PERFIL DE PLAN DE PROYECTO DE INVESTIGACIÓN

Quito – Ecuador, octubre del 2021

PROPUESTA DEL PLAN DE PROYECTO DE INVESTIGACIÓN.

Tema de Proyecto de Investigación:
Comparación de RACL, VACL y PACL para una red configurada en Protocolo OSPFv2.

Apellidos y nombres del/los estudiantes:

Hernández Suasnavas Kevin Joel.
Cholango Toapanta José Patricio.

Carrera:
Tecnología Superior en Electrónica.

Fecha de presentación:
07/10/2021

Quito, 07 de octubre del 2021

Firma del Director del Trabajo de Investigación

Ing. Jennifer Castillo Reimundo.

1.- Tema de investigación

Comparación de Access Control List (ACL) por Router, VLAN y por puertos mediante una topología en una red IPv4 con protocolo de OSPFv2.

2.- Problema de investigación

En la actualidad, las organizaciones son cada vez más dependiente de sus redes informáticas por el crecimiento de las redes y la cantidad de información disponible en estas, dando como resultado a estar expuesta a diversos ataques diariamente.
La falta de políticas integrales y medidas de seguridad para la protección de datos en diferentes identidades es un problema que está en crecimiento, por este motivo varios usuarios al ingresar a una red están exponiendo su información.

Según (Lizette Abril, 2021), El último informe anual de Kaspersky revela que en Ecuador existe un crecimiento del 75% en cuanto a los ataques informáticos, es decir, hay alrededor de 89 ataques por minuto. Según los expertos, esto afecta no solo a las grandes empresas o a los bancos, como ocurría en el pasado, sino que cada vez hay más interés por la información de pequeñas y medianas empresas (pymes).

Por este motivo, la investigación que se realiza es un medio que permite el aprendizaje y la enseñanza, para así prevenir ataques en la red, por lo tanto, el aplicar las configuraciones de manera práctica fortalece la técnica de estos métodos, para así, apoyar la formación académica de los estudiantes. Con base en la anterior lo que se busca es el mejor método para aplicar en seguridad de redes.
Se realizará una comparativa entre las Access Control List (ACL) por Router, VLAN y por puertos para así tratar de administrar los paquetes de IP de datos con la finalidad de encontrar una mejorar seguridad de red.

2.1.- Definición y diagnóstico del problema de investigación

Una Lista de Control de Accesos (ACL: Access Control List) es una serie de instrucciones que controlan que en un Router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de los mismos. **(Infotecs, 2019)**

Una ACL es una serie de comandos del IOS que controlan si un Router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete. Las ACL son una de las características del software IOS de Cisco más utilizadas. (ITESA, 2020)

OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad. En este capítulo, se abarcan las implementaciones y configuraciones básicas de OSPF de área única. (Itesa, 2020)

2.2.- Preguntas de investigación

¿Cuál es la configuración en la que se bloquea el acceso a un Router especifico en una topología IPv4?

¿Qué tipo de configuración permite el bloqueo de red mediante una lista de Access Map?

¿Para realizar un bloqueo punto a punto que tipo de configuración se aplicaría para detener el acceso a la red?

3.-Objetivos de la investigación

3.1.- Objetivo General

Contrastar los Access Control List de Router, VLAN, y por puertos mediante la implementación de una topología de IPv4 con protocolo de OSPFv2 para mejorar la seguridad de la red.

3.2.- Objetivos Específicos

- Implementar la configuración de RACL en una red de protocolo OSPFv2 para bloquear el acceso a servicios de red o a un Router especifico.

- Identificar mediante una lista de Access Map el tráfico a bloquear, para implementar en un Switch de capa 3 la configuración de VACL mediante una red configurada con OSPFv2 de simple área.

- Reconocer los puertos a bloquear en la topología de red, para implementar en un Switch la configuración de PACL mediante una red configurada con OSPFv2 de simple área.

4.- Justificación

En el mundo actual, la seguridad informática debe ir de la mano con la innovación tecnológica, ya que cada día se inventa un nuevo dispositivo incluso se encuentra la vulnerabilidad del mismo. Las organizaciones, empresas, universidades, etc. Buscan tener la mayor seguridad en sus redes, para no tener ataques y evitar pérdidas en su economía, privacidad y de su confidencialidad.

