UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

REINGENIERÍA DE LA RED DE DATOS DEL INSTITUTO DE INVESTIGACIONES BIOMÉDICAS – UNAM MEDIANTE TECNOLOGÍAS OPEN SOURCE

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:

CERVANTES GONZALEZ CHRISTIAN ARTURO

ASESOR:

ING. TORRES RODRIGUEZ GERARDO

NEZAHUALCÓYOTL, ESTADO DE MÉXICO , 2017

AGRADECIMIENTOS:

Dedico estas líneas para expresar mi agradecimiento a todas las personas que de alguna forma ayudaran en mi camino, que aportaron su apoyo moral y físico hacienda posible la culminación de mi carrera profesional.

A todas aquellas personas que con sus actos me alentaron a seguir adelante, con su apoyo logre conseguir el éxito que ahora tengo, por la oportunidad de conocer personas tan únicas y especiales, que forman parte de mi vida:

A mis padres:

Martin Cervantes Cobian

Maria Isabel Gonzalez Reyes

A quienes por haber estado ahí en su momento y darme la vida para sacarle su máximo potencial, les estaré agradecido.

A mis maestros, hermanos, amigos y compañeros que no dejaron de estar ahí conmigo en cada paso que daba, me ofrecieron la experiencia necesaria para aprender nuevos conocimientos necesarios para mi crecimiento.

A toda el área de la sección de cómputo del instituto de Biomédicas Omar Rangel Rivera, Juan Miguel Escobar Muñoz y en especial a Jaime David Rico Malfavon, que gracias a tu entrega y paciencia en mi crecimiento académico y personal logre sobresalir y culminar este trabajo.

A mis tutores Elizabeth Juarez Robles, Gabriel Ortiz Cordero, Jorge Arturo López Hernandez, Enrique Garcia Guzman y en especial a mi maestro Gerardo Torres Rodriguez que gracias a su apoyo incondicional y guía de cada uno de mis avances y dudas logro hacer de mí un profesional capacitado y diestro.

A Karla Cristina Galicia Pérez que siempre me alienta a ser mejor cada día.

Para Francisco Cervantes Ayala por su apoyo incondicional.

Nataly Miroslava Frías Ieran por su apoyo moral y guía en el momento preciso.

Con cariño, admiración y respeto a todos aquellos que forjaron al profesional y persona que ahora soy, GRACIAS, doy y daré siempre lo mejor de mí cada día.

ÍNDICE

INTRODUCCIÓN

Objetivo general

El presente trabajo propone una propuesta factible de reingeniería de la red de datos en el Instituto de Investigaciones Biomédicas de la Universidad Nacional Autónoma de México que se adecué a los requerimientos funcionales y al presupuesto que maneja la dependencia.

El esquema vigente de la red de datos implementado en el Instituto se basa en la configuración de una red plana que hasta el momento ha funcionado correctamente, pero la creciente demanda de los servicios de internet, la extensión de las redes cableadas a inalámbricas, el uso de dispositivos móviles y las necesidades de los usuarios afectarán la disponibilidad de la red de datos en el corto plazo.

Para diseñar una solución útil para el Instituto es necesario conocer los inconvenientes que se presentan en el día a día. Actualmente se han identificado algunos comportamientos que interfieren en el correcto desempeño y administración de la red como:

La asignación de direcciones IP se hace de forma manual y eso implica llevar un control de éstas que sea fiable, adicionalmente los usuarios han sido víctimas de la duplicidad de la dirección IP que tienen configurada estáticamente, también con este tipo de administración potencialmente un usuario pudiera duplicar la ip de la puerta de enlace y provocar una falla de red general del segmento en cuestión.

Durante las videoconferencias se presentan en ocasiones pérdidas de paquetes en los enlaces ocasionados por el tráfico de la red que se maneja en horas pico.

Las cámaras en red del circuito cerrado presentan latencia al visualizarlas en tiempo real desde los equipos de cómputo donde se tiene configurado el acceso a ellas.

El Backbone de fibra óptica que interconecta los edificios soporta hasta 1 Gbps, y a mediano plazo representará un problema para la red de datos considerando que los requerimientos de las aplicaciones son cada vez mayores en el consumo de datos.

La comunidad académica del Instituto requiere la mayor disponibilidad a la red de datos para desempeñar la actividad principal del Instituto que tiene que ver con “el estudio de los fenómenos biológicos en los niveles molecular, celular, organismo y poblacional, y la proyección de sus conocimientos y tecnologías al entendimiento y solución de las enfermedades humanas”.

Para atender los requerimientos del Instituto es necesario un planteamiento que permita mejorar la administración de la red y la experiencia de los usuarios en sus actividades que requieren la red de datos, así como considerar la migración entre el esquema actual y el propuesto de forma gradual. Esta tesis plantea el rediseño lógico de la red y la implementación de redes virtuales de área local(VLAN’s), permitiendo de esta manera la segmentación del tráfico de red, la separación del dominio de colisión/difusión y la modificación de la configuración del firewall actual basado en tecnologías abiertas al nuevo escenario.

Esta tesis consta de los siguientes capítulos:

Introducción: constara de:

Antecedentes: se dará a conocer la historia del Instituto de Investigaciones Biomédicas y como se fue construyendo la infraestructura de red con la que actualmente opera

- Objetivo general: explicación de la finalidad de la tesis.
- Justificación: Planteamiento de los alcances y temas que tratara la tesis.
- Delimitaciones: Explicación de los límites y temas que no serán tratados dentro de la tesis.
- Marco teórico: Descripción de conceptos para la tesis.
- Situación actual: Descripción de la infraestructura de red del Instituto de Investigaciones Biomédicas actualmente.
- Solución propuesta: Definición de las áreas de mejora que pueden ser implementadas en base al diseño de la infraestructura de la red actual.
- Conclusión: Resumen del conocimiento y resultados obtenidos.

- Recomendaciones: Cambios sugeridos para la optimización de la infraestructura de red a futuro.
- Anexos: documentación extra sobre los procesos que se realizaron o referencias.
- Glosario: Catalogo de palabras y expresiones.
- Bibliografía: referencias de libros y publicaciones.

Justificación

Se plantea realizar una reingeniería de la red actual con la final de resolver problemas ya detectados dentro del Instituto de Investigaciones Biomédicas de la nueva sede que son:

- Alcanzando el límite de direcciones IP permitidas en la red
- Problemas de enrutamiento
- Seguridad en la red
- Duplicidad de IP
- Perdida de información

Para la implementación de segmentación de la red con tecnología VLAN se reutilizarán los equipos que la sección de cómputo ya tenía instalados en la institución, se analizaron las características de los Switch con los que se cuentan para asegurar que soportaran correctamente la implementación de VLAN para aprovechar las virtudes que esta ofrece como son:
Una mejor administración de la red y de las IP privadas asignadas a cada segmento y edificio.
Aumento de la seguridad.
Asignación de recursos y permisos en base a perfil de usuario
También se analizó el diseño actual de la red LAN como red plana que es como se encuentra actualmente la red en la institución, para realizar un plan de migración de la red plana a una red segmentada utilizando tecnología VLAN y tener una mejor administración de la red.
La red actualmente es una red plana donde el Broadcast puede llegar a todos los dispositivos de los edificios del Instituto de Investigaciones Biomédicas de la nueva sede que son:

- Edificio A
- Edificio B
- Edificio C
- Unidad de Modelos Biológicos
- Auditorio (como anexo del edifico A)

Todos los grupos de usuarios dentro de la comunidad académica utilizan direcciones IP de clase C con mascara de red de clase C asignados por grupos:

Vlan	Segmento	Área
Vlan 1	132.248.116.0/24	Segmento de red público (Servidores Y FW/NAT/GW)
Vlan 1	192.168.2.0/24	Edificio C
Vlan 1	192.168.3.0/24	Edificio A y servidores internos
Vlan 1	192.168.4.0/24	Edificio B
Vlan 1	192.168.199.0/24	UMB y CCTV
Vlan 1	192.168.6.0/24	Comunidad académica
Vlan 1	192.168.7.0/24	Comunidad académica

Vlan 1	192.168.8.0/24	Investigadores y ruteadores
Vlan 1	192.168.169.0/24	Secretaria técnica y CCTV
Vlan 1	192.168.200.0/24	Administración de SW

Se plantea migrar a los usuarios dentro de la comunidad académica utilizando direcciones IP de clase B con mascara de red de clase C asignados por grupos:

Vlan	Segmento	Área
Vlan 1	132.248.116.0/24	Segmento de red público (Servidores Y FW/NAT/GW)
Vlan 2	172.16.2.0/24	Edificio A
Vlan 3	172.16.3.0/24	Edificio B
Vlan 4	172.16.4.0/24	Edificio C
Vlan 5	172.16.5.0/24	Inalámbrico
Vlan 6	172.16.6.0/24	Administración
Vlan 7	172.16.7.0/24	Servidores con IP no homologada
Vlan 8	172.16.8.0/24	Secretaria técnica y CCTV
Vlan 9	172.16.9.0/24	CCTV y UMB usuarios
Vlan 10	172.16.10.0/24	CCTV-General
Vlan 1	192.168.200.0/24	Administración de SW

La estimación de host con IP privada registrada en cada edificio es la siguiente:
En el Edificio “A” del Instituto se tiene contemplado un total de 124 host de la comunidad académica con IP privada registrada.
En el Edificio “B” del Instituto se tiene contemplado un total de 221 host de la comunidad académica con IP privada registrada.
En el Edificio “C” del Instituto se tiene contemplado un total de 229 host de la comunidad académica con IP privada registrada.
En la Unidad de modelos biológicos del Instituto se tiene contemplado un total de 22 host de la comunidad académica con IP privada registrada.
Haciendo un total de 596 host con IP privada registrada más un estimado.
La topología física del instituto es del tipo jerárquico, estructura que se conservara dado que es la más óptima a utilizar en este caso.

Delimitaciones

El Instituto de Investigaciones Biomédicas de la nueva sede cuenta con servicio de red inalámbrica a través de ruteador y AP (Access point) de la línea hogar, servicio de IDS (sistema de detección de intrusos), servicios de voz analógico y digital, enlace de fibra óptica al *backbone* de red UNAM administrado por la DGTIC entre otros servicios que no se contemplan en esta tesis dado que son temas por si solos para el desarrollo de otros trabajos académicos.

Teniendo en cuenta la magnitud de la infraestructura y servicios ofrecidos por el Instituto esta tesis se centra en la reingeniería del diseño de la red del Instituto en la nueva sede a nivel de capa 2 y capa 3 utilizando los equipos de red actuales.
Por cuestiones de seguridad no se puede hacer pública la configuración actual del servidor FW/NAT/GW.

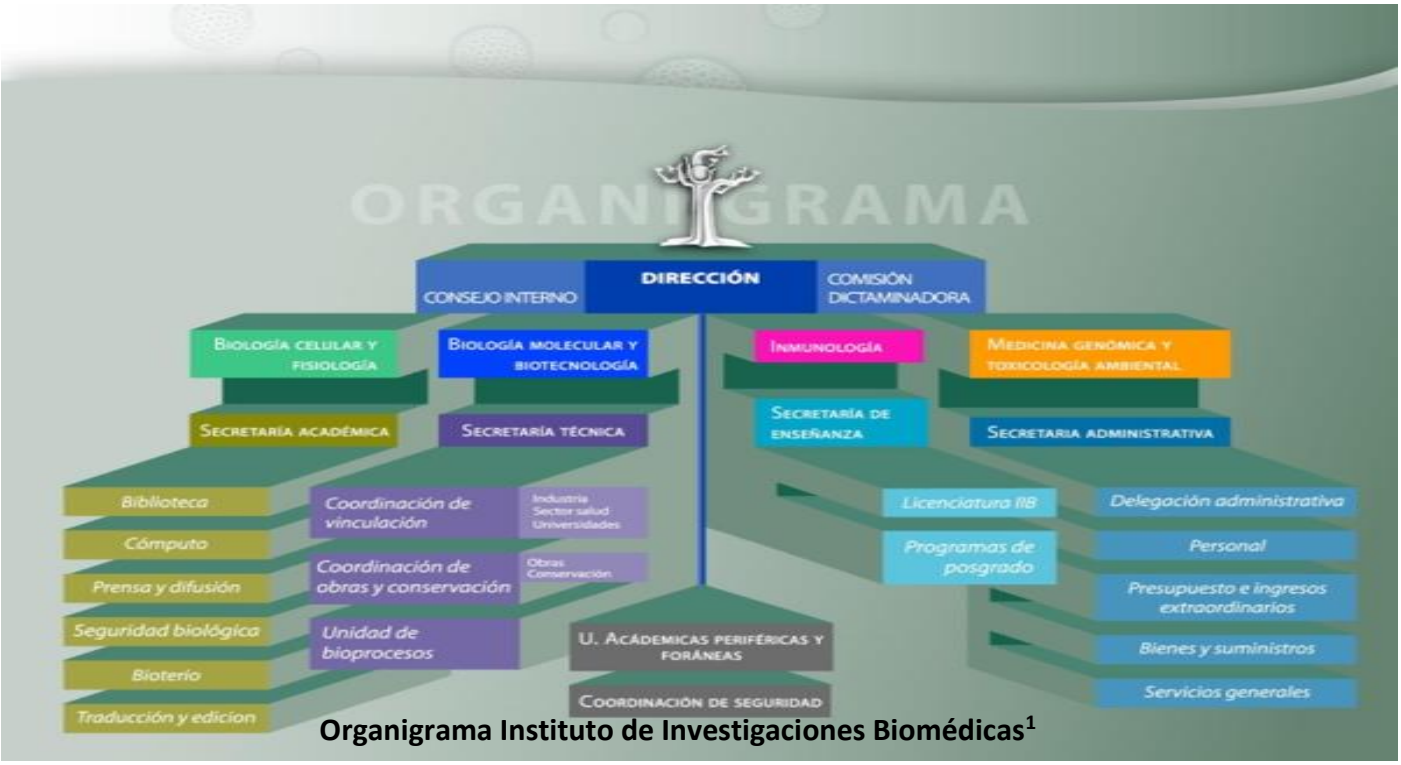
CAPÍTULO I
ANTECEDENTES

1.1 Antecedentes del IIBm

El Instituto de Investigaciones Biomédicas es una Dependencia de la Universidad Nacional Autónoma de México que se enfoca en primera instancia a la investigación de fenómenos biológicos en los niveles molecular, celular, organísmico y poblacional con el fin de proyectar conocimientos además de las tecnologías para lograr un mayor entendimiento de las enfermedades humanas; y en segunda instancia a la generación de recursos humanos a nivel Licenciatura, Maestría y Doctorado.

Físicamente el Instituto se ubica en Ciudad Universitaria y cuenta con dos Sedes, la Sede anterior ubicada en el Circuito Escolar y la Nueva Sede situada en el Tercer Circuito Exterior; durante su historia el Instituto ha trabajado en conjunto con el Sector Salud a través de Unidades Periféricas en los Institutos Nacionales de Cancerología (INCan), Pediatría (INP), Ciencias Médicas y Nutrición "Salvador Zubirán" (INCMNSZ), así como Neurología y Neurocirugía "Manuel Velasco Suárez" (INNNMVZ); además de tener convenios con Instituciones del Sector Salud en la zona metropolitana Biomédicas también colabora con la Universidad de Tlaxcala y Xalapa mediante Unidades Foráneas.

Para cumplir con su actividad principal, el Instituto se encuentra organizado en cuatro Departamentos de investigación: Biología Celular y Fisiología (BCyF), Biología Molecular y Biotecnología (BMyB), Inmunología y Medicina Genómica y Toxicología Ambiental (MGTA); cada uno de éstos se encuentra integrado por investigadores y uno de ellos es el encargado de coordinar el Departamento a su cargo.



Organigrama Instituto de Investigaciones Biomédicas[1]

Existen otras áreas en el Instituto que brindan apoyo a los Departamentos de investigación, el organigrama institucional integra las Secretarías: Académica, Técnica, Enseñanza y Administrativa; éstas a su vez se

[1] Fuente: http://www.biomedicas.unam.mx/imgs/imgss/Organigrama.jpg

encuentran divididas en Departamentos institucionales con tareas muy granulares que facilitan el proceso de investigación institucional, y una de ellas es facilitar los medios a través de Tecnologías de Información y Comunicación. Desde la aparición del Instituto y hasta mediados de los 90's la producción científica se realizaba con las herramientas que en ese momento eran adecuadas, pero al paso de los años aunado a la aparición y uso cada vez más popular de los equipos de cómputo el Instituto necesitaba modernizar su infraestructura y adaptarse a los nuevos cambios tecnológicos. De acuerdo a información obtenida de la columna *"20 años del Internet y Red Biomédicas"* fue en 1994 cuando llega Internet al Instituto; este gran suceso desencadenó la misión de incorporar servicios de red institucionales como la página web y el correo electrónico, así como planear la adquisición de equipos de cómputo para la comunidad. En sus inicios estos servicios de internet eran muy sencillos, la página web institucional tenía un diseño acorde a su época y la información que se ofrecía era limitada comparándola con la actual; para el acceso del correo electrónico los usuarios lo consultaban estableciendo una conexión remota al servidor en línea de texto y posteriormente ejecutaban un cliente de correo (pine) instalado en el servidor. Fue en 2001 cuando se incorporó la consulta de correo a través de una página web(Webmail) y muchos usuarios prefirieron revisar su correo a través de este medio por la practicidad de la solución.

Con el paso del tiempo se fueron perfeccionando las técnicas para el envío de correo electrónico no deseado y el servicio necesitaba alinearse a las nuevas tecnologías web así como incorporar un registro SPF a nivel de DNS así como realizar la configuración del servidor de correo electrónico para evitar riesgos de suplantación de identidad.

En 2010 se instaló la suite de correo zimbra basada en tecnologías abiertas y se migraron los datos de los usuarios, algunos de ellos requirieron asesoría para realizar sus actividades cotidianas en la nueva interfaz y recibieron el soporte técnico necesario para adoptar la nueva tecnología.

En el 2017 se planteó la migración de los equipos actuales de telecomunicaciones a dispositivos *Cisco,* cambio que no se realizó en la fecha planteada por cuestiones de presupuesto y se optó por aprovechar los equipos con los que ya se contaban e implementar tecnología VLAN.

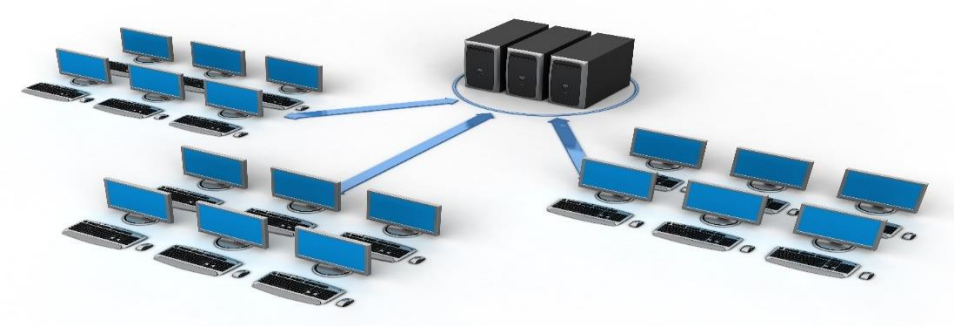
Existen diversos factores necesarios para la vida del ser humano como lo son el comer o el respirar, y para poder convivir con otro ser humano e intercambiar información es necesaria la comunicación, desde los orígenes de los tiempos la necesidad de comunicación ha sido una de las necesidades primordiales para la vida en sociedad, desde simples gestos hasta la estructuración de un leguaje complejo de signos, señas y gestos, la comunicación se convirtió en un elemento necesario para la vida cotidiana.
En sus orígenes la comunicación solo podía darse de emisor a receptor cara a cara con una improvisación se señas y gestos que representaban un suceso o la emisión de un mensaje para un grupo individual de personas, eventualmente cada sociedad estructuraba un leguaje más completo que pudiera ser transmito a un grupo más grande de personas con el fin de estandarizar el lenguaje de comunicación utilizado, cada nuevo avance ampliaba el alcance de las comunicaciones, desde un conjunto de caracteres escrito en papel y lápiz, hasta complejas redes de comunicación como la antenas telefónicas, la televisión, etc. con el fin de establecer una comunicación de un extremo a otro más amplia.
En un principio las redes de datos estaban limitadas a procesos simples de intercambio de información de un sistema informático a otro utilizando caracteres que fueran capaces de enviar, recibir y procesar. A pasos agigantados la tecnología ha ido evolucionado adaptándose a las nuevas necesidades de intercambio de información agregando voz, datos y video entre los diversos dispositivos que procesan y ofrecen este tipo de información, haciendo que la forma de comunicación pasara de un entorno individual a un entorno en común.

Existiendo una amplia variedad de métodos de comunicación se empezaron a establecer estándares y protocolos para adecuar y agilizaba una correcta comunicación entre los diversos medios.
El principio fundamental de una infraestructura de red es: compartir recursos a través de la misma, intercambiar información, ofrecer disponibilidad de servicio y de datos siempre que sean solicitados por algún usuario de la red.
Adicionalmente una infraestructura de red debe ser diseñada de acuerdo a las necesidades que los usuarios tienen de la red, para evitar problemas como: saturación del ancho de banda, colisiones, tormentas de Broadcast, perdida de información, problemas de enrutamiento, seguridad, duplicidad de IP, etc.
El buen diseño de una infraestructura de red es fundamental para la correcta comunicación entre los dispositivos que procesan e intercambian información entre sí, una infraestructura de red puede ser tan compleja como la necesidad de los usuarios la requiera, esto conlleva a la expansión de la red para satisfacer la demanda del recurso.
Una red pequeña es fácilmente administrable ya que no requiere de mucha demanda de personal capacitado y recursos informáticos, eventualmente una red que empieza a expandirse para cumplir con la creciente demanda de los usuarios implica un mayor nivel de administración de personal capacitado y adquisición de nuevos dispositivos informáticos.
Cuando una red de no esta segmentada, es decir una red plana solo existe un dominio de difusión que puede causar problemas en la red como son la saturación del medio o colisiones.
El Instituto de Investigaciones Biomédicas (IIBm) era pequeña en sus orígenes, pero ha ido creciendo constantemente, a medida que fue creciendo no se rediseñó el planteamiento de la red y por lo mismo el problema no se ha atacado de la mejor forma.
Actualmente el Instituto de Investigaciones Biomédicas ha ido ampliándose con nuevos edificios y usuarios que requieren de acceso a los recursos y usos de la red, como lo son servicios, correo, internet, página web institucional, etc., este crecimiento fue dándose paulatinamente por lo que la infraestructura de red en un principio alcanzaba para abastecer a todos los usuarios, llego un punto donde la red empezó a presentar problemas de saturación del recurso debido a que la demanda del acceso a la red excedió la capacidad de administrar correctamente servicio a todos los usuarios.
Este aumento excesivo de usuarios ocasiono que la red de área local empezara a llegar a su límite de direcciones IP que podía proporcionar, saturación del medio, sobre uso de equipos de telecomunicaciones obsoletos que ya estaban en end-life pero seguían siendo utilizados debido a la escases de recursos para nuevos equipos, colisiones, servicio deficiente, etc.
Se tiene planeado realizar un rediseño de la red plana que se tiene actualmente en el Instituto de Investigaciones Biomédicas mediante uso de VLAN, con la finalidad de resolver el problema de duplicidad de IP, segmentación del trafico prioritario en los diferentes edificios, renovación del stock de equipo de telecomunicaciones que se tiene, por ello se consideró el uso de VLAN para resolver varios de estos problemas y poder separar el tráfico en redes mejor administradas en orden de prioridad y uso utilizando subredes, para realizar este cambio se utilizaran dispositivos de telecomunicaciones como SW y Router para administrar la red.
El Instituto de Investigaciones Biomédicas actualmente se encuentra en red plana, es decir, tiene un solo dominio de Broadcast, se empelaran VLAN para segmentar la red resolviendo problemas existentes de la red, tener una mejor administración de redes, mejorar el servicio prioritario de red, aumentar las políticas de seguridad por medio de Iptables, aumentar la disponibilidad del recurso, reduciendo las áreas afectadas por posibles tormentas de Broadcast optimizando la red. Se hará uso de tecnologías OPEN SOURCE para administrar, establecer políticas de seguridad específicas y re direccionar el tráfico de red.

