# Simulation of an Enhanced Network Security Framework for Federal Polytechnic Mubi


## Abstract

*The research, Simulation of an enhanced network security framework for Educational Enterprise system such as Federal Polytechnic Mubi was carried out of the desire to protect the enterprise network against accidental or deliberate attempt to modify or temper with valuable data. The aim is to develop a workable security framework for the enterprise network of Federal Polytechnic, Mubi while focusing on parameters such as authenticity, confidentiality, integrity and non-repudiation of data. These problems were solved in the research by securing unused ports with encrypted passwords and securing access lines of all network devices such as routers and switches. The methodology adopted for the system development was the survey method and this is because it provides reliable results used to identify network security problems and experimental methods for the construction of the framework. While data was elicited from extensive review of related journals articles, lecture notes, textbooks, face to face interview and interaction with relevant stakeholders. Design tools such as Diaw were used to produce structure diagrams effectively. Cisco Packet Tracer was then used to carry out the simulation process and the results was found to be in tune with the overall objective of the design.*



**Keywords: Enhanced, Enterprise, Parameters, Security, Simulation.**


## 1.0 Introduction

The enterprise network is known as that portion of the computing set-up that provides access to network communication services and resources to end users and devices spread over a single geographic location. It might be a single floor, building or even a large group of buildings covering a protracted geographic area. As computers and networked systems thrive in today's world, there is a need for increased robust PC and network security becomes more and more necessary [1]. The escalation of the network system will expose it to several varieties of internet threats. The security precaution embraced include identification, authentication, authorization and to safeguard the integrity, convenience, authenticity of the Packet transmitted over the network. Network security must be designed to suit the requirements of an organization [2]. Campus network as a form of an enterprise network is vital, and it plays an important role in any organization. Network architecture and its security are as vital should be considered by the organization. A campus network is an independent network under the control of an institution within a local geographical place and sometimes it may be a metropolitan area network [1]. The campus network, as defined for the aim of the enterprise design guides, consists of the unified elements that include the set of services used by a group of users and end devices that share the same high-speed communications' fabric. These include the data transport services which can be both wired and wireless, traffic identification and regulation which includes security, and application optimization, traffic monitoring, and organization, and overall systems management and provisioning. These basic functions are implemented in such a way as to provide and directly support the higher-level services provided by the IT organization for use by the end user community [3]. Network security begins with authorization to use the network, commonly with the use of username and password, and consists of the provision of policies adopted by the network administrator to prevent and monitor illegal access, alteration in the system, misappropriation, or denial of a computer network and network-accessible resources. Also, network security involves the sanction for access to data in the network, which is controlled by the network admin. When access is granted, the firewall then enforces policies such as what services are allowed to be accessed by the different levels of the network users. Authorization alone cannot prevent potentially harmful content, such as computer worms or Trojans being transmitted over the network, that is why Anti-virus software or an intrusion detection system (IDS) can be used to detect the malware. Communication between two hosts using a network may use the tunneling technology. This publication will show the proper methods of creating and enforcing an enterprise network security plan. Once there is


UNDER PEER REVIEW

a clear image of what needs the most protection, then all the necessary measure for the protection is put into consideration.

### 1.1 Research Motivation:

Campus network is arguably an integral part of an educational enterprise and due to the enormous security challenges, network security architecture is therefore indispensable. The level of network breeches, cyber crimes and other malicious tendency due to the current system vulnerability has necessitated this research.

Essentially, this research is borne out of the need to design a robust , flexible and enhanced network with the capability to respond to the next generation requirements, trying to prevent the current network from different level of threat, attacks and other malicious tendencies.

## 2.0 Literature review

Different research papers are consulted for security in the campus network. [2] presented various network security problems and their solutions. They denoted the security status of a campus network, analyzed security threats to the campus network and described the strategies to the maintenance of network security.[4] provide theoretical contribution as a format model architecture of a university campus network that can be used to build a vigorous and supple network that responds to the next generation necessities, secure network design is planned based on the requirements and the proposed network infrastructure is realizable with adjustable infrastructure. [6] shows the configuration of standard ACL and extended ACL on the router. The standard ACL creates a filter based on source addresses only and is used for server-based filtering, whereas, extended ACL provide more security by creating filters based on source addresses as Well, destination addresses, protocol, and port number.

Choi et al. (WAP-Wormhole Attack Prevention) [7] have presented a protocol that not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during the route discovery phase. This has been achieved through the use of the neighbor node monitoring method of each node and wormhole route detection method of the source node on the selected route.

Jain and Jain [8] have presented a trust-based model based on identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means. In this method, trust levels are derived in neighboring nodes based upon their sincerity in the execution of the routing protocol. This derived trust is then used to influence the routing decisions, which in turn guides a node to avoid communication through the wormholes.

Saha. et.al [9]: In a mobile ad hoc network, all the nodes cooperate to forward the packets in the network, and hence each node is effectively a router. The process of forwarding network traffic from source to destination is termed as routing. Consider, the scenario in Fig. 1, if node S sends data to node D, which is three hops away, the data traffic will get to its destination only if A and B forward it

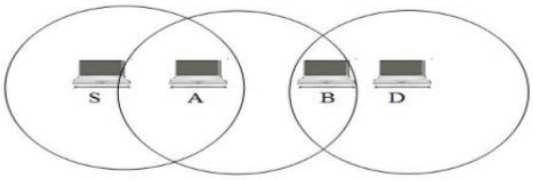


Fig 1: Routing Process in MANET

UNDER PEER REVIEW

Traditional link-state and distance-vector approaches do not scale well in large and dense MANET. Several routing protocols have been proposed to address the problems associated with the link-state and distance-vector approaches in MANET. These protocols can be classified into three different groups reactive (or on-demand), proactive (or table-driven) and hybrid. Reactive protocols obtain the necessary route when it is required, by using the route discovery process. In proactive protocols, nodes periodically exchange information to maintain up-to-date routing information. Hybrid routing protocols combine the basic properties of both approaches. The process of forwarding network traffic from source to destination, such that data traffic is not hampered by active and passive attacks [7], is called secure routing.

Chhabra et al. [10] proposed a protocol to prevent and handle Distributed Denial of Service (DDoS) attacks in the networks as early as possible and before reaching the victim. Dealing with DDoS attacks is difficult due to their properties such as dynamic attack rates, various kinds of targets, the big scale of a botnet, etc. Therefore, it is better to prevent the distributed denial of service attack rather than allowing it to occur and then taking the necessary steps to handle it. The advantage is that, after the victim node is removed from all the network tables, the paths through which this node sends packets are traced and those broadcast ids are nullified. The disadvantage is that it cannot mitigate other attacks.

[11] present an efficient approach for anomaly detection in cybersecurity and analyses intrusion detection evaluation data set and provides a framework which can discriminate between good cybersecurity operations and the bad ones. Also, the paper focuses on the use of knowledge discovery methods with soft computing method to find a solution for this problem. A Hybrid classifier is proposed and used to analyze the data set and extract the decision rules from it. These rules enable cybersecurity managers to make effective decisions and classify the operations as good or bad. The objective of the model developed is to maximize the security and minimize the risk on the behalf of the system.

### 2.1 Conceptual Framework

[12] There are various categories of networks like Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN), Campus Area Network (CAN), Storage Area Network (SAN) and Wide Area Network (WAN). A Personal Area Network (PAN) may be a network organized around a private person. Personal Area Networks usually involve a mobile, a cellphone and/or a hand-held computing device such as PDA. A Local Area Network (LAN) may be a cluster of computers and associated devices that share a standard communications line or wireless link. Typically, connected devices share the resources of one processor or server within a little geographical area. A Metropolitan Area Network (MAN) may be a network that interconnects users with system resources in an exceedingly geographical area or region larger than that filled by even a large Local Area Network (LAN).

