UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

UNAN - MANAGUA

FACULTAD DE CIENCIAS E INGENIERÍA DEPARTAMENTO DE TECNOLOGÍA

MAESTRÍA EN TELECOMUNICACIONES Y REDES TELEINFORMÁTICA

TESIS PARA OPTAR AL TÍTULO DE MÁSTER EN TELECOMUNICACIONES Y REDES INFORMÁTICAS

Tema:

PROPUESTA DE ANÁLISIS Y RESTRUCTURACIÓN DE LA RED DE DATOS Y APLICACIÓN DE PROTOCOLO DE SEGURIDAD EN EL CONSEJO NACIONAL DE UNIVERSIDADES (CNU)

Autor

Lic. Yamil José Durán Sanabria

Tutor

MSc. Harold Augusto González Villarreyna

Marzo 22, 2023

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Dedicatoria

El presente trabajo investigativo se lo dedico principalmente a Dios, por ser el inspirador y darme fuerza para continuar en este proceso de obtener uno de los anhelos más deseados.

A mi padre Jorge Luis Durán, por su amor, trabajo y sacrificio en todos estos años, gracias a él y a mi familia (Esposa Yuridia Gonzales y mi Hijo Dwayne Durán Gonzalez) he logrado llegar hasta aquí y convertirme en lo que soy ahora.

A todas las personas que me han apoyado y han hecho que el trabajo se realice con éxito, en especial a aquellos que me abrieron las puertas y compartieron sus conocimientos.

Agradecimiento

El presente trabajo agradezco a Dios por ser mi guía y acompañarme en el transcurso de mi vida, brindándome paciencia y sabiduría para culminar con éxito mis metas propuestas.

A mí padre por ser mi pilar fundamental y haberme apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron.

Agradezco a mi tutor de tesis MSc. Harold Agusto González Villarreyna quien, con su experiencia, conocimiento y motivación me oriento en la investigación.

Agradezco a todos los docentes de la maestría que, con su sabiduría, conocimiento y apoyo, motivaron a desarrollarme como persona y profesional en la Universidad Nacional Autónoma de Nicaragua, Managua (UNAN-Managua).

Carta de Aprobación del Tutor

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA
UNAN - MANAGUA

CARTA AVAL

El suscrito Tutor de Tesis de la Maestría **"Maestría en Telecomunicaciones y Redes Teleinformáticas"** habiendo sido designado por las autoridades académicas a cargo de dicho programa, extiendo la presente **carta Aval** al **Lic. Yamil José Durán Sanabria,** para la defensa de su Tesis para optar al Título de **"Máster en Telecomunicaciones y Redes Teleinformáticas"** en vista de que cumple con los requisitos científicos, técnicos y metodológicos requeridos para ser presentado y defendido ante un tribunal examinador, organizado para este fin.

En calidad de Maestro Tutor, extiendo la presente carta aval a los 21 días del mes de octubre del año 2022.

Atentamente,

MSc. Harold Augusto González Villarreyna
División de Sistemas de Información y Desarrollo Tecnológico
UNAN-Managua

Resumen

El avance de las redes inalámbricas en el mundo actual ha permitido que las personas se puedan comunicar sin la necesidad de conexión alámbrica, ofreciéndole la libertad de desplazarse sin perder la conectividad. En este contexto, en el Consejo Nacional de Universidades(CNU) se da la necesidad de realizar el estudio de soluciones y reconstrucción en las redes inalámbricas y la red de datos que actualmente posee, en la que servirá para su desarrollo institucional, en otras palabras, utilizar las tecnologías inalámbricas como herramientas de desarrollo en la institución.

El CNU en el 2011 adquirió un edificio propio e inicio con una pequeña red, todas las áreas o oficinas tenían una única red de dirección IPv4, para la Red de Área Local (LAN), en la que había comunicación con todos los dispositivos finales conectado a esa única red (192.168.1.0/24), debido a esa debilidad en la red, el acceso a los servicios era accesible. La información estaba vulnerable en todo los aspecto, interno y externo, para hacer adquirida por cualquier usuario.

Por lo tanto, el presente proyecto consiste en el **Análisis y Restructuración de la Red de Datos del CNU**, segmentando la red, creando redes privadas, escalable y segura a la conexión. De igual manera hacer un modelamiento de optimización del rendimiento en la red WIFI, brindando una conexión estable y segura con la última tecnología WIFI 6, usando programación multiobjetivo, para brindar un análisis del comportamiento de las redes inalámbricas; teniendo como parámetros de entrada más de una función y objetivo de selección como son Eficiencia y Confiabilidad.

1. Introducción

Las redes de datos se pueden definir como unas infraestructuras en la que ha sido creada para poder transmitir la información a través de los intercambios de datos. Es decir, son arquitecturas específicas para este fin, cuya principal es la conmutación de paquetes y que atienden a una clasificación exclusiva, teniendo en cuenta la distancia que es capaz de cubrir su arquitectura física y, por supuesto, el tamaño que presentan.

De la misma forma, Nicaragua a través del Programa Banda Ancha (PBA), en este 2021 tiene instalado en todo el país Fibra Óptica ADSS (All-dielectric self-supporting), en lo que corresponde a una distancia más de 2,000 Km de red construida, la rede de datos a nivel nacional se llevó a través de la última milla y se instalaron los equipos de transporte de datos en varios sitios o nodos, para tener una conectividad a nivel nacional, esto se ha venido realizando por la institución Empresa Nacional de Transmisión Eléctrica (ENATREL).

Asimismo, el Consejo Nacional de Universidades (CNU) cuenta con una red de datos en la que está compuesta por las conexiones LAN (Local Area Network, Red de Área Local) y WLaN (Wireless Local Area Network, Red de Área Local Inalámbrica), para conectar los dispositivos finales y dispositivos intermedios (dispositivos de red) que se etiquetan con direcciones IP numéricas para enviar y recibir datos a través de las redes de datos.

Debido a la lentitud del comportamiento de la red del CNU, se requiere mejorar la conexión con los dispositivos, aprovechar el avance de la tecnología y la movilidad de los equipos finales, así mantener la conexión estable y los servicios en ejecución. La pregunta central del proyecto es ¿Cómo restructura la red de datos con una mejor conexión y seguridad en la ST del CNU?

2. Planteamiento del Problema

Con la presente investigación se propone resolver unas de las dificultades del CNU, que es mejorar la infraestructura de red lógica, realizando una segmentación en la red, crear y administrar las redes virtuales, asegurar la red, que sea escalable y con una calidad de servicio.

Actualmente la institución cuenta con una red lógica pequeña, en donde los usuarios internos y externos, tienen accesos a los servicios de la Intranet e Internet, debido a esa conexión se crea una lentitud en la red, inseguridad y se puede presentar pérdida de la información.

Al compartir una única red privada o local y tener una sola conexión de WIFI sin la creación de redes inalámbrica segmentada, el ancho de banda no es estable y tendremos pérdida de paquete al envió de la información por el medio de conexión. De igual manera al no tener una buena organización o normalización en los equipos de redes, las respuestas de los servidores internos serán lentos o la información no llegará al usuario final.

Se estima que el presente trabajo de solución al problema que genera la actual red dentro del CNU, creando una red confiable y segura, para las áreas e invitados que se encuentren dentro de las instalaciones. Esto permitirá entregar todos los servicios como: Voz, Datos y Vídeos a través de la misma infraestructura de red, creando una red convergente.

3. Antecedentes

La red del Consejo Nacional de Universidades (CNU) se crea con una conexión de unos 5 ordenadores finales y un Hub de 16 puertos, la tecnología que se ocupaba para la salida al servicio de Internet, era la Línea de Abonado Digital Asimétrica (ADSL) con un ancho de banda de 1Mbps. Al tener un mínimo de ancho de banda y el equipo de red (Hub), el resultado era generarse colisiones, en la que se produce un consumo inadecuado de recursos y de ancho de banda, de igual manera si se le quiere enviar datos a un único ordenador no se podría hacerlo sin que cada bit se replique y se envíe también al resto que componen la red.

Debido al avance de la tecnología y el crecimiento de dispositivos finales para el acceso a los servicios de Intranet e Internet, se han venido realizando cambio en los dispositivos de intermedio (dispositivos de Red) y servidores, para aprovechar el avance de la tecnología, teniendo una conexión. Esto es debido a que la infraestructura de red con que inicio el CNU, no cumple con las normas de una Red de Área Local (LAN) o una red inalámbrica (WLAN) para una infraestructura robusta, segura y confiable.

El área de Tecnología de la Información (TI) del CNU, ha venido haciendo trabajo en la red paulatinamente, buscando como mejorar la ejecución de los servicios, una de los trabajos realizado es hacer segmentación en la red y que los equipos soporte dicho trabajo.

Por lo tanto, el presente proyecto actual, consiste en el **Análisis y Restructuración de la Red de Datos del CNU**, con el objetivo de que sea una red convergente, confiable, segura y escalable. Para una mejor conectividad, eficiencia, confiabilidad y se adapte a las nuevas tendencias tecnológica

4. Justificación

El presente estudio se origina debido a la necesidad que presenta la red, actualmente los dispositivos finales y los mismos equipos de redes, no se encuentran segmentado y todos están conectado en una red privada, tanto como internos y externos, debido a esta debilidad, la información del Consejo Nacional de Universidades (CNU), se encuentra vulnerable, esto quiere decir que cualquier dispositivo conectado a la red, podría tener acceso a la información.

El CNU al tener una red no estable y que no se encuentre organizada, los servicios de la Intranet e Internet no estarán estable, se tendrían pérdida de conexión y la información no llegaría estable para los dispositivos finales.

Existe factibilidad para realizar el presente trabajo investigativo, se cuenta con el apoyo necesario de la institución en este caso el CNU, los conocimientos suficientes del investigador, bibliografía especializada y recursos tecnológico.

Por esta razón, la importancia de esta investigación tendrá una utilidad práctica, en la que se demostrará con una propuesta de solución al problema investigado. En la que se mejora la red de datos del CNU, con una arquitectura de calidad de servicio, seguridad y con una red convergente que transporte múltiples servicios, utilizando un conjunto de reglas y normas.

5. Objetivo General:

Restructuración de la red de datos del Consejo Nacional de Universidades (CNU), mediante tecnología ethernet aplicando los estándares para IEEE 802.3 para la LAN y la 802.11ax correspondiente al WIFI 6 y aplicando políticas de seguridad para el control de acceso a los usuarios

5.1.Objetivo Especifico:

Realizar un diagnóstico de la seguridad de la red de datos del CNU en la red de área local (LAN) y la red de área local inalámbrica (WLAN) del CNU para un correcto diseño de la red.

Implementar un modelo de mejor rendimiento para las redes, aplicando los estándares IEE 802.11ax, para una mejor cobertura, eficiencia y la confiabilidad del acceso a los hosts o dispositivos finales del CNU.

Evaluar la red, mediante el conjunto de medidas de eficiencia y confiabilidad por medio de una herramienta de simulación, en toda la infraestructura del CNU.

6. Marco Teórico

Existen redes de todo tamaño. Pueden ir desde redes simples, compuesta por dos pc, hasta redes amplia donde se conectan millones de dispositivos. Para el análisis y restructuración de la red de datos, se requiere conocer los siguientes conceptos en donde se aplicará para obtener una tolerancia a fallas, escalabilidad, calidad de servicio (QoS) y Seguridad, con las siguientes definiciones:

6.1.RED

Una red es la infraestructura tecnológica que permite a las empresas o instituciones interconectar sus aplicaciones. Son un conjunto de dispositivos (hosts) que se conectan entre si con el objetivo intercambiar información.

Según su extensión geográfica, los dispositivos que las conforman y las tecnologías específicas, se podría clasificar las redes de datos en dos grandes grupos: las redes de Área Local (LAN, Local Area Networks) y las Redes de Área Amplia (WAN, Wide Area Networks).

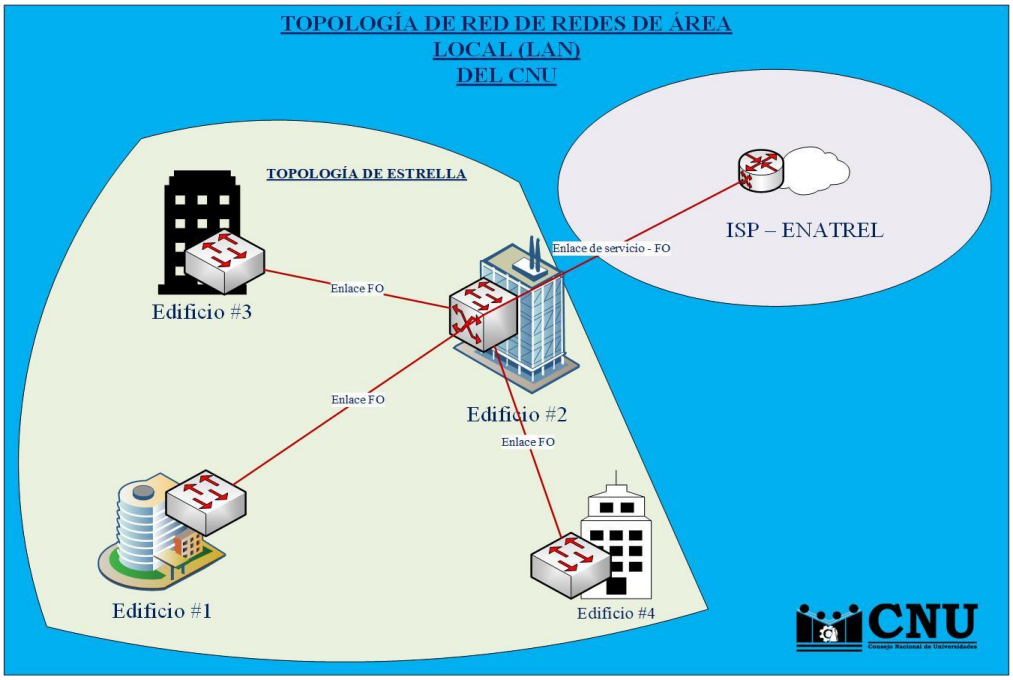
6.1.1. Red de Área Local

Las redes de área local (LAN, Local Area Network) son infraestructuras de red que proporcionan acceso a los usuarios y a los dispositivos finales en un área geográfica pequeña.

En el CNU la topología que se está utilizando, es la de estrella y en la siguiente figura se muestra la LAN del CNU:

Figura 1

Topología de red local, edificios del CNU



Nota. Enlace de conexión entre edificios del CNU, información aprobada por las autoridades del CNU.

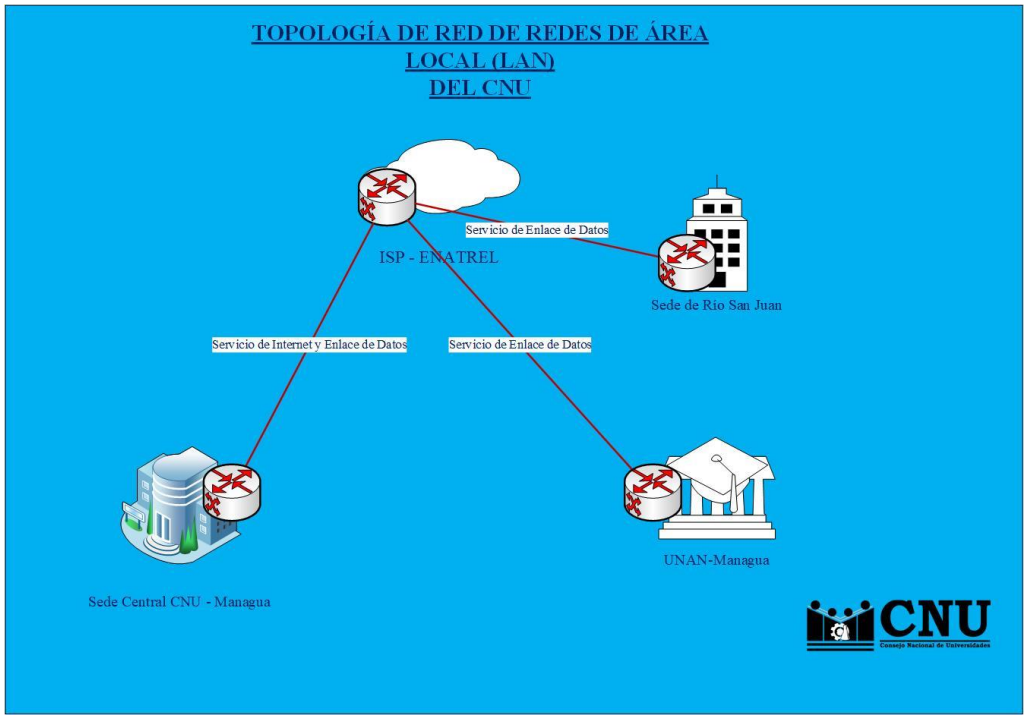
6.1.2. Red de Área Extensa

Las redes de área extensa (WAN, Wide Area Network) son infraestructuras de red que proporcionan acceso a otras redes en un área geográfica extensa.

