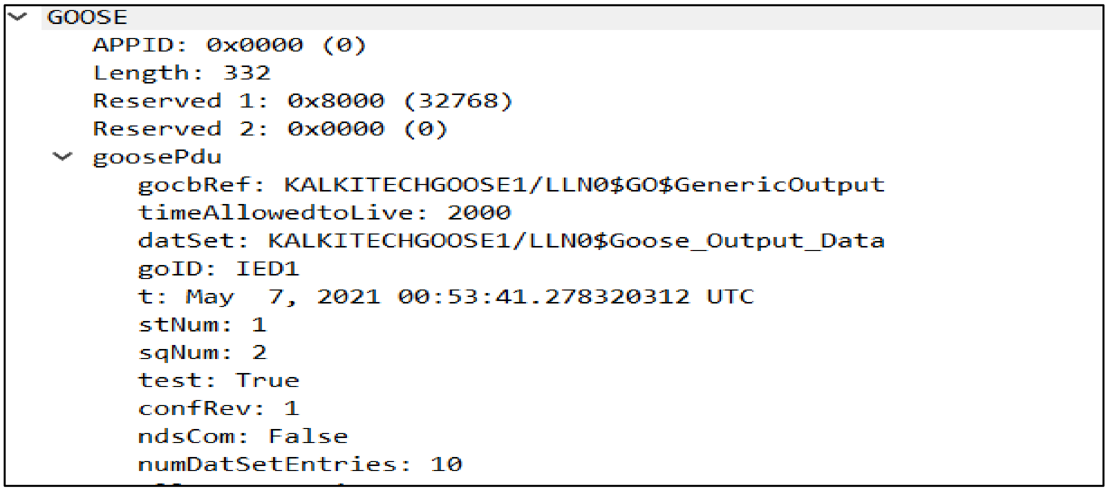
The frame that holds a GOOSE message is an important component of any network test. The frame size and frequency are both factors that may affect the performance of GOOSE messages. The Ethernet frame that holds a GOOSE message is thus a major key to this testing, as frame size and frequency are two elements that influence congestion in a network. Figure 29 describes the information and data size inside a GOOSE message frame. Note that the size of the GOOSE frame, in this case, is 346 bytes. There are three-time setups shown in Figure 29: time delta from the previously captured frame, time delta from the previously displayed frame, and time since reference or first frame. The delta from the previously captured frame (Tc) is the time between two transmitting packets, specifically the second packets time stamp minus that of the first packet of all of the packets that got captured by the Wireshark tool. For example, the tool captured not only the GOOSE messages but other frames that are transmitted as part of network operation. There are ARP frames, UDP, etc. When the tool calculates the time here, it is only GOOSE packets time minus any packets that have been shown in the capture. On the other hand, time delta from the previously displayed frame (Td) is the time between two packets of the frame number 2 minus frame number 1 after the tool filtered and captured a specific frame protocol. For example, the GOOSE message filter will show only the GOOSE messages, and the time delta calculation acts on two consecutive GOOSE frames. Equations (7) and (8) shows formulas for calculating times:

*Tc= Time of captured packet N – Time of captured previous packet N-1* (7)

*Td= Time of displayed packet N – Time of displayed previous displayed packet N-1* (8)

The time since reference or first frame, is the time that the tool first captured a GOOSE frame in the present test sequence.

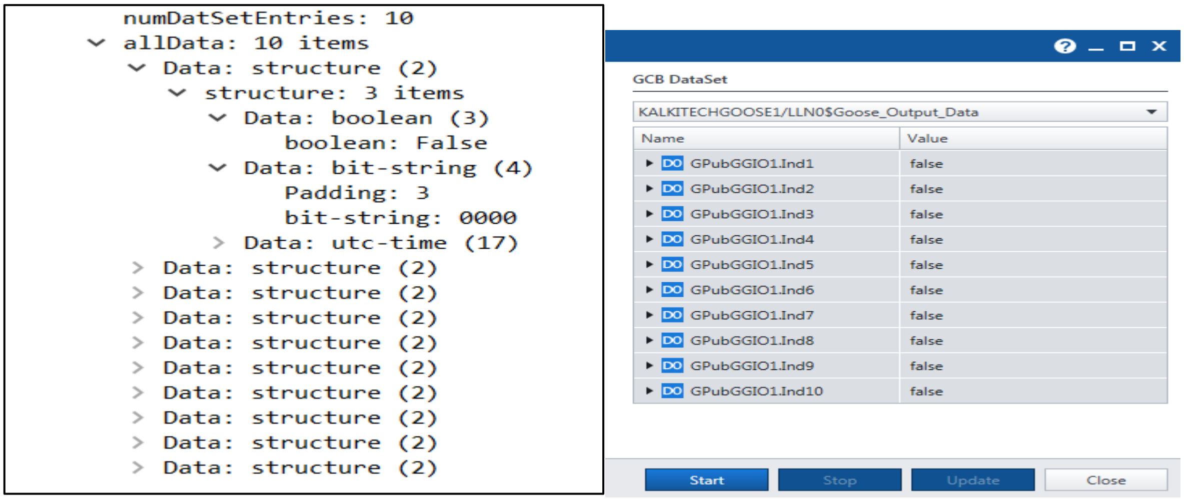
Figure 30 shows that the GOOSE frame has a field named “gocbRef” which is represented in the GOOSE protocol data unit (PDU). The first name before the slash in the “gocbRef” represents the IED name of the device “KLAKITECHGOOSE1” and the control block reference that is publishing this message. The IED name is an IED Scout simulator file that imports an SCL file representing an IED as was explained in the previous section. “goID” is the name of the GOOSE message. “stNum” is a number that is incremented by one every time an analog signal changes its state. For example, when an IED sends a GOOSE message with the same state, the number will be the same. However, when the IED sends a GOOSE frame where the state changed, the state number will increase by 1. “sqNum” indicates that how many times the signal has been transmitted before it stopped. “Test” implies that the signal is under the test mode, and it is not in real-time GOOSE message mode, so it says “True”. In this test Figure 30 shows the signal is in test mode. “confRev” is the number of changes that happened in the GOOSE messages. “ndsCom” is a commission, which is a password permission request, which shows “False” on Figure 30. “numDatasetEntries” is indicating the number of entries in the dataset sent by the simulator IED Scout as shown in Figure 31.



```
GOOSE
    APPID: 0x0000 (0)
    Length: 332
    Reserved 1: 0x8000 (32768)
    Reserved 2: 0x0000 (0)
    goosePdu
        gocbRef: KALKITECHGOOSE1/LLN0$GO$GenericOutput
        timeAllowedtoLive: 2000
        datSet: KALKITECHGOOSE1/LLN0$Goose_Output_Data
        goID: IED1
        t: May  7, 2021 00:53:41.278320312 UTC
        stNum: 1
        sqNum: 2
        test: True
        confRev: 1
        ndsCom: False
        numDatSetEntries: 10
```

Figure 30. GOOSE Message Frame Data

The frame in Figure 31 includes 1 Boolean variable and 1 Bit stream, which is a variable that contains 2 bytes where each bit symbolizes a flag with a meaning. The first variable is the Boolean variable, which represents the trip signal of the device that is "publishing" this message. A "0" value means a false signal and represents the trip signal that is de-activated. A "1" value is a true signal and represents the energized trip signal. Note that the payload of the message does not matter in this test where the objective is to measure the speed at which the frame transits the network.



```
        numDatSetEntries: 10
      allData: 10 items
        Data: structure (2)
          structure: 3 items
            Data: boolean (3)
                boolean: False
            Data: bit-string (4)
                Padding: 3
                bit-string: 0000
            Data: utc-time (17)
        Data: structure (2)
        Data: structure (2)
        Data: structure (2)
        Data: structure (2)
        Data: structure (2)
        Data: structure (2)
        Data: structure (2)
        Data: structure (2)
        Data: structure (2)
```

GCB DataSet

KALKITECHGOOSE1/LLN0$Goose_Output_Data

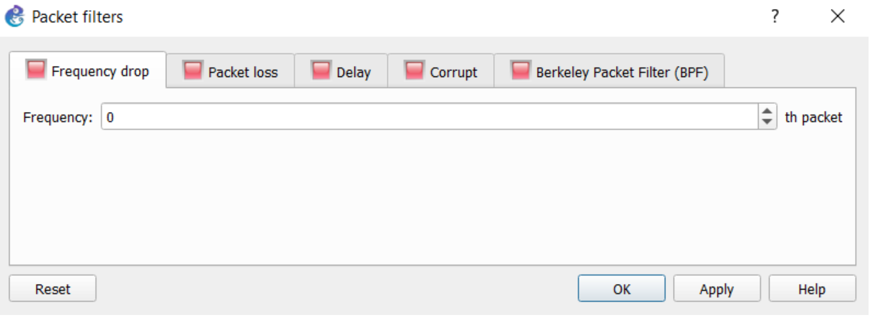
| Name | Value |
|---|---|
| DO GPubGGIO1.Ind1 | false |
| DO GPubGGIO1.Ind2 | false |
| DO GPubGGIO1.Ind3 | false |
| DO GPubGGIO1.Ind4 | false |
| DO GPubGGIO1.Ind5 | false |
| DO GPubGGIO1.Ind6 | false |
| DO GPubGGIO1.Ind7 | false |
| DO GPubGGIO1.Ind8 | false |
| DO GPubGGIO1.Ind9 | false |
| DO GPubGGIO1.Ind10 | false |

Figure 31. GOOSE Message Attributes

The above-mentioned setup was tested and yielded repeatable results. As a first step, we imported the operating system Windows XP in the GNS3 simulator. We used two operating systems because the size and capacity of the CPU on the computer running the test can only run three IED at the same time. Inside each OS an IED Scout simulator was used and ran three

IEDs by importing an SCL file downloading it from the SmartIED website [28]. After that, topologies were designed in order to test each switch type as shown in Figure 22. We then configured the IED Scout as we wanted it, leaving it as general as possible.

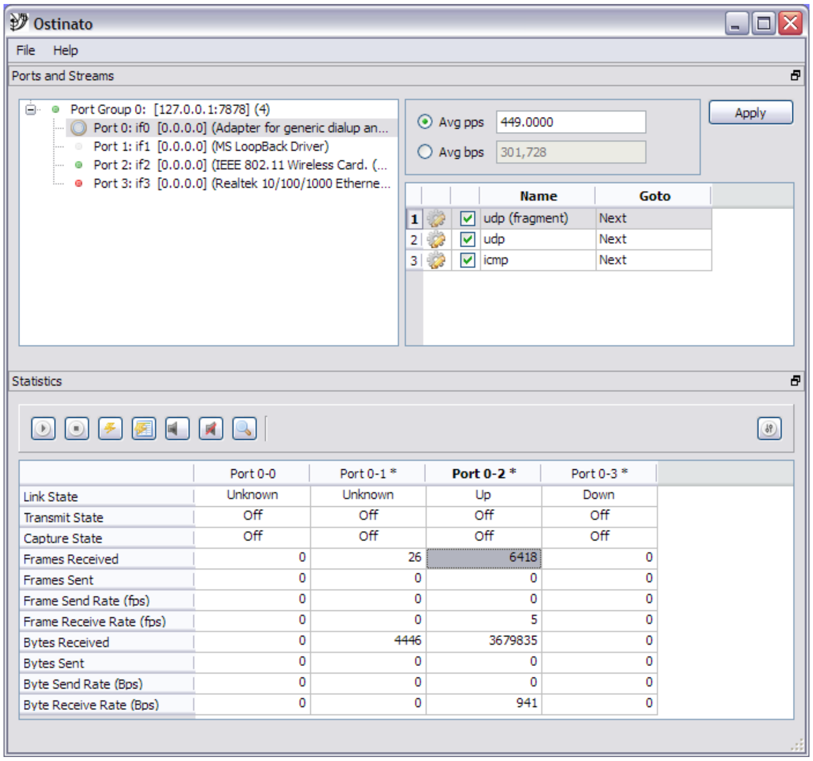
The first scenario tested was that had was no network load, and no filter was added. The four switches in two topologies will be examined. The second scenario was the same topologies and switches with network load, and no filter was added. The following load variations were added, and the tests repeated: a test for high network load with frames of small size (64 bytes) and another test for high network load with frames of large size (1500 bytes). Therefore, multiple messages sent at the same time create congestion within a very small amount of time. The third scenario was the same as the two before; however, a filter was added to observe will happen to the network in abnormal events. Figure 32 shows the filter that was added to the GNS3 filter. The "Frequency drop" is a probability that will drop every packet that have a -1 frequency, so here we added 5%. "Delay" symbolizes the latency, which is the amount of time that it takes for data to travel from the source to destination, and the other is jitter, which is the change in time delay for data packets sent over a network. For the latency, we added 3 and jitter was 2, to be as minimum as possible. for the settings for "Corrupt" and "Berkeley packet filter (BPF) were not used in the test. "Corrupt" represents the percentage chance that a given packet out of the full set will be corrupted. "Berkeley packet filter (BPF)" indicates the drop of any packet that is expressed in the blank. For example, if we put GOOSE in BPF it would drop all packets that in GOOSE messages format and they will never be delivered.



Frequency: 0 th packet

Figure 32. GNS3 Packets Filters Content

In the case of network load tests, the simulator runs an application called Ostinato, as shown in Figure 33. It provides the ability to generate high-volume Ethernet traffic. This test is added because of the possibility of the worst-case scenario that could happen where other spurious network traffic from a DoS attack is transmitted by the switch before the GOOSE could be transmitted. The tool is used to generate and custom frames to load in the network and generate high-volume Ethernet traffic, enabling the custom formation of frames. This feature allows the user to set the size and content of frames for each network connection. The variation of the test results represented in the simulators proved to be accurate and comprehensive as possible. In addition, the conditions that affect GOOSE messages include failure of a switch, failure of a cable that connects an IED to a switch, and network traffic missing from the test.



Port Group 0: [127.0.0.1:7878] (4)
- Port 0: if0 [0.0.0.0] (Adapter for generic dialup an...
- Port 1: if1 [0.0.0.0] (MS LoopBack Driver)
- Port 2: if2 [0.0.0.0] (IEEE 802.11 Wireless Card. (...
- Port 3: if3 [0.0.0.0] (Realtek 10/100/1000 Etherne...

● Avg pps 449.0000
○ Avg bps 301,728

| | | Name | Goto |
|---|---|---|---|
| 1 | ☑ | udp (fragment) | Next |
| 2 | ☑ | udp | Next |
| 3 | ☑ | icmp | Next |

| | Port 0-0 | Port 0-1 * | Port 0-2 * | Port 0-3 * |
|---|---|---|---|---|
| Link State | Unknown | Unknown | Up | Down |
| Transmit State | Off | Off | Off | Off |
| Capture State | Off | Off | Off | Off |
| Frames Received | 0 | 26 | 6418 | 0 |
| Frames Sent | 0 | 0 | 0 | 0 |
| Frame Send Rate (fps) | 0 | 0 | 0 | 0 |
| Frame Receive Rate (fps) | 0 | 0 | 5 | 0 |
| Bytes Received | 0 | 4446 | 3679835 | 0 |
| Bytes Sent | 0 | 0 | 0 | 0 |
| Byte Send Rate (Bps) | 0 | 0 | 0 | 0 |
| Byte Receive Rate (Bps) | 0 | 0 | 941 | 0 |

Figure 33. Ostinato Traffic Generator Tool

## 4.4 A Summary of the Variation Ethernet Switch and Topology

Chapter 3 described the details of types of Ethernet switch and topologies designs. This section will summarize the variety of switches and topologies that are simulated in GNS3 for the test. The first test is a serial topology using a three-hub switch connecting with 6 IEDs that are broadcasting GOOSE messages, as will be described in Section 4.5. In the serial or cascading architecture, each switch is connected to the next switch in the cascade, like a series of switches that are connected via one of its ports. A hub is a network hardware device that can connect multiple Ethernet devices. It has multiple input and output ports, and it acts as a single network segment.

After that, it the same network design will be studied using unmanaged switches in Section 4.5.2. An unmanaged switch is simple, and it is a plug-and-play device where no configuration interface or options that are needed. In addition, it has an in-built quality of service self-test function to make sure it is working completely. Then a managed switch IOU layer 2 will be added, as described in Section 4.5.3. A managed switch has one or more methods to modify its operation. Common management methods include a command-line interface or a web interface. These can be used to modify the configuration of the switch. In addition, some of the features that can programmed in a managed switch are Rapid Spanning Tree Protocol, port mirroring, and others.

The last switch studied will be a Software-Defined Network (SDN) switch. A SDN is a network architecture framework that separates the network control from the main network, moving forwarding and transporting underground so that programmers could program the network control in a straightforward way without any obstacles [15]. Section 4.5.4 shows results with an OpenFlow switch with management connectivity with the command order coming from to an OpenFlow switch.

The second network design is a star topology using the same switch types described above in the same order with 6 IEDs broadcasting GOOSE messages. The case results with the star topology are shown in Section 4.5.1.2.  Switch 3 is referred to as the ‘Central’ or master switch since all the other switches connected give it a star form configuration. Table 1 lists the various tests of the substation communication network conducted; however, the results will be divided in two tables. One table presents results without a filter, as explained at the end of the previous section, and a second table with the filter settings described above to represent disruptions of packet flow on the network.

| Test IEDs | Zero network load | | | With a network load of packets with 64 byte frames | | | With a network load of packets with 1500 byte frames | | |
|---|---|---|---|---|---|---|---|---|---|
| Topology | 2 IED | 4 IED | 6 IED | 2 IED | 4 IED | 6 IED | 2 IED | 4 IED | 6 IED |
| Serial | Hub switch | | | Hub switch | | | Hub switch | | |
| | Unmanaged switch | | | Unmanaged switch | | | Unmanaged switch | | |
| | Managed switch | | | Managed switch | | | Managed switch | | |
| | SDN switch | | | SDN switch | | | SDN switch | | |
| Star | Hub switch | | | Hub switch | | | Hub switch | | |
| | Unmanaged switch | | | Unmanaged switch | | | Unmanaged switch | | |
| | Managed switch | | | Managed switch | | | Managed switch | | |
| | SDN switch | | | SDN switch | | | SDN switch | | |

Table 1. Test Strategy

### 4.5 Tests and Test Results

The following section represents the results obtained during the simulation benchmark testing and the analysis of the results.

#### 4.5.1 Hub Switch

The first test followed the method described in Section 4.1, where a hub switch is used to transmit a GOOSE message from multiple IEDs. Tests 1 and 4 did not include any network traffic other than the GOOSE message itself. Tests 2, 3, 5 and 6 are included a network load of nearly 97%. In addition, the frames used to generate traffic that carried a payload of 64 bytes in tests 2 and 5 and 1500 bytes in tests 3 and 6. The results tables display the slowest captured message (Maximum time), the fastest message (Minimum time), and the average measured time. Many tests were conducted; the results are listed in Table 2. Figure 36 displays the chart of the speed of network traffic transmission.

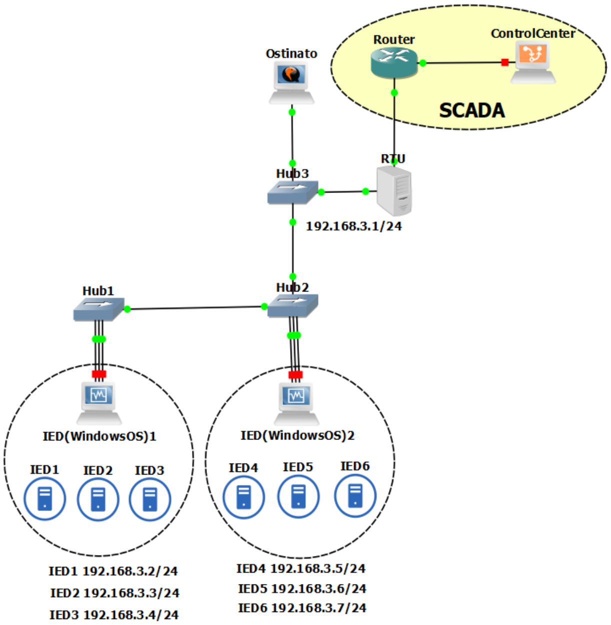


Figure 34. Serial Topology Using Hubs

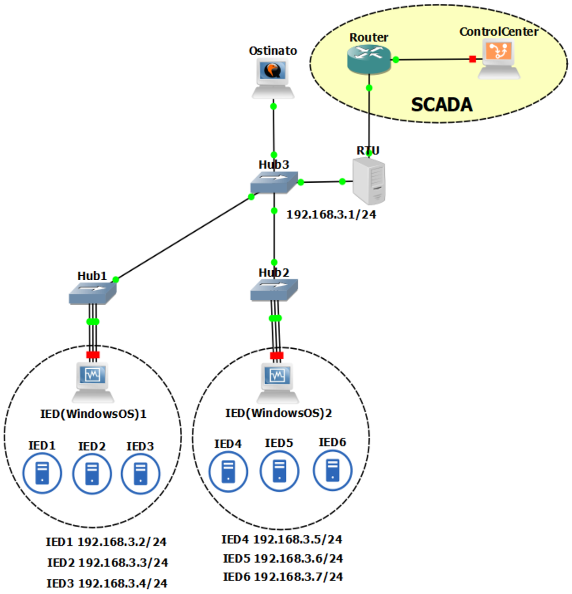


Figure 35. Star Topology Using Hubs

#### 4.5.1.1 Serial Topology

The first topology is a serial or cascaded topology as shown in Figure 34, where three switches are connected sequentially.

- **Test 1: Serial Topology, Hub Switch, Zero Network Load and No Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.1808 | 0.9197 | 10.886 | 0.0624 | 0.8302 | 0.0626 | 7.0089 | 0.8905 | 0.3749 | 0.2666 | 0.3628 | 0.3455 |
| Minimum time (s) | 0.0009 | 0.0784 | 0.1238 | 0.0001 | 0.1534 | 0.0001 | 0.0292 | 0.1230 | 0.1083 | 0.0302 | 0.0001 | 0.2027 |
| Average time (s) | 0.4620 | 0.5342 | 0.4022 | 0.01116 | 0.7413 | 0.0270 | 0.1855 | 0.2508 | 0.2027 | 0.2005 | 0.0556 | 0.2922 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average Time | 0.4981 | | 0.2954 | | | | 0.1979 | | | | | |

Table 2. Serial Topology, Hub Switch, Zero Network Load and No Filters

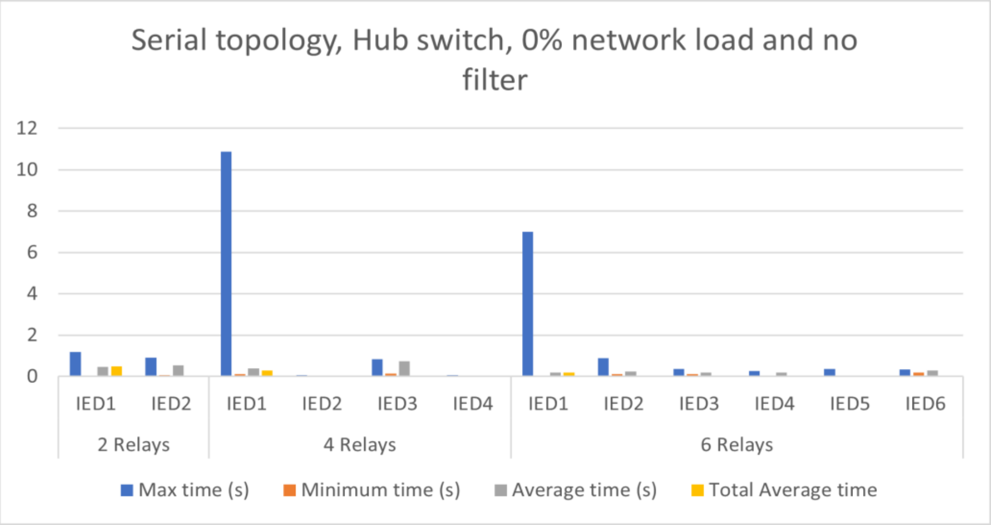


Figure 36. Serial Topology Using Hub Time Measure in Test 1

- **Test 2: Serial Topology, Network Load with 64 Bytes and No Filter**

The Ostinato tool described on the previous section was used to generate traffic with frame sized at 64 bytes that were carried through the switches requiring them to handle a small frames and deal with a higher number of frames per second.

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.9838 | 0.7154 | 0.2440 | 0.6251 | 0.3141 | 0.1265 | 0.3485 | 0.2805 | 0.1864 | 0.2689 | 0.5244 | 0.2522 |
| Minimum time (s) | 0.0009 | 0.0001 | 0.0117 | 0.0009 | 0.0078 | 0.0001 | 0.0001 | 0.0053 | 0.0001 | 0.0076 | 0.0068 | 0.0009 |
| Average time (s) | 0.4581 | 0.0623 | 0.1153 | 0.4045 | 0.2198 | 0.0611 | 0.0788 | 0.1755 | 0.1275 | 0.2010 | 0.2726 | 0.0745 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.2602 | | 0.2002 | | | | 0.1550 | | | | | |

Table 3. Serial Topology, Hub Switch, with 64 Bytes Frame Size Network Load and No Filter

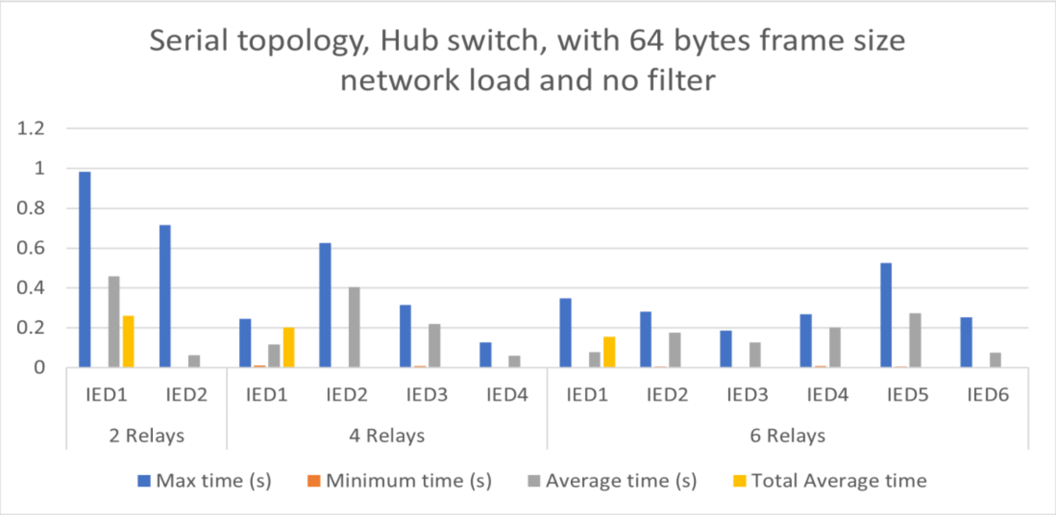


Figure 37. Serial Topology Using Hub Time Measure in Test 2

- **Test 3: Serial Topology, Network Load With 1500 Bytes and No Filter**

This test would be the same as test 2, but now the Ostinato tool generates packets with a maximum total frame size of 1500 bytes that were carried through the switches causing them to handle large frames, and deal with a higher number of frames per second.