CAPÍTULO II
MARCO TEÓRICO

2.1 Definición de red datos

Una red de datos es parte de la infraestructura de telecomunicaciones o red de comunicación diseñada para la transmisión de información mediante el intercambio de datos, en esencia es un conjunto de dispositivos como computadoras, routers y switches que pueden comunicarse entre sí a través de un medio de transmisión, siguiendo un conjunto de reglas y protocolos que permiten realizar el envío y recepción de información de forma ordenada.



Esquema de una red de datos[2]

Las redes de datos tienen como principal objetivo permitir el intercambio de información entre los dispositivos conectados en la red; compartir recursos computacionales (hardware y software) y proporcionar acceso óptimo a recursos que pueden incluso estar a grandes distancias.

2.2 Ethernet

También conocido como Norma IEEE 802.3, es la forma estandarizada de conectar dispositivos a través de una red LAN, determina las características físicas, eléctricas, longitud y diámetro de los cables que debe poseer una red en la capa física del modelo OSI, también determina la configuración y características que deben tener las tramas de datos en la capa de direccionamiento físico del modelo OSI, utiliza el método de acceso al medio por disputa (CSMA/CD).

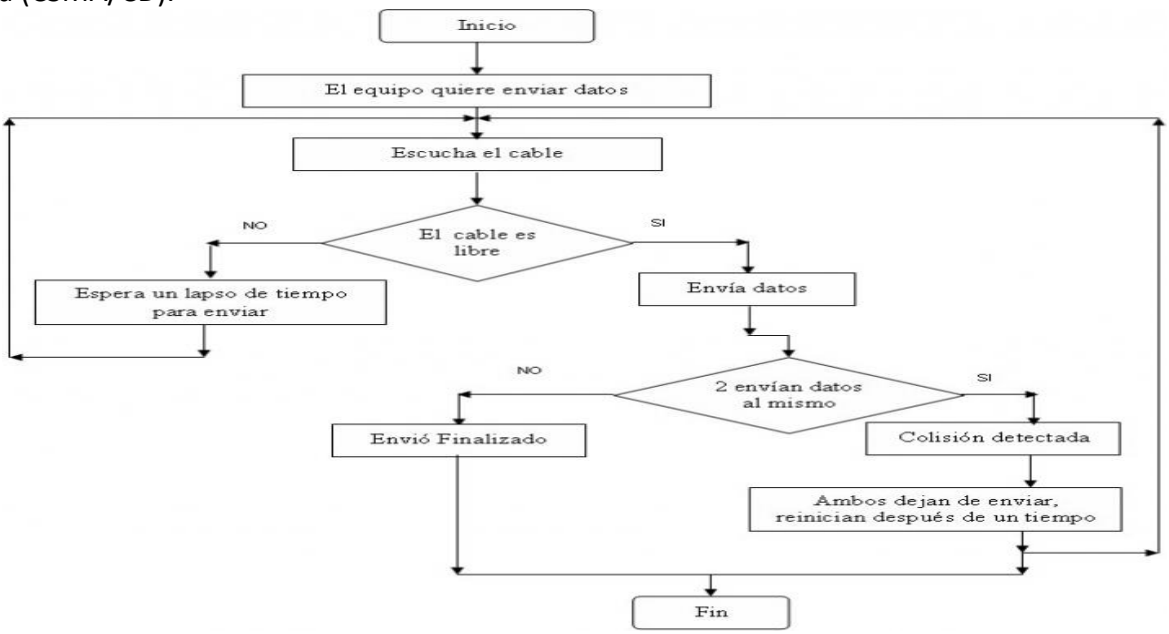
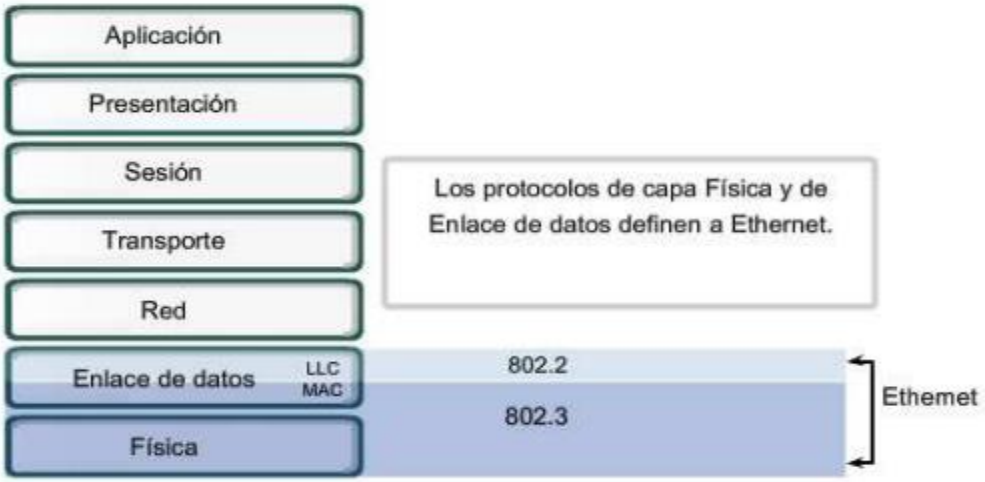


Diagrama de flujo del método CSMA/CD, aquí se ejemplifica como el dispositivo escucha el medio para reservar y evitar colisiones[3]

[2] http://azucenamarez.blogspot.mx/2014/04/las-bases-de-datos-y-los-sistemas-de.html
[3] http://uhu.es/antonio.barragan/content/protocolo-csmacd

El estándar 802.3 es utilizado en la capa física del modelo OSI, y el estándar 802.2 es utilizado en la capa de direccionamiento físico del modelo OSI. El estándar Ethernet especifica la tasa de transferencia de datos en Mb/s, el método de señalamiento utilizado y la máxima longitud de segmento de cable.



El estándar 802.3 usado en capa 1 del modelo OSI y el estándar 802.2 usado en la capa 2 del modelo OSI[4]

2.3 Estándares de cable Ethernet

Ethernet

Nombre	Medio	Velocidad de transmisión	Distancia máxima
10BASE-5	Cable coaxial grueso	10 Mb/s.	500m
10BASE-2	Cable coaxial delgado	10 Mb/s.	185m
10BASE-T	Cable par trenzado	10 Mb/s.	100m
10BASE-F	Cable de fibra óptica	10 Mb/s.	2000m

Implementación: 10BASE-5, 10BASE-2, 10BASE-36, 10BASE-T, 10BASE-F, 10BASE-F, etc.

Fast Ethernet

Nombre	Medio	Velocidad de transmisión	Distancia máxima
100BASE-TX	2-pares de UTP (Categoría 3 o superior)	100 Mb/s.	100m
100BASE-T4	4-pares de UTP (Categoría 3 o superior)	100 Mb/s.	100m
100BASE-FX	2-pares de cable par trenzado para datos (UTP o STP categoría 5 o superior)	100 Mb/s.	2000m

Implementación: 100BASE-TX, 100BASE-T4, 100BASE-FX, etc.

[4] http://blog.utp.edu.co/ee973/files/2012/04/capitulo09-ethernet.pdf

Gigabit Ethernet

Nombre	Medio	Velocidad de transmisión	Distancia máxima
1000BASE-SX	Cable de fibra óptica multimodo (Rango 50/125 µm o 62.5/125 µm)	1000 Mb/s.	500m
1000BASE-LX	Cable de fibra óptica monomodo o multimodo (Rango 50/125 µm o 62.5/125 µm)	1000 Mb/s.	10Km
1000BASE-CX	Cable de cobre blindado especial	1000 Mb/s.	25m
1000BASE-T	4-pares Categoría 5 (o superior) de cable UTP	1000 Mb/s.	100m

Implementación: 1000BASE-SX, 1000BASE-LX, 1000BASE-CX, 1000BASE-T, etc.

2.4 Direcciones IP

En general las direcciones IP son utilizadas para identificar los diferentes nodos en una red. Las direcciones IP están formadas por 4 bytes (32 bits) y se pueden representar en la notación decimal, hexadecimal o binario con punto, de la forma (x.y.w.z) donde cada una las variables es un número comprendido entre 0-255, 00-FF hexadecimal o en binario desde 00000000 hasta 11111111

Clase Red	No. Bits Subred / Host	Direcciones de Subred	No. de IP por subred	Rango Direcciones IP
A	8/24 255.0.0.0	T) 0.0.0.0 - 127.0.0.0 R) 0.0.0.0 P) 10.0.0.0 R) 127.0.0.0	2^{24}-2=16777214	Rango válido 1.0.0.1 -127.255.255.254 Todo para uso público Internet excepto 1 Subred privada 10.0.0.1 -10.255.255.254 1 Subred reservada 127.0.0.1 -127.255.255.254
B	16/16 255.255.0.0	T) 128.0.0.0 - 191.255.0.0 P) 172.16.0.0 - 172.31.0.0 R) 169.254.0.0	2^{16}-2=65534	Rango válido 128.0.0.1 -191.255.255.254 Todo para uso público Internet excepto 16 subredes privadas 172.16.0.1 -172.31.255.254 1 subred reservada 169.254.0.1 - 169.254.255.254
C	24/8 255.255.255.0	T) 192.0.0.0 - 223.255.255.0 P) 192.168.0.0 - 192.168.255.0	2^{8}-2=254	Rango válido 192.0.0.1 - 223.255.255.254 Todo para uso público Internet excepto 255 subredes privadas 192.168.0.1 - 192.168.255.254

T) Total
P) Privadas sólo para uso en redes privadas y no en Internet
R) Reservadas para usos diversos

- Clase A: Hay 126 redes con 16, 777, 214 direcciones para host cada una.
- Clase B: Hay 16384 redes con 65, 534 direcciones para host cada una.
- Clase C: Hay 2097152 redes con 254 direcciones para host cada una.

2.5 Switch

Un switch o conmutador es un dispositivo de red diseñado para la interconexión de equipos dentro de una misma red, junto al cableado constituyen las redes LAN, opera en la capa dos del modelo OSI utilizando direccionamiento físico y comúnmente el estándar Ethernet, manejan velocidades entre 10 Mb/s hasta 10Gb/s dependiendo del modelo de switch que se tenga, por sí solo no puede proporcionar conectividad con otras redes ni conectividad con internet de eso se encarga el router.

2.6 Tipos de Switch

Por Características:

Switch troncal: son utilizados en el núcleo central (core) de las grandes redes, es decir que en estos switches están conectados otros de jerarquía inferior, además de servidores, routers wan, etc.

Switch perimetral: son utilizados en el nivel jerárquico inferior en una red local y a los que están conectados los equipos de los usuarios finales.

Switch gestionable (managed): ofrecen una serie de características adicionales que requieren de configuración y gestión.

Switch no gestionable (unmanaged): ofrecen funcionalidades básicas que no requieren procedimiento de configuración o gestión.

Por Función:

Switch desktop: son los switch más básicos, ofrecen las funciones de conmutación básicas sin ninguna función adicional. Su uso más habitual es en redes de ámbito doméstico o en pequeñas empresas para la interconexión de unos pocos equipos, por lo que no están preparados para su montaje en rack 19" (pulgadas), no requiere ningún tipo de configuración ya que utilizan el modo de autoconfiguración de Ethernet para configurar los parámetros de cada puerto. Suelen tener de 4-8 puertos del tipo RJ-45, normalmente admite velocidades de 10/100Mb/s de manera comercial, aunque también hay modelos que admiten 1000Mb/s. Los Switches más actuales permiten características Auto MDI/MDI-X.

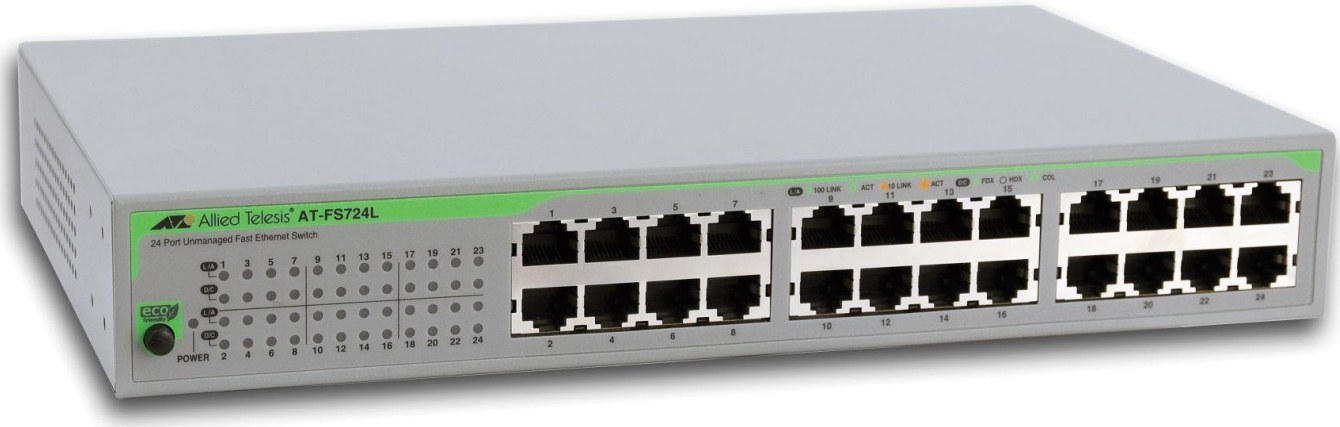
Switch desktop[5]

MDI: Interfaz Dependiente del Medio o Medium Dependent Interface, conocidos como linkup permite conectarse a otros hubs o switches usando un cable de red directo (habitualmente se usaban cable de red cruzado), existen interfaces especiales que detectan automáticamente el tipo de conexión que el cable necesita y configura la conexión automáticamente, estos son los Auto-MDIX ("X" representa "crossover"), es decir, es una función de filtro interno que realiza el cruce de señales necesario dentro del puerto para que se pueda establecer la comunicación.

Switch perimetrales no gestionables: Se utilizan habitualmente para redes de pequeño tamaño con prestaciones medianas. No admiten opciones de configuración y suelen tener características similares a los

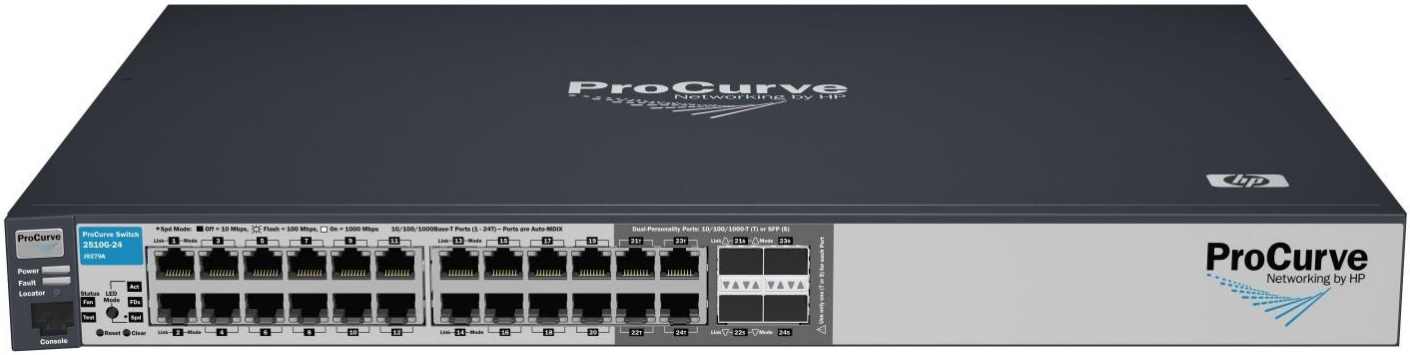
[5] http://redestelematicas.com/tipos-de-switches/

switch desktop, tiene un numero de puertos mayor comúnmente entre 4,8,16 0 24 puertos del tipo RJ-45, admite velocidades de 10/100/1000Mb/s, hay modelos no gestionables que proporcionan Power Over Ethernet (PoE) y la posibilidad de montaje en un rack 19".



Switch perimetral no gestionable[6]

Switch perimetral gestionable: Se utilizan habitualmente para la conexión de los equipos de los usuarios en redes de tamaño mediano y grande, se localiza en el nivel jerárquico inferior, requiere características avanzadas de configuración y gestión, la cantidad de puertos que suele tener esta entre los 16 y 48 puertos del tipo RJ-45 todos con soporte Auto MDI/MDIX, admite velocidades de 10/100/1000Mb/s, incluye puertos adicionales GBIC o SFP para la conexión de un switch troncal, características avanzadas de gestión por SNMP, puerto de consola, navegador web, shh, monitorización Port Mirroring, también permite configuraciones avanzadas en la capa 2 como Port Trunking, Spanning Tree, IEEE 802.1x, QoS, VLAN, soporte de tramas Jumbo, etc., algunos modelos pueden ofrecer Power Over Ethernet en todos los puertos.



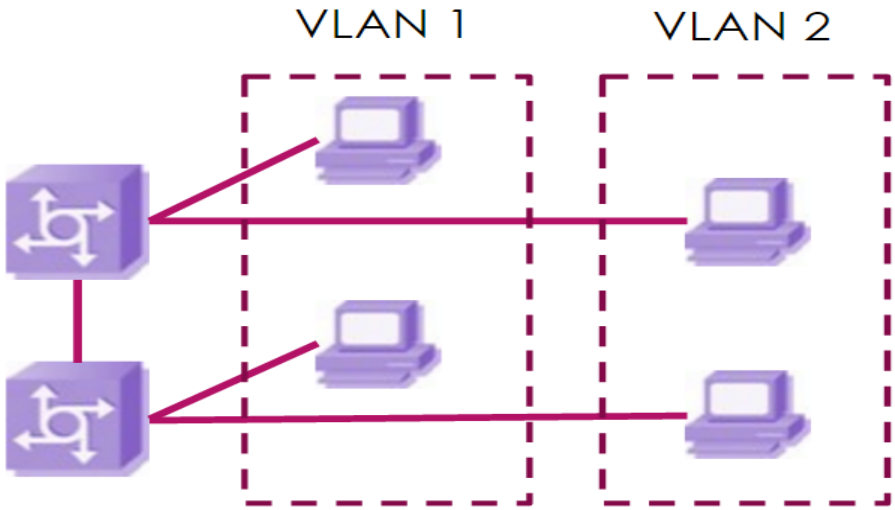
Switch perimetral gestionable[7]

2.7 VLAN

Una red de área local virtual (Virtual Local Area Network o Virtual LAN) se puede definir como la segmentación lógica de una red local, es decir agrupa lógicamente los puertos de un switch en dominios de broadcast diferentes actuando como si tuvieran su propia red independiente aun cuando varias VLAN comparten el mismo dispositivo físico, esto permite al administrador de red llevar una organización más eficiente del dominio de broadcast ya que cada VLAN recibe únicamente el tráfico broadcast de esa VLAN, permite un mejor control sobres los protocolos asignados a cada segmento, se implementan mejores políticas de

[6] http://redestelematicas.com/tipos-de-switches/
[7] http://redestelematicas.com/tipos-de-switches/

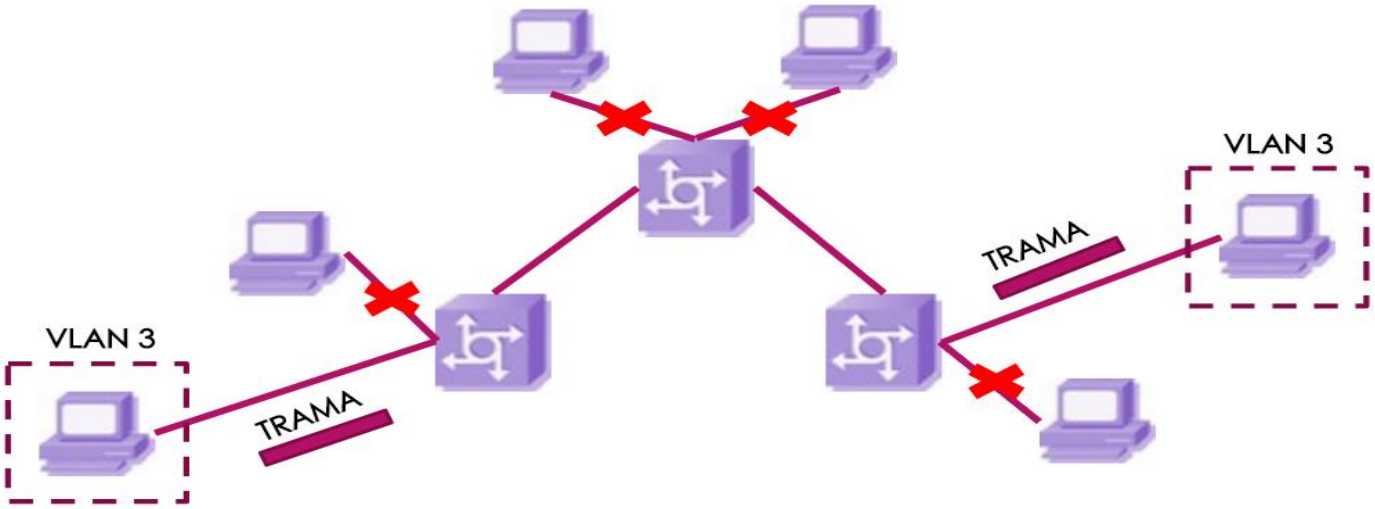
seguridad dependiendo de las funciones de cada uno de los dispositivos conectados a ésta; en términos técnicos la capa 2 del modelo OSI implementa esta característica y a cada puerto de los switches instalados en la red local se puede configurar para que pertenezca a una VLAN, se le asigna un nombre a cada VLAN para facilitar su identificación, es necesaria la intervención de un router para comunicar VLAN's diferentes, para eso se configura el Gateway que es la dirección del router que conoce donde se encuentra la otra VLAN con la que se quiere comunicar, para que varias VLAN se comuniquen a través de un mismo router se puede configurar un puerto troncal.



Esquema de una VLAN[8]

2.8 Ventajas de una VLAN

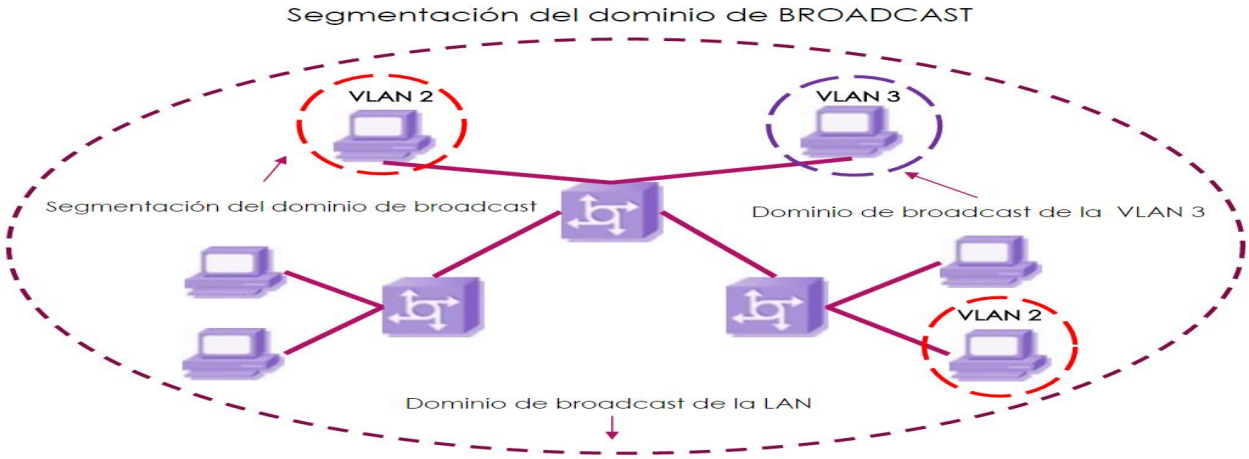
Seguridad: Para mantener la integridad de la información de un usuario o un grupo usuarios se puede configurar una VLAN con políticas de seguridad más estrictas, también se suele aislar el tráfico de esa VLAN del resto de la red disminuyendo el riego de que la información más sensible sea comprometida.