The campus network of this research is designed in a hierarchical manner that may be a common practice of campus and enterprise networks. It offers a typical topology design of standard building blocks that enable the network to evolve simply. A hierarchical design avoids the necessity for a fully-meshed network in which all network nodes are interconnected [13,14]. Designing a campus network might not seem as mesmerizing or thrilling as designing a VoIP network, an associate IP video network, or designing a wireless network. However merging applications like these are engineered upon the campus basis. Very similar to the building a bridge, if the engineering work is skipped at the foundation level, the Bridge can crack and eventually collapse [15,16].

UNDER PEER REVIEW

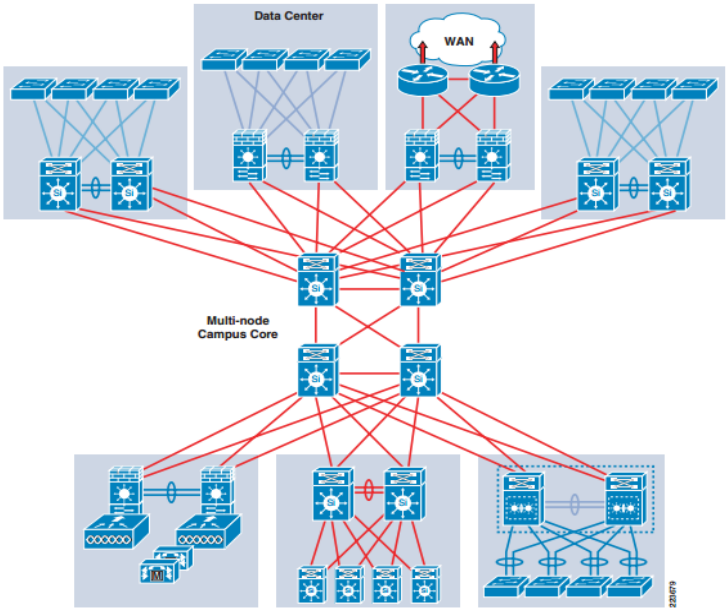


Fig 2: Hierarchical Framework of an enterprise network [15, 16]

### 2.2 Types of Network Attacks

The different types of network attacks include passive network attack, active network attacks, close-in attacks, exploitation from within the network, and attacks through the service provider. Information systems and networks are targets and should be impervious to attack from all threat agents [4][5]. A system should be able to limit the damage done during an attack and recover rapidly after the attacks. Here are some attack types:

i. Passive Attack: Passive Attack on a cryptosystem is one in which the cryptosystem cannot interact with any of the parties involved, attempting to break the system solely based upon observed data[4].
ii. Active Attack: An active attack is a network exploit in which a hacker attempts to change the data on the target or data on course to the target. [5].
iii. Distributed Attack: This is an attack where multiple comprised systems, which are often infected with a trojan, are used to target a single system causing a denial of service attack[5].
iv. Insider Attack: An insider attack is launched by an internal user who may be authorized to use the system that is attacked. It may be intentional or accidental[5].
v. Close-in Attack: A close-in attack is a type of attack where the attacker is physically close to the target system. [5].
vi. Phishing Attack: Phishing attack is a type of social engineering attack often used to steal user data, including login credentials and credit card details. It occurs when an attacker masked as a trusted entity and then dupes a victim. [5].
vii. Hijack attack: A hijack attack is a form of active wiretapping in which the attacker seizes control of previously established communication associations. [5].
viii. Spoof attack: In the context of information security, and especially network security, a spoofing attack is a situation in which a person or a program successfully pretends as by falsifying data, to gain illicit access.[5]
ix. Buffer overflow: A buffer overflow or buffer overrun, is a common software programming mistake that an attacker could exploit to have access to your network. [5].
x. Exploit attack: An exploit is an attack that takes advantage of vulnerabilities in applications, networks or hardware. [5].

UNDER PEER REVIEW

xi. Password attack: Hackers can use cracking programs, dictionary attacks, and password sniffers in password attack. Defense against password attack is rather limited but usually consists of a password policy including a minimum length, unrecognizable words, and frequent changes. [4].

xii. Denial of Service (DoS): Denial of service (DoS) is an interruption of service either because the system is destroyed, or because it is temporarily unavailable. Examples include destroying a computer's hard disk, severing the physical infrastructure, and using up all available memory on a resource. [4].

xiii. ARP Spoofing Attack ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol)messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. We are showing some real time data that attacker using Netcut software exploit the weakness in the stateless ARP protocol due to the lack of authentication in a campus network. [4].

### 2.2.1 Solutions to Network Attacks

i. Antivirus and Antimalware Software: This software is used for protecting against malware, which includes spyware, ransomware, Trojans, worms, and viruses. Malware is very dangerous and can infect a network and then remain quiet for a given period. The antivirus and anti-malware contain the threat through scanning for malware, detecting anomalies, remove the malware, and fix the damage done by the virus or malware. [17].

ii. Network Applications Security: It is essential to have application security for applications running on the network. It is possible for any application to comprise of vulnerabilities, or holes, that are used by attackers to enter your network.

iii. Performance Analytics: To detect irregular network behavior, you will have to know the normal behavior of the network. Performance analytics tools are capable of routinely knowing activities that deviate from normality. Your security team will thus be able to efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats. [17].

iv. Loss of data prevention: Organizations should guarantee that their staff does not send sensitive information outside the network. They should then use Data Loss Prevention technologies, such as network security measures, that avert people from uploading, forwarding, and printing important information in an insecure manner. [17].

v. Email Security: Emails are known to be the number one threat vector for a security fissure in a network. Attackers use the idea of social engineering to build refined phishing operations to deceive users within the network and then send them to sites full of malware. Email security applications are proficient in blocking incoming attacks in an email and controlling sent messages to avoid the loss of sensitive data. [17].

vi. Firewalls: Firewalls place a barrier between your internal network and outside networks, like the Internet. A set of defined rules are used to either block or allow traffic from coming into the network or leaving the network. A firewall can be software, hardware, or both. The free firewall efficiently manages traffic on your PC, monitors in/out connections, and secures all connections when you are online. [17].

vii. Intrusion Prevention System (IPS): An IPS is network security capable of scanning network traffic to actively block attacks. The IPS Setting interface permits the administrator to configure the ruleset updates for Snort. It is possible to schedule the ruleset updates allowing them to automatically run at particular intervals and these updates can be run manually on demand. [17].

viii. Mobile Device Security: Mobile devices and apps are increasingly being targeted by cybercriminals. There is the need to control which devices can have access to your network [17].

UNDER PEER REVIEW

ix. Network Segmentation: Software-defined division put network traffic into varied taxonomies which make enforcing security policies on a network a lot easier. The classifications are based on end-user identity, not just IP addresses. Privileges can be accessed based on location, role, and more so that the right people get the correct level of access. [17].

x. Virtual Private Network (VPN): A VPN is another type of network security that is capable of encrypting the connection from an endpoint to a network, mostly connections over the Internet. A remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between the network and the device. [17].

xi. Web Security: A preferable web security solution is controlling your staff's web usage by denying access to malicious websites and blocking access. [17].

xii. Wireless Security: Wireless networks are not as secure as wired networks and this will be easy for an attacker to penetrate. It is thus important for the wireless security to be strong in the network. It should be well-known that without rigorous security measures on wireless LAN, Ethernet ports should be placed everywhere for wired connections. [17].

xiii. Network Access Control (NAC): This network security process helps in controlling who access a network. It is important to know every device and user in the network to kick out potential attackers. This indeed will help you to enforce your security policies. [17].