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.2030 | 0.8593 | 0.6358 | 0.4685 | 0.2009 | 0.4865 | 0.3183 | 0.4428 | 0.3286 | 0.1715 | 0.3136 | 0.2284 |
| Minimum time (s) | 0.0461 | 0.0156 | 0.0009 | 0.0107 | 0.0029 | 0.0001 | 0.0117 | 0.0029 | 0.0039 | 0.0096 | 0.0117 | 0.0085 |
| Average time (s) | 0.1272 | 0.4458 | 0.3769 | 0.2005 | 0.0563 | 0.1458 | 0.1933 | 0.1461 | 0.2154 | 0.0811 | 0.2131 | 0.0798 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.2865 | | 0.1949 | | | | 0.1548 | | | | | |

Table 4. Serial Topology, Hub Switch, with 1500 Bytes Frame Size Network Load and No Filter

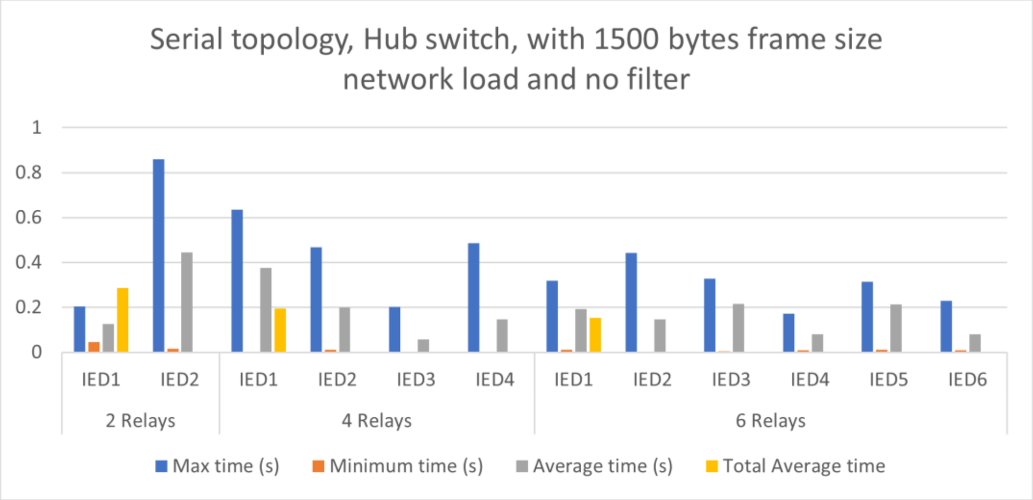


Figure 38. Time Measure of Serial Topology Using Hub in Test 3

- **Test 4: Serial Topology, Zero Network Load, With Filter**

This test used a filter as explained in Section 4.3, to evaluate the impact of non-ideal network behavior for these switches under these specific conditions to see the impact on performance, speed, and response of the switches.

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 2.2723 | 1.0205 | 2.0133 | 1.0008 | 0.9641 | 0.9491 | 11.995 | 1.0123 | 0.2482 | 0.7808 | 0.4196 | 0.8607 |
| Minimum time (s) | 0.0019 | 0.0006 | 0.0001 | 0.0009 | 0.0078 | 0.0585 | 0.0019 | 0.0019 | 0.0029 | 0.0078 | 0.0253 | 0.0087 |
| Average time (s) | 0.5151 | 0.7996 | 0.1708 | 0.6008 | 0.3950 | 0.1473 | 0.4636 | 0.1225 | 0.1187 | 0.0825 | 0.2843 | 0.4968 |
| No. of lost packets | 21 | 25 | 21 | 23 | 25 | 23 | 17 | 39 | 33 | 32 | 34 | 19 |
| Total average time | 0.9032 | | 0.2886 | | | | 0.2803 | | | | | |

Table 5. Serial Topology, Hub Switch, Zero Network Load with Filters

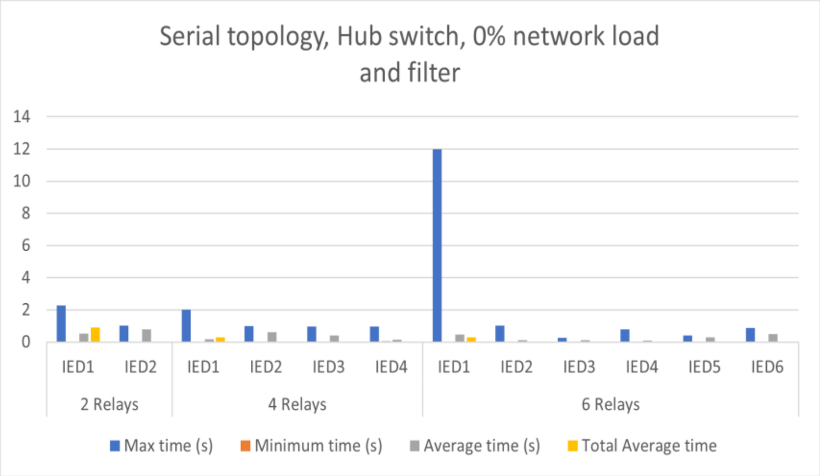


Figure 39. Time Measure of Serial Topology Using Hub in Test 4

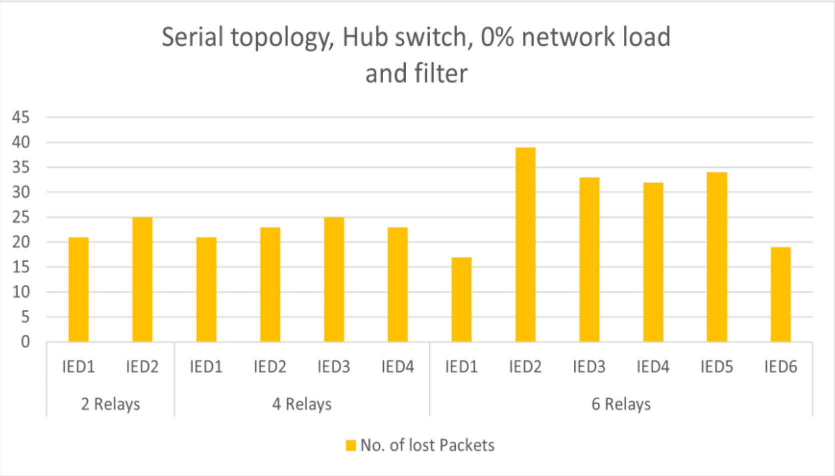


Figure 40. Packets Lost for Serial Topology Using Hub in Test 4

- **Test 5: Serial Topology, Network Load with 64 Bytes, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.9528 | 0.9195 | 0.9233 | 0.9687 | 0.8925 | 0.7773 | 0.6608 | 0.6999 | 0.7358 | 0.7808 | 0.2919 | 0.2829 |
| Minimum time (s) | 0.0009 | 0.0009 | 0.0136 | 0.0019 | 0.0001 | 0.0001 | 0.0009 | 0.0088 | 0.0001 | 0.0078 | 0.0127 | 0.0156 |
| Average time (s) | 0.4395 | 0.1761 | 0.4090 | 0.1709 | 0.1778 | 0.2561 | 0.1540 | 0.1401 | 0.4175 | 0.0825 | 0.1300 | 0.1324 |
| No. of lost packets | 35 | 32 | 23 | 30 | 26 | 24 | 26 | 26 | 25 | 32 | 22 | 20 |
| Total average time | 0.2908 | | 0.2561 | | | | 0.1523 | | | | | |

Table 6. Serial Topology, Hub Switch, with 64 Bytes Frame Size Network Load with Filter

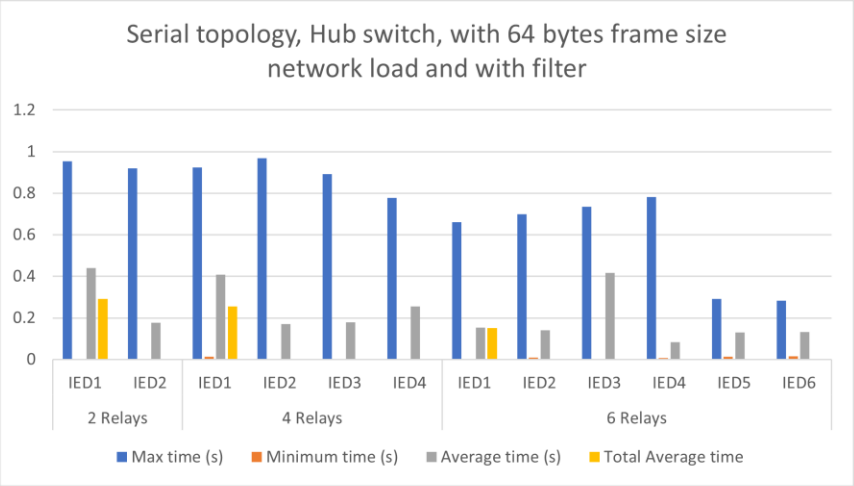


Figure 41. Time Measure of Serial Topology Using Hub in Test 5

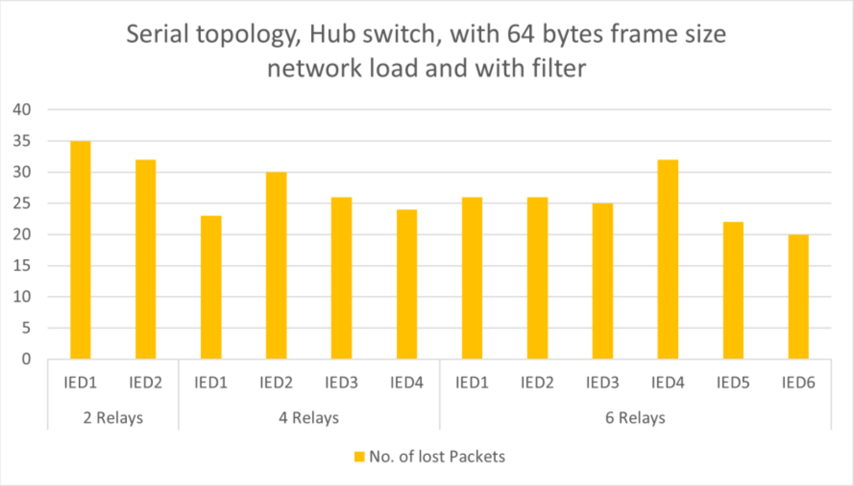


Figure 42. Packet Lost for Serial Topology Using Hub in Test 5

- **Test 6: Serial Topology, Network Load with 1500 Bytes, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.9364 | 0.9439 | 0.5789 | 0.4243 | 0.6256 | 0.6452 | 0.6540 | 0.5295 | 0.2984 | 0.2930 | 0.4503 | 0.2528 |
| Minimum time (s) | 0.0077 | 0.0068 | 0.0087 | 0.0001 | 0.0048 | 0.0048 | 0.0136 | 0.0176 | 0.0117 | 0.0068 | 0.0009 | 0.0029 |
| Average time (s) | 0.1839 | 0.3702 | 0.2474 | 0.2480 | 0.3262 | 0.1580 | 0.2919 | 0.1935 | 0.1826 | 0.1169 | 0.1833 | 0.1191 |
| No. of lost packets | 25 | 25 | 19 | 24 | 22 | 19 | 26 | 28 | 23 | 33 | 22 | 20 |
| Total average time | 0.3929 | | 0.2323 | | | | 0.1523 | | | | | |

Table 7. Serial Topology, Hub Switch, with 1500 Bytes Frame Size Network Load and with Filters

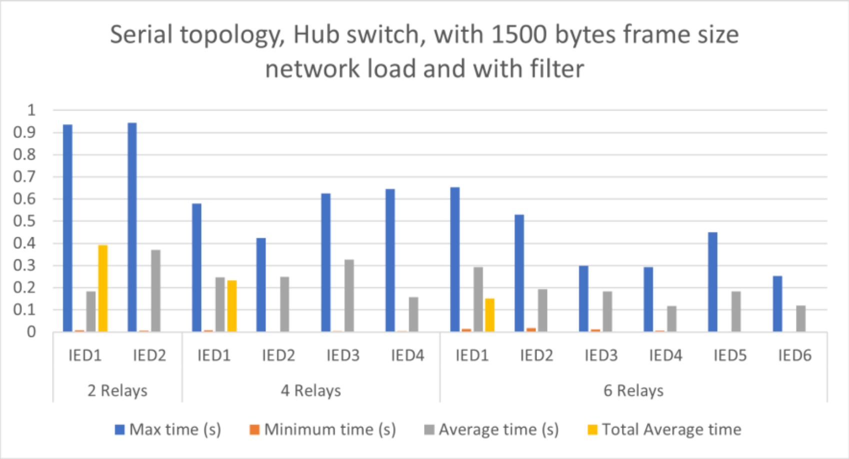


Figure 43. Time Measure of Serial Topology Using Hub in Test 6

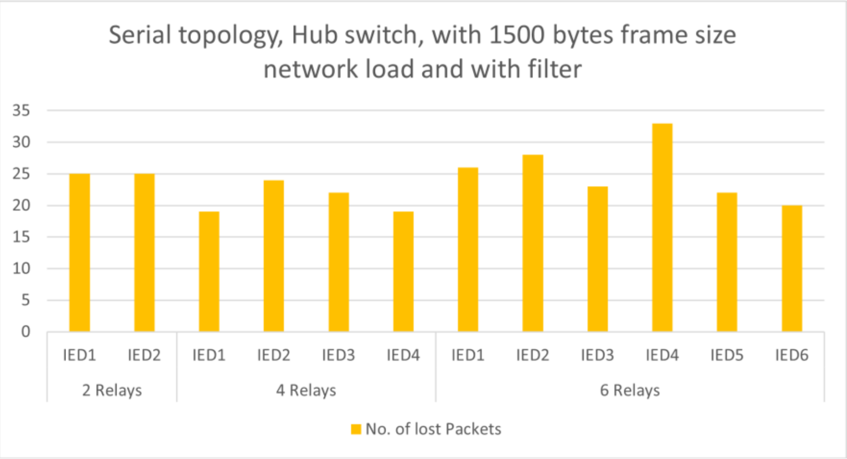


Figure 44. Packets Lost for Serial Topology Using Hub in Test 6

#### 4.5.1.2 Star Topology

The second topology is a star topology as shown in Figure 35, where two switches are connected to a central switch.

- **Test 1: Star Topology, Zero Network Load, No Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 10.2453 | 0.9998 | 9.2523 | 0.1096 | 0.1424 | 0.5163 | 7.9213 | 0.4881 | 0.1093 | 0.3444 | 0.1119 | 0.3383 |
| Minimum time (s) | 0.0001 | 0.0039 | 0.0752 | 0.0009 | 0.0009 | 0.3116 | 0.1195 | 0.0087 | 0.0124 | 0.0009 | 0.0039 | 0.0458 |
| Average time (s) | 0.4381 | 0.3926 | 0.5913 | 0.0372 | 0.0537 | 0.4634 | 0.3676 | 0.1956 | 0.0711 | 0.1668 | 0.0652 | 0.2860 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.4153 | | 0.2864 | | | | 0.1920 | | | | | |

Table 8. Star Topology, Hub Switch, Zero Network Load and No Filter

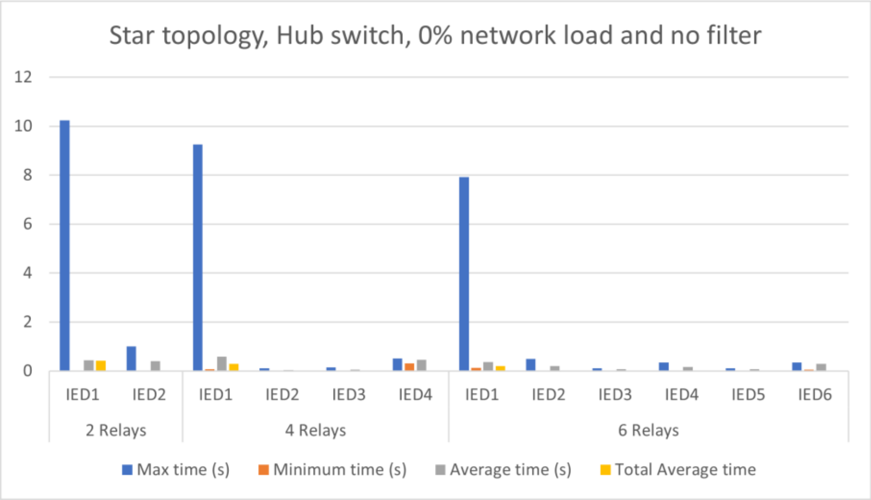


Figure 45. Time Measure of Star Topology Using Hub in Test 1

- **Test 2: Star Topology, Network Load with 64 Bytes and No Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.9557 | 0.9860 | 0.4745 | 0.4833 | 0.2946 | 0.5025 | 0.1327 | 0.2958 | 0.3126 | 0.3990 | 0.2201 | 0.1961 |
| Minimum time (s) | 0.0136 | 0.0009 | 0.0118 | 0.0009 | 0.0009 | 0.0048 | 0.0001 | 0.0009 | 0.0029 | 0.0078 | 0.0009 | 0.0133 |
| Average time (s) | 0.2951 | 0.2469 | 0.1572 | 0.2803 | 0.0913 | 0.2959 | 0.0147 | 0.1131 | 0.2268 | 0.2791 | 0.1554 | 0.1096 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.2710 | | 0.2062 | | | | 0.1498 | | | | | |

Table 9. Star Topology, Hub Switch with 64 Bytes Frame Size Network Load and No Filter

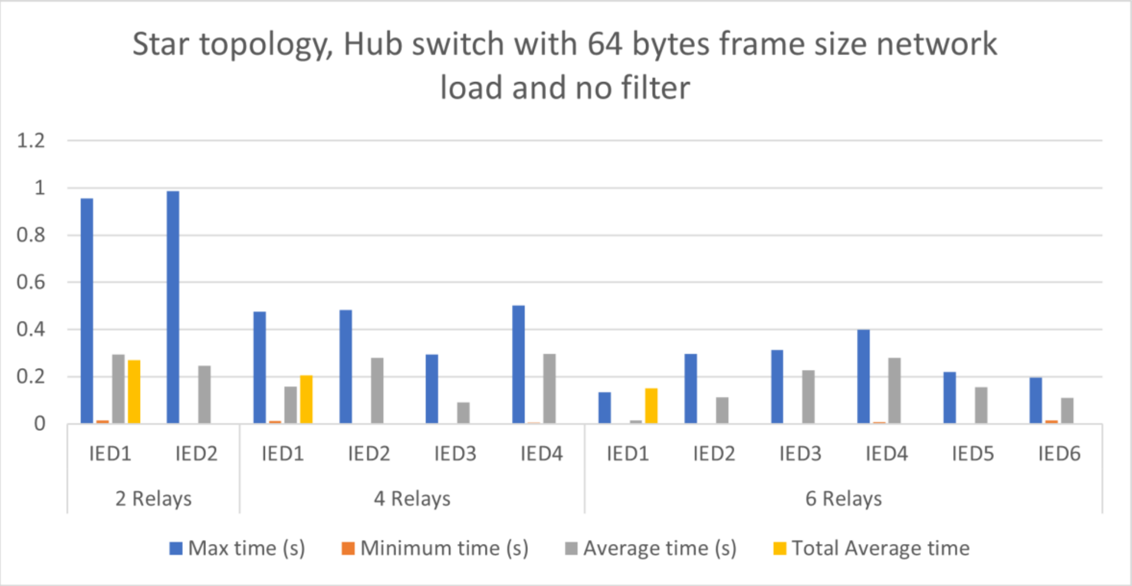


Figure 46. Time Measure of Star Topology Using Hub in Test 2

- **Test 3: Star Topology, Network Load with 1500 Bytes, No Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.2163 | 0.8600 | 0.8873 | 0.8570 | 0.4581 | 0.3778 | 0.4618 | 0.0311 | 0.1337 | 0.3756 | 0.3958 | 0.2764 |
| Minimum time (s) | 0.0068 | 0.0019 | 0.0009 | 0.0001 | 0.0019 | 0.1484 | 0.0019 | 0.0001 | 0.0001 | 0.0009 | 0.0001 | 0.0009 |
| Average time (s) | 0.1610 | 0.4697 | 0.1533 | 0.1002 | 0.2797 | 0.3246 | 0.1601 | 0.0047 | 0.0324 | 0.2501 | 0.1945 | 0.1855 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.3154 | | 0.2144 | | | | 0.1379 | | | | | |

Table 10. Star Topology, Hub Switch with 1500 Bytes Frame Size Network Load and No Filter

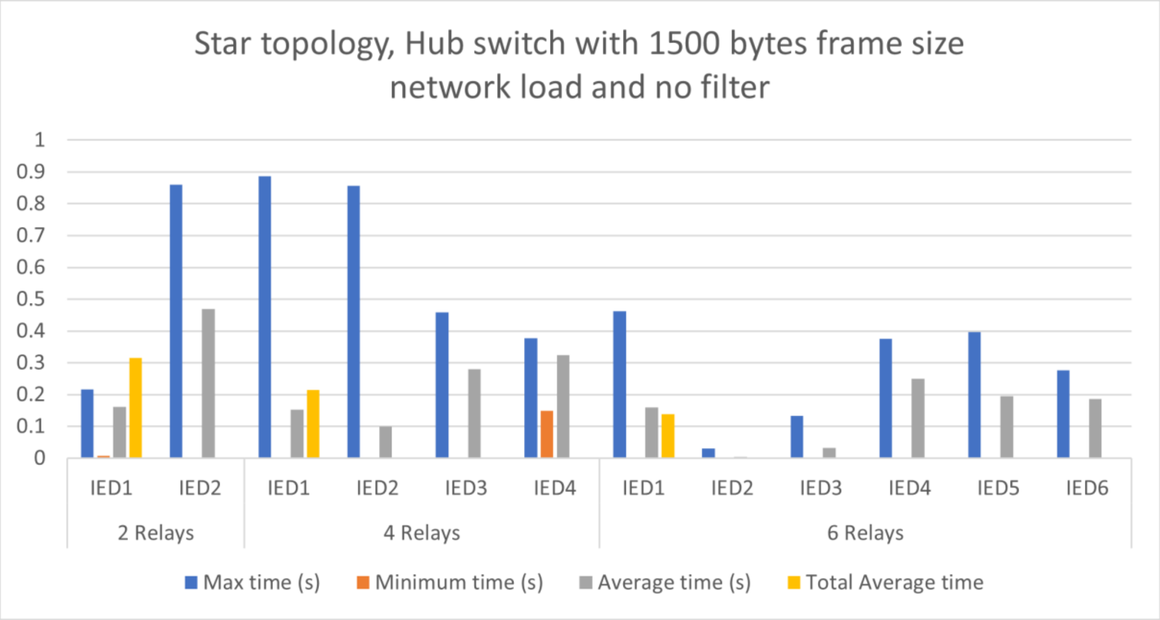


Figure 47. Time Measure of Star Topology Using Hub in Test 3

- **Test 4: Star Topology, Zero Network Load, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 10.1234 | 2.0195 | 1.0156 | 0.9945 | 0.5799 | 0.8004 | 1.0324 | 1.0003 | 0.7624 | 0.5506 | 0.9055 | 0.5817 |
| Minimum time (s) | 0.0078 | 0.0039 | 0.0001 | 0.0009 | 0.0019 | 0.1130 | 0.0087 | 0.0324 | 0.0029 | 0.0420 | 0.0019 | 0.0178 |
| Average time (s) | 0.5637 | 0.8174 | 0.3738 | 0.3598 | 0.1202 | 0.4267 | 0.1533 | 0.3873 | 0.2738 | 0.2469 | 0.2547 | 0.0889 |
| No. of lost packets | 28 | 30 | 20 | 23 | 17 | 27 | 18 | 20 | 31 | 32 | 13 | 19 |
| Total average time | 0.8977 | | 0.3535 | | | | 0.1958 | | | | | |

Table 11. Star Topology, Hub Switch, Zero Network Load with Filter

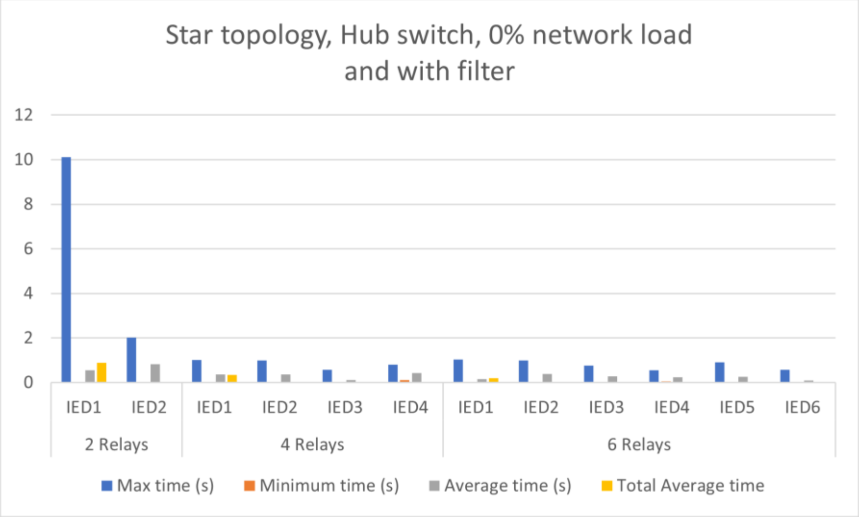


Figure 48. Time Measure of Star Topology Using Hub in Test 4

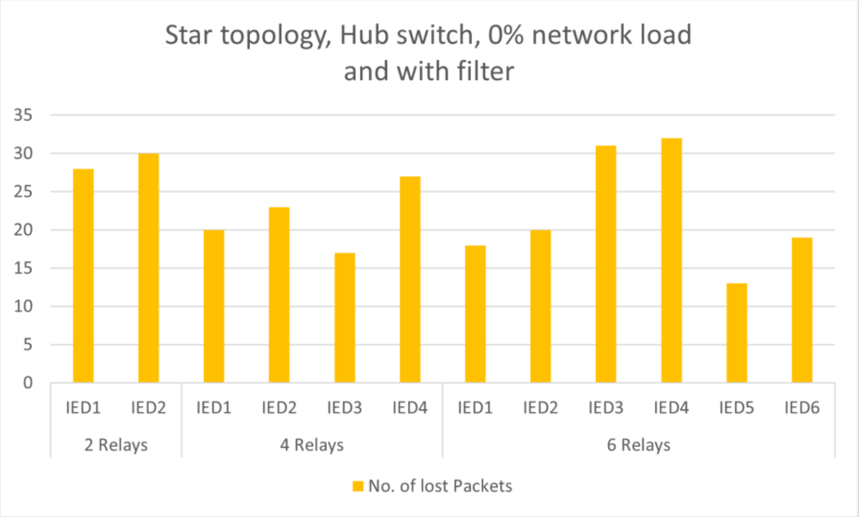


Figure 49. Packets Lost for Star Topology Using Hub in Test 4

- **Test 5: Star Topology, Network Load with 64 Bytes, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.9748 | 0.8873 | 0.6421 | 0.6138 | 0.9134 | 0.8026 | 0.9063 | 0.2843 | 0.4647 | 0.7334 | 0.2943 | 0.7195 |
| Minimum time (s) | 0.0078 | 0.0175 | 0.0029 | 0.0107 | 0.0048 | 0.0019 | 0.0068 | 0.0108 | 0.0001 | 0.0019 | 0.0009 | 0.0146 |
| Average time (s) | 0.3325 | 0.5322 | 0.2602 | 0.1533 | 0.3671 | 0.1652 | 0.4283 | 0.0841 | 0.1392 | 0.0700 | 0.1222 | 0.2122 |
| No. of lost packets | 46 | 40 | 31 | 24 | 32 | 20 | 21 | 23 | 27 | 21 | 22 | 21 |
| Total average time | 0.5322 | | 0.2278 | | | | 0.1725 | | | | | |

Table 12. Star Topology, Hub Switch with 64 Bytes Frame Size Network Load with Filters