El tráfico enviado por la VLAN3 es información sensible por lo que el tráfico enviado por la VLAN3 tiene políticas de seguridad más estrictas y se aísla del resto de la red [9]

[8] http://slideplayer.es/slide/4021292/
[9] http://slideplayer.es/slide/4021292/

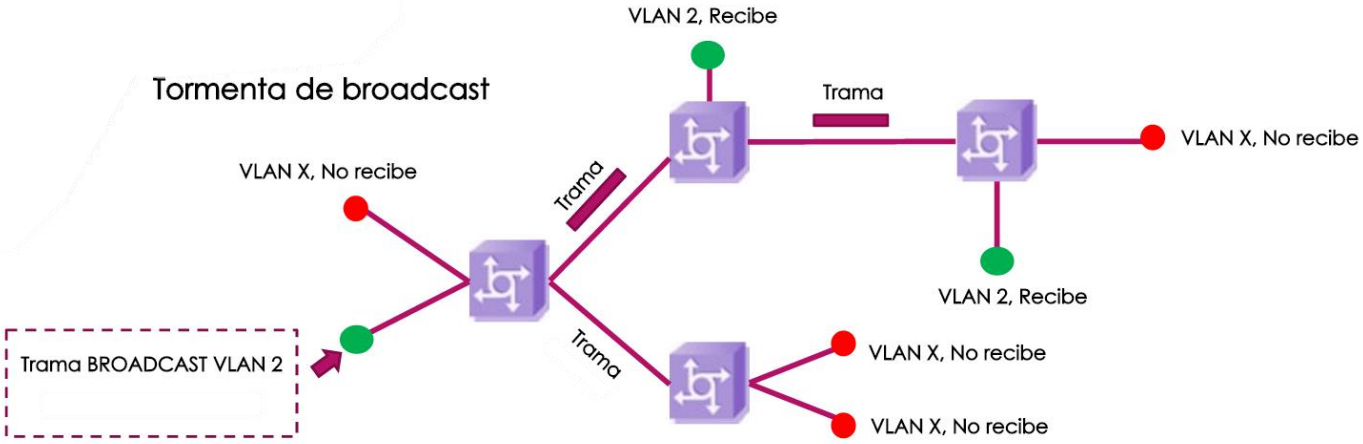
Reducción de costos: Al hacer mejor uso del ancho de banda y de los enlaces que se tienen se ahorra en redes y dispositivos de conmutación.
Mejor rendimiento: la división de la red en grupos lógicos (dominios de broadcast) reduce el trafico innecesario en la red y potencia el rendimiento.



Ejemplo de segmentación de los dominios de broadcast para mejorar el rendimiento de la red[10]

Administración ágil: los usuarios con requerimientos similares de red son asignados a una VLAN especifica que cumple con los requerimientos de red o bien que pertenecen a un grupo exclusivo de usuario el cual tiene una VLAN especial asignada, al tener bien separadas las VLAN facilita su gestión y asignación en base a los requerimientos que tengan los usuarios de la red.

Limitación de posibles tormentas de broadcast: Al segmentar una red LAN en varias VLAN se reduce la cantidad de dispositivos que podrían ser afectados por una tormenta de broadcast evitando que se propague por toda la red.

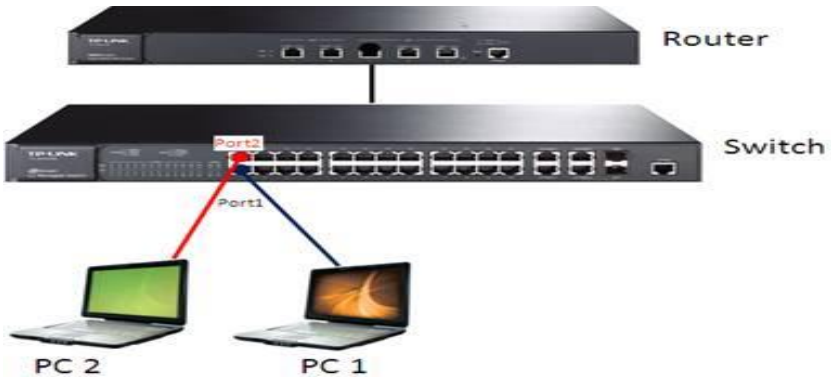


Ejemplo de la mitigación de la tormenta de broadcast[11]

2.9 Tipo de puertos VLAN

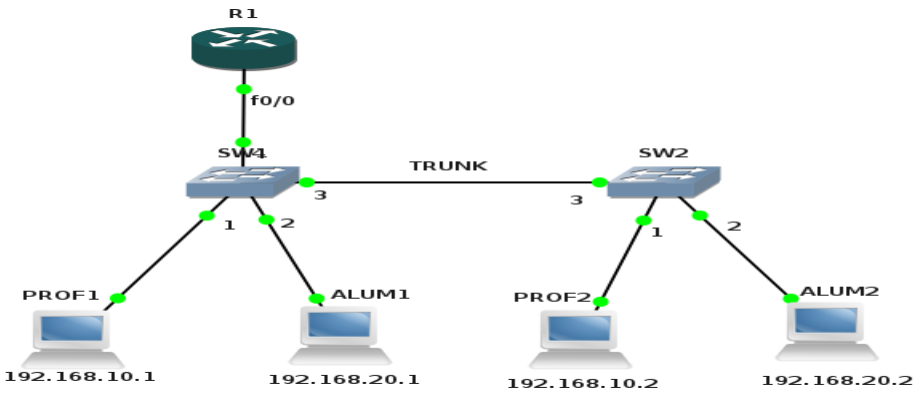
Access link (Puerto de acceso): Es cualquier puerto de un switch que pertenece a una VLAN. Cuando entra una trama Ethernet se le añade el Tag de 802.1Q y cuando sale una trama 802.1Q se le quita el Tag, para que llegue a la estación correspondiente con el formato IEEE 802.3 original

[10] http://slideplayer.es/slide/4021292/
[11] http://slideplayer.es/slide/4021292/



Ejemplo puerto de acceso[12]

Trunk link (Puerto troncal): Es un puerto en un switch que sirve de enlace entre switches para la transmisión de trafico de varias VLAN. Las tramas que le llegan y que salen llevan el Tag 802.1Q.

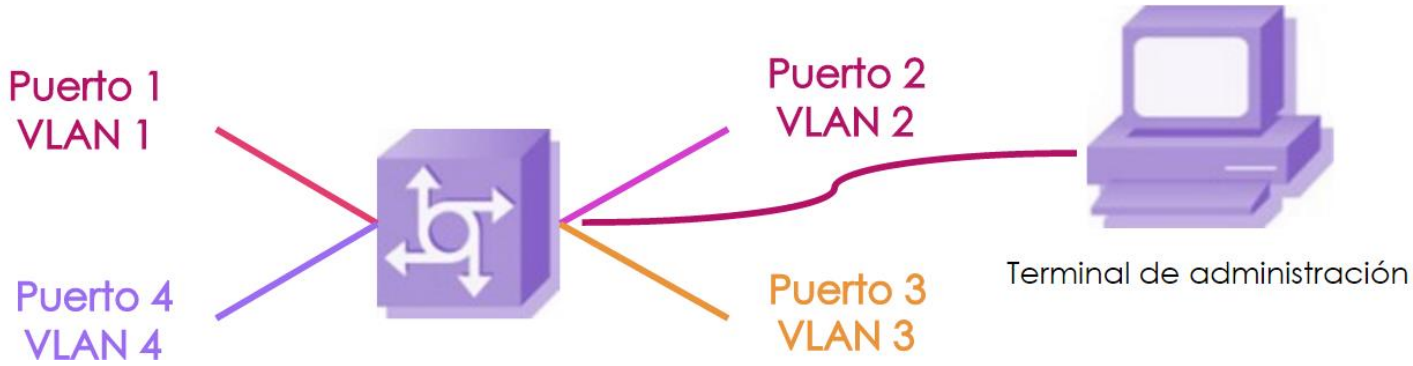


Ejemplo de conexión de switches por medio de un puerto troncal[13]

2.10 Asignación de modos de puertos de SW de VLAN

VLAN estática: el administrador de red es quien asigna de manera fija que puerto pertenecerá a que VLAN, esta configuración solo puede ser cambiada por el administrador, en caso contrario la configuración permanecerá fija, cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto.

[12] http://redesconfiguracion.blogspot.mx/2015/07/que-es-una-vlan-y-su-funcion.html
[13] http://redesconfiguracion.blogspot.mx/2015/07/que-es-una-vlan-y-su-funcion.html



Ejemplo de puertos asignados a una VLAN por el administrador[14]

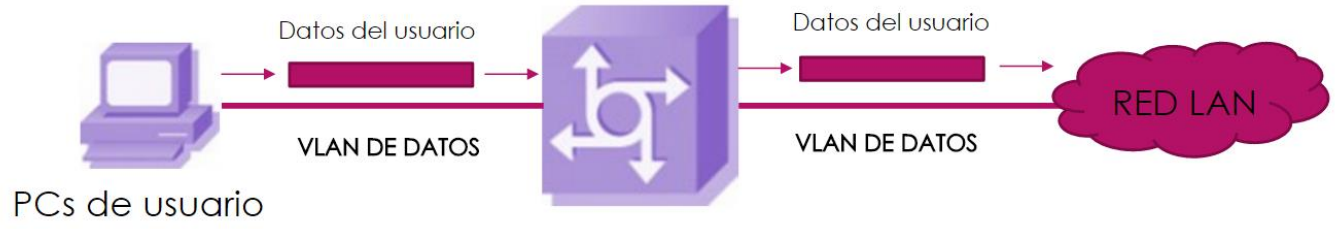
VLAN dinámica: el switch configura de manera automática los puertos a la VLAN que pertenece dependiendo de la dirección de nivel de enlace, direccionamiento lógico, tipo de protocolo de los paquetes, MAC address o nombre de usuario, para configurar un puerto dinámico se utiliza el servicio del VPMS (VLAN Management Policy Server o Servidor de Gestión de Directivas de la VLAN) que hace la función de servidor para la base de datos de asignación de VLAN's dinámicas, una de sus ventajas es la movilidad ya que si un usuario cambia de ubicación física de un puerto de switch a otro es el switch el que asigna el puerto nuevo a la VLAN correspondiente.

Ejemplo de asignación de VLAN por medio de MAC address[15]

2.11 Tipos de VLAN

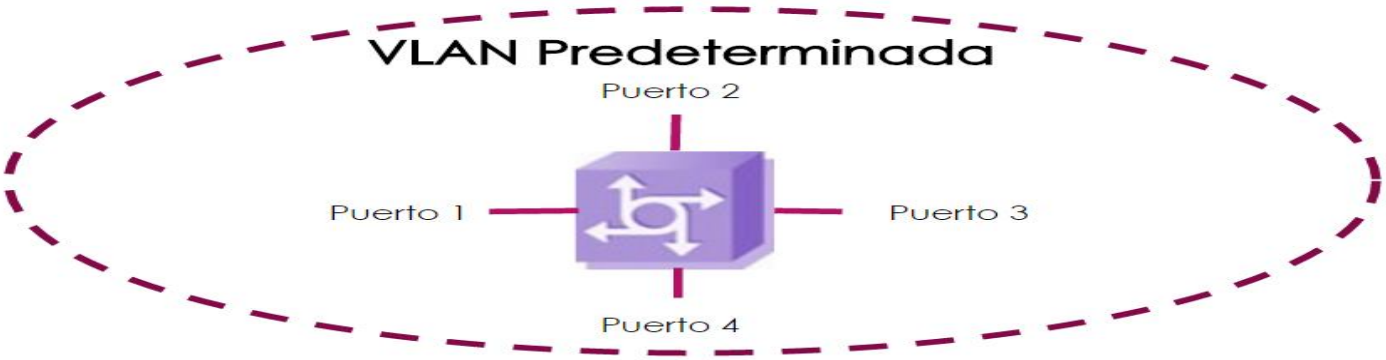
VLAN de datos: Tambien se le conoce como VLAN de usuario, es una VLAN capaz de enivar trafico de datos, voz y el trafico utilizado por el adminitrador, es recomendado tener el trafico de datos separado del trafico de voz y del trafico de control del administrador para identificar las VLAN's que solo envian datos del usuario.

[14] http://slideplayer.es/slide/4021292/
[15] http://slideplayer.es/slide/4021292/



Esquema de una VLAN de datos[16]

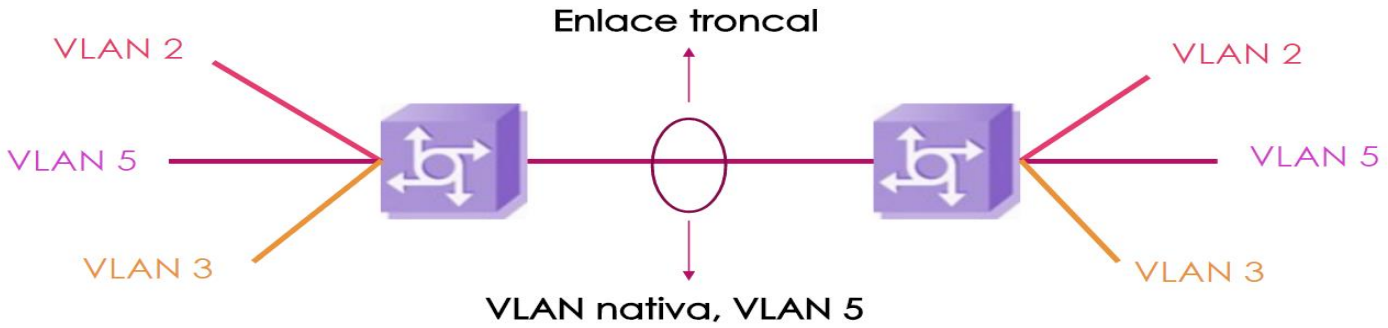
VLAN predeterminada: todos los puertos de switch se vuelven parte de la VLAN predeterminada despues del arranque inicial de un switch que carga la configuración predeterminada, todos los puertos perteneceran inicialmente al mismo dominio de broadcast, por lo que cualquier dispositivo conectado al switch podra comunicarse entre si. La VLAN predeterminada en un switch comunmente es la VLAN1, por seguridad se recomienda cambiar la VLAN predeterminada a otra que no sea la VLAN1.



Esquema de una VLAN predeterminada, donde todos los puertos estan asiganados a la VLAN1 por defecto[17]

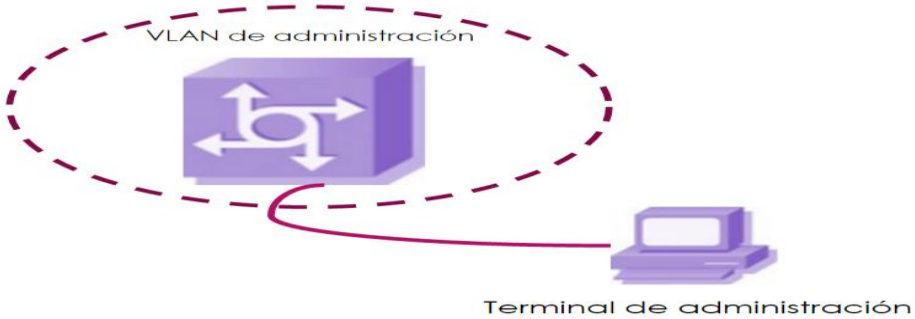
VLAN Nativa: La VLAN nativa esta asignada a un puerto troncal, este tipo de puertos admiten el trafico proveniente de varias VLAN (tráfico etiquetado) y el trafico que no proviene de una VLAN (trafico sin etiquetar), el trafico etiquetado hace referencia al trafico que tiene una etiqueta de 4 byts insertada en el encabezado de la trama de Ethernet original que especifica la VLAN a la que pertenece la trama, el puerto de enlace troncal coloca el trafico sin etiquetar en la VLAN nativa, el trafico sin etiquetar lo genera una computadora conectada a un puerto de switch que esta configurada como VLAN nativa, una VLAN nativa sirve como identificador comun en extremos opuestos de un enlace troncal, es recomendado colocar a la VLAN nativa en cualquier otra VLAN que no seha la VLAN1, comunmente se utiliza la VLAN 99 para ser la VLAN nativa, al configurar un puerto de enlase troncal 802.1Q se asigna el valor de la ID de VLAN nativa a la ID de VLAN de puerto (PVID) predeterminada, todo el trafico sin etiquetar entrante o saliente del puerto 802.1Q se reenviara según el valor de la PVID, por ejemplo si se configura la VLAN 99 como VLAN nativa la PVID es 99 y todo el trafico sin etiquetar se reenvia a la VLAN 99, si la VLAN nativa no se configuro en ningun momento la PVID sera VLAN1.

[16] http://slideplayer.es/slide/4021292/
[17] http://slideplayer.es/slide/4021292/



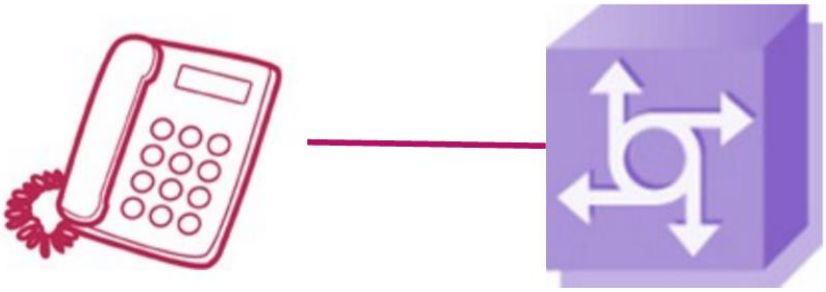
Esquema de una VLAN nativa[18]

VLAN de Administración: Es cualquier VLAN configurada para poder acceder a las funciones de administrador de un switch, a una VLAN de administración se le asigna una dirección IP y una máscara de subred, se puede manejar un switch mediante HTTP, Telnet, SSH o SNMP, la configuración predeterminada tiene a la VLAN1 como la VLAN de administración, es común que esta sea cambiada a cualquier otra VLAN que no sea la VLAN1 por cuestiones de seguridad y control.



Esquema de una VLAN de administrador[19]

VLAN de voz: En telefonia IP se recomienda tener la VLAN de voz separada del la VLAN de datos para tener una mayor calidad de la voz, se configura un puerto en modo de voz para admitir un teléfono IP conectado al mismo, esta configuración debe hacerse en el switch previo a la conexión del dispositivo telefónico IP, cuando un teléfono IP se conecta por primera vez a un puerto de una VLAN de voz el switch le envía mensajes al teléfono IP para proporcionarle la configuración y el ID de la VLAN de voz, este tipo de VLAN permite que el tráfico de voz sea transmitido con mayor prioridad.

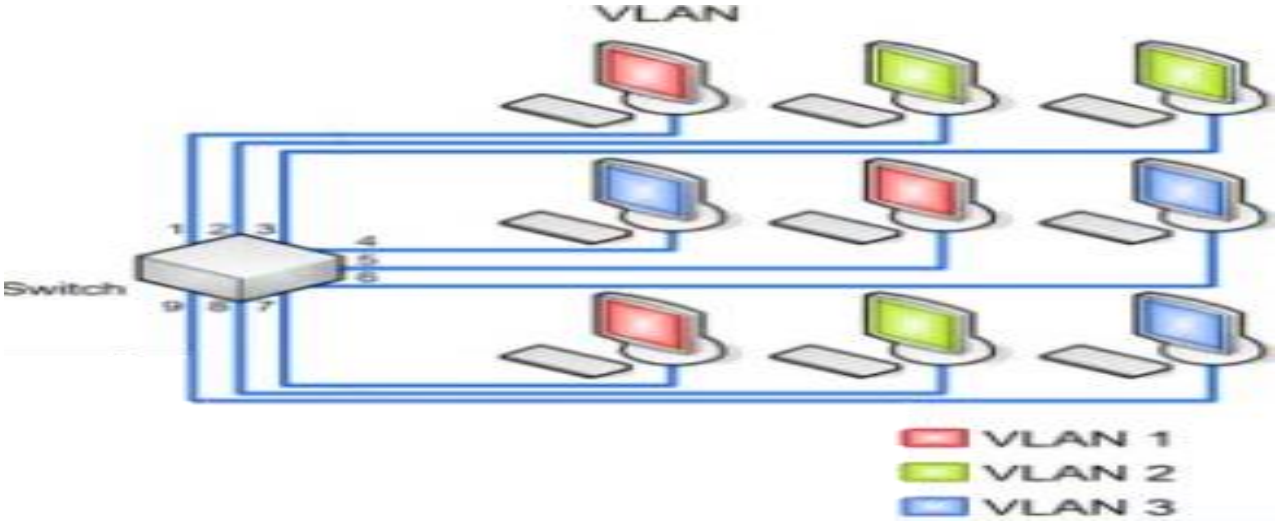


Esquemas de una VLNA de voz[20]

[18] http://slideplayer.es/slide/4021292/
[19] http://slideplayer.es/slide/4021292/
[20] http://slideplayer.es/slide/4021292/

2.12 Clasificación de VLAN

VLAN por puerto: También conocido como "port switching" se especifica que puertos del switch pertenecen a una determinada VLAN, los miembros de dicha VLAN son los que tendrán acceso por estos puertos, una vez se han asignado los puertos de una VLAN no podrán ser movidos al menos que el administrador cambie la configuración, si el usuario cambia de ubicación física hereda las políticas de la VLAN a la que pertenezca el puerto al que ahora está conectado, la VLAN por puerto es la más utilizada y opera en el nivel 1 del modelo OSI.



VLAN por puerto[21]

VLAN por dirección MAC: se asignan los hosts a una VLAN en función de su dirección MAC, tiene la ventaja de que no hay que reconfigurar la VLAN si el usuario cambia de ubicación física, es decir, si el usuario cambiara de puerto seria reconocido por su MAC address y se le asignaría de nuevo a la VLAN correspondiente, suele ser muy útil cuando se tiene pocos usuarios reconocidos, su desventaja radica cuando aumenta el número de usuarios ya que hay que colocarlos uno por uno en una tabla de asignación, opera en el nivel 2 del modelo OSI.

MAC Address	VLAN correspondiente
15.FF.xx.xx.xx.xx	1
1b.cc.xx.xx.xx.xx	2
a3.20.xx.xx.xx.xx	3
12.aa.xx.xx.xx.xx	3
15.2F.xx.xx.xx.xx	1
12.15.xx.xx.xx.xx	2

Ejemplo de tabla de asignación de VLAN por MAC

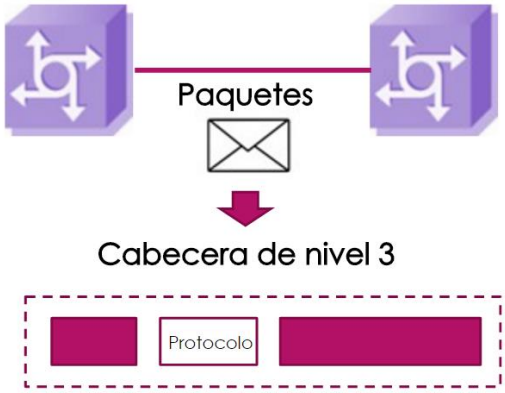
VLAN por tipo de protocolo: la asignación de VLAN queda determinada por el contenido del campo tipo de protocolo de la trama MAC, por ejemplo, se puede crear y asignar la VLAN1 al protocolo IPv4, la VLAN2 al protocolo SSH, la VLAN3 al protocolo SMTP, etc., opera en el nivel 2 del modelo OSI.

