



Universidad Nacional de Ingeniería
Facultad de Ingeniería Eléctrica y Electrónica
Proyecto de Fin de Carrera 2022-1

UNIVERSIDAD NACIONAL DE INGENIERÍA FACULTAD DE INGENIERÍA
ELÉCTRICA Y ELECTRÓNICA



PROYECTO DE FIN DE CARRERA

“Diseño de una red LAN para un correcto y moderno acceso a recursos académicos en el Colegio Monserrat, en sus dos sedes”

Asesor:

Troncoso Castro, Paul Fernando

Autores:

- Bustamante Peredo, Joel Josh
- Huillca Ayma, Eder Leon
- Tesen Romero, José Fernando

Lima - Perú

2022



Índice de Contenido

1. DATOS GENERALES DEL PROYECTO	4
1.1. TÍTULO	4
1.2. ABSTRACT	4
1.3. RESUMEN	4
1.4. PRÓLOGO	5
2. INTRODUCCIÓN	6
2.1 PRESENTACIÓN DEL PROBLEMA	6
2.2. PLANTEAMIENTO DE LA SOLUCIÓN	7
2.2.1. Hipótesis General	7
2.2.2. Hipótesis Específicas	7
2.3. OBJETIVOS Y ALCANCES	7
2.3.1. Objetivo General	7
2.3.2. Objetivos Específicos	7
2.3.3. Alcances	8
3. MARCO TEÓRICO	9
3.1. ANTECEDENTES INTERNACIONALES	9
3.2. ANTECEDENTES NACIONALES	10
3.3. MODELO TCP/IP	11
3.4. LAN ETHERNET	15
3.5. INSTALACIÓN DE REDES ALAMBRICAS	17
3.6. RED LAN	18
3.6.1. Componentes de la Red LAN	18
3.6.2. Servicios de una red LAN: Servicios de red	19
3.7. RED DE ÁREA LOCAL INALÁMBRICA (WLAN)	20
3.7.1. Funcionamiento de la Red WLAN	20
3.7.2. Estándares utilizados en una red WLAN	20
3.7.3 Seguridad de la red WLAN	21
3.8. PROTOCOLOS	22
3.8.1. Protocolos de Red	22
3.8.2. Topología de una Red	22
3.9. SWITCH	24



**Universidad Nacional de Ingeniería
Facultad de Ingeniería Eléctrica y Electrónica
Proyecto de Fin de Carrera 2022-1**

3.10. ROUTER	25
3.11. CABLEADO DE COBRE	25
3.11.1. Estándar EIA	25
3.11.2. Categoría de los cables	25
3.11.3. Tipos de Cableado de Cobre	26
3.12. NORMAS Y ESTÁNDARES	27
4. DESCRIPCIÓN DE LA SOLUCIÓN	27
4.1. Calculando Presupuesto de Enlace	27
4.1.1. Características del Router	29
4.1.2. Características del Switch	30
4.1.3. Características del Access Point (AP)	30
4.1.4. PDU	30
4.2. Configurando la Red LAN	31
4.2.1. Simulación de la Red LAN propuesta (Packet Tracer):	34
5. CONCLUSIÓN	37
6. REFERENCIAS BIBLIOGRÁFICAS	37
7. ANEXOS	38



1. DATOS GENERALES DEL PROYECTO

1.1. TÍTULO

“Diseño de una red LAN para un correcto y moderno acceso a recursos académicos en el Colegio Monserrat, en sus dos sedes”

1.2. ABSTRACT

The problem that the Monserrat school has is that it has an inefficient LAN network because not all of its computers have an optimal internet speed or do not have access to it, its structured cabling is in poor condition and in many places is mixed with electrical cables, and its equipment is old.

In this project we proposed a renewal in the design of its LAN network, and their respective equipment, since there are currently other more modern and with better performance and finally we proposed a total change of the structured cabling system.

For the design of this new LAN network we will use some of the following elements as Switch Cisco SG250 of 24 Ports, Switch TP-LINK SG108 of 8 Ports, where they are going to be connected the different equipments that need a connection to internet as the computers and the Access Point Huawei ES318N Wifi N300, on the other hand we also have the Router TP-Link ER605 omada gigabit VPN of 8 ports that will be connected to the different switches to be able to establish an effective communication. Then we will proceed to the correct installation of the equipment in the cabinet and its configuration of these teams, finally we will proceed to make a correct installation of the structured cabling system, using cable organizers in the cabinet, a numbering system to know which equipment is connected to which cable, and use gutters specifically for this and thus avoid crossing with electrical cables.

1.3. RESUMEN

El problema que se presenta el colegio Monserrat es que cuenta con una red LAN ineficiente ya que no todas sus computadoras cuentan con una velocidad óptima de internet o no tiene acceso a esta, su cableado estructurado se encuentra en malas condiciones y en muchos lugares está mezclado con cables eléctricos, así mismo sus equipos son antiguos.

En este proyecto se planteó una renovación en el diseño de su red LAN, y sus respectivos equipos, ya que en la actualidad hay otros más modernos y con mejores prestaciones y por último se planteó un cambio total del sistema de cableado estructurado.

Para el diseño de esta nueva red LAN utilizaremos algunos de los siguientes elementos como Switch Cisco SG250 de 24 Puertos, Switch TP-LINK SG108 de 8 Puertos, donde van a ir



conectados los diferentes equipos que necesitan de una conexión a internet como las computadoras y los Access Point Huawei ES318N Wifi N300, por otra parte, también tenemos el Router TP-Link ER605 omada gigabit VPN de 8 puertos que irá conectado a los diferentes switches para poder establecer una comunicación efectiva. Luego procederemos a la correcta instalación de los equipos en el gabinete y su configuración de estos equipos, por último, se procederá a realizar una correcta instalación del sistema de cableado estructurado, utilizando organizadores de cables en el gabinete, un sistema de numeración para saber a qué equipo está conectado con que cable, y utilizar canaletas específicamente para esto y así evitar su cruce con cables eléctricos.

1.4. PRÓLOGO

Desde los acontecimientos ocurridos desde el año 2020, específicamente hablando de la pandemia ocasionada por el COVID-19, nos hemos dado cuenta que la sociedad se sostiene en gran parte de las tecnologías de información y comunicaciones. Esto a su vez nos demostró que en nuestro país no estábamos preparados al cien por ciento a los cambios a los que nos vimos obligados a afrontar, específicamente hablando de la virtualidad. Teniendo como ejemplos más importantes a los trabajos remotos, también llamados home office o teletrabajo, y a las clases virtuales, tanto en colegios, universidades e instituciones educativas en general; pudimos notar que en ambos casos se realizó de manera parcialmente exitosa, mostrando improvisaciones en algunos casos.

Actualmente, en nuestro país, ya contamos con trabajos presenciales y remotos al mismo tiempo, así como el retorno a las aulas en modalidad totalmente presencial, semi presencial y en algunos casos continúa la modalidad virtual. Esto evidencia que en los campos laboral y académico hay un sistema híbrido entre la presencialidad y virtualidad, lo cual es algo nuevo que se está experimentando en los últimos meses, pues hace un par de años pasamos de la presencialidad a la virtualidad de golpe, mientras que ahora pasamos de la virtualidad a un sistema híbrido entre la presencialidad y virtualidad, que en algunos casos, como en el sector educación, representa un proceso complicado, pues los estudiantes ya se encuentran acostumbrados a la virtualidad. Esto para nosotros, más que representar un problema, representa una oportunidad para un cambio definitivo.

Tomando como punto de partida lo anterior mencionado, nuestra motivación para la realización de este proyecto de fin de carrera, es optimizar la educación en las dos sedes de un centro educativo que aún se encuentran en proceso de adaptación, tanto para docentes como para estudiantes. Por este motivo, nuestra propuesta se basa en el diseño de una red LAN que interconectan las sedes del colegio Monserrat, así, dicho colegio contará con los recursos necesarios para el actual sistema híbrido en el sector educación, y así estén preparados para un eventual acontecimiento que nos obligue a regresar a la virtualidad.



2. INTRODUCCIÓN

Durante estos dos años de pandemia, el sector de la educación se ha visto severamente afectado, dado que los estudiantes y sus respectivos colegios se tuvieron que adaptar a la virtualidad. Si bien se sabe que actualmente ya se está regresando a la presencialidad aún queda la posibilidad de que en algún momento se pueda volver a declarar cuarentena o por algún eventual caso de covid en dichas instituciones educativas se tenga que volver a la virtualidad momentáneamente.

En la actualidad, y desde hace algunos años, una educación sin acceso a las tecnologías de la información y la comunicación no puede ser considerada como tal.

La globalización, así como la actual coyuntura de la pandemia, obliga a que todos formemos parte de la sociedad de la información y la comunicación.

2.1 PRESENTACIÓN DEL PROBLEMA

En este proyecto nos centraremos en el Colegio Monserrat que cuenta con 5 sedes en los distritos de Los Olivos, San Martín de Porres, Carabayllo, Comas y Puente Piedra de las cuales debido a la coyuntura actual solo se encuentran en operación las sedes de los Olivos y San Martín de Porres, donde se tiene que diseñar una red LAN en cada una de estas.

El Colegio Monserrat, cuenta con una Red LAN ineficiente que no soporta las necesidades básicas para el óptimo funcionamiento de los servicios y aplicaciones requeridas por los estudiantes, profesores y personal administrativo.

El colegio no tiene definida la centralización de una red LAN por lo cual se propone la creación de un cuarto técnico donde se instalen los equipos necesarios para el funcionamiento de la red, esto con el fin de facilitar el mantenimiento y la revisión de la red que se está proponiendo.

El colegio, al no contar con los servicios que puede ofrecer una red LAN, como servicios de e-mail, control de acceso, protocolos de seguridad, servicios DHCP, servicios de DNS, servicios de impresión, etc, la información se encuentra en alto riesgo puesto que es vulnerable a contraer ataques informáticos por parte de terceros.

En las salas de cómputo existen numerosos problemas con la conexión a la red de los equipos, debido a que una buena parte presenta fallas técnicas, lo que genera lentitud y constante intermitencia.



2.2. PLANTEAMIENTO DE LA SOLUCIÓN

La Tecnología de redes LAN está en constante evolución, desarrollo, e innovación a nivel mundial y a pesar de que esta es muy importante en varios sectores económicos, sociales y educativos, aún no lo implementan de forma adecuada.

El presente Proyecto de fin de Carrera tiene el propósito de exponer las necesidades de las redes LAN, en las diferentes instituciones educativas, en este caso del Colegio Monserrat, donde no cuenta con una red de alta calidad.

2.2.1. Hipótesis General

El diseño de una red LAN permitiría tener una guía eficiente para poder montar la infraestructura en cualquier ambiente de ambas sedes del colegio Monserrat.

2.2.2. Hipótesis Específicas

- 1) La selección de la tecnología adecuada y diseñada para redes LAN que permitirá la mejor adaptación y configuración de éstas para la aplicación de una institución educativa.
- 2) Establecer una viabilidad económica permitirá realizar el diseño de la red LAN con las tecnologías adecuadas para las necesidades, el entorno y capacidades de una institución educativa.

2.3. OBJETIVOS Y ALCANCES

2.3.1. Objetivo General

- Diseñar una red LAN para el Colegio Monserrat en sus dos sedes en funcionamiento.

2.3.2. Objetivos Específicos

- Determinación de requerimientos para el diseño de la red LAN.
- Realizar el diseño de Red LAN de las 2 sedes del Colegio Monserrat
- Modelar el diseño de red LAN en el simulador Cisco Packet Tracer



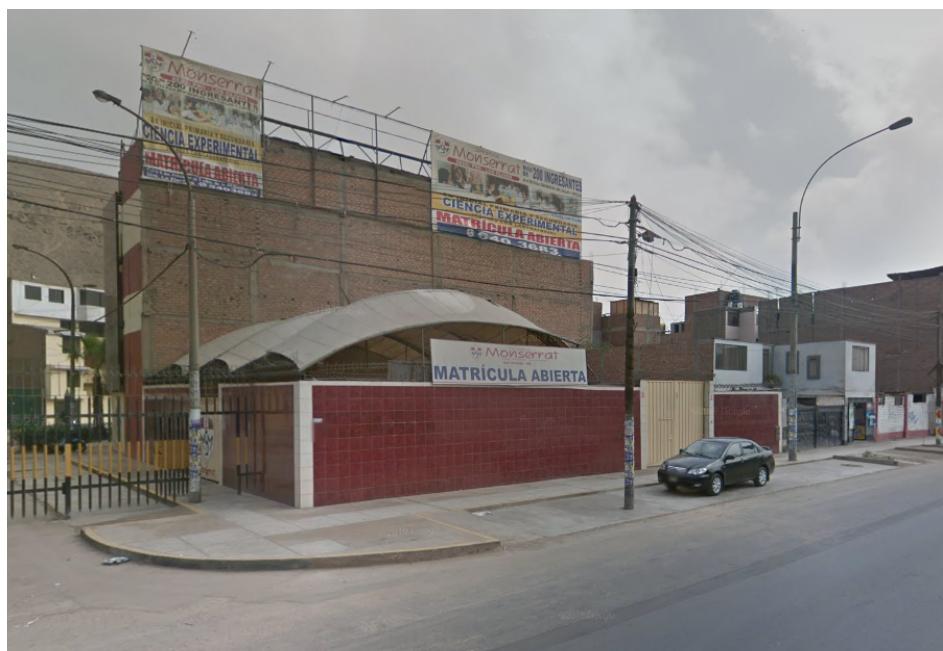
2.3.3. Alcances

Se tuvo planteado como escenarios, a cada uno de los locales de la cadena de colegios Monserrat, sin embargo, actualmente están en funcionamiento dos sedes ubicadas en Lima norte:

- Colegio Monserrat - Sede SMP: Jr. German Stiglich 2052, San Martín de Porres.



- Colegio Monserrat - Sede Los Olivos: Av. Próceres 7610, Los Olivos 15307





3. MARCO TEÓRICO

3.1. ANTECEDENTES INTERNACIONALES

Jairo Jhon, Bernal Gabriel, Angel Camilo (2019) desarrollaron una Tesis sobre, DISEÑO DE UNA RED LAN PARA EL COLEGIO DEPARTAMENTAL INTEGRADO DE MANTA. De la UNIVERSIDAD COOPERATIVA DE COLOMBIA FACULTAD DE INGENIERÍA ELECTRÓNICA SECCIONAL, BOGOTÁ D.C. Colombia.