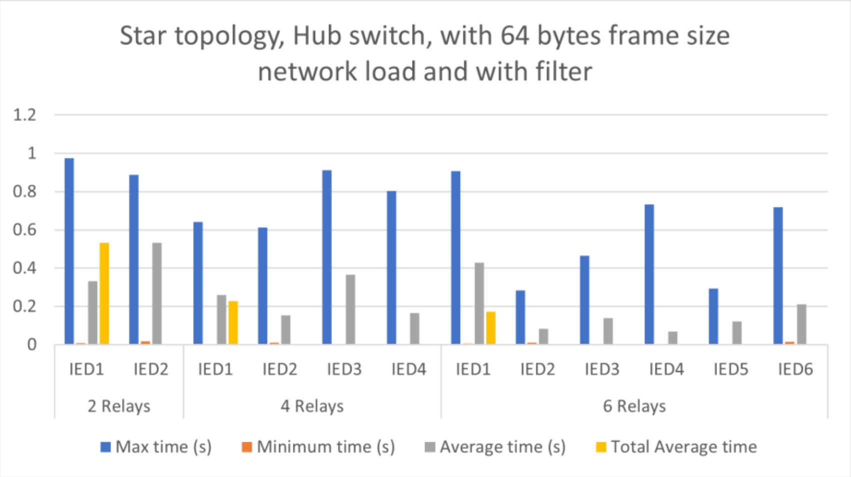


Figure 50. Time Measure of Star Topology Using Hub in Test 5

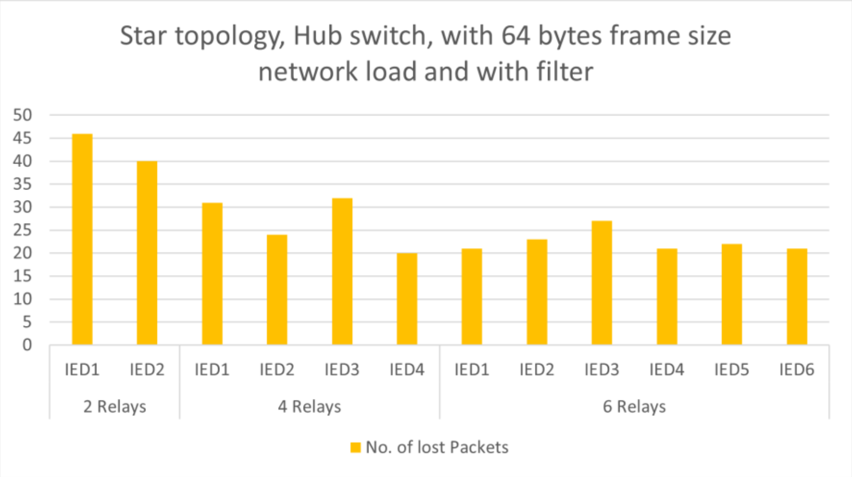


Figure 51. Packets Lost for Star Topology Using Hub in Test 5

- **Test 6: Star Topology, Network Load with 1500 Bytes, with Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.8808 | 0.9828 | 0.5442 | 0.8538 | 0.7066 | 0.9121 | 0.8207 | 0.5445 | 0.6189 | 0.7561 | 0.4115 | 0.6010 |
| Minimum time (s) | 0.1855 | 0.0068 | 0.0009 | 0.0171 | 0.0153 | 0.0019 | 0.0058 | 0.0068 | 0.0156 | 0.0029 | 0.0009 | 0.0078 |
| Average time (s) | 0.5815 | 0.2739 | 0.1898 | 0.3689 | 0.2343 | 0.2124 | 0.2882 | 0.1770 | 0.1914 | 0.2981 | 0.0624 | 0.1908 |
| No. of lost packets | 28 | 18 | 27 | 26 | 32 | 26 | 25 | 26 | 34 | 26 | 34 | 22 |
| Total average time | 0.4586 | | 0.2351 | | | | 0.1791 | | | | | |

Table 13. Star Topology, Hub Switch with 1500 Bytes Frame Size Network Load and No Filter

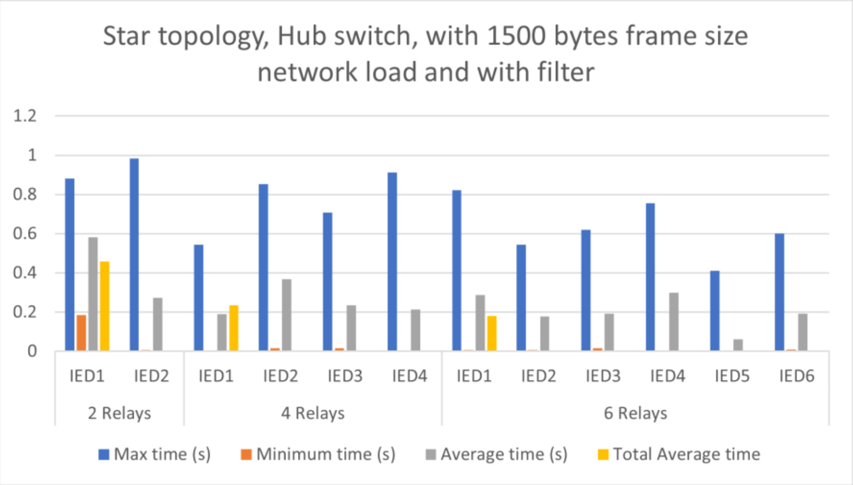


Figure 52. Time Measure of Star Topology Using Hub in Test 6

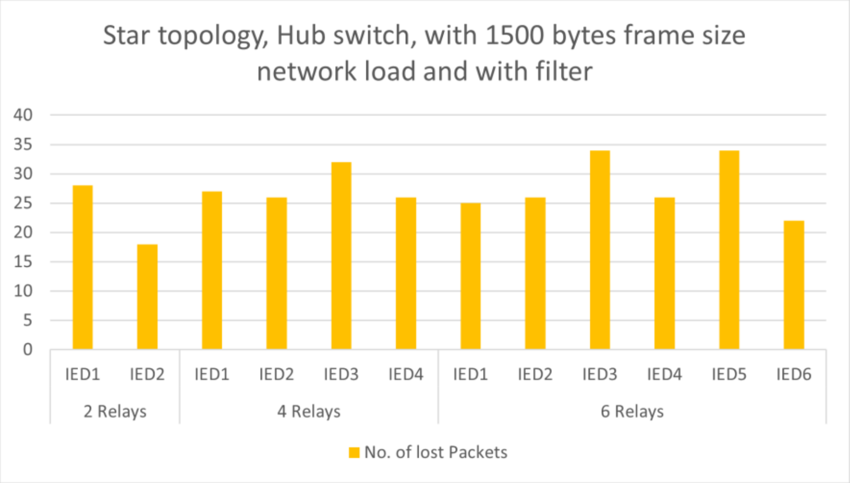


Figure 53. Packets Lost for Star Topology Using Hub in Test 6

#### 4.5.1.3 Hub Switch Analysis Summary

The result with the hub switch implemented in a serial topology shows that there was significant variance in maximum time. Note that the IED1 has the highest delays among all the other IEDs. Therefore, the first IED that begins the transmission is the slowest. In addition, some IEDs in tests 1 and 4 have a much higher maximum time delay in delivering the GOOSE messages; even when there is no load in the network, and the presence of the filter did not matter in time measurement. There is a small difference in max time, which means that the network load seemed to play a minor role in increasing the communication layer time, as shown in tests 2 and 5. As shown in Figures 36 and 38, the maximum time increased a little bit more in test 5 than in test 2, what was also the case comparing tests 3 and 6. However, the filter to cause damage to performance did not affect performance as much as expected. In addition, the minimum time approaches zero. Another observation worth mentioning is that the percentage of lost packets is approximately between 20-35%, which is quite poor. However, the number of lost packets decreases when there is no network load in the system, but tests 5 and 6 have the almost same percentage of lost packets.

The star topology has the same serial results for some of IEDs, especially the first one, which has a maximum time of up to 10 seconds. Some of the tests have a minimum time of 0.2 seconds, which means the topology not as reliable as expected and would pose a problem for real-time operation. However, most of the time some IEDs send the GOOSE messages in under 1 second. As illustrated in Figures 42 and 51, the variance between the max time in serial and max time in star ranged from 1 – 0.8. This observation is of the particular test (test 6) since it has maximum network load and filter characteristics that affect the network performance in every possible way. The percentage of packets lost is higher than for serial, reaching 45 packets lost out of 100 packets for a single IED, which is very poor.

### 4.5.2 Unmanaged Switch

The second set of tests followed the method described in Section 4.1 where Wireshark is used to measure the speed of the communication layer (GOOSE message) and the number of packets that arrive. In this case, the hub switch is replaced with an unmanaged Ethernet switch. This test includes network traffic containing 64 byte frame sizes and 1500 byte frame sizes in addition to the GOOSE message itself. In addition, there is no traffic network included in tests 1 and 4. A total of 12 tests were conducted; the results are listed in tables below. Note that

Figures 54 and 55 display similar topologies for the earlier simulations other than replacing the hubs with unmanaged switches.

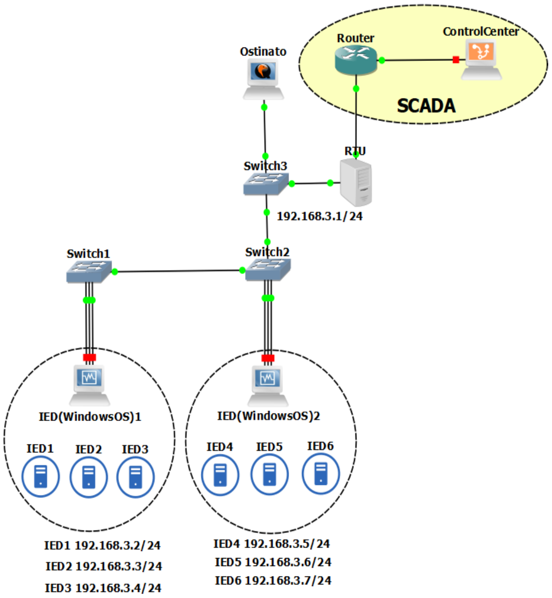


Figure 54. Serial Topology Using Unmanaged Switches

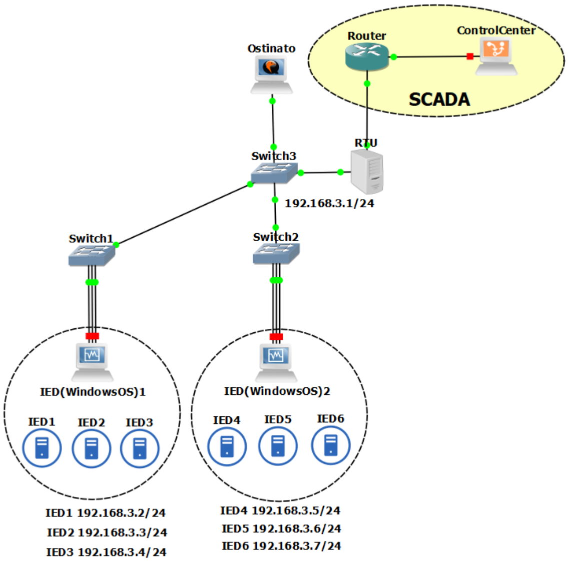


Figure 55. Star Topology Using Unmanaged Switches

#### 4.5.2.1 Serial Topology

- **Test 1: Serial Topology, Zero Network Load and No Filter**

The first topology is a serial or cascaded topology as shown in Figure 54 where three switches are connected sequentially.

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 3.2531 | 0.9994 | 2.1363 | 0.8188 | 0.2491 | 0.2155 | 2.9865 | 0.5646 | 0.2818 | 0.2507 | 0.4562 | 0.2318 |
| Minimum time (s) | 0.0009 | 0.0166 | 0.00001 | 0.0019 | 0.0596 | 0.0292 | 0.0009 | 0.0169 | 0.0001 | 0.0136 | 0.0107 | 0.0110 |
| Average time (s) | 0.2665 | 0.7235 | 0.1494 | 0.0019 | 0.1955 | 0.0889 | 0.1429 | 0.2169 | 0.1994 | 0.0731 | 0.3249 | 0.1562 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.4905 | | 0.2540 | | | | 0.1856 | | | | | |

Table 14. Serial Topology, Unmanaged Switch, with Zero Network Load and No Filter

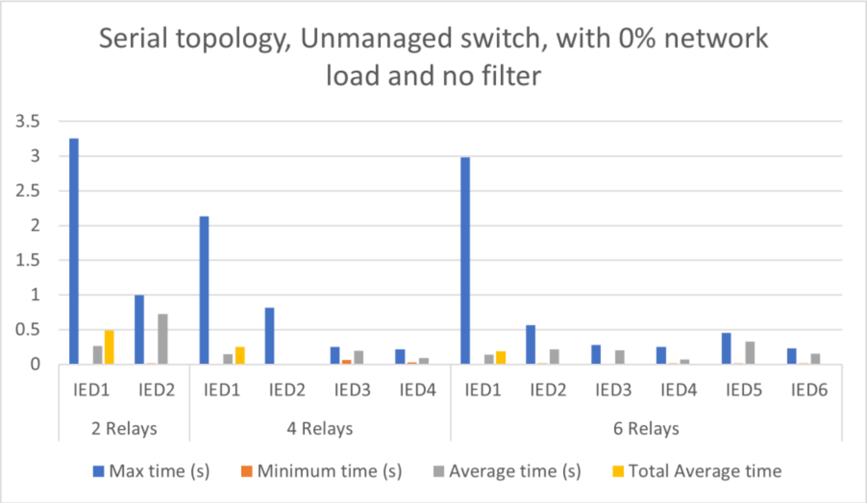


Figure 56. Time Measurement for Serial Topology Using Unmanaged Switch in Test 1

- **Test 2: Serial Topology, Network Load with 64 Bytes and No Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.6285 | 0.4360 | 0.3148 | 0.4382 | 0.2168 | 0.2934 | 0.4995 | 0.4346 | 0.3137 | 0.3388 | 0.1389 | 0.2421 |
| Minimum time (s) | 0.0009 | 0.0129 | 0.0019 | 0.0009 | 0.0078 | 0.0077 | 0.0039 | 0.0019 | 0.0029 | 0.0048 | 0.0001 | 0.0001 |
| Average time (s) | 0.2990 | 0.2756 | 0.1811 | 0.2223 | 0.1461 | 0.1629 | 0.1818 | 0.8881 | 0.2043 | 0.1570 | 0.0884 | 0.1443 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.2873 | | 0.1781 | | | | 0.1441 | | | | | |

Table 15. Serial Topology, Unmanaged Switch, with 64 Bytes Frame Size Network Load and No Filter.

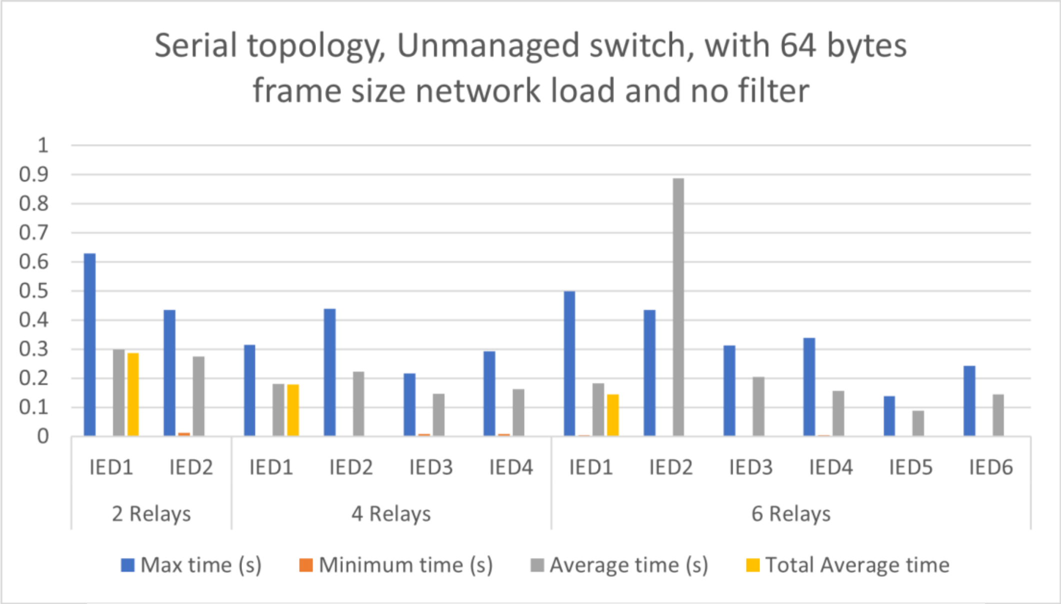


Figure 57 Time Measure of Serial Topology Using Unmanaged Switch in Test 2

- **Test 3: Serial Topology, Network Load with 1500 Bytes, No Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.7685 | 0.4673 | 1.0148 | 0.6833 | 0.3110 | 0.5141 | 0.6894 | 0.4864 | 0.1514 | 0.3600 | 0.1380 | 0.4828 |
| Minimum time (s) | 0.0068 | 0.0097 | 0.0068 | 0.0009 | 0.0096 | 0.0068 | 0.0019 | 0.0019 | 0.0019 | 0.0053 | 0.0069 | 0.0009 |
| Average time (s) | 0.4061 | 0.3594 | 0.2336 | 0.2197 | 0.2408 | 0.1930 | 0.1130 | 0.1497 | 0.0466 | 0.2759 | 0.0864 | 0.2789 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.3828 | | 0.2218 | | | | 0.1584 | | | | | |

Table 16. Serial Topology, Unmanaged Switch, with 1500 Bytes Frame Size Network Load and No Filter

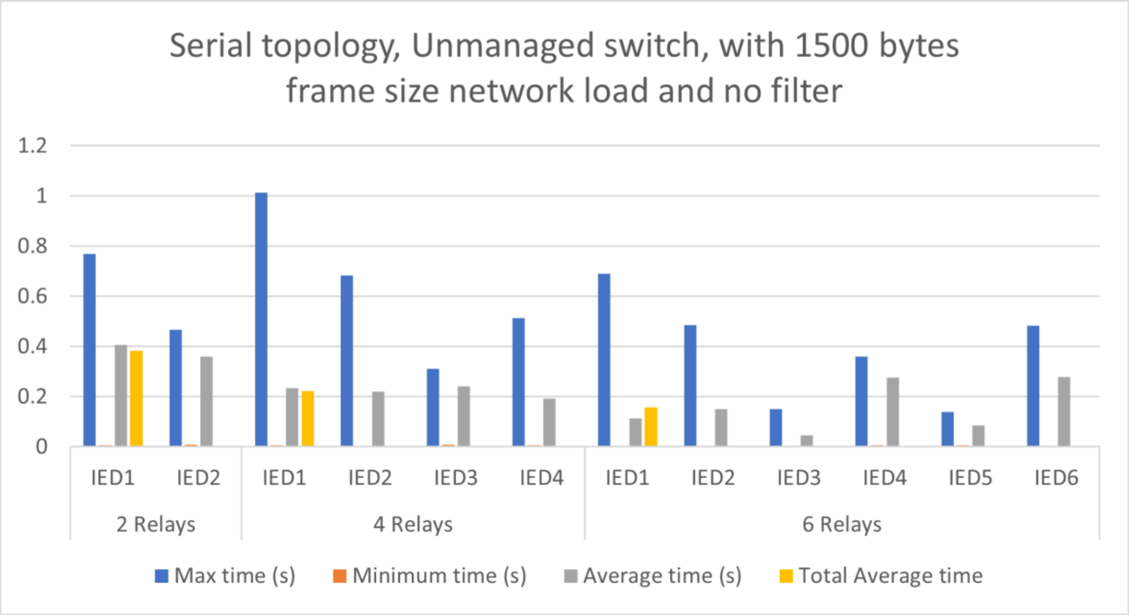


Figure 58. Time Measure of Serial Topology Using Unmanaged Switch in Test 3

- **Test 4: Serial Topology, Zero Network Load, with Filter**

| No. of IEDs | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Time | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.5506 | 1.5438 | 3.5660 | 1.0178 | 0.7189 | 1.0192 | 1.4094 | 0.9816 | 0.8585 | 0.3596 | 0.8985 | 0.4789 |
| Minimum time (s) | 0.0001 | 0.0322 | 0.0019 | 0.0009 | 0.0633 | 0.0029 | 0.0019 | 0.0019 | 0.0048 | 0.2265 | 0.0117 | 0.0761 |
| Average time (s) | 0.5254 | 0.5274 | 0.2374 | 0.5810 | 0.1928 | 0.3457 | 0.2080 | 0.0507 | 0.3023 | 0.2805 | 0.3668 | 0.2124 |
| No. of lost packets | 19 | 26 | 31 | 20 | 33 | 19 | 23 | 18 | 18 | 19 | 27 | 22 |
| Total average time | 0.5264 | | 0.3392 | | | | 0.2368 | | | | | |

Table 17. Serial topology, Unmanaged switch, with Zero Network Load and with Filter

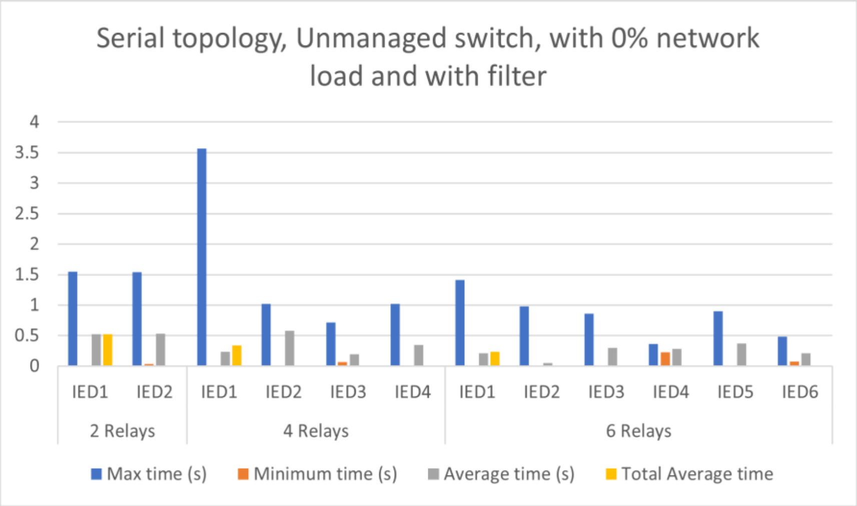


Figure 59. Time Measure of Serial Topology

Using Unmanaged Switch in Test 4

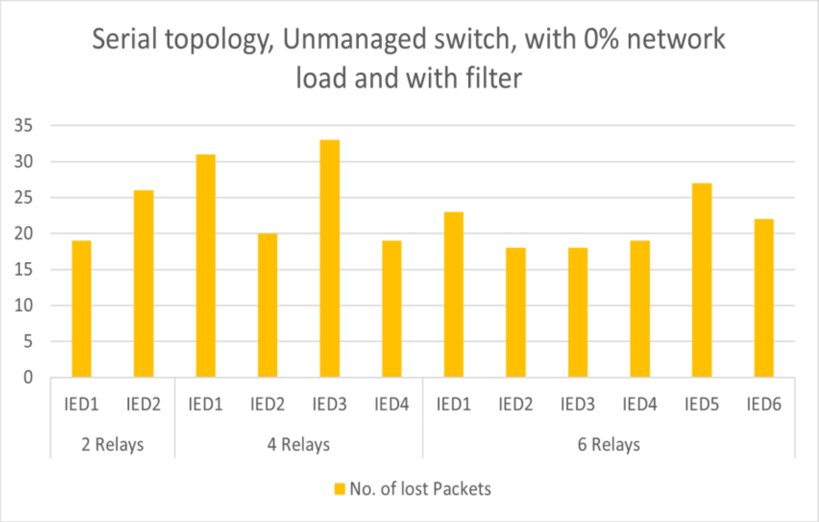


Figure 60. Packet's Loss of Serial Topology

Using Unmanaged Switch in Test 4

- **Test 5: Serial Topology, Network Load with 64 Bytes, with Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.0198 | 0.9938 | 0.9106 | 1.0155 | 0.8970 | 0.0439 | 0.8329 | 0.8110 | 0.9051 | 0.2331 | 0.9048 | 0.3730 |
| Minimum time (s) | 0.0029 | 0.0224 | 0.0019 | 0.0087 | 0.8970 | 0.0029 | 0.0107 | 0.0019 | 0.0019 | 0.0009 | 0.0048 | 0.0108 |
| Average time (s) | 0.4716 | 0.2408 | 0.2532 | 0.4917 | 0.1382 | 0.0783 | 0.1578 | 0.2002 | 0.4113 | 0.0254 | 0.1193 | 0.2264 |
| No. of lost packets | 26 | 21 | 25 | 29 | 30 | 23 | 24 | 33 | 25 | 22 | 23 | 23 |
| Total average time | 0.3562 | | 0.2403 | | | | 0.1901 | | | | | |

Table 18. Serial Topology, Unmanaged switch, with 64 Bytes Frame Size Network Load with Filter

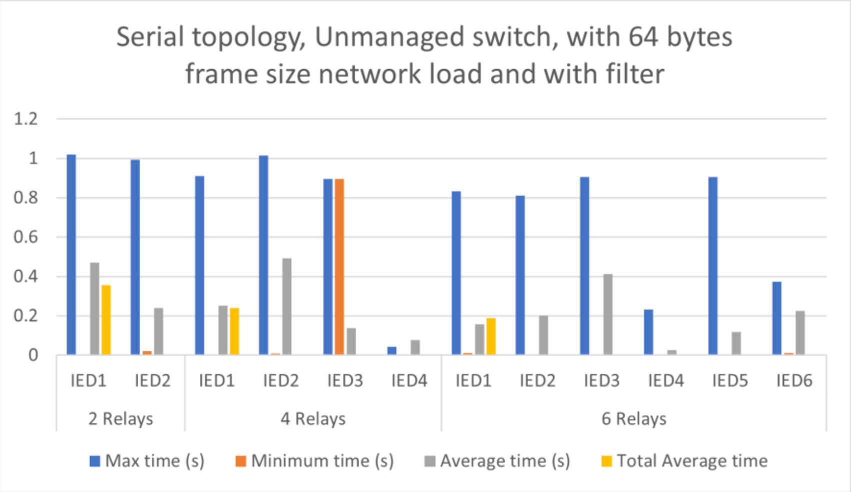


Figure 61. Time Measure of Serial Topology

Using Unmanaged Switch in Test 5

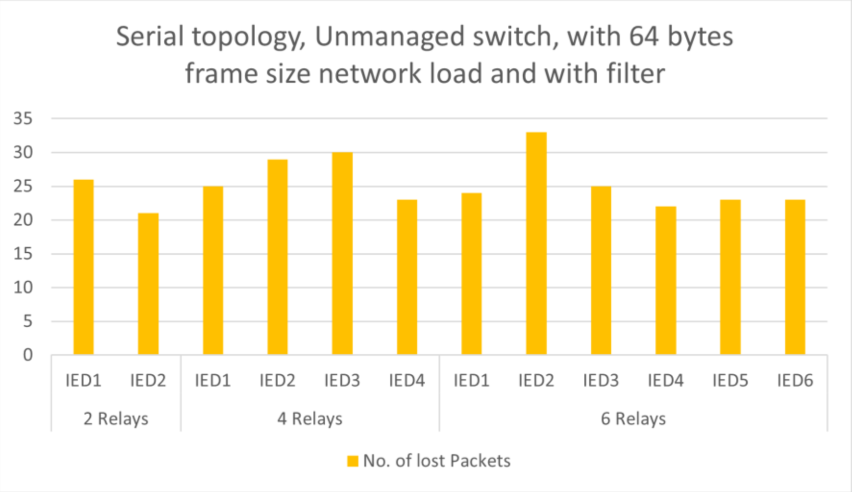


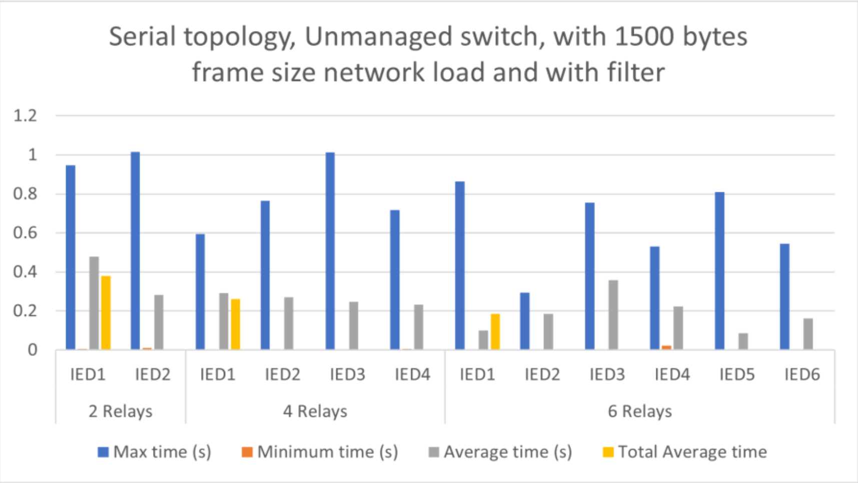
Figure 62. Packet’s Loss of Serial Topology

Using Unmanaged Switch in Test 5

- **Test 6: Serial Topology, Network Load with 1500 Bytes with Filter**

| No. of IEDs | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Time | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.9476 | 1.0145 | 0.5944 | 0.7637 | 1.0142 | 0.7185 | 0.8636 | 0.2946 | 0.7548 | 0.5302 | 0.8098 | 0.5441 |
| Minimum time (s) | 0.0068 | 0.0107 | 0.0029 | 0.0001 | 0.0029 | 0.0058 | 0.0009 | 0.0009 | 0.0009 | 0.0235 | 0.0009 | 0.0009 |
| Average time (s) | 0.4779 | 0.2828 | 0.2916 | 0.2718 | 0.2467 | 0.2326 | 0.1011 | 0.1850 | 0.3576 | 0.2236 | 0.0862 | 0.1631 |
| No. of lost packets | 24 | 26 | 24 | 20 | 24 | 30 | 21 | 21 | 19 | 26 | 24 | 23 |
| Total average time | 0.3804 | | 0.2607 | | | | 0.1861 | | | | | |

