Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

# DISEÑO E IMPLEMENTACIÓN DE SISTEMA DE CONMUTACIÓN REMOTO PARA SEMÁFOROS

**Jaganath Pablo Emmanuel León Carrascoza**
Asesorado por la Inga. Ingrid Salome Rodríguez de Loukota

Guatemala, mayo de 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA


FACULTAD DE INGENIERÍA

# DISEÑO E IMPLEMENTACIÓN DE SISTEMA DE CONMUTACIÓN REMOTO PARA SEMÁFOROS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

**JAGANATH PABLO EMMANUEL LEÓN CARRASCOZA**
ASESORADO POR LA INGA. INGRID SALOME RODRÍGUEZ DE LOUKOTA

AL CONFERÍRSELE EL TÍTULO DE

**INGENIERO ELECTRÓNICO**

GUATEMALA, MAYO DE 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA


**NÓMINA DE JUNTA DIRECTIVA**

| | |
|---|---|
| DECANO | Ing. Pedro Antonio Aguilar Polanco |
| VOCAL I | Ing. José Francisco Gómez Rivera |
| VOCAL II | Ing. Mario Renato Escobedo Martínez |
| VOCAL III | Ing. José Milton de León Bran |
| VOCAL IV | Br. Luis Diego Aguilar Ralón |
| VOCAL V | Br. Christian Daniel Estrada Santizo |
| SECRETARIA | Inga. Lesbia Magalí Herrera López |

**TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO**

| | |
|---|---|
| DECANO | Ing. Pedro Antonio Aguilar Polanco |
| EXAMINADOR | Ing. Julio César Solares Peñate |
| EXAMINADORA | Inga. Ingrid Rodríguez de Loukota |
| EXAMINADOR | Ing. Carlos Eduardo Guzmán Salazar |
| SECRETARIA | Inga. Lesbia Magalí Herrera López |

## HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

**DISEÑO E IMPLEMENTACIÓN DE SISTEMA DE CONMUTACIÓN REMOTO PARA SEMÁFOROS**

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 31 de octubre de 2018.

**Jaganath Pablo Emmanuel León Carrascoza**

Guatemala 4 de marzo de 2019

Ingeniero
Julio Cesar Solares Peñate
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Apreciable Ingeniero Solares.

Me permito dar aprobación al trabajo de graduación titulado "**Diseño e implementación de sistema de conmutación remoto para semáforos**", del señor **Jaganath Pablo Emmanuel León Carrascoza,** por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesora, nos hacemos responsables por el contenido y conclusiones del mismo.

Sin otro particular, me es grato saludarle.

Atentamente,

Inga. Ingrid Rodríguez de Loukota

Colegiada 5,356

Asesora

Ingrid Rodríguez de Loukota
Ingeniera en Electrónica
colegiado 5356

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 15 de marzo de 2019

**Señor Director**
**Ing. Otto Fernando Andrino González**
**Escuela de Ingeniería Mecánica Eléctrica**
**Facultad de Ingeniería, USAC.**

Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado **DISEÑO E IMPLEMENTACIÓN DE SISTEMA DE CONMUTACIÓN REMOTO PARA SEMÁFOROS,** desarrollado por el estudiante **Jaganath Pablo Emmanuel León Carrascoza,** ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

**ID Y ENSEÑAD A TODOS**

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Julio César Solares Peñate
**Coordinador de Electrónica**

**Julio César Solares Peñate**
**Ingeniero Mecánico Electricista**
**Colegiado No. 2330**

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 17. 2019.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto bueno del Coordinador de Área, al trabajo de Graduación de la estudiante: JAGANATH PABLO EMMANUEL LEÓN CARRASCOZA titulado: DISEÑO E IMPLEMENTACIÓN DE SISTEMA DE CONMUTACIÓN REMOTO PARA SEMÁFOROS, procede a la autorización del mismo.

Ing. Otto Fernando Andrino González

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 27 DE MARZO 2019.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 231.2019

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **DISEÑO E IMPLEMENTACIÓN DE SISTEMA DE CONMUTACIÓN REMOTO PARA SEMÁFOROS,** presentado por el estudiante universitario: **Jaganath Pablo Enmanuel León Carrascoza,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Pedro Antonio Aguilar Polanco
Decano

Guatemala, mayo de 2019

/gdech

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

## ACTO QUE DEDICO A:

| | |
|---|---|
| **Dios** | Por ser quien me dio la fuerza y sabiduría para seguir adelante a pesar de las dificultades. |
| **Mis padres** | Carlos León y Alba Carrascoza, por su cariño y esfuerzo para sacarme adelante. |
| **Mis hermanos** | Diego, José y Maya León Carrascoza, quienes siempre estuvieron para apoyarme. |
| **Mi novia** | Andrea, por su apoyo y comprensión en los últimos pasos de la carrera. |
| **Mis amigos** | Quienes estuvieron en las buenas y en las malas durante toda la carrera, con los que siempre conté. |
| **Mi familia** | En general, por siempre darme palabras de ánimo. |

# AGRADECIMIENTOS A:


| | |
|---|---|
| **Universidad de San Carlos de Guatemala** | Por recibirme en sus instalaciones y darme una oportunidad de ser un profesional. |
| **Facultad de Ingeniería** | Por enseñarme lo necesario para desenvolverme en el ámbito laboral. |
| **Mis amigos de la Facultad** | Por su apoyo y comprensión en los distintos ámbitos de la carrera, ya que, sin ellos, esto no sería posible. |

# ÍNDICE GENERAL

# ÍNDICE DE ILUSTRACIONES

## FIGURAS

## TABLAS

# LISTA DE SÍMBOLOS

| Símbolo | Significado |
|---|---|
| **WPA** | Acceso wifi protegido |
| **QoS** | Calidad de servicio |
| **MPLS** | Conmutación de etiquetas multiprotocolo |
| **MAC** | Control de acceso a medios |
| **SSH** | Cubierta segura |
| **DPDT** | Doble tiro doble polo |
| **PoE** | Energía sobre ethernet |
| **CPE** | Equipo local del cliente |
| **HFC** | Híbrido de fibra coaxial |
| **SSID** | Identificador de conjunto de servicios |
| **OSI** | Interconexión de sistemas abiertos |
| **SMS** | Mensaje de texto |
| **PSK** | Modulación por desplazamiento de fase |
| **OSPF** | Primer camino más corto |
| **WEP** | Privacidad equivalente a cableado |
| **BGP** | Protocolo de borde de puerta de enlace |
| **DHCP** | Protocolo de configuración de usuarios dinámica |
| **TCP** | Protocolo de control de acceso |
| **UDP** | Protocolo de datagrama de usuario |
| **EIGRP** | Protocolo de enrutamiento de puerta de enlace |
| **RIP** | Protocolo de información de ruteo |
| **IP** | Protocolo de internet |
| **EoIP** | Protocolo de internet sobre Ethernet |

| | |
|---|---|
| **IPv4** | Protocolo de internet versión 4 |
| **IPv6** | Protocolo de internet versión 6 |
| **PPP** | Protocolo de punto a punto |
| **HTTP** | Protocolo de transferencia de hipertexto |
| **HTTPS** | Protocolo de transferencia de hipertexto seguro |
| **L2TP** | Protocolo de túnel en capa 2 |
| **PPTP** | Protocolo de túnel punto a punto |
| **PPPoE** | Protocolo punto a punto sobre Ethernet |
| **ISP** | Proveedor de servicios de internet |
| **WISP** | Proveedor de servicios de internet inalámbrico |
| **PTP** | Punto a punto |
| **AP** | Punto de acceso |
| **WAN** | Red de área abierta |
| **LAN** | Red de área local |
| **VLAN** | Red de área local virtual |
| **MAN** | Red de área metropolitana |
| **VPN** | Red privada virtual |
| **VPLS** | Servicio de LAN privada virtual |
| **DNS** | Sistema de nombres de dominio |

# GLOSARIO

**Autenticación** Mecanismos del sistema de información para identificar a los usuarios que acceden a sus recursos, y asegurar la integridad y autenticidad de los datos.

**Ancho de banda** Capacidad del rango neto de bits en comunicación digital o medida de datos disponible para tx/rx, expresado en bits por segundo.

**Banda ancha** Denominación que se aplica a un canal de comunicaciones cuyo margen de frecuencias es superior al habitual.

**Bit** La unidad más pequeña de información digital. Un número de un dígito con base 2, ya sea 0 o 1. El ancho de banda es generalmente medido en bits por segundo (BPS).

**Cable coaxial** Tipo de cable utilizado comúnmente en sistemas de televisión por cable, dicho cable está compuesto por dos conductores concéntricos: un cable interior y una cobertura exterior trenzada.

| | |
|---|---|
| **Cifrado** | Técnicas utilizadas para hacer inaccesible la información a personas no autorizadas. Se suele basar en una clave, sin la cual la información no puede ser descifrada. |
| **Comunicación inalámbrica** | Cualquier difusión o transmisión que puede ser recibida a través de microondas o frecuencias de radio sin la utilización de conexiones de cable para su recepción. |
| **Conmutador** | Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa. |
| **Cortafuegos** | Conjunto de componentes hardware y software destinados a establecer unos controles de seguridad en el punto o puntos de entrada a la red de comunicaciones a la que está conectado el ordenador. |
| **DHCP** | Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos. |
| **DNS** | La dirección IP de su servidor ISP, que traduce los nombres de los sitios Web a direcciones IP. |

| | |
|---|---|
| **Extranet** | Interconexión de ordenadores con base en el protocolo internet, que permite extender el acceso a determinados datos internos de la organización (que solo serían accesibles desde la intranet) a contratistas o empresas o instituciones con las que se tengan relaciones comerciales, institucionales, El acceso es restringido, y no es total como en la intranet, permitiendo el acceso sólo a determinados usuarios (claramente identificados) y a determinados datos. |
| **Ethernet** | Protocolo de red estándar de IEEE 802.3 que especifica la forma en que se colocan los datos y se recuperan de un medio de transmisión común. |
| **Fibra óptica** | Método para transmisión de información (sonido, video, datos) en el cual la luz es modulada y transmitida a través de filamentos muy delgados de vidrio de alta pureza. La capacidad de ancho de banda del cable de fibra óptica es mucho mayor a la del cable de cobre. |
| **Gateway** | Puerta de enlace predeterminada. |
| **Hardware** | El aspecto físico de equipos, telecomunicaciones y otros dispositivos de tecnologías de la información. |

| | |
|---|---|
| **HTML** | Es el lenguaje utilizado para crear páginas web. Está compuesto fundamentalmente por etiquetas. Y por lo general, cada etiqueta tiene otra similar de cierre. |
| **HTTP** | Protocolo de transferencia de hipertexto seguro. |
| **HTTPS** | Versión segura de HTTP implementada por medio del protocolo *secure socket layer* (SSL). |
| **Infraestructura** | Equipo de red e informático que se encuentra instalado en el lugar. |
| **Interconexión** | Conexión de un prestador de la red de telecomunicaciones con otro o la conexión de una pieza de equipo telefónico a una red. |
| **Interfaz** | Punto en el cual dos sistemas o piezas de un equipo son conectadas. |
| **Internet** | Red de computadoras expandida alrededor del mundo que vincula a los usuarios con comercios, agencias gubernamentales, universidades y otras personas. Internet brinda a las computadoras la capacidad de conectarse con otras computadoras para comunicar, diseminar y recoger información. |

| | |
|---|---|
| **Intranet** | Interconexión de varios ordenadores entre sedes dispersas geográficamente de una misma organización. Permite el uso a los empleados de dicha organización, restringiendo totalmente el acceso a la misma desde el exterior. Se basa en los mismos protocolos que internet, con lo que para el usuario es como si estuviese trabajando en internet. |
| **IP** | Protocolo de internet, número que identifica de manera lógica y jerárquica a una interfaz de red. |
| **IPSec** | Protocolo VPN utilizado para implementar el intercambio seguro de paquetes en la capa IP. |
| **ISP** | Empresa encargada de ofrecer la infraestructura de acceso para que los clientes puedan conectarse a internet utilizando los medios de acceso estándar. |
| **LAN** | Red de área local (*Local Area Network*). |
| **Máscara de subred** | Código de dirección que determina el tamaño de la red. |
| **Mbps** | Un millón de bits por segundo, unidad de medida de transmisión de datos. |
| **Navegador** | Programa de computación utilizado para explorar, buscar y visualizar información en sitios conectados a internet. |

| | |
|---|---|
| **Nodo** | Unión de red o punto de conexión, habitualmente un equipo o estación de trabajo. |
| **Octeto** | Conjunto de bits que representa un solo carácter. Usualmente hay ocho bits en un octeto, de allí su nombre. |
| ***Password*** | Término en inglés que se traduce por ‘clave de acceso’ o ‘contraseña’. |
| **Ping** | Utilidad de internet que se utiliza para determinar si una dirección IP determinada está en línea. |
| **PoE** | Tecnología que permite a un cable de red Ethernet transmitir tanto datos como corriente. |
| **PPPoE** | Tipo de conexión de banda ancha que proporciona autenticación (usuario y contraseña), además de transporte de datos. |
| **PPTP** | Protocolo VPN que permite tunelar el protocolo punto a punto (PPP) a través de una red IP. |
| **Red** | Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios. |
| **Red punto a multipunto** | Aquellas en las que cada canal de datos se puede usar para comunicarse con diversos nodos. |

| | |
|---|---|
| ***Routing*** | El proceso de mover un paquete de datos de fuente a destino, normalmente se usa un *router*. |
| **Servidor** | Cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios. |
| **TCP** | Un protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados. |
| **Topología** | Distribución física de una red. |
| **UDP** | Protocolo de red para la transmisión de datos que no requieren la confirmación del destinatario de los datos enviados. |
| **VPN** | Medida de seguridad para proteger los datos a medida que abandona una red y pasa otra a través de Internet. |
| **WAN** | Grupo de equipos conectados en red en un área geográfica extensa. El mejor ejemplo de WAN es Internet. |
| **WEP** | Protocolo de seguridad para redes inalámbricas. El objetivo de WEP es proporcionar seguridad mediante el cifrado de datos a través de ondas de radio, de forma que estén protegidos a medida que |

| | |
|---|---|
| | se transmiten de un punto a otro. |
| **Wireless** | Tipo de comunicación en la que no se utiliza un medio de propagación físico alguno, es decir, se utiliza la modulación de ondas electromagnéticas. |
| **WLAN** | Grupo de equipos y dispositivos asociados que se comunican entre sí de forma inalámbrica. |
| **WPA** | Protocolo de seguridad para redes inalámbricas que se fundamenta en los cimientos básicos de WEP. |

# RESUMEN

Con el paso del tiempo, las nuevas tecnologías se han convertido en un angular para el desarrollo de la sociedad; y más que en un ámbito de comodidad (automatización de procesos, comunicaciones, entre otros), en el ámbito económico, que, en su mayoría, es lo que impulsa a que nuevas tecnologías sean implementadas día a día. En la electrónica existen diversos dispositivos que se utilizan para estos desarrollos, ya que pueden ser pasivos, activos, lógicos, entre otros, y pueden utilizarse para la manipulación de parámetros eléctricos como la corriente y tensión. Es importante recalcar que en la electrónica también existen otras ramas, como las telecomunicaciones, las cuales permiten las comunicaciones a distancia a través de distintos medios, como el aire, el cobre, la fibra óptica, entre otros.

Las tecnologías en los últimos tiempos han crecido de forma exponencial, lo que ha llevado a que muchos procesos que en la antigüedad tomaban muchos recursos humanos; por ejemplo, la utilización del buzón de correo, ahora solo depende de abrir una aplicación, escribir lo que se desea y enviarlo al destino que se necesita y todo esto en menos de 1 minuto.

En estos tiempos, el termino IOT *internet of things,* se ha popularizado, ya que esto permite que a través de una intranet o de una red de redes (internet), distintos procesos, como la apertura de una puerta en una casa, pueda hacerse mientras que el usuario se encuentra del otro lado del mundo en cuestión de segundos, o la conmutación de un semáforo desde una central de comunicaciones.