El CNU tiene una red WAN con el proveedor de ISP – ENATREL, enlaces de datos hacia la UNAN-Managua y la sede del CNU ubicada en Río San Juan, a como se muestra en la siguiente imagen:

Figura 2

Topología de red extensa (WAN), las sedes del CNU



Nota. Enlace de conexión entre la sede central, con la sede de Río San Juan y la UNAN-Managua, información aprobada por las autoridades del CNU.

6.1.3. Red de Área Metropolitana

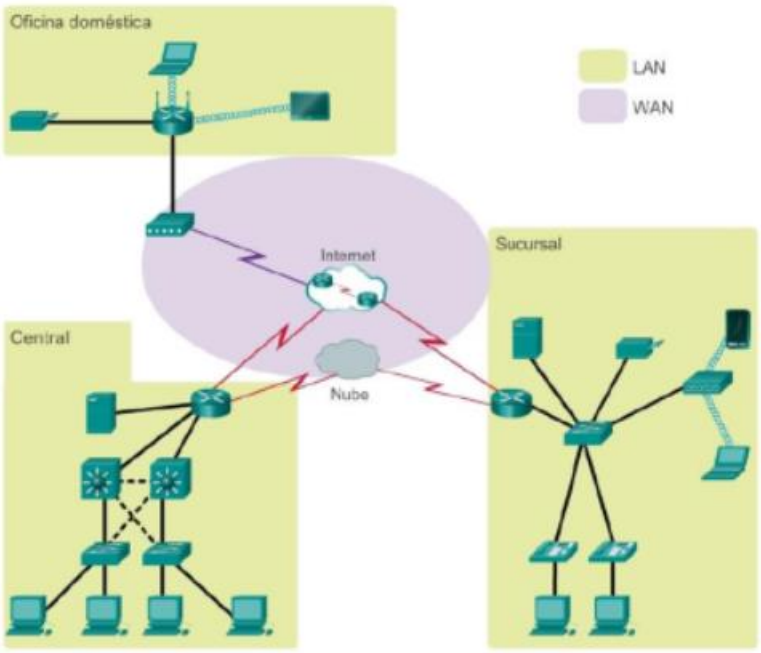
Las redes de área metropolitana (MAN, Metropolitan Area Network) son infraestructura de red que abarcan un área física mayor que la de una LAN, pero menor que la una WAN (por ejemplo, una ciudad). Por lo general, la operación de MAN está a cargo de una única entidad, como una organización de gran tamaño.

6.1.4. LAN Inalámbrica

Las LAN inalámbricas (WLAN, Wireless LAN) son similares a las LAN, solo que interconectan de forma inalámbrica a los usuarios y los extremos en un área geográfica pequeña.

Figura 3

Topología de una red LAN y WAN



Nota. Ejemplo de una topología de red LAN con una conexión a una red WAN.

6.1.5. Red de Área de Almacenamiento

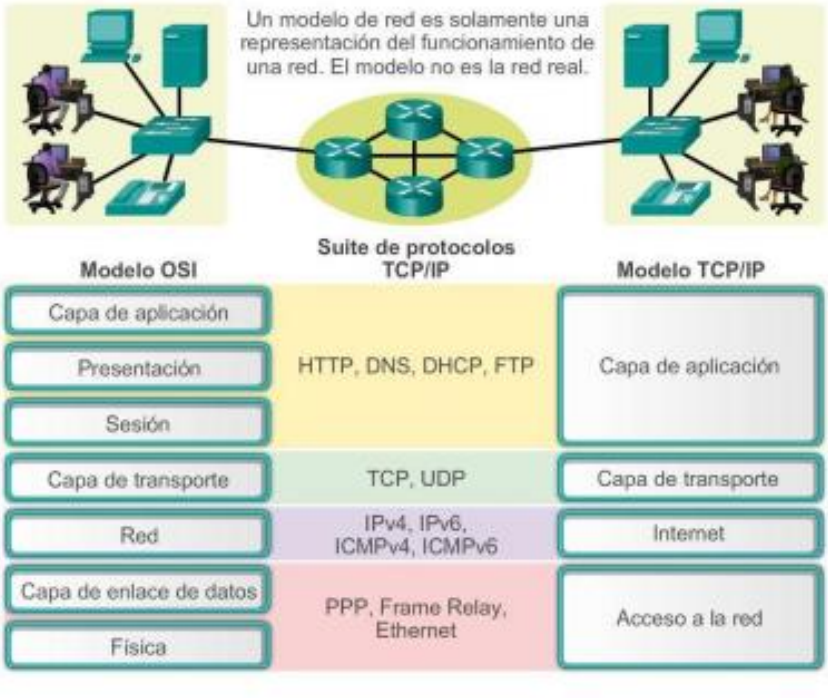
Las redes de área de almacenamiento (SAN, Storage area network) son infraestructuras de red diseñadas para admitir servidores de archivos y proporcionar almacenamiento, recuperación y replicación de datos. Estas incluyen los servidores de tecnología avanzada, matrices de varios discos (denominadas “bloques”) y la tecnología de interconexión de canal de fibra.

6.2.Modelos de Capas

Los modelos en capas, como el modelo TCP/IP, con frecuencia se utilizan para ayudar a visualizar la interacción entre protocolos. Un modelo de capa describe el funcionamiento de los protocolos que se produce en cada capa y la interacción de los protocolos con las capas que se encuentran por encima y por debajo de ellas.

Figura 4

Modelo de Referencia OSI y TCP/IP



Nota. Resumen comparativo del modelo OSI y del modelo TCP/IP.

6.2.1. Modelo de Referencia OSI(Open System Interconnection)

Divide a la red en diferentes capas con el propósito de que cada desarrollador trabaje específicamente en su campo sin tener necesidad de depender de otras áreas. En su conjunto, el modelo OSI se compone de siete capas bien definidas que son:

6.2.2. Capa 1, Física

Se encarga de los medios, conectores, especificaciones eléctricas, lumínicas, radiofrecuencia y de la codificación. Los bits son transformados en pulsos eléctricos, en luz o en radiofrecuencia para ser enviados según sea el medio en que se propaguen.

6.2.3. Capa 2, Enlace de Datos

Proporciona las comunicaciones entre puestos de trabajo en una primera capa lógica, transforma los voltios en tramas y las tramas en voltios. El direccionamiento físico y la determinación de si deben subir un mensaje a la pila de protocolo ocurren en esta capa. Está divida en dos subcapas, la LLC (Logical Link Control) y la subcapa MAC (Media Access Control). Algunos protocolos de capa 2: Ethernet, 802.2, 802.3, HDLC, Frame-Relay.

6.2.4. Capa 3, Red

En esta capa se lleva a cabo el direccionamiento lógico que tiene carácter jerárquico, se selecciona la mejor ruta hacia el destino mediante el uso de tablas de enrutamiento a través del uso de protocolos de enrutamiento o por direccionamiento estático. Protocolos de capa de red pueden ser: IP, IPX, RIP, IGRP, Apple Talk.

6.2.5. Capa 4, Transporte

Es la encargada de la comunicación confiable entre host, control de flujo y de la corrección de errores entre otras cosas. Los datos son divididos en segmentos identificados con un encabezado con un número de puerto que identifica la aplicación de origen. En esta capa funcionan protocolos

como UDP y TCP, siendo este último uno de los más utilizados debido a su estabilidad y confiabilidad.

6.2.6. Capa 5, Sesión

Es la responsable de establecer, administrar y concluir las sesiones de comunicaciones entre entidades de la capa de presentación. La comunicación en esta capa consiste en peticiones de servicios y respuestas entre aplicaciones ubicadas en diferentes dispositivos. Un ejemplo de este tipo de coordinación podría ser el que tiene lugar entre un servidor y un cliente de datos.

6.2.7. Capa 6, Presentación

Los datos formateados se proveen de diversas funciones de conversión y codificación que se aplican a los datos provenientes de la capa de aplicación. Estas funciones aseguran que estos datos enviados desde la capa de aplicación de un sistema origen podrán ser leídos por la capa de aplicación de otro sistema destino.

6.2.8. Capa 7, Aplicación

Es la única capa que no presta servicio a otra puesto que es la capa de nivel superior del modelo OSI directamente relacionada con el usuario. La aplicación a través del software dialoga con los protocolos respectivos para acceder al medio.

6.2.9. Modelo de Referencia TCP/IP

El Departamento de Defensa de EE.UU. (DoD) requería una transmisión de datos confiable hacia cualquier destino de la red, en cualquier circunstancia. La creación del modelo TCP/IP ayudó a solucionar este difícil problema de diseño. Desde entonces, TCP/IP se ha convertido en el estándar en el que se basa Internet.

6.2.10. Protocolos de Capa de Aplicación

Los protocolos describen el conjunto de normas y convenciones que rigen la forma en que los dispositivos de una red intercambian información. Algunos de los protocolos de la capa de Aplicación del modelo TCP/IP son: Telnet, FTP, TFTP, DNS, DHCP, SMTP y SNMP (incluir en glosario).

6.2.11. Protocolo de Capa de Transporte

Se encargan de dar soporte a la capa superior brindando apoyo enviando los datos sin importar el contenido de los mismos. Los dos protocolos extensamente conocidos para tal proceso son: TCP y UDP (incluir en glosario).

6.2.12. Protocolo de Capa de Internet

Estos son algunos de los protocolos más usados que operan en la capa de Internet del modelo TCP/IP: IP, ARP, RARP y ICMP.

6.2.13. Protocolo de Capa de Red

Controla los dispositivos de hardware y los medios que crean la red.

6.3.Protocolo IP

El protocolo IP es el servicio de capa de red implementado por la suite de protocolos TCP/IP.

IP se diseñó como protocolo con baja sobrecarga. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. De ser necesarias, otros protocolos en otras capas llevan a cabo estas funciones.

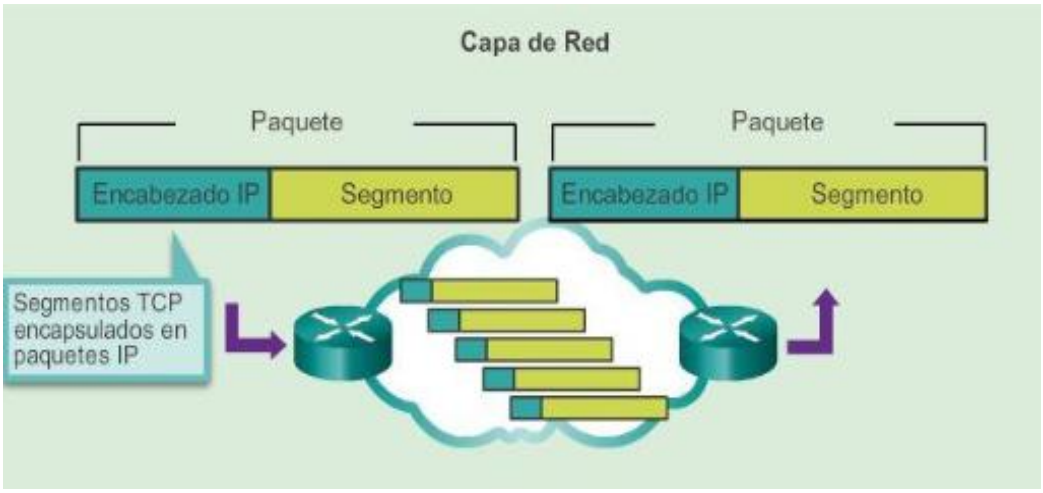
Las características básicas del protocolo IP son las siguientes:

- Sin conexión: no se establece ninguna conexión con el destino antes de enviar los paquetes de datos.

- Máximo esfuerzo (no confiable): la entrega de paquetes no está garantizada.
- Independiente de los medios: la operación es independiente del medio que transporta los datos.

Figura 5

Encapsulación de paquete



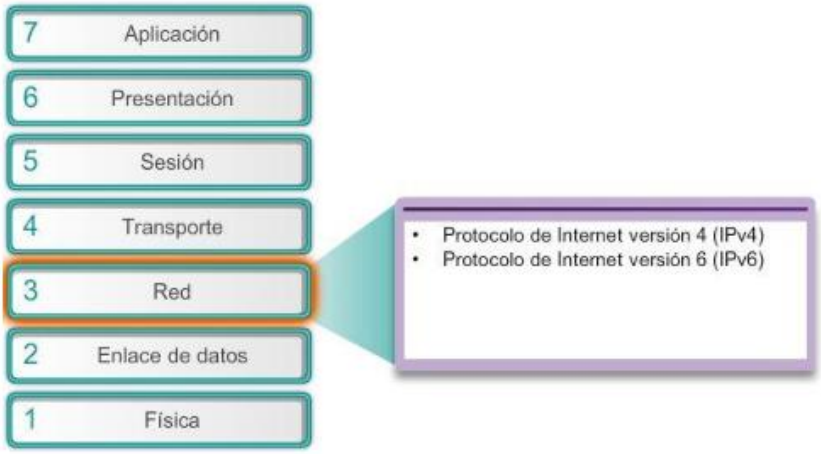
Nota. Descripción de la capa de red, encapsulación por paquetes

Existen varios protocolos de capa de red; sin embargo, solo los dos que se incluyen a continuación se implementan con frecuencia, a como se muestra en la ilustración:

- Protocolo de Internet versión 4 (IPv4)
- Protocolo de Internet versión 6 (IPv6)

Figura 6

Capas del Modelo OSI



Notas. Ubicación de la capa de red, mostrando que el IPv4 e IPv6 pertenecen a la capa de 3.

6.3.1. Direccionamiento IPv4

Para que dos dispositivos se comuniquen entre sí, es necesario poder identificarlos claramente. Una dirección IPv4 es una secuencia de unos y ceros de 32 bits. Para hacer más comprensible el direccionamiento, una dirección IP aparece escrita en forma de cuatro números decimales separados por puntos. La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros.

Una dirección IPv4 consta de dos partes definidas por la llamada máscara de red. La máscara puede describirse a través de una notación decimal punteada o con el prefijo /X, donde X es igual a la cantidad de bits en 1 que contiene dicha máscara. Una parte identifica la red donde se

conecta el sistema y la segunda identifica el sistema en particular de esa red. Este tipo de dirección recibe el nombre de dirección jerárquica porque contiene diferentes niveles. Una dirección IPv4 combina estos dos identificadores en un solo número. Este número debe ser exclusivo, porque las direcciones repetidas harían imposible el enrutamiento. La primera parte identifica la dirección de la red del sistema. La segunda parte, la del host, identifica qué máquina en particular de la red.

Tabla 1

Ejemplo de una dirección IPv4, clase B.

172	16	1	3
10101100	00010000	00000001	00000011
255	255	0	0
11111111	11111111	000000000	00000000
Porción de red		Porción de host	

Notas. Demostración de una dirección IPv4 172.16.1.2 con su máscara de red 255.255.255.0 y en binario

6.3.2. Tipo de direcciones IPv4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

- Dirección de red: la dirección en la que se hace referencia a la red o subred.
- Dirección de broadcast: una dirección especial que se utiliza para enviar datos a todos los hosts de la red.
- Dirección de host: las direcciones asignadas a los dispositivos finales.

6.3.3. Tipo de comunicación IPv4

En una red IPv4, los hosts pueden comunicarse de tres maneras diferentes:

Unicast

Es el método por el cual se envía un paquete de un host individual a otro host individual. La comunicación unicast se usa para una comunicación normal de host a host, tanto en una red de cliente/servidor como una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork.