En vista que la información, es el factor primordial por el cual muchos usuarios malintencionados aplican varios métodos para obtener valiosa información confidencial de manera ilícita, para el mal uso de la misma.

Por otra parte, hay usuarios que no están de acuerdo con el uso de información que se realiza en algunas empresas, por la cual hacen estos ataques para hacer notar dichas falencias que pueden tener sus productos, dando la posibilidad de descubrir otros mercados que puedan contener mejores características de los mismos.

El tema a tratar en la investigación, se sitúa dentro de las tecnologías de información, específicamente en el ámbito de redes de computadoras, pero enfocado concretamente en la seguridad de red.

En la presente investigación tiene la finalidad de mejorar de buena manera la seguridad de la red con diferentes configuraciones de Access Control List que nos permite salvaguardar la información que por la red transita, así como para evitar ataques que atente contra el mal uso de los mismos.

Así mismo, el presente estudio nos ayudara a comprender las diferencias que existen en las configuraciones de RACL, VACL y PACL para mejorar de manera satisfactoria la seguridad de la red y tomar las medidas adecuadas al cuidado de la información digital.

5.- Estado del Arte

Según **(Mifsud, 2012)** El Objetivo de las ACL es limitar el tráfico de red y mejorar el rendimiento de la red. Al restringir el tráfico de vídeo o controlar el flujo del tráfico.

Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.

Establece qué tipo de tráfico se envía o se bloquea en las interfaces del Router. Por ejemplo, permitir que se envíe el tráfico relativo al correo electrónico, y se bloquea el tráfico de ftp u otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP **(Mifsud, 2012)**

Las características de OSPF, las cuales se muestran en la figura 1, incluyen lo siguiente:

- Sin clase: por su diseño, es un protocolo sin clase, de modo que admite VLSM y CIDR.

- Eficaz: los cambios de routing dirigen actualizaciones de routing (no hay actualizaciones periódicas). Usa el algoritmo SPF para elegir la mejor ruta.

- Convergencia rápida: propaga rápidamente los cambios que se realizan a la red.

- Escalable: funciona bien en tamaños de redes pequeños y grandes. Se pueden agrupar los routers en áreas para admitir un sistema jerárquico.

- Seguro: admite la autenticación de síntesis del mensaje 5 (MD5). Cuando están habilitados, los routers OSPF solo aceptan actualizaciones de routing cifradas de peers con la misma contraseña compartida previamente.

La distancia administrativa (AD) es la confiabilidad (o preferencia) del origen de la ruta. OSPF tiene una distancia administrativa predeterminada de 110. Como se muestra en la figura 2, se prefiere OSPF a IS-IS y RIP. (Cisco Networking Academy, 2021)

.6.- Temario Tentativo

1. Resumen
2. Abstract
3. Introducción
4. Desarrollo
    - 4.1. Introducción a Seguridad de Redes
    - 4.2. ACL
    - 4.3. Tipos de ACL
        - 4.3.1. ACL Estándar
        - 4.3.2. ACL Extendida
    - 4.4. Funcionamiento de ACL
    - 4.5. Aplicaciones de ACL
        - 4.5.1. RACL
        - 4.5.2. VACL
        - 4.5.3. PACL
    - 4.6. Materiales y Métodos
        - 4.6.1. Materiales
        - 4.6.2. Método Practico
5. Conclusiones
6. Recomendaciones
7. Bibliografía
8. Anexos

7.- Diseño de la investigación

7.1.- Tipo de investigación

La investigación que se llevará a cabo, conforme con los procedimientos que cumplirá para solución del problema abarca los siguientes tipos de investigación:

Investigación Descriptiva: Con esta investigación se va diferenciar los tipos de ACL en RACL, VACL y PACL identificando sus características de configuración que tiene cada una de ellas ya que con esto nos ayudara a mejorar la seguridad de la red.

Investigación Exploratoria: En esta investigación en la etapa exploratoria utilizaremos información de libros, informe ya que se quiere llegar a profundizar un mejor método para aplicar en seguridad de red que se implementará mediante la práctica en el laboratorio con los equipos adquiridos en esta investigación, ya que se estudiará la administración de la red con tres tipos de ACL como son RACL, VACL y PACL para solucionar la fiabilidad de la red.