**Anomaly modeling techniques in a Network**

i. Statistical models: In Denning's[18] ground laying paper on intrusion detection systems [16], she described several statistical characterizations of events and event counters. These, and more refined techniques, have been implemented in anomaly detection systems. These techniques include (1) Threshold measures: a common example is logging and disabling user accounts after a set number of failed login attempts, (2) Mean and standard deviation: by comparing event measures to a profile mean and standard deviation, a confidence interval for abnormality can be established, (3) Multivariate models: calculating the correlation between multiple event measures relative to the profile expectations

ii. Immune system approach: Application implementations inherently provide a model of normal behavior in the form of application code paths. In the immune system approach, applications are modeled in terms of the system call sequences. One of the first works analyzing system call sequences for intrusion detection is described in [19]. Forrest et al. [19,20] discovered that the short sequences of system calls made by a program during its normal executions are very consistent and deviations from these short sequences of system calls could be used to identify security violations of an executing process. An alarm is fired when the number of anomalies counted exceeds a threshold. This is known as the stide algorithm. The principle behind this scheme is that when an intrusion actually occurs, the majority of the adjacent system call sequences become abnormal.

iii. Markov process model: Markov processes are widely used to model systems in terms of state transitions. Some intrusion detection algorithms exploit the Markov process model. These methods do not use system call sequences, but instead analyze the state transitions for each system call. In state transition analysis, an event is considered anomalous if its probability, given the previous state and associated value in the state transition matrix, is too low [21].

iv. Rule-based algorithm One of the most used rule-based algorithms in the intrusion detection field is Repeated Incremental Pruning to Produce Error Reduction (RIPPER), which is a rule learning system developed by William Cohen [22]. This algorithm performs classifications by creating a list of rules from a set of labeled training examples.

UNDER PEER REVIEW

v. Data mining techniques: Many recent approaches to intrusion detection systems utilize data mining techniques [23]. These approaches build detection models by applying data mining techniques to large data sets of an audit trail collected by a system [24]

vi. Artificial neural network model: ANN is a biologically inspired form of distributed computation. It is composed of simple processing units, or nodes, and connections between them. The connection between any two units has some weight, which is used to determine how much one unit will affect the other. A feed-forward neural network has two stages: a forward pass and a backward pass. The forward pass involves presenting a sample input to the network and letting activations flow until they reach the output layer. The linear sum, sigmoid function and Gaussian function are three often used activation functions. During the backward pass, the network's actual output (from the forward pass) is compared with the target output and error estimates are computed for the output units. The weights connected to the output units can be adjusted to reduce those errors [25].

vii. Support Vector Machine Model (SVM): The SVM attempts to place a linear boundary (solid line) between the two different classes and orients this line in such a way that the margin (space between dotted lines) is maximized. The nearest data points used to define the margin are known as support vectors (gray circles and square). Support vectors, not the number of input features, contain all of the information needed to define the classifier. One remarkable property of SVM is its ability to learn can be independent of the feature space [25]

## 3.0 Materials and Methods

In this research, the survey analysis method was used to identify the network security problems such as lack of secure connection with remote user, porous ports on network devices which is a threat on the network and experimental methods for the construction of the framework was used. From the survey, it was observed that the existing system lack Firewall but uses only password authentication on the end nodes. Essentially, the survey method was used to collect and analyzed network data effectively. In the case of network data collection for security evaluation only some important data were collected, network packets were investigated in the ICT center. Primarily, interviews were carried out to the staff of the MIS and ICT unit, Students and relevant records were also observed. For the secondary method of data collection, Journal articles, Magazines, lecture notes were reviewed in trying to gather relevant data for the research.

To actualize effectively the objectives of this research, Cisco Packet Tracer (for simulating the network), and Diaw (A software for drawing structured diagrams) were used.

### 3.1 Network Design

The Proposed secured network design fills in the gap and minimize attack on the network. From the network design, internal and external firewall is placed so as to filter the packets going out from the network and coming into the networks. Security implemented in the network include: port security, access line security, VPN technology, Restricting the Broadcast Domain, Spanning Tree Protocol security on switches, DHCP Protection, IP spoofing Protection, ARP Spoofing Protection, Broadcast and Multicast storm protection, Creation of VLANs (Virtual LAN) for security.

From the network design, outer attacker cannot penetrate the network because of the presence of both internal and external firewall. The inside attacker will encounter difficulty while trying to access to network since the security mechanism on the network makes the network secured.

UNDER PEER REVIEW

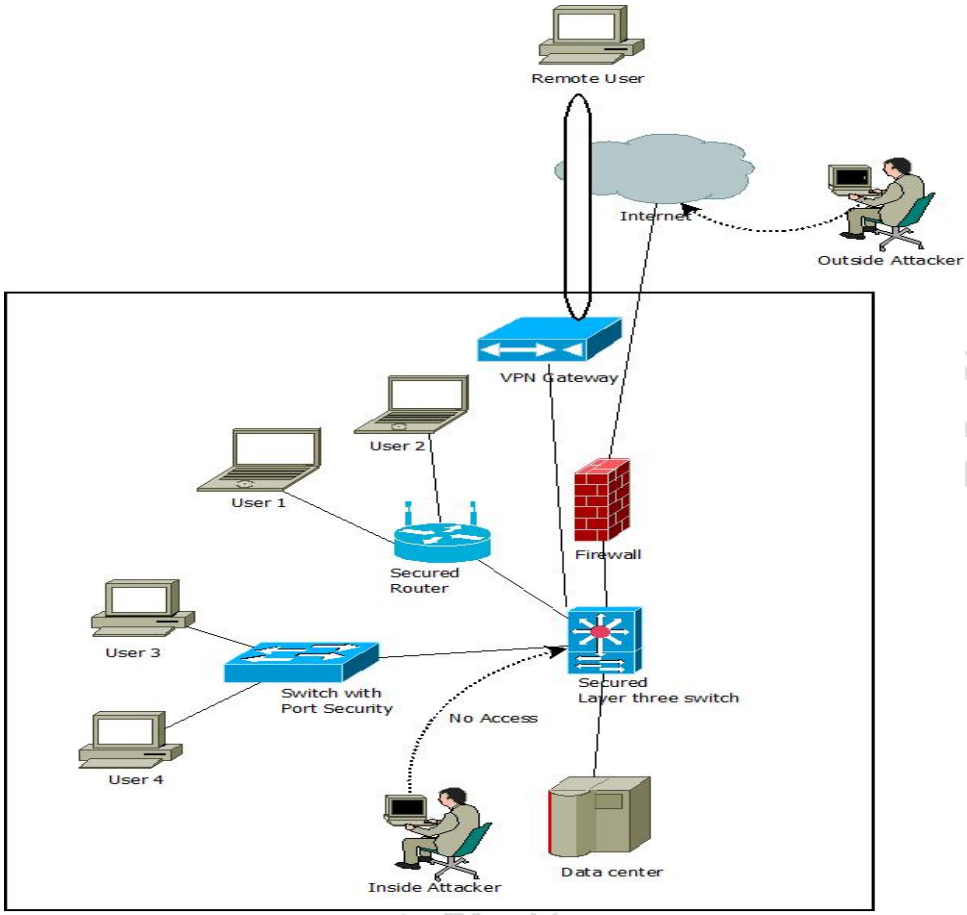


Fig 3: Improved Security Architecture for Fed. Poly. Mubi enterprise network (with firewall, VPN gateway and secured network devices incorporated)