Broadcast:

El método por el cual se envía un paquete de un host a todos los hosts de la red. Existe un direccionamiento particular cuando los bits de la dirección de host están todos en la llamada dirección de broadcast, o de difusión. Este direccionamiento identifica al host origen, mientras que como destino tiene a todos los dispositivos que integran el mismo domino.

Multicast:

Es el mecanismo, por el cual se envía un paquete de un host a un grupo seleccionado de hosts. Un dispositivo IP se une a un grupo reconociendo una dirección IP de otro grupo y reprogramando su tarjeta de red (NIC) para copiar todo el tráfico destinado a la dirección MAC del grupo.

Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen.

6.3.4. Clases de Direcciones IPv4

La RFC1700 agrupa rangos de direcciones unicast en tamaños específicos llamados direcciones de clase. Las direcciones IPv4 se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas. Dentro de cada rango existen direcciones llamadas privadas para uso interno que no veremos en Internet. Las direcciones de clase D son de uso multicast y las de clase E, experimentales.

- Direccionamiento Clase A:

  Rango de direcciones IP: 1.0.0.0 a 127.0.0.0

  Máscara de red: 255.0.0.0 o /8

  Direcciones privadas: 10.0.0.0 a 10.255.255.255

- Direccionamiento Clase B:

  Rango de direcciones IP: 128.0.0.0 a 191.255.0.0

  Máscara de red: 255.255.0.0 o /16

  Direcciones privadas: 172.16.0.0 a 172.31.255.255

- Direccionamiento Clase C:

  Rango de direcciones IP: 192.0.0.0 a 223.255.255.0

  Máscara de red: 255.255.255.0 o /24

  Direcciones privadas: 192.168.0.0 a 192.168.255.255

- Direccionamiento Clase D:

  Rango de direcciones IP: 224.0.0.0 a 239.255.255.255

  Uso multicast o multidifusión

- Direccionamiento Clase E:

  Rango de direcciones IP: 240.0.0.0 a 254.255.255.255

  Uso experimental o científico

En números binarios:

- Las clases A comienzan con 00xxxxxx
- Las clases B comienzan con 10xxxxxx
- Las clases C comienzan con 11xxxxxx
- Las clases D comienzan con 111xxxxx
- Las clases E comienzan con 1111xxxx

6.3.5. Direcciones Reservadas IPv4

Hay determinadas direcciones, que no pueden asignarse a los hosts por varios motivos. También hay direcciones especiales que pueden asignarse a los hosts pero con restricciones en la interacción de dichos hosts dentro de la red.

6.3.6. Direcciones de Red y Broadcast

No es posible asignar la primera ni la última dirección a los hosts dentro de cada red. Éstas son, respectivamente, la dirección de red y la dirección de broadcast del rango de host.

6.3.7. Ruta Predeterminada

La ruta predeterminada IPv4 se presenta como 0.0.0.0. La ruta predeterminada se usa como ruta por defecto cuando no se dispone de una ruta más específica. El uso de esta dirección también reserva todas las direcciones en el bloque de direcciones 0.0.0.0 al 0.255.255.255.255 (0.0.0.0 /8).

6.3.8. Loopback

Es una de las direcciones reservadas IPv4. La dirección de loopback 127.0.0.1 es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para la aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. Al utilizar la dirección de loopback en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden desviar las capas inferiores de la pila TCP/IP. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local.

6.3.9. Direcciones Link-Local

Las direcciones IPv4 del bloque de direcciones desde 169.254.0.0 hasta 169.254.255.255 (169.254.0.0 /16) se encuentran designadas como direcciones Link-local. El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de

una configuración IP. Se puede usar en una red de punto a punto o para un host que no pudo obtener automáticamente una dirección de servidor de protocolo de configuración de host (DHCP).

6.3.10. Subredes

Las redes IPv4 se pueden dividir en redes más pequeñas, para el mayor aprovechamiento de las mismas, son las llamadas subredes, además de contar con esta flexibilidad, la división en subredes permite que el administrador de la red brinde contención de broadcast y seguridad de bajo nivel en la LAN. La división en subredes, además, ofrece seguridad ya que el acceso a las otras subredes está disponible solamente a través de los servicios de un router. Las clases de direcciones IP disponen de 256 a 16,8 millones de hosts según su clase.

El proceso de creación de subredes comienza pidiendo "prestado" al rango de host la cantidad de bits necesaria para la cantidad de subredes requeridas. Se debe tener especial cuidado en esta acción de pedir ya que deben quedar como mínimo dos bits de rango de host.

La máxima cantidad de bits disponible para este propósito depende del tipo de clase:

- **Clase A**, cantidad disponible 22 bits.
- **Clase B**, cantidad disponible 14 bits.
- **Clase C**, cantidad disponible 6 bits.

Cada bit que se toma del rango de host posee dos estados, 0 y 1, por lo tanto, si se toman tres bits existirán 8 estados diferentes:

Tabla 2

Rango de bits por hosts.

Bits prestados	Bits de host	Valor decimal
000	00000	0
001	00000	32
010	00000	64
011	00000	96
100	00000	128
101	00000	160
110	00000	192
111	00000	224

Nota. Demostración del uso de los bits por host, misma tabla se representa por decimal.

El número de subredes se puede usar igual a: 2 elevado a la potencia del número de bits asignados a subred.

2 ^N = Número de subredes

Donde N es la cantidad de bits tomados al rango de host.

Por lo tanto, si se quieren crear 5 subredes, es decir, cumpliendo la fórmula 2, tendrá que tomar del rango de host 3 bits:

2^3 = 8

Observe que no siempre el resultado es exacto, en este caso se pedían 5 subredes, pero se obtendrán 8.

6.4.Topología

Los diagramas de topología son obligatorios para los que trabajan con redes. Estos diagramas proporcionan un mapa visual que muestran cómo está conectada la red.

La topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos. Las topologías LAN y WAN se pueden ver de dos maneras:

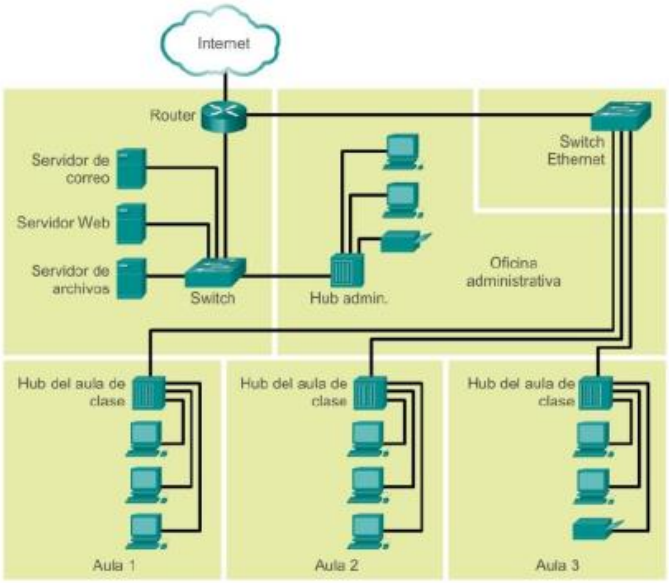
- Topología Física
- Topología Lógica

6.4.1. Topología Física

Se refiere a las conexiones físicas e identifica cómo se interconectan los dispositivos finales y de infraestructura, como los routers, los switches y los puntos de acceso inalámbrico. Las topologías físicas generalmente son punto a punto o en estrella.

Figura 7

Topología física



Nota. Ejemplo de una topología de red, con los equipos de redes y hosts.

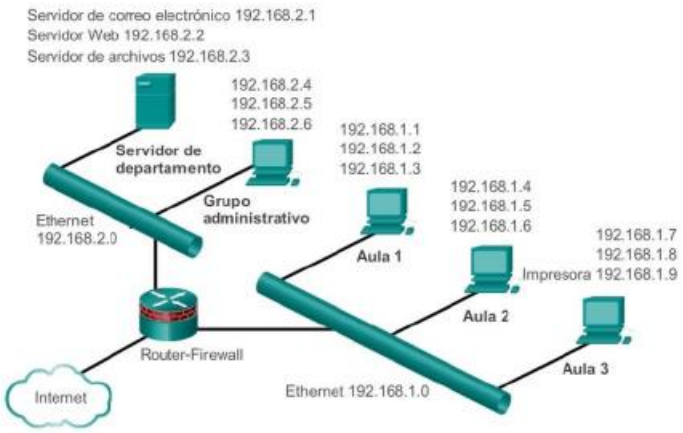
6.4.2. Topología Lógica

Se refiere a la forma en que una red transfiere tramas de un nodo al siguiente. Esta disposición consta de conexiones virtuales entre los nodos de una red. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas.

La topología lógica de los enlaces punto a punto es relativamente simple, mientras que los medios compartidos ofrecen métodos de control de acceso al medio deterministas y no deterministas.

Figura 8

Topología lógica.



Nota. Topología lógica de direccionamiento IP

6.4.3. Topologías físicas de WAN

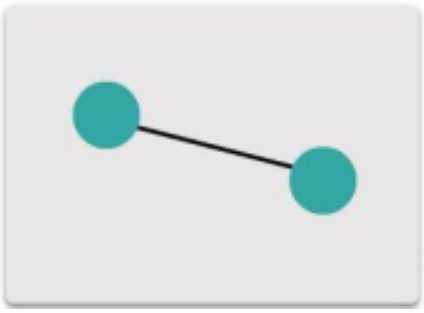
Por lo general, las WAN se interconectan mediante las siguientes topologías físicas:

6.4.3.1.Punto a Punto

Esta es la topología más simple, que consta de un enlace permanente entre dos terminales. Por este motivo, es una topología de WAN muy popular.

Figura 9

Topología punto a punto



Nota. Ejemplo de como es una red punto a punto.

6.4.3.2.Hub-and-Spoke

Es una versión WAN de la topología en estrella, en la que un sitio central interconecta sitios de sucursal mediante enlaces punto a punto.

Figura 10

Topología de Hub-and-Spoke

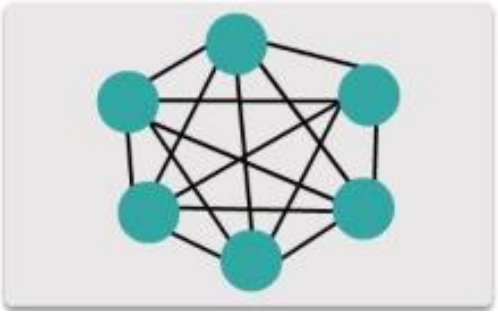
Nota. Topología de Estrella, enlaces de punto a punto.

6.4.3.3.Topología Malla

Esta topología proporciona alta disponibilidad, pero requiere que cada sistema final esté interconectado con todos los demás sistemas. Por lo tanto, los costos administrativos y físicos pueden ser importantes. Básicamente, cada enlace es un enlace punto a punto al otro nodo. Las variantes de esta topología incluyen la topología de malla parcial, en la que se interconectan algunos dispositivos finales, pero no todos.

Figura 11

Topología de Malla



Nota. Ejemplo de la topología de malla, en donde cada enlace es un enlace punto a punto al otro nodo.

6.4.4. Topología Física de LAN

La topología física define cómo se interconectan físicamente los sistemas finales. En las redes LAN de medios compartidos, los dispositivos finales se pueden interconectar mediante las siguientes topologías físicas:

6.4.4.1.Estrella

Los dispositivos finales se conectan a un dispositivo intermediario central. Las primeras topologías en estrella interconectaban dispositivos finales mediante hubs. Sin embargo, en la actualidad estas topologías utilizan switches. La topología en estrella es la topología física de LAN más común, principalmente porque es fácil de instalar, muy escalable (es fácil agregar y quitar dispositivos finales) y de fácil resolución de problemas

Figura 12

Topología de estrella física.

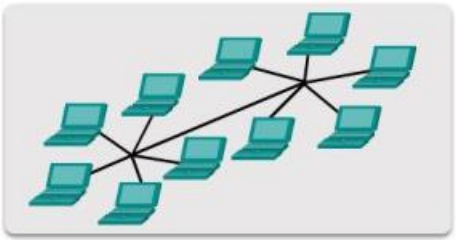
Nota. Topología de estrella más común, por su facilidad de instalación.

6.4.4.2.Estrella extendida o híbrida

En una topología en estrella extendida, dispositivos intermediarios centrales interconectan otras topologías en estrella. En una topología híbrida, las redes en estrella se pueden interconectar mediante una topología de bus.

Figura 13

Topología estrella extendida o híbrida



Nota. Topología hibrida, la topología de estrella se puede conectar mediante de bus.

6.4.4.3.Bus

Todos los sistemas finales se encadenan entre si y terminan de algún modo en cada extremo. No se requieren dispositivos de infraestructura, como switches, para interconectar los dispositivos finales. Las topologías de bus se utilizaban en las antiguas redes Ethernet, porque eran económicas y fáciles de configurar.

Figura 14

Topología de bus.

Nota. Las topologías de bus, fueron utilizadas en las primeras redes.

6.4.4.4.Anillo

Los sistemas se conectan a su respectivo vecino y forman un anillo. A diferencia de la topología de bus, la de anillo no necesita tener una terminación. Las topologías de anillo se utilizaban en las antiguas redes de interfaz de datos distribuida por fibra (FDDI). Específicamente, las redes FDDI emplean un segundo anillo para la tolerancia a fallas o para mejorar el rendimiento.

Figura 15

Topología de anillo

Nota. Fue bien utilizada en las antiguas redes, en Interfaz Datos Distribuidos por Fibra (FDDI)

6.5. Red de Área Local Virtual (VLAN)

El rendimiento de la red es un factor importante en la productividad de una institución o organización. Una de las tecnologías que contribuyen a mejorar el rendimiento de la red es la división de los grandes dominios de difusión en dominios más pequeños. Por una cuestión de diseño, los equipos de redes, como los routers bloquean el tráfico de difusión en una interfaz. Sin embargo, los routers generalmente tienen una cantidad limitada de interfaz LAN. La función principal de un router es trasladar información entre las redes, no proporcionar acceso a la red a las terminales.

La función de proporcionar acceso a una LAN suele reservarse para los switches de capa de acceso. Se puede crear una red de área local virtual (VLAN) en un switch de capa 2 para reducir el tamaño de los dominios de difusión, similares a los dispositivos de capa 3. Por lo general, las VLAN se incorporan al diseño de red para facilitar que una red de soporte a los objetivos de una institución o organización. Si bien las VLAN se utilizan principalmente dentro de las redes de área local conmutadas, las implementaciones modernas de las VLAN les permiten abarcar redes MAN y WAN.

6.5.1. Segmentación de VLAN

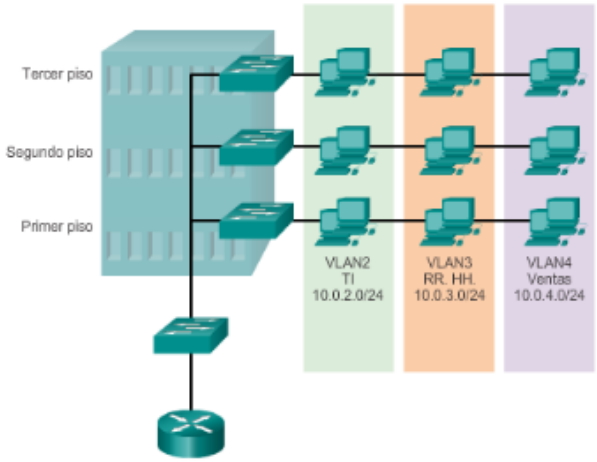
Dentro de un entorno de internetwork conmutada, las VLAN proporcionan la segmentación y la flexibilidad organizativa. Las VLAn proporcionan una manera de agrupar dispositivos dentro de una LAN. Un grupo de dispositivos dentro de una VLAN se comunica como si estuvieran

conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas.

Una VLAN crea un dominio de difusión lógico que puede abarcar varios segmentos LAN físicos. Las VLAN mejoran el rendimiento de la red mediante la división de grandes dominios de difusión en otros más pequeños. Si un dispositivo en una VLAN envía una trama de Ethernet de difusión, todos los dispositivos en la VLAN reciben la trama, pero los dispositivos en otras VLAN no la reciben.