El propósito principal era diseñar una red LAN, que permita acceder a las diferentes plataformas y servicios que ofrece una red LAN. El proyecto pretende el diseño de un sistema de red flexible, escalable y ampliamente con modificaciones de forma escalonada a lo largo del tiempo según las necesidades futuras del Colegio, dejando la puerta abierta para instalar nuevos sistemas y dar cobertura a futuras tecnologías que trabajan sobre la red local a diseñar. En esta investigación se concluyó que la entidad educativa necesita una red LAN de calidad, en donde, de acuerdo al diseño y estructura realizada, esta red está encaminada a cumplir las normas de instalación, con la mejor opción de diseño, estructuración lógica y física que debe llevar una red LAN.

René Abad, Jorge Barba (2018), desarrollaron un proyecto de fin de carrera sobre, DISEÑO DE LA RED LAN PARA LAS ESCUELAS Y COLEGIOS FISCALES DE LA CABECERA DEL CANTÓN GONZANAMÁ DE LA PROVINCIA DE LOJA. De la Universidad Técnica Particular de Loja de la Escuela de Electrónica y Telecomunicaciones, Loja. Ecuador.

Este proyecto plantea que los educandos y educadores puedan acceder a las herramientas más elementales para su aprendizaje, pensando en una posterior implementación y conexión a Internet mediante el diseño de una red de datos para los colegios y escuelas fiscales de la cabecera del cantón Gonzanamá de la provincia de Loja. En este proyecto, se concluyó que para el diseño de su red LAN, se usó la topología estrella para la distribución interna, mientras que el método de acceso a la red mundial internet fue el método de acceso mediante radioenlaces.

Sarhan AlSarhan (2016), desarrolló una investigación de maestría sobre, COMPUTER NETWORK DESIGN FOR UNIVERSITIES IN DEVELOPING COUNTRIES, De Valparaiso University para Master of Science in Infomation Technology, Indiana State, Estados Unidos de América. El objetivo fue diseñar una red con seguridad de alta calidad y bajo costo, de tal manera que los dispositivos de red de las universidades de los países en desarrollo cumplan con los estándares asociados con las universidades de países desarrollados, con la finalidad de ayudar a mejorar la educación en los países en desarrollo.

Esta investigación discutió en detalle los desafíos presupuestarios que enfrentó la red en el desarrollo de los países. Los países en desarrollo tienen un presupuesto limitado que afecta la elección de dispositivos en la red

como servidores. Los servidores utilizados para este diseño de red son el servidor DHCP y los servidores DNS. Este la presentación y el diseño incluye componentes adicionales como un servidor web, un servidor de correo, etc.



3.2. ANTECEDENTES NACIONALES

Osledi Rotceh Cubas Vega (2020), desarrolló una tesis sobre, DISEÑO DE UNA RED DE COMUNICACIONES PARA DEMOSTRAR LA MEJORA EN LA GESTIÓN EDUCATIVA DE LOS COLEGIOS DEL CEBA “MATIANZA RIMACHI”, De la Universidad Nacional Pedro Ruiz Gallo de la Facultad de Ciencias Físicas y Matemáticas, Lambayeque. Perú.

Esta tesis propone el diseño de una red de comunicaciones para demostrar la mejora de gestión educativa del centro referencial y los periféricos del Centro de Educación Básica Alternativa (CEBA) Matiaza Rimachi perteneciente a la provincia de Utcubamba, del departamento de Amazonas. En este proyecto se concluyó que fue necesario la realización de dos diseños, el primero fue el diseño de los servicios, y el segundo fue el diseño de la red, y ambos diseños permitieron diseñar la red LAN y realizar una correcta elección de equipos basados en en estándares de calidad que proponen las empresas tales como Cisco Systems, que garantizan la mejora de los servicios de telecomunicaciones.

Sullcahuaman Valdiglesias (2018), desarrolló una tesis sobre IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL REDUNDANTE UTILIZANDO LA INFRAESTRUCTURA DE UN PROVEEDOR DE SERVICIOS DE INTERNET - ISP, De la Universidad Nacional de Ingeniería de la Facultad de Ingeniería Eléctrica y Electrónica, Lima. Perú.

En trabajo se basó en la implementación de una Red Privada Virtual Redundante con alta disponibilidad segura, escalable y con gestión de calidad de servicio (QoS) utilizando la infraestructura de un Proveedor de Servicios (ISP), siguiendo los estándares publicados en las RFC- Request for Comments de la IETF (Internet Engineering Task Force). Para lograr los objetivos, se requirió el alquiler de la infraestructura de un Proveedor de Servicios de Internet-ISP con arquitectura MPLS y cobertura a nivel nacional para interconectar todas las sedes u oficinas de la institución educativa. El alcance a nivel de equipamiento y el tipo de acceso de última milla ha sido dimensionado en cumplimiento a los requerimientos técnicos de la entidad educativa. Para este proyecto, se concluyó que la red diseñada a implementar, soportará la transmisión de datos y voz, la convergencia de servicios de comunicaciones y aplicaciones del cliente para las distintas oficinas, garantizando la disponibilidad y calidad de la comunicación.

Llantoy Mayta Christian Shadirt (2020), desarrolló una tesis sobre, DISEÑO DE UNA RED INALÁMBRICA PARA EL ACCESO A RECURSOS EN EL COLEGIO EXCELENTI, De la Universidad Peruana Los Andes.

El presente trabajo debe responder al siguiente problema general: ¿De qué manera influye el diseño de una red inalámbrica en el acceso a recursos en el colegio Excelenti?. Este proyecto se basó principalmente en determinar la influencia del diseño de una red inalámbrica en el acceso a recursos en el colegio Excelenti. En este proyecto se concluyó que, después de haber obtenido resultados satisfactorios, el diseño de red inalámbrica mejora la seguridad informática en el Colegio Excelenti. Por ende, se determina que es viable.

3.3. MODELO TCP/IP

El modelo de referencia de interconexión de Sistemas Abiertos (OSI, Open System Interconexión) este modelo de red fue creado por la Organización Internacional para Estandarización (ISO), en 1984. Trató de establecerse como un estándar, dando solución a la disparidad de protocolos y arquitecturas de red existentes en aquel momento y tratando de hacer posible y de forma sencilla la operatividad de interconexión entre los sistemas de los diferentes proveedores, pero por aquella época se imponía como un estándar el cual no han sido desarrollados por ninguna organización de estandarización debidamente acreditada el modelo TCP/IP, el cual era más sencillo, y compacto el cual contenía un desarrollo de protocolos de transporte, aplicación, etc.

OSI, es un modelo teórico compuesto por 7 capas frente a TCP/IP, un modelo práctico con sólo 4 capas, sencillo y compacto. A continuación, se puede apreciar una comparación de las capas entre los dos modelos

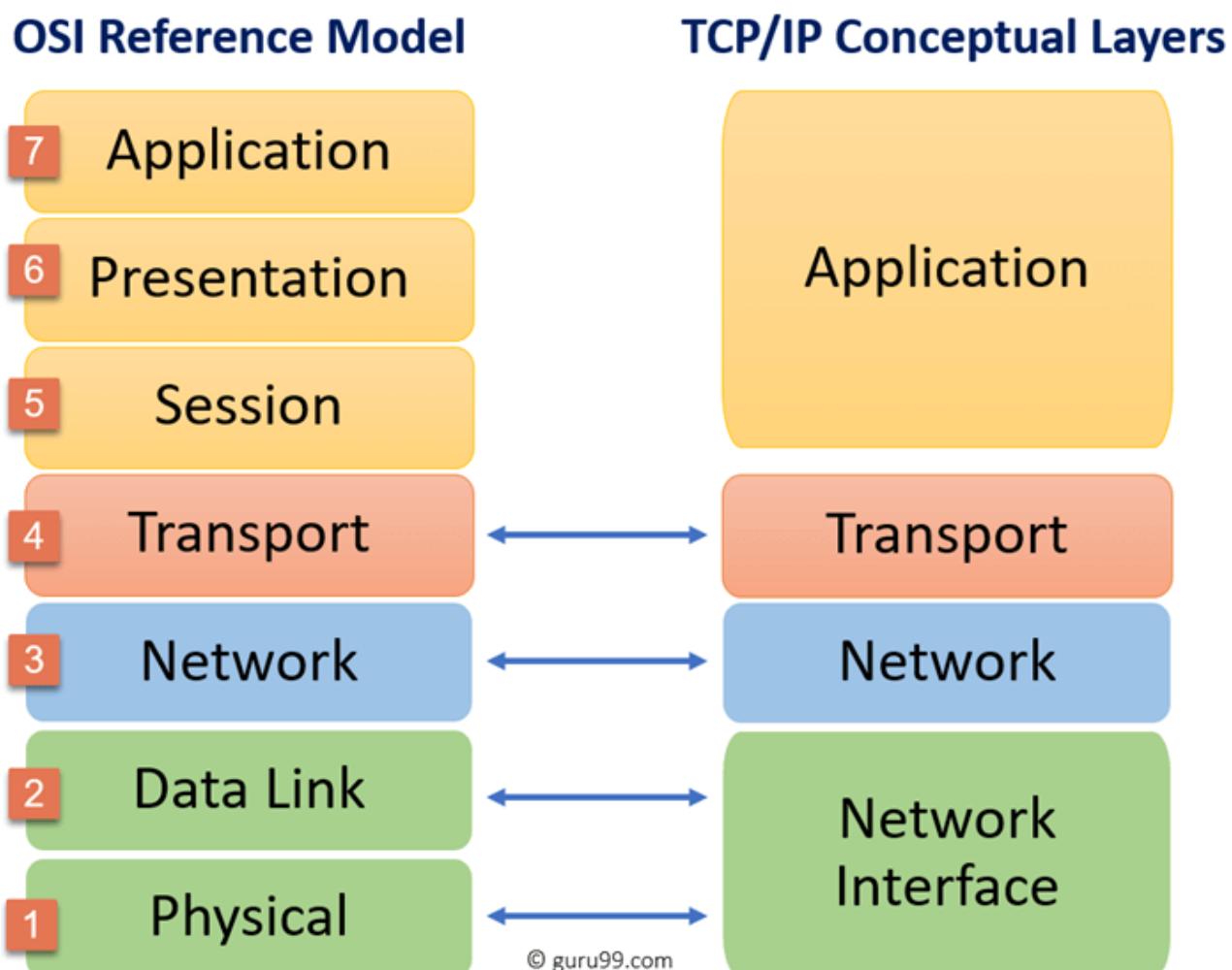


Figura 1. Modelo OSI vs Modelo TCP/IP

Fuente: Recuperado de Jessica. Copyright 2012 Por blogsport.com



El modelo TCP/IP está dividido en 4 capas numeradas en forma ascendente (Ver Figura 1)

Capas 1 (Interfaz de Red): Es la capa de acceso al medio (MAC) y se suele hacer referencia a ella con este nombre, e incorpora las capas 1 (física) y 2 (enlace de datos) del modelo OSI. Esta capa se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, asimismo la distribución ordenada de tramas y del control del flujo, aunque otras capas tienen también su propio control de errores

Capa 2 (Red o Internet): Es la capa de red o internet, incorporada la capa 3 (Red) del modelo OSI. El objetivo de la capa es hacer que los datos lleguen desde el origen al destino, aun firewalls actúan sobre esta capa principalmente, para realizar filtrados por direcciones de máquinas. En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

Capa 3 (Transporte): Es la capa de transporte, incorporada a la capa 4 (Transporte) del modelo OSI. Es la capa encargada de efectuar el transporte de los datos de la máquina origen a la de destino, independizándose del tipo de red física que se está utilizando.

Capa 4 (Aplicación): Capa de aplicación, incorporada a las capas 5 (Sesión), 6 (Presentación) y 7 (Aplicación) del modelo OSI. Ofrece a las aplicaciones posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de base de datos o servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y 22 de 123 puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Aunque hay cierta diferencia en los protocolos a usar en las diferentes capas de la arquitectura, el modelo TCP/IP usa fundamentalmente y de manera características el protocolo IP en la capa de red o internet y los protocolos TCP y UDP en la capa de transporte.

IP: Contiene encapsular las unidades de datos del nivel transporte y es un protocolo no orientado a la conexión. Esto facilita considerablemente la distribución y enrutamiento de la información. Las PDU (Protocol Data Units o Unidades de Datos de Protocolo) de esta capa tienen como nombre datagramas IP

TCP: Contiene encapsulados los datos de la capa de aplicación y es un protocolo orientado a la conexión, lo que significa que antes de la transmisión, ambos extremos deben conectarse entre sí para aceptar el intercambio de información. Esto nos garantiza la entrega de dicha información, así como el orden de llegada de la misma. Al solicitar conexión es un protocolo más lento. Las PDU de este protocolo se llaman segmentos TCP.

UDP: Contiene encapsulados los datos de la capa de aplicación. Es un protocolo no orientado a la conexión, lo cual significa que no existe garantía ni orden en la entrega de los mensajes enviados. Al no requerir conexión ni garantía de entrega, es mucho más rápido y se usa en aplicaciones en las que no es importante la pérdida ocasional de los envíos como el streaming de audio o vídeo, de igual forma consultas al servicio de DNS, etc. Las PDU de este protocolo se llaman datagramas de usuario UDP.



Es evidente que el usuario normalmente no interactúa directamente con la capa de aplicación de TCP/IP. Suele interactuar con aplicaciones de usuario que a su vez interactúan con el nivel de aplicación de TCP/IP, pero ocultando su complejidad.

El funcionamiento esquemático de cualquier protocolo de la capa de aplicación implementado con TCP/IP es muy sencillo. Las capas de la arquitectura funcionan como elementos de una pila, de modo que la información empieza a fluir desde la capa más externa que es (capa aplicación) hasta la capa más interna la cual es (Capa de interfaz de red o capa MAC). Cada capa adicional tiene sus propias cabeceras y encapsula los datos transmitidos desde la capa anterior. En muchos casos, el control de errores o el cifrado se efectúa en capas diferentes. En cada capa el resultado tiene como nombre: paquete, trama, datagrama, segmento, etc. según la capa y el protocolo usado.