**3.1.1 Port security:**

The use of port security technology on the switches added more security to the enterprise network. Port security is the way of preventing network devices from using a particular or set of the port on a switch. At the port level, only certain MAC addresses are allowed or deny to use the port. This can be done either statically or dynamically. MAC addresses are either manually configured or dynamically learned by the switch. MAC Addresses that are dynamically learned can be saved on the switch and manually configured MAC addresses are called static MAC addresses. To enable port security on the switch port, this command is used on an interface that has been set as a switch port:

```
Central(config-if)#switchport port-security
Command rejected: GigabitEthernet1/0/20 is a dynamic port.
```

If an error message pops out, then there is a need to configure the port for switch port mode access before continuing:

```
Central(config-if) #switchport mode access
Central(config-if) # switchport port-security
```

Once Port security is enabled, there are options to use:

```
Central(config-if) #switchport port-security?
```

```
aging                Port-security aging commands
mac-address          Secure mac address
maximum Max          secure addresses
violation            Security violation mode
<cr>
```

In this research, an interface is configured to accept packets only from the MAC address 0001.43B5.1676:

```
Central(config-if) #switchport port-security mac-address 0001.43B5.1676
```

By default, only one MAC address can be added to the permit list. To increase the limit, use the switch port port-security maximum command, hence, you can add another MAC address:

```
Central(config-if) #switchport port-security maximum 5
Central(config-if) # switchport port-security mac-address 0001.16C6.1423
```

When a port is configured with port security, and a packet arrives that is not in the permit list, it's considered a violation. There are three actions the switch can perform when there is a port-security violation:

Protect:

When a violation occurs, the switch drops all packets from the MAC addresses that have not to meet the configured requirements of the switch.

Restrict

When a violation occurs, the switch drops all packets from MAC addresses that do not meet the configured requirements of the switch. And an SNMP trap is generated, the log on the switch is attached, and the violation counter is deployed.

Shutdown

When a violation occurs, the switch puts the port into the error-disabled state. This will stop all packet traffic from entering and leaving the port. This is the default behavior for port-security-enabled ports.

To change the port-security violation action, use the switch port port-security violation command:

```
Central(config-if)#switchport port-security violation ?
protect          Security violation protect mode
restrict         Security violation restrict mode
shutdown         Security violation shutdown mode
```

**3.1.2 Securing Access Lines.**

Access lines are logical or physical interfaces on network devices such as switches and routers that are used for administration of the network. The console and aux port on routers and switches are the physical lines, whereas the logical (VTY) lines are Telnet and SSH. Securing access lines has to do with providing a password on the line using the password command:



UNDER PEER REVIEW

```
Mainrouter(config-line)#password Secret
```

Passwords are case-sensitive and may include space but cannot use special characters. If a password is not set on the VTY lines, you will get an error when telnetting to the network device:

Password required, but none set

Passwords that are entered in clear text are shown by default. To have the IOS encrypt all passwords in the configuration, enable the password encryption service with the service password-encryption command as shown below:

```
Mainrouter#sho run | include password
```

password Secret1

To configure the password-encryption service to encrypt all the passwords, the configuration below is used:

```
Mainrouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Mainrouter(config)# service password-encryption
Mainrouter(config)# exit.
```

**3.1.3 Restrict Broadcast Domain:** A broadcast domain is a logical network segment where all network devices can transmit data directly to the other devices without going through any routing device. Since broadcast domain has to do with the area where broadcasts can be received, routers confine broadcasts. If the router obtains a broadcast signal, it will simply discard it. That is, the router connected to the Internet will not relay a broadcast message. This is challenging and not guaranteed also. Suppose two networks exist that are connected to each other through a router and the first network has a running DHCP server that offers IP addresses to networked systems. On the other side, there is no effective DHCP server running on the other network. Giving IP addresses from the first network's DHCP server to the second network's systems will be a tough task to achieve since DHCP is a broadcast and the router that links to the networks globules the broadcast traffic. That will leave any DHCP request in the second network unrequited. Some router manufacturers provide abilities for DHCP forwarding to solve the problem of Broadcast.

**3.1.4 Spanning Tree Protocol security on switches:** Because VLANs can be pruned from trunks, it is possible that some VLANs may form loops while others do not. For this reason, Cisco switches now default to a multiple-VLAN form of spanning tree called Per-VLAN Spanning Tree (PVST). PVST allows for spanning tree case for each VLAN when used with the ISL trunks. Per-VLAN Spanning Tree Plus (PVST+) provides the same features when used with 802.1Q trunks. From default settings, all VLANs will receive the same values for all spanning tree configurations. However, each VLAN can be configured differently.

**3.1.5 DHCP Protection:** Implement DHCP snooping on access VLANs to protect against DHCP starvation and rogue DHCP server attack. DHCP snooping is a layer two security approach that is integrated into the operating system of accomplished network switch which globules DHCP traffics determined to be undesirable. When deploying DHCP snooping, there is need to set up the trusted ports (the ports through which legitimate DHCP server message will pass) before enabling DHCP snooping on the VLAN.

UNDER PEER REVIEW

**3.1.6 IP spoofing Protection:** This can be achieved by using IP source guard on access ports. IP Source Guard averts IP and MAC address spoofing attacks on unsecured layer two interfaces. Whenever IP source guard is enabled, all traffic is impassable apart from DHCP packets. Once the host obtains an IP address through DHCP, then only the DHCP-allotted source IP address will be permitted. Source guard is not a separate tool, it depends on the information that is in the DHCP snooping database to do its work.

**3.1.7 ARP Spoofing Protection:** This can be actualized using dynamic ARP inspection (DAI) on access VLANs, Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature averts the man-in-the-middle attacks, where an inimical station will intercept traffic mend for other stations by corrupting the ARP caches of its unwary neighbors. The scoundrel sends ARP desires or replies mapping the other station's IP address to its own MAC address. DAI depend on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid tuples (MAC address, IP address, VLAN interface). When DAI is enabled, the switch drops ARP packet if the sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database.

**3.1.8 Broadcast and Multicast storm protection:** This is done by enabling storm control on access ports. Storm control averts the broadcast, multicast, and unicast storms from crushing the network. Storms can be the result of a number of issues, from bridging loops to virus outbreaks. With storm control, one can control the amount of storm traffic that will access the switch ports. Outbound traffic is unlimited. With storm control enabled, the switch monitors will then monitor packets coming into the configured interface. It determines the amount of unicast, multicast, or broadcast traffic every 200 milliseconds, then compares that amount with a configured threshold. Packets that exceed the threshold are dropped.

**3.1.9 Creation of VLANs (Virtual LAN) for security:** It's easy to see why virtual LANs have become extremely popular on networks of all sizes. In real situation, multiple VLANs are the same as having multiple and different physical networks within an organization without the difficulty of controlling multiple cable plants and switches. Because VLANs tends divides the network into different LANs, hence creating different broadcast domains, they also efficiently permit traffic from the broadcast domains to remain isolated while improving the network's bandwidth, availability and security [4].