[21] http://redesconfiguracion.blogspot.mx/2015/07/que-es-una-vlan-y-su-funcion.html

PC's conectadas	Tipo de protocolo	VLAN correspondiente
PC1	IPv4	1
PC2	SSH	2
PC3	SMTP	3
PC4	SMTP	3
PC5	IPv4	1
PC6	IPv4	1

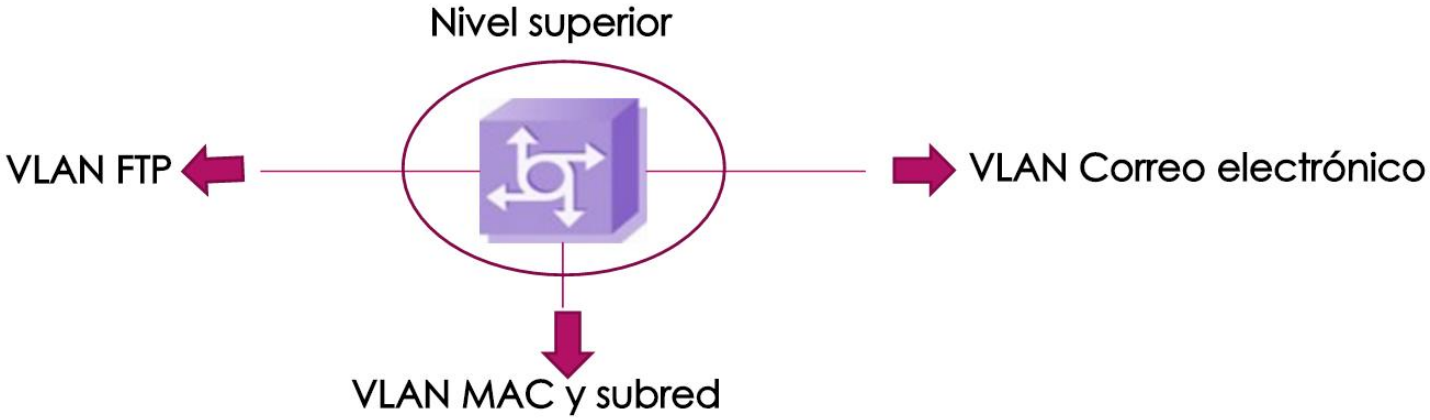
Ejemplo de tabla de asignación de VLAN por protocolo

VLAN por direcciones de subred (subred virtual): La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece, en este tipo de VLAN no son los host's, si no los paquetes los que pertenecen a la VLAN, estaciones con múltiples protocolos de red (nivel 3 del modelo OSI) estarán en múltiples VLAN's.



VLAN por direcciones de subred utilizando la cabecera de nivel 3[22]

VLAN de niveles superiores: Se crea una VLAN para cada tipo de protocolo que se necesitara, como: FTP,SMTP, etc., la pertenencia a una VLAN puede basarse en una combinacion de factores como el tipo de puerto, la MAC address, protocolo, etc.



En la imagen se ve que se creo una VLAN independiente para el protocolo FTP, MAC, subred, etc.[23]

[22] http://slideplayer.es/slide/4021292/
[23] http://slideplayer.es/slide/4021292/

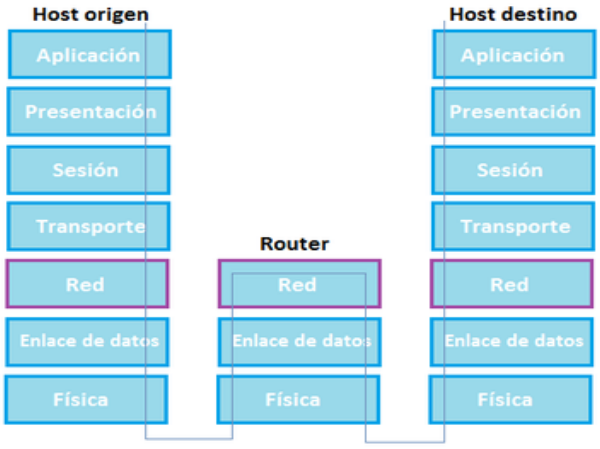
2.13 Router

También conocido como enrutador o encaminador, es un dispositivo de red que permite el enrutamiento de paquetes entre redes independientes, es decir, interconecta redes, este enrutamiento se realiza de acuerdo a un conjunto de reglas que forman la tabla de enrutamiento, opera en la capa 3 del modelo OSI, un router utiliza protocolos de enrutamiento que le permite comunicarse con otros enrutadores para compartir información entre si y determinar cuál es la ruta más rápida o adecuada para enviar datos, la función de enrutamiento trata las direcciones IP en función de sus direcciones de red definidas por la máscara de subred y las direcciona de acuerdo a su tabla de enrutamiento, los protocolos de enrutamiento pueden ser implementados de acuerdo a la arquitectura de la red y los enlaces de comunicación entre los sitios y entre las redes, un router permite que varias redes compartan la misma conexión a internet.

Esquema de uso de un router[24]

2.14 Protocolos de enrutamiento

Los protocolos de enrutamiento permiten el intercambio de información entre routers, los más comunes son:
Estado de enlace: se basa en la calidad y el rendimiento del medio de comunicación que los separa, de este modo cada router puede construir una tabla del estado de la red para utilizar la mejor ruta **(OSPF)**
Vector distancia: cada router indica a los otros la routers la distancia que los separa, estos elaboran una cartografía de cada host en la red **(RIP)**
Hibrido: combina los protocolos de OSPF y de RIP, formando el protocolo **EIGRP**.



Esquema del proceso de enrutamiento en el modelo OSI[25]

[24] http://www.wonderwhizkids.com/wwkimages/Know_Why/Router_2.jpg
[25] https://upload.wikimedia.org/wikipedia/commons/thumb/d/d6/OSI_model_router.png/440px-OSI_model_router.png

2.15 Firewall

También conocido como cortafuegos, se encarga gestiona y filtra el trafico entrante y saliente entre dos redes u ordenadores de una misma red, el trafico entrante o saliente tiene que cumplir una seria de reglas o políticas configuradas en el FW para que pueda acceder o salir de una red, host o servidor, en caso de no cumplir con las reglas o políticas establecidas por el FW el tráfico entrante o saliente será bloqueado, es decir, el FW es una barrera protectora que examina el tráfico de red entrante y/o saliente para decir que paquetes deben pasar y cuales bloquear en función de reglas previamente establecidas, estas medidas de seguridad pueden mitigar ciertas vulnerabilidades conocidas como puertos abiertos de manera innecesaria, impedir el acceso no autorizado a una red, host o servicio, robo o pérdida de información, infección por virus o spyware, un FW puede ser implementado por hardware (servidores, routers, etc.), software (sistemas operativos, aplicaciones, etc.) o ambas.

Para configurar las políticas de seguridad de un FW se pueden utilizar un conjunto de reglas predefinidas:

"allow": autorizar una conexión

"deny": bloquea una conexión avisando al emisor, cuando el FW recibe un "echo request" devuelve un "echo reply"

"drop": bloquea una conexión sin avisar al emisor, cuando el FW recibe un "echo request" no devuelve un "echo reply"

"any": permitir cualquiera, no es recomendable utilizar este tipo de regla ya que no se estaría aprovechando las fortalezas del FW

2.16 Tipo de Firewall

Firewall por hardware: Es un dispositivo dedicado a ser FW, comúnmente se encuentra entre el host y la conexión a la red, al ser diseñados como FW optimizan sus funciones de protección contra amenazas y una mayor configuración, además de que no consumen los recursos del host, se requiere un mayor conocimiento para su configuración, actualización y mantenimiento, algunos router's ya implementan las funciones de FW.

Firewall cisco ASA 5520 [26]

Firewall por software: Es el tipo de FW más común, económico y de fácil instalación relativamente, utiliza los recursos del host donde se encuentre instalado, muchos sistemas operativos (S.O.) ya incluyen el FW por software el cual puede ser configurado, cuando se adquiere algún FW de software es necesario tomar ciertas precauciones como: revisar que el software no contenga algún virus o malware malicioso que provocaría vulnerabilidades en el S.O., que sea compatible con el S.O. del host donde se quiere instalar, se requiere menor conocimiento para la configuración y actualización del FW de software.

Netfilter es un módulo en el kernel de Linux que implementa la función de FW[27]

[26] http://www.digitcom.ca/digitcomcaciscoasa5520seriesadaptivesecurityappliances.aspx
[27] http://geekland.eu/que-es-y-para-que-sirve-un-firewall/

2.17 Ventajas de un Firewall

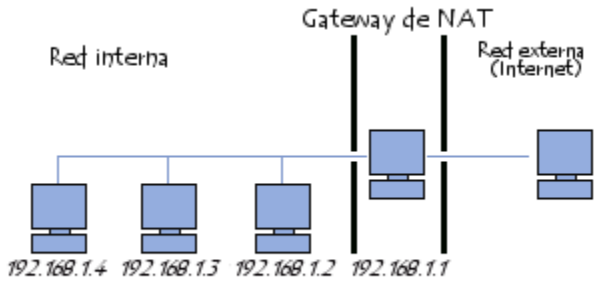
Un FW nos da la libertad de configurar las reglas y políticas que consideremos necesarias para mantener la integridad y seguridad de nuestra red, servidor o host.
Aumenta la protección contra ataques de código malicioso, virus, acceso no autorizado por puerto o protocolo
Configurar que puertos estarán abiertos y que puertos estarán cerrados, se recomienda mantener todos los puertos cerrados al menos que sean necesarios.
Configurar que tipo de protocolos podrán acceder y salir de una red, host o servidor, esto aumenta la seguridad e integridad de nuestra red, host o servidor, por ejemplo, si queremos alojar una página Web en un servidor podríamos configurar un FW para que solo permita las comunicaciones a través del puerto de Web (puerto 80) y por medio del protocolo HTTP, dejando al resto de los puertos y protocolos deshabilitados.
El FW puede ser implementado por medio de hardware, software o ambas.
Permite únicamente las conexiones autorizadas, es decir, todo lo que no está autorizado esta explícitamente prohibido
Impide cualquier conexión que está prohibida, dependiendo de las reglas que este siguiendo puede revolver un echo reply"
Un FW puede mantener un registro detallado de todo el tráfico e intentos de conexión que se producen, esto lo almacena en un log, cuando un atacante quiere encontrar un puerto abierto empieza a enviar paquetes de datos de manera aleatoria en busca de una red, host o servidor conectado y luego buscar un puerto abierto sin políticas de seguridad establecidas, teniendo una correcta configuración de FW se pueden prevenir este tipo de ataques, posteriormente se puede revisar el log de actividades de ese ataque para determinar cómo y de dónde surgió el ataque.

2.18 Desventajas de un Firewall

Un FW no puede proteger contra ataques cuyo tráfico no pase a través de él, un FW es un filtro de tráfico, por lo que en definición cualquier tráfico que no pase a través del FW constituye una vulnerabilidad a la seguridad, un usuario negligente o incluso un espía corporativo podría acceder a la red, host o servidor por medios físicos
Un FW mal configurado podría dejar puertos abiertos por los cuales un atacante podría acceder o que las políticas establecidas no consideraron posibles riesgos o amenazas de seguridad
Un FW no protege contra todos los virus o códigos maliciosos, para eso es mejor tener un antivirus actualizado.

2.19 NAT

El Network Address Translation, cuando surgió el internet se utilizó el protocolo IPv4 con 32 bits de direcciones pensando que sería suficiente para satisfacer todas las conexiones de los dispositivos a internet, sin embargo, el crecimiento exponencial de la cantidad de dispositivos que requerían una conexión a internet empezó a agotar las IP's disponibles del protocolo IPv4, fue entonces cuando surgió NAT para poder resolver este problema y eventual mente surgió el protocolo IPv6 con 128 bits de direcciones como una mejora del protocolo IPv4.
El NAT permite que múltiples dispositivos de una red interna se pueden conectar a internet utilizando la misma dirección IP publica, el NAT se implementa en un servidor como conexión de pasarela o Gateway para poder conectar todos los dispositivos de la red interna a internet, esta pasarela debe contener al menos una interfaz de red conectada a la red interna y al menos una interfaz de red conectada a internet, un router puede tener las funciones de NAT.



Esquema de un servidor NAT conectado a una red interna y a internet[28]

Para que un dispositivo de la red interna tenga acceso a internet se le debe configurar el Gateway del servidor NAT, cuando un dispositivo de la red interna realiza una petición a internet es el servidor NAT quien realiza la petición en su lugar cambiando la dirección IP privada por su dirección IP publica, el servidor NAT utiliza una tabla NAT en la que guarda una entrada por cada conexión, es decir, cuando un dispositivo de la red interna realiza una petición al exterior el servidor NAT asigna una entra en la tabla NAT y le asigna un puerto que no esté siendo utilizado para que cada vez que el servidor NAT reciba una respuesta de ese dispositivo sepa a qué IP privada devolverla, un dispositivo de la red interna es invisible al exterior, haciendo creer a las redes externas que todas las peticiones provienen del servidos NAT brindando una protección extra de seguridad.
Usaremos las siguientes IP's y puertos para demostrar el funcionamiento de un servidor NAT:

IP privada PC "A"	Puerto PC "A"	IP a la que se quiere acceder	IP publica del router	Puerto del router
192.168.3.11	5643	132.248.116.245 (www.biomedicas.unam.mx)	1.2.3.4	9898

Paquete enviado	
IP origen	192.168.3.11
Puerto origen	5643
IP destino	132.248.116.245
Puerto destino	80

El servidor NAT cambia la IP privada del dispositivo origen por la IP publica del servidor NAT, guarda el puerto origen en la tabla NAT y le asigna un puerto que no esté siendo utilizado

Servidor NAT

Paquete recibido	
IP origen	1.2.3.4
Puerto origen	9898
IP destino	132.248.116.245
Puerto destino	80

Representación del proceso de un servidor NAT enviando y recibiendo las peticiones de un dispositivo de la red interna

Si se quiere que un dispositivo de la red interna pueda ser accedido desde el exterior se deben configurar una entrada fija en las tablas NAT para establecer que todo el tráfico de un determinado puerto se envié al dispositivo de la red interna establecido en las tablas NAT

Paquete enviado	
IP origen	132.248.116.245
Puerto origen	80

[28] http://es.ccm.net/contents/271-nat-conversion-de-direcciones-de-red-habilitacion-de-puertos-y

IP destino	192.168.3.11
Puerto destino	5643

El servidor NAT cambia la IP destino de la petición externa por la IP de la red interna correspondiente desacuerdo a la tabla NAT

Servidor NAT

Paquete recibido	
IP origen	132.248.116.245
Puerto origen	80
IP destino	1.2.3.4
Puerto destino	9898

Representación del proceso de un servidor NAT recibiendo y enviando las peticiones de un dispositivo de la red externa

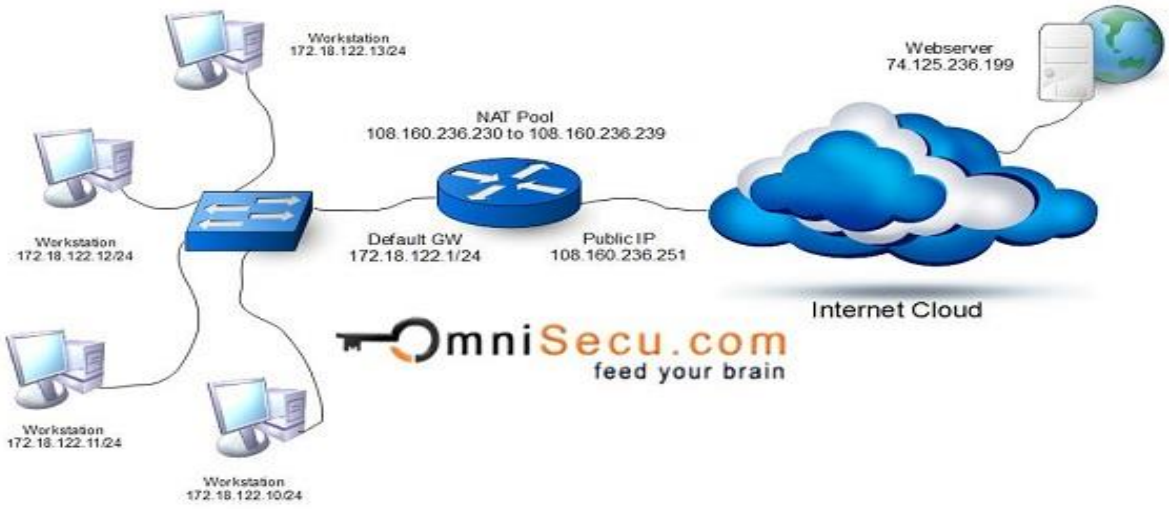
2.20 Tipos de NAT

NAT estático: El servidor NAT mapea (asigna) una dirección IP privada a una dirección IP publica de forma fija, este tipo de NAT es utilizado cuando un dispositivo dentro de la red interna tiene que estar accesible desde internet, aquí se utiliza el DNAT.

NAT estático[29]

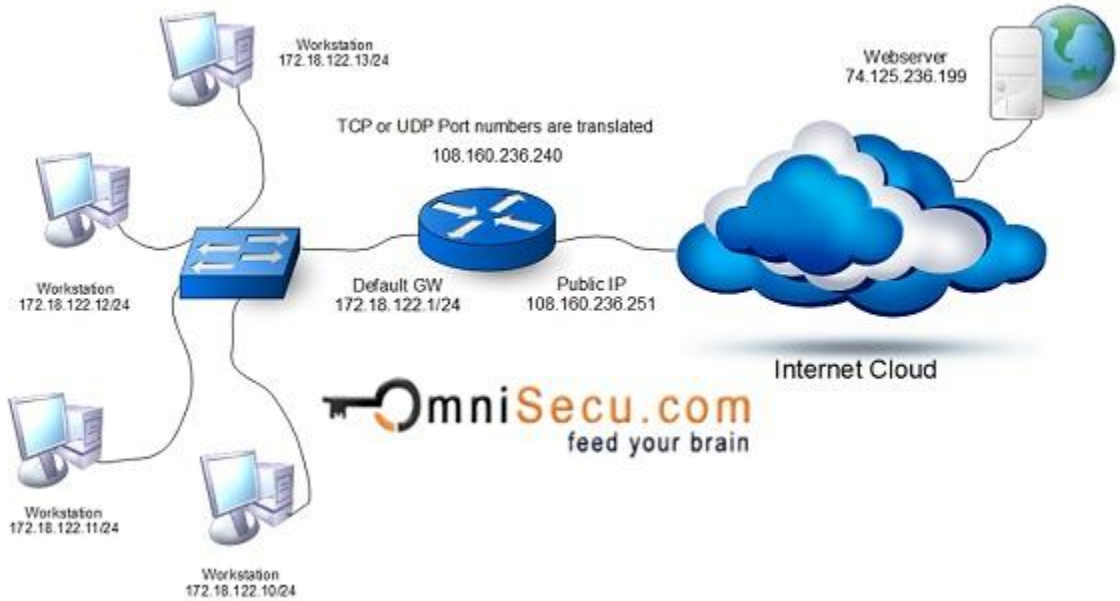
NAT dinámico: El servidor NAT establece una correspondencia de una dirección IP privada a una dirección IP publica, la IP publica es obtenida de un grupo de IP publicas configuradas en la pasarela denominado NAT pool, una dirección IP publica que se asignada a una dirección IP privada estará reservada hasta que la IP privada deje de utilizarla y se asigne a otra IP privada.

[29] http://www.omnisecu.com/cisco-certified-network-associate-ccna/static-nat-dynamic-nat-and-pat.php



NAT dinámico[30]

NAT PAT: Port Address Translation, asigna varias direcciones IP privadas a una única dirección IP publica, cuando un dispositivo de la red interna hace una petición a internet el servidor NAT realiza la petición en su lugar cambiando la dirección y puerto por la propia, en una tabla guarda la asignación de puertos para saber a quién referencia la información una vez recibe una respuesta, aquí se utiliza el SNAT.



NAT PAT[31]

[30] http://www.omnisecu.com/cisco-certified-network-associate-ccna/static-nat-dynamic-nat-and-pat.php
[31] http://www.omnisecu.com/cisco-certified-network-associate-ccna/static-nat-dynamic-nat-and-pat.php

CAPÍTULO III
SITUACIÓN ACTUAL

3.1 Antecedentes de la red actual

La Sección de Computo ha hecho varios esfuerzos para mantener operando óptimamente la red de datos en ambas sedes del Instituto de Investigaciones Biomédicas, por múltiples factores como es la disposición de recursos económicos suficientes para adquirir los equipos de telecomunicaciones necesarios y asegurar la compatibilidad entre las diferentes marcas instaladas en los IDF's por otro lado, el rendimiento de la red de datos instalada actualmente en la nueva sede es aceptable pero aún existe el reto de adecuarla a la nuevas necesidades del Instituto, como es el caso del circuito cerrado que hoy en día presenta retraso en el monitoreo en tiempo real de las cámaras de seguridad.

Cuando se construyó la Nueva sede del Instituto se siguió la misma política de instalación y configuración de los equipos activos en la red de la antigua sede, heredando así también los problemas que se presentaban anteriormente, como es el caso de la duplicidad de direcciones IP, y el tráfico de red poco estructurado. En sus inicios la infraestructura de red de la Nueva sede era suficiente para permitir el acceso a la red de datos a todos los usuarios y en la medida que se fueron migrando usuarios de la Sede anterior a la nueva gradualmente el personal encargado de la administración de la red fue agregando equipos de telecomunicaciones para cubrir los requerimientos de la red que surgieron en su momento, aunque la creciente demanda en los servicios de red y las nuevos requerimientos de los usuarios de la red de datos han provocado la necesidad de reestructurar el diseño lógico de la red.

De acuerdo a los registros de la Sección de Cómputo del Instituto se tiene que en el 2009 la infraestructura de red de la Nueva sede estaba basada en la marca 3com, la cual tenía un desempeño satisfactorio aunado a que tenían muy buen desempeño los equipos ante la variación de corriente eléctrica, algo que coloquialmente se le llama "hechos para toda la vida", sin embargo en Tecnologías de Información y Comunicación en bien sabido que este paradigma es imposible de mantener dado que en este mundo tan cambiante la tecnología se renueva de forma constante; ante esto la Sección de Cómputo decidió actualizar los equipos activos de la red en capa 2 del modelo OSI y consideró en primera instancia la adquisición de equipos 3com 5500 para evitar problemas de compatibilidad y explotar al máximo las bondades que ofrecía la marca, mismos que fueron sustituidos en áreas estratégicas; para atender el punto anterior se diseñó un plan de rotación de la infraestructura de la red de datos evaluando los requerimientos de red por parte de la comunidad académica y el costo-beneficio que aportaban las principales marcas de equipos de red para la administración de éstos. Después de realizar la evaluación de los equipos de red finalmente se tomó la decisión de apostar por la misma marca, pero hubo un inconveniente, en abril de 2010 *3com* fue adquirida por la compañía *HP*; durante

la transición los costos de los equipos se elevaron a tal grado que ya no fue viable adquirir nuevos equipos de esta marca. Posteriormente se reevaluó el proyecto nuevamente teniendo como premisa la necesidad de ofrecer a la comunidad un servicio de red confiable y esta vez se eligió la marca *Enterasys* por el gran desempeño de los equipos y la durabilidad, pero nuevamente se repitió la experiencia en 2013, esta vez *Enterasys* fue adquirida por *Extreme Networks*.
Actualmente la infraestructura de red de la nueva sede está basada en su mayoría en Enterasys seguido de 3com-HP en un ambiente mixto y se tiene planeado cambiar la infraestructura de red a *Cisco* por el prestigio de la marca y la confiabilidad en el mercado que ha servido de referencia en el mundo de las telecomunicaciones y ha permanecido a la vanguardia por varios años, por lo que es poco probable que sea absorbida por otra marca y/o desaparezca del mercado.
Es importante mencionar que se tiene pensado a futuro migrar a la comunidad académica restante en la antigua sede a la nueva en el mediano plazo y teniendo en cuenta lo anterior aunado a la falta de presupuesto para adquirir switches, se diseñó la estrategia de mantener la red de la antigua sede con los equipos actualmente instalados y en caso de que se presentará alguna incidencia por daño físico en un equipo, sustituirlo con el stock de switches recuperados que se tiene en la Sección de cómputo.
Cualquier red de datos funcional debe contar con ciertas características esenciales como buenas prácticas para mantenerse en buen funcionamiento y no tener problemas innecesarios a largo plazo, se debe planificar la topología física y lógica que cumpliría mejor con la demanda y estructura de la red para la institución.