Table 19. Serial Topology, Unmanaged Switch, with 1500 Bytes Frame Size Network Load with Filter



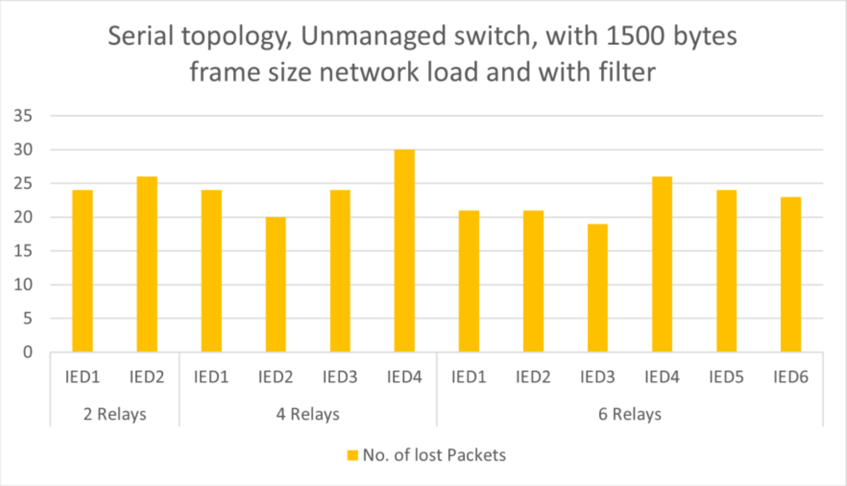


Figure 63. Time Measure of Serial Topology Using Unmanaged Switch in Test 6

Figure 64. Packet's Loss of Serial Topology Using Unmanaged Switch in Test 6

### 4.5.2.2 Star Topology

- **Test 1: Star Topology, Zero Network Load and No Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 2.7963 | 0.9832 | 2.3026 | 0.1727 | 0.5639 | 0.2371 | 1.0253 | 0.4685 | 0.3906 | 0.1394 | 0.3596 | 0.3274 |
| Minimum time (s) | 0.0153 | 0.0130 | 0.0624 | 0.0156 | 0.0769 | 0.0087 | 0.0001 | 0.0009 | 0.1106 | 0.0127 | 0.0126 | 0.1236 |
| Average time (s) | 0.0988 | 0.7425 | 0.3214 | 0.0991 | 0.4465 | 0.1641 | 0.2847 | 0.0691 | 0.3088 | 0.0736 | 0.1831 | 0.2175 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.4206 | | 0.2578 | | | | 0.1895 | | | | | |

Table 20. Star Topology, Unmanaged Switch, Zero Network Load and No Filter

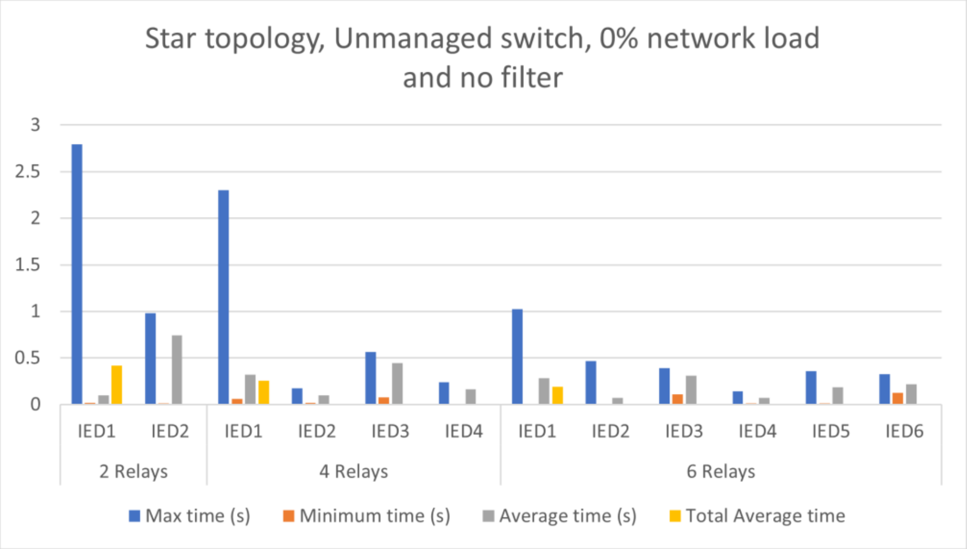


Figure 65. Time Measure of Star Topology Using Unmanaged Switch in Test 1

### Test 2: Star Topology, Network Load with 64 Bytes and No Filter

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.9500 | 0.1697 | 0.4204 | 0.5811 | 0.1215 | 0.2326 | 0.5635 | 0.4427 | 0.1398 | 0.1693 | 0.1386 | 0.1694 |
| Minimum time (s) | 0.0077 | 0.0001 | 0.0009 | 0.0019 | 0.0019 | 0.0009 | 0.0068 | 0.0019 | 0.0053 | 0.0009 | 0.0009 | 0.0001 |
| Average time (s) | 0.2841 | 0.0817 | 0.1661 | 0.2348 | 0.0560 | 0.1540 | 0.2560 | 0.1995 | 0.0822 | 0.0948 | 0.0711 | 0.0536 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.1829 | | 0.1527 | | | | 0.1262 | | | | | |

Table 21. Star Topology, Unmanaged Switch, with 64 Bytes Frame Size Network Load and No Filter

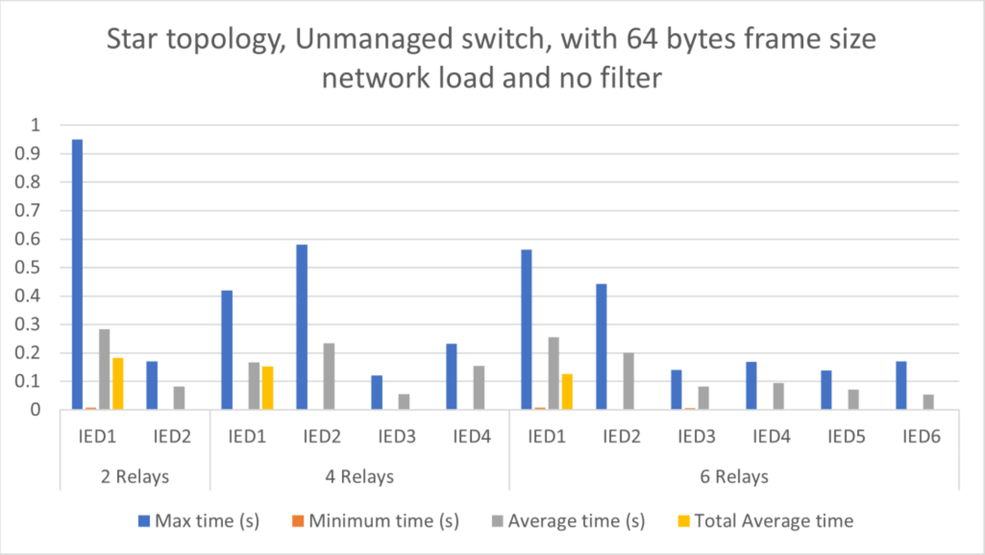


Figure 66. Time Measure of Star Topology Using Unmanaged Switch in Test 2

- **Test 3: Star Topology, Network Load with 1500 Bytes and No Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.9084 | 0.2619 | 0.1869 | 0.7870 | 0.8115 | 0.0784 | 0.3119 | 0.7021 | 0.2177 | 0.3593 | 0.1850 | 0.2000 |
| Minimum time (s) | 0.0078 | 0.0088 | 0.0058 | 0.0078 | 0.0133 | 0.0001 | 0.0107 | 0.0097 | 0.0019 | 0.0097 | 0.0009 | 0.0029 |
| Average time (s) | 0.5135 | 0.1699 | 0,0916 | 0.1148 | 0.5120 | 0.0366 | 0.0915 | 0.3060 | 0.0243 | 0.2786 | 0.0495 | 0.1197 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.3417 | | 0.1887 | | | | 0.1449 | | | | | |

Table 22. . Star Topology, Unmanaged Switch, with 1500 Bytes Frame Size Network Load and No Filter

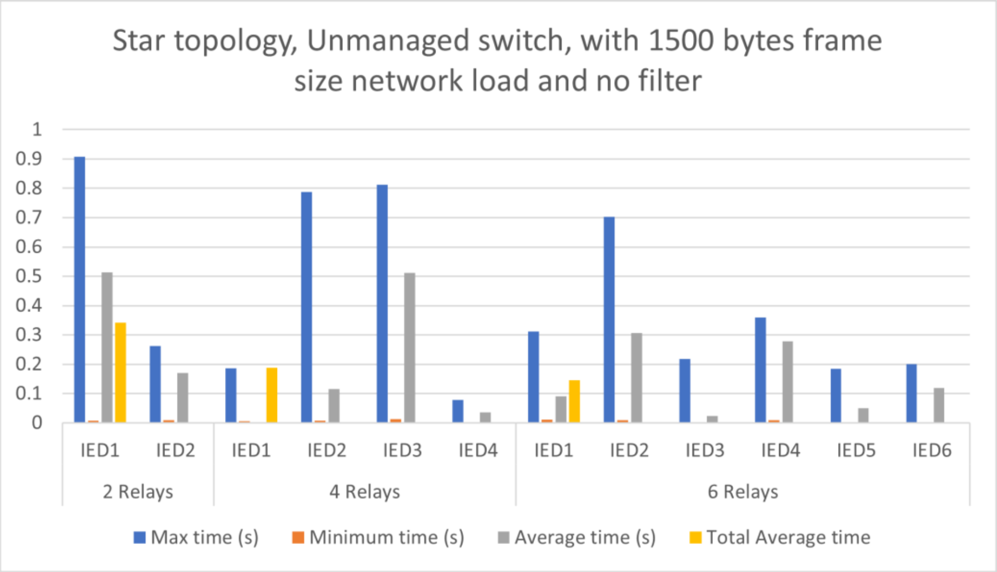


Figure 67. Time Measure of Star Topology Using Unmanaged Switch in Test 3

- **Test 4: Star Topology, Zero Network Load, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.1629 | 1.9214 | 18.199 | 1.8858 | 1.0163 | 1.0186 | 2.0380 | 1.0174 | 0.8223 | 0.3601 | 0.4221 | 0.6117 |
| Minimum time (s) | 0.0622 | 0.0338 | 0.0166 | 0.0001 | 0.0009 | 0.0009 | 0.0029 | 0.0126 | 0.0481 | 0.1064 | 0.0667 | 0.0009 |
| Average time (s) | 0.2737 | 0.7535 | 0.4446 | 0.4808 | 0.1164 | 0.5865 | 0.4251 | 0.1861 | 0.2408 | 0.1822 | 0.1522 | 0.2707 |
| No. of lost packets | 26 | 25 | 23 | 33 | 27 | 21 | 23 | 30 | 27 | 18 | 21 | 26 |
| Total average time | 0.5136 | | 0.5865 | | | | 0.2428 | | | | | |

Table 23. Star Topology, Unmanaged Switch, Zero Network Load with Filter

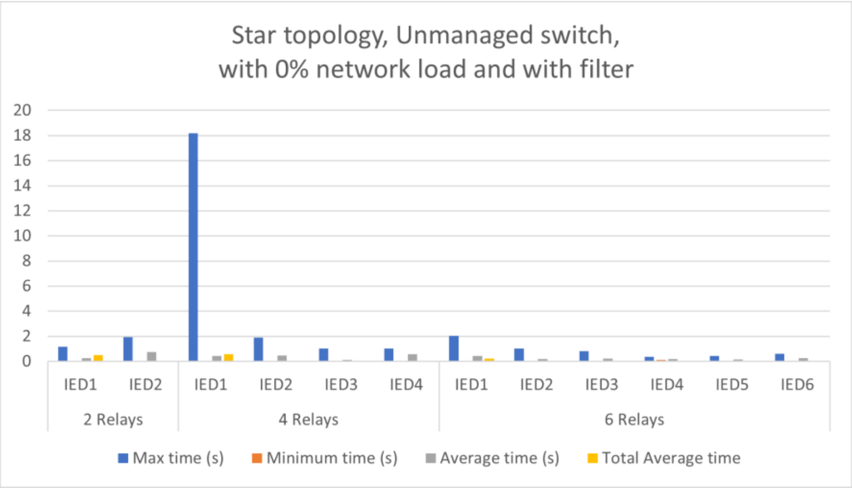


Figure 68. Time Measure of Star Topology

Using Unmanaged Switch in Test 4

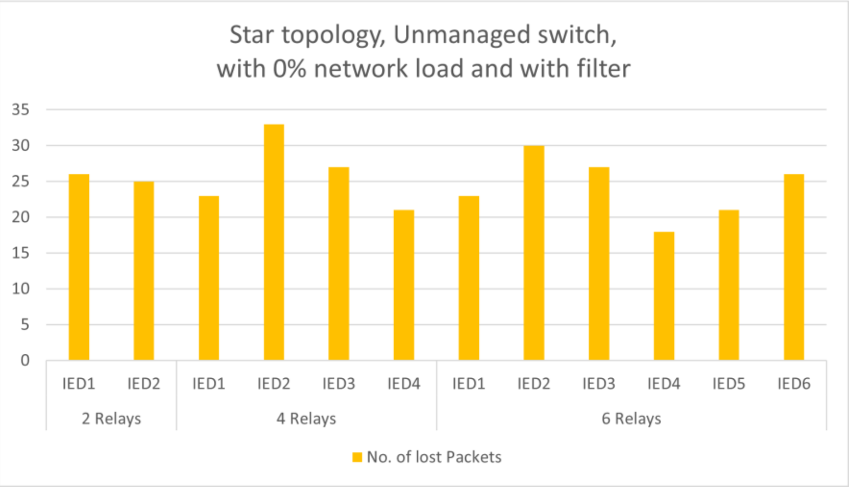


Figure 69. Packet’s Loss of Star Topology

Using Unmanaged Switch in Test 4

- **Test 5: Star Topology, Network Load with 64 Bytes, with Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.0124 | 0.9994 | 1.0011 | 0.8623 | 0.9807 | 0.7961 | 1.0038 | 0.7676 | 0.7966 | 0.7170 | 0.2633 | 0.7272 |
| Minimum time (s) | 0.0029 | 0.0136 | 0.0009 | 0.0001 | 0.0019 | 0.0048 | 0.0009 | 0.0048 | 0.0019 | 0.0009 | 0.0068 | 0.0029 |
| Average time (s) | 0.4113 | 0.2332 | 0.4673 | 0.2358 | 0.1306 | 0.2442 | 0.1282 | 0.4291 | 0.1464 | 0.1314 | 0.1219 | 0.1808 |
| No. of lost packets | 14 | 22 | 28 | 26 | 20 | 27 | 27 | 24 | 29 | 22 | 23 | 29 |
| Total average time | 0.3222 | | 0.2695 | | | | 0.1896 | | | | | |

Table 24. Star Topology, Unmanaged Switch, with 64 Bytes Frame Size Network Load with Filter

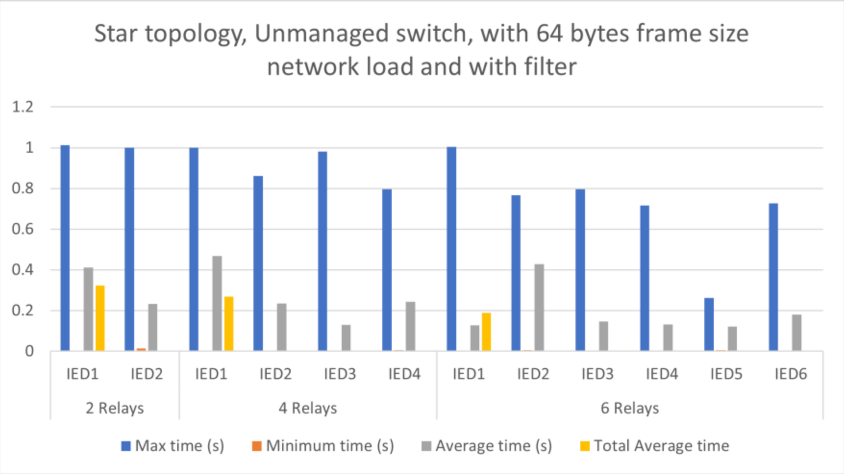


Figure 70. Time Measure of Star Topology

Using Unmanaged Switch in Test 5

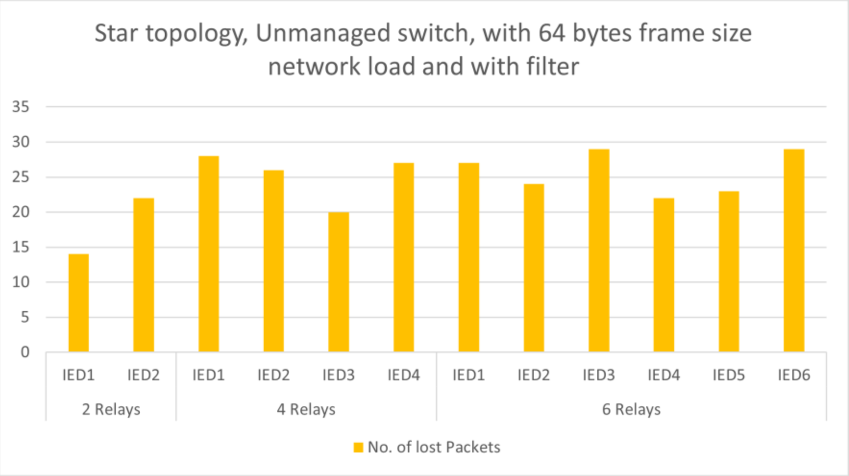


Figure 71. Packet's Loss of Star Topology

Using Unmanaged Switch in Test 5

- **Test 6: Star Topology, Network Load with 1500 Bytes, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.9141 | 1.0883 | 1.9487 | 0.7708 | 0.9391 | 0.6091 | 1.0179 | 0.4550 | 0.7970 | 0.3627 | 0.4522 | 0.6859 |
| Minimum time (s) | 0.0136 | 0.0146 | 0.0009 | 0.0097 | 0.0009 | 0.0087 | 0.0117 | 0.0009 | 0.0019 | 0.0001 | 0.0009 | 0.009 |
| Average time (s) | 0.4716 | 0.1760 | 0.2352 | 0.4249 | 0.1904 | 0.2253 | 0.3830 | 0.0760 | 0.1870 | 0.0712 | 0.1919 | 0.1733 |
| No. of lost packets | 22 | 17 | 24 | 24 | 27 | 25 | 27 | 31 | 29 | 27 | 25 | 24 |
| Total average time | 0.3238 | | 0.2689 | | | | 0.1804 | | | | | |

Table 25. Star Topology, Unmanaged Switch, with 1500 Bytes Frame Size Network Load with Filter

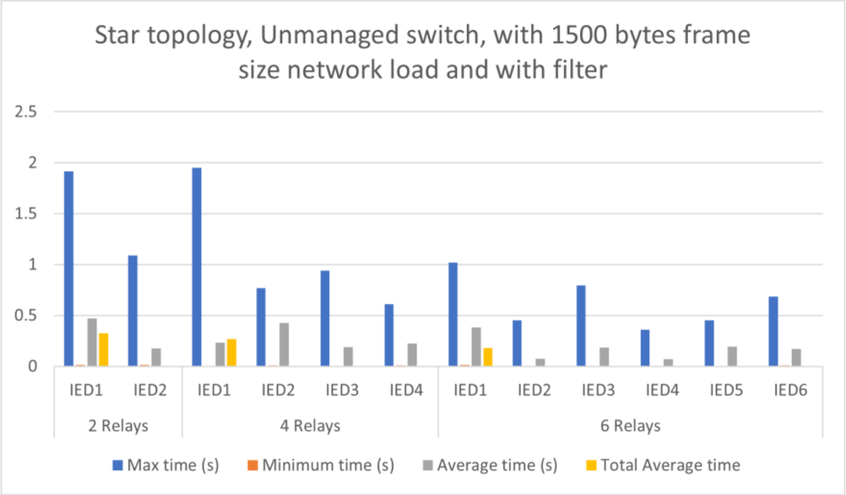


Figure 72. Time Measure of Star Topology Using Unmanaged Switch in Test 6

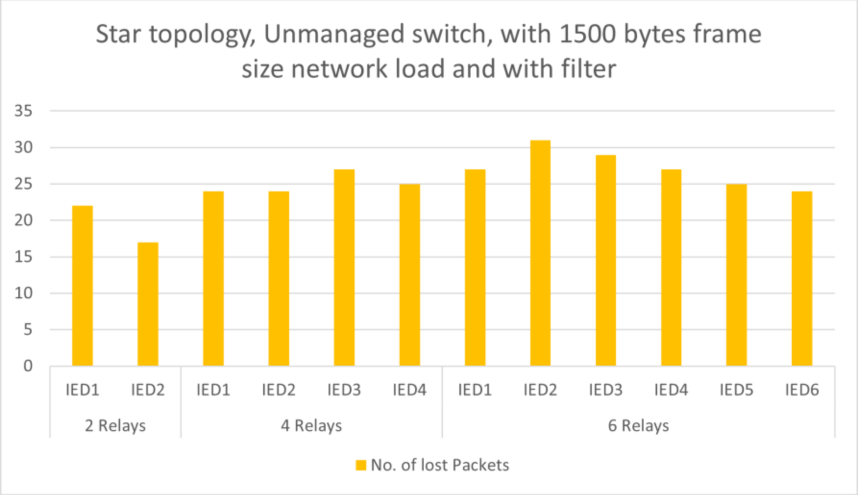


Figure 73. Packet's loss of Star Topology Using Unmanaged Switch in Test 6

#### 4.5.2.3 Unmanaged Switch Analysis Summary

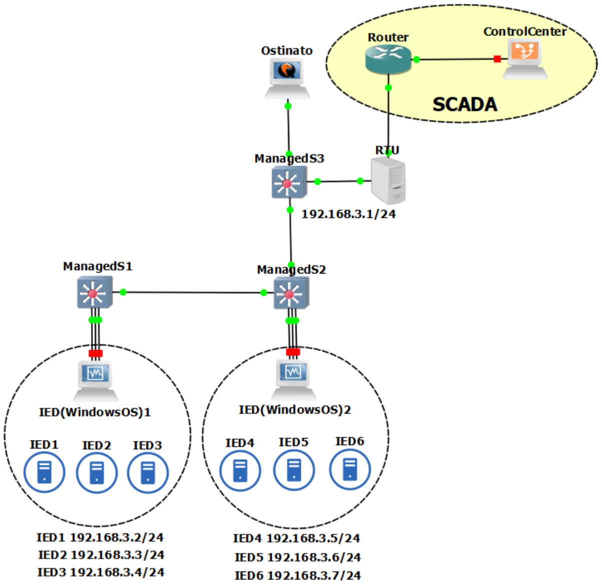
The results for the cases with unmanaged switches in a serial topology show a significant timing variance, as noted in maximum time results. Note that IED1 has the highest delays among all IEDs, the same result as seen for tests with hubs in the same topology. IED1 is the first one that is transmitting the frames; therefore, these frames are the slowest of all the others since they have the longest path to follow. In addition, some IEDs in tests 1 and 4 have a higher maximum time or delay for delivering GOOSE messages, up to 3.5 seconds when there is no network load and no filter applied to create delay or lost packets to impact time performance. In fact, the network load did not seem to play a significant role in increasing the communication layer time. However, there is an increase in maximum time in all tests under the network load tests. As shown in the unmanaged switch tests charts above, there is an increase of up to 1 second in all tests under a filter, which is slightly more than in the hub switch tests. However, the filter did affect network performance. Another observation worth mentioning is that number of lost packets is approximately between 20 -35%, which is the same as the hub switch results, and is quite high. However, the number of lost packets is more when there is no network load in the system, for tests 5 and 6 it was about 35% of packets lost.

With the star topology, the serial results are same as some of IEDs, especially the first IED from all tests which has a maximum time of up to 18 seconds. In some of the tests a filter was used, and the maximum time reached to 2 seconds. Furthermore, most of the time some IEDs were sending the GOOSE messages in under 1 second and lower. As illustrated in Figures 66 and 69, the noted variance between the max time in serial and max time in star ranged between 0.8 and below. The observations of tests with filter noted an impact on the network performance because the maximum network load of frames is included. This act has an increase on time delay, which reaches up to 1 second in all tests with the filter of the simulator. In the case of lost packets, there was less loss than a serial, which reaches under 35 packets lost out of 100 packets in a single IED. In addition, the unmanaged switch is much better than the hub switch in the packet loss, where the number of lost packets was less than expected.

This analysis point was summarized in the results displayed in the tables above listed under the unmanaged switch for both topologies. The time taken for the GOOSE messages to reach their destination is the most important factor used here to measure the performance of different types of switches. In addition, the number of frames that reach the destination is another important aspect that can be used to evaluate the switch’s performance.

### 4.5.3 Managed switch

The third test also followed the method described in Section 4.1, except it now uses managed switches to transmit a GOOSE message from multiple IEDs. This test included 6 IEDs publishing GOOSE messages, which are triggered by the same conditions as in the earlier tests. Tests 1 and 4 did not include any network traffic other than the GOOSE messages. Tests 2, 3, 5 and 6 included a network load of nearly 97%, causing congestion within a very small amount of time. In addition, the frames used to generate traffic carried a payload of 64 bytes in tests 2 and 5 and 1500 bytes in tests 3 and 6. This certainly increased the average time since the GOOSE messages are processed in a serial manner. The results tables display the slowest captured message (Maximum time), the fastest message (Minimum time), and the average measured time. Many tests were conducted, and the results are listed in tables and figures shown below.



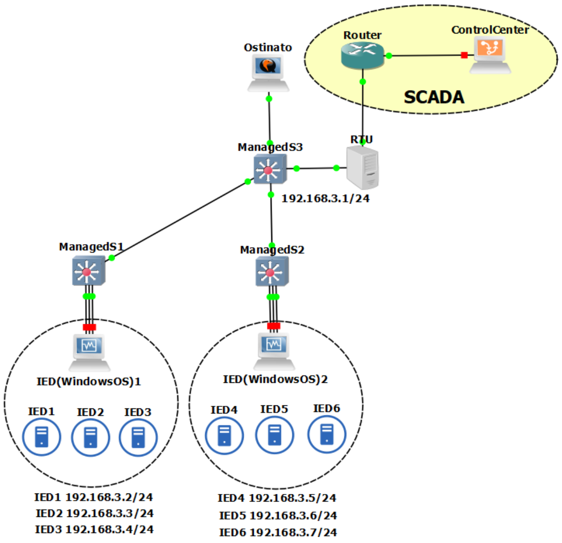


Figure 74. Serial Topology Using Managed Switches

Figure 75. Star Topology Using Managed
Switches

#### 4.5.3.1 Serial Topology

- **Test 1: Serial Topology, Hub Switch, Zero Network Load and No Filter**

The first topology is a serial or cascaded topology as shown in Figure 73 where three switches are connected sequentially.