Figura 16

Segmentación de VLAN



Nota. Definición de grupos de VLAN

6.5.2. VLAN de datos

Una VLAN de datos es una VLAN configurada para transportar tráfico generado por usuarios. Una VLAN que transporta tráfico de administración o de voz no sería una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. A veces a una VLAN de datos se le denomina VLAN de usuarios. Las VLAN de datos se usan para dividir la red en grupos de usuarios o dispositivos.

6.5.3. VLAN predeterminada

De manera técnica, todos los puertos de switch se vuelven parte de la VLAN predeterminada después del arranque inicial de un switch que carga la configuración predeterminada. Los puertos de switch que participan en la VLAN predeterminada forman parte del mismo dominio de difusión. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch.

6.5.4. VLAN nativa

Las VLAN nativas se definen en la especificación IEE 802.1Q a fin de mantener la compatibilidad con el tráfico sin etiquetar de modelos anteriores común a las situaciones de LAN antiguas. Una VLAN nativa funciona como identificador común en extremos opuestos de un enlace troncal.

6.5.5. VLAN de administración

Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch.

6.6. Protocolos de Enrutamientos

Para que un dispositivo de capa tres pueda determinar la ruta hacia un destino debe tener conocimiento de las diferentes rutas hacia él y cómo hacerlo. El aprendizaje y la determinación de estas rutas se lleva a cabo mediante un proceso de enrutamiento dinámico a través de cálculos y algoritmos que se ejecutan en la red o enrutamiento estático ejecutado manualmente por el administrador o incluso ambos métodos.

La información de enrutamiento que un equipo de red (router) aprende desde sus fuentes se coloca en su propia tabla de enrutamiento. El router se vale de esta tabla para determinar los puertos de salida que debe utilizar para retransmitir un paquete hasta su destino.

La tabla de enrutamiento es la fuente principal de información del router acerca de las redes. Si la red de destino está conectada directamente, el router sabrá de antemano el puerto que debe usar para reenviar paquetes. Si las redes de destino no están conectadas directamente, el rotuer debe aprender y calcular la ruta óptima a usar para reenviar paquetes a dichas redes. La tabla de enrutamiento se constituye mediante uno de estos dos métodos o ambos:

6.6.1. Rutas estáticas

Aprendidas por el router a través del administrador, que establece dicha ruta manualmente, quien también debe actualizar cuando tenga lugar un cambio en la topología.

6.6.2. Rutas dinámicas

Rutas aprendidas automáticamente por el router a través de la información enviada por otro rotuers, una vez que el administrador ha configurado un protocolo de enrutamiento que permite el aprendizaje dinámico de rutas.

6.6.3. Distancia administrativa

Los routers son multiprotocolos, lo que quiere decir que pueden utilizar al mismo tiempo diferentes protocolos incluidas rutas estáticas. Si varios protocolos proporcionan la misma información de enrutamiento se les debe otorgar un valor administrativo. La distancia administrativa permite que un protocolo tenga mayor prioridad sobre otro si su distancia administrativa es menor. Este valor viene por defecto, sin embargo, el administrador puede configurar un valor diferente si así lo determina.

Tabla 3

Rango de la distancia administrativa.

Interfaz física	0
Ruta estática	1
Ruta sumaizada EIGRP	5

BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200
Inalcanzable	255

Nota. Valor predeterminado de la distancia administrativa de los protocolos de enrutamientos, que va del 1 a 255.

6.6.4. Enrutamiento estático

Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador.

Las rutas estáticas por defecto (default) especifican una puerta de enlace (Gateway) de último recurso, a la que el router debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir que desconoce.

Las rutas estáticas se utilizan habitualmente en enrutamientos desde una red hasta una red de conexión única, ya que no existe más que una ruta de entrada y salida en una red de conexión única, evitando de este modo la sobrecarga de tráfico que genera un protocolo de enrutamiento.

6.6.5. Enrutamiento dinámico

Los cambios que una red puede experimentar hacen poco factible la utilización de rutas estáticas, el administrador se vería forzado a reconfigurar los routers ante cada cambio. El enrutamiento dinámico permite que los routers actualicen conocimientos ante posibles cambios sin tener que recurrir a nuevas configuraciones. Un protocolo de enrutamiento permite determinar dinámicamente las rutas y mantener actualizadas sus tablas.

Es importante diferencia los protocolos enrutados y los de enrutamiento. Un protocolo enrutado lleva una completa información de capa tres, como TCP/IP, IPX, APPLE TALK, Net BEUI. Un protocolo de enrutamiento es el utilizado por los routers para mantener tablas de enrutamiento y así poder elegir la mejor ruta hacia un destino.

Existen dos grandes núcleos de protocolos de enrutamiento:

Protocolo de Gateway interior (IGP): Se usan para intercambiar información de enrutamiento dentro de un sistema autónomo (AS). (RIP, EIRGRP, OSPF).

Protocolo de Gateway exterior (EGP): Se usan para intercambiar información de enrutamiento entre sistemas autónomos (AS). (BGP).

6.6.6. Enrutamiento vector distancia

Los algoritmos de enrutamiento basados en vectores pasan copias periódicas de una tabla de enrutamiento de un rotuer a otro y acumulan vectores de distancia. Distancia es una medida de

longitud, mientras que vector significa una dirección. Las actualizaciones regulares entre routers comunican los cambios en la topología. Cada protocolo de enrutamiento basado en vectores de distancia utiliza un algoritmo distinto para determinar la ruta óptima. El algoritmo genera un número, denominado métrica de ruta, para cada ruta existente a través de la red. Normalmente cuanto menor es este valor, mejor es la ruta.

Los dos ejemplos típicos de protocolos por vector distancia son:

RIP (Routing Information Protocol). Protocolo suministrado con los sistemas UNIX. Es el protocolo de Gateway interior (IGP) más comúnmente utilizado. RIP utiliza el número de saltos como métrica de enrutamiento. Existen dos versiones. Rip v1 como protocolo tipo Classfull y RIP v2, más completo que su antecesor, como protocolo classless.

IGRP (Interior Gateway Routing Procol). Protocolo desarrollado para tartar los problemas asociados con el enrutamiento en redes de gran envergadura. IGRP es un protocolo tipo classfull.

6.7. Dispositivos de Red Intermedio

Los dispositivos intermediarios interconectan dispositivos finales. Estos dispositivos proporcionan conectividad y operan detrás de escena para asegurar que los datos fluyan a través de la red. Los dispositivos intermediarios conectan los hosts individuales a la red y pueden conectar varias redes individuales para formar una internetwork.

Los siguiente son ejemplos de dispositivos de red intermediarios:

- Acceso a la red (Switches y puntos de acceso inalambrico)
- Internetworking (routers)
- Seguridad (firewalls)

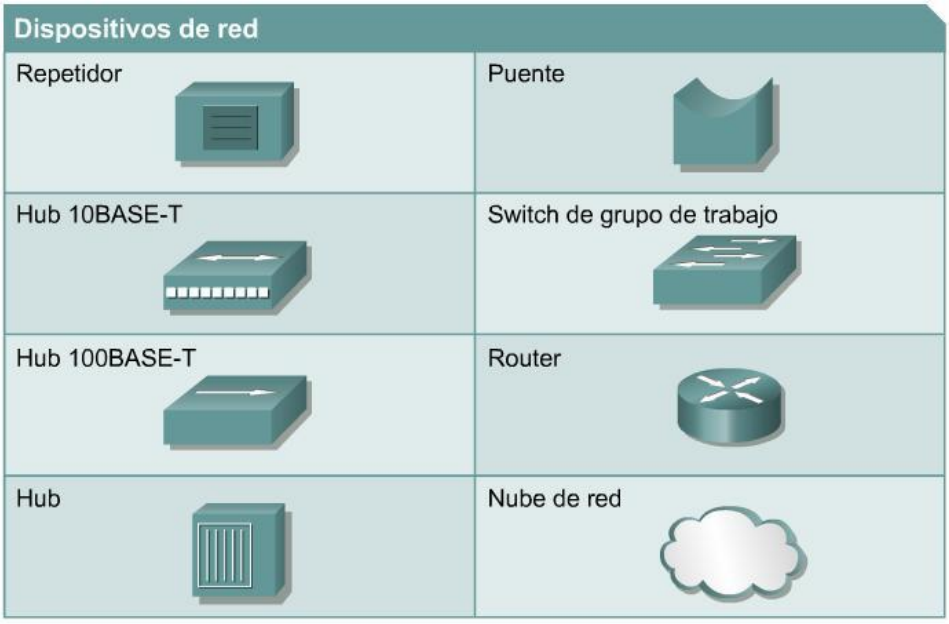
La administración de datos, así como fluye en la red, es también una función de los dispositivos intermediarios. Estos dispositivos utilizan la dirección host de destino, conjuntamente con información sobre las interconexiones de la red para determinar la ruta que deben tomar los mensajes a través de la red.

Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones:

- Volver a generar y transmitir las señales de datos.
- Conservar información acerca de las rutas que existen a través de la red y de internetwork.
- Notificar a otros dispositivos los errores y las fallas de comunicación.
- Clasificar y dirigir los mensajes según las prioridades de calidad de servicio (QoS, Quality of Service).
- Permitir o denegar el flujo de datos de acuerdo con la configuración de seguridad.

Figura 17

Dispositivos de red intermediarios



Nota. Simbología de los dispositivos de red intermediario, para

6.8. Medios Inalámbricos

Los medios inalámbricos transportan señales electromagnéticas mediante frecuencias de microondas y radiofrecuencias que representan los dígitos binarios de las comunicaciones de datos. Como medio en sí mismo, el sistema inalámbrico no se limita a condiciones físicas, como en el caso de los medios de fibra o de cobre. Sin embargo, el medio inalámbrico es susceptible a la interferencia y puede distorsionarse por dispositivos comunes como teléfonos inalámbricos domésticos, algunos tipos de luces fluorescentes, hornos microondas y otras comunicaciones inalámbricas.

Los estándares IEEE sobre las comunicaciones inalámbricas abarcan las capas físicas y de enlace de datos. Los cuatro estándares comunes de comunicación de datos que se aplican a los medios inalámbricos son:

- ***IEEE estándar 802.11:*** comúnmente denominada Wi-Fi, se trata de una tecnología LAN inalámbrica (red de área local inalámbrica, WLAN) que utiliza una contención o sistema no determinista con un proceso de acceso a los medios de Acceso múltiple con detección de portadora/Prevención de colisiones (CSMA/CA).

- ***IEEE estándar 802.15:*** estándar de red de área personal inalámbrica (WPAN), comúnmente denominada Bluetooth, utiliza un proceso de emparejamiento de dispositivos para comunicarse a través de una distancia de 1 a 100 metros.

- ***IEEE estándar 802.16:*** comúnmente conocida como WiMAX (Worldwide Interoperability for Microwave Access), utiliza una topología punto a multipunto para proporcionar un acceso de ancho de banda inalámbrico en una extensa cobertura.

- ***Sistema global para comunicaciones móviles (GSM):*** incluye las especificaciones de la capa física que habilitan la implementación del protocolo Servicio general de radio por paquetes (GPRS) de capa 2 para proporcionar la transferencia de datos a través de redes de telefonía celular móvil.

6.9.Internet

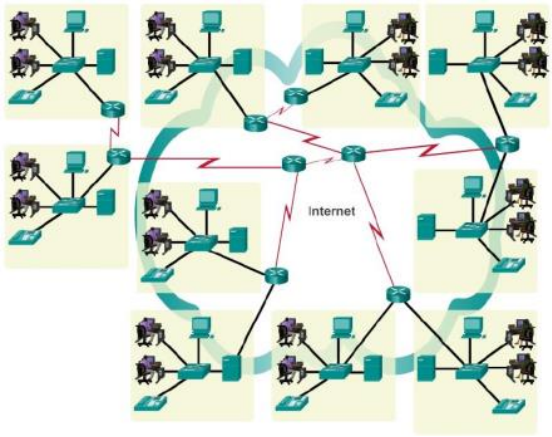
Es una colección mundial de redes interconectadas (abreviado: internetworks o internet), que colaboran para intercambiar información sobre la base de estándares comunes. A través de

cables telefónicos, cables de fibra óptica, transmisiones inalámbricas y enlaces satelitales, los usuarios de Internet pueden intercambiar información de diversas formas.

Internet es un conglomerado de redes que no es propiedad de ninguna persona ni de ningún grupo. Para garantizar una comunicación eficaz en esta infraestructura heterogénea, se requiere la aplicación de tecnologías y estándares coherentes y comúnmente reconocidos, así como la cooperación de muchas entidades de administración de redes. Existen organizaciones que se desarrollaron con el fin de ayudar a mantener la estructura y la estandarización de los protocolos y los procesos de Internet. Entre estas organizaciones, se encuentran Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN) e Internet Architecture Board (IAB), entre muchas otras.

Figura 18

Topología de conexión a Internet



Nota. Las redes LAN, conectadas a la WAN y con salida a Internet.

6.10. Intranet

se suele utilizar para hacer referencia a una conexión privada de redes LAN y WAN que pertenece a una organización y que está diseñada para que solo accedan a ella los miembros y los

empleados de la organización u otras personas autorizadas. Básicamente, las intranets son internets a la que solamente se puede acceder desde dentro de la organización.

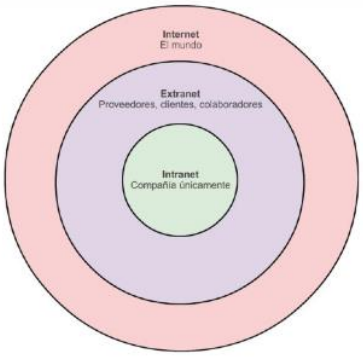
6.11. Extranets

Es posible que una organización utilice una extranet para proporcionar acceso seguro a las personas que trabajan para otra organización, pero requieren datos de la compañía. Entre los ejemplos de extranets, se incluyen los siguientes:

- Una compañía que proporciona acceso a proveedores y contratistas externos.
- Un hospital que cuenta con un sistema de registro para que los médicos puedan cargar citas con sus pacientes.
- Una secretaría de educación local que proporciona información sobre presupuesto y personal a las escuelas del distrito.

Figura 19

El Intranet.



Nota. Diseño del funcionamiento de la Intranet.

6.12. Virtualización

Los servicios en la nube y la virtualización se utilizan generalmente como sinónimos sin embargo, significan cosas diferentes. Mientras que los servicios en la nube separan la aplicación del hardware, la virtualización separa el sistema operativo (OS) del hardware.

a virtualización es el fundamento del funcionamiento en la nube. Varios proveedores ofrecen servicios en la nube virtual que puede aprovisionar servidores dinámicamente según sea necesario.Un servidor físico, Host, tiene un alto poder de procesamiento. Un Host puede almacenar varias máquinas virtuales VM (Virtual Machine).

6.12.1. Virtualización de la Red

Las dos principales arquitecturas de red desarrolladas para soportar la virtualización de la red son las siguientes:

- SDN (Software Defined Networking) una arquitectura de red que permite virtualizar la red.
- ACI (Cisco Application Centric Infrastructure) una solución de hardware especialmente diseñado para integrar los procesos en nube y la gestión del centro de datos.

Las siguientes son otras tecnologías de virtualización de red, algunos de los cuales están incluidos como componentes en SDN y ACI:

- OpenFlow, desarrollado en la Universidad de Stanford para gestionar el tráfico entre los routers, switches, puntos de acceso inalámbrico y un controlador.
- OpenStack, utilizado comúnmente por Cisco ACI. Es el proceso de automatizar el aprovisionamiento de componentes de red.

6.12.2. Virtualización de Servidores.

La virtualización de servidores se utiliza para enmascarar los recursos de los servidores ante sus usuarios. Esto puede incluir el número y la identidad de los sistemas operativos, los procesadores y los servidores físicos individuales.

La virtualización de servidores es el proceso de dividir un servidor físico en múltiples servidores virtuales únicos y aislados por medio de una aplicación de software. Cada servidor virtual puede ejecutar sus propios sistemas operativos de manera independiente.

6.13. Servidores

Los servidores son hosts con software instalado que les permite proporcionar información, por ejemplo, correo electrónico o páginas Web, a otros hosts de la red. Cada servicio requiere un software de servidor diferente. Por ejemplo, para proporcionar servicios Web a la red, un host necesita un software de servidor Web.