# OBJETIVOS

## General

Diseñar un sistema unificado de conmutación de semáforos a través de una intranet con interconexión hacia todos los sitios remotos en el ejercicio de mejorar el tráfico vehicular en la ciudad.

## Específicos

1. Implementar el protocolo TCP para la comunicación de dispositivos dentro de una red.

2. Desarrollar una red privada que permita la visualización de dispositivos específicos para su control a distancia.

3. Diseñar, configurar y programar el hardware y software necesario para la conmutación a nivel físico del semáforo.

# HIPÓTESIS

En el transcurso del día, el tráfico en la ciudad suele ser un factor importante entre llegar a tiempo a un lugar o no y la salud mental; cuando se vuelve un problema, tiende a causar disgustos para las personas que dependen de un medio de transporte para movilizarse. La movilidad de los vehículos en las denominadas 'horas pico', es controlada por agentes de la policía municipal de tránsito por medio de la conmutación de los distintos semáforos, los cuales tienen la potestad de elegir que vías son las más importantes y por cuales debería cursar con mayor tiempo el flujo vehicular, con la limitante de no ver más allá de lo que le permite su estatura, o el lugar desde el cual están tomando esos datos. Estas decisiones provocan disgusto entre los conductores y la persona encargada de hacerlo, que atenta contra su integridad si en algún caso uno de los conductores decide actuar contra él.

- Hipótesis nula

Actualmente, la Municipalidad de Guatemala cubre las distintas áreas de la ciudad capital con cámaras, las cuales están conectadas a través de una intranet o una red privada; incluso, en algunas vías pueden verse las antenas CPE por las que se crea la comunicación hacia una central, la cual podría ser aprovechada en infraestructura para conectar a través de ella una red independiente para los conmutadores de los semáforos sin invertir en infraestructura nueva.

- Hipótesis alternativa

De no permitir acceso a esta intranet, se procederá a evaluar la posibilidad de crear una red Wireless, FTTx o VPNs, para alcanzar los distintos puntos remotos.

# INTRODUCCIÓN

Actualmente, se cuenta con un sinfín de tecnologías que pueden disminuir la necesidad de que personas realicen trabajos que pueden ser pesados y, hasta cierto punto, peligros para su integridad; por lo que es importante tener presente que, por medio de su utilización, estos procesos pueden automatizarse de forma segura y confiable.

La integración de tecnologías en la sociedad ya no debería tomarse como una opción, sino como una necesidad; más que dar ser un lujo, representa una oportunidad para tener un mejor control sobre los distintos ambientes de una ciudad; como en este caso, el tránsito vehicular, ya que, con el paso del tiempo, el número de automóviles ha crecido y seguirá creciendo.

Este trabajo tiene como idea principal desarrollar un sistema que pueda ser capaz de adaptarse a las necesidades de una ciudad que cuente con el problema de las aglomeración vehicular y poder tener un control más certero de lo que diariamente a través de medios como cámaras municipales, las cuales tienen una mejor cobertura visible y cuentan con un sistema de telecomunicaciones que permite que estas sean monitoreadas desde una central.

Todo esto mediante el conocimiento de los distintos dispositivos capaces de hacer que un sistema pueda conmutar remotamente con el simple hecho de tener una corriente y un voltaje; y muy importante también, el conocimiento de los distintos protocolos de comunicación y medios físicos por los cuales los datos pueden ser intercambiados.

# 1. APLICACIÓN DEL PROTOCOLO TCP Y MODELO OSI PARA LA COMUNICACIÓN REMOTA DE DISPOSITIVOS DENTRO DE UNA RED

## 1.1. Modelo OSI

Una de las ramas de las telecomunicaciones a nivel mundial la representan las redes, en las cuales se permiten interconectar diferentes dispositivos dentro de un sistema, el cual puede estar caracterizado por la zona geográfica donde se encuentra, ya que para las comunicaciones entre redes; se necesita de un direccionamiento que puede ser privado o público, lo que permite conocer el origen y destino de una solicitud, que tiene también puertos, los cuales caracterizan el tipo de comunicación que se está teniendo en determinado momento.

Internet Protocol, el protocolo de internet, comúnmente llamado direccionamiento IP, es utilizado para identificar dispositivos dentro de una red, ya que, sin este, no se puede tener comunicación. Este protocolo tiene dos versiones: la versión IPv4 y la versión IPv6, en las cuales se tiene la misma función; sin embargo, el segundo tiene mejoras sobre el primero.

Este direccionamiento consta de cuatro octetos, los cuales están separados por un punto '.', por ejemplo:

192.168.98.0/24

Las direcciones IP, con el paso del tiempo, fueron utilizándose a conveniencia, ya que, al principio, no se pensó en que un día las direcciones estarían escasas, por lo que decidieron separarlas por clases y por direccionamiento privado y público.

Las clases, al principio, eran utilizadas porque no existía el concepto de separar una red por medio de una máscara, o sea, la separación de las direcciones IP. Por lo que la clase determinaba la función que tenía una dirección y el uso que podía tomar. Las clases son las siguientes:

- Clase A: desde 0.0.0.0 hasta 127.255.255.255
- Clase B: desde 128.0.0.0 hasta 191.255.255.255
- Clase C: desde 192.0.0.0 hasta 223.255.255.255
- Clase D: desde 224.0.0.0 hasta 239.255.255.255
- Clase E: desde 240.0.0.0 hasta 247.255.255.255

Cada clase tiene su función, y aún se logra observar en la clase D o conocida como Multicast, que son direcciones que se asignan para una comunicación entre uno y varios dispositivos; y las direcciones de clase E, las cuales son usadas para investigación y no pueden ser propagadas por una intranet o extranet.

A partir de que se formuló el concepto de 'subneteo', que utiliza una máscara detrás de una dirección IP, las clases desaparecieron; se puede así utilizar de una forma más flexible estas direcciones.

La clasificación más importante del direccionamiento IPv4 es la distinción entre direcciones públicas y privadas, ya que las públicas son las que se utilizan para la comunicación a través de internet por medio del enrutamiento BGP y las

privadas son utilizadas para redes locales. La clasificación del direccionamiento privado es el siguiente:

- Clase A: 10.0.0.0/8
- Clase B: 172.16.0.0/12
- Clase C: 192.168.0.0/16

La barra “/” después de la dirección IP se utiliza para identificar el tipo de máscara con la que se está trabajando; por ejemplo, la “/8”, la cual indica que se podrán usar únicamente los últimos 3 octetos de la dirección, denotada como 255.0.0.0 (máscara).

El 255 será equivalente al valor $2^8$. 0.0.0, lo cual indica que el primer octeto ya se encuentra lleno, por lo que se necesita que se utilicen los siguientes, y así sucesivamente.

Sin el direccionamiento IP es imposible tener comunicación dentro de una red.

Las redes pueden ser clasificadas como LAN, WAN y MAN, las cuales obedecen distintos roles dentro de un sistema, tal como se describe a continuación:

- LAN: *Local Area Network*, la red de área local, como su nombre lo dice, es una red que se usa en las denominadas 'intranet', en la que los usuarios o dispositivos finales, únicamente se comunican entre el mismo dominio de *broadcast* (dentro de la misma red); y en este se utiliza direccionamiento IP privado, en el cual se pueden utilizar las direcciones a conveniencia, ya que puede que se trabajen desde 10 dispositivos

hasta 100 000, lo cual presentará un cálculo en el uso de las direcciones de no querer desperdiciarlas.

MAN: *Metropolitan Area Network*, como lo dice su nombre, es una red de área metropolitana, la cual es utilizada para las llamadas 'Redes Metro', en las cuales se hace la infraestructura de red de un ISP (*Internet Service Provider*), a través de los diferentes medios de transmisión, como la fibra óptica, radio frecuencia, etc. En estas redes puede utilizarse el direccionamiento privado y público de ser necesario, ya que posiblemente se quiera entrelazar un punto con otro dentro de la misma región o ciudad; por ejemplo, en el cual sea necesario utilizar VPNs (*Virtual Private Network*), que son túneles de ingeniería utilizados para viajar a través de internet y conocer la red a la que se desea llegar sin necesidad de cambiar de proveedor si este fuera el caso.

WAN: *Wide Area Network*, este tipo de red describe las conexiones que abarcan los sitios más remotos por medio de equipos de transmisión. Comúnmente se utilizan para identificar las salidas internacionales a nivel de un proveedor de servicios, ya que pueden ser conectadas para conocer enlaces desde un equipo de núcleo hacia otro de núcleo.

Una estructura de telecomunicaciones, tomando como referencia la rama de las redes, cumple con la siguiente jerarquía:

> "En la tecnología de redes, un diseño jerárquico implica dividir la red en capas independientes. Cada capa (o nivel) en la jerarquía proporciona funciones específicas que definen su función dentro de la red general. Esto ayuda al diseñador y al arquitecto de red a optimizar y seleccionar las características, el hardware y el software de red adecuados para llevar a cabo las funciones específicas de esa capa de red. Los modelos jerárquicos se aplican al diseño de LAN y WAN."[1]

[1] Itesa. *Estructura de telecomunicaciones*. http://www.itesa.edu.mx/netacad/networks /course/module1/1.1.2.1/1.1.2.1.html. Consulta: 27 de noviembre de 2018.

Un diseño típico de red jerárquica incluye las siguientes tres capas:

- Capa de acceso: proporciona acceso a la red para los grupos de trabajo y los usuarios.

- Capa de distribución: proporciona una conectividad basada en políticas y controla el límite entre las capas de acceso y de núcleo.

- Capa de núcleo: proporciona un transporte rápido entre los *switches* de distribución dentro del campus empresarial.

## 1.2. Análisis de las 7 capas del modelo OSI

A continuación, se muestra el análisis de las 7 capas del modelo OSI.

### 1.2.1. Capa 1, determinación y conocimiento del medio por el que pueden transportarse los datos

La capa 1 del modelo OSI describe la forma como los datos son transmitidos a través de varios medios, como lo son las radiofrecuencias, por medio de radio enlaces punto a punto o punto multipunto, pulsos eléctricos, por medio de cables coaxiales, utp, stp, entre otros; y pulsos de luz, por medio de tranceptores y fibra óptica.

Los radioenlaces se realizan a través de radio frecuencias, las cuales viajan por medio del aire, ya que, para establecer una conexión, independientemente que sea punto a punto (ptp) o punto multipunto (ptmp), deben tener 'línea vista', que es una expresión para definir que el medio debe

ser 'limpio', o no tener ningún tipo de barrera en su camino, como lo pueden ser árboles, vallas publicitarias, torres de radiobases, entre otros.

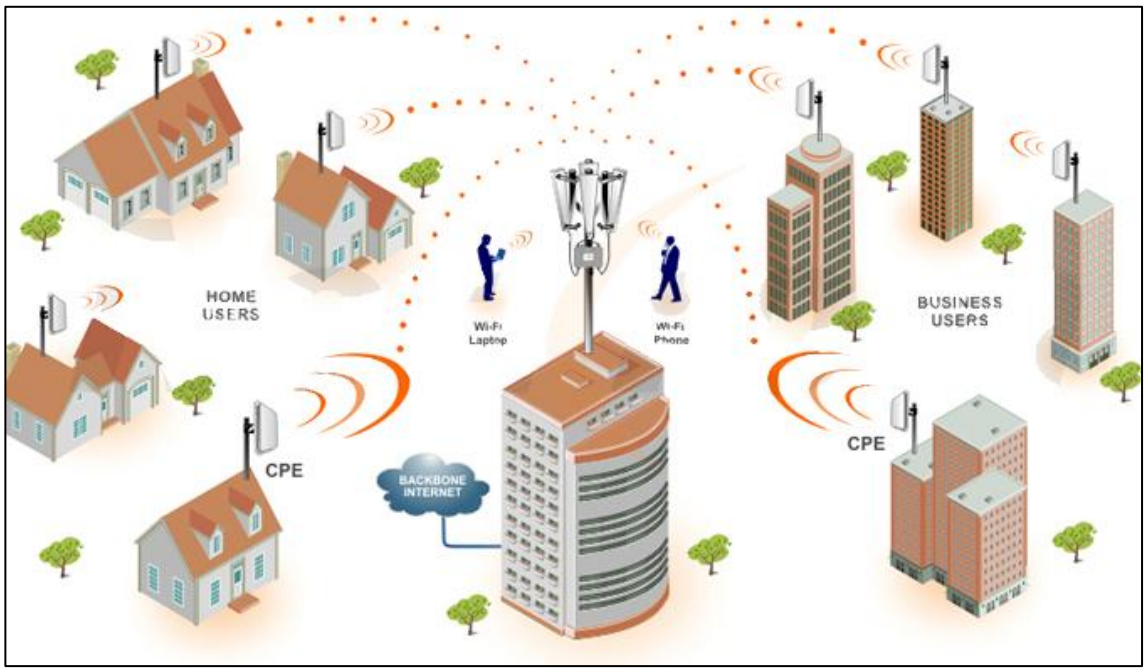
Estos enlaces también deben contar con varios parámetros adicionales a la línea vista, como la potencia de la antena, la ganancia, la distancia a la que se encuentran una de la otra y la alineación entre ellas.

La utilización de este tipo de transmisión se basa en que existen lugares a los que no se puede acceder por los otros dos medios descritos, ya que podrían involucrar una inversión muy grande o simplemente no existe forma de se pueda llegar físicamente. La ventaja de un radio enlace es que únicamente necesita de energía para alimentar la antena receptora y la configuración preliminar para establecer la conexión.

Los equipos para crear esta estructura de red de transmisión, independientemente de la marca que se utilice, son los siguientes: antena punto-multipunto, antena CPE (cliente.

Como se aprecia en la figura 1, la comunicación se hace desde un punto hacia varios puntos.

Figura 1. **Diagrama de WISP**




Fuente: Taringa. *Diagrama de Wisp*. https://www.taringa.net/+ebooks_tutoriales/vender-internet-wi-fi-y-crea-tu-red-wisp_ufvzg. Consulta: 30 de noviembre de 2018.

Estas comunicaciones pueden ser susceptibles al ruido que puede generar el ambiente, pero realizando un análisis de espectro y utilizando frecuencias no saturadas, puede ser muy estable.

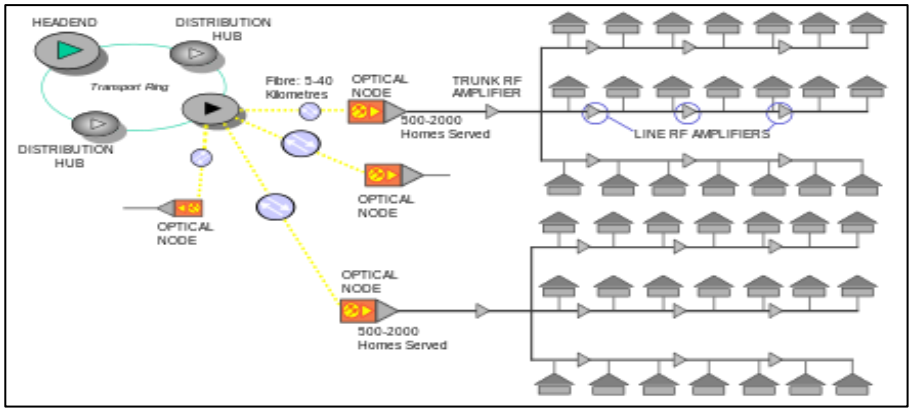
La comunicación a través de medios eléctricos puede ser una de las formas de transmisión más seguras que existen, ya que no son tan 'delicadas' como puede ser un radio enlace o fibra óptica, ya que en su mayoría se utiliza cobre, lo cual es un material bastante sólido; pero tiene la desventaja de que al ser un material conductor, cuenta con resistividad (resistencia de un elemento por unidad de longitud), lo cual compromete la comunicación si la señal a transmitir se atenúa en distancias muy largas. Este tipo de transmisión

actualmente es casi obsoleta, ya que no permite escalabilidad en términos de crecimiento ni manejar anchos de banda elevados. Se necesita mantener una cantidad de amplificadores o repetidores en el camino para que la señal pueda llegar a su destino sin interferencias, lo cual eleva demasiado los costos de operación.