3.2 Descripción de la red actual

La infraestructura de red del Instituto de Investigaciones Biomédicas en sus inicios se pensó y diseño para cubrir la demanda de cada uno de los usuarios que se tenía en su fundación en el 2007. La nueva sede cubría las necesidades de la comunidad académica de aquel entonces, paulatinamente el aumento de usuarios hizo necesaria la adquisición de nuevo equipo, teniendo un crecimiento tan grande en tan poco tiempo; el control de las redes y su configuración solo se limitó a proveer el acceso a la red a cada uno de los académicos de la institución, desatendiendo problemas que en redes pequeñas no podrían ser tan notorios o perjudiciales.
Ahora la demanda actual de acceso a la red requiere una mejor administración que permita una administración más eficiente y evitar problemas ya detectado como lo son:

- Saturación del ancho de banda
- Perdida de información
- Problemas de enrutamiento
- Seguridad en la red
- Duplicidad de IP

Entre otros tantos problemas estos son los de mayor relevancia para la institución.
Se examinó el funcionamiento y configuración actual de la infraestructura de red, definiendo algunos puntos prioritarios como son:

- Topología lógica
- Topología física
- Distribución del medio y métodos utilizados
- Políticas de seguridad
- Prioridad de servicio (roles) dentro de la comunidad académica

Recursos disponibles para brindar los servicios que tiene la institución y el acceso a la red
Una vez detectados los problemas actuales de la red y analizada la infraestructura se listaron los programas (software) y/o herramientas con las que deberá contara la institución para aumentar la seguridad en la red.

Esta recopilación de información se utilizó para elaborar una proyección a futuro de lo que era posible realizar y como llevarlo a cabo, en base a los recursos disponibles por parte de la institución ya que un cambio completo de equipo no era factible en este momento por la falta de recursos económicos, los que nos llevó al uso de:

- Tecnologías Open Sourse
- Metodologías renovadas para la segmentación de red empleando VLAN
- Implementación de políticas de seguridad más estrictas dentro del FW/NAT/GW
- Asignación de roles para los usuarios de la red de la comunidad académica (por cuestiones de seguridad ya que cada usuario tiene una necesidad diferente y tener un registro más preciso de la estructura de la red del Instituto de Investigaciones Biomédicas)

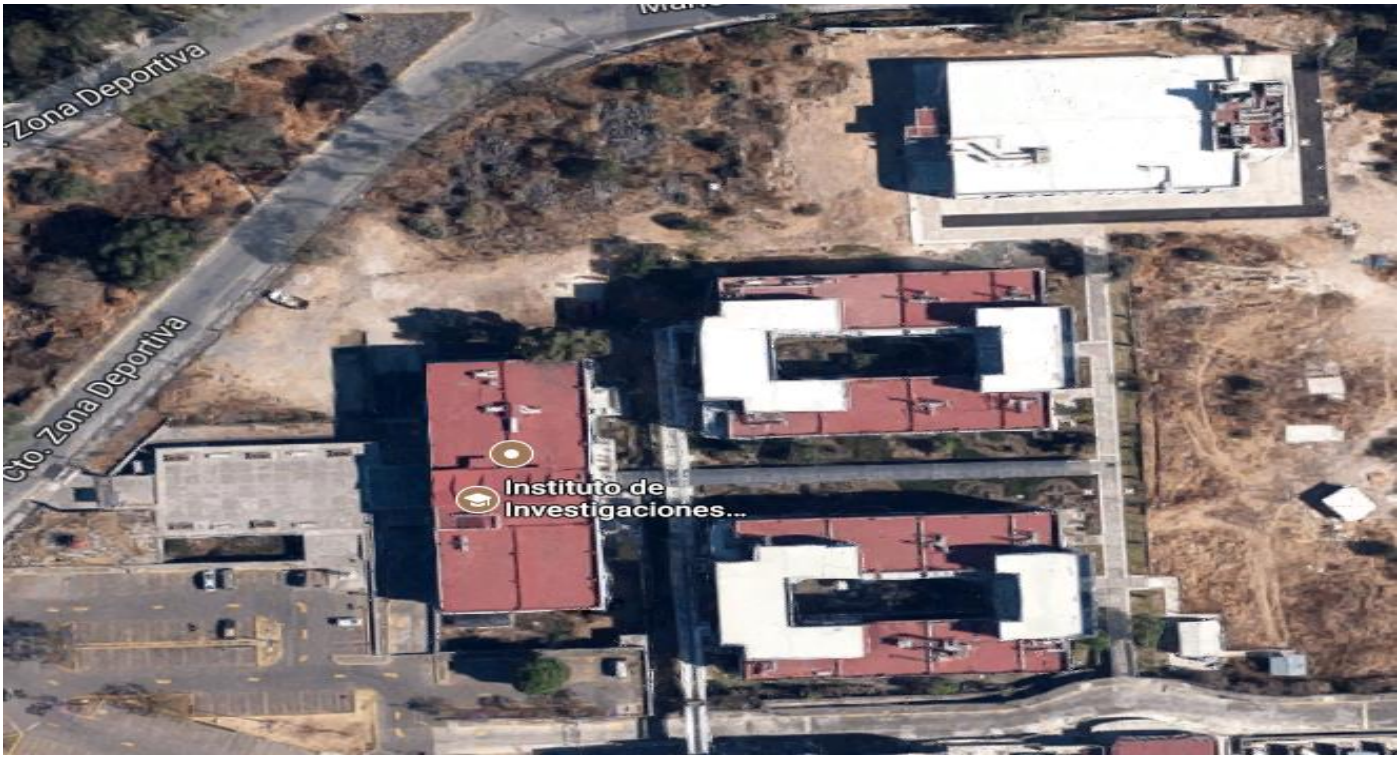
Como el S.O. GNU/Linux de la distribución Debian, la herramienta Iptables para administrar las políticas de seguridad que filtran el tráfico en la red dentro del FW/NAT/GW, así como la disposición de switch's capaces de soportar varias VLAN's a tasas de transferencia de 10/100/1000 Mbps.
Para implementar correctamente la segmentación de la red por medio de tecnología VLAN se debe analizar las características de los Switch con los que se cuentan para asegurar que soportaran correctamente la implementación de estas y tener una mejor administración de la red.
La condición actual de la red, (el Broadcast puede llegar a todos los dispositivos de los edificios del Instituto de Investigaciones Biomédicas), compromete la escalabilidad, buen funcionamiento y administración de los servicios a los diferentes edificios que lo componen:

- Edificio A
- Edificio B
- Edificio C
- Unidad de Modelos Biológicos
- Auditorio (como anexo del edifico A)

El diseño actual de la infraestructura a de red de la nueva sede esta basa en la topología jerárquica siendo el FW/NAT/GW quien controla y restringe los segmentos anteriormente mencionados.
Se plantea tener una mejor administración, segmentación, flexibilidad y seguridad de la red LAN con la implementación de tecnologías VLAN y mejor asignación de recursos a servicios prioritarios.
Esto mejorara la distribución de recursos, el tráfico, asignación de prioridad de servicio en base a funciones, servicios diferenciados ofrecidos en cada SW y disminuirá el riesgo de duplicidad de direcciones IP.

3.3 Topología física actual

En total la nueva sede está constituido por 4 edificios donde la sección la sección de computo está encargada de brindarles acceso a la red y mantener en óptimas condiciones el estado de la misma. En la fundación de la nueva sede solo se tenía contemplado los requerimientos de dos edificios, entonces se diseñó una infraestructura de red que cumpliera con las necesidades de los usuarios de aquel entonces, paulatinamente se fueron construyendo dos nuevos edificios que necesitarían de igual forma acceso a la red, lo que llevo a que la infraestructura de red creciera.
La sección de computo se encarga de brindarle servicio al Edificio A, Edificio B, Edificio C, Unidad de Modelos Biológicos y Auditorio (como anexo del edifico A).



Vista aérea del instituto de Investigaciones Biomédicas de la nueva sede

En la topología física actual del Instituto de Investigaciones Biomédicas de la nueva sede se tiene contemplado un total de 596 host de la comunidad académica, y es la siguiente:
En el Edificio “A” se tiene contemplado un total de 124 host de la comunidad académica, mismos que se encuentran distribuidos de la siguiente manera:

En el Edificio “A” del Instituto se tiene contemplado un total de 124 host de la comunidad académica, mismos que se encuentran distribuidos de la siguiente manera:

Edificio “A”, Planta baja, 40 host:

- Salón 7: 11 PC
- Sala de videoconferencias: 1 códec de videoconferencias, 1 PC
- Secretaria técnica: 3PC, 1 router, 1 impresora en red
- AAPAUNAM: 1 PC
- Delegación administrativa: 1 PC, 1 router
- Jefe de servicios generales: 2 PC
- Servicios generales: 2 PC
- Secretaria de enseñanza: 4 PC, 1 router, 1 impresora en red
- Auditorio: 1 PC, 1 router, 1 codec
- Pasillo: 2 cámara
- MDF 1: 4 SW
  - SW core: SW “A”
  - SW de distribución y acceso: SW “B”
  - SW de acceso: SW “C” y SW “D”)

Edificio “A”, Planta Baja

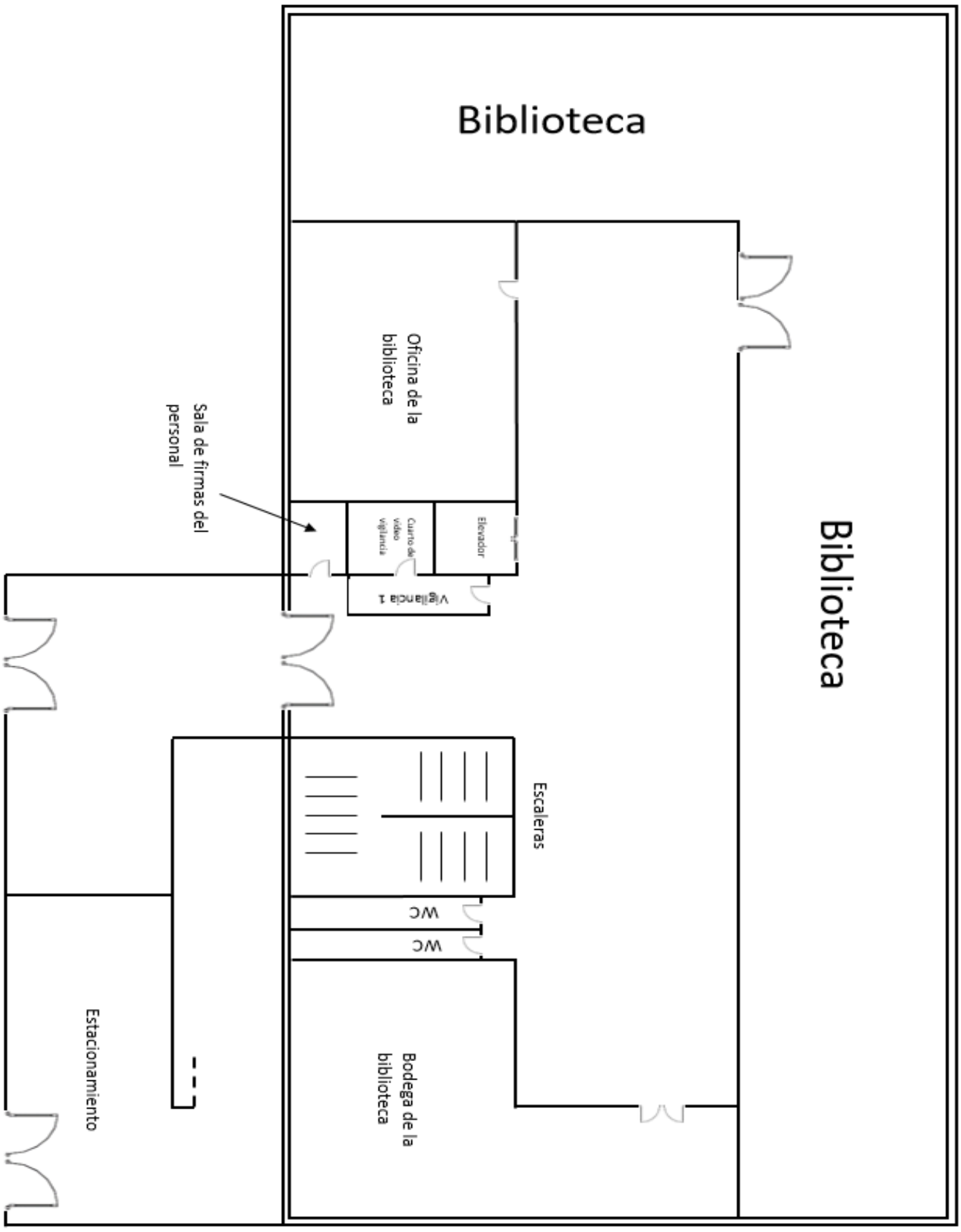
-Diagrama físico del Edificio “A”, Planta Baja

-Ubicación de los equipos en el diagrama físico del Edificio “A”, Planta Baja

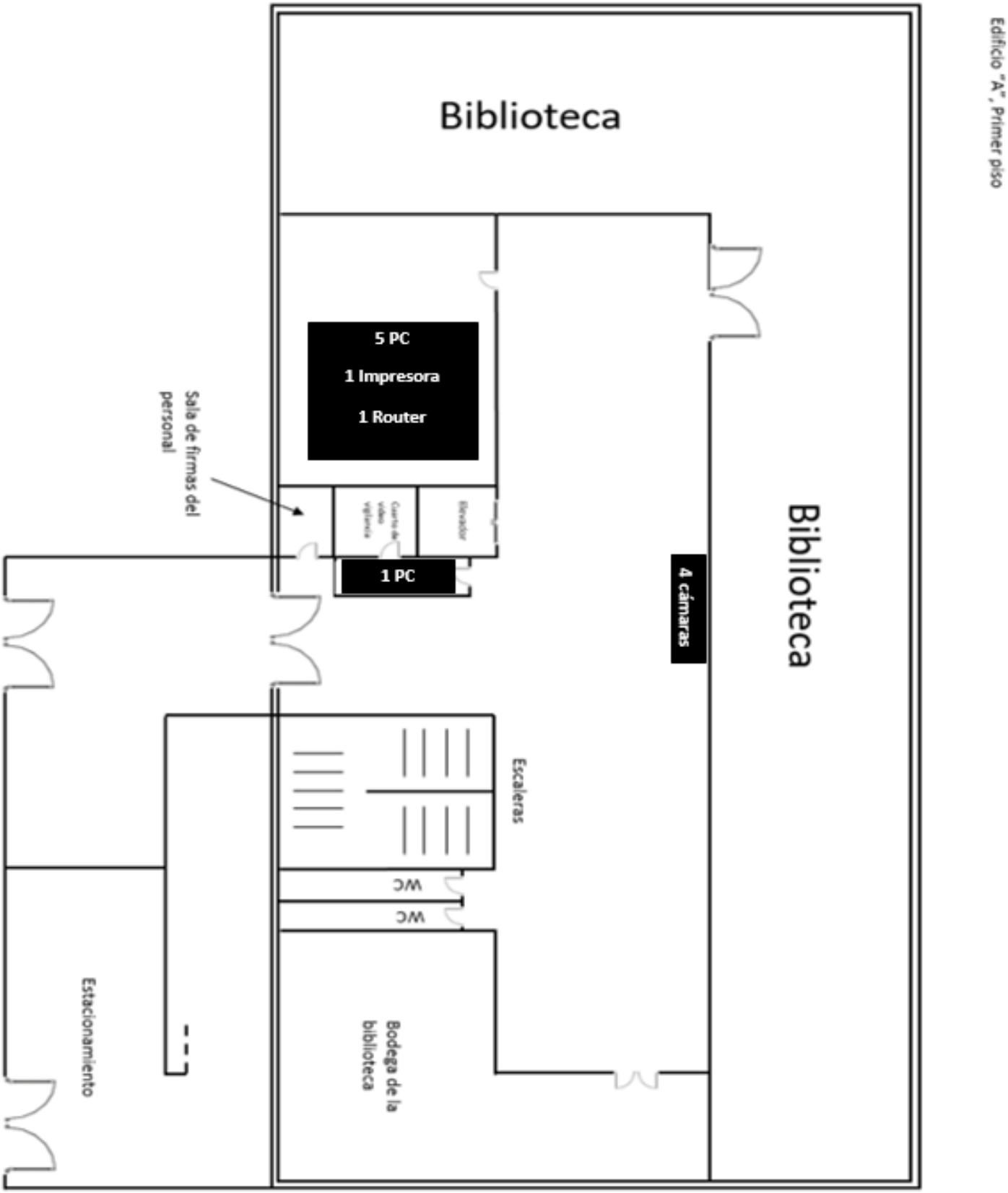
Edificio “A”, Primer piso, 12 host:

- Oficina de la biblioteca: 5 PC, 1 impresora en red, 1 router
- Cuarto de video vigilancia: 1 PC
- Pasillo: 4 cámara

-Diagrama físico del Edificio “A”, Primer Piso



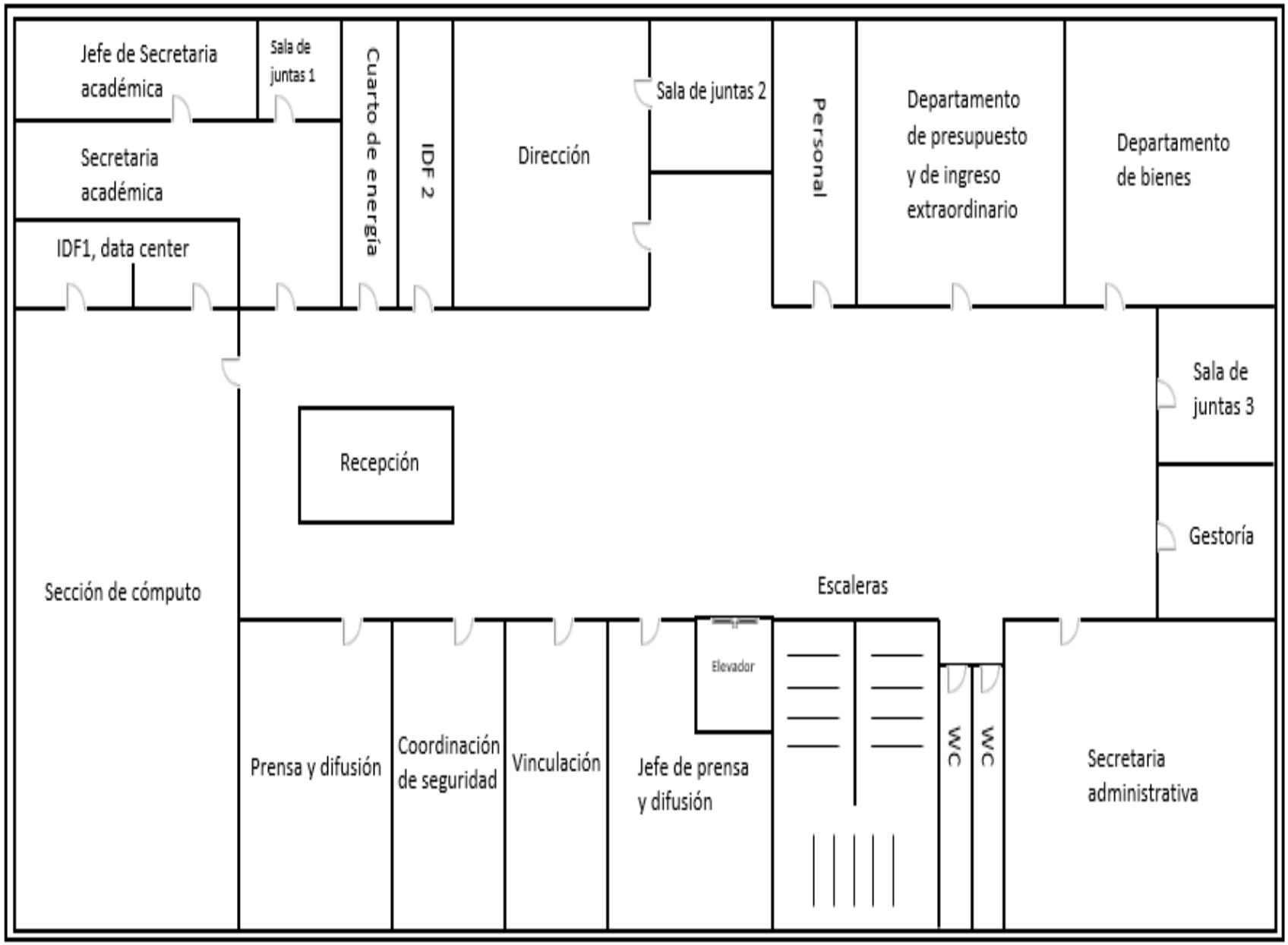
-Ubicación de los equipos en el diagrama físico del Edificio “A”, Primer Piso



Edificio “A”, Segundo piso, 72 host:

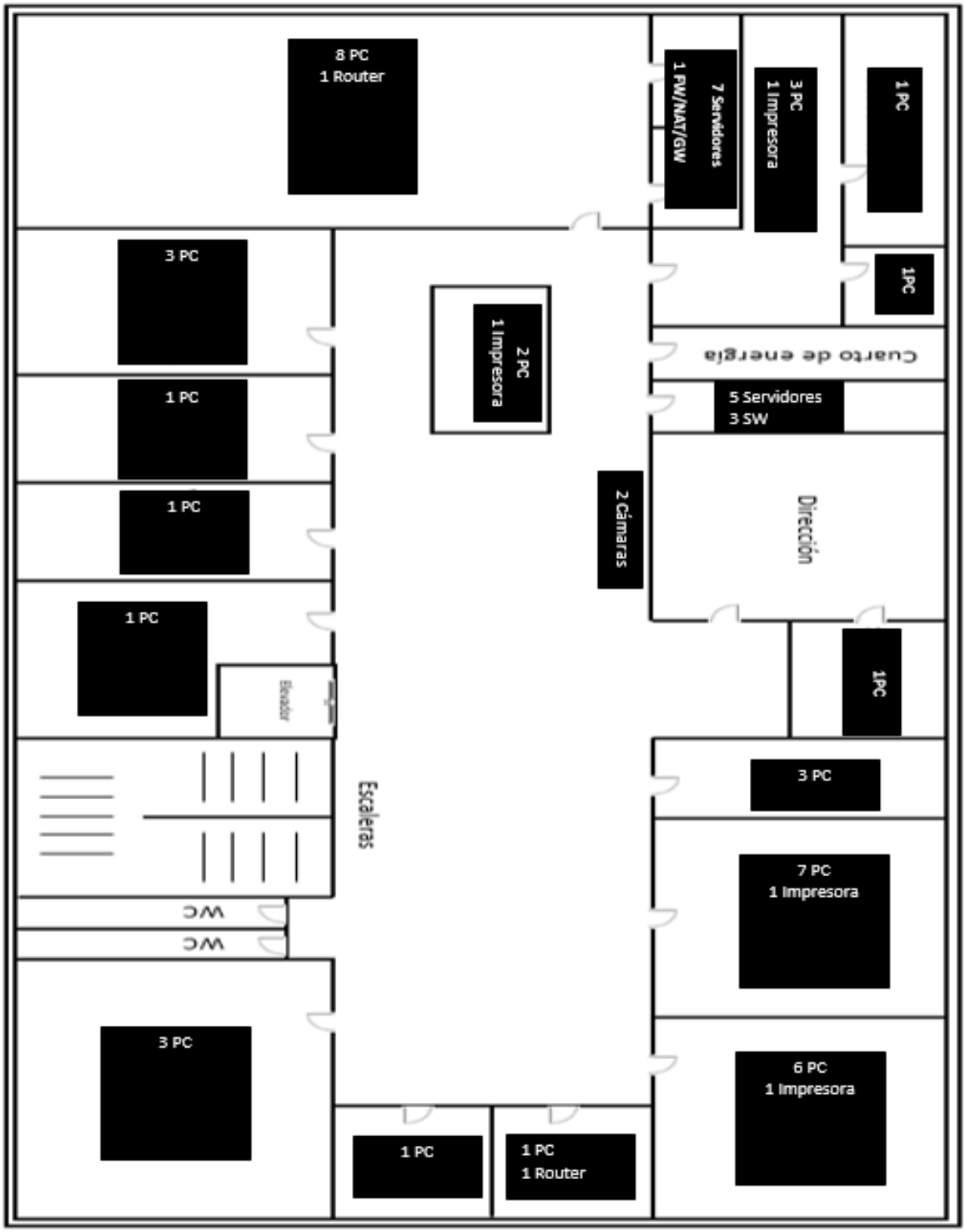
- IDF 1: 7 servidores, 1 FW/NAT/GW, 1 SW → SW de acceso: SW “H”
- IDF 2: 5 servidores, 3 SW → SW en stack: SW “E”, SW “F” y SW “G”
- Jefe de secretaria académica: 1 PC
- Secretaria académica: 3 PC, 1 impresora en red
- Sala de juntas 1: 1 PC
- Dirección: 3 PC, 1 router
- Sala de juntas 2: 1 PC
- Personal: 3 PC
- Departamento de presupuesto y de ingreso extraordinario: 7 PC, 1 impresora en red
- Departamento de bienes:6 PC, 1 impresora en red
- Sala de juntas 3: 1 PC, 1 router
- Gestoría: 1 PC
- Secretaria administrativa: 3 PC
- Jefe de prensa y difusión: 1 PC
- Vinculación: 1 PC
- Coordinación de seguridad: 1 PC
- Prensa y difusión: 3 PC
- Sección de cómputo: 8 PC, 1 router
- Recepción: 2 PC, 1 impresoras en red
- Pasillo: 2 cámaras