**3.1.10 Implementation of Internal and External Firewall:** A firewall works to monitor and block or allow network traffic, both incoming and outgoing, on a private network. The hardware firewall helps in protecting the campus network security, it also affects certain outgoing traffics and prevents unauthorized incoming traffics. NetBIOS, SMTP and other assorted ports tends to pose a security risk are gridlocked in the outbound direction. This does not affect the majority of academic work-related programs used on the campus. Also, majority of academic process requiring authentication are supported by the firewall. The configuration on the fire wall on Email server should be: POP, IMAP, and SMTP (TCP ports 110, 143, and 25) should be allowed and any other ports should not be permitted from the Internet to access the network. Configuration on Web server should be: HTTP and HTTPS (TCP ports 80 and 443) should be allowed and all other ports should be denied from the Internet. And configuration on DNS server should be: Only DNS (UDP port 53, and TCP port 53) should be allowed from the Internet. All other ports should be denied [4].

UNDER PEER REVIEW

**3.1.11 Virtual Private Network (VPN) Use for branch Campus:** A Virtual Private Network (VPN) extends a private network across a public network, such as the Internet. It permits a computer and other network-driven devices to send and receive packets across public networks as if it were connected directly to the private network, while benefiting from the functionality, security and other assorted management policies of the public network. A VPN is created by provide a virtual point-to-point connectivity with the use of dedicated connection, virtual tunneling protocols, or traffic encryption. Major applications of VPN are the Open VPN and IPsec. Campus VPN delivers a full tunnel VPN service which is an encrypted connection to the network from off campus. Common application of the VPN in campus network include access to file ,sharing drives and some applications that will require a Campus IP address. With the VPN, provision of general security service, The CBT, online portal activities will immensely tap into these invaluable security services and increasing data integrity, Privacy etc.[4].

**3.2 Analysis of the existing system:**

The existing network system has less security features. Passwords of network devices such as routers and switches are stored in clear text which is visible when tracking packets using software like Wireshark. The unused ports on the routers and switches are vulnerable to inside attack since they are not secured. The absence of a firewall within the network makes outside attack easier on the servers in the network. On the existing network, there is no secure connection for a remote user of the network.

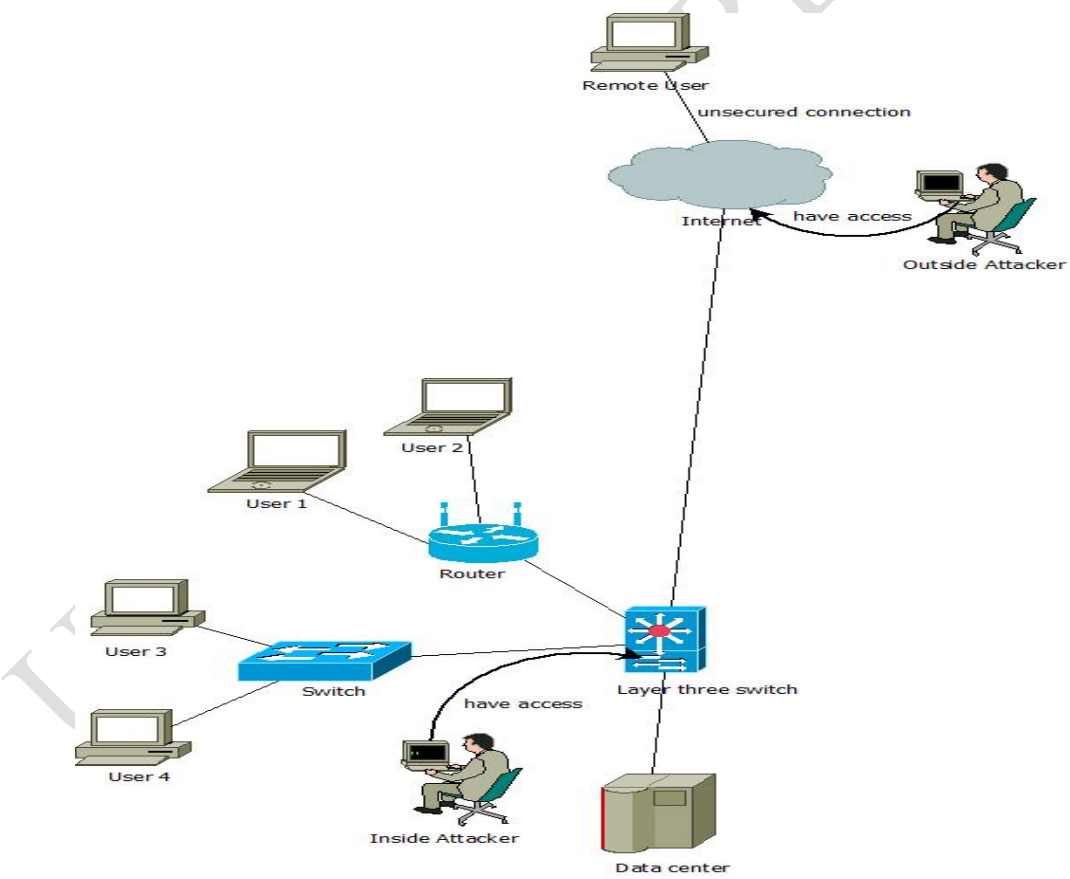


Fig 4: Existing network Architecture (having only end nodes with password facility for authentication and zero network security)

PREVIEW

### 3.3 Analysis of the Proposed system:

The proposed system in this research have capabilities and features that provide a counter against the loopholes in the existing system. In the proposed system, all unused ports of the network devices are secured using encrypted passwords whereby only authorized users are allowed to use the devices and hence, inside attacks to the network are contained. A firewall is placed between the internet connection to the network and the core layer switch of the network: hence, preventing an outer attacker from having access to the network. Remote users of the network can have a secured connection to the network using the VPN technology. Access lines to the network devices are all secure with encrypted password authentication which enables only the network administrator access for the management of the devices.

An in-depth comparative study of what obtains currently in the existing system and the improvements made and suggested have been shown in Figs. 3 and 4 above.

UNDER PEER REVIEW

## 4.0 Results

The results and analysis of tests carried out are discussed in the following sections

### 4.1 Result for Port-security on interface fa0/4 of a switch

Figure 5: Depicts the result of the command on the core router's command line interface as input "**show port-security interface fa0/4**" and the result is as follows:

Port security: Enabled

Port status: Secure down

Violation Mode: Shutdown

This shows that the Unused ports are all secured to prevent unauthorized parties.

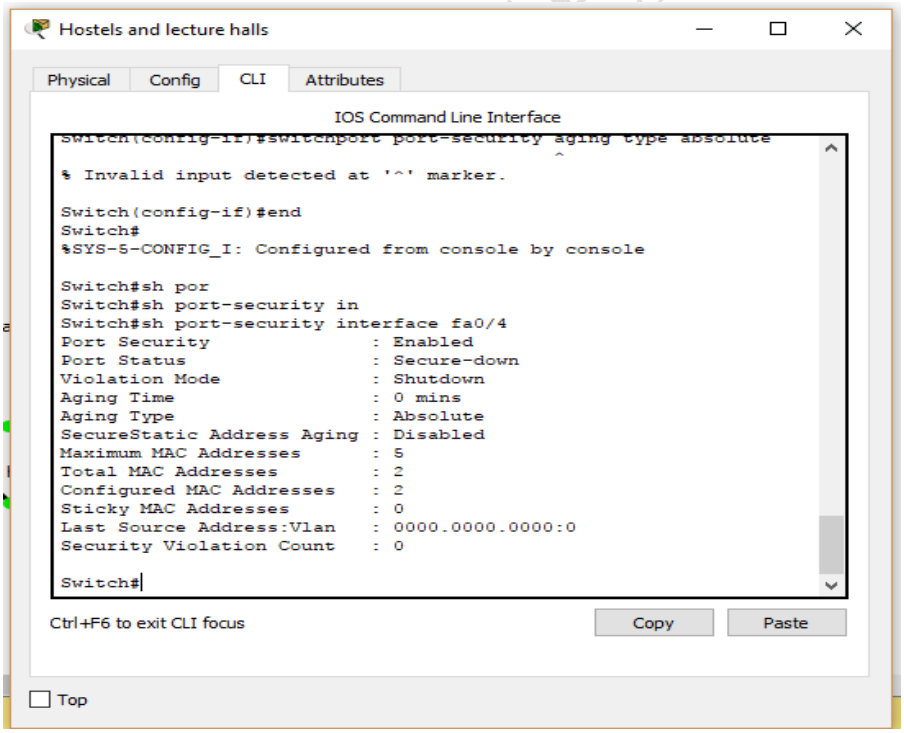


Fig 5: Port security on Interface fa0/4

### 4.2 Result for Secured Console Port of Router

Figure 6: Below shows password authentication of the console line to access the network device this happens whenever the computer is connected with the console cable to the network device. The password timeout warning shows when the password does not input on time.