7.2. Fuentes

- **Fuentes primarias:** Se utilizará como fuentes primarias el Instituto Superior Universitario “Central Técnico”, Laboratorio de redes, que incluyen los

siguientes componentes que son: Computadoras, Router , Switch de capa 2, Switch de capa 3 y aplicar cableado estructurado para las conexiones de los equipos, Conectores RJ-45, Cable UTP y el software de Cisco Packet Tracer, que a partir de este programa se realizara pruebas y simulaciones de la investigación.

- **Fuentes secundarias:** Se utilizará como fuentes secundarias la bibliografía que actualmente está a disposición, como lo es, repositorios universitarios, Internet, páginas web, libros, revistas científica, artículos científicos, informes técnicos, investigaciones, tesis, periódicos, manuales de los equipos que son de gran aporte para esta investigación.

7.3.- Métodos de investigación

Se realizará un análisis de cada uno de los Tipos de ACL a estudiar, para diferenciar sus configuraciones y características de cada uno de ellos mediante el método científico y experimental describiendo la mejor configuración que pueda brindar una mayor seguridad en la red.

El método científico comenzara mediante una indagación para obtener un conocimiento valido desde el punto de vista científico, utilizando una base de características de cada uno de los equipos de la investigación. Con ello el método científico comenzara con la identificación de cada uno de los puertos de conexión que tengan los equipos, para los enlaces mediante la experimentación.

Para el método experimental, con la base que se obtendrá en la investigación nos ayudará a tener nuevos conocimientos o corregir e integrar conocimientos previos, con la observación sistemática que se lleve a cabo.
Además, la experimentación se realizará con las configuraciones a realizar en el software del Cisco Packet Tracer, y la modificación de hipótesis o comparación de la misma para obtener el mejor resultado.

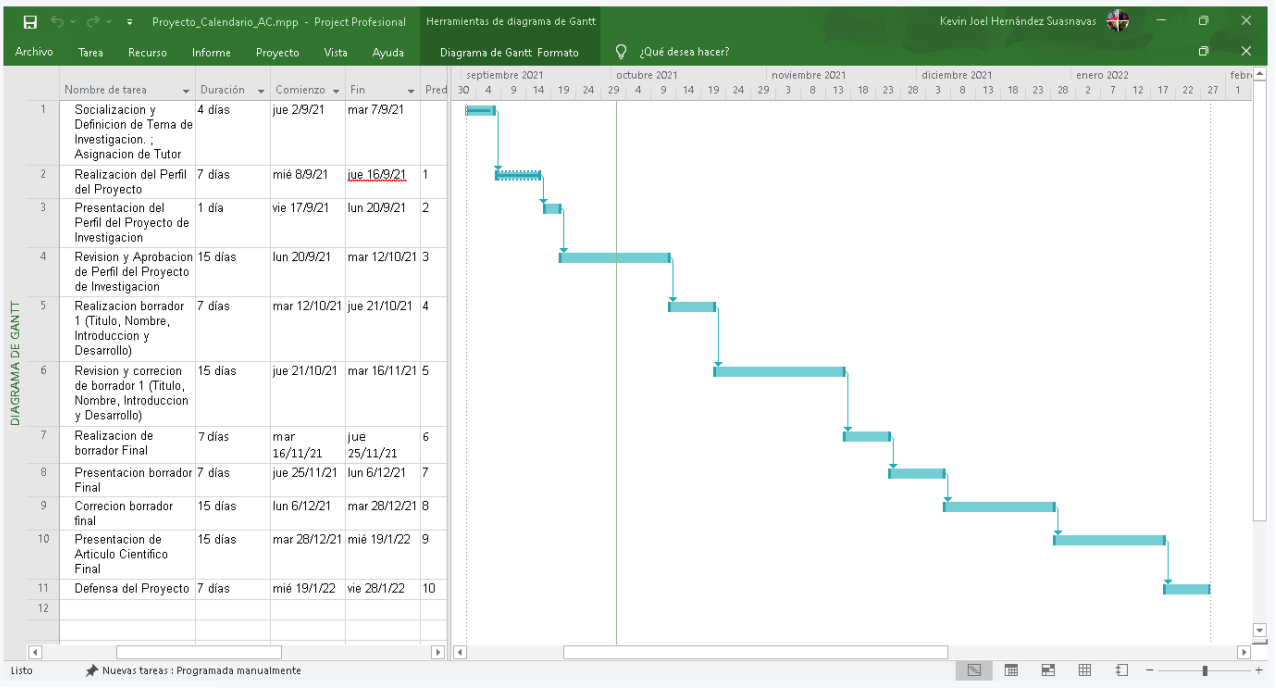
7.4.- Técnicas de recolección de la información