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.0005 | 1.0068 | 5.7225 | 0.9588 | 0.4940 | 0.4217 | 1.0152 | 0.4363 | 0.4399 | 0.2155 | 0.4406 | 0.2893 |
| Minimum time (s) | 0.0001 | 0.0051 | 0.0043 | 0.0005 | 0.0037 | 0.0623 | 0.0001 | 0.0266 | 0.0100 | 0.00013 | 0.0031 | 0.0307 |
| Average time (s) | 0.5248 | 0.4133 | 0.3097 | 0.0991 | 0.3509 | 0.3411 | 0.1474 | 0.2051 | 0.1623 | 0.0520 | 0.2596 | 0.2463 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.4690 | | 0.2752 | | | | 0.1788 | | | | | |

Table 26. Serial Topology, Managed Switches, Zero Network Load and No Filter

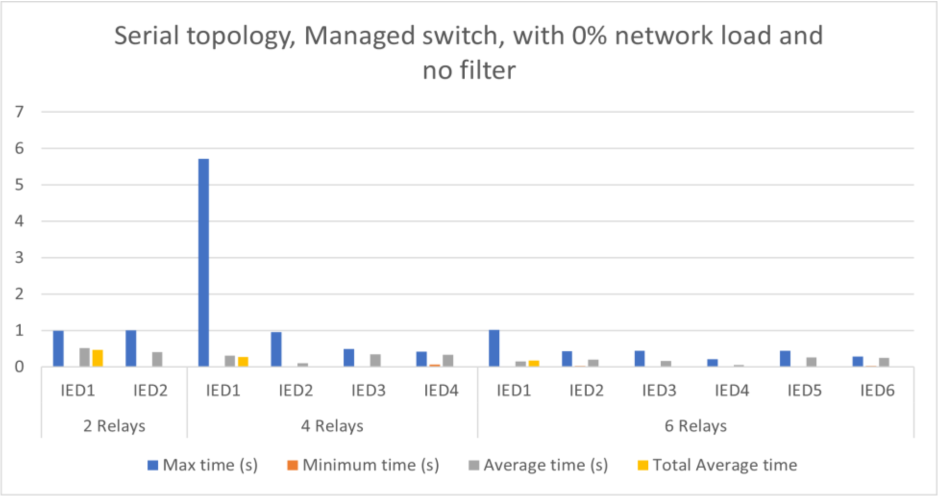


Figure 76. Time Measure of Serial Topology Using Managed Switches in Test 1

- **Test 2: Serial Topology, Network Load with 64 Bytes and No Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.2494 | 0.8320 | 1.9205 | 0.3768 | 0.3797 | 0.6212 | 0.9420 | 0.0797 | 0.6064 | 0.2061 | 0.5156 | 0.5357 |
| Minimum time (s) | 0.1534 | 0.0241 | 0.0092 | 0.0069 | 0.0014 | 0.0022 | 0.0103 | 0.0005 | 0.0023 | 0.0279 | 0.0001 | 0.0003 |
| Average time (s) | 0.2010 | 0.4499 | 0.1095 | 0.1568 | 0.1651 | 0.3431 | 0.2618 | 0.0243 | 0.3069 | 0.1629 | 0.0447 | 0.0850 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.3255 | | 0.1936 | | | | 0.1476 | | | | | |

Table 27. Serial Topology, Managed Switches, with 64 Bytes Frame Size Network Load and No Filter

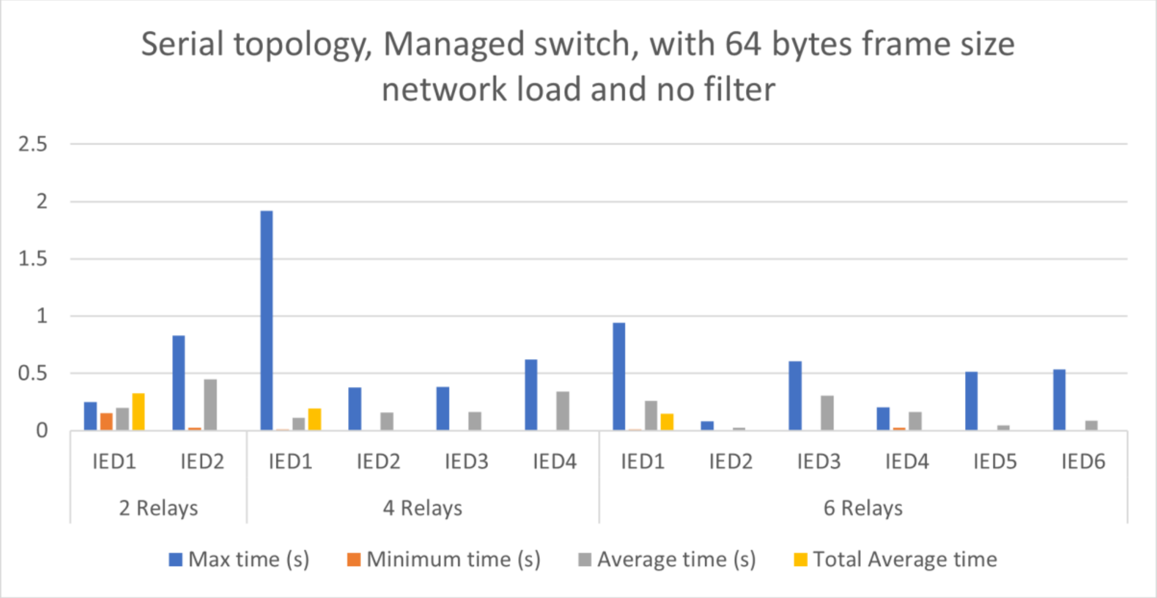


Figure 77. Time Measure of Serial Topology Using Managed Switches in Test 2

- **Test 3: Serial Topology, Network Load with 1500 Bytes, No Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.5695 | 0.8953 | 0.9339 | 0.5101 | 0.3114 | 0.1356 | 0.5415 | 0.3657 | 0.0969 | 0.2741 | 0.5487 | 0.0837 |
| Minimum time (s) | 0.0106 | 0.0098 | 0.0082 | 0.0072 | 0.0084 | 0.0036 | 0.0120 | 0.0007 | 0.0005 | 0.0012 | 0.0081 | 0.0002 |
| Average time (s) | 0.1779 | 0.5370 | 0.3998 | 0.1828 | 0.2245 | 0.0787 | 0.1965 | 0.0801 | 0.0390 | 0.1682 | 0.3411 | 0.0269 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.3574 | | 0.2214 | | | | 0.1420 | | | | | |

Table 28. Serial topology, Managed switches, with 1500 Bytes Frame Size Network Load and No Filter

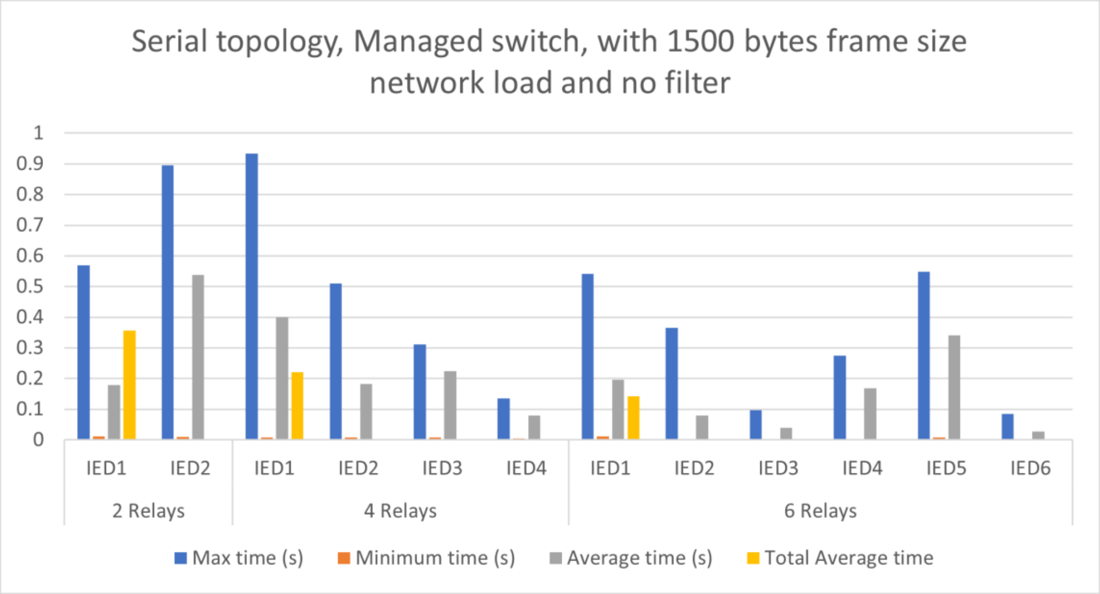


Figure 78. Time Measure of Serial Topology Using Managed Switches in Test 3

- **Test 4: Serial Topology, Zero Network Load, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 4.4568 | 2.8482 | 1.0408 | 1.0021 | 1.0300 | 1.0000 | 3.0452 | 1.0010 | 0.5848 | 0.5813 | 0.6065 | 0.7035 |
| Minimum time (s) | 0.1344 | 0.4688 | 0.0001 | 0.0014 | 0.0003 | 0.0011 | 0.0001 | 0.0040 | 0.1628 | 0.0040 | 0.0131 | 0.0032 |
| Average time (s) | 0.6731 | 0.9966 | 0.5010 | 0.1600 | 0.5322 | 0.1440 | 0.3684 | 0.3222 | 0.2528 | 0.1184 | 0.2411 | 0.2432 |
| No. of lost packets | 40 | 38 | 26 | 28 | 28 | 26 | 35 | 29 | 26 | 26 | 22 | 36 |
| Total average time | 0.8348 | | 0.3343 | | | | 0.2577 | | | | | |

Table 29. Serial Topology, Managed Switches, Zero Network Load with Filter

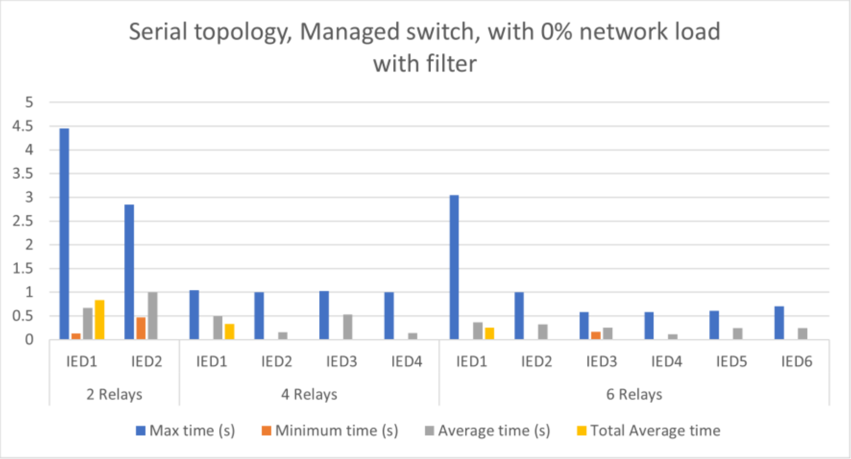


Figure 79. Time Measure of Serial Topology

Using Managed Switches in Test 4

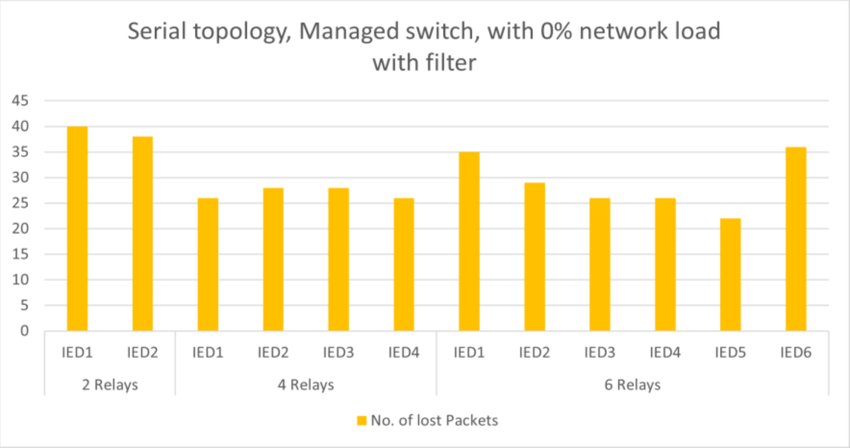


Figure 80. Packet's Loss of Serial Topology

Using Managed Switches in Test 4

- **Test 5: Serial Topology, Network Load with 64 Bytes, with Filter**

| No. of IEDs | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Time | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.0047 | 0.8905 | 1.0157 | 0.7258 | 0.9560 | 0.6096 | 0.9817 | 0.8125 | 0.7334 | 0.5633 | 0.7157 | 0.2031 |
| Minimum time (s) | 0.0098 | 0.0143 | 0.0013 | 0.0011 | 0.0029 | 0.0159 | 0.0025 | 0.0015 | 0.0109 | 0.0012 | 0.0054 | 0.0011 |
| Average time (s) | 0.3412 | 0.4318 | 0.0741 | 0.1472 | 0.3487 | 0.3992 | 0.3474 | 0.2374 | 0.3598 | 0.0371 | 0.1764 | 0.0166 |
| No. of lost packets | 27 | 25 | 26 | 18 | 25 | 25 | 30 | 26 | 23 | 22 | 23 | 21 |
| Total average time | 0.3865 | | 0.2423 | | | | 0.1958 | | | | | |

Table 30. Serial Topology, Managed Switches, with 64 Bytes Size Frame Network Load with Filter

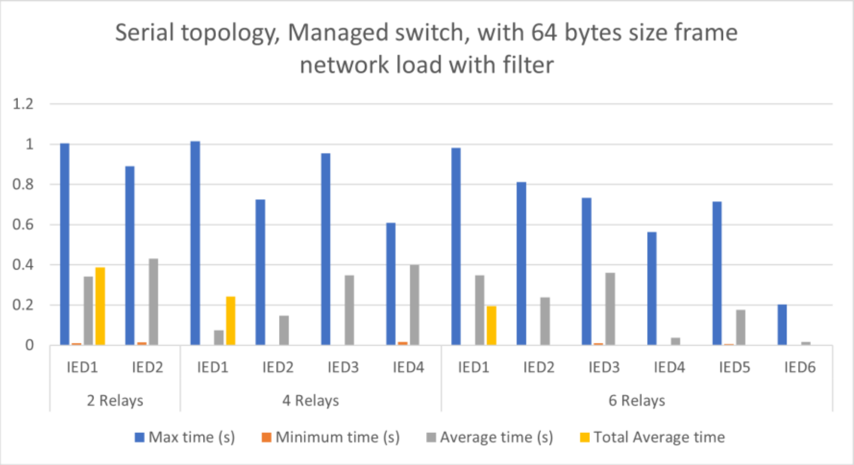


Figure 81. Time Measure of Serial Topology

Using Managed Switches in Test 5

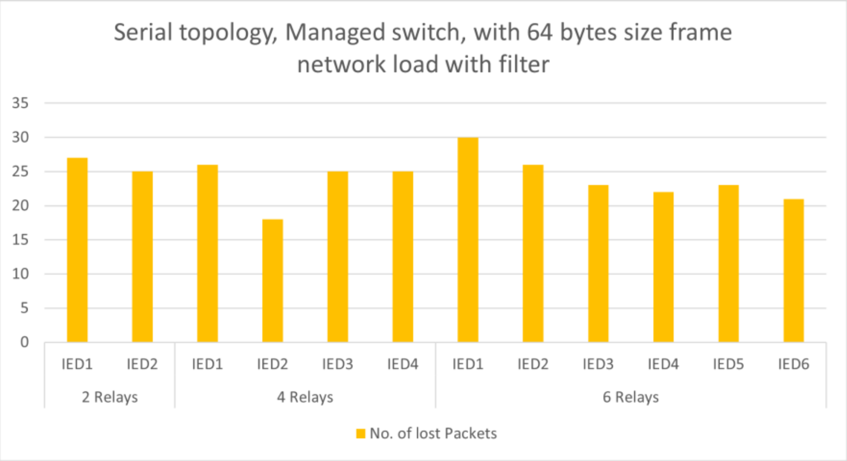


Figure 82. Packet's Loss of Serial Topology

Using Managed Switches in Test 5

- **Test 6: Serial Topology, Network Load with 1500 Bytes, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.0150 | 1.0011 | 0.7179 | 0.3729 | 0.7498 | 0.7794 | 0.9622 | 0.6893 | 0.5896 | 0.5157 | 0.3608 | 0.8276 |
| Minimum time (s) | 0.1000 | 0.0118 | 0.0046 | 0.0011 | 0.0006 | 0.00055 | 0.0077 | 0.0015 | 0.0173 | 0.0102 | 0.0027 | 0.0087 |
| Average time (s) | 0.2920 | 0.4580 | 0.2694 | 0.1101 | 0.4208 | 0.1626 | 0.3719 | 0.1524 | 0.1163 | 0.1500 | 0.1307 | 0.2113 |
| No. of lost packets | 29 | 32 | 27 | 17 | 20 | 27 | 25 | 24 | 26 | 22 | 26 | 28 |
| Total average time | 0.3750 | | 0.2407 | | | | 0.1888 | | | | | |

Table 31. Serial Topology, Managed Switches, with 1500 Bytes Size Frame Network Load with Filter

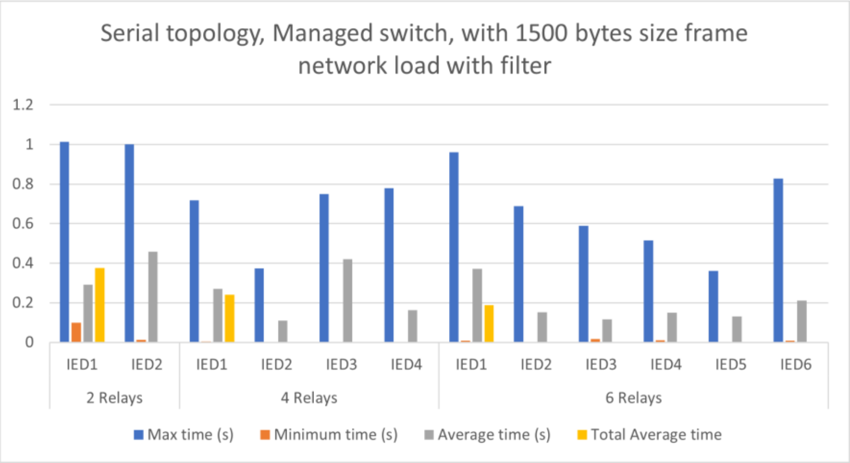


Figure 83. Time Measure of Serial Topology Using Managed Switches in Test 6

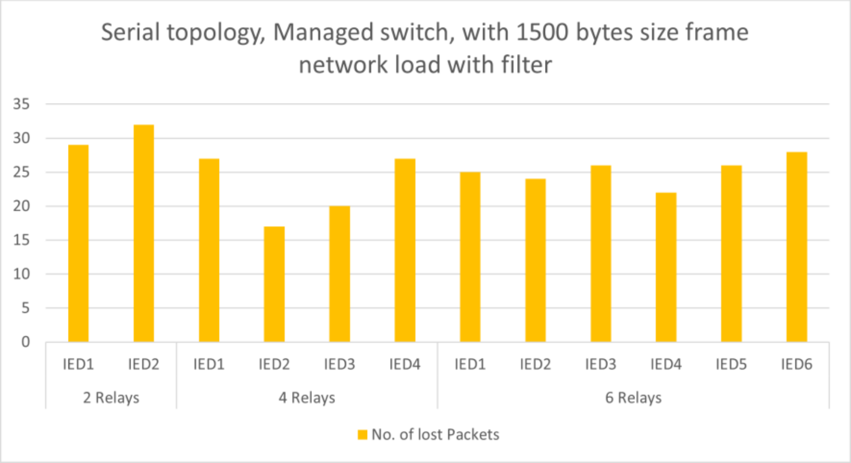


Figure 84. Packet's Loss of Serial Topology Using Managed Switches in Test 6

### 4.5.3.2 Star Topology

- **Test 1: Star Topology, Zero Network Load and No Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 11.925 | 0.9575 | 18.350 | 0.4119 | 0.3774 | 0.0580 | 1.0019 | 0.6234 | 0.1091 | 0.3710 | 0.3892 | 0.2234 |
| Minimum time (s) | 0.0573 | 0.0175 | 0.0112 | 0.0003 | 0.0024 | 0.00019 | 0.0024 | 0.0115 | 0.0005 | 0.1580 | 0.0016 | 0.0465 |
| Average time (s) | 0.2354 | 0.8308 | 0.8491 | 0.0625 | 0.2472 | 0.0070 | 0.1925 | 0.1721 | 0.0192 | 0.2849 | 0.2764 | 0.1373 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.5331 | | 0.2915 | | | | 0.1804 | | | | | |

Table 32. Star Topology, Managed Switches, Zero Network Load with No Filter

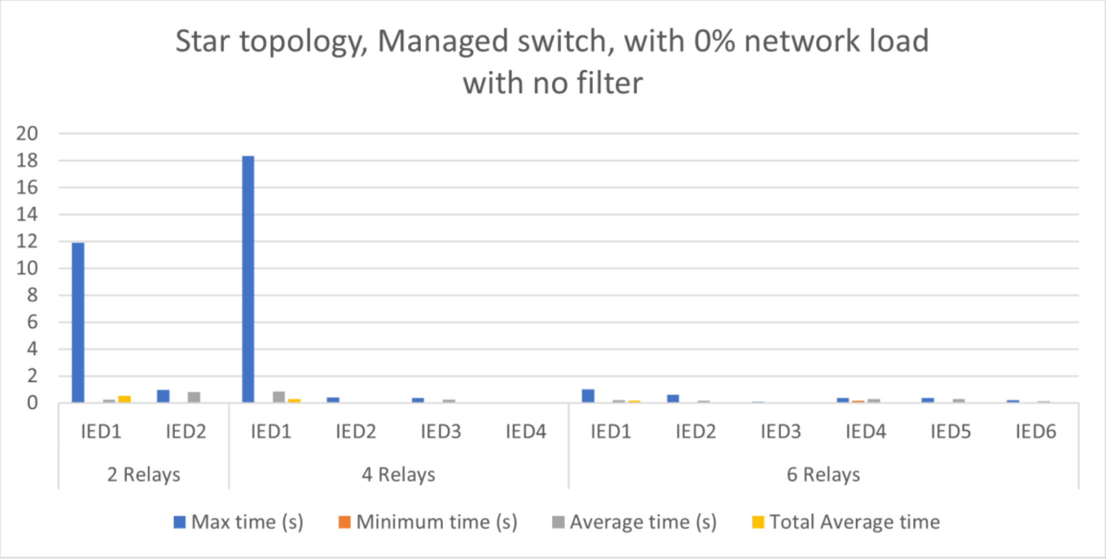


Figure 85. Time Measure of Star Topology Using Managed Switches in Test 1

- **Test 2: Star Topology, Network Load with 64 Bytes, No Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.8839 | 1.0010 | 0.5934 | 0.6068 | 0.3939 | 0.1450 | 1.0016 | 0.7184 | 0.1709 | 0.0299 | 0.1565 | 0.2977 |
| Minimum time (s) | 0.0023 | 0.0053 | 0.0020 | 0.0109 | 0.0063 | 0.0014 | 0.0004 | 0.0064 | 0.0009 | 0.0002 | 0.0090 | 0.0011 |
| Average time (s) | 0.2342 | 0.3305 | 0.0852 | 0.4300 | 0.2682 | 0.0628 | 0.0308 | 0.4113 | 0.0946 | 0.0049 | 0.0828 | 0.2204 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.2823 | | 0.2115 | | | | 0.1408 | | | | | |

Table 33. Star Topology, Managed Switches, with 64 Bytes Frame Size Network Load with No Filter

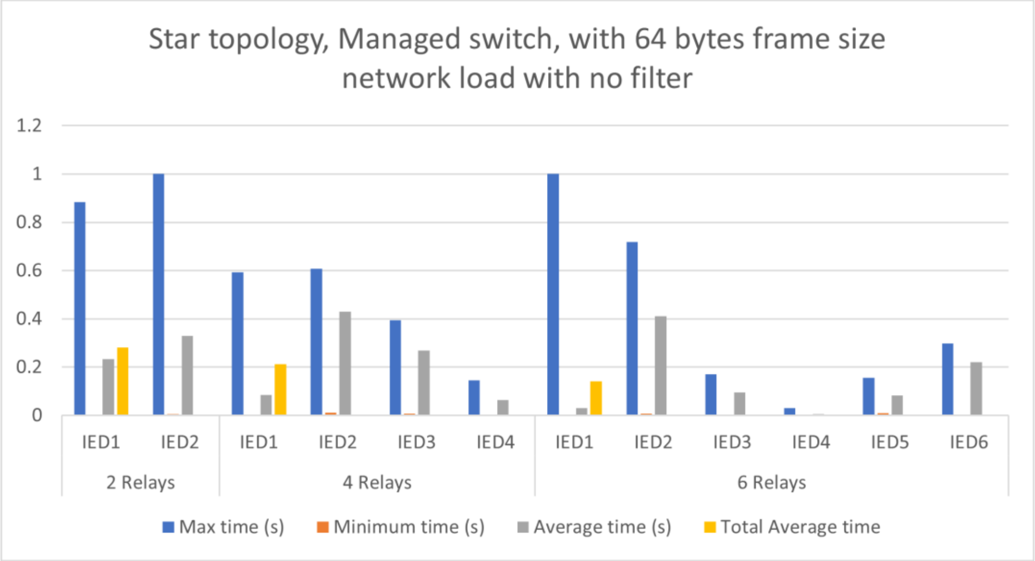


Figure 86. Time Measure of Star Topology Using Managed Switches in Test 2

- **Test 3: Star Topology, Network Load with 1500 Bytes, No Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.8201 | 0.7985 | 0.8115 | 0.5697 | 0.6884 | 0.2884 | 0.4543 | 0.5946 | 0.2030 | 0.3491 | 0.1900 | 0.1777 |
| Minimum time (s) | 0.0178 | 0.0056 | 0.0002 | 0.0064 | 0.0093 | 0.0011 | 0.0123 | 0.0035 | 0.0035 | 0.0053 | 0.00081 | 0.0011 |
| Average time (s) | 0.2554 | 0.4317 | 0.1313 | 0.1433 | 0.4163 | 0.0937 | 0.3113 | 0.1251 | 0.0706 | 0.2601 | 0.0416 | 0.0569 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.4317 | | 0.1962 | | | | 0.1443 | | | | | |

Table 34. Star Topology, Managed Switches, with 1500 Bytes Frame Size Network Load with No Filter

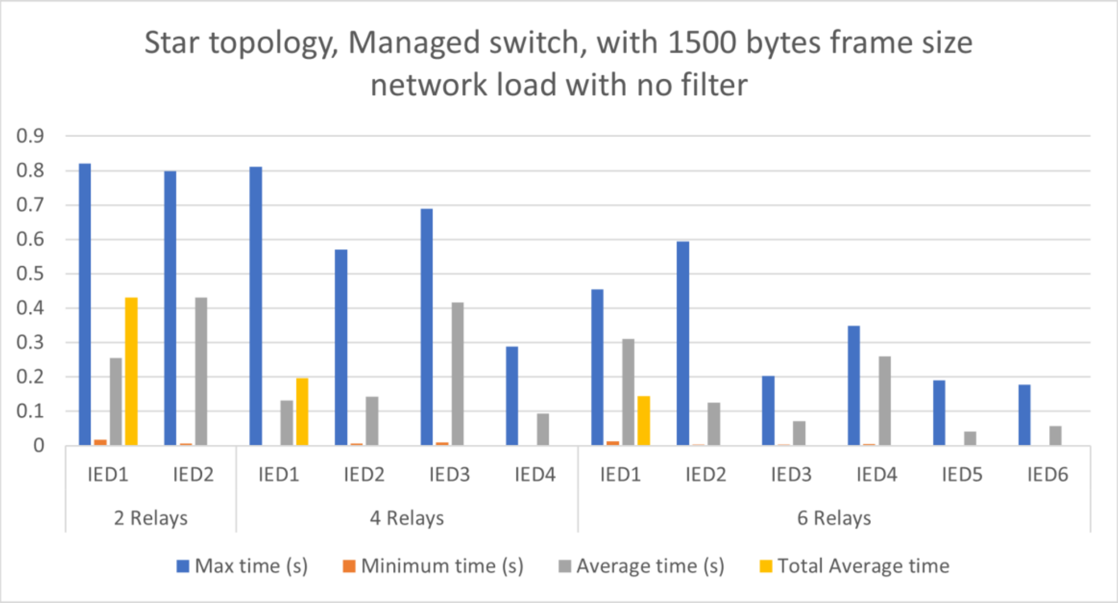


Figure 87. Time Measure of Star Topology Using Managed Switches in Test 3

- **Test 4: Star Topology, Zero Network Load, with Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 2.0279 | 1.8363 | 1.0226 | 1.0183 | 1.0180 | 0.4547 | 2.0175 | 1.1778 | 0.7527 | 0.9099 | 0.7965 | 0.2209 |
| Minimum time (s) | 0.1744 | 0.2342 | 0.0001 | 0.1899 | 0.0010 | 0.0320 | 0.0001 | 0.0003 | 0.0815 | 0.00052 | 0.0012 | 0.0025 |
| Average time (s) | 0.4498 | 1.0094 | 0.4517 | 0.3334 | 0.4915 | 0.1345 | 0.4708 | 0.0684 | 0.5533 | 0.0430 | 0.1341 | 0.0985 |
| No. of lost packets | 32 | 32 | 24 | 23 | 33 | 24 | 19 | 21 | 27 | 11 | 18 | 35 |
| Total average time | 0.7296 | | 0.3528 | | | | 0.2280 | | | | | |