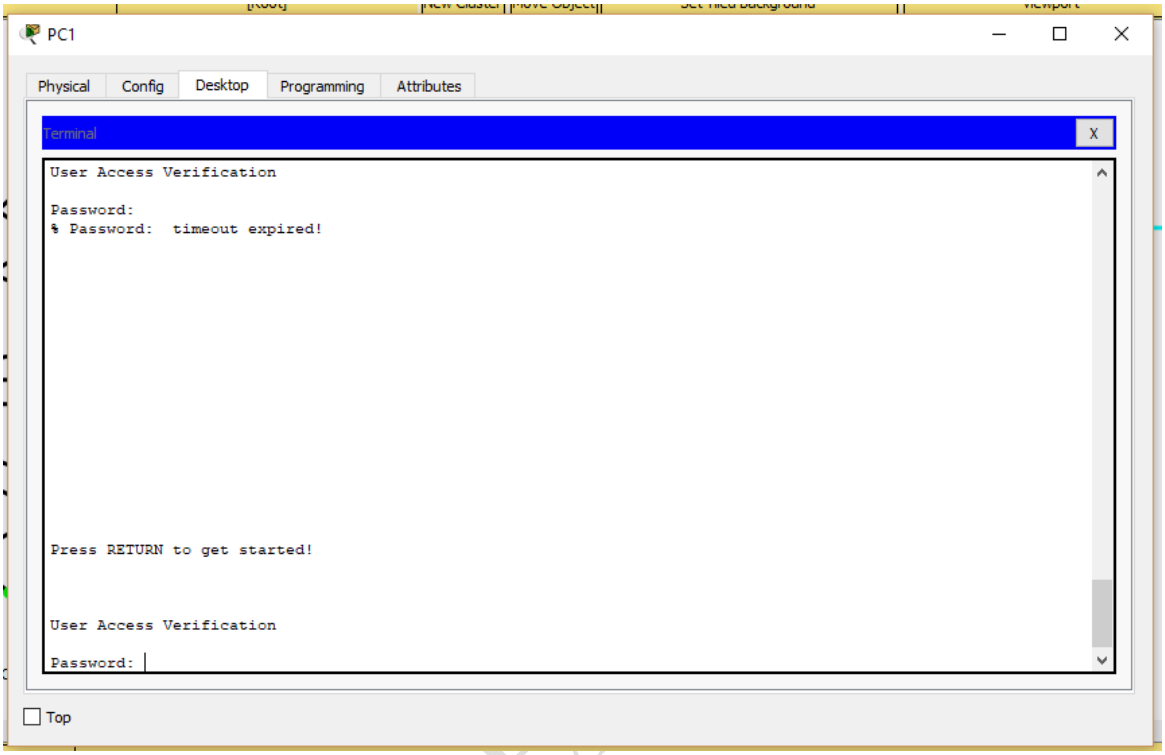


Fig 6 Secured console port

### 4.3 Result for Secured VTY Port

Figure 7: The input “telnet 172.16.120.1” was keyed in to access the network devices, hence authentication is required by the input of a password.

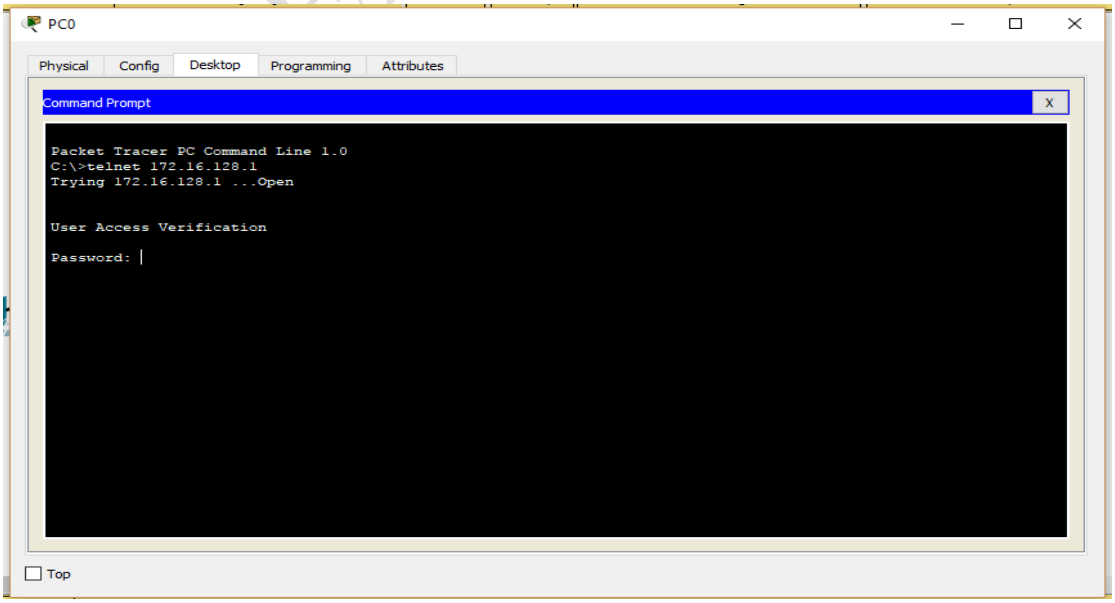

Fig 7: Secured Telnet with Password Authentication.

### 4.4 Testing the Remote Access VPN functionality

Verification and testing of the IPsec Remote Access VPN connection was achieved through the following:

i. Using the VPN client software on the Cisco packet tracer

ii. Using the commands '*show crypto isakmp sa*' and '*show crypto IPsec sa*' which are entered onto the packet tracer's CLI (command line interface)