Los equipos necesarios para esta comunicación son los siguientes: transmisor de potencia, modulador de señal, amplificadores, receptor, demodulador.

Como se aprecia en la figura 2, la red consta de una parte óptica, la cual es conocida como HFC, *hybrid fiber-coaxial*, en la que actúa la transmisión óptica y eléctrica desde una misma red; pero en la parte derecha, después de los nodos ópticos, se aprecia la estructura de una red coaxial, en la que deben existir una cantidad determinada de amplificadores para que la señal no se atenúe y pueda conectar varios lugares desde una troncal.

Figura 2. **Diagrama de red HFC**




Fuente: Wikipedia. *Diagrama de red*. https://es.wikipedia.org/wiki/H%C3%ADbrido_de_fibra_coaxial. Consulta: 30 de noviembre de 2018.

Las transmisiones por fibra óptica actualmente son las que predominan el sector de las telecomunicaciones a nivel mundial, ya que estas permiten una comunicación de alta capacidad, fiabilidad, libre de interrupciones y bajo mantenimiento, ya que, al ser la transmisión por pulsos de luz, estos viajan a velocidades altas por ser una onda electromagnética. Existen distintos materiales de los que pueden realizarse estas fibras.

Las fibras ópticas pueden ser de dos tipos:

- Multimodo: son utilizadas para comunicaciones *full duplex* entre distancias no mayores a 5 km, ya que por el amplio núcleo que poseen. Tienden a causar pérdidas por dispersión cromática o por retraso de grupo en la transmisión; además, permiten trabajar con diferentes longitudes de onda de forma simultánea, que logra transmitir distinta información en menos hilos sin necesidad de equipos especializados para multiplexación de longitudes de onda.

- Monomodo: son utilizadas para las comunicaciones a grandes escalas o redes WAN, como lo pueden ser las fibras submarinas o fibras que atraviesan países. Por sus características, solo permiten las comunicaciones *half duplex*, caso contrario, se utiliza un equipo de transmisión WDM (*wavelength division multiplexing*), el cual realiza la multiplexación de las diferentes longitudes de onda que quieran utilizarse. El núcleo de estas fibras suele tener un diámetro menor al de las fibras multimodo, ya que esto permite que el haz de luz no choque contra las paredes de material y no tenga pérdidas por dispersión.

Existen muchos tipos de equipos de transmisión para fibra óptica, los cuales pueden crear comunicaciones *full duplex* o *half duplex*, dependiendo de

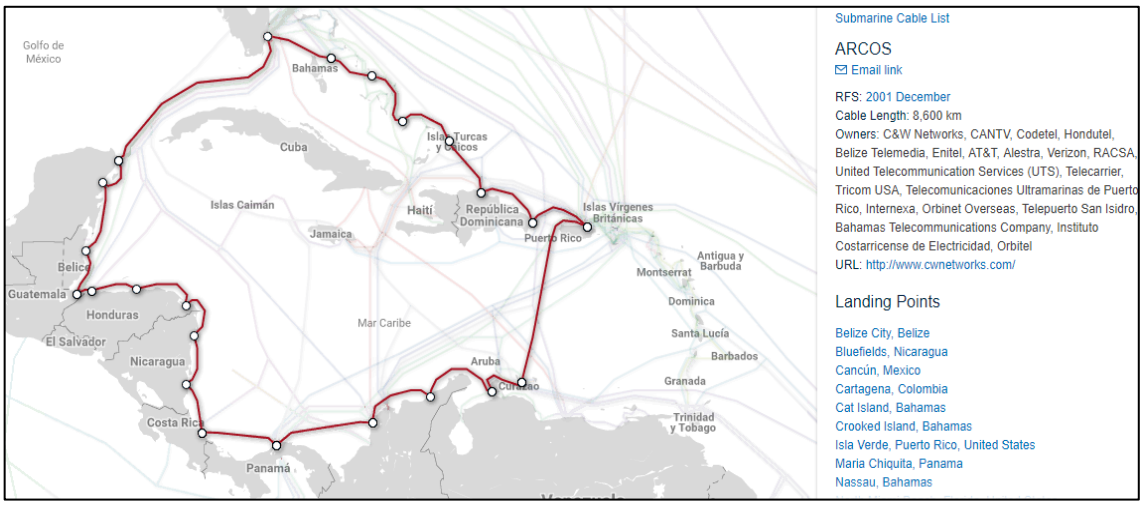
la conveniencia y ancho de banda que se quiera manejar. Una de las empresas dedicadas a las intercomunicaciones entre continentes es Infinera, la cual se dedica a crear equipos de transmisión que contemplan velocidades en Terabits.

> "Scalable: The Cloud Xpress incorporates Infinera's ultra-reliable optical engine based on the photonic integrated circuit (PIC) and delivers a 500 Gb/s dense wavelength-division multiplexing (DWDM) super-channel in only 2 rack units (2RU). Data center operators can start by using a fraction of the platform's capacity and scale up as needed with Infinera's unique Instant Bandwidth capability, which allows point-and-click activation of capacity without requiring any new hardware truck rolls, installation or configuration. Multiple Cloud Xpress units can be racked, stacked and managed as a single unit in order to scale capacity up to multiple terabits per second (Tb/s) per fiber pair."[2]

En la figura 3 puede verse la interconexión de una de las fibras internacionales que entran a Guatemala, la cual pertenece a la empresa ARCOS o Cable & Wireless, esto gracias a la versatilidad que tiene este medio de transmisión.

[2] Infinera. *Fibra óptica*. https://www.infinera.com/wp-content/uploads/infinera-ds-Cloud-Xpress.pdf. Consulta: 2 de diciembre de 2018.

Figura 3. **Diagrama de fibra submarina perteneciente a ARCOS**




Fuente: Submarinecablemap. *Fibra submarina*. https://www.submarinecablemap.com/#/submarine-cable/south-america-1-sam-1. Consulta: 3 de diciembre de 2018.

### 1.2.2. Capa 2, conocer los dispositivos de *switching* necesarios para envío de paquetes

En la capa 2 del modelo OSI se contemplan los dispositivos que trabajan con tramas, los cuales tienen la propiedad de identificar estas tramas y encaminarlas a través de su dirección física o MAC Address, la cual consta de 48 bits y es una dirección única a nivel mundial. Estas direcciones son asignadas por la IEEE, y están divididas en 6 bloques hexadecimales por el símbolo ':', y se identifican con los primeros 24 bits para el proveedor y 24 bits que el proveedor asigna al dispositivo según su conveniencia.

Estos dispositivos conocidos como *'switches*', sirven para repartir un dominio de *broadcast* o red entre una comunicación *unicast*, *multicast* o

*broadcast*. También, pueden servir para dividir dominios de *broadcast* por medio de interfaces virtuales (VLAN).

El uso más común que se le da a estos dispositivos es tener una cantidad mayor de puertos físicos disponibles y poder conectar más dispositivos a la red.

### 1.2.3. Capa 3, direccionamiento lógico para comunicación de dispositivos (IP) y determinación de dispositivo *router* a usarse

La capa 3 del modelo OSI es una de las más importantes y la que define la comunicación desde donde se hará una petición desde un dominio de *broadcast*, hacia el mismo u otro dominio. Como se describió antes, existen diferentes tipos de direccionamiento, en los cuales se contemplaba el direccionamiento privado y el público, de los cuales el de interés será el privado, ya que se utilizará en una intranet. Este direccionamiento es utilizado en los equipos de capa 3, los cuales son conocidos como *'routers'* o enrutadores, los cuales harán la decisión de los caminos que debe tomar un paquete para llegar a su destino.

En un dominio de *broadcast* deben existir 3 parámetros que no pueden faltar para la configuración de una red:

- Nombre de la red: es la IP que identifica el segmento de red que se utilizará, por ejemplo: 172.16.0.0/24.

- Puerta de enlace predeterminada (*gateway*): es la IP que identifica la 'salida' por la que un paquete debe seguir para conocer otros dominios de broadcast o redes, por ejemplo: 172.16.0.1.

- *Broadcast*: es la IP que crea la comunicación hacia todos los dispositivos dentro de una red, por ejemplo: 172.16.0.255.

La función de los *routers* es almacenar en ellos una tabla de rutas, la cual debe guardadas las redes a las que podrá comunicarse de ser necesario. Estas redes pueden ser compartidas por medio de ruteo estático o dinámico (OSPF, EIGRP, RIP, BGP, entre otros) desde otros equipos que trabajan con los mismos protocolos de enrutamiento. Al tener conocimiento de estas rutas por medio de su tabla, las comunicaciones podrán ser exitosas sin importar la zona geográfica en la que se puedan encontrar estos dispositivos.

### 1.2.4. Capa 4, determinación de puertos TC/UDP necesarios para comunicación entre aplicaciones asociadas al proyecto

La capa 4, o de transporte, es la primera que empieza a interactuar con las capas superiores, las cuales se encargan de representar los datos de una forma en la que el usuario o persona pueda interpretarla. Cada comunicación debe tener un identificador que pueda hacer la diferencia entre un protocolo y otro.

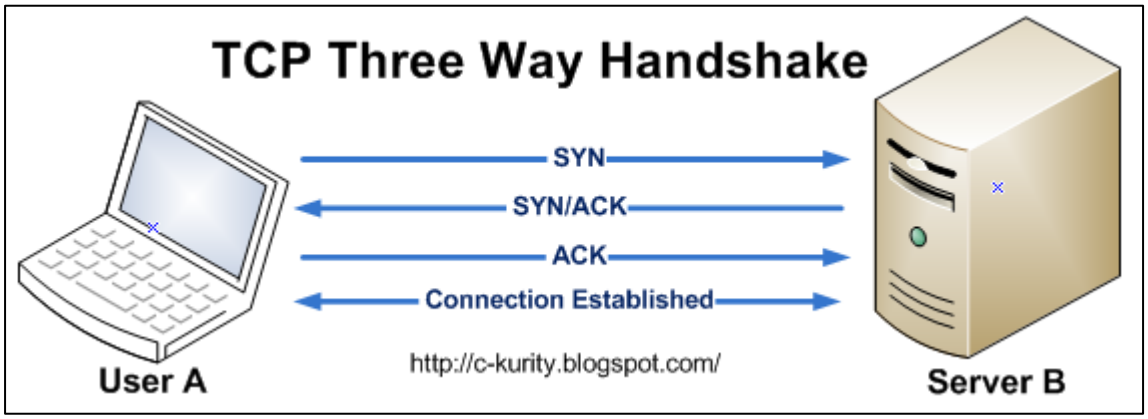
Los protocolos de comunicación en esta capa podrán ser TCP (*transmission control protocol*) o UDP (*user datagram protocol*), en los cuales se definirán los puertos en los que se harán las conexiones y los servicios a los cuales se quiere ingresar.

TCP es un protocolo orientado a las conexiones confiables y de control de flujo. En estas comunicaciones es necesario establecer una conexión inicial conocida como 3 *way hand shake*, en la cual el equipo 'cliente' tendrá que hacer

una solicitud de conexión hacia el 'servidor' que almacena la aplicación. Después de realizar la solicitud, el servidor le contestará al cliente informando que recibió su mensaje y que puede empezar a establecerse la comunicación.

Como se aprecia en la figura 4, el 'User A' envía como inicio un mensaje SYN o de sincronización, después de recibirla el 'Server B', devuelve un mensaje de acuse de recibido o ACK, juntamente con el mensaje de sincronización. Después de que el User A devuelve el mensaje de acuse de recibido, la conexión se establece y empieza la comunicación.

Figura 4. **Comunicación TCP**



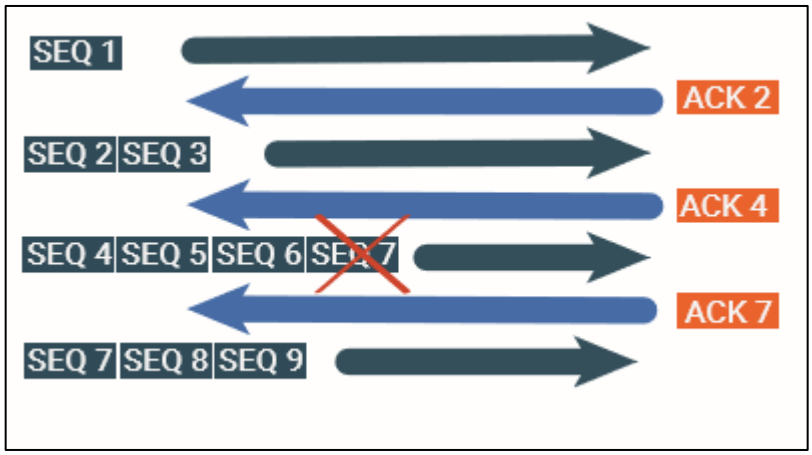

Fuente: STEEMIT. *Comunicación TCP*. https://steemit.com/hack/@pierlave/understand-tcp-3-way-handshake. Consulta: 5 de diciembre de 2018.

Las comunicaciones en TCP están orientadas a que los paquetes de envío y recibo puedan realizarse a un 100 %, sin perder.

Existe un concepto llamado 'ventana deslizante', la cual actuará después de establecer la conexión 3 *way handshake*, en la que el cliente hará una petición hacia el servidor y le hará saber que está recibiendo los paquetes que

solicita y que puede enviar uno más, y así consecutivamente. Llegará un punto en el que la ventana llegará a su límite y empezará a perder paquetes, por lo que le hará saber al cliente que no pueden transmitirse más paquetes de los que ya se están transmitiendo y que se mantenga así para tener una comunicación óptima, como se observa en la figura 5.

Figura 5. **Tamaño de ventana deslizante**

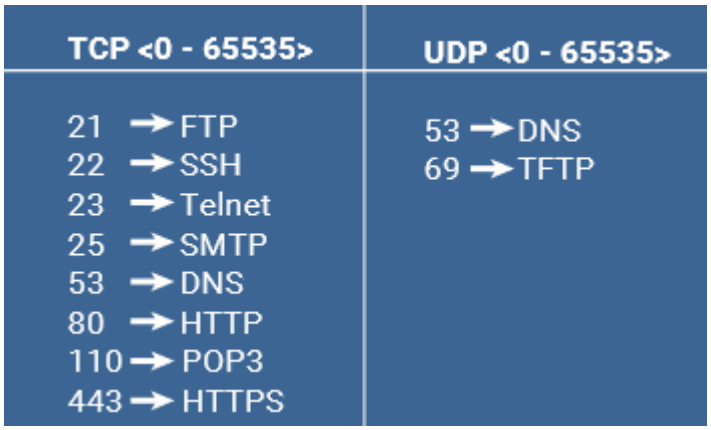



Fuente: elaboración propia.

El protocolo UDP es también un protocolo de comunicación, en el cual prevalecerán los servicios que no necesiten una comunicación de envío de datos confiable, ya que no necesita establecer conexiones antes de empezar a transmitir los datos.

Cada protocolo puede trabajar con sus propios puertos, todos independientes y que, según su número, así es la aplicación a la que están asociados, como se observa en la figura 6.

Figura 6. **Puertos TCP/UDP**




Fuente: elaboración propia.

Después de que se conoce el puerto por el que se va a establecer la conexión, se crea un '*socket*', en el cual se incluirá la dirección IP y el puerto al que se realizará la solicitud, por ejemplo: 8.8.8.8:53

El *socket* separa la IP y el puerto con un símbolo de ':'.

En el ejemplo, se está haciendo una solicitud de DNS al servidor de Google, el cual está alojado en la IP 8.8.8.8, la cual es una comunicación UDP.