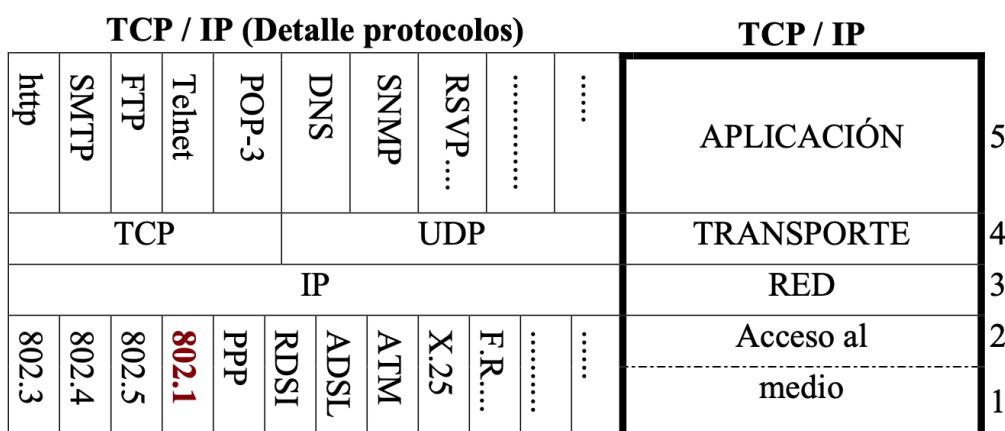


Figura 2. Transición de la información. Protocolos de red.

Fuente: Recuperado de Acorletti. Por darfe.es

Cuando se llega a la capa de más bajo nivel, la información se transmite por el medio y llega al otro extremo, donde esta misma se desordena y se reconstruye la información original pasando por cada capa en orden inverso y aplicando los algoritmos correspondientes de descifrado, corrección y detección de errores, etc. Cada capa ejecuta las tareas complementarias de su mismo nivel. Si en el emisor se incluyó un CRC de control, el receptor lo comprueba, si se cifró la información, se descifra, etc.

Algunos de los protocolos y servicios más conocidos que utilizan la capa de aplicación de TCP/IP son FTP, HTTP, SMTP, POP, etc.

Un esquema de cómo funciona el encapsulado y desencapsulado de la información de aplicación en la torre TCP/IP puede ser el mostrado en la imagen del recorrido de la información TCP/IP. En ella se evidencia claramente como desde arriba hacia abajo se van añadiendo cabeceras y/o colas en cada capa y se respetan los datos que vienen de la capa superior, encapsulándolos en el campo de datos de la capa actual. En el extremo contrario, el proceso sería simétrico e inverso hasta recopilar los datos que forman la información que la aplicación de usuario ha pasado a la capa de aplicación en el emisor. Esta técnica hace que se

puedan entender máquinas con diferentes arquitecturas, sistemas operativos, siempre que respeten el orden y las características del modelo TCP/IP en la programación de los protocolos de comunicación de nivel aplicación.

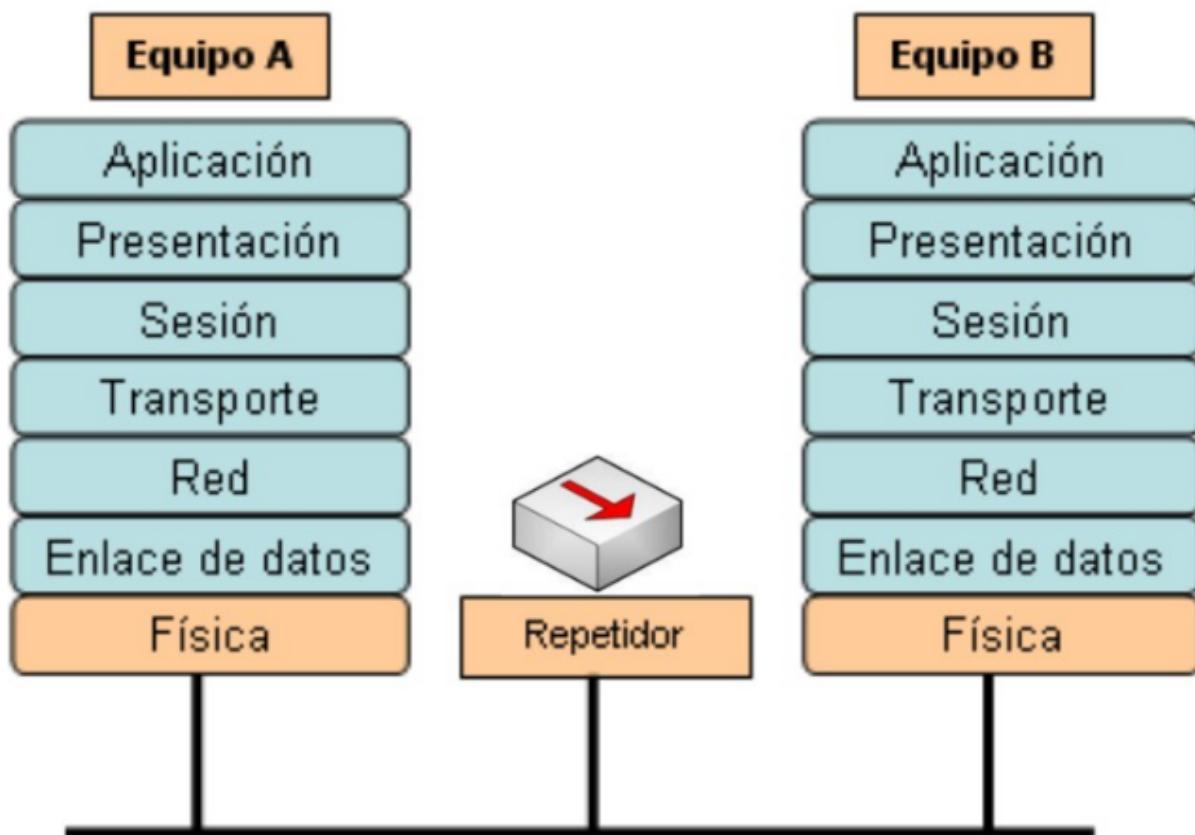


Figura 3. Envío y recepción de datos.

Fuente: Recuperado de Jose Muñoz. Copyright 2017 Por sphinx-doc.org

Un sencillo ejemplo del escenario descrito que se ve a diario en todo el mundo es un navegador Microsoft Internet Explorer corriendo sobre un sistema operativo Microsoft Windows que accede usando el protocolo HTTP o FTP a un servidor Linux para obtener una información. En la imagen del envío y recepción de datos se evalúa una comunicación basada en TCP/IP entre el equipo A (cliente) y el equipo B (servidor). La transmisión pasa a través de un router intermedio que une ambas redes. Este esquema es totalmente escalable, de modo que en una situación normal en la que el cliente y el servidor estén en puntos opuestos del planeta puede haber decenas de saltos entre routers hasta llegar de un extremo al otro.



3.4. LAN ETHERNET

Ethernet es el estándar de facto para redes informáticas de área local con acceso al medio por contienda CSMA/CD. Las diferentes normas IEEE que definen Ethernet incluyen las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos.

Ethernet es anterior en el tiempo y se tomó como base para la redacción del estándar internacional IEEE 802.3. Usualmente se toman Ethernet e IEEE 802.3 como sinónimos. Ambas se diferencian básicamente en uno de los campos de la trama de datos. Las tramas Ethernet e IEEE 802.3 pueden coexistir en la misma red.

Preámbulo	Destino	Origen	Tipo	Datos	Relleno	FCS
8 bytes	6 bytes	6 bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	2 ó 4 bytes

Figura 4. Trama Ethernet

Fuente: recuperado de oocities.org. Copyright 2009 por oocities.org

Preámbulo	SOF	Destino	Origen	Longitud	Datos	Relleno	FCS
7 bytes	1 byte	2 ó 6 bytes	2 ó 6 bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	4 bytes

Figura 5. Trama 802.3.

Fuente: recuperado de oocities.org. Copyright 2009 por oocities.org

Se puede ver respectivamente el formato de la trama Ethernet y el de la 802.3, donde se aprecian las sutiles diferencias entre ambas. Normalmente en las redes locales actuales (LAN) predomina el uso de IEEE 802.3 aunque en el argot suelen ser referidas como redes LAN Ethernet, 27 de 123 pero no está en uso el tipo de trama original descrito en este documento.



La descripción de los campos es la siguiente:

Preámbulo: Un campo de 7 bytes (56 bits) con una secuencia de bits usada para sincronizar y estabilizar el medio físico antes de iniciar la transmisión de datos. El patrón del preámbulo es: 10101010 10101010 10101010 10101010 10101010 10101010 10101010.

Estos bits se transmiten en orden, de izquierda a derecha y en la codificación Manchester representan una forma de onda periódica.

SOF: Inicio de Trama: Campo de 1 byte (8 bits) con un patrón de 1s y 0s alternados y que termina con dos 1s consecutivos. El patrón del SOF es: 10101011. Indica que el siguiente bit será el bit más significativo del campo de dirección MAC de destino. Aunque se detecte una colisión durante la emisión del preámbulo o del SOF, el emisor debe continuar enviando todos los bits de ambos hasta el fin del SOF.

Dirección de destino: Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo IEEE EUI-48 hacia la que se envía la trama. Esta dirección de destino puede ser de una estación, de un grupo multicast o la dirección de broadcast de la red. Cada estación reconoce este campo para determinar si debe aceptar la trama (si es la estación destinataria). La IEEE 802.3 permite que este campo sea de 2 bytes, mientras que en Ethernet sólo puede ser de 6.

Dirección de origen: Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo IEEE EUI-48 desde la que se envía la trama. La estación que deba aceptar la trama conoce por este campo la dirección de 28 de 123 la estación origen con la cual intercambiará datos. La IEEE 802.3 permite que este campo sea de 2 bytes, mientras que en Ethernet sólo puede ser de 6.

Tipo / Longitud: Campo de 2 bytes (16 bits) que en Ethernet identifica el protocolo de red de alto nivel asociado con la trama y en IEEE 802.3 contiene la longitud del campo de datos. La capa de enlace de datos interpreta este campo. En la IEEE 802.3 el campo longitud debe ser menor o igual a 1500 bytes y el campo tipo debe ser mayor o igual a 1536 bytes.

Datos: Campo de 0 a 1500 Bytes de longitud. Cada Byte contiene una secuencia arbitraria de valores. El campo de datos es la información recibida del nivel de red (la carga útil). Este campo, también incluye los H3 y H4 (cabeceras de los niveles 3 y 4), provenientes de niveles superiores.

Relleno: Campo de 0 a 46 bytes que se utiliza cuando la trama Ethernet no alcanza los 64 bytes mínimos para que no se presenten problemas de detección de colisiones cuando la trama es muy corta.

FCS: (Frame Check Sequence / Secuencia de Verificación de Trama): Suele ser un campo de 32 bits (4 bytes) que contiene un valor de verificación CRC. El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor lo recalcula, si el valor calculado es 0 la trama es válida. En Ethernet podría ser de 2 bytes, mientras que en IEEE 802.3 siempre son 4.



Algunas de las diferencias más significativas entre Ethernet e IEEE 802.3 son:

El campo preámbulo de la trama. El propósito del preámbulo es anunciar la trama y permitir a todos los receptores en la red sincronizarse. El preámbulo en Ethernet tiene una longitud de 8 bytes, pero en IEEE 802.3 la longitud del mismo es de 7 bytes, en este último el octavo byte se convierte en el comienzo del delimitador de la trama.

El campo tipo de trama que se encuentra en la trama Ethernet. Un campo tipo es usado para especificar al protocolo que es transportado en la trama.

Esto posibilita que muchos protocolos puedan ser transportados en la trama. El campo tipo fue reemplazado en el estándar IEEE 802.3 por un campo longitud de trama, el cual es utilizado para indicar el número de bytes que se encuentran en el campo de datos.

Los campos de dirección, tanto de destino como de origen. Mientras que el formato de IEEE 802.3 permite el uso tanto de direcciones de 2 como de 6 bytes, el estándar Ethernet permite sólo direcciones de 6 Bytes.

Todas las versiones de Ethernet son similares en que comparten la misma arquitectura de acceso al medio múltiple con detección de errores, CSMA/CD. Sin embargo, el estándar IEEE 802.3 ha evolucionado en el tiempo de forma que ahora soporta múltiples medios en la capa física, incluyendo cable coaxial de 50 _ y 75 _, cable UTP, STP o fibra óptica.

Otras diferencias entre los dos incluyen la velocidad de transmisión, el método de señalamiento y la longitud máxima del cableado, etc.2

3.5. INSTALACIÓN DE REDES ALAMBRICAS

Las redes alámbricas se describen como una disposición que involucra un cableado para establecer enlaces a Internet, con computadores y con otros dispositivos en la red. Los datos se transfieren de un dispositivo a otro mediante cables Ethernet.

Se utiliza el término “alámbrico” para distinguir entre las conexiones que incluyen un cableado y las inalámbricas. A diferencia de los dispositivos inalámbricos que se comunican por aire, una red alámbrica utiliza cables físicos para transportar datos entre los diferentes dispositivos y sistemas informáticos.

Desde que se tiene acceso telefónico, la forma en que los empleados acceden a los datos y aplicaciones ha cambiado drásticamente con el surgimiento de nuevas tecnologías y conexiones a Internet más rápidas. De hecho, las últimas tendencias apuntan a cortar los cables por completo en favor de una mayor movilidad y flexibilidad.

Aunque la movilidad inalámbrica constituye una gran ventaja de acceso a la información, gran cantidad de entes le dan mayor preferencia a la seguridad de las redes inalámbricas.



3.6. RED LAN

Se conoce como red LAN (*Local Área Network*, que traduce Red de Área Local) a una red informática cuyo alcance se limita a un espacio físico reducido, como una casa, un departamento o a lo sumo un edificio.

Desarrollan velocidades de transmisión de 10 y 100 Mbps generalmente para compartir recursos entre varias computadoras y aparatos informáticos (como teléfonos celulares, tablets, etc.), tales como periféricos (impresoras, proyectores, etc.), información almacenada en el servidor (o en las computadoras conectadas) e incluso puntos de acceso a la Internet, a pesar de hallarse en habitaciones o incluso pisos distintos.

Las redes de área local se distinguen de otro tipo de redes por su tamaño, cableado y tecnología de transmisión. Entre los dispositivos que conforman dicha red podemos encontrar servidor, estación de trabajo, Gateway, Tarjeta de red, concentradores de cableado, ordenadores, placa de red, medios de comunicación, etc

3.6.1. Componentes de la Red LAN

- Servidor:

Estos dispositivos suministran a los usuarios conexión a la red, por medio de la cual los usuarios comparten, crean y obtienen información. Tienen una conexión física con los medios de red ya que tienen una tarjeta de interfaz de red (NIC). "Server" o servidor, también llamado "Host" o anfitrión; es una computadora especializada con muy altas capacidades de proceso.

- Estación de trabajo:

Pc's conectadas a la red aprovechan o tienen a su disposición los recursos que ofrece la red, así como los servicios que proporcionan los Servidores a los cuales pueden acceder podemos acceder a los recursos compartidos en dicha red como discos, impresoras, módems, etc. Pueden carecer de la mayoría de los periféricos, pero siempre tendrán un NIC, un monitor, un teclado y un CPU.

