ANTECEDENTES

PROYECTOS TERMINALES

- "Implementación de una VPN con el microcontrolador Rabbit [1], para acceso a una red de cámaras web". Se diseñó e implementó una red privada virtual (VPN) con un microcontrolador Rabbit, el cual dio acceso remoto y de forma segura a la red de cámaras web instaladas en el Departamento de Electrónica de la Universidad Autónoma Metropolitana Unidad Azcapotzalco. La relación que existe con este proyecto es que se habla de protocolos usados cuya función es asegurar las comunicaciones, estableciendo una transmisión segura entre dos redes remotas sobre un canal inseguro.La diferencia con el proyecto antes descrito es que en la propuesta que se presenta, se tomarán un conjunto de medidas para tener bajo protección todos los recursos de la red corporativa[1].

- "Sistema de filtrado para redes de computadoras con herramientas gráficas en Linux". Diseña una aplicación para administrar de manera gráfica una red de computadoras, aplicando herramientas del Sistema Operativo Linuxcomo son los Iptables [2] (filtrado de paquetes) para la creación de firewalls[3] .
  Existe relación con este proyecto en la manera de cómo administrar una red mediante el manejo de herramientas, tanto para la creación de firewalls como para el monitoreo de la red. La desigualdad existiría en que si la arquitectura de red sobre la cual trabaja la empresapermitirá implementar todas estas funciones [2].

- "Implementación de un firewall utilizando FPGA [4]". Genera un sistema firewall que no fuera dependiente de los recursos de una computadora para el procesamiento de tráfico de red, que pueda ser programado en un dispositivo FPGA de manera sencilla con reglas (Iptables), hechas de acuerdo al criterio del usuario.
  La relación existente con este proyecto esla de dotar un sistema firewall mediante reglas que el usuario crea conveniente aplicar para el procesamiento de tráfico en la red. La diferencia puede radicar en que el cliente no requiera de este dispositivo para la implementación de dichas reglas [3].

- **"**Diseño e Implementación de una aplicación para la administración de una red en el sistema operativo Linux (Complemento)". La aplicación ha sido desarrollada para funcionar en el sistema operativo Unix como Windows. Es una herramienta capaz de comunicarse con un router o switch por medio de su dirección IP, utilizando el protocolo SNMP[5], mostrando una serie de gráficas referente a la información existente en el dispositivo, en tiempo real.

---

[1]Empresa que diseña microcontroladores específicamente para control, comunicaciones y conectividad Ethernet.
[2]Iptableses un poderoso firewall integrado en el kernel de Linux y que forma parte del proyecto netfilter.
[3]Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
[4]FPGA (Field Programmable Gate Array) , matriz de puertas programable por un usuario en el campo de una aplicación.
[5]SNMP (Protocolo simple de administración de red), es un protocolo que les permite a los administradores de red administrar dispositivos de red y diagnosticar problemas en la red.

Asociamos el siguiente proyecto con la necesidad de administrar una red de manera más agradable para el administrador, utilizando una aplicación que nos ayude a preservar el buen funcionamiento de la red. La disimilitud que podemos encontrar sería que la arquitectura de red sobre la cual trabaja la empresa quizá no permita implementar todas estas funciones[4].

TESIS

- "Diseño de redes corporativas de datos basadas en la tecnología de puentes y enrutadores". Describe todas las tecnologías relacionadas con el diseño de una red corporativa. La relación es el uso de puentes y enrutadores para análisis y desarrollo de comunicaciones [5].

ARTÍCULOS DE INVESTIGACIÓN

- "Corporate Network Security". En este artículo habla del creciente uso de las redes de computadoras, así como mantener bajo protección los recursos y la información con que se cuenta en las redes corporativas. La relación es que describe medidas para minimizar las vulnerabilidades y confrontar los diferentes tipos de ataques en la red corporativa [6].