Table 35. Star Topology, Managed Switches, with Zero Network Load with Filter

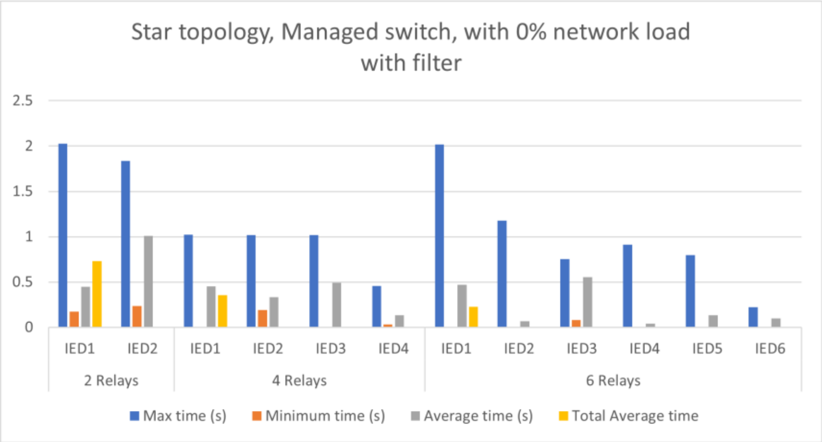


Figure 88. Time Measure of Star Topology Using Managed Switches in Test 4

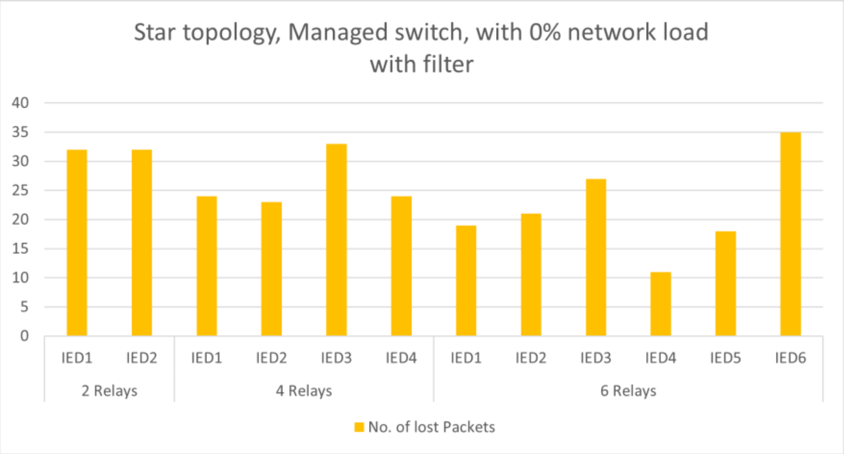


Figure 89. Packet's Loss of Star Topology Using Managed Switches in Test 4

- **Test 5: Star Topology, Network Load with 64 Bytes, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.3005 | 0.9757 | 1.0006 | 1.0107 | 0.7629 | 0.6959 | 0.7194 | 1.0061 | 0.5767 | 0.3781 | 0.5063 | 0.3127 |
| Minimum time (s) | 0.0083 | 0.0051 | 0.0233 | 0.0005 | 0.0015 | 0.0032 | 0.0055 | 0.0176 | 0.0017 | 0.0050 | 0.0017 | 0.0029 |
| Average time (s) | 0.3276 | 0.5046 | 0.1101 | 0.3328 | 0.1342 | 0.4223 | 0.2134 | 0.1798 | 0.3229 | 0.2031 | 0.1188 | 0.1529 |
| No. of lost packets | 26 | 26 | 29 | 26 | 23 | 36 | 23 | 26 | 29 | 15 | 28 | 22 |
| Total average time | 0.4161 | | 0.02498 | | | | 0.1985 | | | | | |

Table 36. Star Topology, Managed Switches, with 64 Bytes Frame Size Network Load with Filter

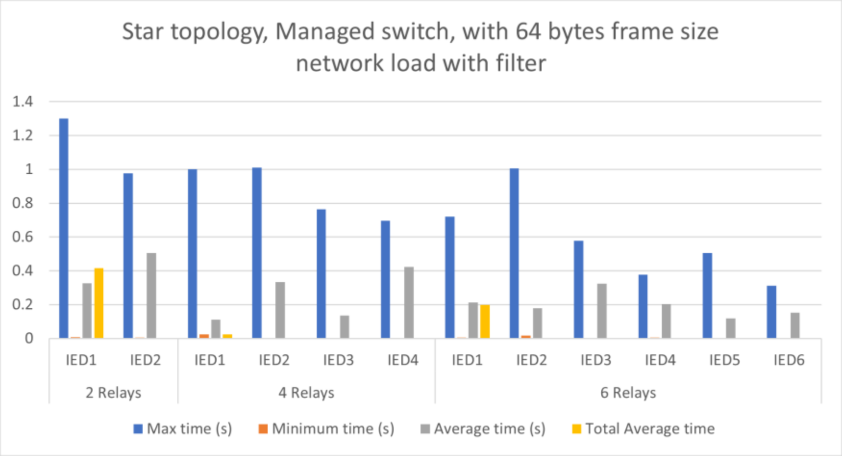


Figure 90. Time Measure of Star Topology Using Managed Switches in Test 5

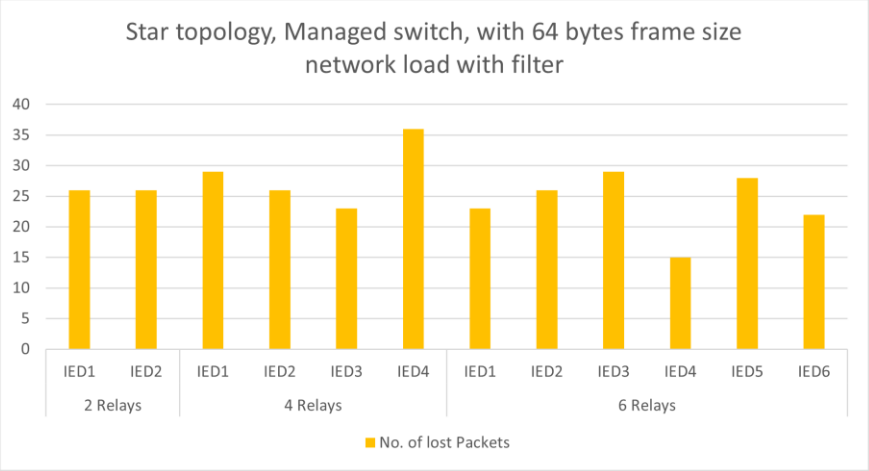


Figure 91. Packet's Loss of Star Topology Using Managed Switches in Test 5

- **Test 6: Star Topology, Network Load with 1500 Bytes, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.9966 | 1.0033 | 0.8906 | 0.5884 | 0.8597 | 0.7828 | 0.9137 | 0.8812 | 0.5052 | 0.5503 | 0.5504 | 0.3076 |
| Minimum time (s) | 0.0010 | 0.0030 | 0.0149 | 0.0108 | 0.0103 | 0.0124 | 0.0018 | 0.0008 | 0.0147 | 0.0014 | 0.0041 | 0.0018 |
| Average time (s) | 0.4916 | 0.2265 | 0.3389 | 0.1708 | 0.2058 | 0.3726 | 0.2273 | 0.0676 | 0.2490 | 0.1388 | 0.2391 | 0.2382 |
| No. of lost Packets | 21 | 24 | 21 | 22 | 28 | 25 | 23 | 34 | 17 | 20 | 23 | 28 |
| Total Average time | 0.3590 | | 0.2720 | | | | 0.1933 | | | | | |

Table 37. Star Topology, Managed Switches, with 1500 Bytes Frame Size Network Load with Filter

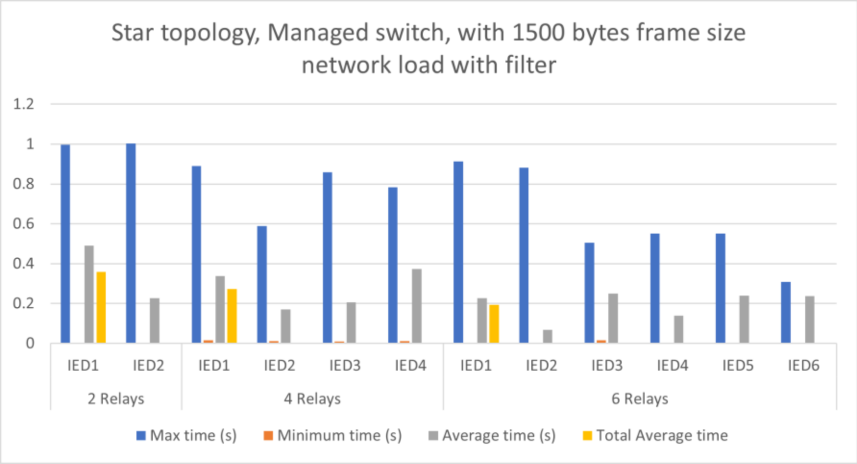


Figure 92. Time Measure of Star Topology Using Managed Switches in Test 6

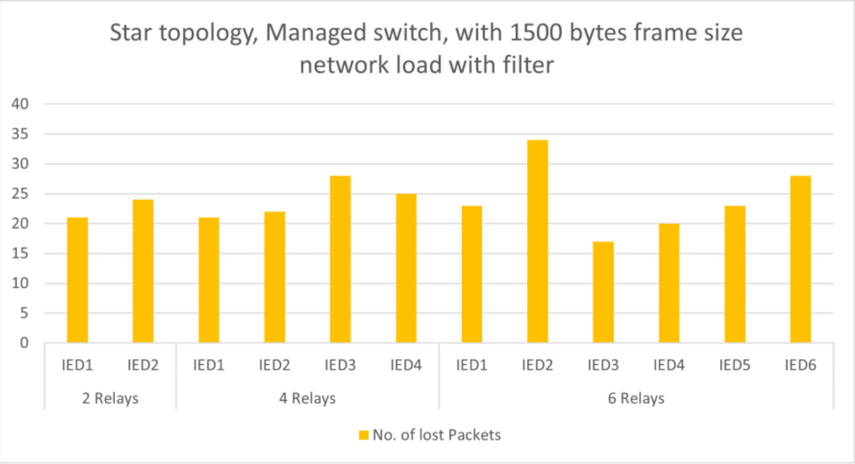


Figure 93. Packet's Loss of Star Topology Using Managed Switches in Test 6

#### 4.5.3.3 Managed Switch Analysis Summary

The results for the managed switch cases connected in a serial topology shows a significant timing variance noted in maximum time results. Note that IED1 had the highest delays among all the other IEDs, the same as shown in the previous sections. IED1 is the first one transmitting frames; therefore, these frames are the slowest of all the others. In addition, some IEDs in tests 1, 2, and 4 had the highest maximum time or delay for delivering the GOOSE messages that reached up to 5.5 seconds, even in cases with no network load and without the applied. In fact, the network load did not seem to play a significant role in increasing the communication layer time. The minimum time increased here more often than with the previous switches even without the latency filter. Another observation worth mentioning is that number of lost packets is approximately between 20 - 40% higher than in the unmanaged switch observation. However, the number of lost packets is higher when there is no network load in the system, and for tests 5 and 6 with load it ranged under 30% of packets lost.

With the star topology, the time result is higher than seen in the serial configuration, as some IEDs especially IED1 from all tests have a maximum time up to 18 seconds, which would be unacceptable for real time operation. Some of the tests with filter had a maximum time of 2 seconds. However, most of the time some of the IEDs sent the GOOSE messages in under 1 second er. As illustrated in the charts, the noted variance between the max time in serial and max time in the star topology ranged from 0.8 seconds and below. This observation of tests with filter show that it influences network performance due to changes in latency it introduced. This action increased the time delay, which reaches up to 1 second in all tests by simulator filter. In the case of lost packets, there was less loss than a serial, which reached under 35% packets lost from a single IED. In addition, a managed switch is a manually operated and programmed switch, and therefore an improvement over previous switch. It is a general this type of switch is most commonly used in practice. As shown in the tables above, the number of lost packets is less than in the hub and unmanaged switch setups, which makes this switch more reliable for delivering the messages without losing too many frames that could disrupt performance.

### 4.5.4 Software-Defined Switch

The final set of tests followed the methods described in Section 4.1, where OpenFlow switches within a Software-Defined Network switch were used to transmit GOOSE messages from multiple IEDs. This test included 6 IEDs publishing GOOSE messages, which was triggered by the same condition as used in the earlier tests. Tests 1 and 4 did not include any network traffic other than the GOOSE messages. Tests 2, 3, 5, and 6 included a network load of nearly 97% to cause a congestion within a very small amount of time. In addition, the frames were used to generate traffic that carried a payload of 64 bytes in tests 2 and 5 and 1500 bytes in tests 3 and 6. This would certainly increase the average time, since the GOOSE messages are processed in a serial manner. The results tables display the slowest captured message (maximum time), the fastest message (minimum time), and the average measured time. In addition, the number of lost packets is calculated out of 100 frames that were captured and analyzed. Many tests were conducted, with the results listed in the tables and figures below. Note that Figures 93 and 94 display a similar design and topologies in the simulation that were seen during previous tests, but OpenFlow management was attached to all three SDN switches and acted as controller, as described in Section 3.4.

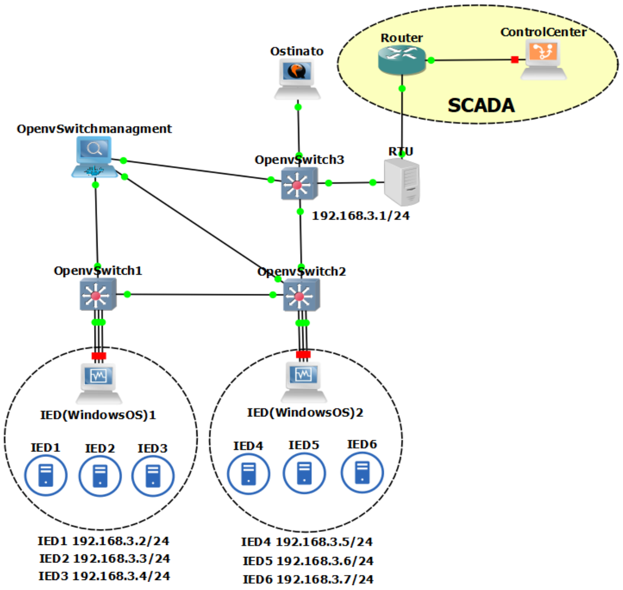


Figure 94. Serial Topology Using OpenvSwitches

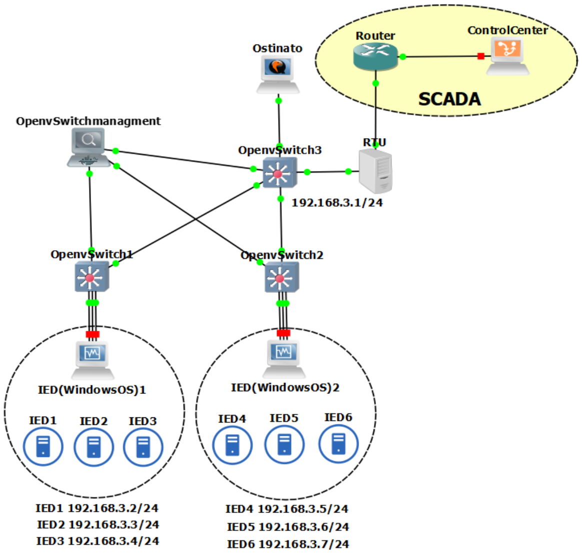


Figure 95. Star Topology Using OpenvSwitches

#### 4.5.4.1 Serial Topology

- **Test 1: Serial Topology, Hub Switch, Zero Network Load and No Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.5939 | 0.9932 | 1.0659 | 0.0444 | 1.0007 | 0.5809 | 1.015 | 0.4528 | 0.3114 | 0.4406 | 0.2166 | 0.2207 |
| Minimum time (s) | 0.0223 | 0.0222 | 0.0001 | 0.0001 | 0.0013 | 0.1452 | 0.0001 | 0.0839 | 0.0910 | 0.0627 | 0.0013 | 0.0481 |
| Average time (s) | 0.0829 | 0.8124 | 0.3875 | 0.0104 | 0.1431 | 0.5068 | 0.1388 | 0.3013 | 0.2143 | 0.1542 | 0.1752 | 0.1358 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.447 | | 0.2619 | | | | 0.1863 | | | | | |

Table 38. Serial Topology, OpenvSwitch, with Zero Network Load and No Filter

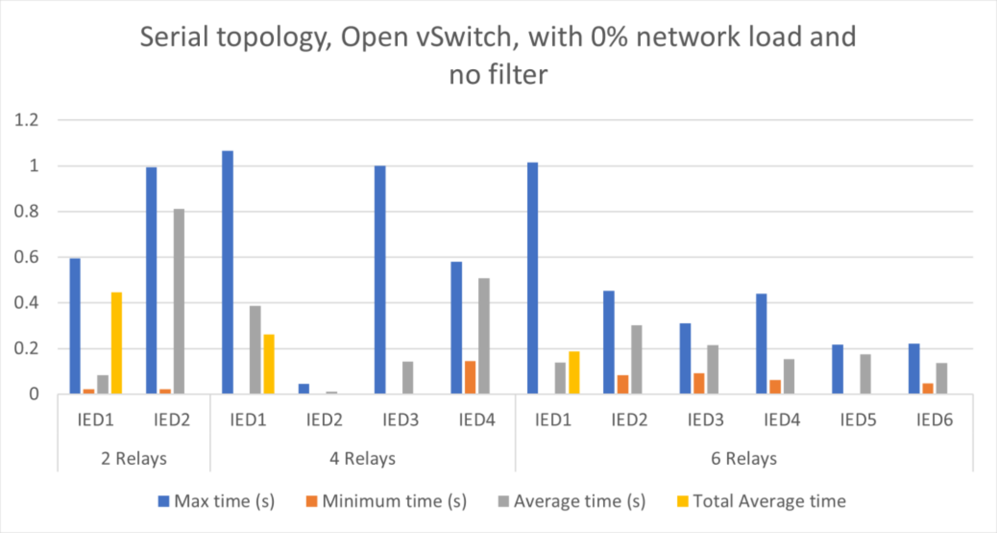


Figure 96. Time Measure of Serial Topology Using OpenvSwitch in Test 1

- **Test 2: Serial Topology, Network Load with 64 Bytes, No Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.8127 | 0.9994 | 0.8551 | 0.0676 | 0.9105 | 0.1450 | 0.5368 | 0.1412 | 0.5053 | 0.2672 | 0.2984 | 0.0935 |
| Minimum time (s) | 0.0016 | 0.0011 | 0.00012 | 0.0028 | 0.0019 | 0.0004 | 0.0001 | 0.0088 | 0.0157 | 0.0012 | 0.0087 | 0.0017 |
| Average time (s) | 0.0674 | 0.4628 | 0.3330 | 0.0361 | 0.2929 | 0.0798 | 0.1466 | 0.0760 | 0.3594 | 0.0863 | 0.2113 | 0.0500 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.2651 | | 0.1854 | | | | 0.1549 | | | | | |

Table 39. Serial Topology, OpenvSwitch, with 64 Bytes Frame Size Network Load and No Filter

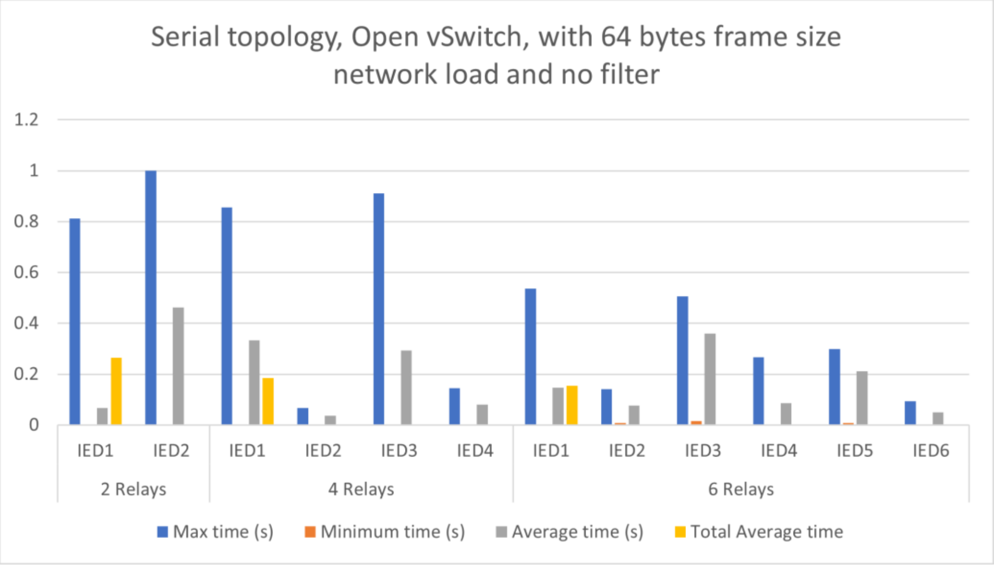


Figure 97. Time Measure of Serial Topology Using OpenvSwitch in Test 2

- **Test 3: Serial Topology, Network Load with 1500 Bytes, No Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.8168 | 0.9188 | 1.0291 | 0.2967 | 0.2498 | 0.2553 | 0.7832 | 0.2492 | 0.1073 | 0.3793 | 0.2871 | 0.2677 |
| Minimum time (s) | 0.0016 | 0.0076 | 0.0089 | 0.0082 | 0.0004 | 0.0098 | 0.0001 | 0.0044 | 0.0001 | 0.0005 | 0.0078 | 0.0011 |
| Average time (s) | 0.1602 | 0.4616 | 0.3556 | 0.2073 | 0.1023 | 0.1772 | 0.2347 | 0.1738 | 0.0447 | 0.2587 | 0.2064 | 0.0663 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.3109 | | 0.2094 | | | | 0.1641 | | | | | |

Table 40. Serial Topology, OpenvSwitch, with 1500 Bytes Frame Size Network Load and No Filter

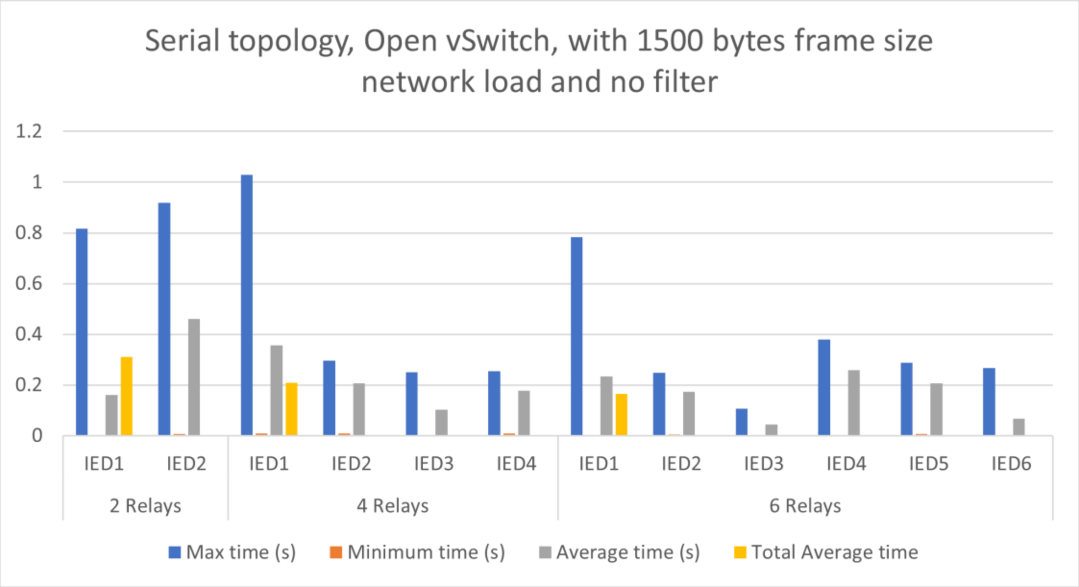


Figure 98. Time Measure of Serial Topology Using OpenvSwitch in Test 3

- **Test 4: Serial Topology, Zero Network Load, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 8.0926 | 2.0159 | 17.566 | 1.2186 | 1.0167 | 1.0046 | 1.0897 | 0.6284 | 0.9133 | 0.2690 | 0.9072 | 0.3283 |
| Minimum time (s) | 0.0061 | 0.1776 | 0.0059 | 0.1442 | 0.0481 | 0.0592 | 0.0001 | 0.0002 | 0.0157 | 0.0934 | 0.0009 | 0.0446 |
| Average time (s) | 0.4095 | 0.9419 | 0.7885 | 0.3759 | 0.2891 | 0.2116 | 0.3530 | 0.0502 | 0.6762 | 0.1633 | 0.1084 | 0.1593 |
| No. of lost packets | 24 | 19 | 29 | 26 | 33 | 27 | 32 | 27 | 30 | 39 | 20 | 24 |
| Total average time | 0.6756 | | 0.4163 | | | | 0.2517 | | | | | |

Table 41. Serial Topology, OpenvSwitch, with Zero Network Load with Filter

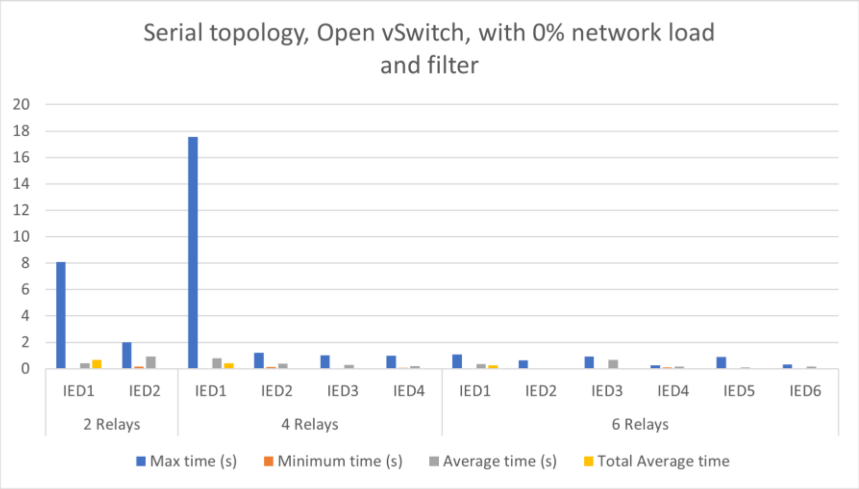


Figure 99. Time Measure of Serial Topology Using OpenvSwitch in Test 4

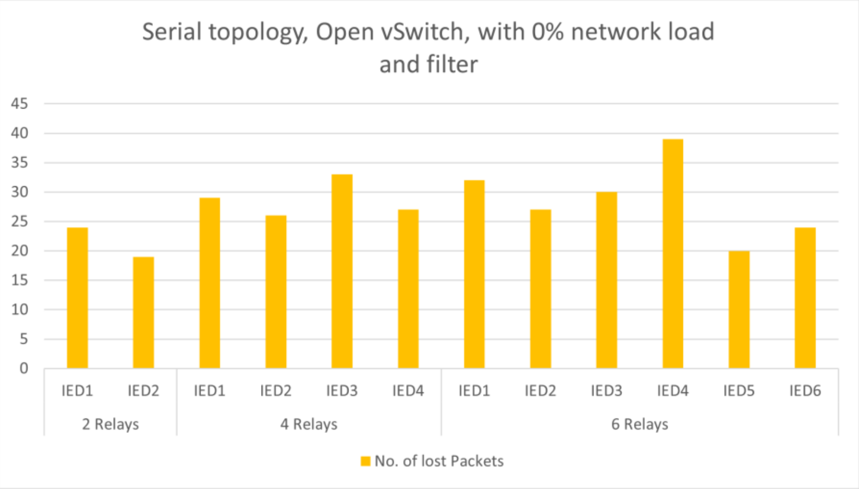
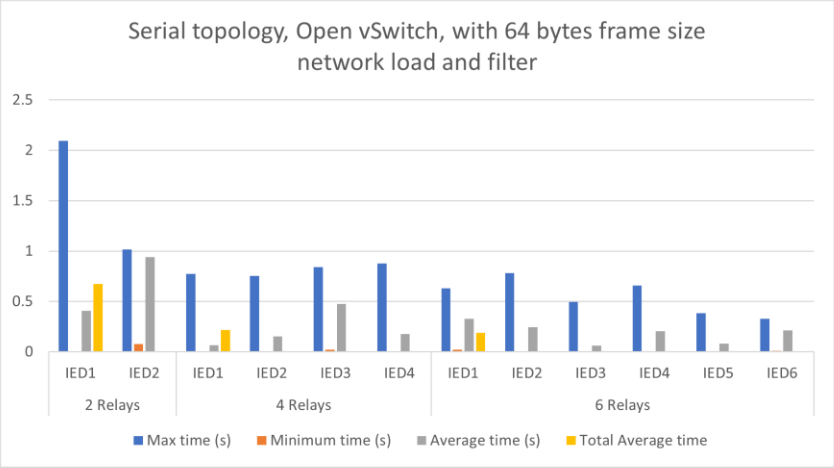