- Gateways:

También llamadas pasarelas es un hardware y software que permite las comunicaciones entre la red local y grandes ordenadores (mainframes)

- Bridges o puentes:

Permite que se conecten dos redes locales entre sí. Un puente interno es el que se instala en un servidor de la red, y un puente externo es el que se hace sobre una estación de trabajo de la misma red. Los puentes también pueden ser locales o remotos. Los puentes locales son los que conectan a redes de un mismo edificio, usando tanto conexiones internas como externas. Los puentes remotos conectan redes distintas entre sí, llevando a cabo la conexión a través de redes públicas, como la red telefónica, RDSI o red de conmutación de paquetes



- Tarjeta de red:

Básicamente realiza la función de intermediario entre el ordenador y la red de comunicación.

- Concentradores de cableado:

Las redes de área local usan concentradores de cableado para realizar las conexiones de las estaciones, en vez de distribuir las conexiones el concentrador las centraliza en un único dispositivo manteniendo indicadores luminosos de su estado e impidiendo que una de ellas pueda hacer fallar toda la red. Existen dos tipos de concentradores de cableado: 1. Concentradores pasivos: actúan como un simple concentrador cuya función principal consiste en interconectar toda la red. 2. Concentradores activos: además de su función básica de concentrador también amplifican y regeneran las señales recibidas antes de ser enviadas. Los concentradores de cableado tienen dos tipos de conexiones: para las estaciones y para unirse a otros concentradores y así aumentar el tamaño de la red.

- Soporte Físico de Interconexión

Es el soporte (generalmente cableado, es decir que es un cable) utilizado para conectar los equipos entre sí. Los principales medios de soporte físicos utilizados son: el cable coaxial, el par trenzado y la fibra óptica. Son dispositivos que permiten a los puestos de trabajo conectarse al sistema de cableado para crear el nivel físico. Sus principales funciones son: Almacenamiento temporal de información hasta que el canal de transmisión se libere. Filtrado de la información circulante por la red, aceptando sólo la propia. Conversión de la información de la red en serie de bits, a información del puesto de trabajo en octetos.

3.6.2. Servicios de una red LAN: Servicios de red

- "File Services" Un usuario de la red puede buscar información y tener acceso a través de los recursos de la red. Usando este servicio un miembro de la institución puede conservar o publicar información a través de la red.
- "Mail Services" El usuario envía y recibe correspondencia electrónica. El correo electrónico facilita la comunicación entre miembros del ambiente de computadoras. Usando correo electrónico, un especialista puede establecer una conversación con un estudiante, usuario, científico, etc. y enviar archivos a otros departamentos y distribuir información.
- "Terminal Emulation Services" Permite acceso a diferentes tipos de estaciones de trabajo con diferentes sistemas operativos.
- "Communication Services" Permite que el usuario desde una estación remota pueda comunicarse vía MODEM, RAS, etc. y que tenga acceso a los servicios de la red. Este servicio permite a un usuario desde su casa hacer transacciones en línea y/o realizar consultas de interés.



3.7. RED DE ÁREA LOCAL INALÁMBRICA (WLAN)

En WLAN utilizamos el aire como medio de transmisión, es decir, hacemos uso de la tecnología Wi-Fi normalmente. En cuanto a los diferentes estándares que podremos utilizar en nuestros routers, actualmente hacemos uso de los estándares Wi-Fi 4, Wi-Fi 5, y si tu router es de última generación, es posible que utilice el nuevo estándar Wi-Fi 6. Dependiendo del equipo que tengamos, este podrá tener WLAN en una sola banda de frecuencias (normalmente 2.4GHz), podremos tener doble banda simultánea (2.4GHz y 5Ghz) e incluso podremos tener equipos con triple banda simultánea (2.4GHz, 5GHz con canales «bajos» y 5GHz con canales «altos»)

3.7.1. Funcionamiento de la Red WLAN

El funcionamiento de una red de área local inalámbrica consiste en transmitir información o datos de un punto a otro a través de ondas electromagnéticas, ya sea ondas de radio u ondas de luz mejor conocida como luz infrarroja, este medio permite la movilidad de los dispositivos y la facilidad de instalación de la red. Para que la red pueda utilizar las ondas de radio o la luz infrarroja, los dispositivos tienen que estar adaptados a cualquiera de estos medios de transmisión. También es importante establecer cuál norma de la 802.11 de la IEEE se va a utilizar. La comunicación de los equipos inalámbricos es sencilla, ya sea por medio de ondas de radio la cual utiliza una banda de frecuencia desde 3KHz a 300GHz, en donde son captadas por antenas que poseen los dispositivos, o utilizando luz infrarroja la cual viaja en forma de rayos

3.7.2. Estándares utilizados en una red WLAN

El estándar original es el 802.11, éste ha ido evolucionando y ahora las posibilidades de alcance y velocidad son varias. Siempre hablando de Wifi algunas variantes son estas:

- IEEE 802.11b y IEEE 802.11g, ambos disponen de una banda de 2.4 GHz el primero alcanza una velocidad de 11Mbps y el segundo de 54 Mbps. Son de los estándares más extendidos lo que les brinda una gran aceptación internacional.
- IEEE 802.11a, más conocido como Wifi5 porque su banda es de 5 GHz, al tener mayor frecuencia que el estándar anterior dispone también de menor alcance, aproximadamente un 10% menos. Por otro lado, al ser un sistema bastante nuevo todavía no hay otras tecnologías que lo usen, así que la conexión a Internet desde el ordenador es muy limpia y sin interferencias.
- IEEE 802.11n, éste trabaja también a 2.4 GHz pero la velocidad es mucho mayor que la de sus predecesores, 108Mbps.



3.7.3 Seguridad de la red WLAN

Las especificaciones para la comunicación en redes inalámbricas son definidas por la norma IEEE 802.11 del Institute of Electrical and Electronics Engineers (IEEE), cerca de Nueva York. Sin embargo, a la hora de definir los estándares WLAN, no se prestó mucha atención a la seguridad. En sus inicios, la transmisión de datos se realizaba sin cifrar y sin necesidad de una autenticación de usuario, permitiendo que todo el que se encontrara dentro de su alcance tuviera libre acceso a la red inalámbrica. En última instancia, la demanda de medidas de seguridad WLAN favoreció el desarrollo de los siguientes métodos de cifrado y autenticación:

- **Wired Equivalent Privacy (WEP):** creado en 1997, WEP es el estándar de cifrado inalámbrico más antiguo. Dispone de dos métodos de autenticación: Open System Authentication (todos los clientes están habilitados) y Shared Key Authentication (activación a través de la contraseña). Adicionalmente, WEP contiene el método de cifrado RC4. Debido a algunos puntos débiles, WEP es considerado como inseguro y obsoleto.
- **Wi-Fi Protected Access (WPA):** WAP se basa en la arquitectura WEP y fue diseñado para erradicar las debilidades de este último. Para lograrlo, WPA utiliza una clave dinámica basada en el Temporal Key Integrity Protocol (TKIP). Debido a que WPA tiene ciertas deficiencias de seguridad, no está permitido que nuevos puntos de acceso inalámbrico (desde 2011) y todos los dispositivos WLAN (desde 2012) lo utilicen.
- **Wi-Fi Protected Access 2 (WPA2):** en 2004, aparece el estándar IEEE 802.11i junto con el método de cifrado y autenticación actual más seguro: WPA2. En vez de utilizar TKIP, WPA2 utiliza el moderno método de cifrado AES. Como consecuencia, al configurar un WLAN siempre deberás considerar WPA2 antes que WEP y WPA.
- **Wi-Fi Protected Setup (WPS):** el estándar WPS no es una técnica de transmisión o cifrado, sino un mecanismo de gestión que tiene como objetivo facilitar la configuración de nuevos participantes en la red inalámbrica. La autenticación se realiza pulsando un botón (WPS-PBC), es decir, físicamente desde el punto de acceso o virtualmente a través de un botón implementado en el software, o ingresando un PIN (WPS-PIN). Alternativamente existe la oportunidad de compartir la configuración de red en una memoria USB o por medio de la tecnología NFC (Tecnología de radio de corto alcance).

Aunque WPA2 representa un legítimo y seguro sucesor para WEP y WPA, algunos operadores siguen utilizando estos obsoletos estándares para cifrar sus redes inalámbricas, siempre y cuando sean compatibles con el punto de acceso. Es irrelevante si se hace sin intención o por razones de compatibilidad (para garantizar el acceso de los dispositivos más antiguos), pero lo que está claro es que con estos modos las redes están expuestas a un riesgo de accesos no autorizados mucho mayor. Esta negligencia es una de las principales razones de las críticas a la seguridad de las redes inalámbricas. Otros errores que llaman la atención de los atacantes y que, por lo tanto, tienen consecuencias fatales para las redes inalámbricas son, entre otros:

- Introducir los nombres de usuario y contraseñas estándar en Wireless Access Points
- Aceptar configuraciones básicas inseguras en Wireless Access Points



- Una implementación errónea de WPA2 y WPS

Además, aun con la ayuda de las medidas estándar de seguridad WLAN mencionadas anteriormente, toda red inalámbrica es vulnerable a ataques DoS y DDoS y a los llamados ataques Evil Twin (gemelo malvado). En este último, con un firmware especial, los atacantes se infiltraron en la red creando un Wireless Access Point falso para mantener el contacto con los participantes de la red. El gemelo malvado reacciona creando una solicitud de autenticación falsa para recibir los datos de acceso al dispositivo de red conectado al WLAN. Adicionalmente, este asume la dirección MAC del cliente (MAC Spoofing) y de esta forma tiene todos los datos que necesita para establecer la conexión. Especialmente las redes LAN de acceso público suelen estar bajo la amenaza de este tipo de ataques.

3.8. PROTOCOLOS

3.8.1. Protocolos de Red

Un protocolo de red contiene una serie de reglas o acuerdos para permitir la transferencia de datos entre dos equipos a través de la red, como las condiciones de intercambio, el enrutamiento, o el control de fallos, entre otras. Los protocolos de la capa de red actúan en la capa de nivel 3 del modelo de OSI y permiten que dos o más computadoras puedan comunicarse entre sí.

Para que dos dispositivos se comuniquen entre sí deben utilizar el mismo protocolo de red, ya que así acuerdan las condiciones de transmisión (tamaño de los paquetes, tipo de paquetes, emisor y destinatario, y si se utilizan otros protocolos).

Podemos entender los protocolos de red como un conjunto de reglas que se encargan de gestionar y controlar las comunicaciones entre todos los dispositivos que se conectan a una red.

3.8.2. Topología de una Red

- Punto a Punto

Los enlaces punto a punto le permiten interconectar 2 redes remotas como si fueran una misma, mediante un canal de comunicación inalámbrico. Dichos enlaces son viables desde 500 mts o menos hasta una distancia máxima aproximada de 80 Km. Estos enlaces podrían tener los siguientes usos:

Comunicación de red, internet, video y telefonía IP para una empresa, sucursal, casa de campo, rancho o facilidad ubicada en áreas remotas donde los servicios de Internet no llegan.



- Interconexión de las redes de 2 ubicaciones o extensión de la red de 1 ubicación a otra, permitiendo intercambio de archivos, impresión en red, internet compartido, servicios de red, aplicaciones, intranet, etc.
- Interconexión de las redes de 2 ubicaciones para enlazar servicios de voz mediante VOIP, permitiendo comunicación de extensiones, líneas telefónicas compartidas y enlace a líneas virtuales.
- Interconexión de las redes de 2 ubicaciones para compartir servicios de video vigilancia y monitoreo de espacios a distancia.

- Punto a multipunto

Cuando se habla de una red inalámbrica punto a multipunto, se refiere a una comunicación que existe entre un único equipo central que cumple la función de transmisor con diferentes equipos receptores comunicándose en conjunto hacia él, teniendo así una conexión centralizada en un nodo específico hacia diferentes lugares. Estas redes punto a multipunto se encuentran conformados ya sea por una antena omnidireccional o varias antenas sectoriales que cumplen la función de equipo transmisor y varios dispositivos suscriptores o antenas direccionales que se encargan de la resección de la señal transmitida para que así los abonados tengan conexión al nodo principal y por ende salida a la red global como es internet.

Para poder elaborar una red inalámbrica punto multipunto es necesario el análisis del área que se desea cubrir, lo cual va depender directamente de la distribución de las familias en dicha población, así como de la ubicación de la estación base o punto de acceso que será donde se conecten de forma inalámbrica todos los clientes, esto tomando en consideración que para que los abonados se puedan conectar a la estación base es necesario que exista línea de vista entre ellos.

- Mallada

También es denominado MESH (malla). En una red multipunto a multipunto, no hay una autoridad central. Cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos los nodos se comunican directamente entre sí.

El beneficio de este diseño de red es que aun si ninguno de los nodos es alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí. Las buenas implementaciones de redes MESH son autorreparables, detectan automáticamente problemas de enrutamiento y los corrigen. Extender una red MESH es tan sencillo como agregar más nodos. Si uno de los nodos en la “nube” tiene acceso a internet, esa conexión puede ser compartida por todos los clientes.

Dos grandes desventajas de esta topología son el aumento de la complejidad y la disminución del rendimiento. La seguridad de esta red también es un tema importante, ya que todos los participantes pueden potencialmente transportar el tráfico de los demás. La resolución de todos los problemas de las redes multipunto a multipunto tiende a ser



complicada, debido al gran número de variables que cambian al moverse los nodos. Las redes multipunto a multipunto generalmente tienen la misma capacidad que las redes punto a punto, o las redes punto a multipunto, debido a la sobrecarga adicional de administrar el enrutamiento de la red y el uso más intensivo del espectro de radio.

Sin embargo, las redes MESH son útiles en muchas circunstancias, en desastres, en una implementación rápida y barata para una pymes, para una red comunitaria, para una biblioteca o parque, para un colegio o inclusive, para un campus universitario.

- **Anillo**

Es un tipo de topología de red simple, en donde las estaciones de trabajo o computadoras, se encuentran conectadas entre sí en forma de un anillo. La información viaja en un solo sentido, por lo tanto, que si un nodo deja de funcionar se ace la red o deja de abastecer información a las demás computadoras que se encuentran dentro del anillo

- **Árbol**

Este tipo de topología de red es una de las más sencillas. Como su nombre lo indica, las conexiones entre los nodos (terminales o computadoras) están dispuestas en forma de árbol, con una punta y una base. Si un nodo falla, no se presentan problemas entre los nodos subsiguientes. Cuenta con un cable principal llamado Backbone, que lleva la comunicación a todos los nodos de la red, compartiendo un mismo canal de comunicación.