### 1.2.5. Capa 7, aplicación que se desarrollará para el control remoto

La capa de aplicación es la que se encarga de interactuar entre el usuario final y toda la comunicación a nivel lógico de las capas inferiores. Esta aplicación ya deberá estar creada en una plataforma que esté alojada en un servidor por medio de una IP y un nombre de dominio (DNS). En este caso, se

trabajará sobre un servicio HTTP o HTTPS, en la cual se estará enviando información desde la aplicación hasta el conmutador remoto, atravesando la intranet diseñada para la comunicación.

# 2. DESARROLLO DEL HARDWARE DE CONTROL PARA SEMÁFORO

## 2.1. Diseño de electrónica para conmutación

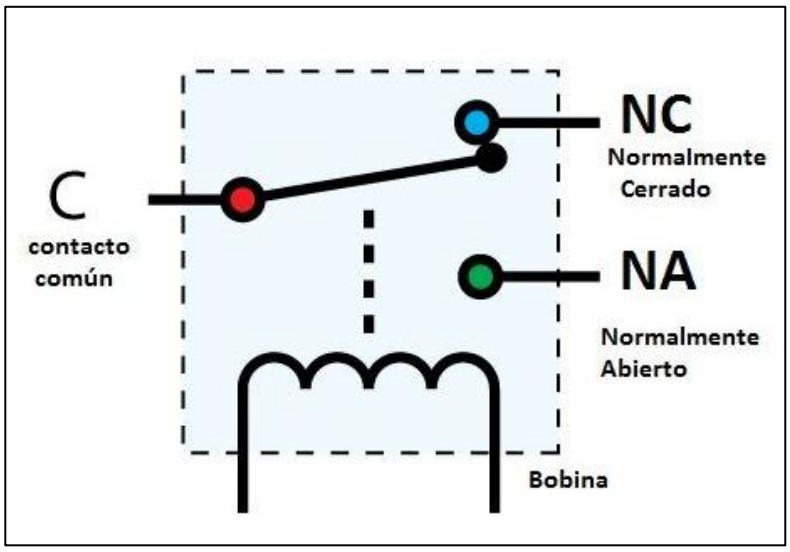
A continuación, se presenta el diseño de electrónica para conmutación.

### 2.1.1. Control de relé para cambio de función en semáforo (automático a manual)

Es un aparato eléctrico que funciona como un interruptor, abrir y cerrar el paso de la corriente eléctrica, pero accionado eléctricamente. El relé permite abrir o cerrar contactos mediante un electroimán, por eso también se llaman relés electromagnéticos o relevador.

Como se aprecia en la figura 7, existe un común entre los 2 contactos, el cual está denotado como C; NC cuando opera sin inducción en la bobina y NA cuando la bobina es inducida. Esto, como bien se mencionaba antes, se hace a través de un electroimán, el cual creará un campo magnético ya traerá el contacto hacia NA.

Figura 7. **Relé de conmutación simple tiro simple polo**




Fuente: Areatecnologia. *Relé de comunicación*.
https://www.areatecnologia.com/electricidad/rele.html. Consulta: 7 de diciembre de 2018.

Los relés eléctricos son básicamente interruptores operados eléctricamente que vienen en muchas formas, tamaños y potencias adecuados para todo tipo de aplicaciones. Los relés también pueden ser relés de potencia, más grandes y utilizados para la tensión mayores o aplicaciones de conmutación de alta corriente. En este caso se llaman contactores, en lugar de relés.

Los semáforos, también conocidos técnicamente como señales de control de tráfico, son dispositivos de señales que se sitúan en intersecciones viales y otros lugares para regular el tráfico, por ende, el tránsito peatonal.

- Funcionamiento

Los semáforos de control de tráfico vehicular pueden funcionar de dos maneras distintas; el cambio de estado puede depender del tiempo o bien del tránsito. En ciertas intersecciones hay que presionar un botón para activar el cambio de estado a rojo para que los peatones y los vehículos puedan pasar. Esto posibilita una circulación fluida.

- Estados

    - Verde: los vehículos tienen derecho al paso.

    - Amarillo: advierte a los conductores de los vehículos que el estado verde está a punto de cambiar para pasar al estado rojo posteriormente y, por lo tanto, debe asumir una conducta de prevención como acabar su marcha si está muy próximo a la intersección y una frenada brusca podría ocasionar situaciones peligrosas con los vehículos de atrás y detener su marcha con el fin de que la intersección no sea bloqueada y los vehículos de las demás corrientes pueden circular en el período de verde que va a iniciar. Cuando se ilumina la lente amarilla con destellos intermitentes, los conductores de los vehículos realizan el cruce con precaución. El amarillo intermitente se emplea en la vía que tenga preferencia.

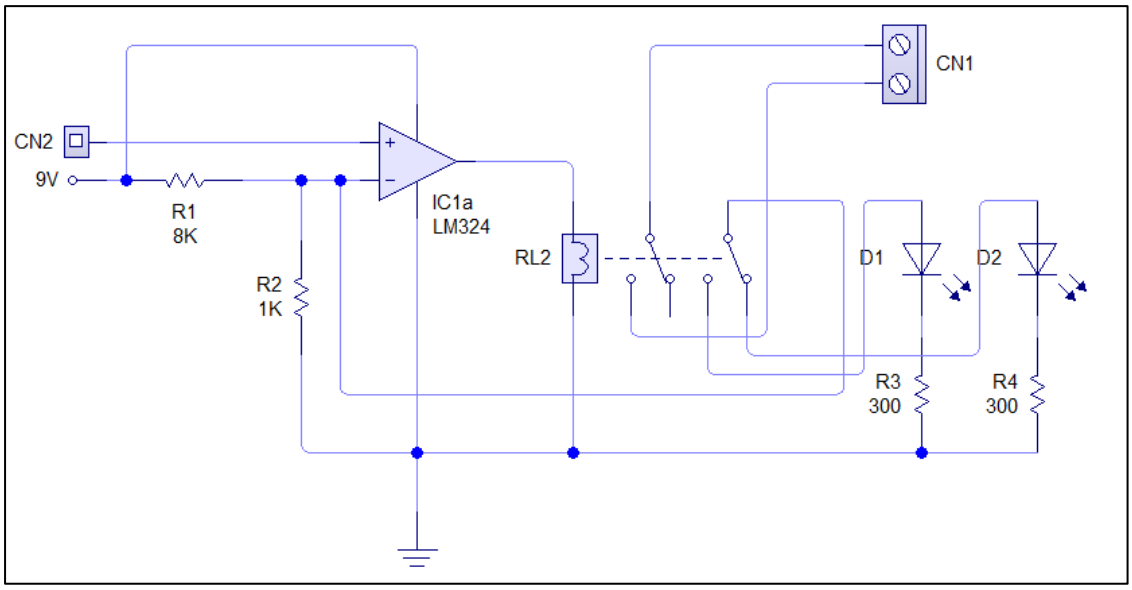
    - Rojo: los vehículos deben detenerse a una distancia de dos metros del semáforo.

La definición del dispositivo de conmutación se debió a que, en su mayoría, los semáforos cuentan con modos de operación, los cuales pueden trabajar permanentemente en modo automático, o bien cambiar a modo manual, lo cual se hace con un interruptor común y corriente, y un botón de pulso, el cual le va a indicar al semáforo cuando tiene que hacer la conmutación al siguiente estado.

En esta etapa del proyecto se realizará la circuitería necesaria para mantener el semáforo en un modo de operación.

Diagrama de circuito creado en el programa LiveWire:

Figura 8. **Diagrama de circuito de conmutación**




Fuente: elaboración propia, empleando LiveWire y PCB Wizard.

Descripción del diagrama:

- CN2: entrada física del microcontrolador, la cual enviará el nivel de voltaje a comparar en el amplificador operacional.
- R1: resistencia para divisor de voltaje.
- R2: resistencia para divisor de voltaje.
- IC1a: amplificador operacional LM324 para comparador de ventana.
- RL2: relé doble tiro doble polo para accionar el sistema en un modo de operación.
- CN1: entrada física de las terminales asociadas al interruptor que controla el modo de operación del semáforo.
- D1: indica que el estado del semáforo está trabajando en modo automático.
- D2: indica que el estado del semáforo está trabajando en modo manual.
- R1. R2: resistencias para proteger a los led de D1 y D2.

El diagrama consta de un relé DPDT (doble tiro doble polo), el cual tiene el control de 2 contactores a través de una bobina en su interior. Con uno de los contactores realizará el control del modo de operación del semáforo y con el segundo indicará por medio de un led el estado en el que se encuentra trabajando.

Al principio del circuito se observa un comparador de ventana, el cual tomará los valores de entrada del microcontrolador Arduino y un valor a comparar con un divisor de voltaje. El comparador, mientras el valor del voltaje del microcontrolador sea menor a +1V, el relé no se encenderá; cuando el valor del voltaje del microcontrolador sea mayor a +1V, este alimentará el relé con un voltaje de +9V, los cuales harán que el relé conmute hacia el estado del semáforo en el que estará en modo manual.

De esta manera, mientras el microcontrolador tenga un pulso alto de salida, el semáforo estará funcionando de forma manual, lo cual permitirá que la segunda parte del circuito, la cual consta de la conmutación de colores del semáforo, esté activa.

La ecuación para determinar el valor de salida del comparador está dada por la siguiente expresión:

$$Vout = (Vin * R2)/(R1 + R2)$$
$$Vin = 9v$$
$$R2 = 1\,000\ \Omega$$
$$R1 = 8\,000\ \Omega$$
$$Vout = 1v$$

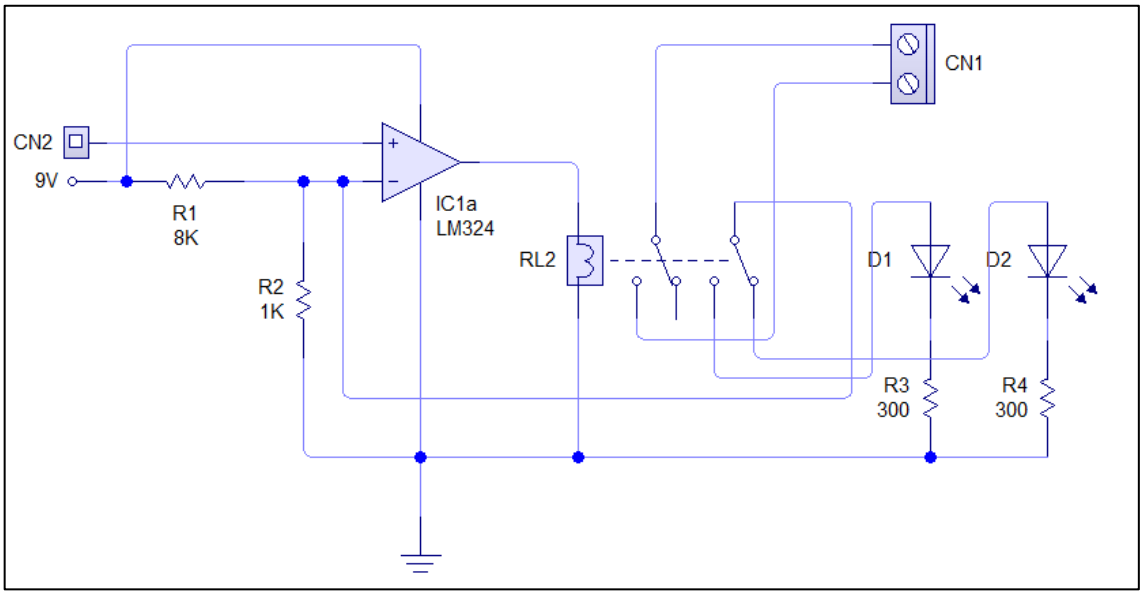
### 2.1.2. Control de relé de conmutación para estados de semáforo

A diferencia del controlador para el modo de funcionamiento, este control estará encargado de cumplir la función de un botón de pulso. El tiempo en el que este mecanismo va a entrar en función estará definido por el microcontrolador, el cual enviará un pulso al comparador de ventana, en el que

el relé hará la conmutación y esta cambiará nuevamente de estado al ya no recibir el pulso del microcontrolador.

El diagrama del circuito será similar al anterior:

Figura 9. **Diagrama de conmutación**




Fuente: elaboración propia, empleando LiveWire y PCB Wizard.

Descripción del diagrama:

- CN2: entrada física del microcontrolador, la cual enviará el nivel de voltaje a comparar en el amplificador operacional.

- R1: resistencia para divisor de voltaje.

- R2: resistencia para divisor de voltaje.

- IC1a: amplificador operacional LM324 para comparador de ventana.

- RL2: relé doble tiro doble polo para accionar el sistema en un modo de operación.

- CN1: entrada física de las terminales asociadas al interruptor que controla el modo de operación del semáforo.

- D1: indica que el estado del semáforo está trabajando en modo automático.

- D2: indica que el estado del semáforo está trabajando en modo manual.

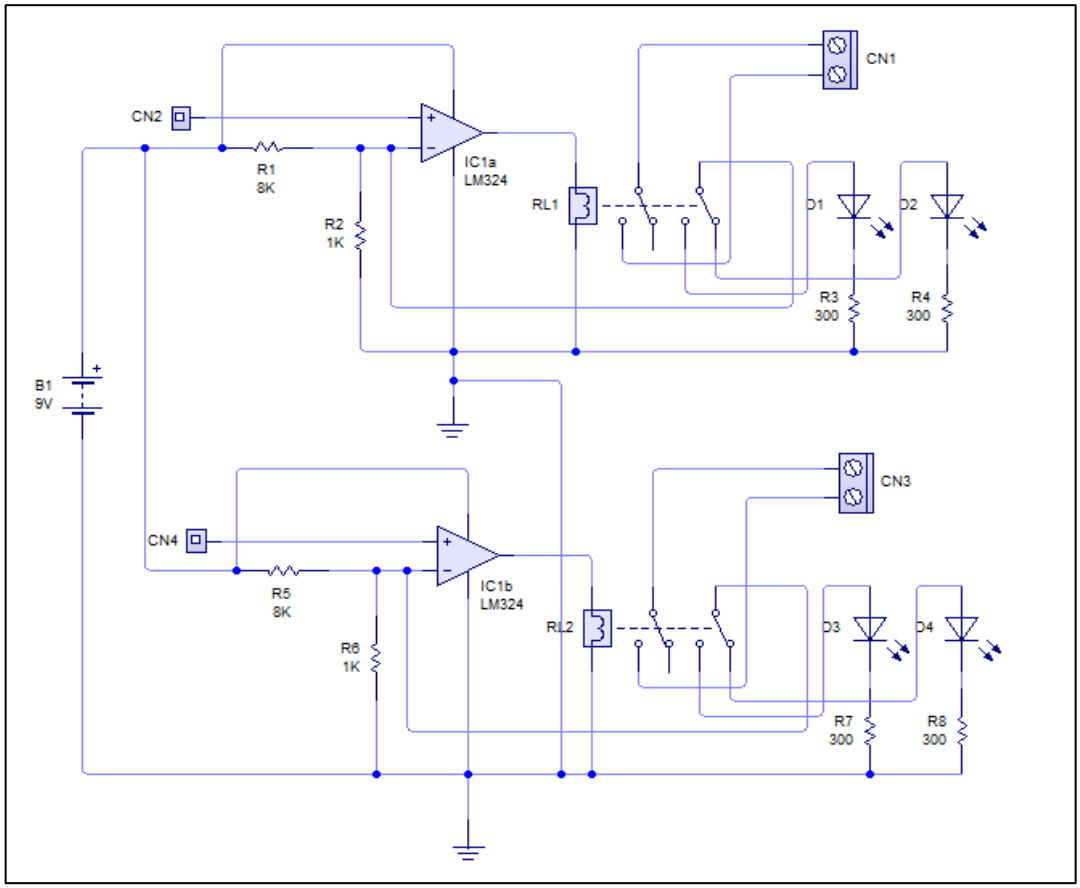
- R1. R2: resistencias para proteger a los led de D1 y D2.