Se utilizará tres tipos de técnicas de recolección:

Observación, que es una técnica ocular, ya que se encarga de la toma de datos generados desde el software Cisco Packet Tracer, para la experimentación en los equipos a utilizar en la práctica de la investigación. Además, se va utilizar la técnica de comparación o confrontación que ayudara a cabo a definir las diferencias que existen entre los tipos de ACL a estudiar, otra técnica a usar seria la comprobación, ya que con ella con la información obtenida en la investigación nos permite verificar el funcionamiento de RACL, VACL y PACL para hacer un análisis de las configuraciones con la finalidad de identificar las diferencias que existen en entre estos tipos de ACL.

8.- Marco administrativo

8.1.- Cronograma



	Nombre de tarea	Duración	Comienzo	Fin	Pred
1	Socializacion y Definicion de Tema de Investigacion. ; Asignacion de Tutor	4 días	jue 2/9/21	mar 7/9/21	
2	Realizacion del Perfil del Proyecto	7 días	mié 8/9/21	jue 16/9/21	1
3	Presentacion del Perfil del Proyecto de Investigacion	1 día	vie 17/9/21	lun 20/9/21	2
4	Revision y Aprobacion de Perfil del Proyecto de Investigacion	15 días	lun 20/9/21	mar 12/10/21	3
5	Realizacion borrador 1 (Titulo, Nombre, Introduccion y Desarrollo)	7 días	mar 12/10/21	jue 21/10/21	4
6	Revision y correcion de borrador 1 (Titulo, Nombre, Introduccion y Desarrollo)	15 días	jue 21/10/21	mar 16/11/21	5
7	Realizacion de borrador Final	7 días	mar 16/11/21	jue 25/11/21	6
8	Presentacion borrador Final	7 días	jue 25/11/21	lun 6/12/21	7
9	Correcion borrador final	15 días	lun 6/12/21	mar 28/12/21	8
10	Presentacion de Articulo Cientifico Final	15 días	mar 28/12/21	mié 19/1/22	9
11	Defensa del Proyecto	7 días	mié 19/1/22	vie 28/1/22	10
12					

Fuente: Propia

8.2.- R e c u r s o s y materiales

8.2.1.-Talento humano

Tabla 1.

Participantes en el proyecto de investigación.

№	Participantes	Rol a desempeñar en el proyecto	Carrera
1	Cholango Toapanta José Patricio	Investigador	Electrónica
2	Hernández Suasnavas Kevin Joel	Investigador	Electrónica
3	Ing. Jennifer Priscila Castillo Reimundo	Investigador	Electrónica

Fuente: Propia.

8.2.2.- Materiales

Tabla 2.

Recursos materiales requeridos para el desarrollo del proyecto de investigación.

Ítem	Recursos Materiales requeridos
1	Laboratorio de Redes del ISUCT
2	Computadora o Laptop
3	Router Cisco
4	Switch Capa 3

5	Switch Capa 2
6	Cable UTP
7	Conectores RJ-45
8	Software de Cisco Packet Tracer

Fuente: Propia.

8.2.3.-Económicos

Ítem	Aportes	Cuota
1	Cholango Toapanta José Patricio.	$820
2	Hernández Suasnavas Kevin Joel	$820
	TOTAL	**$1640**

Fuente: Propia.

8.3.- Fuentes de información

BIBLIOGRAFÍA.