- **Estrella**

Acá la distribución de la información va desde un punto central o Host, hacia todos los destinos o nodos de la red. En la actualidad, es muy utilizada por su eficiencia y simpleza. Se puede notar que el Host realiza todo el trabajo (una especie de servidor local que administra los servicios compartidos y la información). Por supuesto, cuenta con la ventaja que, si un nodo falla, la red continuará trabajando sin inconveniente, aunque depende del funcionamiento del Host.

- **Híbrida**

Como su nombre lo indica, es una combinación de dos o más topologías de red diferentes, para adaptar la red a las necesidades del cliente. De este modo, podemos combinar las topologías que deseemos, obteniendo infinitas variedades, las cuales, deben ajustarse a la estructura física del lugar en donde estará la red y los equipos que estarán conectados en dicha red.

3.9. SWITCH

Un switch de red o conmutador es un dispositivo de interconexión que sirve para conectar todos los equipos en una red; incluidos los computadores, las consolas, las impresoras y los servidores. Junto con el cableado forman lo que se conoce como red de área local (LAN).

Este dispositivo por sí solo no brinda conectividad con otras redes ni tampoco internet; para eso es necesario un router.

La función básica del switch de red es conectar dispositivos. Gracias a ello, los equipos conectados pueden:



- Compartir archivos. Cualquier equipo que forme parte de la red puede activar la función de compartir archivos. De esta forma, el resto de los dispositivos podrán acceder a la información.
- Compartir impresoras. Todos los dispositivos pueden utilizar la misma impresora.
- Compartir la conexión a Internet. Todos los equipos pueden acceder a Internet por medio de un router que está conectado al switch de red.

Se dice que los primeros switches de red surgieron en la década de los años 80. Con el avance de los grandes centros de cómputos, apareció el problema de tener cientos de computadores, teclados y ratones que ocupaban mucho espacio. De hecho, uno de los problemas de los técnicos era tener que desplazarse de un servidor a otro para hacer sus trabajos.

Con el switch solo tienen que ingresar en un computador y ver desde allí la información de los otros.

3.10. ROUTER

Los routers o encaminadores, son dispositivos hardware para interconexión de redes de ordenadores ya que permiten asegurar el enrutamiento de paquetes entre diferentes redes o determinar la ruta que debe tomar un determinado paquete de datos en función de la dirección destino. Operan en la capa de red o internet de TCP/IP.

Los routers guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web.

Los paquetes de datos tienen varias capas o secciones; una de ellas transporta la información de identificación, como emisor, tipo de datos, tamaño y, aún más importante, la dirección IP (protocolo de Internet) de destino. El router lee esta capa, prioriza los datos y elige la mejor ruta para cada transmisión.

3.11. CABLEADO DE COBRE

3.11.1. Estándar EIA

La norma EIA es un estándar de un sistema de cableado estructurado, es decir, una normativa que trata definir la manera de diseñar, construir y administrar cableado estructurado.

3.11.2. Categoría de los cables

En el estándar EIA-568-A se consideran varios tipos o categorías de cables UTP

- Cat 5: Es muy frecuente en redes ethernet, fast ethernet (100 Mbit/s). Diseñado para transmisión a frecuencias de hasta 100 MHz



- Cat 5e: Se encuentra en redes fast ethernet (100Mbit/s) y gigabit ethernet (1000 Mbit/s). Diseñado habitualmente para transmisión a frecuencias de 100 MHz, pero puede superarlos
- Cat 6: Actualmente definido en la TIA/EIA 568-B. Usado en redes gigabit ethernet (1000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 250 MHz
- Cat 6e: Definido en TIA/EIA 568-B. Usado en redes 10 gigabit ethernet (10000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 500 MHz
- Cat 7: Caracterización para cable de 600 MHz según la norma internacional ISO-1180. Se usa en redes 10 gigabit ethernet y comunicaciones de alta confiabilidad
- Cat 7A: Caracterización para cable de 1000 MHz según la norma internacional ISO 1180 ad-1 de 2008. Se emplea en redes 10 gigabit ethernet y futuras comunicaciones de mayor velocidad de transmisión de datos
- Cat 8: Ofrece un ancho de banda de hasta 2 GHz y velocidad de hasta 25 Gb y 40Gb. Tiene hasta 30 m de longitud.

3.11.3. Tipos de Cableado de Cobre

- Par trenzado no blindado (UTP): Es el medio de red más común, consta de 4 pares de hilos codificados por colores que están trenzados entre sí y recubiertos con revestimiento de plástico que los protege contra daños físicos menores. El trenzado de los hilos ayuda a proteger contra las interferencias de señales de otros hilos
- Par trenzado blindado (STP): Combina técnicas de blindaje para contrarrestar las Interferencias electromagnéticas (EMI) y la RFI, y el trenzado de hilos para contrarrestar el crosstalk, que se trata de una perturbación causada por los campos eléctricos o magnéticos de una señal de un hilo a la señal de un hilo adyacente, además cuenta con una malla para su conexión a tierra
- Par trenzado apantallado (FTP): En este caso tenemos un cable cuyos pares trenzados están separados entre ellos por un sistema básico basado en plástico o material no conductor. En este caso el apantallamiento no es individual, sino global que envuelve a todo el grupo de pares trenzados
- Pares trenzado Laminados blindado individual (SSTP): Ahora tenemos un cable con la estructura propia de un cable STP, pero a su vez encontramos un forro global alrededor de material LSZH
- Par trenzado apantallado individual (SFTP): Este cable se basa en la construcción del cable FTP, pero con el apantallamiento global se ha añadido una malla metálica LSZH



3.12. NORMAS Y ESTÁNDARES

Las principales normas y estándares relacionados con el cableado estructurado y la instalación de redes de datos y telecomunicaciones en la actualidad son los siguientes:

- ANSI/EIA/TIA-568: Estándar de cableado para telecomunicaciones en edificios comerciales. Establece los requisitos de los elementos de la red y los medios empleados para la transmisión. Es una norma definida para los EE. UU. pero, en la práctica, se ha asumido a nivel mundial.
- ANSI/TIA/EIA-569: Estándar para espacios y canalizaciones de telecomunicaciones en edificios comerciales. Define la metodología de diseño y construcción en los edificios, y entre estos, para poder integrar en ellos una red de datos y telecomunicaciones.
- ANSI/TIA/EIA-570: Estándar de cableado para telecomunicaciones en edificios residenciales y de pequeños comercios.
- ANSI/TIA/EIA-606: Estándar de administración de la infraestructura de telecomunicaciones en edificios comerciales. Establece el estándar de rotulación del cableado, así como el registro y mantenimiento de la documentación de la red.
- J-STD-607: Estándar de requisitos de conexión a tierra y conexión de telecomunicaciones en edificios comerciales. Especifica las características de la red de conexión a tierra, así como los sistemas empleados.
- ANSI/TIA/EIA-942: Estándar de infraestructura de telecomunicaciones para centros de datos. Define las características de un centro de datos como un edificio o una parte del edificio dedicados a alojar salas de telecomunicaciones y de equipos de gran envergadura.

4. DESCRIPCIÓN DE LA SOLUCIÓN

4.1. Calculando Presupuesto de Enlace

Se realizó un estudio al Colegio Monserrat de los recursos necesarios para el proyecto propuesto. Fundamentalmente incluye el costo de los dispositivos, instalación y configuración.

Se plantea una opción óptima, en la cual detallamos todos los componentes necesarios para que el proyecto propuesto cubra las necesidades y objetivos planteados.

De acuerdo a los requerimientos, se presenta el detalle de los elementos que se necesitan y el costo de los mismos para el desarrollo del proyecto de ambas sedes del colegio.



**Universidad Nacional de Ingeniería
Facultad de Ingeniería Eléctrica y Electrónica
Proyecto de Fin de Carrera 2022-1**

- Colegio Monserrat - Sede SMP: Jr. German Stiglich 2052, San Martín de Porres.

Producto	UNID	VALOR UNIT	VR. TOTAL
RACK GABINETE DE PISO 48RU - RITAL	1	\$ 685.00	\$ 685.00
KIT VENTILACIÓN SUPERIOR PARA RACK	1	\$ 270.00	\$ 270.00
SWITCH CISCO SG250 24 PUERTOS	2	\$ 329.00	\$ 658.00
SWITCH TP-LINK SG108 8 PUERTOS	2	\$ 34.00	\$ 68.00
ROUTER TP-LINK ER605 OMADA GIGABIT VPN	1	\$ 73.00	\$ 73.00
ORDENADOR DE CABLES HORIZONTAL - N102.127BK -NEXANS	2	\$ 60.00	\$ 120.00
CABLE RED UTP CAT 6 60/40 305 MTS	2	\$ 162.00	\$ 324.00
CONECTORES RJ45 - 50 UND	2	\$ 12.00	\$ 24.00
AP HUAWEI ES318N WIFI N300	4	\$ 17.00	\$ 68.00
PDU REGLETA ELECTRICA 8 TOMAS	1	\$ 70.00	\$ 70.00
TOTAL			\$ 2,360.00

Tabla 1. Presupuesto para la Red LAN en La sede San Martín de Porres.

AREA	CANTIDAD DE EQUIPOS	UBICACIÓN
Sala de Computo	31 Pc's	Tercer Piso
Sala de Computo	3 Switches	Tercer Piso
Sala de Computo	1 Router	Tercer Piso
Secretaria	1 Switch	Primer Piso
Secretaria	2 Pc's	Primer Piso
Secretaria	1 AP	Primer Piso
Pasadizo	1 AP	Segundo Piso
Pasadizo	1 AP	Tercer Piso
Pasadizo	1 AP	Cuarto Piso

Tabla 2. Cantidad de equipos a instalar en la sede SMP.



- Colegio Monserrat - Sede Los Olivos: Av. Próceres 7610, Los Olivos 15307

Producto	UNID	VALOR UNIT	VR. TOTAL
RACK GABINETE DE PISO 48RU - RITAL	1	\$ 685.00	\$ 685.00
KIT VENTILACIÓN SUPERIOR PARA RACK	1	\$ 270.00	\$ 270.00
SWITCH CISCO SG250 24 PUERTOS	1	\$ 329.00	\$ 329.00
SWITCH TP-LINK SG108 8 PUERTOS	2	\$ 34.00	\$ 68.00
ROUTER TP-LINK ER605 OMADA GIGABIT VPN	1	\$ 73.00	\$ 73.00
ORDENADOR DE CABLES HORIZONTAL - N102.127BK -NEXANS	2	\$ 60.00	\$ 120.00
CABLE RED UTP CAT 6 60/40 305 MTS	1	\$ 162.00	\$ 162.00
CONECTORES RJ45 - 50 UND	1	\$ 12.00	\$ 12.00
AP HUAWEI ES318N WIFI N300	4	\$ 17.00	\$ 68.00
PDU REGLETA ELECTRICA 8 TOMAS	1	\$ 70.00	\$ 70.00
TOTAL			\$ 1,857.00

Tabla 3. Presupuesto para la Red LAN en la sede Los Olivos.

AREA	CANTIDAD DE EQUIPOS	UBICACIÓN
Sala de Computo	20	Segundo Piso
Sala de Computo	2 Switches	Segundo Piso
Sala de Computo	1 Router	Segundo Piso
Secretaria	1 Switch	Segundo Piso
Secretaria	2 Pc's	Primer Piso
Secretaria	1 AP	Primer Piso
Pasadizo	1 AP	Segundo Piso
Pasadizo	1 AP	Tercer Piso
Pasadizo	1 AP	Cuarto Piso

Tabla 4. Cantidad de equipos a instalar en la sede Los Olivos.

4.1.1. Características del Router

- Cantidad de puertos: 8 puerto 10/100/1000
- Router TP-Link SG108 OMADA GIGABIT VPN
- Simple: interfaz de usuario intuitiva en caja, aplicación móvil y tablero de negocios Cisco simplifica las operaciones de red y automatiza la gestión del ciclo de vida
- Seguridad y enrutamiento: IEEE 802.1X y acceso a control de seguridad de puerto a tu red, la prevención de ataques del servicio (DoS) aumenta el tiempo de funcionamiento de la red durante un ataque, mientras que el enrutamiento estático ayuda a la comunicación entre segmentos de red



- Diseño innovador: diseño elegante y compacto, ideal para la instalación fuera del armario de cableado como tiendas minoristas, oficinas de plan abierto y aulas.



Fig 5.1 Router TP-Link SG108 OMADA GIGABIT VPN

4.1.2. Características del Switch

- Configuración del puerto de Ethernet: 24 puertos 10/100/1000, 2 x 1G combo SFP.
- Configuración y control: WebUI en caja fácil de usar, CLI ofrece capacidades básicas, SNMP, Cisco FindIT Network Manager, PnP, detección automática, implementación sin contacto.
- Características de L2+: enrutamiento estático, VLAN, QoS, VLAN de voz, GVRP, MSTP e IGMP Snooping.
- Características de seguridad: Lista de control de acceso (ACL), 802.1X / RADIUS, prevención DoS, SSH/SSL.
- Tranquilidad: garantía limitada de por vida, soporte técnico de un año y correcciones de software gratuitas para el plazo de la garantía.
- EFICIENTE ENERGÉTICO: Optimiza el uso de energía para reducir el coste de operación. Cumple con IEEE802.3az Energy Efficient Ethernet.



Fig 5.2 Switch CISCO SG250 24 puertos



Fig 5.3 Switch TP - link SG108 8 puertos



4.1.3. Características del Access Point (AP)

- Capacidad 802.11n. 2 x 3 entradas múltiples de salida múltiple (MIMO) con dos flujos espaciales (2x3:2)
- Montaje: incluye un soporte de montaje fácil de instalar y multiusos; UL 2043 con clasificación completa para opciones de instalación por encima del techo o suspendido de techos de caída; cerraduras para protección contra robos.
- Compatibilidad con la diversidad de cambios cíclicos



Fig 5.4 AP HUAWEI ES318N N300

4.1.4. PDU

- Main Input Voltage: 100V, 120V
- Main Output Voltage: 120V
- Plug standard: NEMA 5-15P
- Número de unidad de rack: 1RU

4.2. Configurando la Red LAN

Realizando un análisis para elección de los switches, se evalúa un equilibrio entre calidad y precio; Se pensó en varios modelos de marcas asequibles, por ejemplo, el SMCGS24C-Smart EZ Switch de SMC, el SNMP-GSH2402 de la marca Airlive (Filial de Ovislink) e incluso el SMB SRW2024-EU de Cisco. Todos ellos son switches gestionables 10/100/1000 en todos sus puertos RJ45, pero finalmente escogimos Switch Cisco SG250 24 puertos y Switch TP-Link SG108 8 puertos para las computadoras y la conmutación de éstos, respectivamente.