6.14. Tipos de servidores

Existen diferente tipos de servidores, para ejecutar los servicios

DHCP (Protocolo de Configuración Dinámica de Host)

Es un método para asignar direcciones IP en forma automática a clientes de red. Puede configurar su Firebox como un servidor DHCP para las redes que protege. Si tiene un servidor DHCP, recomendamos que continúe usando ese servidor para DHCP.

DNS (Sistema de Nombre de Dominio)

Es una red de servidores que traducen direcciones IP numéricas en direcciones de Internet legibles, y viceversa. El DNS toma el nombre de dominio amistoso que ingresa cuando desea ver

un sitio web en particular, como www.example.com, y encuentra la dirección IP equivalente, como 203.0.113.2. Los dispositivos de red necesitan la dirección IP real para encontrar el sitio web, pero los nombres de dominio son más fáciles de ingresar y recordar para los usuarios que las direcciones IP.

Servidor WEB

es aquel servidor instalado en un equipo determinado con el fin de trabajar offline y online. Es una alternativa especialmente útil si lo que buscamos es un entorno en el que desarrollar un sitio web o una aplicación y que nos permita realizar todo tipo de pruebas sin correr riesgos.

Servidor de Correo

Un servidor de correo es una aplicación informática que permite gestionar el correo electrónico en un ordenador o computadora.

Active Directory Domain Services (AD DS)

Es una infraestructura jerárquica que almacena información sobre objetos en la red. Un servicio de directorio, como servicio de dominio de Active Directory (AD DS), proporciona los métodos para almacenar datos de directorio y poner estos datos a disposición de los usuarios y administradores de la red.

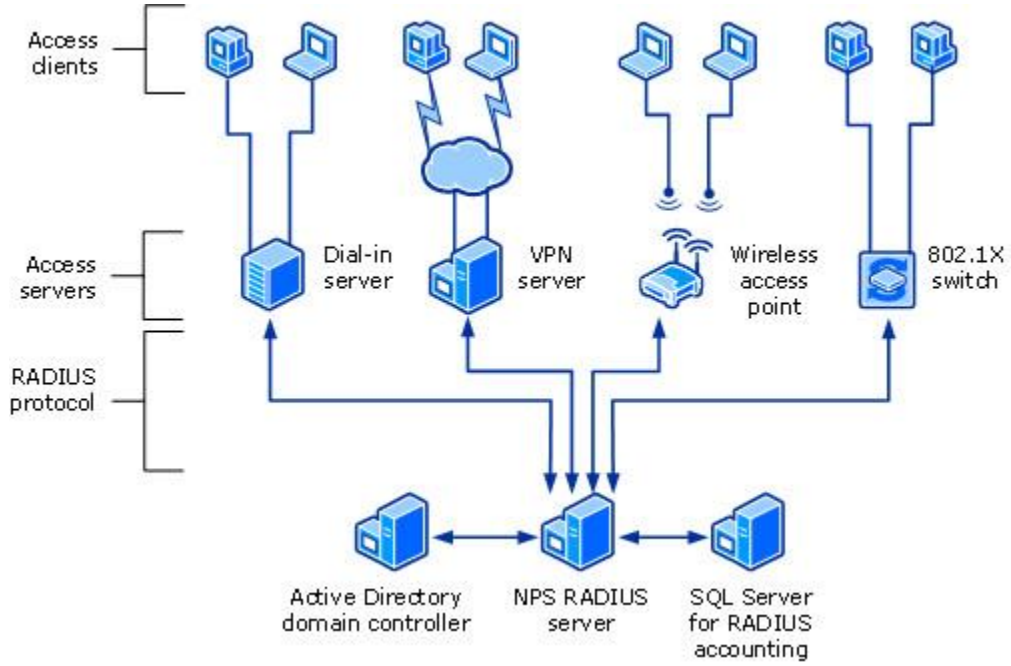
Para aplicar un AD DS en la institución y asegurar la información, se recomienda integrarlo con servidor de directivas de red (NPS), haciendo uso de la autenticación de inicio de sesión y el control de acceso a los objetos del directivo.

Servidor de directivas de red (NPS)

Permite crear y aplicar directivas de acceso de red en toda la organización para la autenticación y autorización de solicitudes de conexión. Esto permitirá que sea configurado y administrado de forma centralizada la autenticación, autorización y contabilidad de acceso a la red.

Figura 20

Administración de un servidor NPS



Nota. Administración de los hosts, por medo de políticas y en conjunto con el AD.

6.15. Seguridad de Red

Los ataques contra infraestructura informática ya sean simples o complejas, han existido siempre que lo han hecho los equipos. No obstante, durante la última década, una cantidad creciente de organizaciones de todos los tamaños y de todas las partes del mundo han sido atacadas

y puestas en peligro de maneras que han cambiado significativamente el panorama de las amenazas.

Para proteger las computadoras y servidores individuales conectados a la red de la institución, es importante controlar el tráfico de entrada y de salida de la red. A través de:

6.15.1. Firewall

Que es una de las herramientas de seguridad más eficaces disponibles para la protección de los usuarios internos de la red contra amenazas externas. El firewall reside entre dos o más redes y controla el tráfico entre ellas, además de evitar el acceso no autorizado. Los productos de firewall usan diferentes técnicas para determinar qué acceso permitir y qué acceso denegar en una red. Estas técnicas son las siguientes:

- Filtrado de paquetes: evita o permite el acceso según las direcciones IP o MAC.
- Filtrado de aplicaciones: evita o permite el acceso de tipos específicos de aplicaciones según los números de puerto.
- Filtrado de URL: evita o permite el acceso a sitios Web según palabras clave o URL específicos.
- Inspección de paquetes con estado (SPI): los paquetes entrantes deben constituir respuestas legítimas a solicitudes de los hosts internos. Los paquetes no solicitados son bloqueados, a menos que se permitan específicamente. La SPI también puede incluir la capacidad de reconocer y filtrar tipos específicos de ataques, como los ataques por denegación de servicio (DoS).

Los productos de firewall pueden admitir una o más de estas capacidades de filtrado. Además, los firewalls suelen llevar a cabo la traducción de direcciones de red (NAT). La NAT traduce una dirección o un grupo de direcciones IP internas a una dirección IP pública y externa

que se envía a través de la red. Esto permite ocultar las direcciones IP internas de los usuarios externos. A como se refleja en el Anexo #7 y Anexo #9.

Figura 21

Equipos de seguridad

Nota. Diferentes equipos de seguridad, para proteger la red.

Firewalls basados en aplicaciones

Un firewall basado en una aplicación es un firewall incorporado en un dispositivo de hardware dedicado, conocido como una aplicación de seguridad.

Firewalls basados en servidor: un firewall basado en servidor consta de una aplicación de firewall que se ejecuta en un sistema operativo de red (NOS), como UNIX o Windows.

Firewalls integrados

Un firewall integrado se implementa mediante la adición de funcionalidades de firewall a un dispositivo existente, como un router.

Firewalls personales

Los firewalls personales residen en las computadoras host y no están diseñados para implementaciones LAN. Pueden estar disponibles de manera predeterminada en el OS o pueden provenir de un proveedor externo.

Cada servicio de Internet que se utiliza o preste, existe riesgo para el sistema y para la red a la que está conectado. Para prevenir riesgo por parte usuarios internos o externos, lo recomendable es realizar Políticas de seguridad.

Las Políticas de seguridad es un conjunto de reglas que se aplican a las actividades del sistema y a los recursos de comunicaciones que pertenecen a una institución. Esta reblas incluyen áreas como la seguridad Física, personal, administrativa y de la red, se comparte una imagen de política de seguridad aplicada en el Nexo #3,

Los objetivos de seguridad son cuando cree y desarrolle una política, debería tener claro los objetivos de la gestión de la red, para aplicar las políticas de seguridad.

6.16. Ancho de Banda.

Los diferentes medios físicos admiten la transferencia de bits a distintas velocidades. Por lo general, la transferencia de datos se analiza en términos de ancho de banda y rendimiento.

El ancho de banda es la capacidad de un medio para transportar datos. El ancho de banda digital mide la cantidad de datos que pueden fluir desde un lugar hasta otro en un período determinado. El ancho de banda generalmente se mide en kilobits por segundo (kb/s) o megabits por segundo (Mb/s).

El ancho de banda práctico de una red se determina mediante una combinación de factores:

- Las propiedades de los medios físicos
- Las tecnologías seleccionadas para la señalización y la detección de señales de red

Las propiedades de los medios físicos, las tecnologías actuales y las leyes de la física desempeñan una función al momento de determinar el ancho de banda disponible.

Tabla 4

Unidad de medida

Unidad de ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1bps=unidad fundamental de ancho de banda
Kilobits por segundo	kbps	1kbps=1000bps = 10^3bps
Megabits per second, megabits por segundo	Mbps	1Mbps =1000000bps=10^6bps
Gigabits per second, gigabits por segundo	Gbps	1Gbps=1000000000bps=10^9bps
Terabits per second, terabits por segundo	Tbps	1Tbps=1000000000000bps=10^12bps

Nota. Las unidades de medidas, del ancho de banda que se llegue a utilizar en una Red.

6.17. Dispositivos Finales

Los dispositivos de red con los que las personas están más familiarizadas se denominan "dispositivos finales" o "hosts". Estos dispositivos forman la interfaz entre los usuarios y la red de comunicación subyacente.

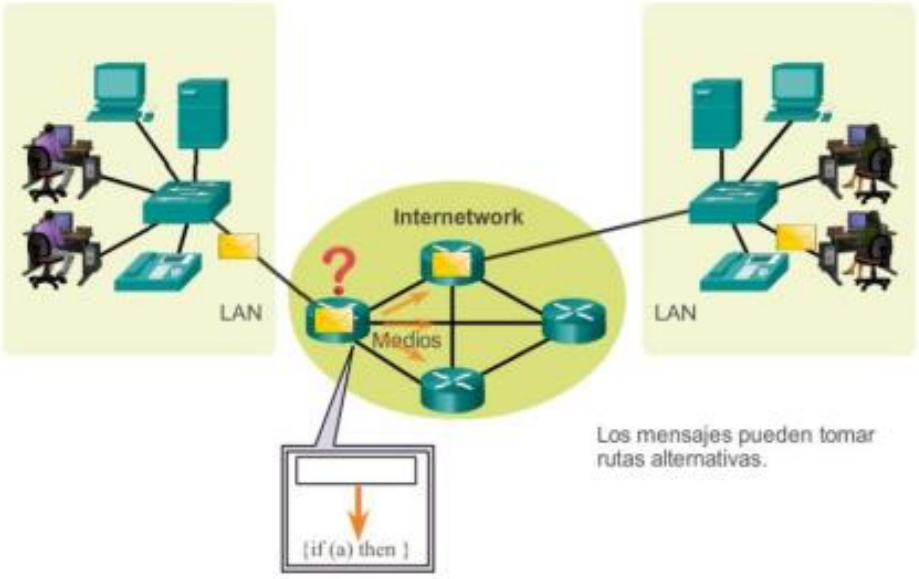
Algunos ejemplos de dispositivos finales son:

- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web)
- Impresoras de red
- Teléfonos VoIP
- Terminales de TelePresence
- Cámaras de seguridad
- Dispositivos portátiles móviles (como smartphones, tablet PC, PDA y lectores inalámbricos de tarjetas de débito y crédito, y escáneres de códigos de barras).

Un dispositivo host es el origen o el destino de un mensaje transmitido a través de la red, tal como se muestra en la animación. Para distinguir un host de otro, cada host en la red se identifica por una dirección. Cuando un host inicia la comunicación, utiliza la dirección del host de destino para especificar a dónde se debe enviar el mensaje.

Figura 22

Dispositivos finales (hosts)



Nota. Dispositivos finales que se conectan a la red LAN y ejecutar los servicios que corren en la red.

7. Estudio de Factibilidad

Según Varela “Se entiende posibilidades las posibilidades que tiene de lograrse un determinado proyecto”. El estudio de factibilidad es el análisis que realiza una empresa para determinar si el negocio que se propone será bueno o malo, y cuáles serán las estrategias que se deben desarrollar para que sea exitoso.

Según el diccionario de la Real Academia Española, la Factibilidad es la “cualidad o condición de factible”. Factible: “que se puede hacer”.

7.1.El servicio es Factible

Operativamente

Porque serán adaptado a los servicios que brinda la institución y se cumple con un personal que puede gestionar o administrar dicha los equipos de redes de acceso, de seguridad y servidores.

Técnicamente

La institución cuenta con el personal técnico para la implementación de la infraestructura, respondiendo de manera favorable y eficiente para el desarrollo del proyecto que tendría planificado.

Tabla 5

Estudio Económico

No	Descripción	Cantidad	Costo Unitario	Total
1	Switch 48puerto POE	5.00	C$155,160.00	C$775,800.00
2	SWitch 24puerto POE	3.00	C$77,580.00	C$232,740.00
3	AP	20.00	C$21,924.00	C$438,480.00
4	Licencia cloud AP	20.00	C$12,312.00	C$246,240.00
5	Firewall	1.00	C$150,601.00	C$150,601.00
6	Servicios de instalación y configuración	1.00	C$35,000.00	C$35,000.00
7			Monto total	**C$1,878,861.00**

Nota. Estudio económico para la adquisición de los equipos de red y seguridad.

8. Hipótesis o Preguntas Directrices

¿Qué es una RED?

¿Cómo funciona una red?

¿Qué son los dispositivos de redes?

¿Cuáles son los dispositivos de redes?

¿Cómo funciona las redes virtuales?

¿Quién administra las redes virtuales y equipos de redes?

¿Que son los servicios de red?

¿Cómo funciona la seguridad de red?

¿Cómo esta segmentadas las redes?

¿Cómo funciona la red inalámbrica?

9. Diseños Metodológico

9.1.Metodología

9.1.1. Tipos de Investigación

Esta tesis está basada en el análisis y restructuración de la red de datos para que se le brinde los servicios del internet e intranet a las direcciones del CNU.

El presente trabajo es del tipo de investigación Básica-Aplicativa, que consiste en analizar las diferentes teorías de investigación y aplicarlas en la infraestructura de red del CNU.

"La investigación básica denominada también pura o fundamental, busca el progreso científico, acrecentar los conocimientos teóricos, sin interesarse directamente en sus posibles aplicaciones o consecuencias prácticas; es más formal y persigue las generalizaciones cambistas al desarrollo de una teoría basada en principios y leyes. Zorrilla (1993)

La investigación aplicada, guarda íntima relación con la básica, pues depende de los descubrimientos y avances de la investigación básica y se enriquece con ellos, pero se caracteriza por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos. La investigación aplicada busca el conocer para hacer, para actuar, para construir, para modificar. Zorrilla (1993)

9.1.2. Método de Investigación

El método de investigación a utilizar será Analítica que es aquel método de investigación que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método nos permite conocer más del objeto de estudio, con lo cual se

puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías. Zorrilla (1993).

9.1.3. Técnicas e instrumentos de Recolección de Datos.

Se utilizó la técnica de observación directa. Que se desarrolló a través de la observación del funcionamiento de la red de datos del CNU.

9.1.4. Universo, Muestra de estudio y Muestreo.

El **universo** red de datos.

La **muestra** red de datos del CNU.

9.1.5. Diseño de la investigación.

El diseño de la investigación está comprendido por fases de ejecución entregables, que se muestran a continuación:

Fase 1. Recolección de la información

- Recolectar información sobre la red del CNU.
- Identificar los requerimientos de la red.
- Recursos disponibles en el CNU

Fase 2. Análisis de la información

- Analizar la información recolectada de la red de datos del CNU, diseñar una topología lógica y segmentar la red en redes virtuales.
- Analizar los requerimientos para la red de datos y hacer una restructuración en la red, con los protocolos y el tipo de clase de direccionamiento IP.
- Definir las aplicaciones a utilizar para el diseño de topología lógica, configuración e implementación de la red de datos del CNU

Fase 3. Diseño y Configuración

- Diseñar la topología lógica de la red de datos
- Diseño de la segmentación de la red de datos.
- Diseño e implementación de la configuración de los equipos de redes para la red de datos.