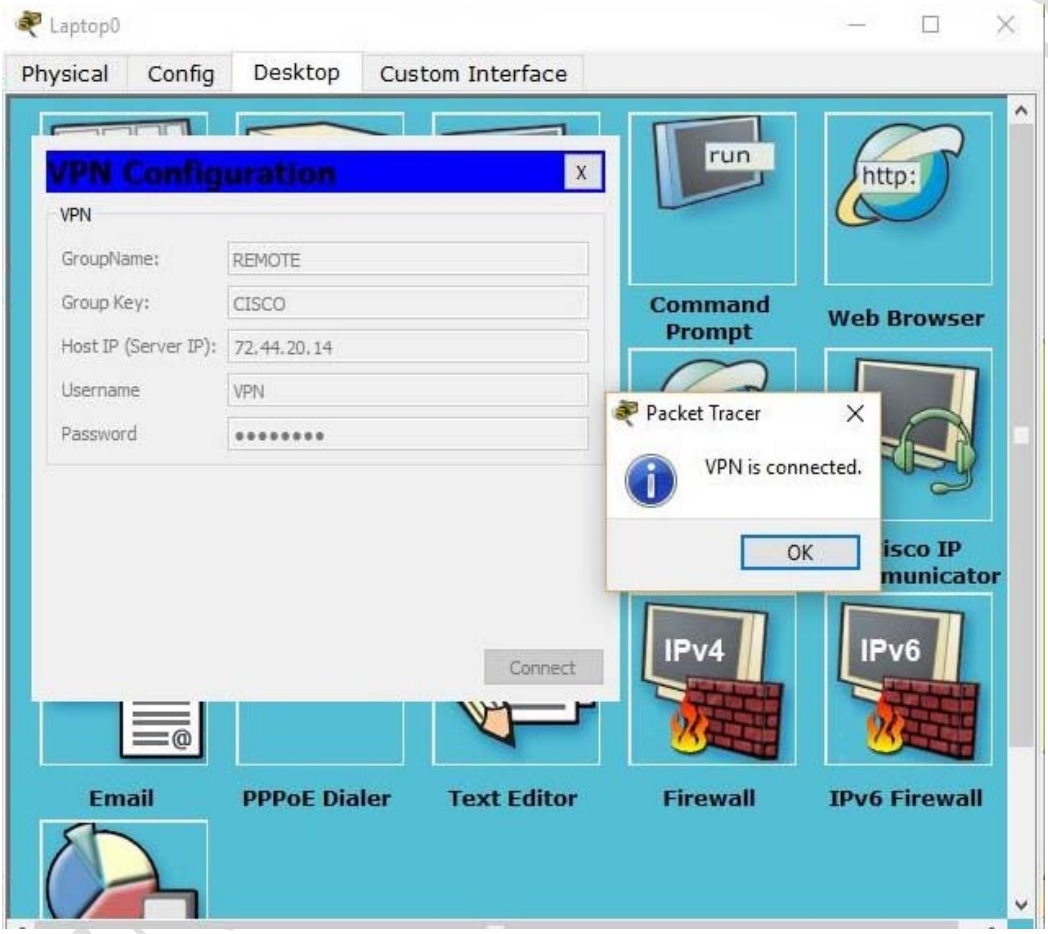


Figure 8 IPsec client connection – confirms connection for remote user of the Network

From figure 9, the remote user of the network has been assigned an IP address from DHCP pool server. The assign IP address can have access to the server.

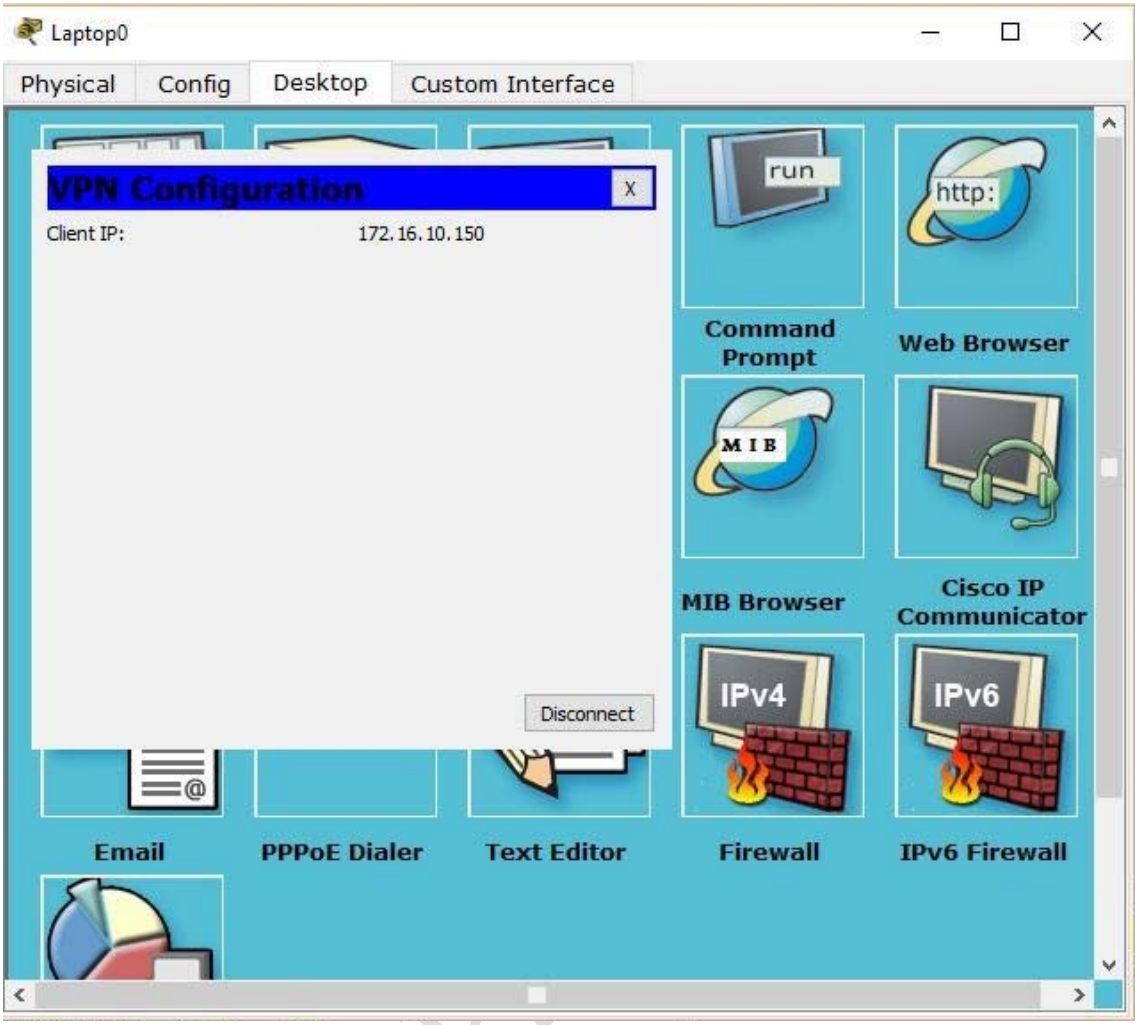


Fig 9 - shows that the remote user is assigned an IP address

From figure 10 ,When the command prompt is used and the command *ipconfig /all is* entered, the following it will be seen that a secured tunnel is created to access the network. The tunnel uses the public network (Internet)