Ya que estos dispositivos solo son de conmutación, no necesitan una configuración de red, cosa que sí necesitan nuestras computadoras, routers y access point.

Escogimos este tipo de switch para la alta disponibilidad y la contingencia, en esta solución no usaremos la posibilidad de unir los switch's con fibra, pero merece la pena disponer de



**Universidad Nacional de Ingeniería
Facultad de Ingeniería Eléctrica y Electrónica
Proyecto de Fin de Carrera 2022-1**

esa opción desde el principio por si fuese necesario, ya que podríamos, en el futuro si fuese necesaria más velocidad en el enlace todas las plantas, incluir tarjetas de fibra en los correspondientes switch's y disponer de toda la red a la misma velocidad, eliminando el cuello de botella que supone el enlace wifi en este momento. Incluso si se usaran los 4 conectores de fibra, podríamos tener una troncal a 4 Gbps en las plantas.

Estos equipos tienen garantía de por vida dada por el fabricante directamente y cumplen con creces las necesidades de este proyecto. Incluyen soporte para gestión de QoS y soportan el estándar IEEE 802.1q para implementación y etiquetado de VLAN's.

Respecto a los equipos PC, encontramos las computadoras ya habidas antes de la evaluación, por lo que no hay problema en sus especificaciones, ya que la configuración en estos equipos es escalable, así que nos centramos en la configuración del router y los access point.

Debido al entorno donde se implantará la solución y al nivel de seguridad requerido, se propone el diseño de una red con dirección IP clase C, con dos VLAN configuradas de la siguiente manera.

VLAN 1	
IP	192.168.10.0/24
MASCARA	255.255.255.0
BROADCAST	192.168.10.255
RANGO DE IP'S VALIDAS	192.168.10.1 - 192.168.10.254

Tabla 5. Vlan 1 para el tercer piso, del colegio Monserrat sede San Martin de Porres.

VLAN 2	
IP	192.168.20.0/24
MASCARA	255.255.255.0
BROADCAST	192.168.20.255
RANGO DE IP'S VALIDAS	192.168.20.1 - 192.168.20.254

Tabla 6. Vlan 2 para el primer piso, del colegio Monserrat sede San Martin de Porres.



VLAN 1	
IP	192.168.30.0/24
MASCARA	255.255.255.0
BROADCAST	192.168.30.255
RANGO DE IP'S VALIDAS	192.168.30.1 - 192.168.30.254

Tabla 7. Vlan 1 para el segundo piso, del colegio Monserrat sede Los Olivos.

VLAN 2	
IP	192.168.40.0/24
MASCARA	255.255.255.0
BROADCAST	192.168.40.255
RANGO DE IP'S VALIDAS	192.168.40.1 - 192.168.40.254

Tabla 8. Vlan 2 para el primer piso, del colegio Monserrat sede Los Olivos.

Se estima que podrían llegar a conectarse a cada sede un aproximado de 50 personas, contando la red ethernet e inalámbrica, cuya capacidad es de 254 portadores (capacidad de distribución de IPs).

La salida a Internet se realizará a través de una sola dirección IP pública facilitada por el proveedor de acceso contratado en las condiciones pactadas con él (IP dinámica) y se hará NAT a través del módem-router de salida, de ese modo, todo el direccionamiento de la red es privado y no es alcanzable desde Internet directamente.

La mayoría de los equipos a conectar a la red son PCs que tomarán los datos de red (dirección IP, puerta de enlace, servidores de DNS, etc) de un servidor de DHCP, por lo que cualquier cambio en el direccionamiento IP de la red será muy sencillo de implantar porque afectará a pocos elementos: conmutadores, modem-router e impresoras fundamentalmente, que tendrán su IP establecida de forma fija y manual.

Se trata de un centro educativo y no hay datos sensibles en casi ningún equipo conectado a dicha red, salvo quizás en el despacho de secretaría.

En los equipos con datos sensibles, propone la instalación de cortafuegos software y evitar dejar recursos compartidos, con el fin de velar por la integridad y seguridad de la información.

No hay previsiones de crecimiento a corto plazo, por lo que unas 25 direcciones IP más que los puntos de red disponibles, son en principio suficientes para posibles ampliaciones: más equipos, posibles APs de una red wifi para profesores y alumnos, etc, teniendo en cuenta que además no se instalarán inicialmente todos los PCs en las aulas ni estarán conmutados todos los puntos de red cableados.



**Universidad Nacional de Ingeniería
Facultad de Ingeniería Eléctrica y Electrónica
Proyecto de Fin de Carrera 2022-1**

Finalmente, para comprobar la conectividad en nuestro simulador, procedemos a usar el comando -ping de pc a pc, y de pc a router. De esta manera poder asegurarnos la conectividad del sistema antes de la muy probable instalación.

Configuración de cada PC respecto al protocolo DHCP que otorgará las IPS de éstas.

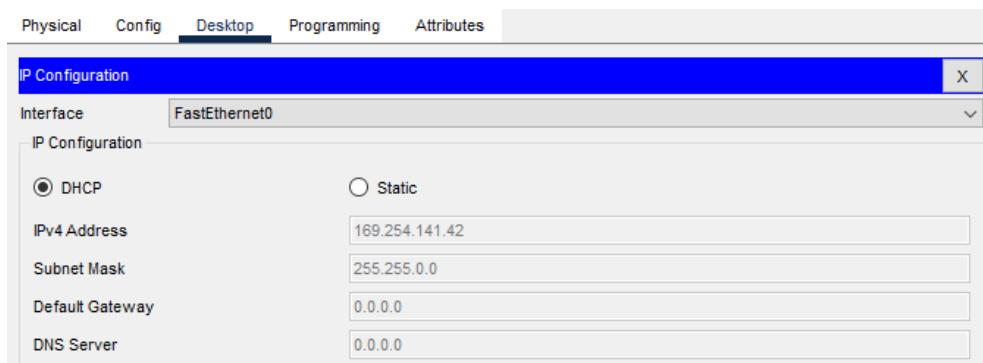


Figura 6. Interfaz de la configuración DHCP para un computador.

Configurando cada Access Point, con IP estática.

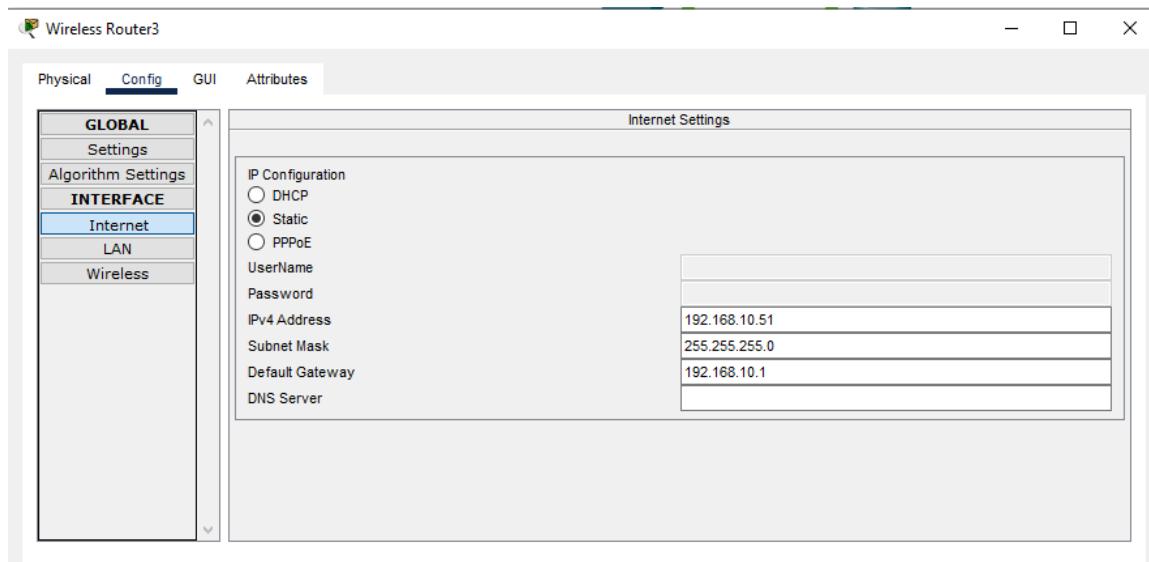


Figura 7. Interfaz de la configuración IP estática para un Acces Point.

Configurando cada interfaz de un Router.

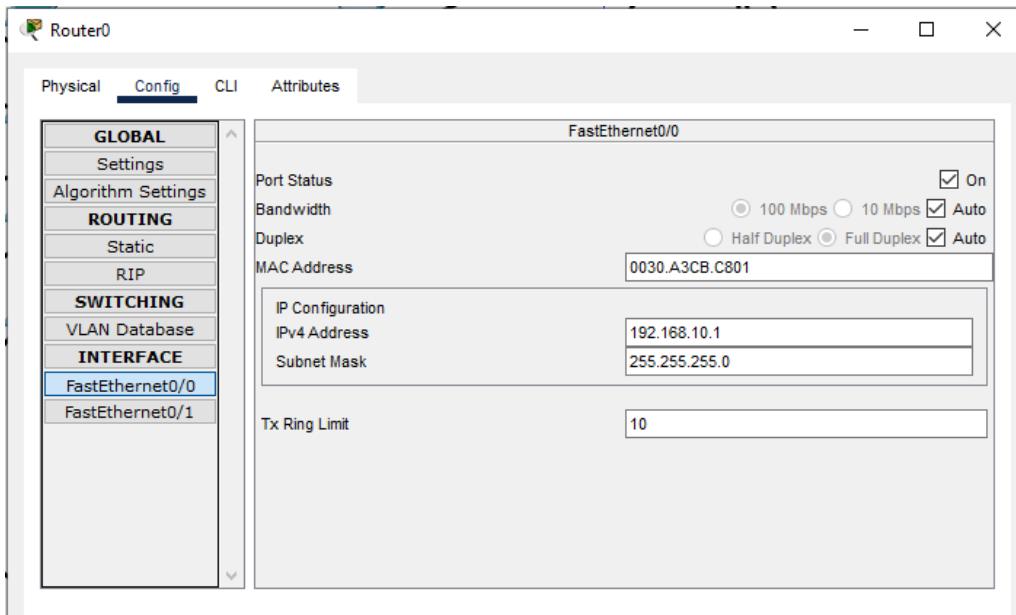


Figura 8. Configuración de cada interfaz de un router.

Cada configuración es de un dispositivo de red distinto, los datos ya fueron adjuntados en las tablas 5, 7 y 8.

4.2.1. Simulación de la Red LAN propuesta (Packet Tracer):

La solución planteada se basa en una simulación mediante Packet Tracer, en la cual se está diseñando las redes LAN de ambas sedes del colegio Monserrat.

Dado que el programa se centra en diseñar enlaces de redes, este nos proporciona una herramienta para simular la arquitectura de red.

Al simular con los componentes y protocolos descritos anteriormente, nos ilustra las figuras 9 y 10.



Universidad Nacional de Ingeniería
Facultad de Ingeniería Eléctrica y Electrónica
Proyecto de Fin de Carrera 2022-1

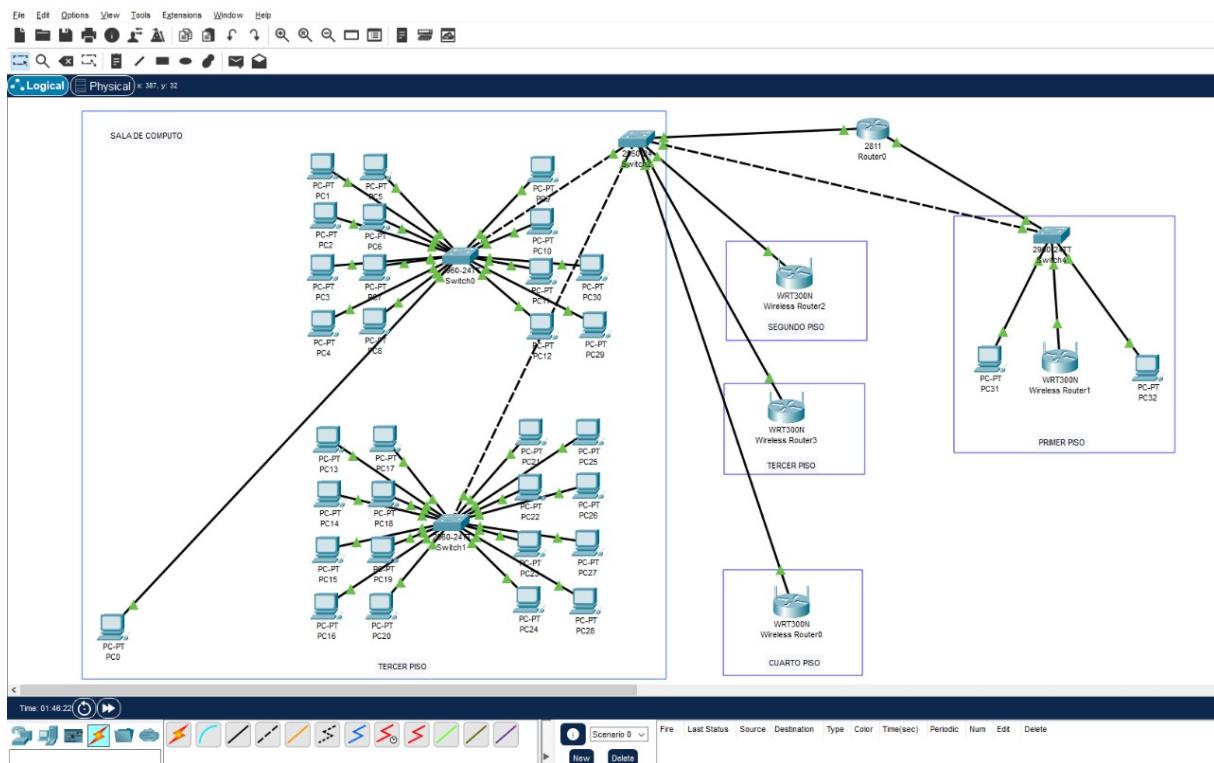


Figura 9. Representación de la simulación de mi red LAN en el colegio Monserrat, sede San Martín de Porres.