Edificio “A”, Segundo piso



-Diagrama físico del Edificio “A”, Segundo Piso

-Ubicación de los equipos en el diagrama físico del Edificio “A”, Segundo Piso

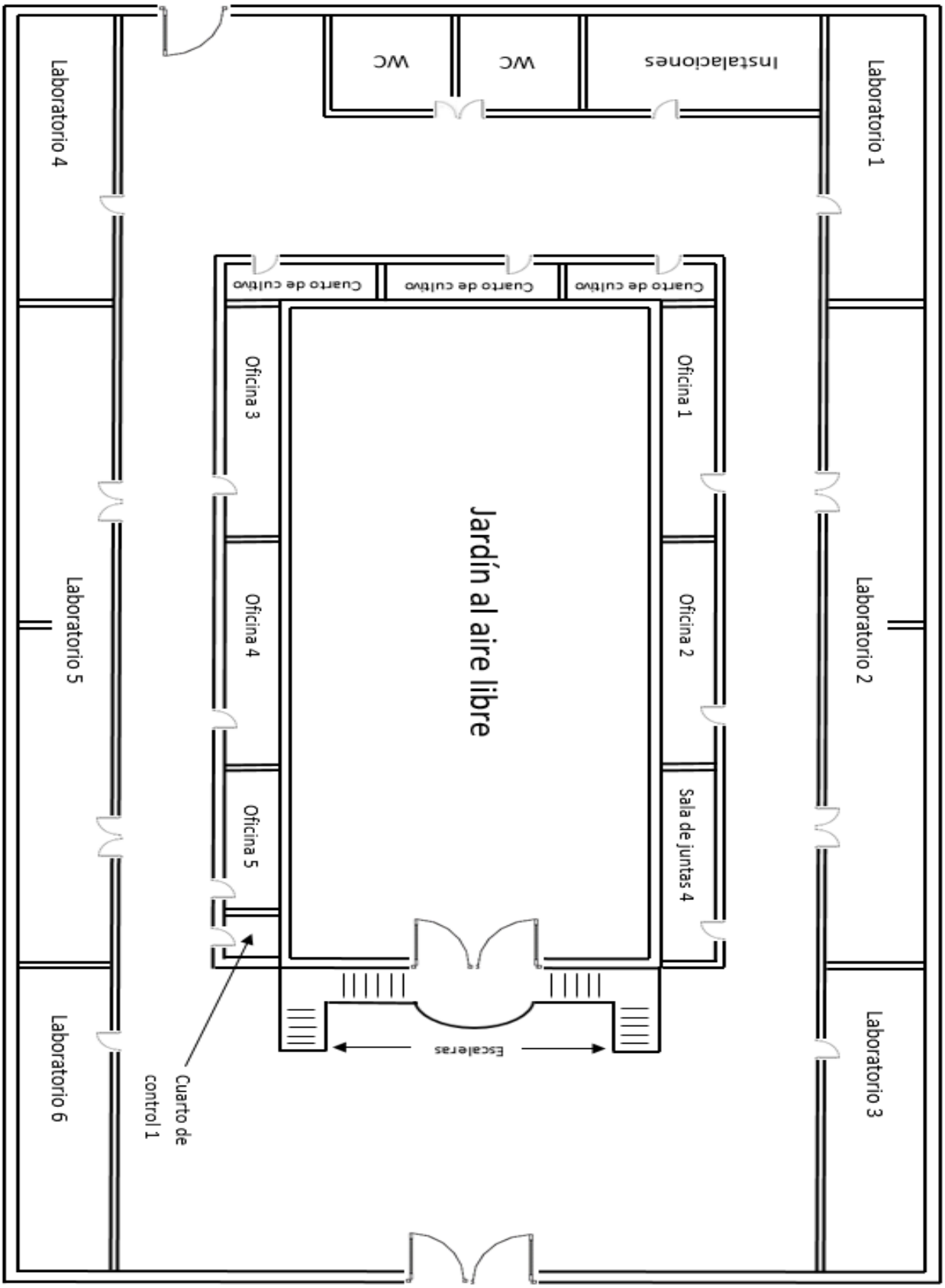


En el Edificio “B” del Instituto se tiene contemplado un total de 221 host de la comunidad académica, mismos que se encuentran distribuidos de la siguiente manera:

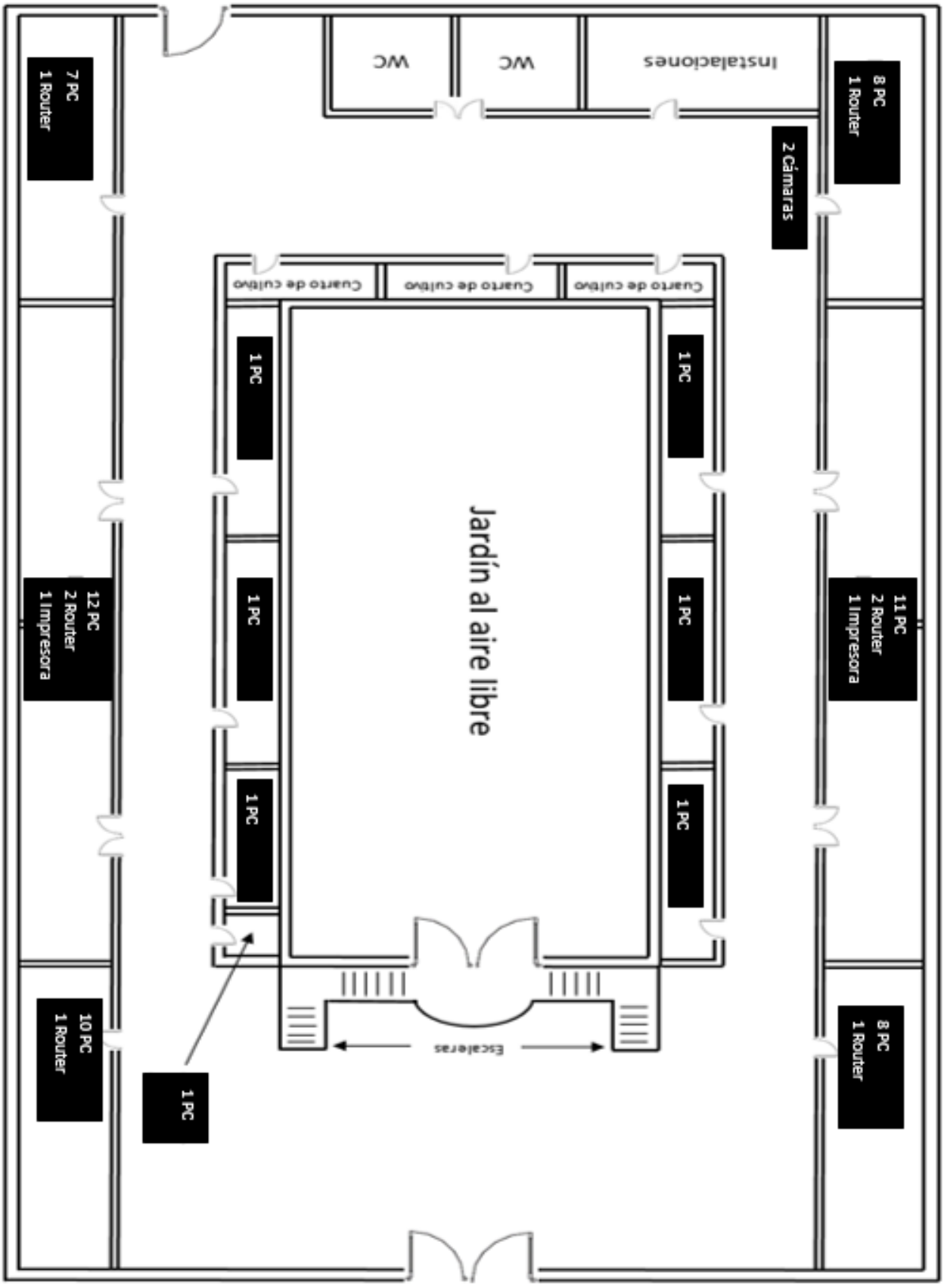
Edificio “B”, Planta baja, 75 host:

- Laboratorio 1: 8 PC, 1 router
- Laboratorio 2: 11 PC, 2 router, 1 impresora en red
- Laboratorio 3: 8 PC, 1 router
- Laboratorio 4: 7 PC, 1 router
- Laboratorio 5: 12 PC, 2 router, 1 impresora en red
- Laboratorio 6: 10 PC, 1 router
- Oficina 1: 1 PC
- Oficina 2: 1 PC
- Oficina 3: 1 PC
- Oficina 4: 1 PC
- Oficina 5: 1 PC
- Sala de juntas 4: 1 PC
- Cuarto de control 1: 1 PC
- Pasillos: 2 cámaras

-Diagrama físico del Edificio “B”, Planta Baja



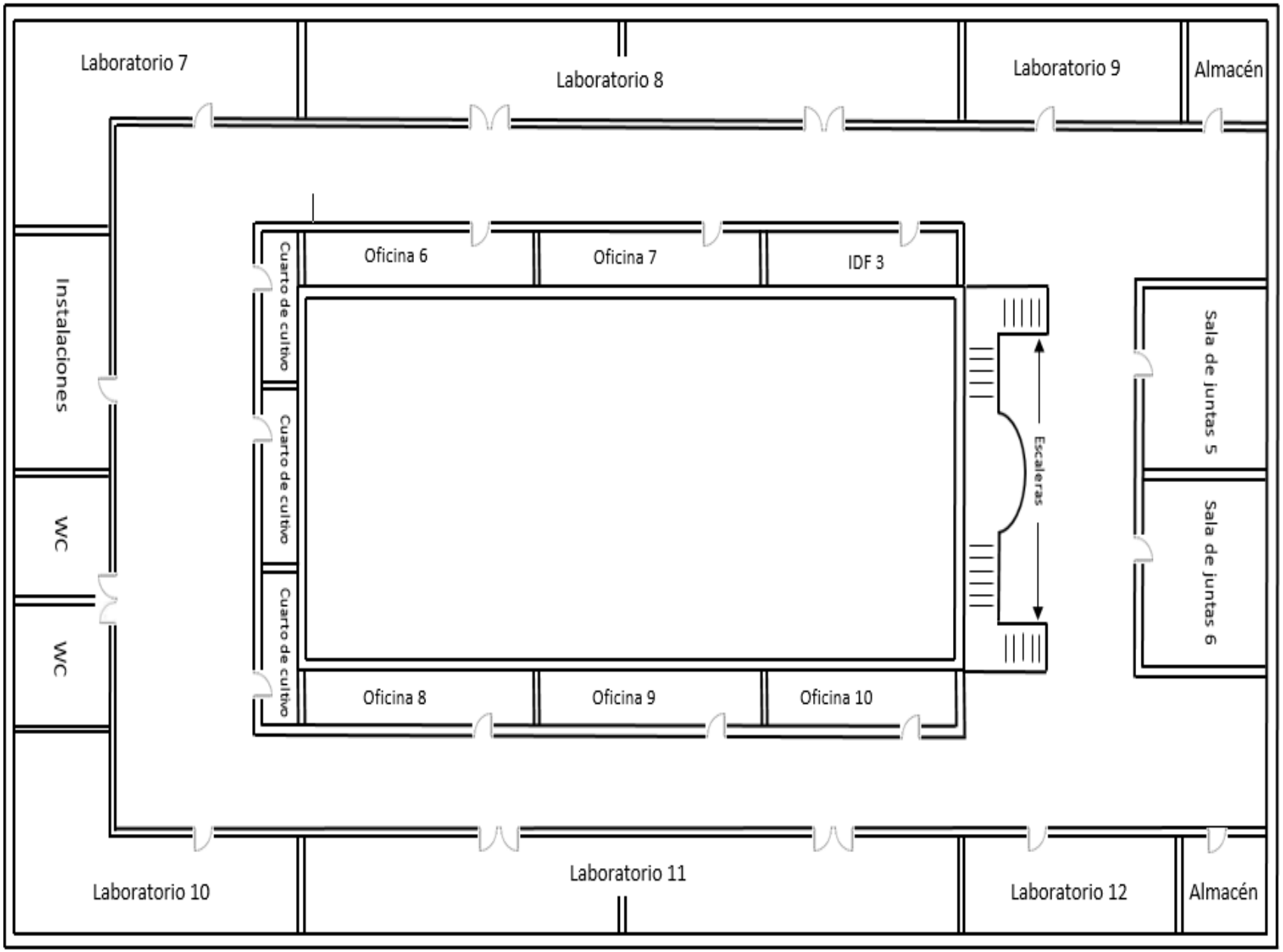
-Ubicación de los equipos en el diagrama físico del Edificio “B”, Planta Baja



Edificio “B”, Primer piso, 75 host:

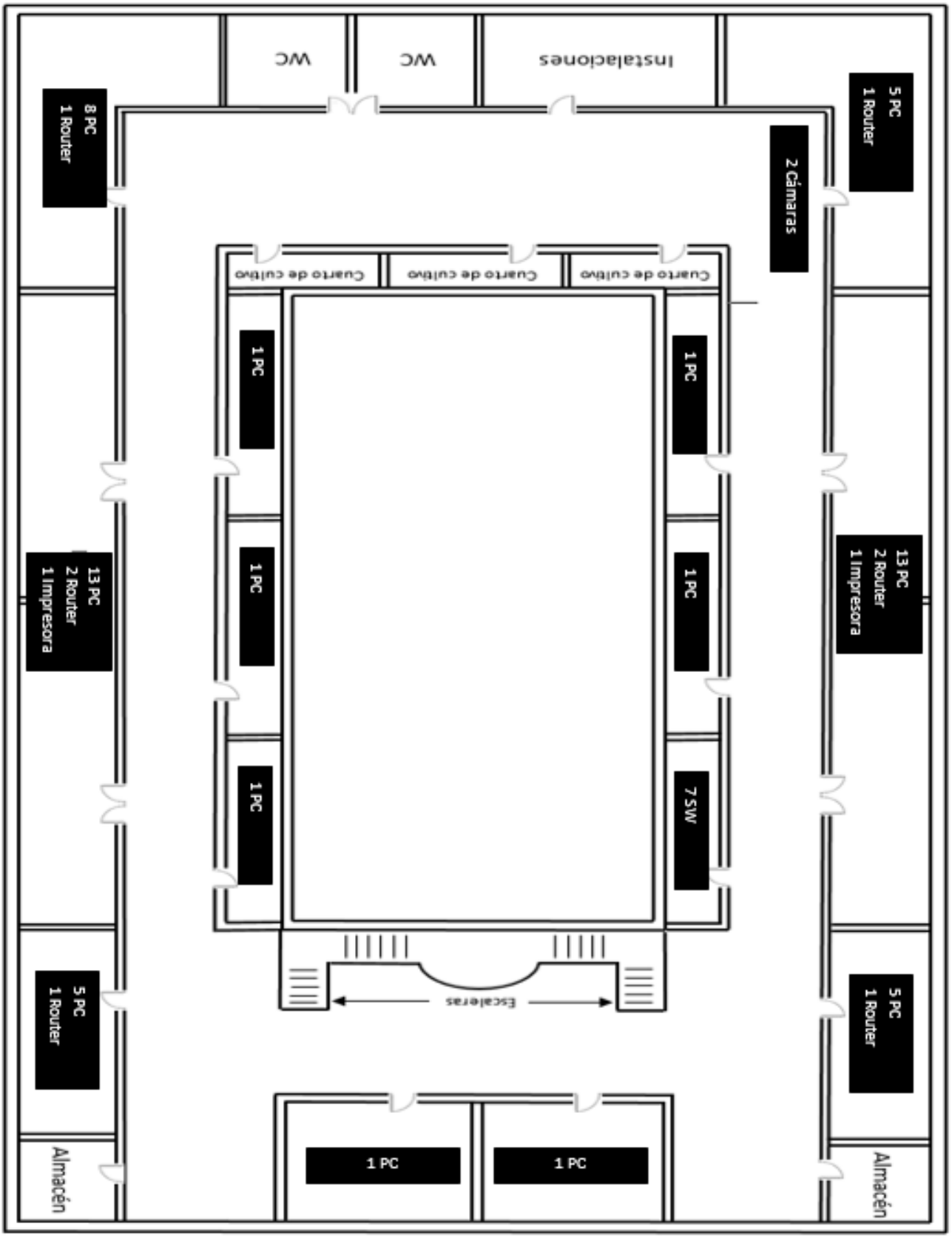
- Laboratorio 7: 5 PC, 1 router
- Laboratorio 8: 13 PC, 2 router, 1 impresora en red
- Laboratorio 9: 5 PC, 1 router
- Laboratorio 10: 8 PC, 1 router
- Laboratorio 11: 13 PC, 2 router, 1 impresora en red
- Laboratorio 12: 5 PC, 1 router
- Oficina 6: 1 PC
- Oficina 7: 1 PC
- Oficina 8: 1 PC
- Oficina 9: 1 PC
- Oficina 10: 1 PC
- Sala de juntas 5: 1 PC
- Sala de juntas 6: 1 PC
- Pasillos: 2 cámaras
- IDF 3: 7SW
  - SW de distribución: SW “I”.
  - SW de acceso: SW “J”, SW “K”, SW “L”, SW “M”, SW “N” y SW “O”)

Edificio “B”, Primer piso



-Diagrama físico del Edificio “B”, Primer Piso

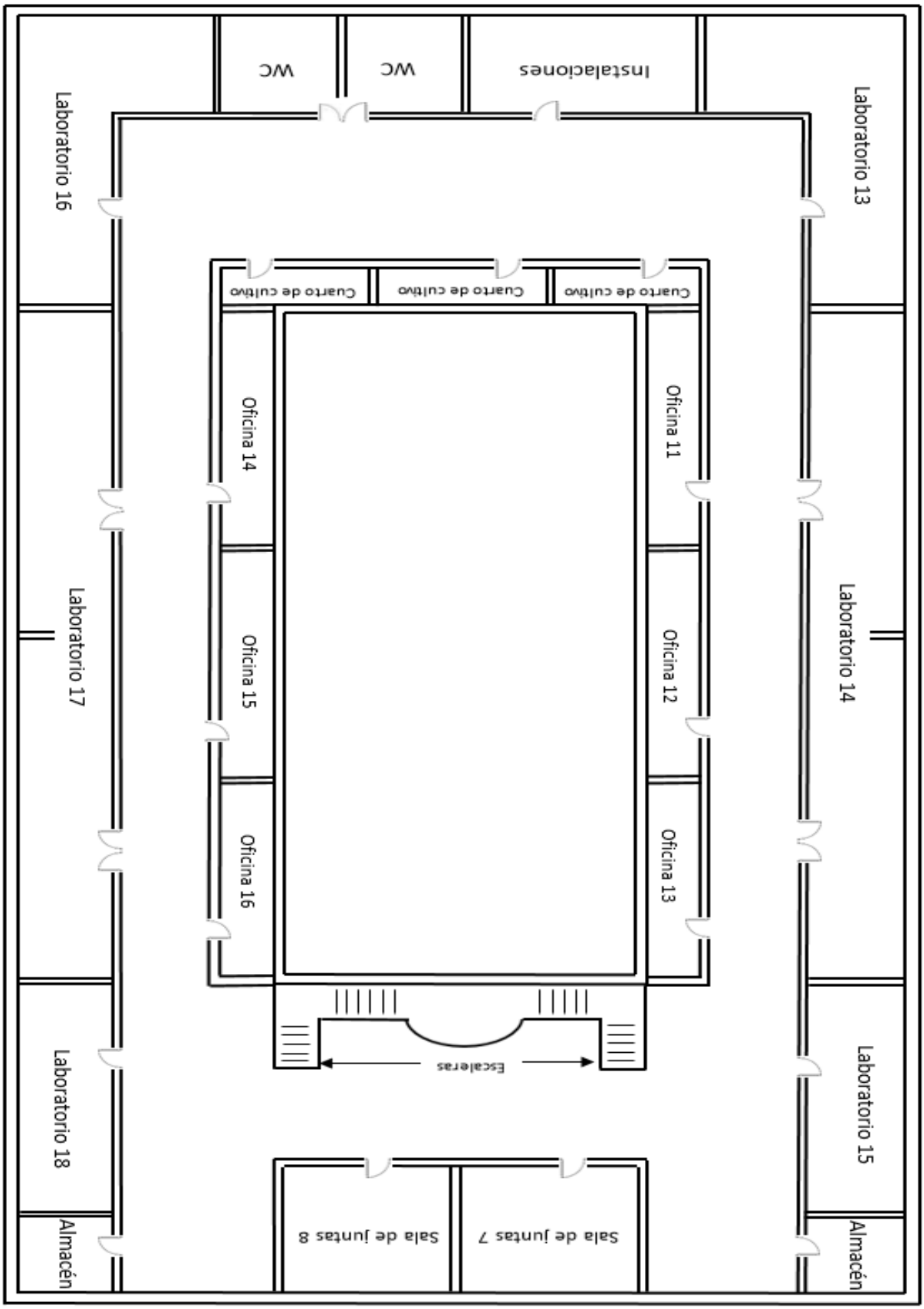
-Ubicación de los equipos en el diagrama físico del Edificio “B”, Primer Piso



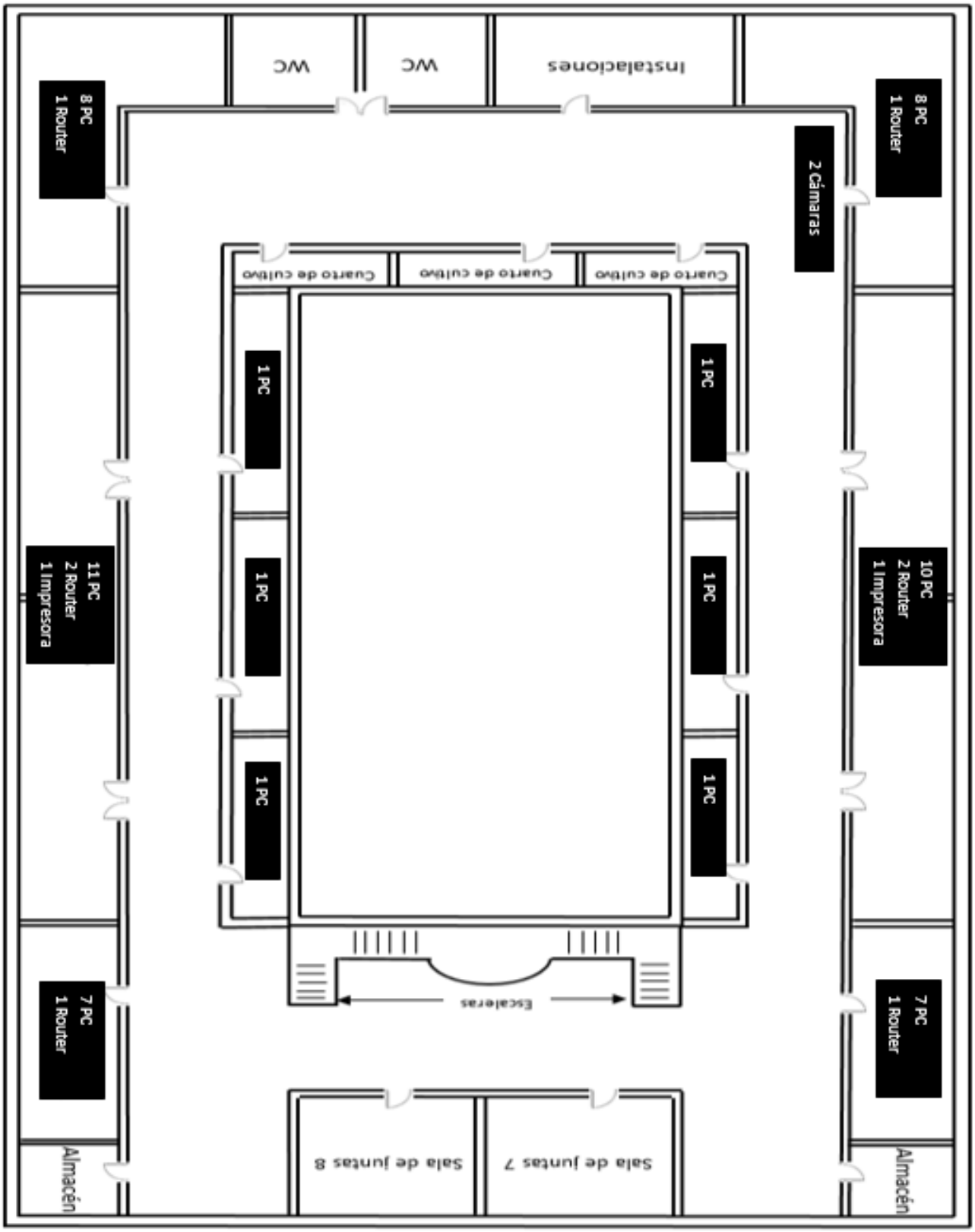
Edificio “B”, Segundo piso, 71 host:

- Laboratorio 13: 8 PC, 1 router
- Laboratorio 14: 10 PC, 2 router, 1 impresora en red
- Laboratorio 15: 7 PC, 1 router
- Laboratorio 16: 8 PC, 1 router
- Laboratorio 17: 11 PC, 2 router, 1 impresora en red
- Laboratorio 18: 7 PC, 1 router
- Oficina 11: 1 PC
- Oficina 12: 1 P C
- Oficina 13: 1 PC
- Oficina 14: 1 PC
- Oficina 15: 1 PC
- Oficina 16: 1 PC
- Sala de juntas 7: 1 PC
- Sala de juntas 8: 1 PC
- Pasillos: 2 cámaras

-Diagrama físico del Edificio “B”, Segundo Piso



-Ubicación de los equipos en el diagrama físico del Edificio “B”, Segundo Piso

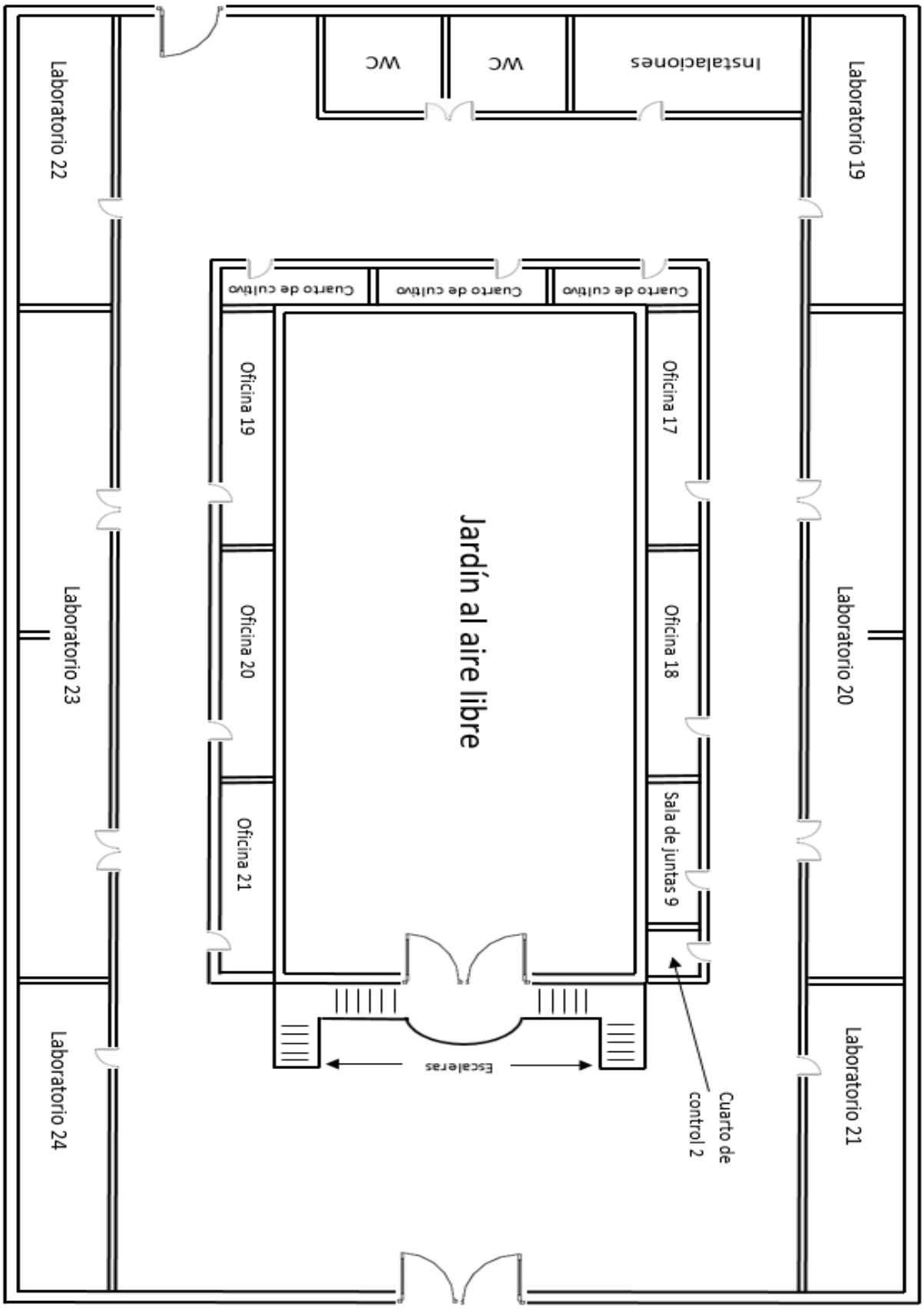


En el Edificio “C” del Instituto se tiene contemplado un total de 229 host de la comunidad académica, mismos que se encuentran distribuidos de la siguiente manera:

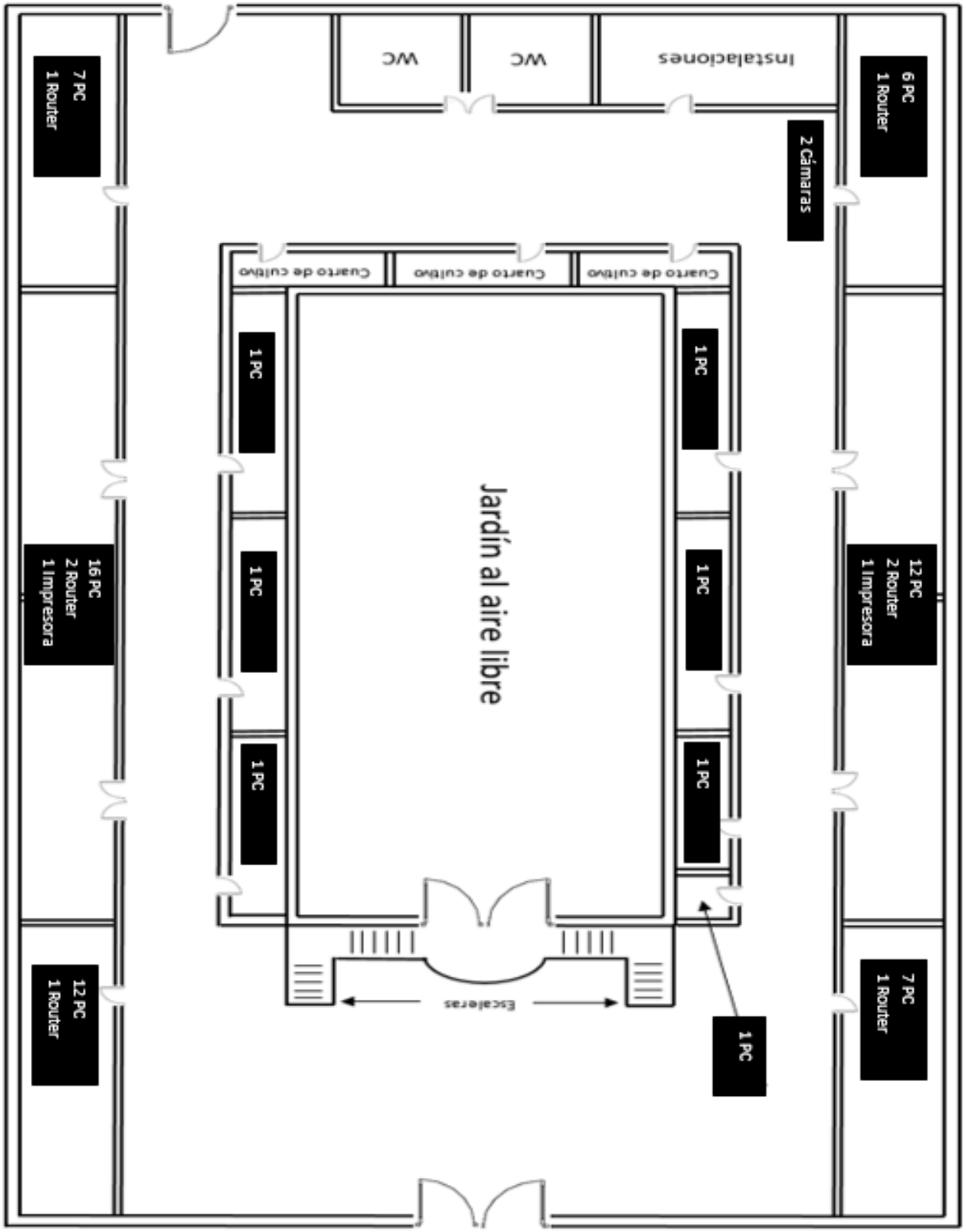
Edificio “C”, Planta baja, 79 host:

- Laboratorio 19: 6 PC, 1 router
- Laboratorio 20: 12 PC, 2 router, 1 impresora en red
- Laboratorio 21: 7 PC, 1 router
- Laboratorio 22: 7 PC, 1 router
- Laboratorio 23: 16 PC, 2 router, 1 impresora en red
- Laboratorio 24: 12 PC, 1 router
- Oficina 17: 1 PC
- Oficina 18: 1 PC
- Oficina 19: 1 PC
- Oficina 20: 1 PC
- Oficina 21: 1 PC
- Sala de juntas 9: 1 PC
- Cuarto de control 2: 1 PC
- Pasillos: 2 cámaras

-Diagrama físico del Edificio “C”, Planta Baja



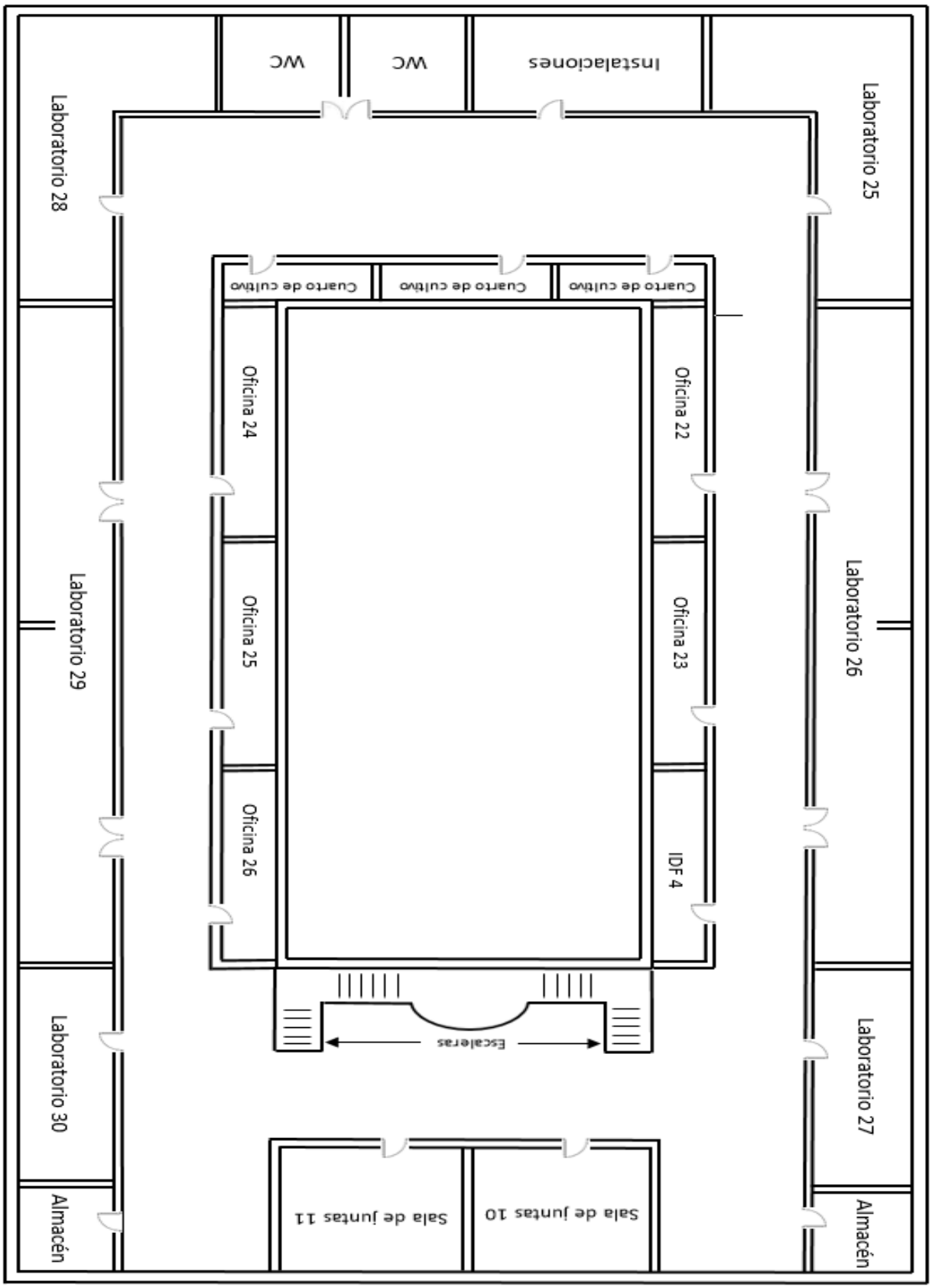
-Ubicación de los equipos en el diagrama físico del Edificio “C”, Planta Baja



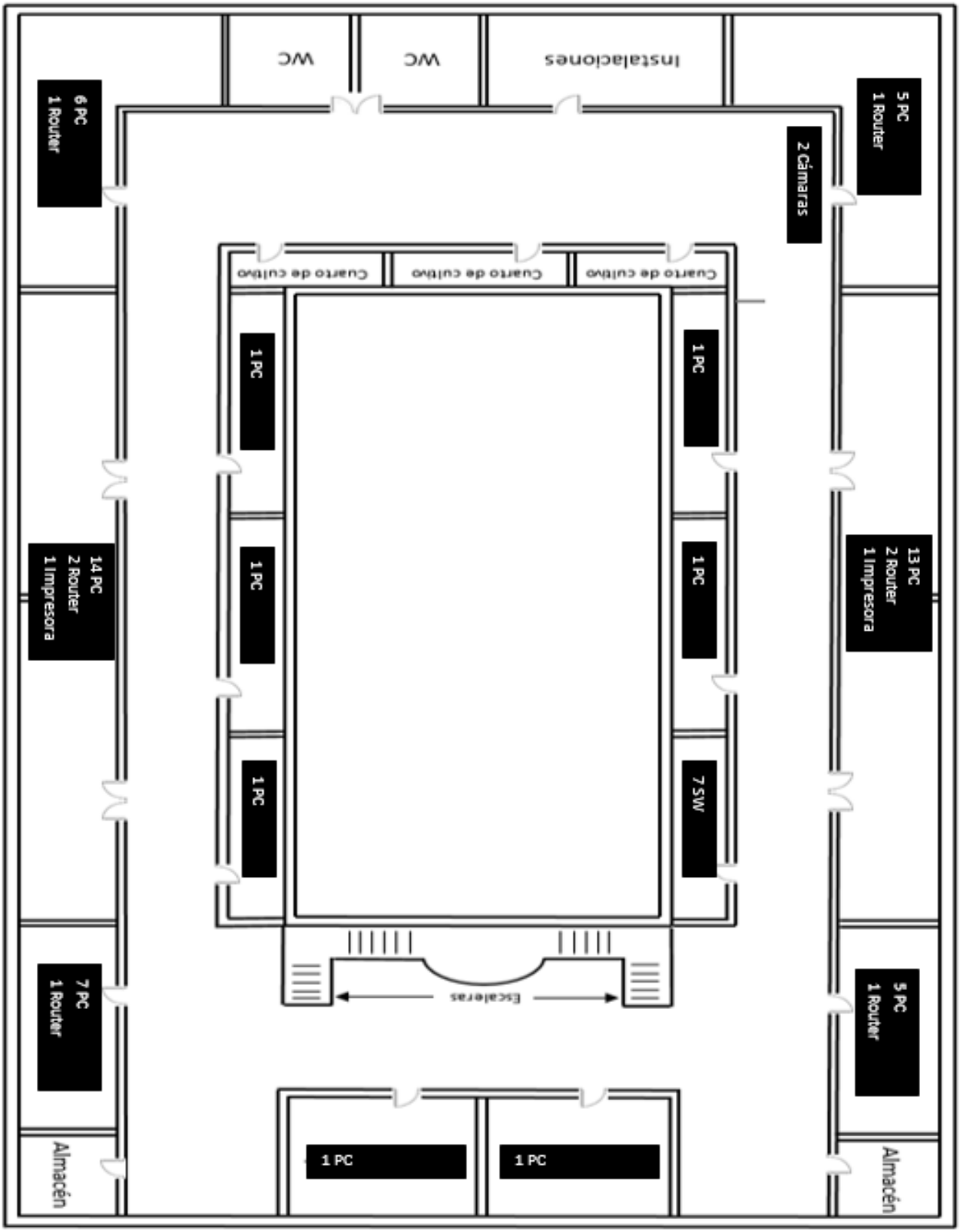
Edificio “C”, Primer piso, 76 host:

- Laboratorio 25: 5 PC, 1 router
- Laboratorio 26: 13 PC, 2 router, 1 impresora en red
- Laboratorio 27: 5 PC, 1 router
- Laboratorio 28: 6 PC, 1 router
- Laboratorio 29: 14 PC, 2 router, 1 impresora en red
- Laboratorio 30: 7 PC, 1 router
- Oficina 22: 1 PC
- Oficina 23: 1 PC
- Oficina 24: 1 PC
- Oficina 25: 1 PC
- Oficina 26: 1 PC
- Sala de juntas 10: 1 PC
- Sala de juntas 11: 1 PC
- Pasillos: 2 cámaras
- IDF 4: 7SW
  - SW de distribución: SW “P”
  - SW de acceso: SW “Q”, SW “R”, SW “S”, SW “T”, SW “U” y SW “V”

-Diagrama físico del Edificio “C”, Primer Piso



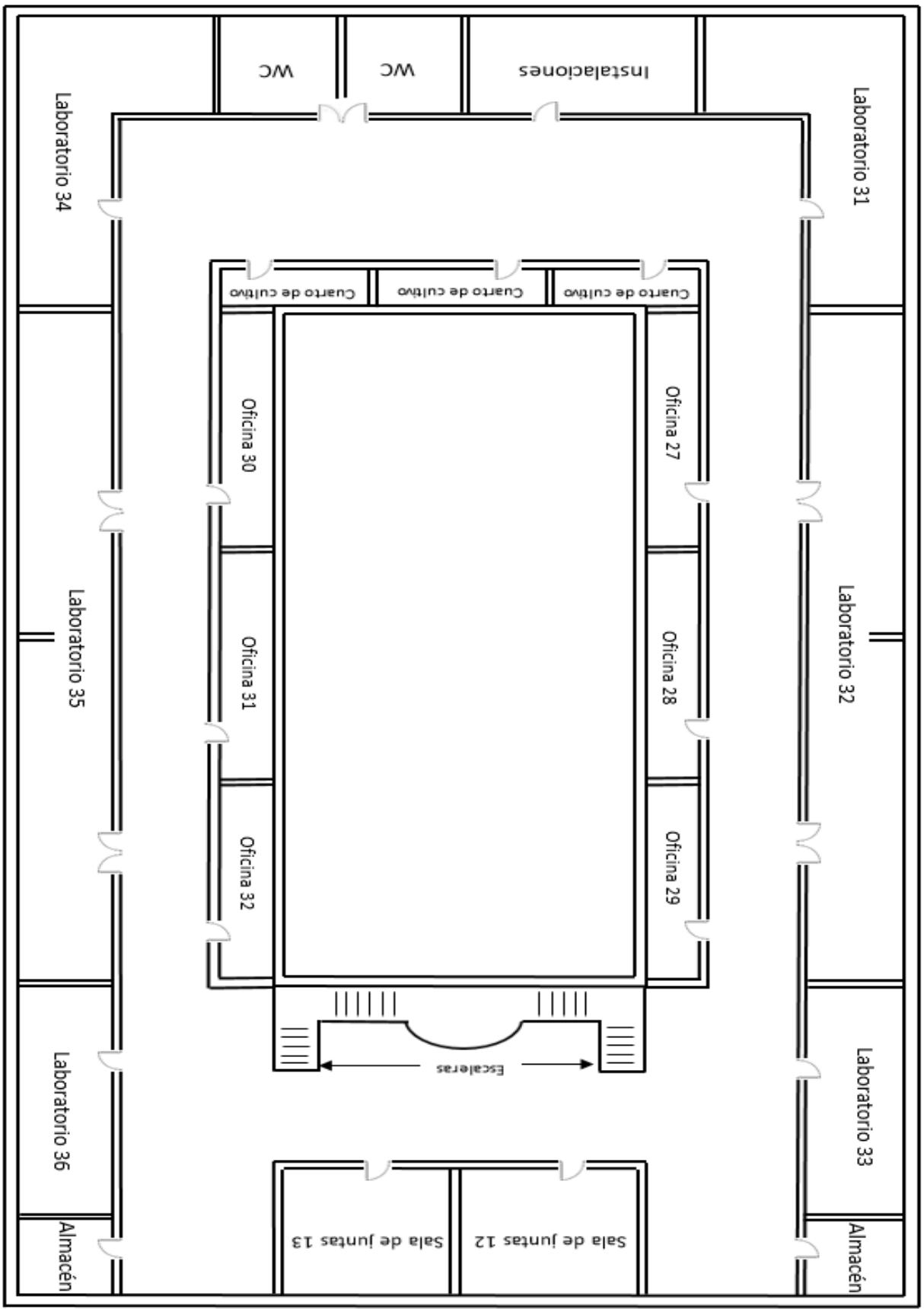
-Ubicación de los equipos en el diagrama físico del Edificio “C”, Primer Piso