### 2.1.3. Diseño de placa para circuitería

Para la placa del circuito, se tomarán en cuenta las 2 configuraciones mencionadas en el punto anterior, en las que actuará el modo de operación (automático o manual) y la conmutación del estado del semáforo; este diagrama está diseñado en PCB Wizard.

Diagrama final:

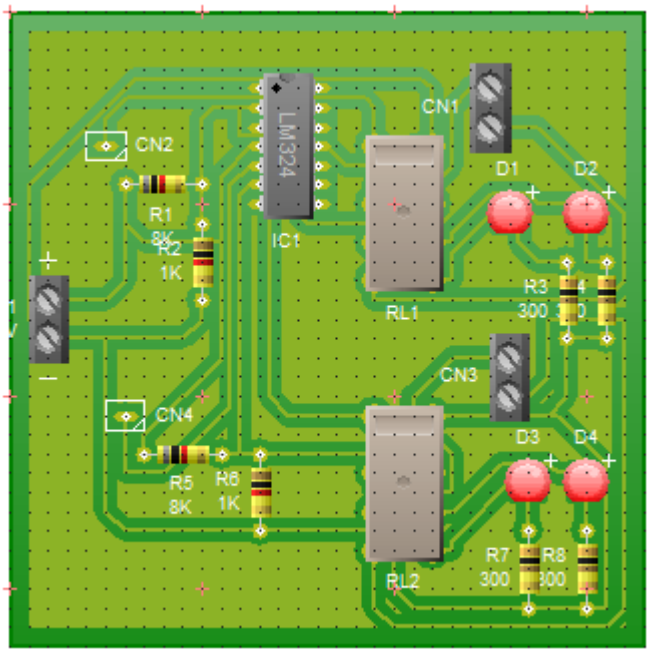
Figura 10. **Diagrama de conmutación para ambos circuitos**




Fuente: elaboración propia, empleando LiveWire y PCB Wizard.

La figura 11 muestra cómo puede llegar a verse la placa terminada con sus dispositivos electrónicos incluidos.

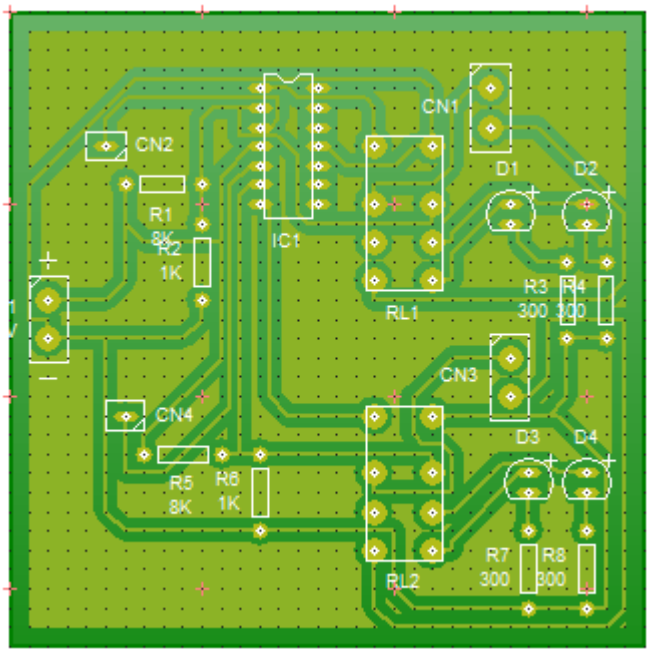
Figura 11. **Placa superficial del circuito**




Fuente: elaboración propia, empleando LiveWire y PCB Wizard.

La figura 12 muestra el impreso en cobre e indica en donde debe ir cada componente.

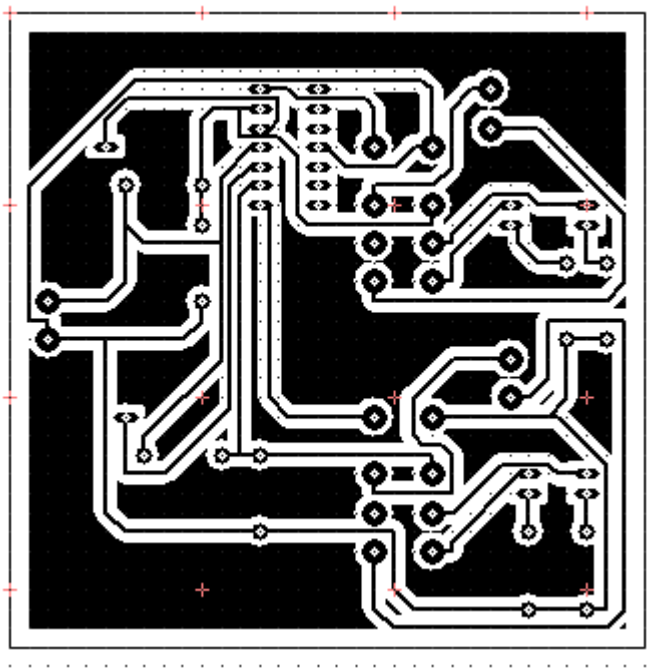
Figura 12. **Placa esquemática del circuito**




Fuente: elaboración propia, empleando LiveWire y PCB Wizard.

La figura 13 muestra la parte inferior de la placa, la cual se utilizará para realizar el impreso sobre la placa virgen de cobre.

Figura 13. **Placa de arte**



Fuente: elaboración propia, empleando LiveWire y PCB Wizard.

## 2.2. Microcontrolador Arduino

A continuación, se presenta la descripción del microcontrolador Arduino.

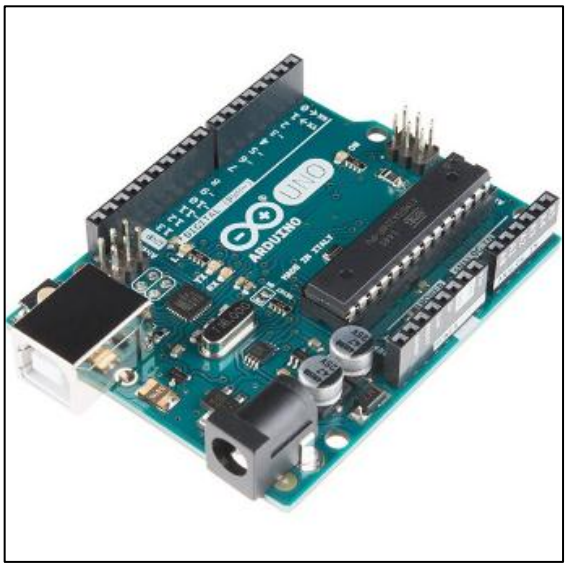
### 2.2.1. Arduino para el desarrollo de control

Arduino es una compañía de hardware libre, y comunidad tecnológica, que diseña y manufactura placas de desarrollo de hardware y software compuesta respectivamente por circuitos impresos que integran un microcontrolador, y un

entorno de desarrollo  en donde se programa cada placa. Arduino se enfoca en acercar y facilitar el uso de la electrónica y programación de sistemas embebidos en proyectos multidisciplinarios. Toda la plataforma, tanto para sus componentes de hardware como de software, es liberada bajo licencia de código abierto que permite libertad de acceso a los mismos.

El hardware consiste en una placa de circuito impreso con un microcontrolador, usualmente Atmel AVR, puertos digitales y analógicos de entrada/salida, los cuales pueden conectarse a placas de expansión (*shields*) que amplían las características de funcionamiento de la placa Arduino. Asímismo, posee un puerto de conexión USB desde donde se puede alimentar la placa y establecer comunicación serial con la computadora.

Figura 14. **Arduino UNO**



Fuente: Arduino. *Tarjetas Arduino*. https://tienda.bricogeek.com/arduino/305-arduino-uno-805833349009.html. Consulta: 10 de diciembre de 2018.

Las tarjetas Arduino son tarjetas que pueden ser utilizadas para muchos fines relacionados a implementaciones del conocido 'internet de las cosas', el cual contempla las disciplinas de las redes de telecomunicaciones, la electrónica y la programación, gracias a sus shields.

### 2.2.2. Integración de Shield Ethernet para comunicación TCP

Arduino cuenta con la Shiel Ethernet, la cual trabaja para la comunicación entre el microcontrolador y la red sobre la que se quiere implementar la comunicación. Estas trabajan en conjunto desde un mismo plano de programación.

Figura 15. **Shield Ethernet**

Fuente: Arduino. *Shield Ethernet*. https://www.amazon.com/Generic-Ethernet-Schild-Ethernet-shield-Arduino/dp/B00QFXE9K8. Consulta: 11 de diciembre de 2018.

## 2.3. Programación de tarjeta Arduino

A continuación, se presentarán las características necesarias en la programación para incluir la tarjeta Shield Ethernet y el Arduino para que pueda permitir comunicación hacia la red destino, que en este caso, se hará en la intranet diseñada para conectarse a la central. Adicional, se hará la configuración de la interfaz gráfica y la definición de puertos para que esta se pueda comunicar hacia la tarjeta de conmutación.

- Bloque 1

Se incluyen las librerías necesarias para la comunicación ethernet y serial:

```
#include <SPI.h>
#include <Ethernet.h>
```

- Bloque 2

Se configuran los parámetros de la red que tendrá el servidor web por medio del direccionamiento IP, direccionamiento físico MAC y puerto de comunicación:

```
byte mac[] = { 0xDE, 0xAD, 0xBE, 0xEF, 0xFE, 0xED };   //  Dirección física
byte ip[] = { 192, 168, 1, 50 };                    // IP del servidor, la cual servirá para la conexión
byte gateway[] = { 192, 168, 1, 1 };                // Puerta de enlace o gateway
byte subnet[] = { 255, 255, 255, 0 };               // Máscara de red
EthernetServer server(80);                          // Puerto web, el cual puede cambiar a conveniencia
```

String readString; // Lee las variables de los vectores anteriores

- Bloque 3

Inicialización de la comunicación serial y conexión ethernet, definición de puertos de salida :

```
void setup() {

  Serial.begin(9600);
   while (!Serial) {
    ;
  }
  pinMode(2,OUTPUT);
  pinMode(3,OUTPUT);
  pinMode(4, OUTPUT);
  pinMode(5,OUTPUT);
  pinMode(6,OUTPUT);
```

Ethernet.begin(mac, ip, gateway, subnet); // Inicializa la conexión ethernet y el servidor

```
  server.begin();
  Serial.print("web server: ");
  Serial.println(Ethernet.localIP());    // Imprime la dirección IP
}
```

- Bloque 4

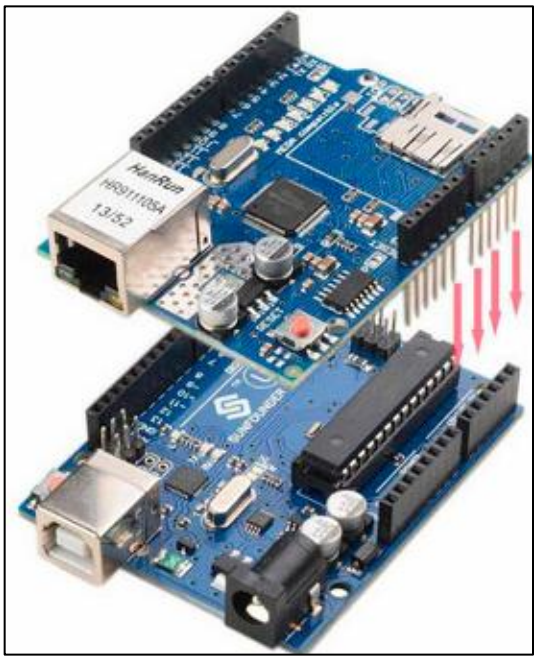
En este bloque se observa la ejecución del código que presentará la plataforma o interfaz web a través de HTTP, en donde se hará la definición de los botones que darán la orden para ejecutar un proceso y la acción que debe tomar al ser presionado:

```
void loop() {
  // Crea una conexión cliente
  EthernetClient client = server.available();
  if (client) {
    while (client.connected()) {
      if (client.available()) {
        char c = client.read();
        //Lee caracter por caracter HTTP
        if (readString.length() < 100) {
          //Almacena los caracteres a un String
          readString += c;
         }
         // si el requerimiento HTTP fue finalizado
         if (c == '\n') {
           Serial.println(readString); //Imprime en el monitor serial
           client.println("HTTP/1.1 200 OK");          //envía una nueva página en código HTML
           client.println("Content-Type: text/html");
           client.println();
           client.println("<HTML>");
           client.println("<HEAD>");
           client.println("<TITLE>CONTROL DE SEMAFORO</TITLE>");
```

```
            client.println("</HEAD>");
            client.println("<BODY>");
            client.println("<hr />");
            client.println("<H1>Intellisys</H1>");
            client.println("<a href=\"/boton1on\"\"> CAMBIO A MODO MANUAL
</a> ");
            client.println(" | | | ");
            client.println("<a     href=\"/boton1off\"\">     CAMBIO     A     MODO
AUTOMATICO </a><br /> ");
            client.println("<br />");
            client.println("<a  href=\"/boton2on\"\"> CONMUTAR  A  SIGUIENTE
ESTADO </a> ");
            client.println(" | | | ");
            client.println("</BODY>");
            client.println("</HTML>");
            delay(1);
            //detiene el cliente servidor
            client.stop();
             //control del arduino si un botón es presionado
            if (readString.indexOf("boton1on") >0){
               digitalWrite(2, HIGH);
            }
            if (readString.indexOf("boton1off") >0){
               digitalWrite(2, LOW);
            }
             if (readString.indexOf("boton2oN") >0){
               digitalWrite(3, HIGH);
          delay(60);
           digitalWrite(3, LOW);
```

```
            }
             // Limpia el String cadena de caracteres para una nueva lectura
             readString="";
           }
         }
       }
}
```

Figura 16. **Arduino UNO y Shield Ethernet**



Fuente: Arduino. *Arduino y shield Ethernet*. https://www.luisllamas.es/arduino-ethernet-shield-w5100/. Consulta: 11 de diciembre de 2018.

# 3. UNIFICACIÓN DE RED Y HARDWARE PARA COMUNICACIÓN Y CONTROL DE DISPOSITIVOS

## 3.1. Segmentación de red para comunicación entre los puntos remotos y central de comunicación

La segmentación de redes es utilizada para la separación en dominios de *broadcast* y asignación de roles dentro de una intranet compuesta por redes privadas.

### 3.1.1. Asignación de IPs para cada punto remoto

La comunicación entre los dispositivos se hará a través de redes punto a punto, ruteadas desde la central de comunicaciones, en la cual serán declaradas las IPs de conexión, las redes LAN y las políticas de acceso que estas redes pueden tener. También se tomará en cuenta la utilización de VPNs, las cuales serán L2TP por su manejo de datos en L2 o capa 2 del modelo OSI, que en MikroTik funciona de la siguiente manera:

- L2TP

L2TP es un protocolo de túnel seguro para el transporte de tráfico IP utilizando PPP. L2TP encapsula PPP en líneas virtuales que se ejecutan sobre IP, Frame Relay y otros protocolos (que actualmente no son compatibles con MikroTik RouterOS). L2TP incorpora PPP y MPPE (Microsoft Point to Point Encryption) para hacer enlaces encriptados. El propósito de este protocolo es permitir que los puntos finales de capa 2 y PPP residan en diferentes

dispositivos interconectados por una red de conmutación de paquetes. Con L2TP, un usuario tiene una conexión de capa 2 a un concentrador de acceso - LAC (por ejemplo, un banco de módem, ADSL DSLAM, entre otros.), y el concentrador luego conecta los marcos PPP individuales al servidor de acceso a la red - NAS. Esto permite que el procesamiento real de los paquetes PPP se separe de la terminación del circuito de capa 2. Desde la perspectiva del usuario, no hay ninguna diferencia funcional entre hacer que el circuito L2 termine en un NAS directamente o usar L2TP.