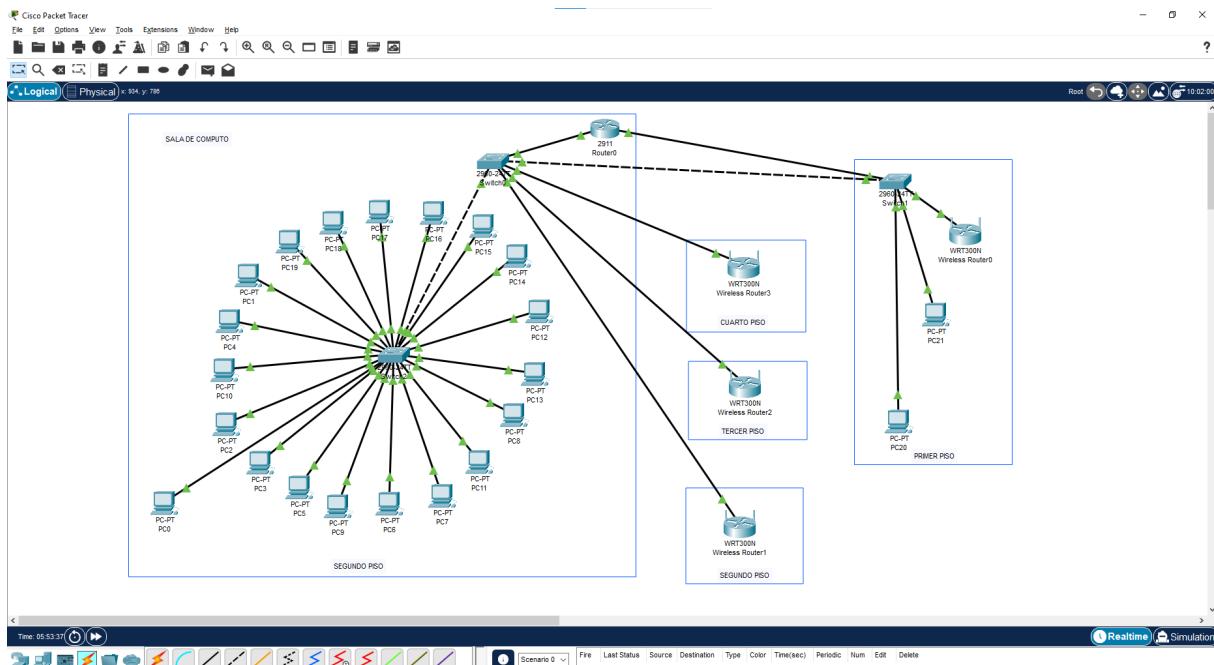


Figura 10. Representación de la simulación de mi red LAN en el colegio Monserrat, sede Los Olivos.



**Universidad Nacional de Ingeniería
Facultad de Ingeniería Eléctrica y Electrónica
Proyecto de Fin de Carrera 2022-1**

De acuerdo a los datos recogidos del estudio preliminar, configuramos la red para una Vlan de 31 computadoras en la sede San Martín de Porres, y 20 computadoras en la sede Los Olivos.

De acuerdo a los datos y especificaciones recolectados, y los protocolos a usar, realizamos nuestra simulación de las 2 redes en ambos colegios, donde el procedimiento para configurar cada dispositivo se encuentra en las figuras 6, 7 y 8.

Para confirmar la conexión y la confirmación del correcto funcionamiento de nuestra simulación, procedemos a realizar una función ping desde una pc a pc, luego de router a PC.

The screenshot shows a window titled "PC31" with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. Inside, there is a "Command Prompt" window with the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 169.254.70.5
Invalid Command.

C:\>ping 169.254.70.5

Pinging 169.254.70.5 with 32 bytes of data:

Reply from 169.254.70.5: bytes=32 time<1ms TTL=128

Ping statistics for 169.254.70.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figura 10. Función Ping de la PC31 a la dirección 169.254.70.5.



5. CONCLUSIÓN

Al implementar esta red en la institución se logrará aplicar una conectividad adecuada para cada dependencia de la institución, logrando así disminuir la tolerancia a fallos, la seguridad de la información y una escalabilidad de la red cuando ésta se vea necesaria de aplicar.

Por medio del uso adecuado de los equipos dentro de la institución, se logrará obtener una mejor cobertura y conectividad, asignando en cada área el equipo adecuado y de características ideales para el punto donde fue instalado.

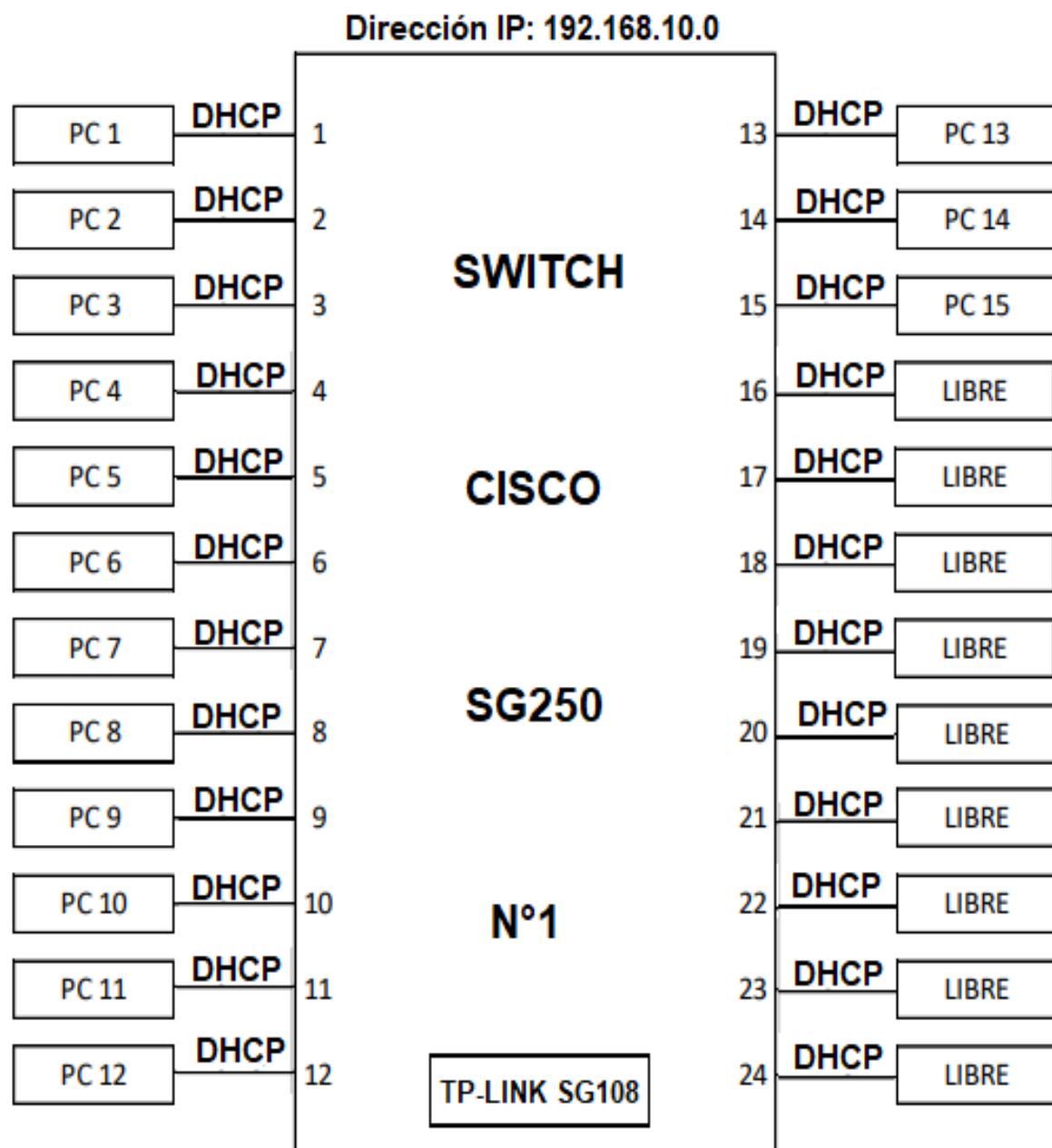
6. REFERENCIAS BIBLIOGRÁFICAS

- Barrera Gabriel, Aldana Camilo, Hernández (2019)
https://repository.ucc.edu.co/bitstream/20.500.12494/13066/1/2019-diseno_red_colegio.pdf
- Abad Albán, Barba Guamán (2018)
https://dspace.utpl.edu.ec/bitstream/123456789/575/3/UTPL_Abad_Alban_Rene_Franco_04x730.pdf
- Sarhan AlSarhan (2016)
<https://scholar.valpo.edu/cgi/viewcontent.cgi?article=1002&context=itcrpr>
- Osledi Rotceh (2020)
<https://repositorio.unprg.edu.pe/handle/20.500.12893/9005>
- Sulcahuaman Valdiglesias (2018)
<http://cybertesis.uni.edu.pe/handle/uni/13282>
- Llantoy Mayta Christian Shadirt (2020)
https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/1736/T037_44675738_T.pdf?sequence=1&isAllowed=y



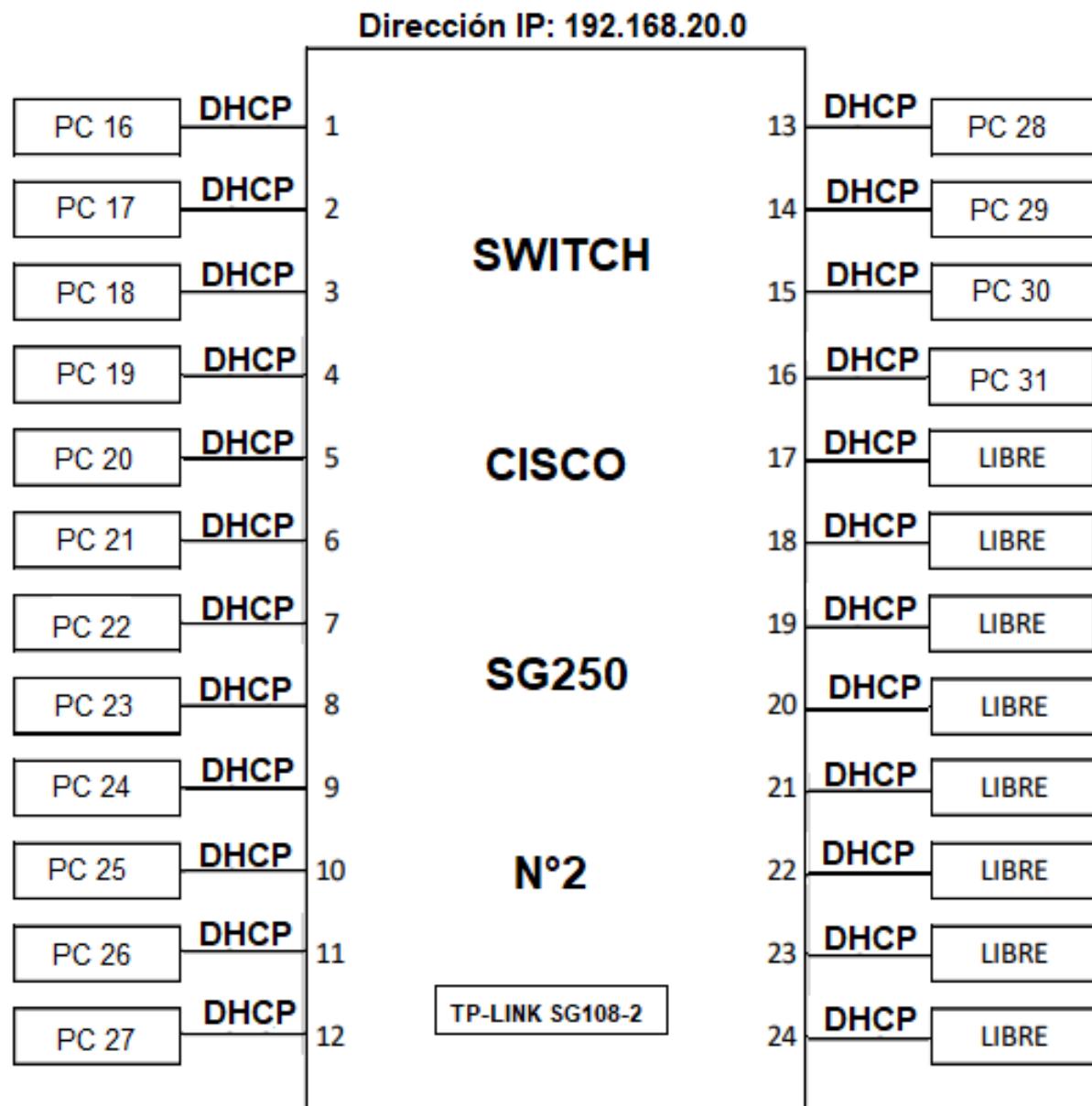
7. ANEXOS

- ANEXO A. Plano Conectividad Switch N°1 para la sede SMP: Jr. German Stiglich 2052, San Martín de Porres