Fase 4. Implementación

- Pruebas de la configuración de la red de datos del CNU

10. Resultados

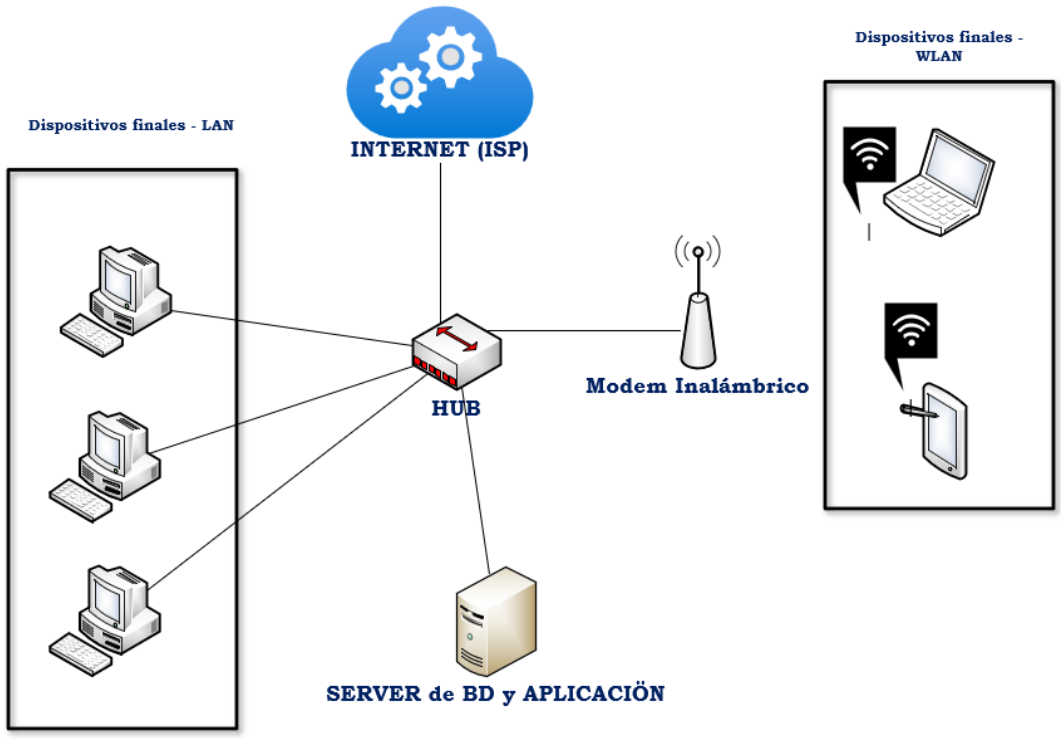
Una vez recolectada la información, identificar los requerimientos y los recursos disponible (Fase 1. Recolección de la información), se identificó que la red no estaba segura y había saturación en el ancho de banda, esto es debido a la repetición masiva de los datos por el hub (concentrador). En la Figura #1 se muestra la topología de la red.

Analizando los requerimientos del levantamiento (Fase 2 y Fase3), se recomienda realizar un diseño en la red, como un diagrama de topología física, en donde se ilustren los dispositivos de finales, dispositivos intermedios (Red), las conexiones entre los dispositivos y un diagrama de topología lógica, mostrando una red segmentada y segura.

Por lo tanto, es necesario realizar las pruebas (Fase 4.) de conexión, validando y monitoreando el comportamiento de la red, luego de haber aplicado una configuración y tener el acceso a la misma administración, mediante de software o equipo de red, que permita realizar dicho comportamiento.

Figura 23

Topología de red, con un hub



Nota. En la ilustración se observa que el hub envía datos a todos los dispositivos finales o dispositivos de red conectados, eso hace que se gaste excesivamente el ancho de banda.

A como podemos observar en la ***Figura 23,*** el trafico que genera el dispositivo intermediario es aumentar una colisión. Una colisión se denomina al proceso que un ordenador realiza al enviar información a otro ordenador de forma simultánea que se encuentra realizando la misma tarea.

Debido a la conexión a como se muestra en la figura anterior, no se podrían sacar muestra del consumo o que se está ejecutando en la red, porque los dispositivos no soportan el Protocolo d Simple de Administración de Redes (SNMP).

11. Análisis y Discusión de Resultados

A partir de los hallazgos encontrado, en la red del Consejo Nacional de Universidades (CNU), el aumento de las posibles colisiones, que cuando los mensajes se chocan se realiza una perdida y se necesita volver a enviar la información, para que no se lleve a cabo otra colisión, debido a este embotellamiento que pasa en la red, se necesita aplicar un cambio en la infraestructura de red de datos, de manera física y lógica, para obtener una infraestructura robusta, segura y confiable.

11.1. Direcciones IPv4 de la Red del CNU

El Consejo Nacional de universidades (CNU) no contaba con la administración o gestión de direcciones IP privada, el Proveedor de Servicio de Internet (ISP) asignaba una dirección IP privada con la clase C y la más común 192.168.0.1 /24, saliendo a los servicios de Internet por medio de un Network Address Translation (NAT) a como se muestra en la Figura#1 de los resultados y en el anexo #6.

Para una mejor organización en la dirección IP y controlar las entradas y salidas a los servicios de Internet e Intranet, se sugiere que se realice una segmentación en la red lógica, que es el caso del direccionamiento de red IPv4, en este escenario se eligió la clase B y su mascara de red en clase C, como ejemplo de red principal 172.16.0.0 /24, para el segmento privado o Red de Área Local (LAN). Misma es administrada por el área de Tecnología de la Información (TI) del CNU y se encuentra distribuida de la siguiente manera:

Tabla 6

Direccionamiento IPv4, en clase B.

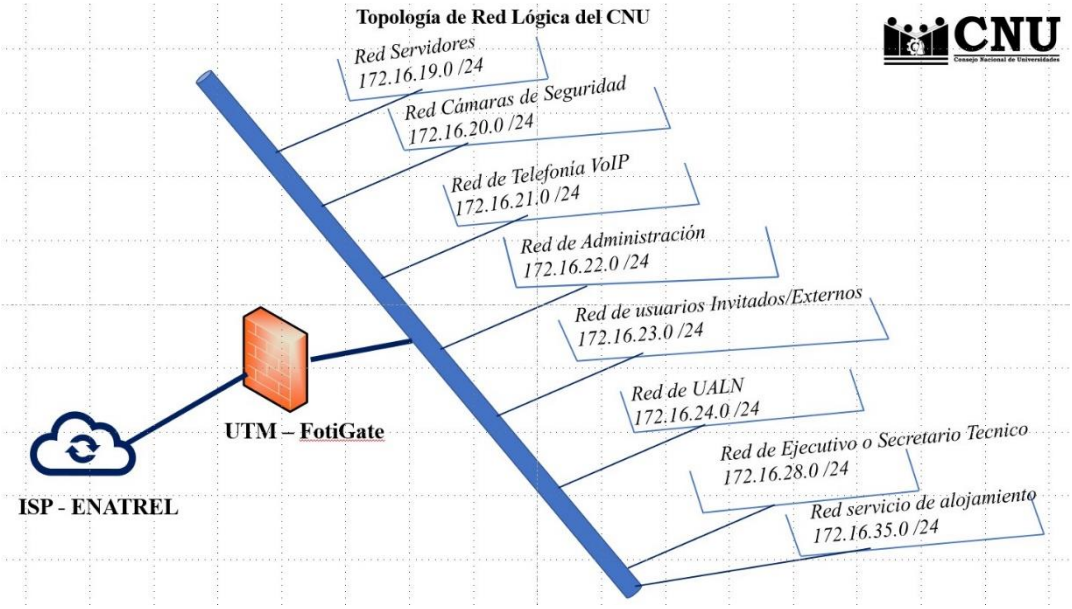
Ítem	Red	Máscara de red	Área/Oficina asignada
1	172.16.19.0	/24 (255.255.255.0)	Servidores
2	172.16.20.0	/24 (255.255.255.0)	Cámaras de seguridad
3	172.16.21.0	/24 (255.255.255.0)	Telefonía VoIP
4	172.16.22.0	/24 (255.255.255.0)	Administración
5	172.16.23.0	/24 (255.255.255.0)	Invitados/usuario externo
6	172.16.24.0	/24 (255.255.255.0)	UALN
7	172.16.26.0	/24 (255.255.255.0)	Nativa, Administración dispositivos de RED
8	172.16.28.0	/24 (255.255.255.0)	Ejecutivos/ST
9	172.16.35.0	/24 (255.255.255.0)	Server alojado, externo

Nota. Direccionamiento IPv4 de clase B, como ejemplo que se utiliza en las direcciones del Consejo Nacional de Universidades (CNU). Informaciones aprobadas por las autoridades del CNU.

En el anexo 1 y 2, se observa de como estaría distribuida la topología de la red segmentada con las direcciones IPv4.

Figura 24

Topología de red Lógica.



Nota. La siguiente figura, se muestra las direcciones IPv4 del CNU, una topología lógica que es administrada y gestionada por el UTM y el switch Core.

Tener una topología lógica, que son las direcciones IPv4, que se utilizan en la institución, nos ayudan a tener una mejor organización en el acceso a los servicios de la institución y así distribuir el ancho de banda a cada dirección asignada a una dirección. De igual manera agiliza a la implementación de asignación de las políticas de seguridad, creándose desde el equipo de seguridad UTM

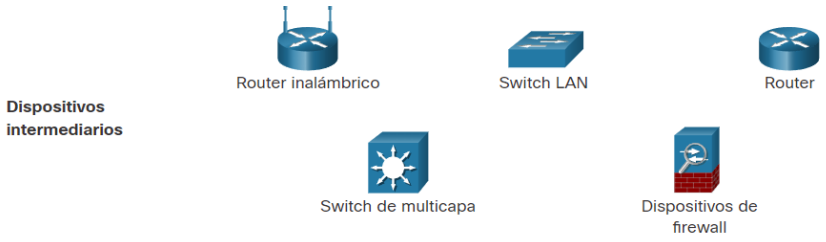
11.2. Dispositivos de intermedio o de redes

Los dispositivos intermedios del CNU conectan los dispositivos finales individuales a la red. Pueden conectar múltiples redes individuales para formar una red interna. Los dispositivos intermedios proporcionan conectividad y garantizan el flujo de datos en toda la red.

Los dispositivos intermedios usan la dirección del dispositivo final de destino, junto con información sobre las interconexiones de la red, para determinar la ruta que los mensajes deben tomar a través de la red.

Figura 25

Dispositivos de red



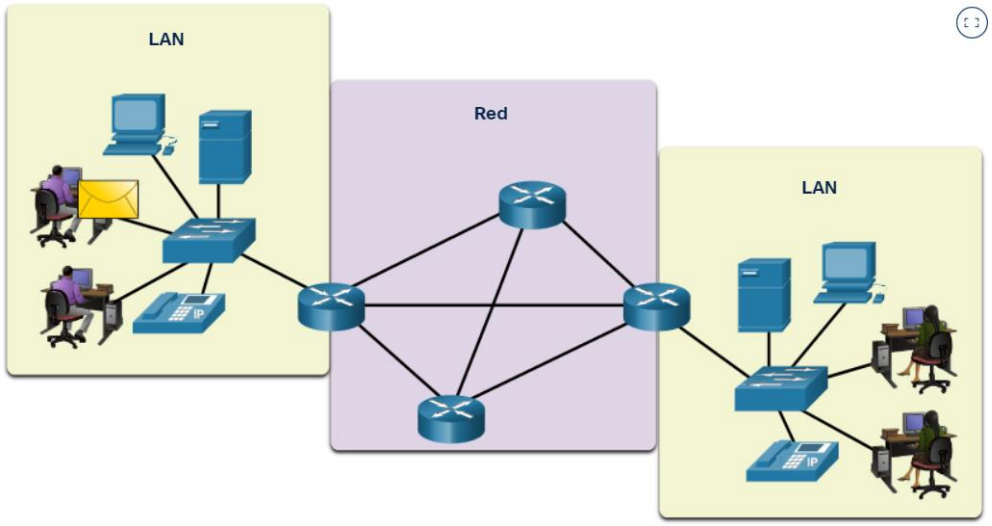
Nota. Dispositivos de red, para interconectar varias redes y se ejecuten los servicios de los hosts.

11.3. Dispositivos Finales

Los dispositivos de red con los que las personas están más familiarizadas se denominan dispositivos finales. Para distinguir un dispositivo final de otro, cada dispositivo final de una red tiene una dirección. Cuando un dispositivo final inicia la comunicación, utiliza la dirección del dispositivo final de destino para especificar dónde entregar el mensaje.

Figura 26

Dispositivos finales en una red LAN



Nota. Un terminal es el origen o el destino de un mensaje transmitido a través de la red.

11.4. Medio de Red

La comunicación en las oficinas del CNU, se transmite a través de una red en los medios. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Cobre

Medio de conexión entre los equipos finales y los equipos de redes, para transportar la información o la data que corre en el cable de cobre, el que se utiliza para este tipos de conexión es el UTP.

Fibra Óptica

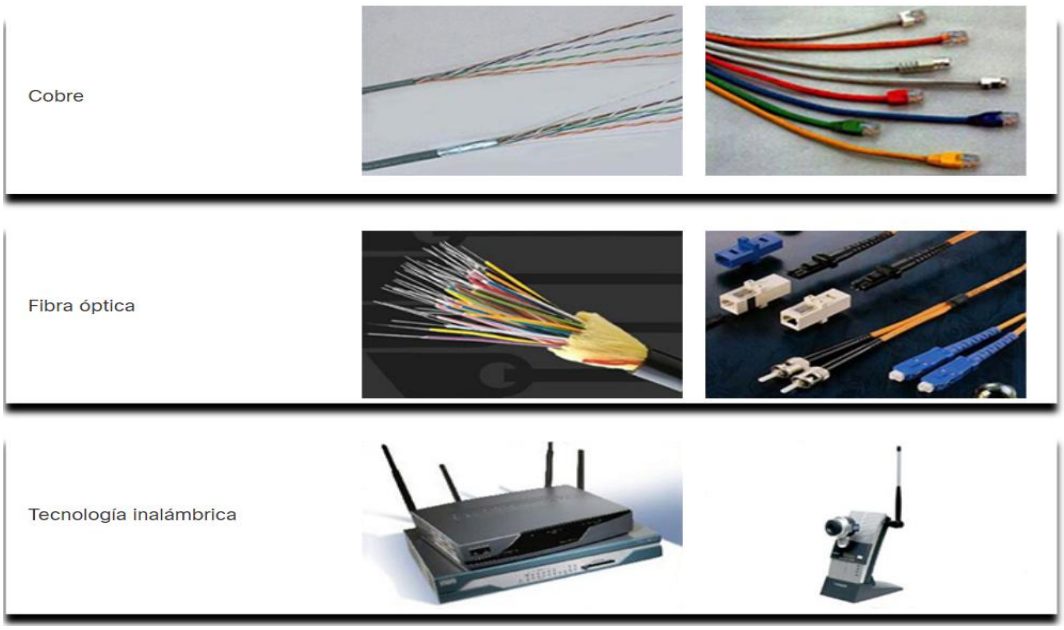
En este medio de comunicación, es utilizado para los servicios de internet y los enlaces de datos, para una mayor de velocidad y distancia entre los equipos que se encuentran a larga distancia.

Inalámbrica

Conexión para los dispositivos que se conectan mediante Wifi y tengan una mejor movilidad en los edificios de la institución o el lugar donde se encuentren y exista cobertura de conexión inalámbrica.

Figura 27

Medios de conexión



Nota. Medios de conexión, para transportar o que corran todos los paquetes de una red. De igual manera interconectar de manera física los equipos de redes.