Figure 100. Packet's Loss of Serial Topology Using OpenvSwitch in Test 4

- **Test 5: Serial Topology, Network Load with 64 bytes, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 2.0926 | 1.0159 | 0.7751 | 0.7525 | 0.8424 | 0.8761 | 0.6316 | 0.7798 | 0.4965 | 0.6563 | 0.3819 | 0.3281 |
| Minimum time (s) | 0.0001 | 0.0776 | 0.0001 | 0.0040 | 0.0211 | 0.0026 | 0.0224 | 0.0008 | 0.0014 | 0.0035 | 0.0002 | 0.0095 |
| Average time (s) | 0.4095 | 0.9419 | 0.0676 | 0.1531 | 0.4765 | 0.1751 | 0.3288 | 0.2464 | 0.0625 | 0.2044 | 0.0826 | 0.2134 |
| No. of lost packets | 23 | 18 | 26 | 29 | 21 | 23 | 25 | 20 | 22 | 18 | 26 | 28 |
| Total average time | .6756 | | 0.2181 | | | | 0.1897 | | | | | |

Table 42. Serial Topology, OpenvSwitch, with 64 Bytes Frame Size Network Load and Filter



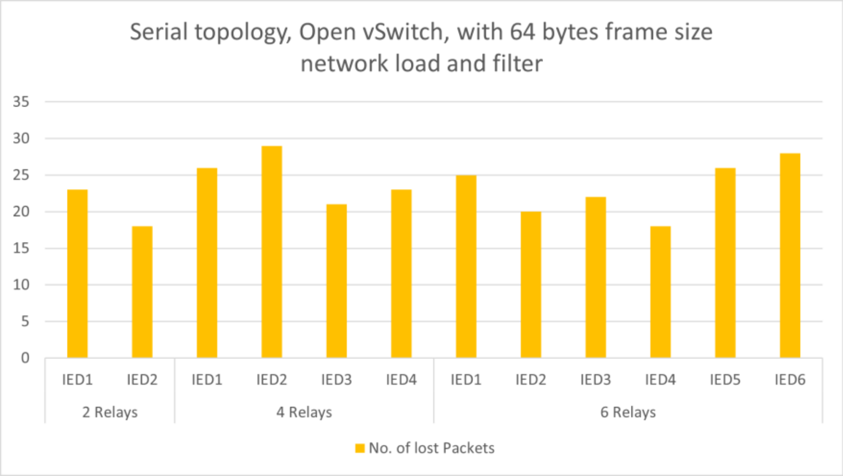


Figure 101. Time Measure of Serial Topology Using OpenvSwitch in Test 5

Figure 102. Packet's Loss of Serial Topology Using OpenvSwitch in Test 5

- **Test 6: Serial Topology, Network Load with 1500 Bytes, with Filter**

| **Serial Topology, OpenvSwitch, with 1500 Bytes Frame Size Network Load and Filter** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.0306 | 1.3909 | 0.5277 | 0.9749 | 1.1841 | 0.7585 | 0.9710 | 0.6350 | 0.7285 | 0.4366 | 0.4131 | 0.3160 |
| Minimum time (s) | 0.0001 | 0.0010 | 0.0405 | 0.0035 | 0.0151 | 0.0007 | 0.0309 | 0.0017 | 0.0053 | 0.0236 | 0.0013 | 0.00005 |
| Average time (s) | 0.4585 | 0.2282 | 0.2299 | 0.2542 | 0.2083 | 0.1769 | 0.4323 | 0.1383 | 0.1419 | 0.2690 | 0.0730 | 0.1802 |
| No. of lost packets | 28 | 23 | 25 | 17 | 30 | 22 | 30 | 19 | 24 | 26 | 25 | 29 |
| Total average time | 0.3434 | | 0.2423 | | | | 0.1802 | | | | | |

Table 43. Serial Topology, OpenvSwitch, with 1500 Bytes Frame Size Network Load and Filter

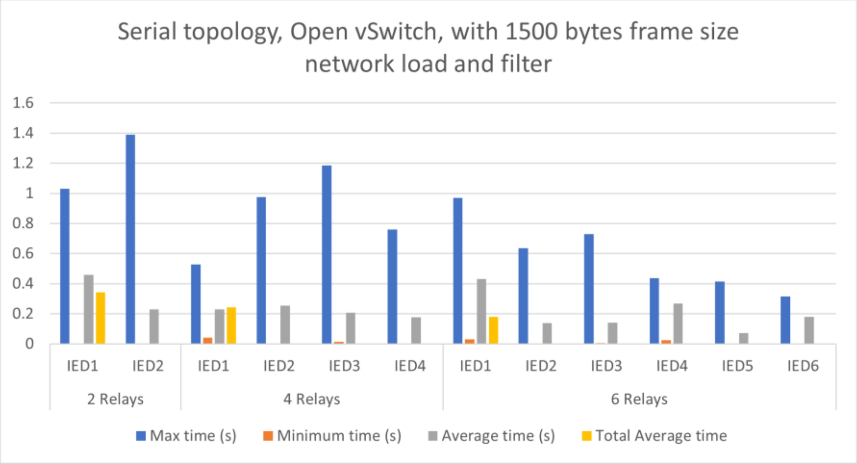


Figure 103. Time Measure of Serial Topology Using OpenvSwitch in Test 6

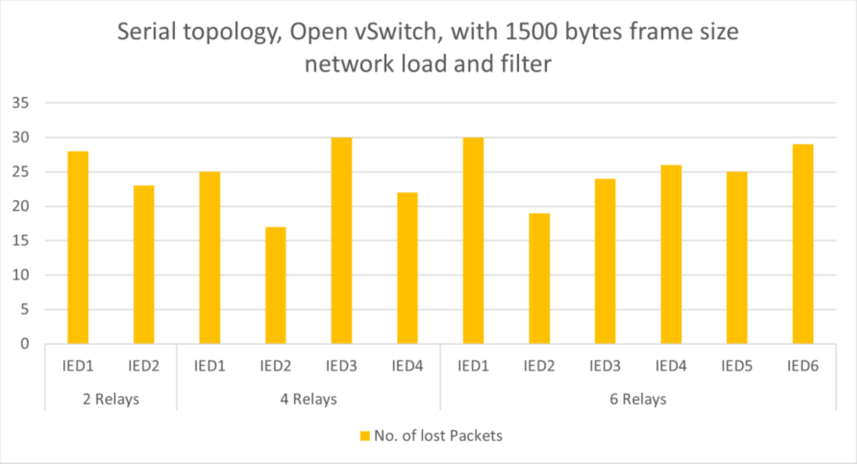


Figure 104.Packet's Loss of Serial Topology Using OpenvSwitch in Test 6

#### 4.5.4.2 Star Topology

- **Test 1: Star Topology, Zero Network Load, and No Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 22.416 | 0.3761 | 3.6829 | 0.9734 | 0.2645 | 0.4231 | 15.378 | 0.5870 | 0.1574 | 0.0898 | 0.1746 | 0.2518 |
| Minimum time (s) | 0.0448 | 0.0234 | 0.0011 | 0.0666 | 0.0166 | 0.0185 | 0.0125 | 0.0376 | 0.0010 | 0.0018 | 0.1243 | 0.0001 |
| Average time (s) | 0.9057 | 0.2827 | 0.0871 | 0.4870 | 0.1687 | 0.3341 | 0.3095 | 0.5123 | 0.0744 | 0.0506 | 0.1511 | 0.00008 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.5942 | | 0.2692 | | | | 0.2042 | | | | | |

Table 44. Star Topology, OpenvSwitch, with Zero Network Load and No Filter

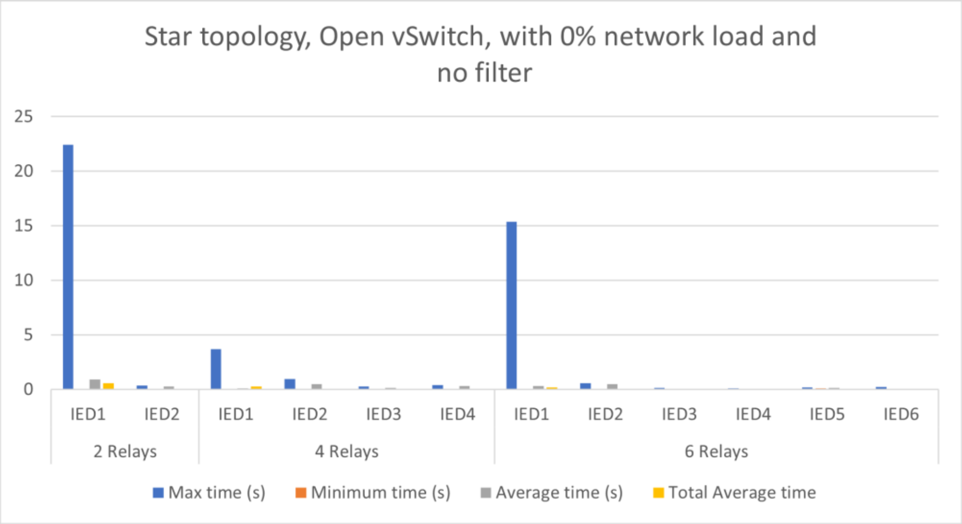


Figure 105. Time Measure of Star Topology Using OpenvSwitch in Test 1

- **Test 2: Star Topology, Network Load with 64 Bytes and No Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.8442 | 0.8781 | 0.4052 | 0.4533 | 0.5322 | 0.4236 | 0.4024 | 0.9155 | 0.2692 | 0.5134 | 0.1275 | 0.3938 |
| Minimum time (s) | 0.0052 | 0.0054 | 0.0116 | 0.0066 | 0.0063 | 0.0001 | 0.0015 | 0.0091 | 0.0087 | 0.0086 | 0.0003 | 0.0016 |
| Average time (s) | 0.1666 | 0.4827 | 0.0885 | 0.1789 | 0.3001 | 0.2465 | 0.0635 | 0.1788 | 0.1967 | 0.1596 | 0.0836 | 0.2875 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.3247 | | 0.2035 | | | | 0.1615 | | | | | |

Table 45. Star Topology, OpenvSwitch, with 64 Bytes Frame Size Network Load and No Filter

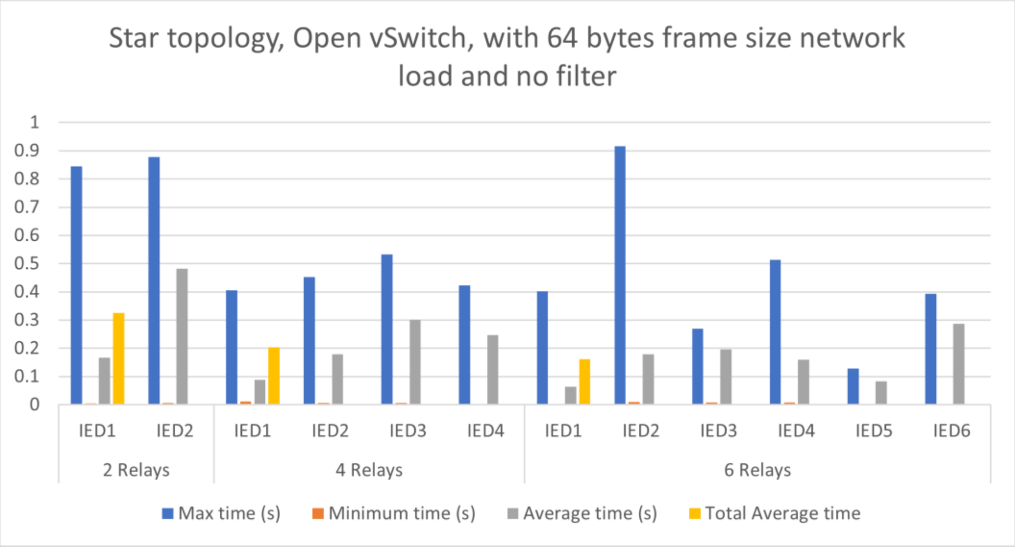


Figure 106. Time Measure of Star Topology Using OpenvSwitch in Test 2

- **Test 3: Star Topology, Network Load with 1500 Bytes and No Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.9520 | 0.1924 | 1.0071 | 0.4532 | 0.1290 | 0.3924 | 0.9943 | 0.8733 | 0.0934 | 0.3379 | 0.5577 | 0.0778 |
| Minimum time (s) | 0.0088 | 0.0149 | 0.0110 | 0.0039 | 0.0043 | 0.0036 | 0.00009 | 0.0031 | 0.0010 | 0.0194 | 0.0061 | 0.00008 |
| Average time (s) | 0.4599 | 0.1477 | 0.3939 | 0.1130 | 0.0826 | 0.2480 | 0.0474 | 0.3094 | 0.0243 | 0.1484 | 0.3737 | 0.0134 |
| No. of lost packets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total average time | 0.3038 | | 0.2094 | | | | 0.1528 | | | | | |

Table 46. Star Topology, OpenvSwitch, with 1500 Bytes Frame Size Network Load and No Filter

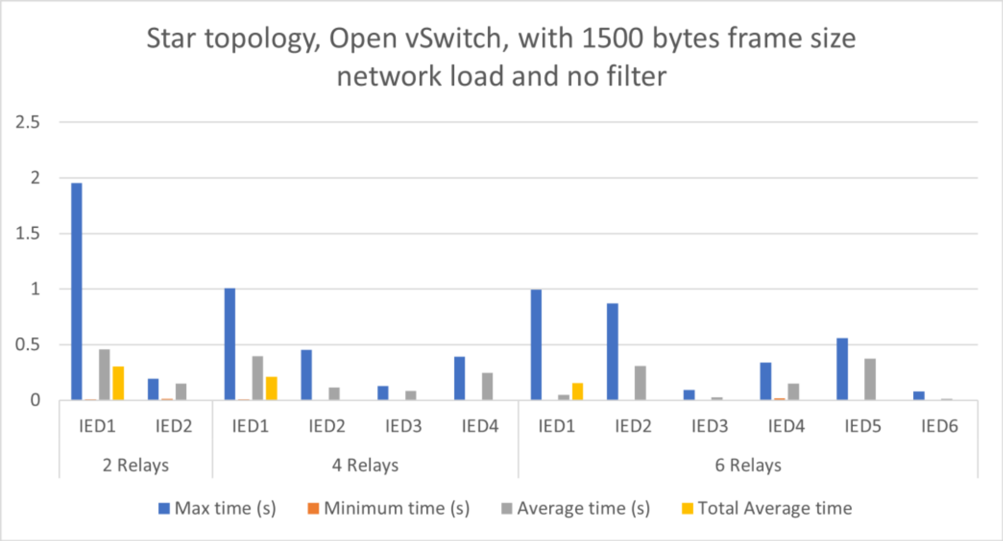


Figure 107. Time Measure of Star Topology Using OpenvSwitch in Test 3

- **Test 4: Star Topology, Zero Network Load, with Filter**

| No. of IEDs<br>Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.2119 | 1.6579 | 2.1628 | 0.3290 | 1.0140 | 0.9717 | 1.0172 | 1.7142 | 0.6521 | 0.7806 | 0.5827 | 0.5275 |
| Minimum time (s) | 0.0731 | 0.1487 | 0.3300 | 0.0110 | 0.1251 | 0.0026 | 0.0001 | 0.0095 | 0.0040 | 0.0852 | 0.0359 | 0.0003 |
| Average time (s) | 0.3554 | 0.8337 | 0.7508 | 0.1014 | 0.3502 | 0.1173 | 0.4550 | 0.1593 | 0.1662 | 0.3173 | 0.1056 | 0.2318 |
| No. of lost packets | 22 | 23 | 22 | 29 | 20 | 24 | 24 | 20 | 28 | 29 | 25 | 21 |
| Total average time | 0.5945 | | 0.3299 | | | | 0.2392 | | | | | |

Table 47. Star Topology, OpenvSwitch, Zero Network Load and Filter

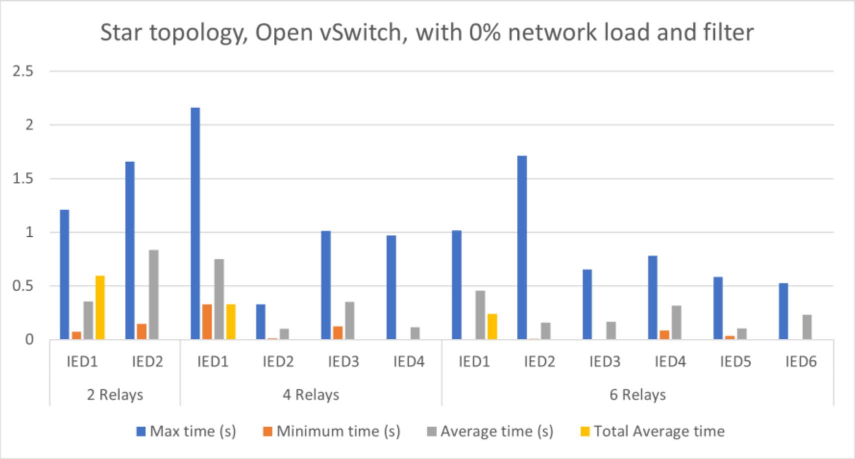


Figure 108. Time Measure of Star Topology Using OpenvSwitch in Test 4

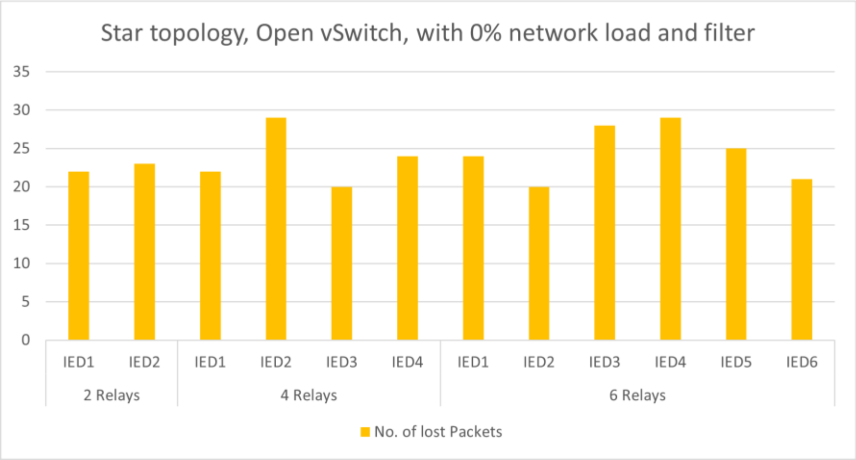


Figure 109. Packet’s Loss of Star Topology Using OpenvSwitch in Test 4

- **Test 5: Star Topology, Network Load with 64 Bytes, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 1.2299 | 1.0010 | 1.0087 | 0.7960 | 0.6762 | 0.9451 | 0.5627 | 0.8069 | 0.4704 | 0.4976 | 0.5815 | 0.4691 |
| Minimum time (s) | 0.0072 | 0.0088 | 0.0035 | 0.0066 | 0.0132 | 0.0111 | 0.0058 | 0.0074 | 0.0012 | 0.00005 | 0.0015 | 0.0060 |
| Average time (s) | 0.2634 | 0.5337 | 0.1907 | 0.2378 | 0.2254 | 0.3777 | 0.2438 | 0.3171 | 0.1182 | 0.0573 | 0.1938 | 0.2408 |
| No. of lost packets | 23 | 28 | 21 | 25 | 30 | 20 | 22 | 27 | 19 | 29 | 25 | 27 |
| Total average time | 0.3986 | | 0.2579 | | | | 0.1952 | | | | | |

Table 48. Star Topology, OpenvSwitch, with 64 Bytes Frame Size Network Load and Filter

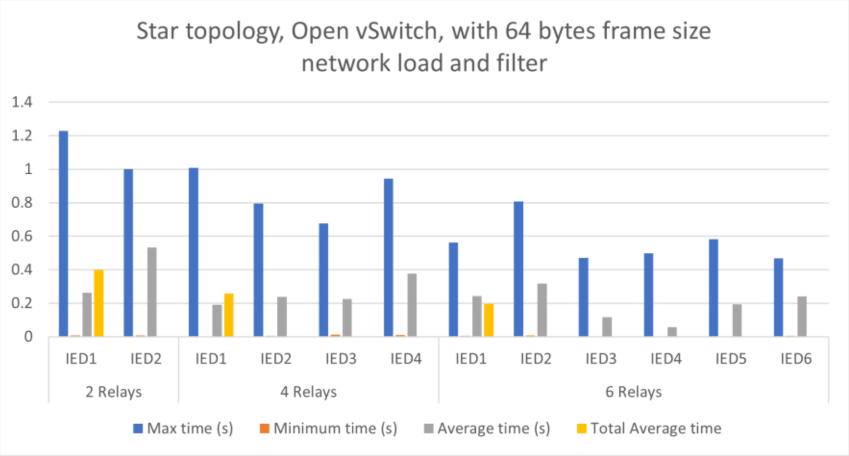


Figure 110. Time Measure of Star Topology Using OpenvSwitch in Test 5

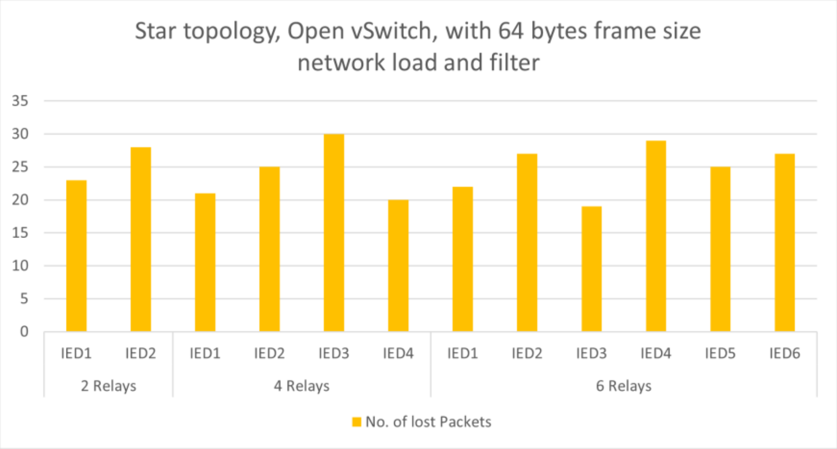


Figure 111. Packet's Loss of Star Topology Using OpenvSwitch in Test 5

- **Test 6: Star Topology, Network Load with 1500 Bytes, with Filter**

| No. of IEDs / Time | 2 Relays | | 4 Relays | | | | 6 Relays | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | IED1 | IED2 | IED1 | IED2 | IED3 | IED4 | IED1 | IED2 | IED3 | IED4 | IED5 | IED6 |
| Max time (s) | 0.9995 | 1.0205 | 0.7496 | 0.8929 | 0.3094 | 0.8358 | 0.9341 | 1.0009 | 0.7641 | 0.2941 | 0.8877 | 0.6600 |
| Minimum time (s) | 0.0235 | 0.0071 | 0.0088 | 0.0096 | 0.0021 | 0.0234 | 0.0071 | 0.0016 | 0.0098 | 0.02653 | 0.0046 | 0.0020 |
| Average time (s) | 0.5243 | 0.2305 | 0.2567 | 0.2261 | 0.1108 | 0.4358 | 0.1869 | 0.0511 | 0.3586 | 0.2008 | 0.2273 | 0.0943 |
| No. of lost Packets | 28 | 27 | 21 | 22 | 22 | 16 | 29 | 17 | 24 | 23 | 29 | 25 |
| Total Average time | 0.3774 | | 0.2574 | | | | 0.1865 | | | | | |

Table 49. Star Topology, OpenvSwitch, with 1500 Bytes Frame Size Network Load and Filter

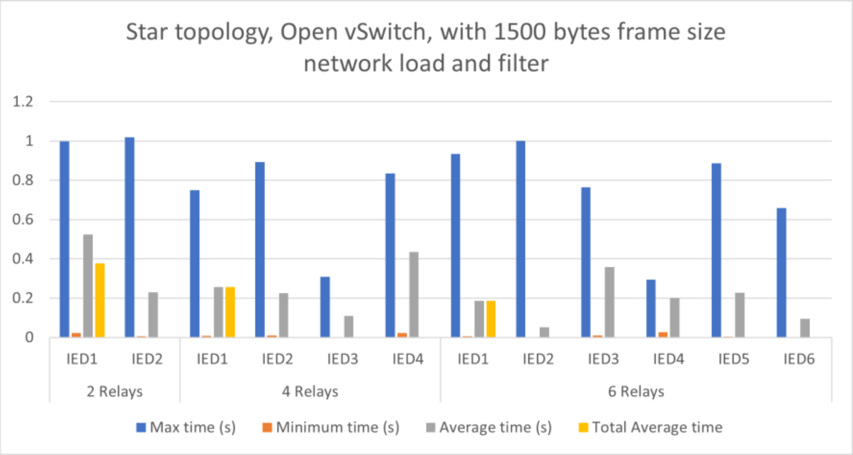


Figure 112. Time Measure of Star Topology Using OpenvSwitch in Test 6

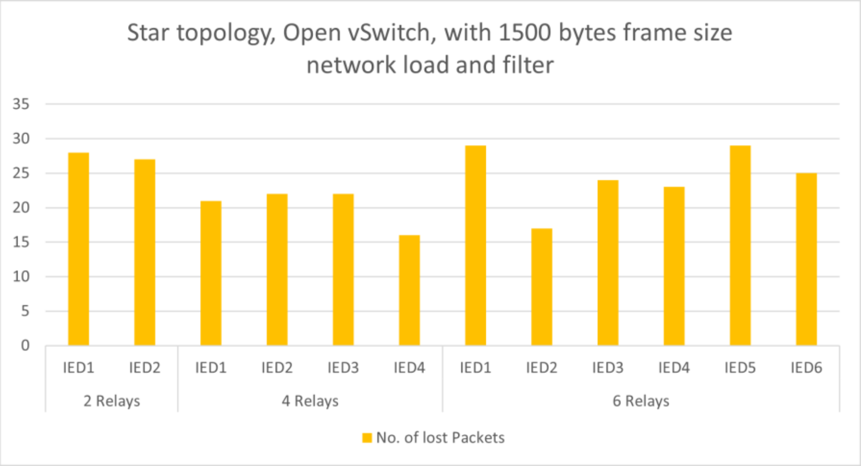


Figure 113. Packet's Loss of Star Topology Using OpenvSwitch in Test 6

#### 4.5.4.3 SDN Summary Analysis

The SDN switch test results with a serial topology show a significant timing variance in the maximum time results. Note that the IED1 had the highest delays among all the IEDs, as was the case with the other switch types. IED1 is the first one transmitting the frames; therefore, these frames are the slowest of all the others. In addition, some IEDs in tests 1, 4, and 5 had a higher maximum time or delay for delivering the GOOSE messages, reaching up to 17 seconds and applying the filter did not increase delay. In fact, the network load did seem to play a significant role in increasing the communication layer time. As shown in the charts, each test under SDN switch is consistently under 1 second in some tests that used a filter, which slightly more than other switch tests. The minimum time increased more often than for the previous switches, especially without using the latency filter and with zero network load. Another observation is that the number of lost packets is approximately between 20 - 40%, which is similar what was observed using  the managed switched. However, the number of lost packets is higher in SDN tests when there is no network load in the system and the lost packets for the loaded tests, tests 5 and 6 ranged under 30 lost packets.