También, puede ser útil usar L2TP como cualquier otro protocolo de tunelización con o sin cifrado. El estándar L2TP dice que la forma más segura de cifrar datos es usar L2TP sobre IPsec (tenga en cuenta que es el modo predeterminado para el cliente Microsoft L2TP), ya que todos los paquetes de datos y control L2TP para un túnel en particular aparecen como paquetes de datos homogéneos de UDP / IP para el Sistema IPsec.

Se admite el PPP de multienlace (MP) para proporcionar MRRU (la capacidad de transmitir paquetes de tamaño completo de 1 500 y más grandes) y conectar enlaces PPP (mediante el protocolo de control de puente (BCP) que permite enviar tramas Ethernet sin formato a través de enlaces PPP). De esta manera es posible configurar el puente sin EoIP. El puente debe tener una dirección MAC configurada administrativamente o una interfaz similar a Ethernet, ya que los enlaces PPP no tienen direcciones MAC.

L2TP incluye autenticación PPP y contabilidad para cada conexión L2TP. La autenticación completa y la contabilidad de cada conexión se pueden realizar a través de un cliente RADIUS o localmente.

Se admite el cifrado MPPE 128bit RC4.

El tráfico L2TP utiliza el protocolo UDP tanto para el control como para los paquetes de datos. El puerto UDP 1701 se usa solo para el establecimiento del enlace.

Tomando en cuenta las clases de IPs privadas que existen, se pueden segmentar de la siguiente manera:

- La clase A se utilizará para enlaces que necesiten de una conexión a través de VPN, ya que esta depende de un servidor que estará configurado en el router central y realiza la comunicación a los clientes por medio de una IP local y una remota, teniendo como local la IP 10.1.1.1/24.

- La clase B se utilizará para la asignación de redes LAN en los puntos remotos, la cual tendrá cada servidor web para comunicarse a la central.

- La clase C se utilizará para las conexiones punto a punto (PTP), las cuales se tomarán como las direcciones WAN de cada punto remoto. Estas estarán asignadas sobre la interfaz de comunicación, ya sea por medio de una interfaz física, una VLAN o un túnel en capa 2 o 3.

En el cuadro mostrado en la tabla I se observa la asignación de las redes, tomando en cuenta que pueden ser más servicios los que se conecten.

Tabla I. **Asignación de redes**

| Nombre | Clase A | Clase B | Clase C |
|---|---|---|---|
| Semáforo 1 | 10.1.1.11/24 | 172.16.1.0/24 | 192.168.0.0/30 |
| Semáforo 2 | 10.1.1.12/24 | 172.16.2.0/24 | 192.168.0.4/30 |
| Semáforo 3 | 10.1.1.13/24 | 172.16.3.0/24 | 192.168.0.8/30 |
| Semáforo 4 | 10.1.1.14/24 | 172.16.4.0/24 | 192.168.0.12/30 |
| Semáforo 5 | 10.1.1.15/24 | 172.16.5.0/24 | 192.168.0.16/30 |
| Semáforo 6 | 10.1.1.16/24 | 172.16.6.0/24 | 192.168.0.20/30 |
| Semáforo 7 | 10.1.1.17/24 | 172.16.7.0/24 | 192.168.0.24/30 |
| Semáforo 8 | 10.1.1.18/24 | 172.16.8.0/24 | 192.68.0.28/30 |
| Semáforo 9 | 10.1.1.19/24 | 172.16.9.0/24 | 192.168.0.32/30 |

Fuente: elaboración propia.

## 3.2. Conexión entre *router* y tarjeta Arduino

Para iniciar la comunicación entre el *router* del cliente o semáforo y la tarjeta Arduino, lo primero a configurar es la dirección IP que el servidor web utilizará, que en este caso es el Arduino. Esta configuración debe estar tanto en la tarjeta arduino como en el router. Esto servirá para indicarle al servidor a que dominio de *broadcast* pertenece.

A continuación, se detallan las configuraciones necesarias en el servidor y en el *router*:

- Configuraciones *router* MikroTik

    - Definir la interfaz a la que estará conectado el servidor y la interfaz WAN.

/interface ethernet
set [ find default-name=ether1 ] name=ether1-wan
set [ find default-name=ether2 ] name=ether2-servidor-web1

En este caso, se tomará en cuenta el ether2 como la conexión hacia el servidor web (Arduino).

    - Configuración del direccionamiento IP sobre la interfaz de acceso e interfaz WAN.

/ip address
add address=172.16.1.1/24 interface=ether2-servidor-web1 network=172.16.1.0
add address=192.168.0.2/30 interface=ether1-wan network=192.168.0.0

Como se observa en la configuración, el servidor pertenece a la red 172.16.1.0/24, por lo que tendrá que tener configurada una IP de este dominio.

    - Configuración del direccionamiento IP sobre servidor web

```
byte ip[] = { 172, 16, 1, 50 };
byte gateway[] = { 172, 16, 1, 1 };
byte subnet[] = { 255, 255, 255, 0 };
```

Estas configuraciones permitirán que el servidor pueda conocer a la red asignada por el *router* a través del puerto ether2-servidor-web1.

Al momento de estar conectado el servidor, se pueden realizar pruebas de comunicación entre ambos dispositivos, por medio de un PING (ICMP) y la tabla ARP del equipo MikroTik.

- Pruebas ICMP entre router y servidor

```
[admin@Semaforo_1] > ping 172.16.1.50
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 172.16.1.50                              56 128 0ms
    1 172.16.1.50                              56 128 0ms
    2 172.16.1.50                              56 128 1ms
    3 172.16.1.50                              56 128 0ms
    4 172.16.1.50                              56 128 3ms
    5 172.16.1.50                              56 128 0ms
    6 172.16.1.50                              56 128 0ms
    7 172.16.1.50                              56 128 0ms
    8 172.16.1.50                              56 128 0ms
    9 172.16.1.50                              56 128 1ms
   10 172.16.1.50                               56 128 0ms
   11 172.16.1.50                               56 128 0ms
   12 172.16.1.50                               56 128 1ms
   13 172.16.1.50                               56 128 1ms
   14 172.16.1.50                               56 128 1ms
   15 172.16.1.50                               56 128 0ms
   16 172.16.1.50                               56 128 1ms
   17 172.16.1.50                               56 128 0ms
```

18 172.16.1.50 56 128 0ms

19 172.16.1.50 56 128 1ms

sent=20 received=20 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=3ms

En esta prueba se puede apreciar que los paquetes fueron enviados a su IP destino con éxito, teniendo un total de 20 paquetes enviados, 20 recibidos, 0 % de pérdida y un promedio de 0ms en el retardo.

- Prueba desde tabla ARP llamada desde equipo MikroTik en terminal

[admin@Semaforo_1] > ip arp
[admin@Semaforo_1] /ip arp> print
Flags: X - disabled, I - invalid, H
C - complete
# ADDRESS MAC-ADDRESS
0 DC 172.16.1.50 28:F1:0E:43:96

Desde esta tabla se ve la dirección lógica (IP) y física (MAC) del servidor conectado directamente al router.

# 4. DISEÑO DE INTRANET (RED)

## 4.1. Definición de *router* central y remotos para el control en capa 2 y 3 de los datos

MikroTik es una empresa perteneciente a Latvia Letonia, la cual empezó a funcionar en 1996 ofreciendo sistemas operativos para redes de baja y alta eficiencia, la cual llamaron RouterOS el siguiente año. Su producto llegó al mercado en el año 2002, siendo un hardware que aprovechará al máximo sus grandes capacidades de multiprocesamiento y multinúcleo, el cual es conocido como el hardware RouerBOARD.

Con el paso de los años, a partir del nacimiento del internet, los administradores de red han visto pasar varios fabricantes por sus rarcks; el referente a Cisco; sin embargo, este producto siempre presentó un alto costo, lo cual fue importante a la hora de la toma de decisiones e implementaciones en una red a nivel de ISP/WISP.

Mikrotik, hasta hace unos años, empezó a conocerse en Latinoamérica, siendo partícipes los diferentes emprendedores, los cuales no contaban con un capital muy sólido como las grandes empresas de telecomunicaciones, por lo que optaron por incluir RouterOS y RouterBOARD en sus implementaciones.

Hoy en día, en Guatemala, un buen porcentaje de proveedores de internet en el interior de país trabajan con estos dispositivos, tanto para configuraciones en sus core, como a nivel de transporte de datos, ya que MikroTik ofrece una

alta gama de dispositivos útiles en la comunicación a nivel de fibra óptica y radiofrecuencia.

Estos equipos han ido escalando en las empresas de telecomunicaciones, ya que, por su bajo costo en comparación con otros equipos con las mismas cualidades, han llevado a que los usuarios confíen de tal manera que estructuren redes LAN y WAN con las mismas, a nivel de core, distribución y transporte.

Las prestaciones de estos equipos no se limitan al tema de ruteo o transporte, ya que ofrecen otros servicios bastante útiles, como los son sus opciones de firewall, balanceo de carga, utilización de VPNs, MPLS, VPLS y QoS, lo cual es indispensable en una intranet o extranet por temas de seguridad y alta disponibilidad.

- RouterOS

MikroTik RouterOS es el sistema operativo del hardware RouterBOARD, que tiene las características necesarias para ISP: Firewall, Router, MPLS, VPN, Wireless, HotSpot, QoS, entre otros.

Es un sistema operativo independiente basado en el kernel de Linux v3.3.5 que proporciona todas las funciones en una instalación rápida y sencilla, con una interface fácil de usar.

Puede instalarse en PCs y otros dispositivos de hardware compatibles con x86, como tarjetas embedidas, sistemas minilTX. RouterOS soporta computadoras multicore y multiCPU, soporta también multiprocesamiento

simétrico (SMP: Symmetric MultiProcessing). Se puede ejecutar en tarjetas madre Intel más recientes y aprovechar los nuevos CPUs multicore.

- Multiprocesamiento simétrico

Es una arquitectura de software y hardware donde dos o más procesadores idénticos son conectados a una simple memoria compartida; tiene acceso a todos los dispositivos I/O, y que son controlados por una simple instancia del OS (sistema operativo), en el cual todos los procesadores son tratados en forma igualitaria, sin que ninguno sea reservado para propósitos especiales.

RouterOS soporta una gran variedad de interfaces de red, que incluye tarjetas Ethernet de 10 Gbps, tarjetas wireless 802.11a/b/g/n/ac y modems 3 G y 4 G.

- Características de RouterOS

    - Instalación basada en red desde una tarjeta de red.

    - Configuración basada en MAC e IP a través de WinBox, WebFig, CLi, APi.

    - Respaldo y restauración por medio de configuración binaria o formato de texto.

    - Firewall, filtrado basado en el estado del paquete (*statefull filtering*), NAT, marcas internas, filtrado basado en IP, puerto,

listas de direcciones, filtros en capa 7, soporte IPv6, PCC por clasificación de conexiones para balanceo de carga.

- Ruteo estático, VRF, ruteo basado en políticas, interfaz de ruteo, ruteo ECMP, ruteo dinámico IPv4 con RIP v1/2, OSPF v2, BGP v4, ruteo IPv6 y BFD.

- MPLS, LDP para IPv4, SLB para IPv4, túneles de ingeniería de tráfico RSVP, VPLS MP-BGP, etc.

- VPNs IPsec, túnel y modo de transporte, certificado o PSK, protocolo de seguridad AH y ESP, PTP tunneling con PPTP, PPPoE, L2TP, SSTP, IPIP, EoIP, 6to4 (IPv6 sobre redes IPv4, VLAN para IEEE 802.1q, soporta Q-in-Q. VPNs basadas en MPLS.

- Wireless AP IEEE 802.11a/b/g, IEEE 802.11n, protocolos propietarios Nstreme y Nstreme2, protocolo NV2, WDS, Virtual AP, WEP, WPA, WPA2, control por lista de acceso (access list), *roaming* de cliente.

- DHCP server por interface, DHCP client y relay, arrendamiento de direcciones IP (leases) DHCP estáticas y dinámicas, soporte RADIUS, opciones personalizadas de DHCP

- HotSpot, acceso plug and play a la red, autenticación de clientes de redes locales, contabilización de usuarios.

- QoS, sistema HTB (*hierarchical token bucket*), rafagas y soporte de prioridades, colas simples, entrega equitativa de ancho de banda al cliente de forma dinámica (PCQ).

- Proxy, servidor para almacenamiento en caché de HTTP, proxy transparente HTTP, soporte de protocolos SOCKS, entradas estáticas DNS, *access control list*, *caching list*.

- Herramientas

  - Ping
  - Traceroute
  - Test de ancho de banda (bandwidth test)
  - Ping flood
  - Packet sniffer
  - Torch
  - Telnet
  - SSH
  - E-mail y herramientas de envío de SMS
  - Herramienta de ejecución de Scritps automatizados
  - Generador avanzado de tráfico

- RouterBOARD

Es una familia de soluciones de hardware con circuitos diseñados por MikroTik para responder a las necesidades de los clientes a nivel mundial. Todas las placas RouterBOARD operan con el mismo sistema operativo RouterOS.

Esta división de hardware se caracteriza por incluir su sistema operativo RouterOS y actualizaciones de por vida. Estos dispositivos tienen la ventaja de tener una excelente relación costo/beneficio comparados con otras soluciones en el mercado.

Tabla II. **Arquitecturas soportadas**

| Arquitectura | Series |
|---|---|
| mipsbe | CRS, NetBox, NetMetal, PowerBox, RB9xx, hAP, mAP, RB4xx, cAP, hEX, wAP, BaseBox, DinaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx |
| smips | hAP Lite |
| tile | CCR |
| pcc | RB3xx, RB600, RB8xx, RB1xxx |
| arm | RB3011 |
| x86 | PC / x86, RB230 |
| mipsle | RB1xx, RB5xx, RB Crossroads |

Fuente: elaboración propia.

Todas las series descritas antes son los diferentes RouterBOARD que en la actualidad están disponibles en el catálogo de MikroTik y cada una tiene una función específica, como los equipos con arquitectura 'tile', la cual se utiliza para router Cloud Core, que por lo regular tienen un número mayor o igual a 9 núcleos, los cuales se utilizan para redes core o distribución para manejo de anchos de banda mayores a 1 Gbps y otras utilidades relacionadas con multiprocesamiento.

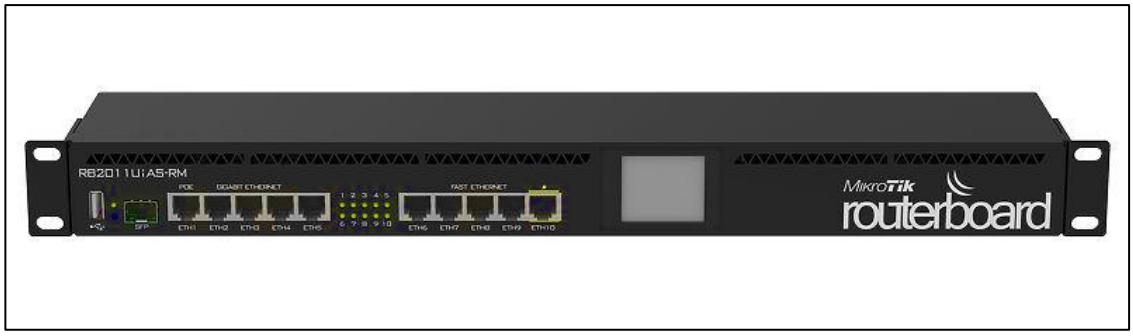
### 4.1.1. Equipos MikroTik para creación de redes LAN y WAN

Después de haber visto un resumen de lo que representan los equipos MikroTik, su escalabilidad y funcionalidad; se describen a continuación algunos de los equipos que pueden utilizarse para la implementación de este proyecto:

- Red core

Dado que no será para el manejo de anchos de banda elevados, puede tener como router principal un equipo RB2011UiAS-RM.