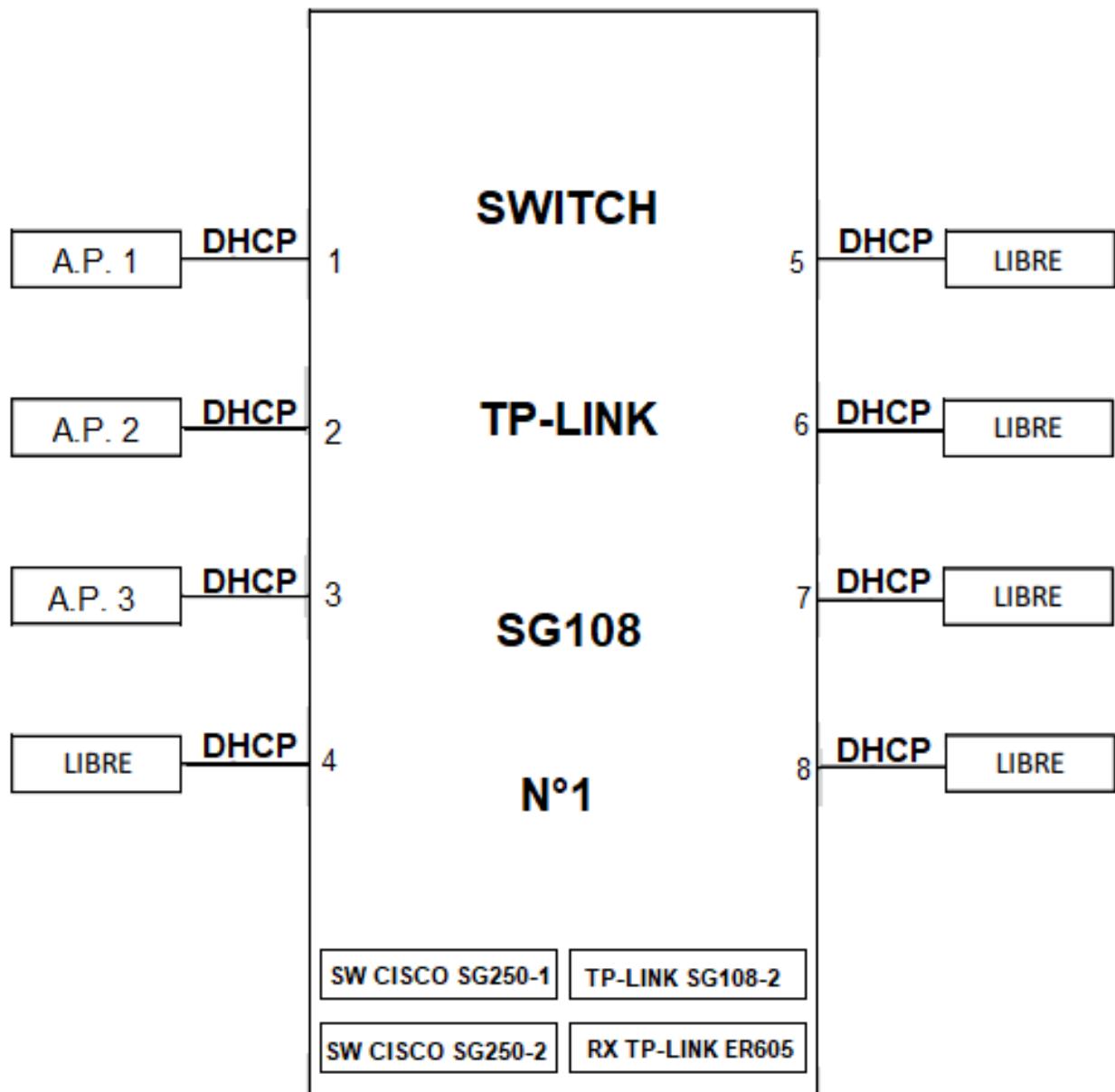


- ANEXO B. Plano Conectividad Switch N°2 para la sede SMP: Jr. German Stiglich 2052, San Martín de Porres



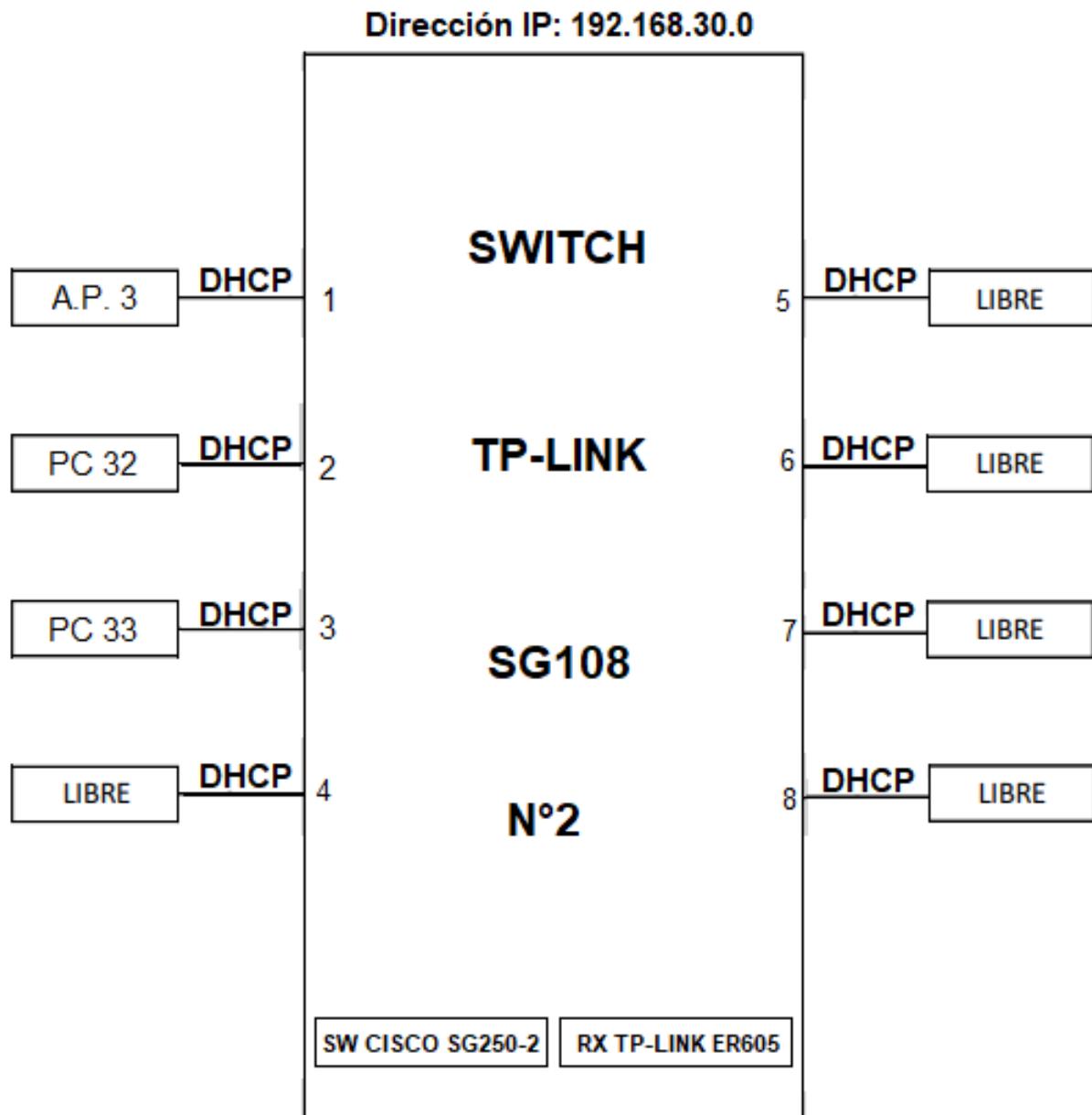


- ANEXO C. Plano Conectividad Switch N°3 para la sede SMP: Jr. German Stiglich 2052, San Martín de Porres



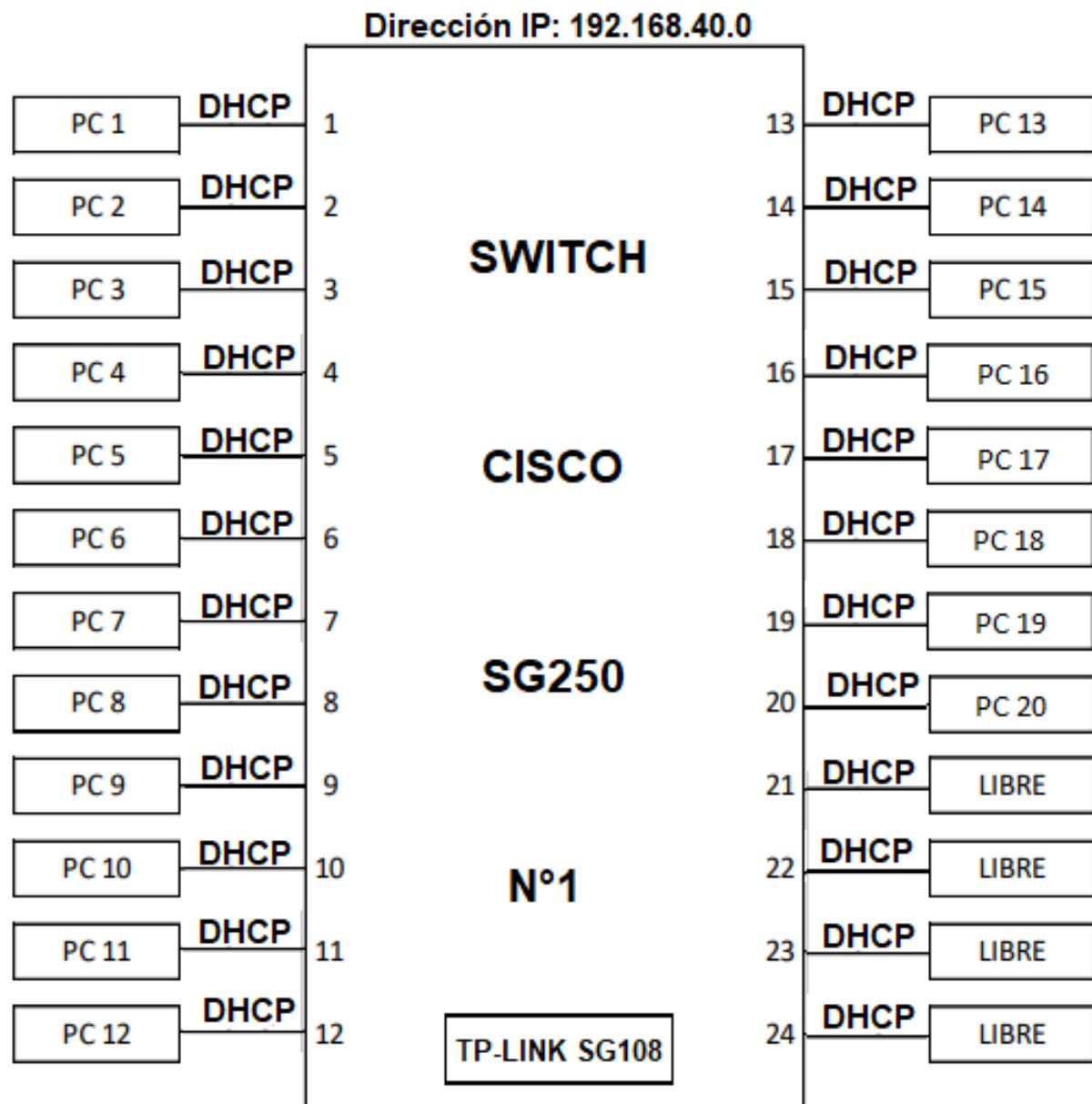


- ANEXO D. Plano Conectividad Switch N°4 para la sede SMP: Jr. German Stiglich 2052, San Martín de Porres



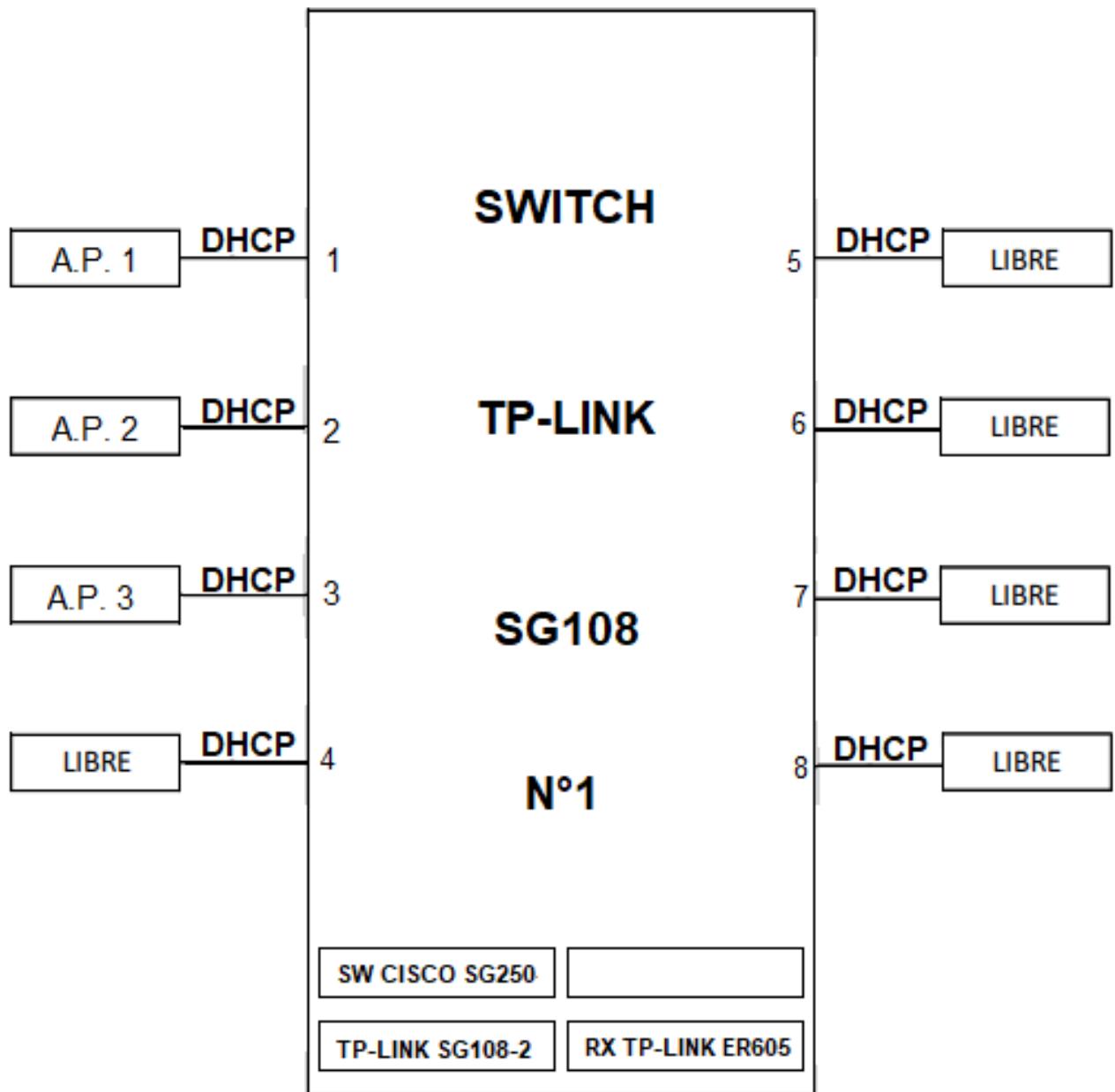


- ANEXO E. Plano Conectividad Switch N°1 para la sede Los Olivos: Av. Próceres 7610, Los Olivos 15307





- ANEXO F. Plano Conectividad Switch N°2 para la sede Los Olivos: Av. Próceres 7610, Los Olivos 15307





- ANEXO G. Plano Conectividad Switch N°3 para la sede Los Olivos: Av. Próceres 7610, Los Olivos 15307