For the star topology, maximum time results were higher than a serial result, as some of IEDs especially IED1 in all tests has a maximum time delay reach to 22 seconds. Test 1 achieved the highest maximum time among all other tests. Some of the tests where a filter was used had a maximum time that reached 2 seconds. Furthermore, most of the time, some IEDs sent the GOOSE messages in an estimated time of 1 second or less. The charts above noted that a variance between the max time in serial and max time in star ranged from 1 and below. These observations of tests with filter noted that the filter has an influence on the network performance due to the changes in latency. This act increased time delay, which reached up to 1 second in all tests with a simulator filter.

In the case of lost packets, there are fewer lost than with a serial configuration, which falls under 30 packets lost out of 100 packets in a single IED. In addition, a SDN switch is a controllable and manually programmable switch; therefore, it is more advanced than managed switches due to separation of control from the payload data, which makes it easy to program the entire network with a single center. SDN switches are modern switches that have been used for communications in industrial substations. As shown in the tables in Section 4.5.4, the number of lost packets is less than was the case with the hub, unmanaged, and managed switches, which makes this switch more reliable and dependable for delivering the messages without losing too many frames that could disrupt the substation performance.

The time taken for the GOOSE messages to reach their destination is the most important factor that can be used to measure the performance of a switch. In addition, the number of frames lost in transit through the switch is another important aspect that can be used to evaluate the switch's performance. Note that the switch average time seems to be equal to the managed switch. This test was expected, as previous tests on managed switches demonstrated that network load does not increase the amount of time the communication layer takes, thus resulting in similar positions test times. The total average time ranged from 0.5 to 0.2 seconds, which is consistent with the expected results.

### 4.6 Analysis and Summary

This chapter presents the results of 48 tests. Out of all these tests, note that not a single instance of a failed test or dropped frame in tests that did not use a filter. However, after using the simulator filter to model network media performance problems there were some losses in packets, and they always ranged at the same number in all switches. The test results demonstrated high reliability and consistency of the simulated switches for this investigation. This level of reliability was maintained despite extremely high network load conditions simulated in the network. The author believes that the average amount of network load used in these test cases are unlikely to occur within a substation automation system since such networks are separated from the general Internet. Even though the GOOSE messages were found to be 100% reliable in all switches, there was a significant timing variance noted in the test results. Noticed that, as previously described, the maximum time takes from 0.2 to 1 seconds in some of IEDs, which is a bit long for GOOSE messages. However, there are some abnormal cases IEDs where they reach 20 seconds, which is quite inefficient transmission.

Another observation worth mentioning is the fact that network load did not seem to play a significant role in increasing the communication time in delivering the GOOSE messages. It was rather the size of the artificial load that transmitting frames data set that played the most significant role in increasing the time it took the message to reach its destination. It was noted that tests seem to display an up and down zigzag pattern, which has approximately the same result in each test. The reason why these results were obtained was not known. There was no reason identified to explain why the test results behaved in this way. In addition, it seems there were no significant differences between all the switches in time and latency, especially since the delivered GOOSE packets time largely took less than 1 second, eliminating the possibility of any type of processing congestion issues or major delays when applying any of these switches in a network.

From a security perspective, unmanaged switches have very basic physical security. They are equipped with built-in security features called lockable port covers that prevent unauthorized access. However, an unmanaged switch has open ports that put the switch at a high-security risk. On the other hand, a managed switch has a security protocol for data, management, and control planes. Some of the security benefits of managed switches are their ability to monitor and control the entire network, as well as their ability to provide various protection options. Nevertheless, managed switches can be difficult to control and monitor, and therefore they should only be monitored and controlled by a network technician with the highest level of privileges. The managed switch can be configured such that collisions occur in a full-duplex network configuration since it has a spanning-tree protocol that prevents a loop from being established.

A dynamic network has a central controller that constantly exchanges network control traffic with its various switches. It can be considered a major vulnerability for a SDN because of the high amount of traffic that it handles. This potentially makes it vulnerable to DoS attacks. However, if security controls have been designed and implemented correctly, they should be able to detect and prevent DoS attacks. In addition, data spoofing may be less likely to occur in SDN compared to other Ethernet switches because the nature of SDN updates it is possible to discover the changes quickly. Both managed and SDN switches have advantages in any looped network due to their spanning protocols technique; however, SDN has a complex configuration, which leads to a high risk of security threats due to configuration errors. In summary, the following conclusions can be drawn based on the test results:

1. In general, all switch types have similar levels of packet loss and time latency.
2. Test results indicate that both are heavy network load affect the speed at which GOOSE messages transit the communication network. The timing ranges between 0.2 to 1 seconds.
3. Managed switches and SDN switches have enhanced capabilities compared to the hub and unmanaged switches.

4. The star topology is more reliable than serial topology and faster in delivering GOOSE messages; however, it has higher packet loss than a serial topology.
5. As one might expect, the biggest factor that contributes to GOOSE message latency is the filter to simulator non-ideal behavior of the transmission media. This factor delayed the average time of the captured packets by 5%.
6. By injecting the network more load of any frames that are associated with GOOSE messages in the network; it will increase the GOOSE messages speed and increase the level of performance of the network in substation, as shown in the tests.
7. Unmanaged switches and hub are easy to use since they are a plug-and-play switches, but the security risk level is excessive.
8. The managed switches are more reliable and secure than an unmanaged Ethernet switch, but they have a higher cost and need more programming time.
9. SDN switches are less secure against DoS attacks but more secure against spoofing attacks due their ability to dynamically change the network. They have a higher cost and are more complicated to program.

# Chapter 5: Summary, Conlclusions and Future Work

The IEC 61850 family of standards is a widely used standard for the materialization of smart grid in many countries and is starting to see use in the United States. It has been acknowledged by the National Institute for Standards and Technology as a potential key component of the smart energy system [cite reference]. The research covered in this document evaluates the the capability of emulated Ethernet switches to transmit GOOSE messages in various types and their ability to transport information in an almost real time. This work has aimed to provide an overview of the a few research activities that can be used to real-time control communication technologies.

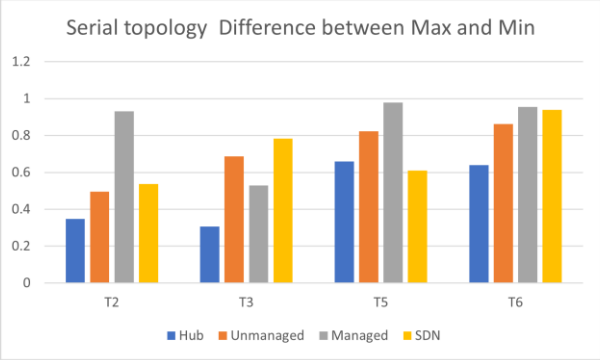
The IEC 61850 framework is an ideal platform for building robust, yet simple, automation applications. Its ability to organize and mobilize data from multiple devices enables them to be easily integrated and utilized. As communication networks in modern power substations network have increased in both size and complexity of topologies, it is important to maintain high levels of reliability, availability, and security. The proper implementation of time-sensitive functions such as monitoring and the protection of a substation automation system in the electric power system requires a high-speed communication system. The performance characteristics of Ethernet switches were presented in this thesis in terms of handling data traffic in the worst-case scenarios. A substation control network architecture using Ethernet switches was reviewed. An examination of Ethernet switches is critical to figure which are more suitable and reliable than the others. The reliable transmission of packets and traffic flow in a substation is important for the the performance of networks.

## 5.1 Research Summary

Chapter 4 demonstrated the capabilities in terms of speed, loss, and reliability of transmitting GOOSE messages in various Ethernet switch types. Simulation tests were run and demonstrated the performance of the Ethernet switch in transmitting GOOSE messages is well within the specifications presented in the standard. One of the accomplishments was to compare the performance of multiple types of Ethernet switches in simulation using a small and maximum payload, for transferring GOOSE messages during periods of very high network load. This observation is very interesting as it shows how effective Ethernet switches are in ensuring the delivery of all messages due to the Ethernet switch’s ability to provide buffering and fast-switching times. However, note that Table 50 and Figures 113 and 114 show a very small degradation of performance, especially for the Hub switch both topologies in tests 2, 3, 5, and 6. However, there is a major delay in the Hub switch in tests 1 and 4 that is higher than any other Ethernet switch for both network topologies. Furthermore, the filter to emulate network media degradation did affect the network performance even when the payload was included in both topologies.

| Switch Type | Serial topology difference between max and min time | | | | Star topology difference between max and min time | | | |
|---|---|---|---|---|---|---|---|---|
| | Test 2 | Test 3 | Test 5 | Test 6 | Test 2 | Test 3 | Test 5 | Test 6 |
| Hub | 0.348 | 0.306 | 0.659 | 0.640 | 0.132 | 0.459 | 0.899 | 0.814 |
| Unmanaged | 0.495 | 0.687 | 0.822 | 0.862 | 0.556 | 0.301 | 1.002 | 1.006 |
| Managed | 0.931 | 0.529 | 0.979 | 0.954 | 1.001 | 0.442 | 0.713 | 0.911 |
| SDN | 0.536 | 0.783 | 0.609 | 0.940 | 0.400 | 0.994 | 0.556 | 0.927 |

Table 50. Summary of Test Results with Network Load



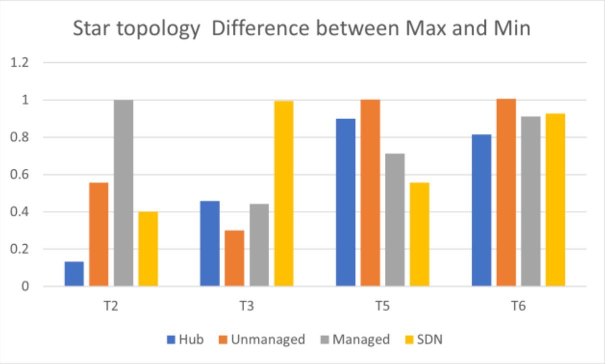


Figure 114. Time Measure of Serial Topology Summary

Figure 115. Time Measure of Star Topology Summary

| Switch Type | Star topology difference between max and min time | | serial topology difference between max and min time | |
|---|---|---|---|---|
| | Test 1 | Test 4 | Test 1 | Test 4 |
| Hub | 6.979 | 11.99 | 7.801 | 1.023 |
| Unmanaged | 2.985 | 1.407 | 1.025 | 2.035 |
| Managed | 1.015 | 3.045 | 0.999 | 2.017 |
| SDN | 1.014 | 1.089 | 15.365 | 1.017 |

Table 51. Summary of Test Results Without Network Load

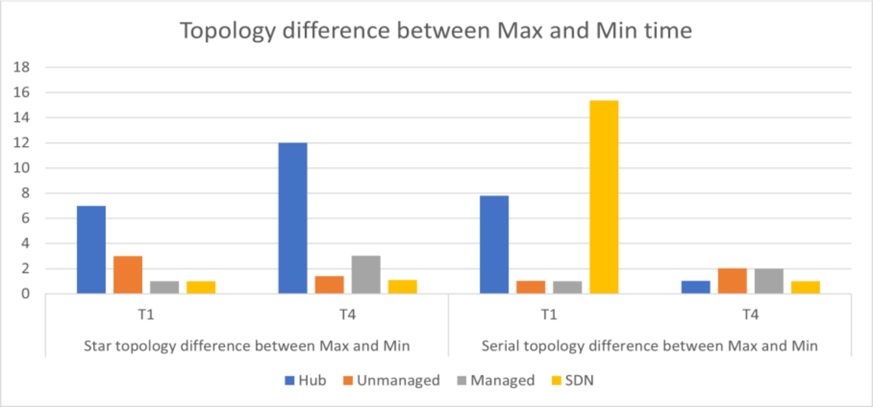


Figure 116. Time Measure Summary

The second finding of the tests was the fact that network load influences the performance of the GOOSE messages' transfer speed. A minor increase in speed was recorded when publishing GOOSE messages with many frames with other payloads included in the same network. As shown in Table 51 and Figure 115, there was a significant increase in time in tests 1 and 4 for different types of switches. This observation should be taken into consideration during the design stage of any communications network projects and ensure that the network carrying GOOSE messages sees little other traffic. A frame generator application kept sending empty data frames and kept the Ethernet switch standing and ready for any circumstances. This helped GOOSE messages, or any important data are delivered more rapidly.

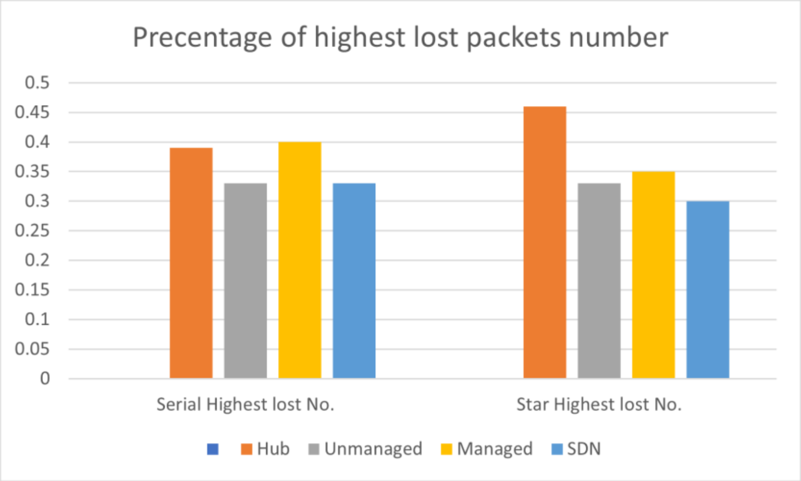


Figure 117. Packet Loss Summary

| Switch Type | Highest Serial Topology Lost Number | Highest Star Topology Lost Number |
|---|---|---|
| Hub | 39% | 46% |
| Unmanaged | 33% | 33% |
| Managed | 40% | 35% |
| SDN | 33% | 30% |

Table 52. Summary of Test Results of Packet Loss

The percentage of GOOSE messages that can be lost in the experiment is relevant. Even with a retransmission mechanism, which is used for sending messages to other GOOSE subscribers, only 60-65% of the messages can be published by a single IED and received by the RTU. Figure 116 illustrates and demonstrates this point based on a Wireshark capture. The network GOOSE messages that can be generated to accomplish a trip operation were a very large number. The tests went on to explore the network load created by retransmission of GOOSE messages under abnormal circumstances, and the Ethernet switch will transmit as many frames as possible. As such, a filter simulating degradation  added 5% to packets lost has a major impact since the IED can transmit only 100 frames. The tests revealed that GOOSE message network load was applied on all switch types on both topologies and have the nearly the same values of lost packets. This value is very large compared to the transmitted packets in tests without a filter.

### 5.2 Conclusion

The selection of the right network topology and switch type is very important to a successful network design. However, achieving a balance between the various requirements can be challenging. Requirements such as efficiency, reliability, real-time performance, and costs are hard to achieve at the same time and cannot be simultaneously satisfied. However, the results obtained by the various switch types relate to the expected operation of a communication network. The GOOSE message transmission algorithm, which takes advantage of the serial and star topologies, performed well in all switches. This work was limited to two topologies only because the hub switch and the unmanaged switch cannot handle a loop method in a ring topology since they lack the spamming protocol. In summary, the following conclusions can draw based on the results of the tests:

1. A hub switch is faster when there is a network load but slower without the network load. In addition, the hub experiences more packet loss compared to the others, especially in a star topology.

2. The unmanaged switch is more stable relative to other switches and has the lowest packets lost and cost.
3. A managed switch has the highest time rank; however, some tests show a quicker speed in time for the other switches, and all have a steady packet loss performance in both topologies in a filter test.
4. SDN has a complex programming mechanism, but it had the same rank as a managed switch in speed; however, the number of packets lost is fewer in star topology when the number of switches is less.
5. By far, the topology that contributes most to GOOSE message loss is star topology; this topology causes the loss to increase by 40%.
6. The timing could vary anywhere between 0.1% - 16%. Increasing network load helps in increasing the speed of GOOSE messages through the network.
7. Test results indicate that star topology has an impact in increasing the speed of GOOSE messages and is more reliable than a serial topology, but only by 0.1%.
8. The unmanaged switch and hub are usually easy to use, but they have a higher security risk level. Usually, the managed switch is more secure and reliable, but it is an expensive switch.
9. A managed switch is more secure and reliable than an Ethernet switch, but it consumes a programming time and costs more.
10. SDN is more secure against DoS attack but less secure against spoofing attack because of its dynamic programming changing. It also requires more programming time and costs more.

| Switch Type | Speed Rate | Packet Loss | Security Ability | Programming Complexity | Filter Affect | Network Load Help Speed Rate |
|---|---|---|---|---|---|---|
| Hub | high | 46% | No | No | Yes | Yes |
| Unmanaged | moderate | 33% | No | No | Yes | Yes |
| Managed | high | 40% | Yes | Yes | No | Yes |
| SDN | moderate | 33% | Yes | Yes | Yes | Yes |

Table 53. Comparison Summary

### 5.3 Future Work

This topic will be of interest to students learning the field of electric power grid modernization. As automation and efficiency gain widespread acceptance, this field will be evaluated to see how it can improve the reliability and efficiency of the grid. With the increasing popularity of IEC 61850, further research and education is needed to make system operators comfortable with these new features.

#### 5.3.1 Simulating More Topologies

This work was limited to two topologies only; therefore, future work should address these limitations and build on this research by collecting data from other topologies such as ring, hybrid, redundant, etc. This next step would be to examine other topologies using specific Ethernet switches, especially managed and SDN switches, because they have a spanning protocol. In addition, this examination should predict if a frame is dropped or not based on filter factors that the GNS3 program has with the same test requirements such as network load and traffic type. These test cases should be able to predict the operation of an Ethernet switch network based on its configuration. It should also be able to provide a measure of the degree of accuracy in transmitting GOOSE messages. Additionally, the findings should also reveal that the time spent on transmitting the frames is largely dependent on the Ethernet switch and could be used to develop new network design connectivity.

#### 5.3.2 Perform Simulation Tests on IEC 61850 Using Sampled Values Signals

IEC 61850 9-2 establishes a protocol that enables measurement application specific IEDs to distribute processed measurement over a network, eliminating the need for physical cabling for voltage and current measurements. These sampled values are broadcast in a synchronous fashion. This protocol eliminates the need for protective relays to connect to instrument transformers i for analog voltage and current signals. Performing network load and reliability tests with SV in the same fashion as the tests in Chapter 4, on a wide variety of Ethernet switches to help determine necessary network capabilities. Simulation tests should be conducted to compare the response of multiple IEDs and evaluate the performance speed and reliability using sampled values data sources, known as merging units, on a variety of Ethernet switches and topologies. In addition, determining and analyzing the effects of dropped frames on the operation of high-speed protective relaying elements in different types of Ethernet switches could help end-users understand the relationship between the performance of their communication network and the reliability of their systems.

### 5.3.3 Perform Simulation Tests on IEC 61850 Using Cybersecurity Elements

Another area for potential work is testing the comparison of a variation of Ethernet switches using security elements such as firewalls, IDS, and secure gateways in the communication networks. Therefore, this work would focus on these elements and build on this research by collecting the same sorts of data as in the previous tests method to evaluate the impacts of the security aspects. Simulation tests are performed to evaluate the response of multiple IEDs and the performance of various Ethernet switches using basic security functionality. In addition, this study would investigate the effects of dropped frames on different types of high-speed relay elements transmitting GOOSE or SV through Ethernet switches. The testing will identify the factors that could affect substation network system reliability. Weak security measures leave the system vulnerable, even with the proper implementation of GOOSE and SV. So, the proposed system should be able to provide a high degree of accuracy in delivering GOOSE messages. In addition, it should also be able to transmit GOOSE messages smoothly, secure the network efficiently and minimize threats as possible.

### 5.3.4 Comparing the Physical Test with Simulator Tests

The primary limitation of this work was that it was a network simulation only, with simulations carried out to evaluate performance in terms of the IEDs measurement in a substation. This test is not limited to analyzing the network traffic of a single device. It also applies to other devices that are performing real-time operations. It needs to be determined whether the observations made for simulation are compatible with a physical test and have the same results. However, more data needs to be collected from a variety of physical Ethernet switches. The proposed system should be able to provide a high degree of accuracy in delivering GOOSE messages physically. In addition, future work should examine the effects of dropped frames on high-speed protective relaying components of Ethernet switches and measure the speed of transmitting GOOSE messages. The 0.2 second transmission times seen in the test results would be considered excessive in protection applications, so it is important to verify if physical testing has faster performance. It will help engineers to identify the reliability and performance of their network in simulation and physical substation network.

### 5.3.5 Educational Laboratory Applications

The testing approach in Chapter 4, as well as the proposed future work from earlier in this chapter all have value as education tools for university settings. The switch simulation provides the ability for students to do more complex studies even if they don't have access to network switches.

# Bibliography

[1] D. Formby, A. Walid and R. Beyah, “A case study in power substation network dynamics,” *ACM SIGMETRICS Performance Evaluation Review*, vol. 45, no. 1, pp. 66-66, 2017. Available: 10.1145/3143314.3078525.

[2] A. Schnakofsky, *Measuring the Reliability and Speed of Ethernet for Real Time Control Applications in Electrical Substations*. Master’s Thesis University of Idaho*, 2012.*

[3] A. Leal and J. Botero, "Defining a reliable network topology in software-defined power substations,” *IEEE Access*, vol. 7, pp. 14323-14339, 2019. Available: 10.1109/access.2019.2893114.

[4] V. Skendzic and G. W. Scheer, “Performance of redundant ethernet networks for electric substation instrumentation and control.” *11th Annual Western Power Delivery Automation Conference,* April 2009.

[5] G.W. Scheer and D. J. Dolezilek, “Comparing the reliability of Ethernet network topologies in substation control and monitoring networks.” *Western Power Delivery Automation Conference, Spokane, Washington*. 2000.

[6] M. Pozzuoli and R. Moore, “Ethernet in the substation,” *2006 IEEE Power Engineering Society General Meeting,* 2006.

[7] T. Sidhu and Y. Yin, “Modelling and simulation for performance evaluation of IEC61850-based substation communication systems,” *IEEE Transactions on Power Delivery,* vol. 22, no. 3, pp. 1482-1489, 2007. Available: 10.1109/tpwrd.2006.886788.

[8] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, “A review of security attacks on IEC61850 substation automation system network,” *Proceedings of the 6th International Conference on Information Technology and Multimedia*, 2014.

[9] I. Alsmadi and D. Xu, “Security of software defined networks: A survey,” *Computers & Security*, vol. 53, pp. 79–108, 2015.

[10] K. Benzekki, A. El Fergougui and A. Elbelrhiti Elalaoui, “Software-defined networking (SDN): a survey,” *Security and Communication Networks,* vol. 9, no. 18, pp. 5803-5833, 2016. Available: 10.1002/sec.1737.

[11] I. Ali and M. S. Thomas, “Ethernet enabled fast and reliable monitoring, protection and control of electric power substation,” *2006 International Conference on Power Electronic, Drives and Energy Systems*, 2006.

[12] M. G. Kanabar and T. S. Sidhu, “Reliability and availability analysis of IEC 61850 based substation communication architectures,” *2009 IEEE Power & Energy Society General Meeting,* 2009.

[13] T. Kiravuo, M. Sarela and J. Manner, “A survey of ethernet LAN security,” *IEEE Communications Surveys & Tutorials,* vol. 15, no. 3, pp. 1477-1491, 2013. Available: 10.1109/surv.2012.121112.00190.

[14] "Unmanaged 24-Port Ethernet Switch", *selinc.com,* 2021. [Online]. Available: https://selinc.com/products/2730u/. [Accessed: 29- Nov- 2021].

[15] Z. Hu, M. Wang, X. Yan, Y. Yin, and Z. Luo, “A comprehensive security architecture for SDN,” *2015 18th International Conference on Intelligence in Next Generation Networks,* 2015.

[16] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, “Security in software-defined networking: Threats and countermeasures,” *Mobile Networks and Applications,* vol. 21, no. 5, pp. 764–776, 2016.

[17] W. Xia, Y. Wen, C. H. Foh, D. Niyato and H. Xie, “A survey on software-defined networking,” in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 27-51, First quarter 2015, doi: 10.1109/COMST.2014.2330903.

[18] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-defined networking: A comprehensive survey,” *Proceedings of the IEEE,* vol. 103, no. 1, pp. 14–76, 2015.

[19] J. Hoyos, M. Dehus, and T. X. Brown, “Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure,” *2012 IEEE Globecom Workshops,* 2012.

[20] K. Choi, X. Chen, S. Li, M. Kim, K. Chae and J. Na, “Intrusion detection of NSM based DoS attacks using data mining in smart grid,” *Energies*, vol. 5, no. 10, pp. 4091-4109, 2012. Available: 10.3390/en5104091.

[21] C. Steven, D. Bruno, F. Martin, L. Ulf, S. Keith, V. Alfonso, “Using model-based intrusion detection for SCADA networks,” *presented at the SCADA Security Scientific Symposium,* January 2007

[22] U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh and J. Tan, “Security analysis and auditing of IEC61850-based automated substations,” *IEEE Transactions on Power Delivery,* vol. 25, no. 4, pp. 2346-2355, 2010. Available: 10.1109/tpwrd.2010.2043122.

[23] C. Yoon, T. Park, S. Lee, H. Kang, S. Shin and Z. Zhang, “Enabling security functions with SDN: A feasibility study,” *Computer Networks*, vol. 85, pp. 19-35, 2015. Available: 10.1016/j.comnet.2015.05.005.

[24] *gns3.com*. [Online]. Available: http://www.GNS3.com/. [Accessed: 28-Jun-2021].

[25] “Innovative Power System Testing Solutions - OMICRON,” *Omicronenergy.com*, 2021. [Online]. Available: https://www.omicronenergy.com/en/. [Accessed: 28- Jun-2021].

[26] “Cisco - Networking, cloud, and cybersecurity Solutions,” *Cisco*, 2021. [Online]. Available: https://www.cisco.com/. [Accessed: 28- Jun- 2021].

[27] “Wireshark· Go deep,” *Wireshark.org*, 2021. [Online]. Available: https://www.wireshark.org/. [Accessed: 28- Jun- 2021].

[28] “Protocol testing & measurement leader for energy & utilities | ASE systems,” *Applied Systems Engineering Inc.*, 2021. [Online]. Available: https://www.ase-systems.com/. [Accessed: 28- Jun- 2021].

[29] "IEEE 802.3-2018 - IEEE Standard for Ethernet", *Standards.ieee.org*, 2021. [Online]. Available: https://standards.ieee.org/standard/802_3-2018.html. [Accessed: 29- Nov-2021].

[30] "Managed 24-Port Ethernet Switch", *selinc.com*, 2021. [Online]. Available: https://selinc.com/products/2730m/. [Accessed: 29- Nov- 2021].

[31] "Software-Defined Network Switch SEL-2740S", *selinc.com*, 2021. [Online]. Available: https://selinc.com/products/2740s/. [Accessed: 29- Nov- 2021].

# Appendix A

## Code for Calculating Time Measurement and Packets Loss

```
import numpy as np
import pandas as pd
import statistics
dataset = pd.read_csv("Test file .csv" )
dataset.head(2)
def all_avg(IED):
    df = dataset.loc[dataset['goID'] == IED]
    time = df['Time delta from previous captured frame']
    index = time.index

    total = 0
    for i in range(len(index)):
        if i in index:
            total = total + time[i]

    Min time = min(time)
    Max time = max(time)

    print('The number of recieved packets = ', len(time)) # A 100 frames
should arrived each IED
    print('The number of lost packets = ', 100 - len(time)) # it
calculates the packets lost of each IED
    print('Max time = ',max(time)) # calculate the maximum time of each
IED
    print('Min time = ',min(time)) # calculate the Minimum time of each
IED

    print ('++++++++++++++')

    avg = sum(time) / len(time) # calculate the avrage time of each IED
    print('average time using number of recieved packets = ',avg)

    return avg

IED_list = dataset['goID'].value_counts().index.tolist()
IED_list.sort()
total_avg = 0
total_avr_len = 0
for i in range(len(IED_list)):
    print('The' ,IED_list[i],'is:')
    avg_1 , avg_2  = all_avg(IED_list[i])
    print('---')
    total_avr_len = total_avr_len + avg_1 # calculate the total avrage
time of all IEDs

print('The total average time of all IEDs = ', total_avr_len /
len(IED_list))
```