Figura 17. **RB2011UiAS-RM**




Fuente: LLAMAS, Luis. *Routerboard.* https://www.luisllamas.es/Routerboard-w5100/. Consulta: 11 de diciembre de 2018.

Este equipo tiene las siguientes características:

El RB2011 es una serie de dispositivos multipuerto de bajo costo. Diseñado para uso en interiores y disponible en muchos estilos diferentes, con una multitud de opciones.

El RB2011 está alimentado por RouterOS, un sistema operativo de enrutamiento con todas las funciones que se ha mejorado continuamente durante quince años. Enrutamiento dinámico, *hotspot*, *firewall*, MPLS, VPN, calidad de servicio avanzada, equilibrio de carga y enlace, configuración y monitoreo en tiempo real, solo algunas de las muchas funciones que admite RouterOS.

El RB2011iL-RM incluye una nueva función, el inyector de energía en el puerto Ethernet 10, que puede alimentar a otros dispositivos con capacidad PoE con el mismo voltaje que se aplica a la unidad. La carga máxima en el puerto es de 500mA. Está alimentado por el nuevo procesador de red Atheros 600MHz 74K MIPS, tiene 64 MB de RAM y una licencia nivel 4 RouterOS, así como cinco puertos Gigabit Ethernet,  cinco puertos Fast Ethernet y un puerto óptico Gigabit Ethernet.

RouterBOARD RB2011UiAS-RM viene con una caja de montaje en rack de 1U y fuente de alimentación.

- Detalles: código de producto RB2011UiAS-RM, arquitectura MIPSBE, CPU AR9344, CPU core count 1, frecuencia nominal de la CPU 600 MHz, nivel de licencia 4, sistema operativo RouterOS, tamaño de memoria RAM 128 MB, tamaño de almacenamiento 128 MB, tipo de almacenamiento NAND, temperatura ambiente probada -40 °C a 60 °C.

Este equipo también permite hasta 250 conexiones simultáneas de carácter virtual, como VPNs PPTP, L2TP, PPPoE, IPIP, las cuales serán útiles si los medios de transmisión como fibra óptica o radiofrecuencia no fueran posibles según el diseño de la intranet.

- Red clientes

Para equipos CPE no es necesario de un equipo robusto para hacer múltiples procesos, ya que, al no utilizar navegación, el ancho de banda a transportarse no será mayor a 1 Mbps y no consume muchos recursos. Dadas sus propiedades, tanto el equipo con mayores prestaciones como el más pequeño, cuentan con las mismas características, por lo que se podrá usar el equipo hAP mini, que cuenta con las siguientes características:

AP tamaño pequeño de 2,4 GHz para el hogar con tres puertos LAN.

El hAP mini es un pequeño punto de acceso inalámbrico de 2 GHz para el hogar o pequeñas oficinas. Tiene tres puertos, que están configurados como un puerto de internet y dos puertos LAN, pero se pueden reconfigurar como se desee, utilizando las poderosas opciones de configuración de RouterOS.

La poderosa CPU de 650 MHz le brinda acceso completo a la amplia variedad de funciones provistas por el versátil sistema operativo RouterOS, pero si lo que desea es un punto de acceso simple, ya está configurado de manera inmediata. Simplemente necesita abrir la página de configuración web y proporcionarle una contraseña.

- Detalles: código de producto RB931-2nD, CPU QCA9533, CPU core count 1, frecuencia nominal de la CPU 650MHz, dimensiones 48x78x81 mm, nivel de licencia 4, sistema operativo RouterOS, tamaño de memoria RAM 32MB, tamaño de almacenamiento 16 MB, tipo de almacenamiento FLASH, temperatura ambiente probada -20 °C a 70 °C

Este equipo, a pesar de no ser muy robusto, cuenta con la mayoría de las funcionalidades que servirán para la integración de los puntos remotos a través de la red intranet o VPNs.

Figura 18. **hAP mini**


Fuente: MikroTik. *hAP mini*. https://mikrotik.com/product/RB931-2nD#fndtn-gallery. Consulta: 11 de diciembre de 2018.

## 4.2. Propuesta de equipos para medios de comunicación

Los equipos, como ya se había mencionado antes, serán de la marca MikroTik, por su costo y funcionalidad.

### 4.2.1. Radiofrecuencia con MikroTik (radio enlaces)

En MikroTik existe un catálogo amplio para la estructuración de redes WISP (*Wireless Internet Service Provider*), los cuales incluyen equipos utilizados como APs (*Access Point*), y también CPEs (*Costumer Premises Equipment*), los cuales recibirán la señal wireless por medio de dos parámetros:

- SSID

Del inglés *Service Set Identifier,* o identificador de paquetes de servicio en castellano, se trata del nombre que identifica una red inalámbrica con respecto a otras. Esto quiere decir que, cuando un paquete es enviado, es acompañado por esta información para saber en todo momento cuál es la red origen. De esta forma, el destino sabe también a que red debe enviar la respuesta, si es necesario. Cuando el dispositivo se conecta a una red inalámbrica, el SSID pasa a ser compartido. O lo que es lo mismo, es una información que no solo la tiene el punto de acceso, también todos los que forman parte de él.

Puede estar formado por un máximo de 32 caracteres ASCII, es decir, letras, números y símbolos, aunque es bastante habitual encontrar los dos primeros tipos de caracteres.

- Perfiles de seguridad

Las contraseñas en redes wireless han ido evolucionando con el tiempo, después de las herramientas y sistemas que funcionan bajo una red doméstica o empresarial, la cual puede verse comprometida si algún usuario no perteneciente quisiera conectarse a ella.

Las contraseñas son introducidas dentro de la comunicación entre el dispositivo AP y cliente, en el que esta le indicará al dispositivo desde donde se está solicitando la conexión y hacia dónde direccionarlo.

Los primeros cifrados fueron conocidos como WEP, los cuales fueron volviéndose comprometidas, a tal punto que no se necesita más de un par de minutos para descifrar la contraseña y comprometer una red. Después de este cifrado, se crearon otros tipos, de los cuales están el WPA y WPA2, los cuales fueron más seguros, ya que utilizan un sistema de claves PSK o claves pre compartidas. La mejoría más importante de WPA2 sobre WPA fue el uso del estándar de cifrado avanzado (AES) para el cifrado. AES es aprobado por el gobierno de EE.UU. para cifrar la información clasificada como de alto secreto, por lo que debe ser lo suficientemente bueno para proteger las redes domésticas.

Los equipos que deben conectarse deberán tener estas propiedades para crear la comunicación a nivel de transporte o capa 2.

A continuación, se presenta el listado de equipos que podrían utilizarse para la implementación de la red por medio de wireless:

mANTBox 15, punto de acceso a la red wireless (AP):

Antena integrada con sector de polarización dual de 5 GHz y 120 grados 15dBi con CPU de 720 MHz, 128 MB de RAM, SFP, PSU y PoE

El mANTBox se basa en las nuevas antenas sectoriales MANT, pero también tienen un enrutador inalámbrico integrado. Con el dispositivo RB921, el mANTBox viene listo para usar con todo lo que está incluido. El dispositivo

utiliza una CPU de alta velocidad de 720 MHz y tiene un dispositivo inalámbrico 802.11 ac / a / n integrado con una potencia de salida de hasta 31 dBm.

- Detalles: código de producto RB921GS-5HPacD-15S, CPU QCA9557, CPU core count 1, frecuencia nominal de la CPU 720 MHz, dimensiones 140x348x82 mm, nivel de licencia 4, sistema operativo RouterOS, tamaño de RAM 128 MB, tamaño de almacenamiento 128 MB, tipo de almacenamiento NAND, temperatura ambiente probada -40 °C a 70 °C.

Esta antena, como bien indican sus especificaciones, cuenta con un nivel de licencia 4, lo cual es importante tener en cuenta, ya que ésta permite utilizar la antena como AP (*Access Point*), lo cual no pueden hacer las antenas CPE a menos de que se eleve la licencia de nivel 3 a 4.

Estas antenas pueden llegar a tener hasta 100 suscriptores, siempre teniendo en cuenta las propiedades que deben tener los radioenlaces, como la línea vista, la zona de Freznell, la distancia, la potencia y el patrón de radiación, los cuales decidirán si la conexión se realizó de forma confiable y estable para la comunicación con los dispositivos dentro de la red.

Figura 19. **mANTBox**

Fuente: MikroTik. *mANTBox*. https://mikrotik.com/product/RB921GS-5HPacD-15S#fndtn-gallery. Consulta: 11 de diciembre de 2018.

Estas antenas tienen que estar en un ambiente donde se pueda tener la mejor cobertura a nivel de visibilidad con los puntos remotos, que en este caso serán los semáforos, tomando en cuenta también la distancia a la que los CPEs estarán.

SXT Lite5 para CPEs de los semáforos en cuestión:

SXT Lite5 es un dispositivo inalámbrico para exteriores de 5 GHz de bajo costo y alta potencia de transmisión. Puede usarse para enlaces punto a punto o como CPE para instalaciones punto a multipunto.

- Detalles: código de producto RBSXT5nDr2, arquitectura MIPSBE, CPU AR9344, CPU core count 1, frecuencia nominal de la CPU 600 MHz, dimensiones 140x140x56mm, nivel de licencia 3, sistema operativo RouterOS, tamaño de memoria RAM 64 MB, tamaño de almacenamiento 128 MB, tipo de almacenamiento NAND, temperatura ambiente probada 40 °C a 70 °C.

Estas antenas cuentan con un nivel de licencia 3, lo cual solo permite realizar la conexión punto a punto siendo utilizadas como receptoras. Si se quisiera crear una conexión punto a punto entre dos antenas de estas, se necesitaría subir una de licenciamiento.

Figura 20. **SXT Lite5**

Fuente: MikroTik. *SXT Lite5*. https://mikrotik.com/product/RBSXT5nDr2#fndtn-gallery. Consulta: 13 de diciembre de 2018.

### 4.2.2. Fibra óptica mediante equipos MikroTik

MikroTik también cuenta con equipos para distribución de fibra óptica, los cuales se hacen a través de equipos que poseen interfaces ópticas conocidas como SFPs, las cuales permitirán conectar transceptores en ellas y lograr velocidades mínimas de 1 Gbps y máximas de 10 Gbps, esto utilizando únicamente la limitante de la interfaz.

Si se deseara aumentar esta velocidad, se podría hacer mediante protocolos como Bonding, lo cual permite utilizar un conjunto de interfaces y a nivel lógico crear una sola interfaz, por ejemplo, si en el Bonding se utilizaran dos interfaces de 10 Gbps, se tendrá un total de 20 Gbps.

A diferencia de las redes wireless con MikroTik, las redes ópticas tienen un impacto económico mucho mayor, ya que el tendido de fibra óptica es costoso, las fusiones y los equipos, pero se tiene la ventaja de que son redes más estables y que no son susceptibles al ruido del ambiente.

Como se mencionó al principio del documento, la jerarquía que deben obedecer las redes ópticas es indispensable para el buen uso de los recursos encomendados, por lo que estos equipos tendrán la función de conectar los enlaces hasta los puntos finales desde un nodo de distribución.

Para estas redes se pueden utilizar los siguientes equipos:

RB2011UiAS-RM para nodo central, el cual cuenta con un puerto óptico, descrito anteriormente para la red core.

CRS212-1G-10S-1S para nodos de distribución.

Smart Switch, 1x Gigabit LAN, 10x SFP jaulas, 1x SFP + jaula, LCD, 400MHz CPU, 64MB RAM, Estuche de metal para escritorio, RouterOS L5

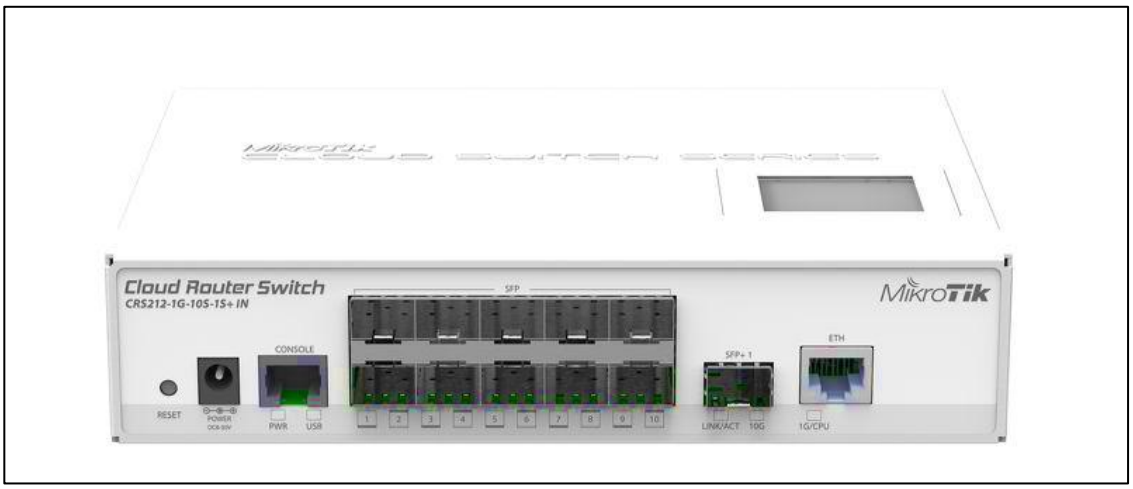
Cloud Router Switch 212-1G-10S-1S + IN es un nuevo miembro de "pequeño tamaño y bajo costo" de la serie CRS. Viene con un puerto Gigabit Ethernet RJ45, diez cajas SFP y una caja 10 G SFP +, así como un panel LCD y un puerto serie (RJ45).

La serie CRS combina las mejores características de un enrutador completamente funcional y un conmutador de capa 3, alimentado por el conocido RouterOS. Todas las opciones específicas de configuración del enrutador están disponibles en un menú especial del conmutador, pero si lo desea, los puertos se pueden eliminar de la configuración del conmutador y usarse con fines de enrutamiento.

- Detalles: código de producto CRS212-1G-10S-1S + IN, arquitectura MIPSBE, CPU QCA8519, CPU core count 1, frecuencia nominal de la CPU 400 MHz, dimensiones 200x144x47 mm, nivel de licencia 5, sistema operativo RouterOS, tamaño de memoria RAM 64 MB, tamaño de almacenamiento 16MB, tipo de almacenamiento FLASH, temperatura ambiente probada -40 °C a 70 °C.

Tomando en cuenta que los puntos a enlazar serán semáforos, los 10 puertos ópticos que este equipo posee serán suficientes si el nodo de distribución se encuentra en un lugar estratégico, tratando de abarcar la mayor cantidad de puntos finales con la menor distancia posible, ya que por temas de costos, esto sería lo más prudente por hacer.

Figura 21. **CRS212-1G-10S-1S+**




Fuente: MikroTik. *Cloud router switch*. https://mikrotik.com/product/CRS212-1G-10S-1SplusIN#fndtn-gallery. Consulta: 13 de diciembre de 2018.

### 4.2.3. Enlaces a través de VPN L2TP con MikroTik

Para estos enlaces únicamente se necesitará el equipo de cada semáforo (hAP mini) y el equipo core (RB2011), y un enlace de internet convencional.

Esta es la forma de comunicación más sencilla de las antes mencionadas, ya que la comunicación se realiza a través de internet con una VPN con L2TP IPsec, creando la configuración del servidor en el equipo core que tendrá una IP pública y la de cada cliente VPN

## 4.3. Diseño de red

Para el diseño de la red se tomarán en cuenta las configuraciones necesarias en los equipos MikroTik, tales como las VLANs asignadas a cada

servicio o semáforo, su direccionamiento IP, las interfaces wireless en el caso de los APs y CPEs, que incluye también la configuración del servidor L2TP y los clientes L2TP. Estas configuraciones se harán con fines educativos, aunque sí pueden ser aplicadas en un ambiente real con las descripciones mencionadas a lo largo del documento.