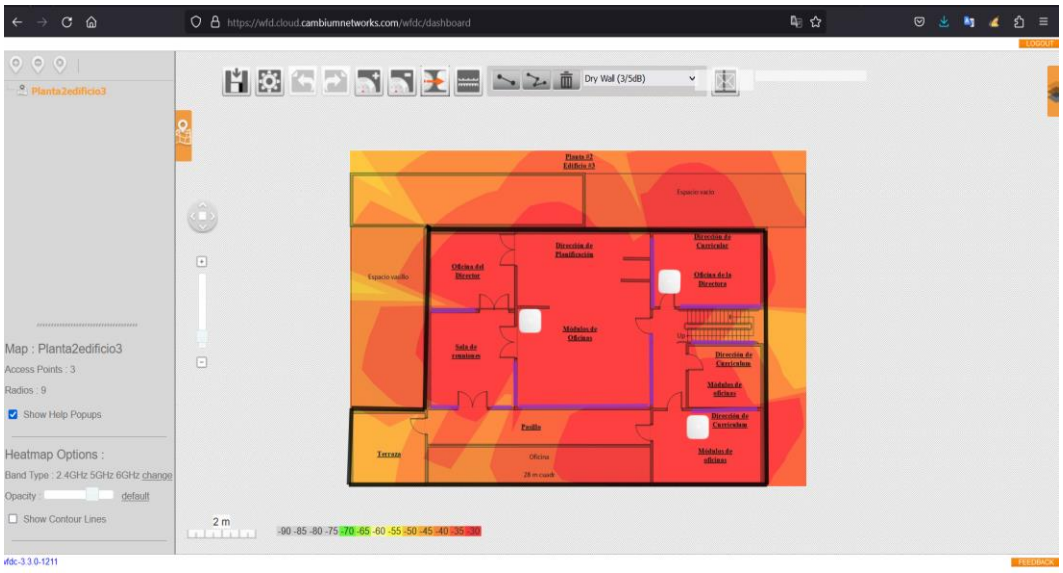
11.5. Herramientas de simulación para redes WAN, LAN y WLAN

Para la instalación de los dispositivos de red y su conexión alámbrica (UTP o FO), para que la red inalámbrica y la red alámbrica no se ralentice, así el tráfico de datos, vos y vídeo se más eficiente y además aprovechar el ancho de banda, el área de tecnología de la información realiza un estudio y una simulación de los equipos de red, en herramientas de simulación para Wifi, las LAN y WAN.

Para una mejor cobertura en redes wifi en las oficinas y en la parte exteriores de los edificios del CNU, se realiza un analices en sitio, con el propósito de saber la cantidad de Puntos de Acceso (AP) a ocuparse.

Figura 28

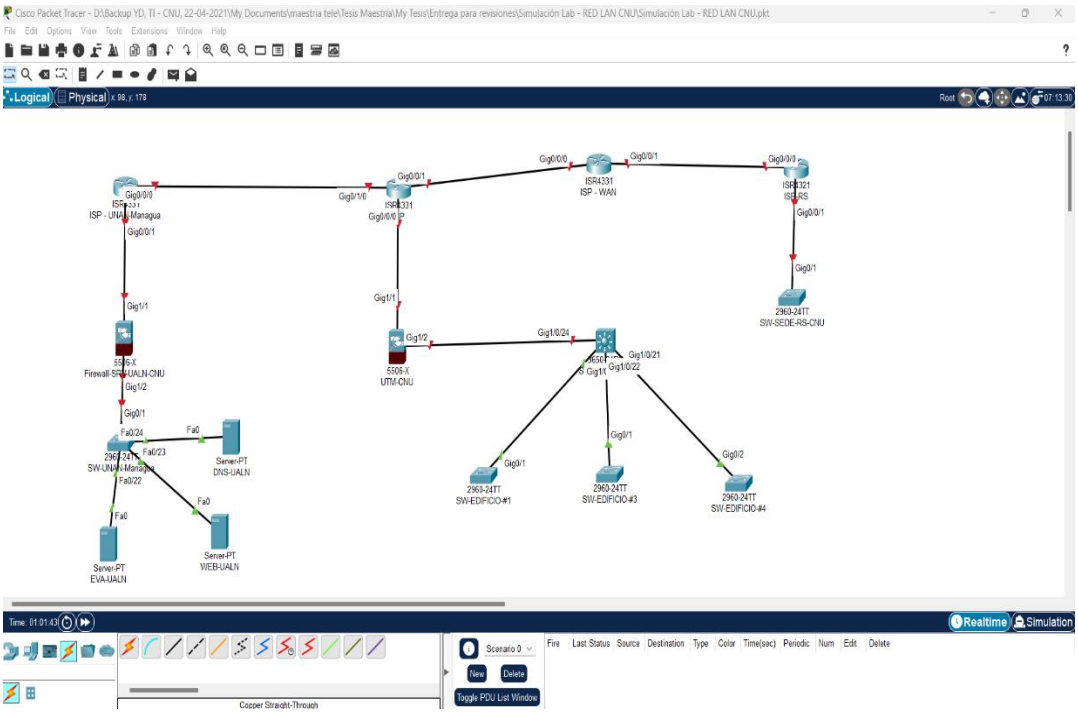
Herramienta de red.



Nota. Herramienta Wifi Designer, para diseño de redes wifi y planos de redes. Laboratorio practico y luego ponerlo en producción.

Figura 29

Herramienta de red.



Nota. Cisco Packt Tracer es un programa de simulación de redes que permite hacer el experimento con los comportamientos de las redes y resolver problemas, antes de hacer configuraciones en los equipos de producción o se encuentran ejecutando.

11.6. Implementación de la IEE 802.11ax

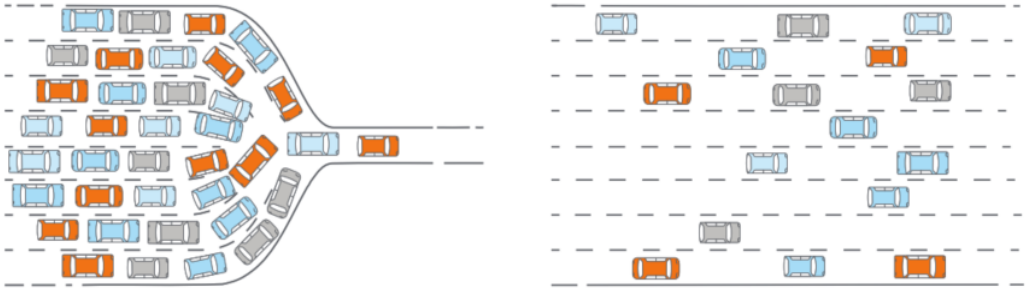
Tener un mejor rendimiento y la creciente densidad de los dispositivos de la institución, además de la diversidad de aplicaciones que se utilizan en el CNU. Parea hacer frente a estos retos, se utilizó el estándar 802.11ax, así tener una característica muy importante, como multiusuario llamado OFDMA (Acceso múltiple por división de frecuencia ortogonales).

Esto quiere decir que múltiples dispositivos con diferentes necesidades de ancho de banda pueden recibir servicios simultáneamente en lugar del modelo anterior que es el estándar 802.11ac.

De igual manera en multiusuario: múltiples entradas/múltiples salidas (MU MIMO) es otra forma de gestionar el trafico de múltiples dispositivos que se introdujo originalmente en 802.11ac. Dentro de 802.11.

Figura 30

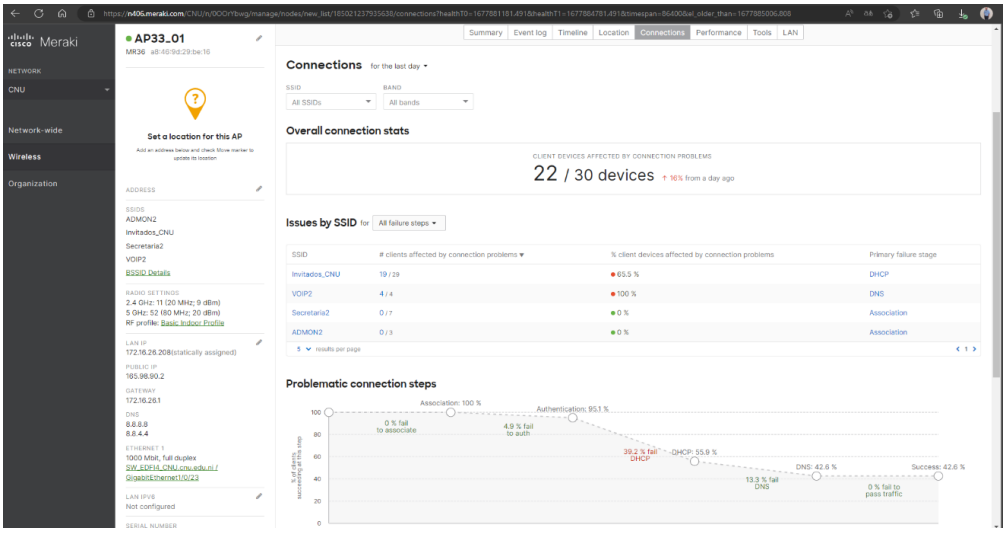
Trafico de red



Nota. En la ilustración o Figura 29, se muestra como sería el tráfico, a la parte izquierda tendremos el 802.11ac y en la parte derecha el 802.11ax.

Figura 31

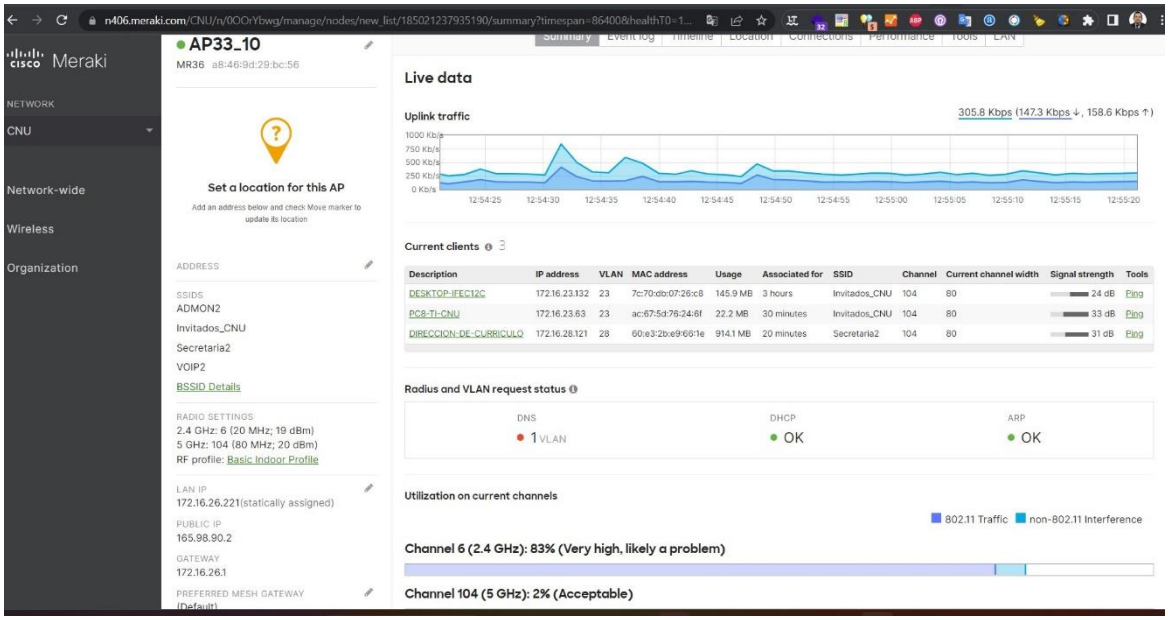
Herramienta de monitoreo.



Nota. Herramienta de monitoreo, para lo puntos de acceso (AP), ver el comportamiento de las redes wifi 6.

Figura 32

Rendimiento de los Acceso conexión Wifi



Nota. En la figura 32, se muestra el rendimiento de los Acces Point (AP) del consumo del ancho de banda.

Con los equipos de acceso de conexión inalámbrica, a como se observa en la figura que son equipos de CISCO y con un modelo MR36, muestran el consumo de los dispositivos o hosts conectado a la red wifi. En el *Dashboard* se observa el ancho de banda subida y bajada del consumo de cada dispositivos, se observa todo el tráfico, en el SSI conectado, la dirección IP que se le brindo y el canal donde se encuentra conectada.

12. Conclusiones

En esta tesis se analizó y restructuro la red de datos del Consejo Nacional de Universidades (CNU) mediante la norma IEEE 802.11ax correspondiente al WIFI 6, la Red de Área Local de la 802.3 (LAN) y aplicando políticas de seguridad para el control de acceso de los usuarios y el monitoreo de la red de entrada y salida. Porque implementaban el acceso a los miembros de la institución, para los servicios de la Intranet.

Se realizó un diagnóstico de la seguridad de la red de datos del CNU en la red de área local (LAN) y la red de área local inalámbrica (WLAN) del CNU para un correcto diseño de la red, creando políticas de seguridad con el equipo de intermedio (Firewall).

Con la identificación de los puntos de acceso (AP) y las pruebas realizadas, se implementó el Modelo de Rendimiento para las redes 802.11ax, que considera la eficiencia y confiabilidad para los hosts o dispositivos finales del CNU.

Para el estado de la red y el consumo del ancho de banda, se evaluó el conjunto de medidas de eficiencia y confiabilidad mediante herramienta de simulación, en la que se utilizó la herramienta del firewall (FortiView). Ver en el anexo #3.

Por medio el equipo de seguridad de la institución, se estableció políticas de seguridad para el control de acceso de los usuarios internos y externos, que necesitan acceder a los servicios que se ejecutan en la red.

13. Recomendaciones

Implementar un Servidor de Directivas de Redes (NPS), en la que permite crear y aplicar directivas de acceso de red en toda la institución para la autenticación y autorización de solicitudes de conexión. Ver anexo #4.

Establecer políticas para identificar el tráfico de la red, esta identificación puede usarse posteriormente para filtrarlo y conseguir una mejor administración y rendimiento del tráfico global de la red. Trabajándolo con los servicios que ocupan los equipos de intermedio (routers y switch) por medio el servicio de control ACL (Access Control List),

Para una mejor estructura jerárquica en la institución, se debe almacenar la información sobre los objetos de la red. Se recomienda implementar un Servicio de dominio de Active Directory (AD), el AD va a proporcionar los métodos para almacenar datos de directorio y poner estos datos a disposición de los usuarios y administradores de la red. Ver anexo #5

14. Bibliografía

Ernesto Ariganello, Ra-Ma (2020). Redes de Datos, Guía de estudio para la certificación CCNA 200-301.

Kevin Wallace, (2015). CCNP Routing and Switching Route 300-101.

Alfonso Anibal, F. M. J (2018). Guía de infraestructura tecnológica con Windows server 2012.

Mónica Liberatori, (2018). Redes de datos y sus protocolos

Andrew S. Tanenbaum, David J. Wetherall (2012). Redes de Computadoras (5ta edición).

William Stallings, (2012). Comunicaciones y redes de computadores (6ta Edición)

José E. Briceño M., (2005). Transmisión de datos (Tercera Edición).

David Hucaby (2016). CCNA Wireless 200-355 Official Cert Guide.

Zorrilla Arena, Santiago. (2009). Introducción a la Metodología de la investigación (2da Ed.). Cal y Arena.