Bibliografía

Cisco Networking Academy. (2021). Obtenido de ITESA: https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.1.1.2

Diaz Jaspe, H. J. (05 de 07 de 2011). *Universidad Católica Andrés Bello*. Obtenido de http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAS2281.pdf

Infotecs. (21 de 01 de 2019). Obtenido de Infotecs: https://infotecs.mx/blog/acl-lista-de-control-de-accesos.html

Itesa. (2020). Obtenido de Itesa: https://www.itesa.edu.mx/netacad/switching/course/module8/index.html#8.0.1.1

ITESA. (2020). Obtenido de ITESA: https://www.itesa.edu.mx/netacad/switching/course/module9/9.1.1.1/9.1.1.1.html

Lizette Abril. (03 de 09 de 2021). *El Comercio EC*. Obtenido de El Comercio EC: https://www.elcomercio.com/tendencias/tecnologia/ataques-informaticos-pymes-crecen-ecuador.html

MANCHENO TORRES, H. C., & ROBLES CORONEL, I. L. (03 de 10 de 2013). *Universidad Católica de Santiago de Guayaquil*. Obtenido de http://201.159.223.180/bitstream/3317/1399/1/T-UCSG-PRE-TEC-ITEL-13.pdf

Mifsud, E. (30 de 09 de 2012). *Observatorio Tecnológico* . Obtenido de Ministerio de Educación, Cultura y Deporte de España: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1065-listas-de-control-de-acceso-acl?start=3

ORELLANA BENAVIDES, L. A., & HERNÁNDEZ VÁSQUEZ, R. C. (10 de 2003). *Universidad Don Bosco*. Obtenido de http://rd.udb.edu.sv:8080/jspui/bitstream/11715/281/1/033380_tesis.pdf

Sánchez, R. B. (s.f.). *UAEH*. Obtenido de https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf

CARRERA: ELECTRÓNICA

FECHA DE PRESENTACIÓN: 07 DE OCTUBRE 2021

APELLIDOS Y NOMBRES DEL / LOS EGRESADOS:
Hernández Suasnavas Kevin Joel.
Cholango Toapanta José Patricio.

TÍTULO DEL PROYECTO: Comparación de RACL, VACL y PACL para una red configurada en Protocolo OSPFv2.

ÁREA DE INVESTIGACIÓN:	**LÍNEA DE INVESTIGACIÓN:**
Redes y Telecomunicaciones	Seguridad de Red en Topología configurada con OSPFv2.

PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN:	CUMPLE	NO CUMPLE
• OBSERVACIÓN Y DESCRIPCIÓN	X	
• ANÁLISIS	X	
• DELIMITACIÓN.	X	

PLANTEAMIENTO DE OBJETIVOS:

GENERALES:

REFLEJA LOS CAMBIOS QUE SE ESPERA LOGRAR CON LA INTERVENCIÓN DEL PROYECTO

SI	NO
X	

ESPECÍFICOS:

GUARDA RELACIÓN CON EL OBJETIVO GENERAL PLANTEADO

SI	NO
X	

MARCO TEÓRICO:

	SI CUMPLE	NO NO CUMPLE
TEMA DE INVESTIGACIÓN.	X	
JUSTIFICACIÓN.	X	
ESTADO DEL ARTE.	X	
TEMARIO TENTATIVO.	X	
DISEÑO DE LA INVESTIGACIÓN.	X	
MARCO ADMINISTRATIVO.	X	

TIPO DE INVESTIGACIÓN PLANTEADA
OBSERVACIONES:
……
……

MÉTODOS DE INVESTIGACIÓN UTILIZADOS:
OBSERVACIONES:……
……
……

CRONOGRAMA:
OBSERVACIONES:……
……
……
FUENTES DE INFORMACIÓN:……
……

RECURSOS:	CUMPLE	NO CUMPLE
HUMANOS	X	
ECONÓMICOS	X	
MATERIALES	X	

PERFIL DE PROYECTO DE INVESTIGACIÓN

Aceptado [X]

Negado ☐ el diseño de investigación por las siguientes razones:

a) .....
.....
.....

b) .....
.....
.....

c) .....
.....
.....

ESTUDIO REALIZADO POR EL DIRECTOR DEL PROYECTO DE INVESTIGACIÓN:

NOMBRE Y FIRMA DEL DIRECTOR: Ing. Jennifer Castillo Reimundo

Firmado electrónicamente por:
JENNIFFER PRISCILA CASTILLO REIMUNDO

---

07 OCTUBRE 2021
DÍA MES AÑO
FECHA DE ENTREGA DE ANTEPROYECTO