UNDER P

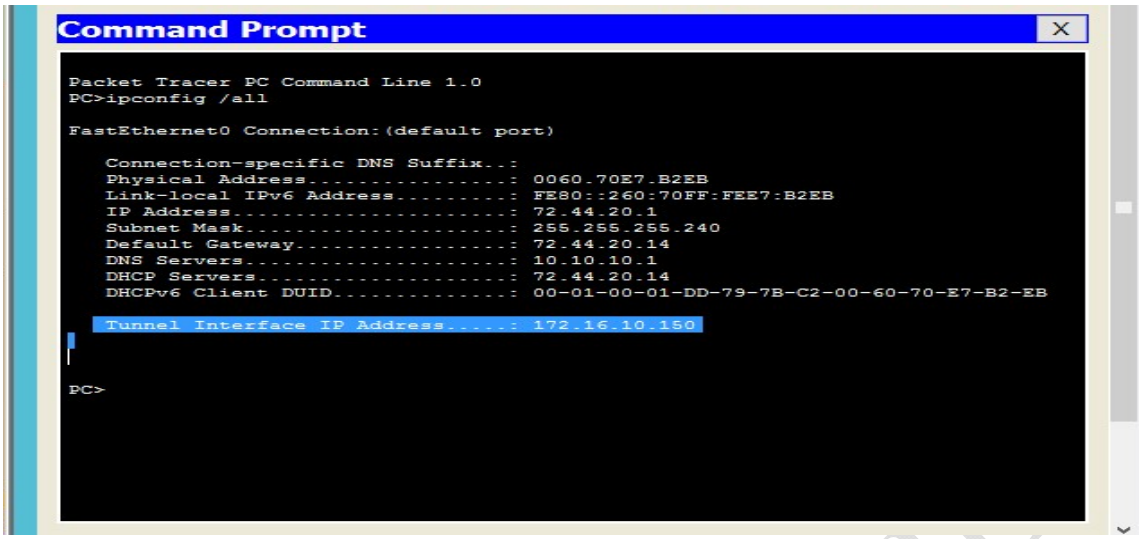

Figure 10 – Remote user confirming Tunnel created using CMD

## 4.5 Discussion of Results:

From Figure 5, Using the Command line interface (CLI) on the router or switch the command "show port-security interface fa0/4" is input to check the security status of the ports. After using the necessary configuration, and the result obtained is as follows:

```
Port security: Enabled
Port status: Secure down
Violation Mode: Shutdown
```

The results show that the port security is implemented on network devices leading to an improved security compared to what obtains in the existing network.

Figure 6 is the password authentication added to the console line access to the network device. The console line gives the physical connection to network devices using the console cable. Authentication on the network devices using console line is achieved.

Accessing network devices using telnet has been configured to require authentication as seen in Figure 7. When the IP address of the device is input on the CMD of a computer system, Password is required and hence add more security to the devices.

Implementation od VPN technology is added to the network as seen in figure 8 and a successful connection as seen ensures secured remote connection. Creating VPN connection is confirmed when the remote user obtains IP address from the network. Figure 9 is the result of a remote user obtained IP address and hence connection to the network.

Figure 10 is the remote user confirmation of a tunnel network when the command "*ipconfig /all is"* is input on the command prompt on a computer.

Based on these results, the major components that were used for the design together with other existing technologies interacted through simulation to produce an improved network security when compared to the system on ground.

UNDER PEER REVIEW

## 5.0 Conclusion and future work

Network architecture and its security are necessary for any organization. If the hierarchic network design is used the network will be scalable, with high performance and security increased. Generally, when dealing with network security, emphasis is laid on the fact that the entire network needs to be secure. Focus should not be on the end nodes as during data transfer, the communication channel is also vulnerable to attack by hackers trying to get data, decrypt the data and re-insert a duplicate which manipulate or tempered the data thereby compromising the integrity of the data. This research has left no stone unturned by proffering solutions on how best to tackle problems associated with data security. The

proposed network infrastructure is achievable with flexible infrastructure. It conjointly provides a summary of the most effective practices in mitigating the known attacks and recommendation on a way to stop reoccurrence attacks.

In future research, more network protocol such as the UDP and ICMP can be employed in extended ACL on the network that is designed. Aside RIP, other routing protocols such as EIGRP, OSPF and likes of BGP routing protocol may be chosen for routing Packets securely.

## References


[1] Mohammed, N. B. A. Network Architecture and Security Issues in Campus Networks, Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). 2013

[2] Lalita, K., Swapan D., Radhey, S. Security Problems in Campus Network and Its Solutions, 1, Department of Computer Science1-2, NIT Agartala, India, National Informatics Centre, India.

[ 3] Cisco Inc.*Administrative Guide - WAP4410N Wireless-N Access Point*. San Jose: Cisco Press, 2016; 2-4.

[4] Nadir, M., Emran, M. Design and Implementation of a Secure Campus Network, *International Journal of Emerging Technology and Advanced Engineering*, 2015;5(6), 5-6

[5]Shilpa P., Ashutosh G., and Ratul D. Different Type Network Security Threats and Solutions, A Review, *IPASJ International Journal of Computer Science (IIJCS)*, 2017; 5(4) .

[6] Suman, K., and Agrawal, N.F. Implementation and configuration of ACL in an enterprise network, *Indian Journal of researches*. 2016; 9(7), 8-10.

[7] Choi, S., Kim, D.Y. Lee and J.I.Jung, "Attack Prevention Algorithm in Mobile Ad Hoc Networks, "in porc. of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008; 343-348

[8] Jain, A., Jain, A., and P. K. Sagar.," Various Security Attacks and Trust-Based Security Architecture for MANET," *Global Journal of Computer Science and Technology*, 2010; (10)14,32-36.

[9] Saha, H. N., Bhattacharyya, D., Banerjee, P. K., Bhattacharyya, A., Banerjee, A. and D.Bose, "Study of Different Attacks in MANET with its Detection & Mitigation Schemes," *International Journal of Advanced Engineering Technology (IJAET)*, 2012; 3(1), 383-389,

[10] Chhabra, M., Gupta B., and A. Almomani. "A Novel Solution to Handle DDOS Attack in MANET," *Journal of Information Security*. 2013; 165-179,

[11] Ali Sever. A Machine Learning Algorithm Based on Inverse Problems for Cyber Anomaly Detection. *Current Journal of Applied Science and Technology*, 2018; 28(3): 1-14.

[12] Michael, G. Design and Implementation of a Secure Campus Network *International Journal of Pure and Applied Mathematics* 2017; 116(8), 303-307

[13] University of California, Davis http://manuals.ucdavis.edu/ppm/310/310-17.htm

[14] Udayakumar R., Kaliyamurthie K.P., Khanna, Thooyamani K.P., Data mining a boon: Predictive university topper women in academia, *World Applied Sciences Journal*, 2014; 29(14) ,86-90.


UNDER PEER REVIEW

[15] Thooyamani K.P., Khanna V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, *Middle - East Journal of Scientific Research*, 2014; 20(12) 2464-2470.

[16] Kalaiprasath R.., Elankavi R.., and Udayakumar, R. Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, *International Journal Of Civil Engineering And Technology* (Ijciet). 2017; 8(4), 376–385.

[17] Richman C. A.,. The Necessity of Network Security, Computer Engineering Technology Student, Houdegbe North American University Benin, 2018; 4-7

[18] Denning DE. An intrusion-detection model. IEEE Transactions on Software Engineering 1987; 13:222–32.

[19] Forrest S, Hofmeyr SA, Somayaji A, LongstaL TA. A sense of self for UNIX processes. Proceedings of the 1996IEEE Symposium on Security and Privacy, 1996.

[20] Forrest S, Hofmeyr SA, Somayaji A. Computer immunology. Communications of the ACM 1997; 40:88–96.

[21] Warrender C, Forrest S, Pearlmutter B. Detecting intrusions using system calls: alternative data models. Proceedings of 1999 IEEE Symposium on Security and Privacy, 1999.

[22] Cohen WW. Fast eLective rule induction. Proceedings of the 12th International Conference on Machine Learning, 1995.

[23] Lam KY, Hui L, Chung SL. A data reduction method for intrusion detection. Systems Software 1996; 33:101–8.

[24] Helmer G, Liepins G. Statistical foundations of audit trail analysis for the detection of computer misuse. IEEE Transactions on Software Engineering 1993; 19:866–901.

[25] Chen W.H, Hsu S.H. Application of SVN and ANN for intrusion detection. *Computers and Operations research* . 2015; 32(10), 2617-2634,

UNDER PEER REVIEW