Arias, F. (2006). El Proyecto de Investigación (3era Edición). Editorial

15. Sitio web de consulta

https://www.enatrel.gob.ni/nicaragua-mas-cerca-de-contar-con-mayor-conectividad-digital/

https://docs.oracle.com/cd/E56339_01/html/E53805/ipref-13.html

https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/networksetup/configure_dhcp_server_c.html

https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/overview/networksecurity/dns_about_c.html?Highlight=dns

https://www.unir.net/ingenieria/revista/servidor-web-local/

https://mx.godaddy.com/blog/servidor-de-correo-electronico-como-funciona/

https://mx.godaddy.com/blog/servidor-de-correo-electronico-como-funciona/

https://learn.microsoft.com/es-es/windows-server/networking/technologies/nps/nps-top

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

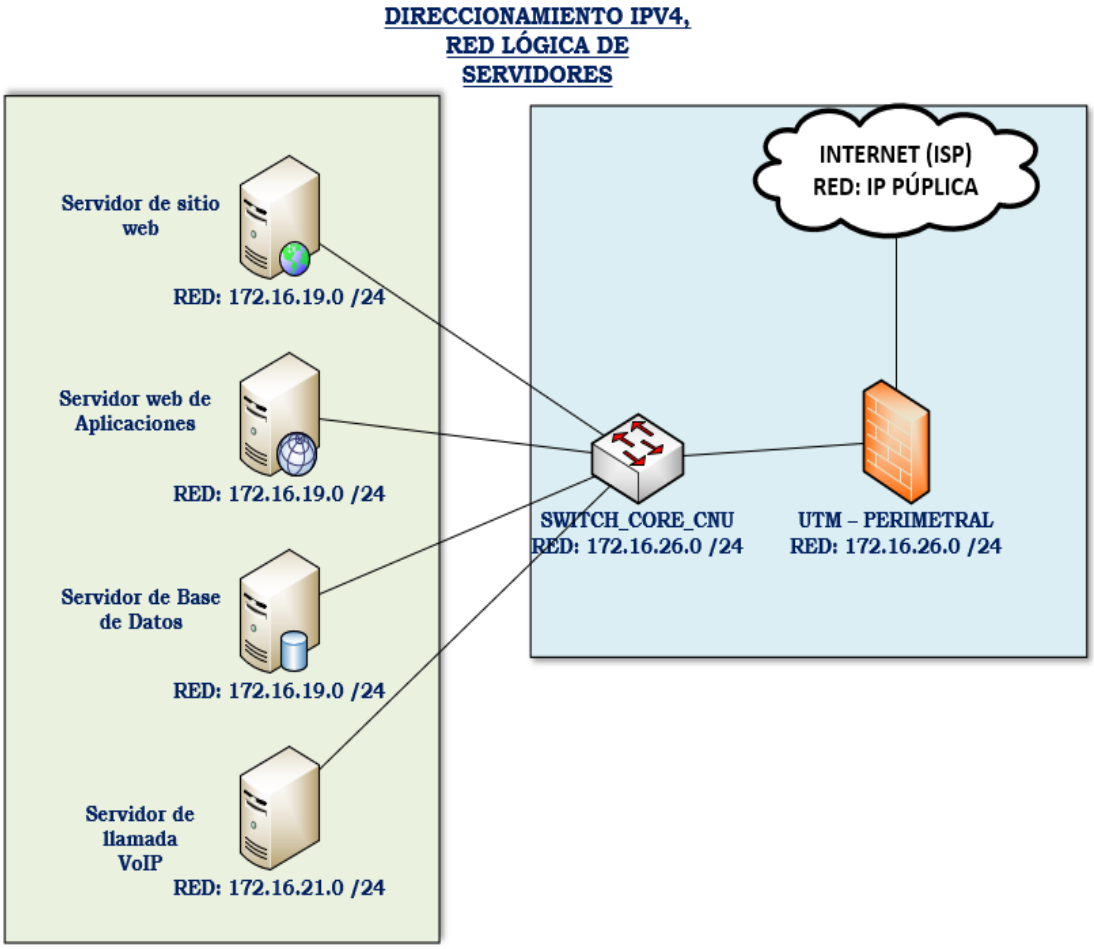
https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

https://wfd.cloud.cambiumnetworks.com/wfdc/

16. Anexos

Anexo 1.

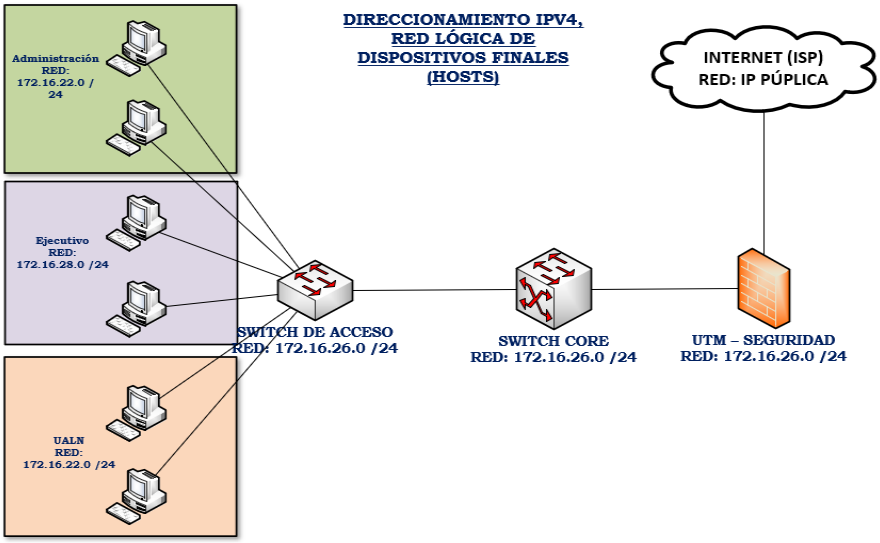
Red lógica.



Nota. Direccionamiento IPv4, de la red de los servidores del CNU, información aprobada por las autoridades del CNU, para su presentación en el documento.

Anexo 2.

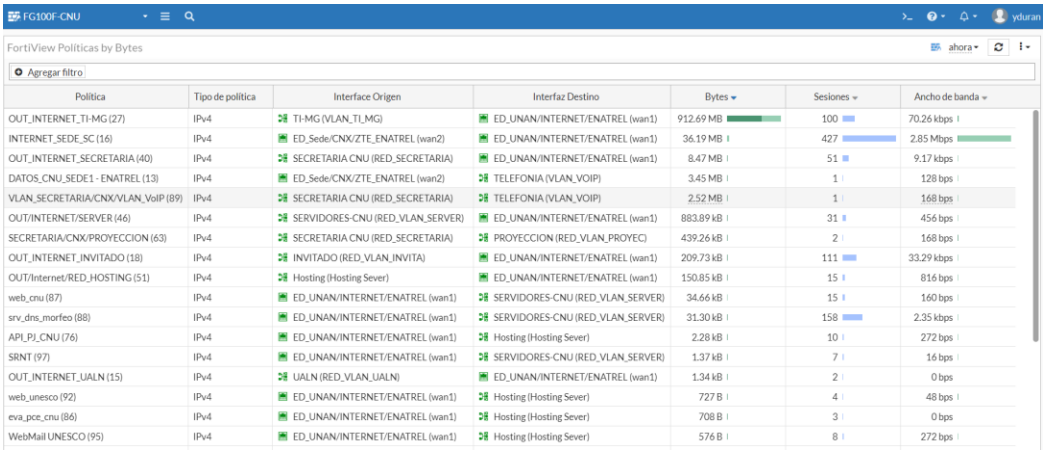
Topología lógica, IPv4.



Nota. Direccionamiento IPv4 en clase B, de los hosts, en la red del CNU, información aprobada por las autoridades del CNU, para ser presentada en la documentación.

Anexo 3.

Políticas de seguridad de red.


FG100F-CNU

FortiView Políticas by Bytes

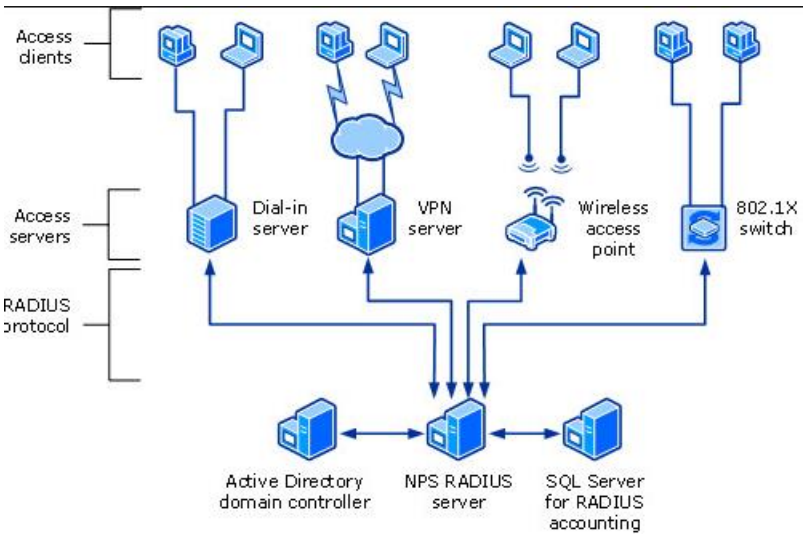
Agregar filtro

Política	Tipo de política	Interface Origen	Interfaz Destino	Bytes	Sesiones	Ancho de banda
OUT_INTERNET_TI-MG (27)	IPv4	TI-MG (VLAN_TI_MG)	ED_UNAN/INTERNET/ENATREL (wan1)	912.69 MB	100	70.26 kbps
INTERNET_SEDE_SC (16)	IPv4	ED_Sede/CNX/ZTE_ENATREL (wan2)	ED_UNAN/INTERNET/ENATREL (wan1)	36.19 MB	427	2.85 Mbps
OUT_INTERNET_SECRETARIA (40)	IPv4	SECRETARIA CNU (RED_SECRETARIA)	ED_UNAN/INTERNET/ENATREL (wan1)	8.47 MB	51	9.17 kbps
DATOS_CNU_SEDE1 - ENATREL (13)	IPv4	ED_Sede/CNX/ZTE_ENATREL (wan2)	TELEFONIA (VLAN_VOIP)	3.45 MB	1	128 bps
VLAN_SECRETARIA/CNX/VLAN_VoIP (89)	IPv4	SECRETARIA CNU (RED_SECRETARIA)	TELEFONIA (VLAN_VOIP)	2.52 MB	1	168 bps
OUT/INTERNET/SERVER (46)	IPv4	SERVIDORES-CNU (RED_VLAN_SERVER)	ED_UNAN/INTERNET/ENATREL (wan1)	883.89 kB	31	456 bps
SECRETARIA/CNX/PROYECCION (63)	IPv4	SECRETARIA CNU (RED_SECRETARIA)	PROYECCION (RED_VLAN_PROYEC)	439.26 kB	2	168 bps
OUT_INTERNET_INVITADO (18)	IPv4	INVITADO (RED_VLAN_INVITA)	ED_UNAN/INTERNET/ENATREL (wan1)	209.73 kB	111	33.29 kbps
OUT/Internet/RED_HOSTING (51)	IPv4	Hosting (Hosting Sever)	ED_UNAN/INTERNET/ENATREL (wan1)	150.85 kB	15	816 bps
web_cnu (87)	IPv4	ED_UNAN/INTERNET/ENATREL (wan1)	SERVIDORES-CNU (RED_VLAN_SERVER)	34.66 kB	15	160 bps
srv_dns_morfeo (88)	IPv4	ED_UNAN/INTERNET/ENATREL (wan1)	SERVIDORES-CNU (RED_VLAN_SERVER)	31.30 kB	158	2.35 kbps
API_PJ_CNU (76)	IPv4	ED_UNAN/INTERNET/ENATREL (wan1)	Hosting (Hosting Sever)	2.28 kB	10	272 bps
SRNT (97)	IPv4	ED_UNAN/INTERNET/ENATREL (wan1)	SERVIDORES-CNU (RED_VLAN_SERVER)	1.37 kB	7	16 bps
OUT_INTERNET_UALN (15)	IPv4	UALN (RED_VLAN_UALN)	ED_UNAN/INTERNET/ENATREL (wan1)	1.34 kB	2	0 bps
web_unesco (92)	IPv4	ED_UNAN/INTERNET/ENATREL (wan1)	Hosting (Hosting Sever)	727 B	4	48 bps
eva_pce_cnu (86)	IPv4	ED_UNAN/INTERNET/ENATREL (wan1)	Hosting (Hosting Sever)	708 B	3	0 bps
WebMail UNESCO (95)	IPv4	ED_UNAN/INTERNET/ENATREL (wan1)	Hosting (Hosting Sever)	576 B	8	272 bps

Nota. Herramienta de administración del equipo de seguridad de red

Anexo 4.

Administración de un servidor NPS



Nota. Administración de los hosts, por medo de políticas y en conjunto con el AD.

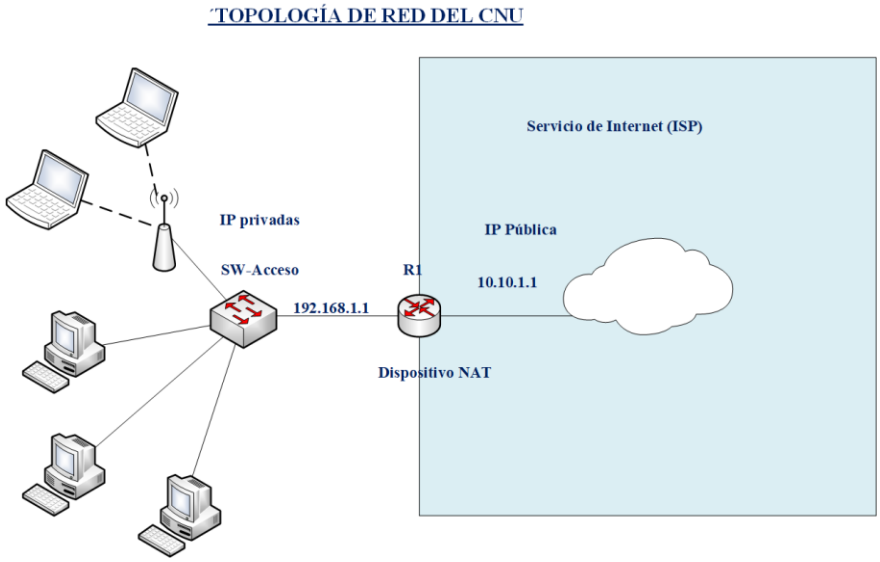
Anexo 5.

Controlador de Dominio

Nota. Esquema de controlador de dominio, para administrar por grupo o bosques, los usuarios y los equipos que se encuentren en la red.

Anexo 6

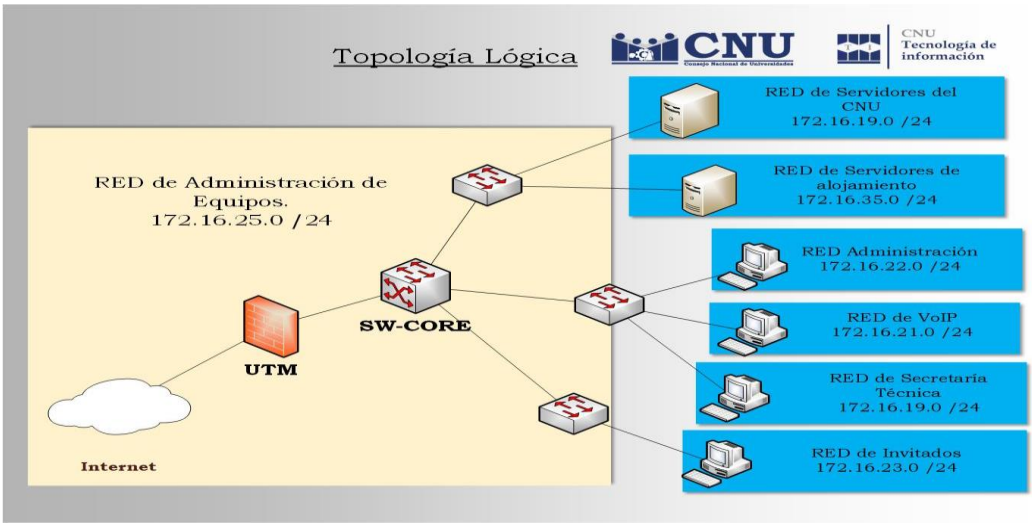
Topología de red, básica.



Nota. En la ilustración se observa una topología de red básica, donde existe la colisión de paquete, todos los servicios no eran fluidos y había perdida paquetes.

Anexo 7

Red segmentada



Nota. En la ilustración se observa una red segmentada, con una buena fluides de paquetes. Información aprobada por la autoridades del CNU, para el documento.

17. Glosarios

HTTP: Hypertext Transfer Protocol o Protocolo de Transferencia de Hipertexto en español

HTTPS: Hypertext Transfer Protocol Secure

ISP: Proveedor de servicio de internet

IP: Protocolo de Internet

AS: Sistema Autónomo

AP: Puntos de Acceso

AD: Hypertext Transfer Protocol Secure

DNS: Sistema de nombre de dominio

NPS: Servidor de directivas de red.

HPN: Redes de alto rendimiento

EAP: Protocolo de autenticación extensible

DHCP: Protocolo de configuración dinámica de host

QoS: Directiva de calidad de servicios

VPN: Red privada virtual

SNMP: Protocolo simple de Administración de Redes.

EIGRP: Enhanced Interior Gateway Routing Protocol

ISP: Proveedor de Servicio de Internet.