Configuración del equipo core, tomando en cuenta la utilización del puerto óptico del equipo core y la interfaz a la que la antena AP debería estar conectada.

Las configuraciones se dividirán en bloques.

- Router core:

```
MikroTik RouterOS 6.41.3 (c) 1999-2018       http://www.mikrotik.com/
                                                                    .
[admin@ROUTER_CORE_SEMAFOROS] > export
# jan/02/1970 00:40:09 by RouterOS 6.41.3
# software id = 1UPZ-AV0X
# model = 2011UiAS
# serial number = 60890507D413
```

- Bloque 1, creación de las interfaces virtuales (VLAN) para la identificación de los semáforos remotos:

```
/interface ethernet
set [ find default-name=ether5 ] name=ether5-hacia-antenaAP
set [ find default-name=sfp1 ] name=sfp1-hacia-fibra-optica
/interface vlan
```

add comment=SEMAFORO_1 interface=sfp1-hacia-fibra-optica name=vlan101 vlan-id=101
add comment=SEMAFORO_2 interface=sfp1-hacia-fibra-optica name=vlan102 vlan-id=102
add comment=SEMAFORO_3 interface=sfp1-hacia-fibra-optica name=vlan103 vlan-id=103
add comment=SEMAFORO_4 interface=sfp1-hacia-fibra-optica name=vlan104 vlan-id=104
add comment=SEMAFORO_5 interface=sfp1-hacia-fibra-optica name=vlan105 vlan-id=105
add comment=SEMAFORO_6 interface=ether5-hacia-antenaAP name=vlan106 vlan-id=106
add comment=SEMAFORO_7 interface=ether5-hacia-antenaAP name=vlan107 vlan-id=107
add comment=SEMAFORO_8 interface=ether5-hacia-antenaAP name=vlan108 vlan-id=108

- Bloque 2, creación del servidor L2TP con IPsec para la conexión remota de los clientes:

/interface l2tp-server server
set enabled=yes ipsec-secret=holamundo use-ipsec=yes

- Bloque 3, asignación de las redes WAN a las VLANs respectivas según la asignación mencionada anteriormente:

/ip address
add address=192.168.0.1/30 comment=WAN_SEMAFORO_1 interface=vlan101 network=192.168.0.0

add address=192.168.0.5/30 comment=WAN_SEMAFORO_2 interface=vlan102 network=192.168.0.4

add address=192.168.0.9/30 comment=WAN_SEMAFORO_3 interface=vlan103 network=192.168.0.8

add address=192.168.0.13/30 comment=WAN_SEMAFORO_4 interface=vlan104 network=192.168.0.12

add address=192.168.0.17/30 comment=WAN_SEMAFORO_5 interface=vlan105 network=192.168.0.16

add address=192.168.0.21/30 comment=WAN_SEMAFORO_6 interface=vlan106 network=192.168.0.20

add address=192.168.0.25/30 comment=WAN_SEMAFORO_7 interface=vlan107 network=192.168.0.24

add address=192.168.0.29/30 comment=WAN_SEMAFORO_8 interface=vlan108 network=192.168.0.28

add address=10.1.1.1/24 comment=WAN_VPN_L2TP interface=ether2 network=10.1.1.0

add address=45.5.200.5/30 comment=IP_PUBLICA_FICTICIA interface=ether1 network=45.5.200.4

- Bloque 4, creación de las rutas para conocer las redes LAN de los semáforos, a través de su red WAN:

/ip route

add comment=RUTA_DEFAULT_FICTICIA distance=1 gateway=45.5.200.6

add distance=1 dst-address=172.16.1.0/24 gateway=192.168.0.2

add comment=LAN_SEMAFORO_1 distance=1 dst-address=172.16.1.0/24 gateway=192.168.0.2

add comment=LAN_SEMAFORO_2 distance=1 dst-address=172.16.2.0/24 gateway=192.168.0.6

add comment=LAN_SEMAFORO_3 distance=1 dst-address=172.16.3.0/24 gateway=192.168.0.10

add comment=LAN_SEMAFORO_4 distance=1 dst-address=172.16.4.0/24 gateway=192.168.0.14

add comment=LAN_SEMAFORO_5 distance=1 dst-address=172.16.5.0/24 gateway=192.168.0.18

add comment=LAN_SEMAFORO_6 distance=1 dst-address=172.16.6.0/24 gateway=192.168.0.22

add comment=LAN_SEMAFORO_7 distance=1 dst-address=172.16.7.0/24 gateway=192.168.0.26

add comment=LAN_SEMAFORO_8 distance=1 dst-address=172.16.8.0/24 gateway=192.168.0.30

add comment=LAN_SEMAFORO_9_L2TP distance=1 dst-address=172.16.9.0/24 gateway=10.1.1.19

- Bloque 5, creación del cliente L2TP:

/ppp secret

add local-address=10.1.1.1 name=SEMAFORO_9 password=holamundosemaforo9 remote-address=10.1.1.19 service=l2tp

- Bloque 6, identificación del router core:

/system identity

set name=ROUTER_CORE_SEMAFOROS

[admin@ROUTER_CORE_SEMAFOROS] >

- Router cliente semáforo 1, VLAN:

```
[admin@SEMAFORO_1] > export
# jan/02/1970 00:14:49 by RouterOS 6.41.3
# software id = 1UPZ-AV0X
# model = 2011UiAS
# serial number = 60890507D413
```

- Bloque 1, creación de interfaz virtual:

```
/interface vlan
add comment=SEMAFORO_1 interface=ether1 name=vlan101 vlan-id=101
```

- Bloque 2, asignación de red LAN y WAN:

```
/ip address
add address=192.168.0.2/30 comment=WAN_SEMAFORO_1 interface=vlan101 network=192.168.0.0
add address=172.16.1.1/24 comment=LAN_SEMAFORO_1 interface=ether2 network=172.16.1.0
```

- Bloque 3, asignación de ruta por defecto:

```
/ip route
add comment=RUTA_DEFAULT distance=1 gateway=192.168.0.1
```

- Bloque 4, creación de nombre para dispositivo:

/system identity
set name=SEMAFORO_1

- Router cliente semáforo 9, L2TP:

Este semáforo, por ser un servicio fuera de la intranet, necesita configuraciones preliminares para tener navegación antes de la configuración de la VPN:

[admin@SEMAFORO_9] > export
# jan/02/1970 00:11:27 by RouterOS 6.41.3
# software id = 1UPZ-AV0X
# model = 2011UiAS
# serial number = 60890507D413

- Bloque 1, creación de la interfaz del cliente L2TP:

/interface l2tp-client
add connect-to=45.5.200.5 disabled=no ipsec-secret=holamundo name=SEMAFORO_9_CORE password=holamundosemaforo9 profile=default use-ipsec=yes user=SEMAFORO_9

- Bloque 2, asignación de la dirección LAN:

/ip address
add address=172.16.9.1/24 comment=LAN_SEMAFORO_9 interface=ether2 network=172.16.9.0

- Bloque 3, creación del cliente DHCP para conectarse a internet:

/ip dhcp-client
add dhcp-options=hostname,clientid interface=ether1

- Bloque 4, creación de regla NAT para conectarse a internet:

/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1

- Bloque 5, ruta que conoce la red del router central y los demás routers:

/ip route
add comment="CONOCE LAS RUTAS DE LA CENTRAL Y LOS DEMAS SEMAFOROS" distance=1 dst-address=172.16.0.0/16 gateway=SEMAFORO_9_CORE

- Bloque 6, creación de nombre para dispositivo:

/system identity
set name=SEMAFORO_9

- Antena AP:

# jan/29/2019 19:00:34 by RouterOS 6.42.7
# software id = LFG0-QNJJ
# model = RouterBOARD 952Ui-5ac2nD
# serial number = 7C300751B072

- Bloque 1, creación de interfaz wireless en modo ap-bridge con SSID:

/interface wireless
set [ find default-name=wlan1 ] ssid=MikroTik
set [ find default-name=wlan2 ] band=5ghz-onlyac mode=ap-bridge ssid=ANTENA_AP_SEMAFOROS

- Bloque 2, creación de perfil de seguridad:

/interface wireless security-profiles
set [ find default=yes ] authentication-types=wpa-psk,wpa2-psk eap-methods="" mode=dynamic-keys supplicant-identity=MikroTik wpa-pre-shared-key=holamundo \
wpa2-pre-shared-key=holamundo

- Antena CPE:

# jan/29/2019 19:03:50 by RouterOS 6.42.7
# software id = LFG0-QNJJ
# model = RouterBOARD 952Ui-5ac2nD
# serial number = 7C300751B072

- Bloque 1, creación de interfaz wireless en modo station-bridge con SSID:

/interface wireless
set [ find default-name=wlan1 ] ssid=MikroTik
set [ find default-name=wlan2 ] band=5ghz-onlyac mode=station-bridge

- Bloque 2, creación de perfil de seguridad:

```
/interface wireless security-profiles
set [ find default=yes ] authentication-types=wpa-psk,wpa2-psk eap-methods="" mode=dynamic-keys supplicant-identity=MikroTik wpa-pre-shared-key=holamundo \
    wpa2-pre-shared-key=holamundo
```

### 4.4. Ventajas y desventajas entre los tres tipos de transmisión

- Fibra óptica, ventajas: comunicaciones confiables, baja latencia, bajo costo de mantenimiento (sin incluir fallas), escalable, anchos de banda elevados, no susceptible al ruido del ambiente.

- Fibra óptica, desventajas: alto costo de implementación, infraestructura grande, tiempo de instalación, altos costos en fallas.

- Radioenlaces, ventajas: bajo costo de implementación, tiempo corto de instalación, infraestructura pequeña.

- Radioenlaces, desventajas: susceptible al ruido del ambiente, anchos de banda limitados.

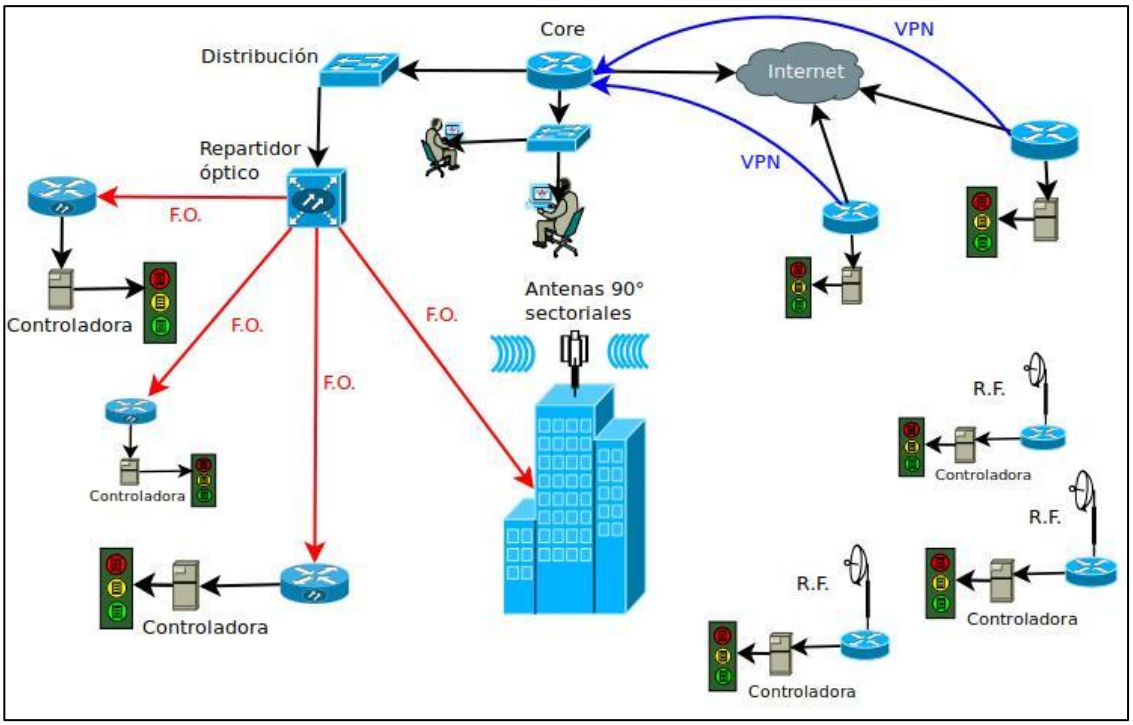
- VPNs, ventajas: comunicaciones únicamente con navegación a Internet, bajo costo de implementación, tiempo corto de instalación.

- VPNs, desventajas: dependen del peering a nivel de BGP con los proveedores adyacentes, conexión a través de internet (implementación de perfiles de seguridad), latencia elevada según estado de navegación.

## 4.5. Diseño de diagramas la intranet

Como se aprecia en la figura 22, todos los medios de transmisión van directamente conectados al *router core*, ya que este maneja todas las políticas de ruteo y acceso para los diferentes puntos.

Figura 22. **Diagrama de sistema de conmutación remoto para semáforos**




Fuente: elaboración propia, empleando LiveWire y PCB Wizard.

# CONCLUSIONES

1. Las comunicaciones dentro de una red interna, gracias a la variedad de protocolos que existen y medios de transmisión, pueden hacerse de tal forma que se acomoden tanto a los recursos como a la experiencia de los usuarios para la implementación de cualquier tipo de proyecto.

2. La creación de una intranet no depende netamente en que su estructura este hecha físicamente, ya que, según su posición geográfica, es difícil que esto pueda darse en su totalidad; sin embargo, gracias a los tipos de conexiones seguras que existen a través de internet, como los son las VPNs, no importa la localización de los puntos remotos.

3. Dentro del marco referente a lo que se conoce como 'el internet de las cosas', se puede concluir que no se necesitan dispositivos muy específicos para su implementación, ya que como se observó en este proyecto, los protocolos de comunicación pertenecen a estándares, los cuales permiten que los dispositivos de hardware y software puedan trabajar en conjunto sin mayores complicaciones.

4. El control de tráfico a través de las vías públicas es una de las preocupaciones más grandes que una sociedad puede tener, por lo que en la actualidad, se han ido creando métodos para que todo funcione de manera óptima, tomando en cuenta la conmutación remota de semáforos a través de centrales de comunicación.

# RECOMENDACIONES

1. Es importante realizar un análisis financiero antes de cualquier implementación en telecomunicaciones, ya que de esto depende el éxito de cualquier proyecto, teniendo en cuenta el referente técnico y profesional del encargado.

2. En telecomunicaciones existen diferentes medios de comunicación para transporte de dato, los cuales, según la experiencia de las personas encargadas de la implementación, pueden tomarlas en cuenta para ahorro recursos.

3. Todas las configuraciones vistas en el documento fueron realizadas con equipos MikroTik, lo que permite la configuración en cualquier plataforma de RouterOS, por lo que no funcionaría en cualquier otro dispositivo que no tenga esas propiedades.

# BIBLIOGRAFÍA


1. BOYLESTAD, R. L.; NASCHELSKY, L. *Electrónica: teoría de circuitos y dispositivos electrónicos*. México: Pearson Educación, 2010. 159 p.

2. ESCALANTE, Mauro. *Conceptos funamentales de MikroTik RouterOS*. México: Pearson Educación, 2010. 180 p.

3. Robótica y Electrónica libre. *Estructuración Ethernet con Arduino. Obtenido de The Teacher G*. [en línea]. <https://create. arduino.cc/editor/ProfeGarcia/130221bd-b506-40a0-96ad-916fa6e9f673/preview>. [Consulta: 17 de diciembre de 2018].

4. TORRENTE ARTERO, Oscar. *Arduino, curso práctico de formación*. España: Mediterráneo, 2015. 182 p.

5. WENDELL, Odom. *Cisco CCENT/CCNA ICND1 100-101 Routing&Switching. Learn, prepare, and practice for exam success*. México: Pearson Education, 2007. 213 p.