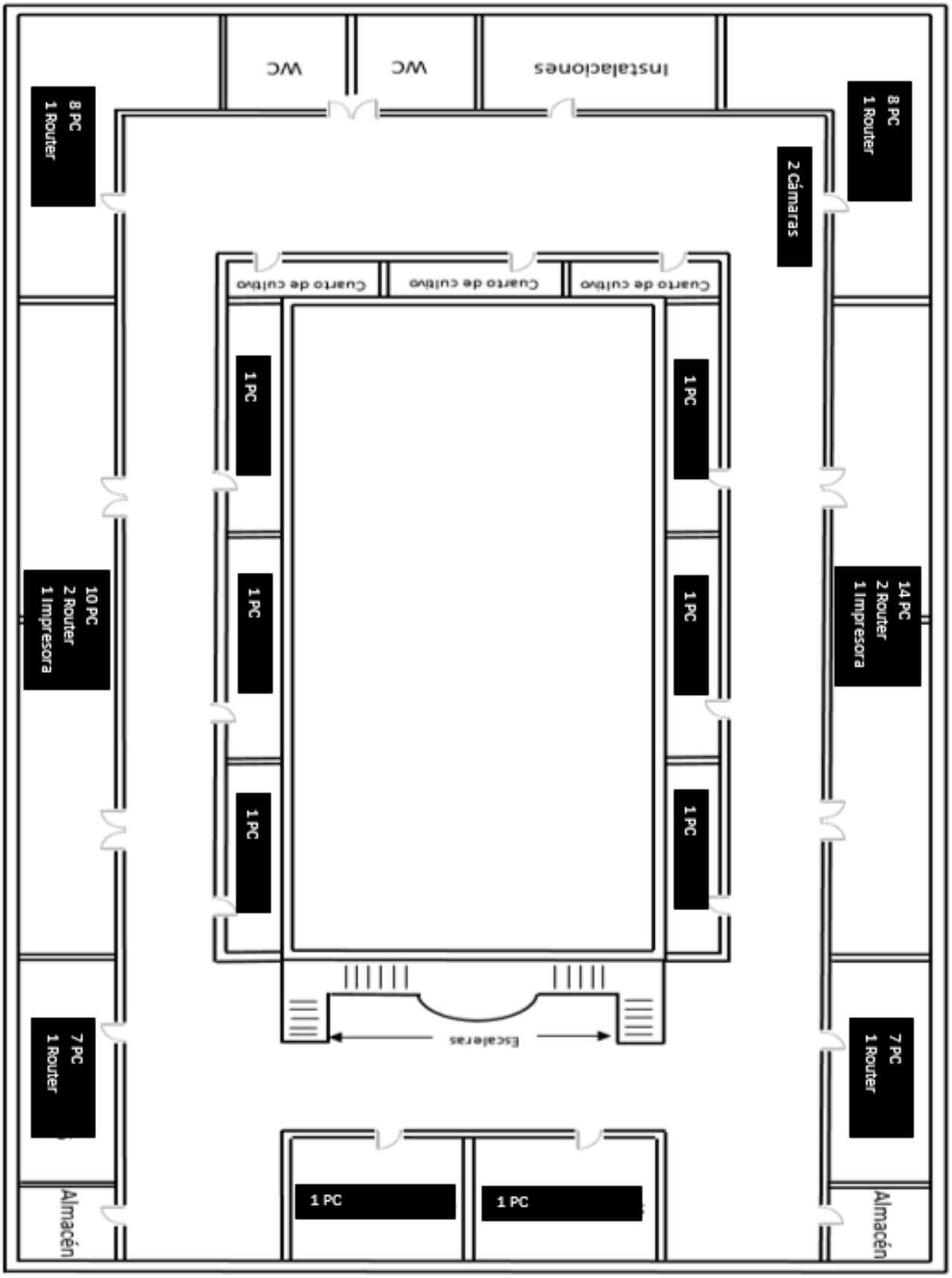
Edificio “C”, Segundo piso, 74 host:

- Laboratorio 31: 8 PC, 1 router
- Laboratorio 32: 14 PC, 2 router, 1 impresora en red
- Laboratorio 33: 7 PC, 1 router
- Laboratorio 34: 8 PC, 1 router
- Laboratorio 35: 10 PC, 2 router, 1 impresora en red
- Laboratorio 36: 7 PC, 1 router
- Oficina 27: 1 PC
- Oficina 28: 1 PC
- Oficina 29: 1 PC
- Oficina 30: 1 PC
- Oficina 31: 1 PC
- Oficina 32: 1 PC
- Sala de juntas 12: 1 PC
- Sala de juntas 13: 1 PC
- Pasillos: 2 cámaras

-Diagrama físico del Edificio “C”, Segundo Piso



-Ubicación de los equipos en el diagrama físico del Edificio “C”, Segundo Piso

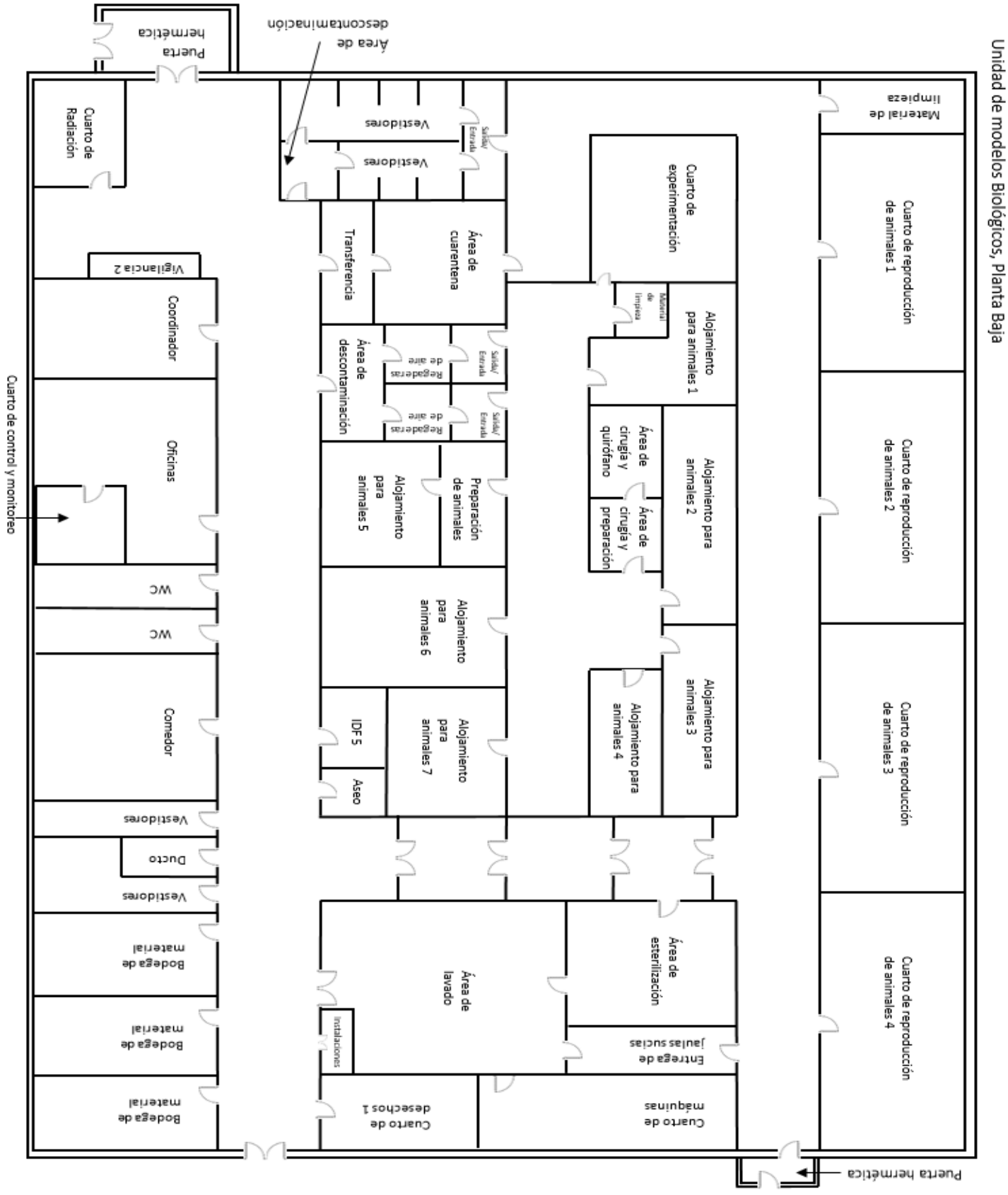


-Topología física de la Unidad de Modelos Biológicos:

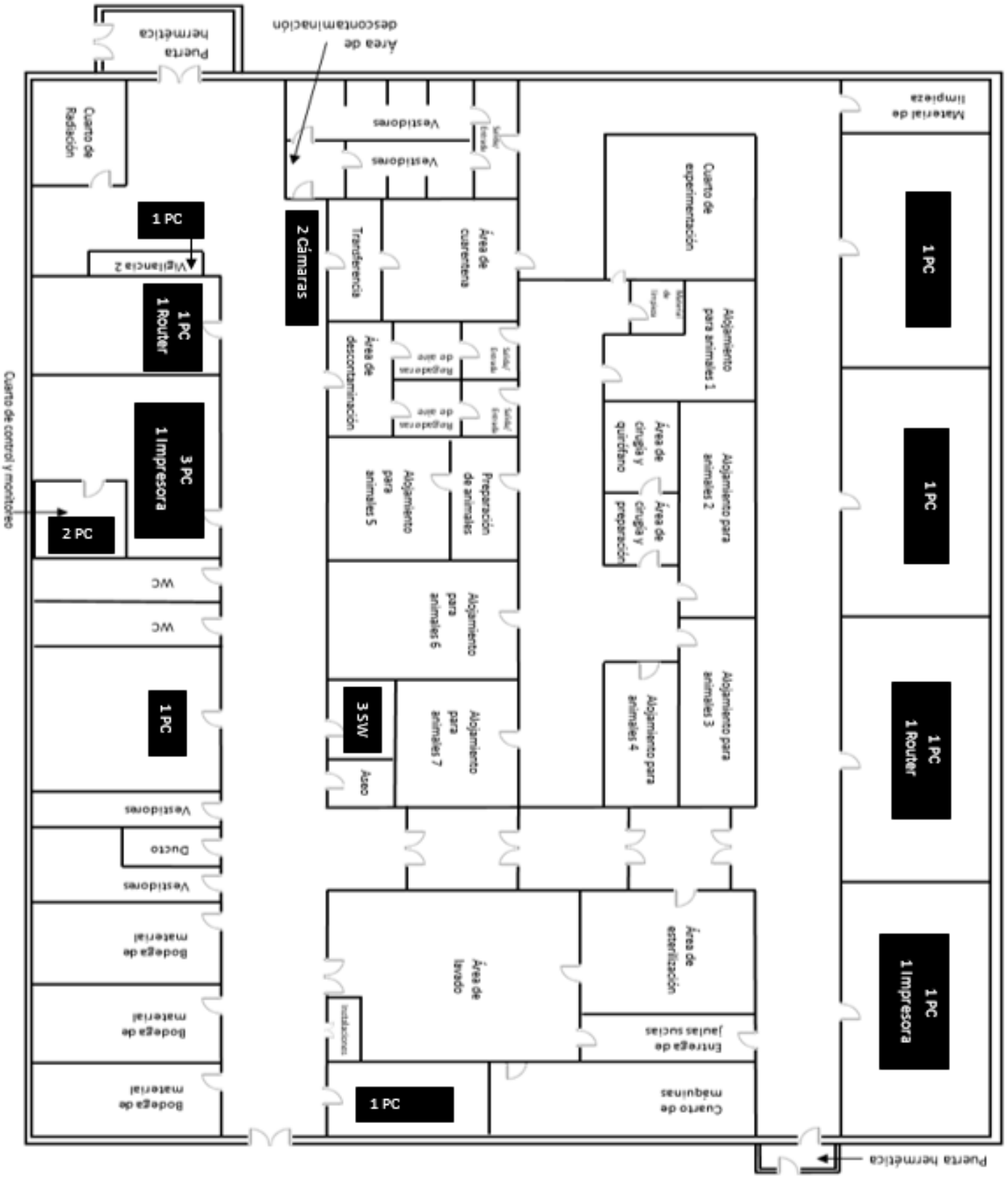
Unidad de Modelos Biológicos, Planta baja, 22 host:

- Cuarto de reproducción de animales 1: 1 PC
- Cuarto de reproducción de animales 2: 1 PC
- Cuarto de reproducción de animales 3: 1 PC, 1 router
- Cuarto de reproducción de animales 4: 1 PC, 1 impresora en red
- Vigilancia 2: 1 PC
- Coordinación: 1 PC, 1 router
- Oficinas: 3 PC, 1 impresora en red
- Cuarto de control y monitoreo: 2 PC
- Comedor: 1 PC
- Cuarto de desechos 1: 1PC
- Pasillos: 2 cámaras
- IDF 5: 3 SW
  - SW de distribución: SW “W”
  - SW de acceso: SW “X” y SW “Y”

-Diagrama físico de la Unidad de Modelos Biológicos, Planta Baja



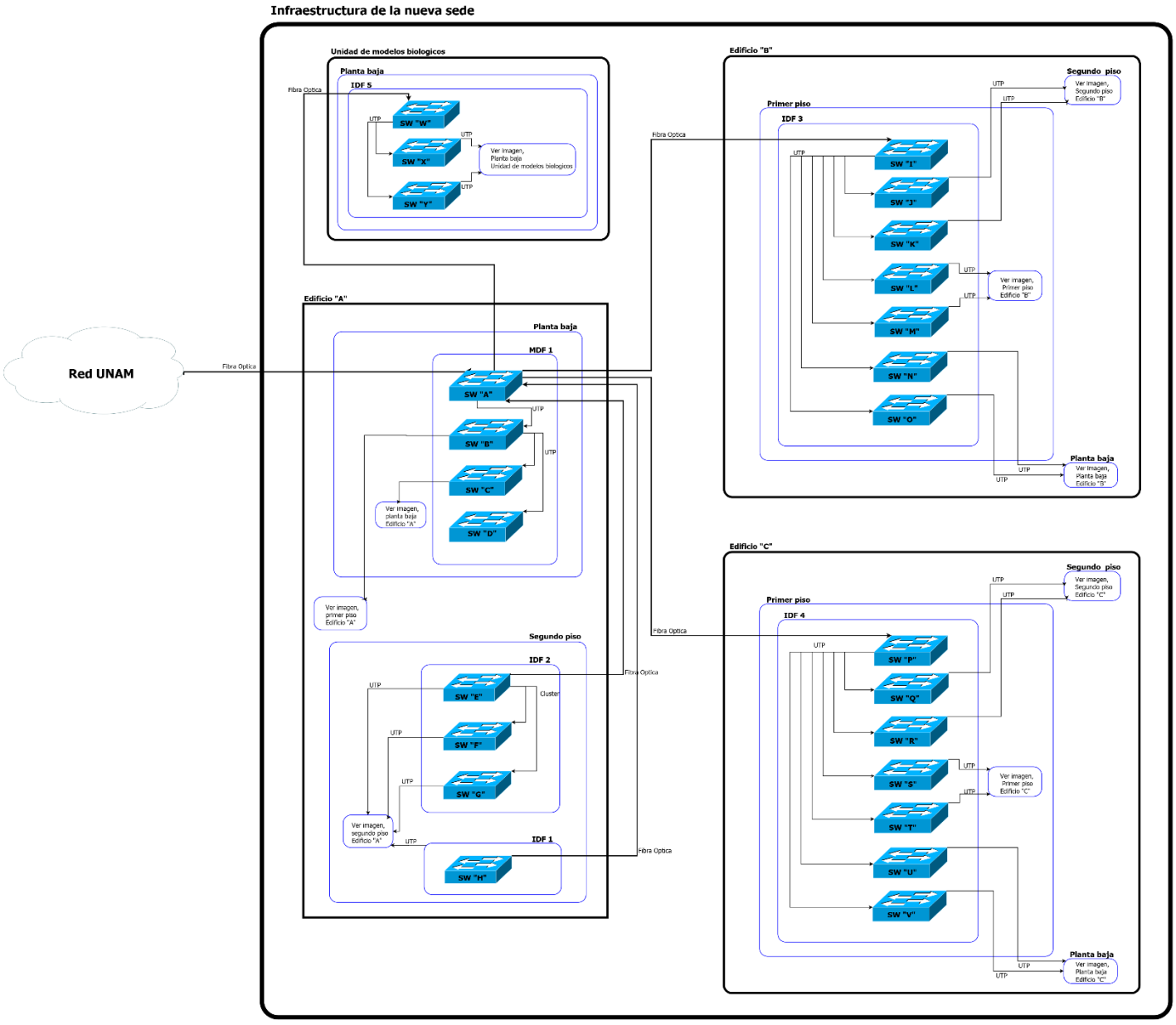
-Ubicación de los equipos en el diagrama físico de la Unidad de Modelos Biológicos, Planta Baja



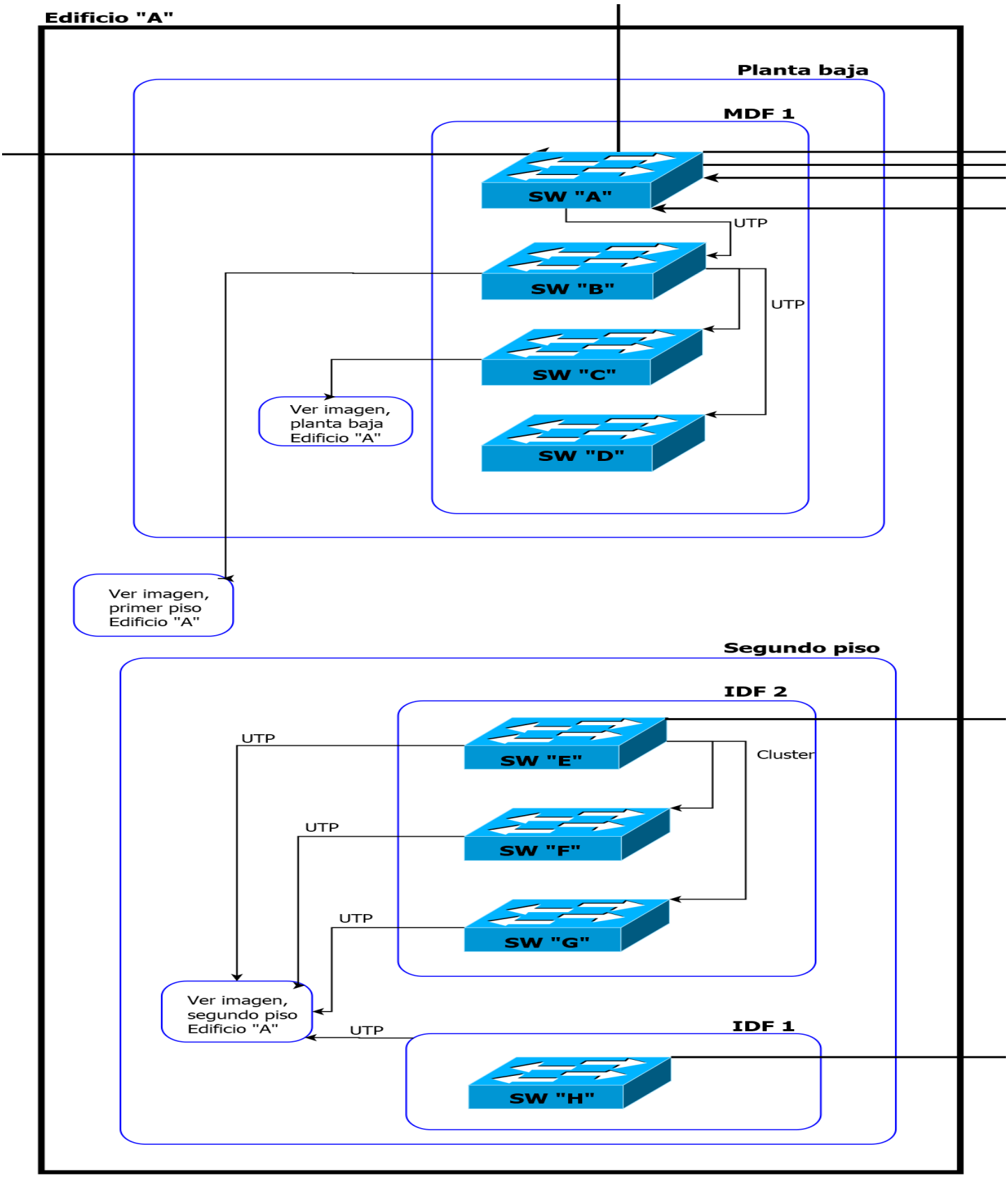
3.4 Topología lógica actual

Se analizó las funciones, servicios y usuarios a los que se les brindaba acceso a la red en cada piso de los edificios del Instituto para comprender como está configurado cada entorno dentro de la infraestructura de red, y poder llevar a cabo la segmentación por medio de tecnologías VLAN a futuro; hay que comprender bien la topología lógica actual de la institución, la cual tiene diferentes grupos de usuarios en cada uno de los pisos de los edificios y todos conviven en una VLAN en común (la VLAN1 por default que tienen los SW de fábrica), la topología lógica actualmente es la siguiente:

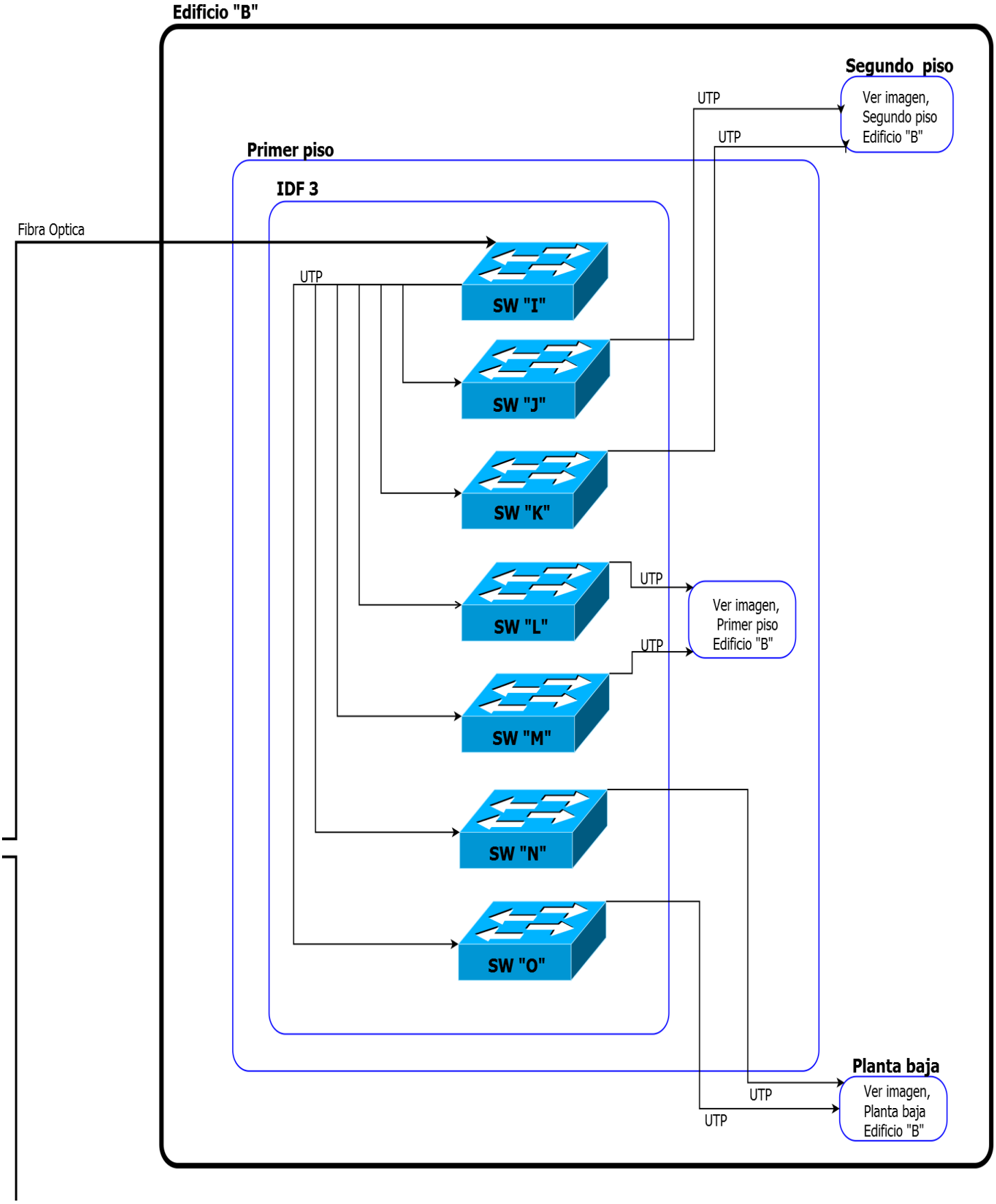
-Diagrama lógico general del Instituto de Investigaciones Biomédicas de la nueva sede



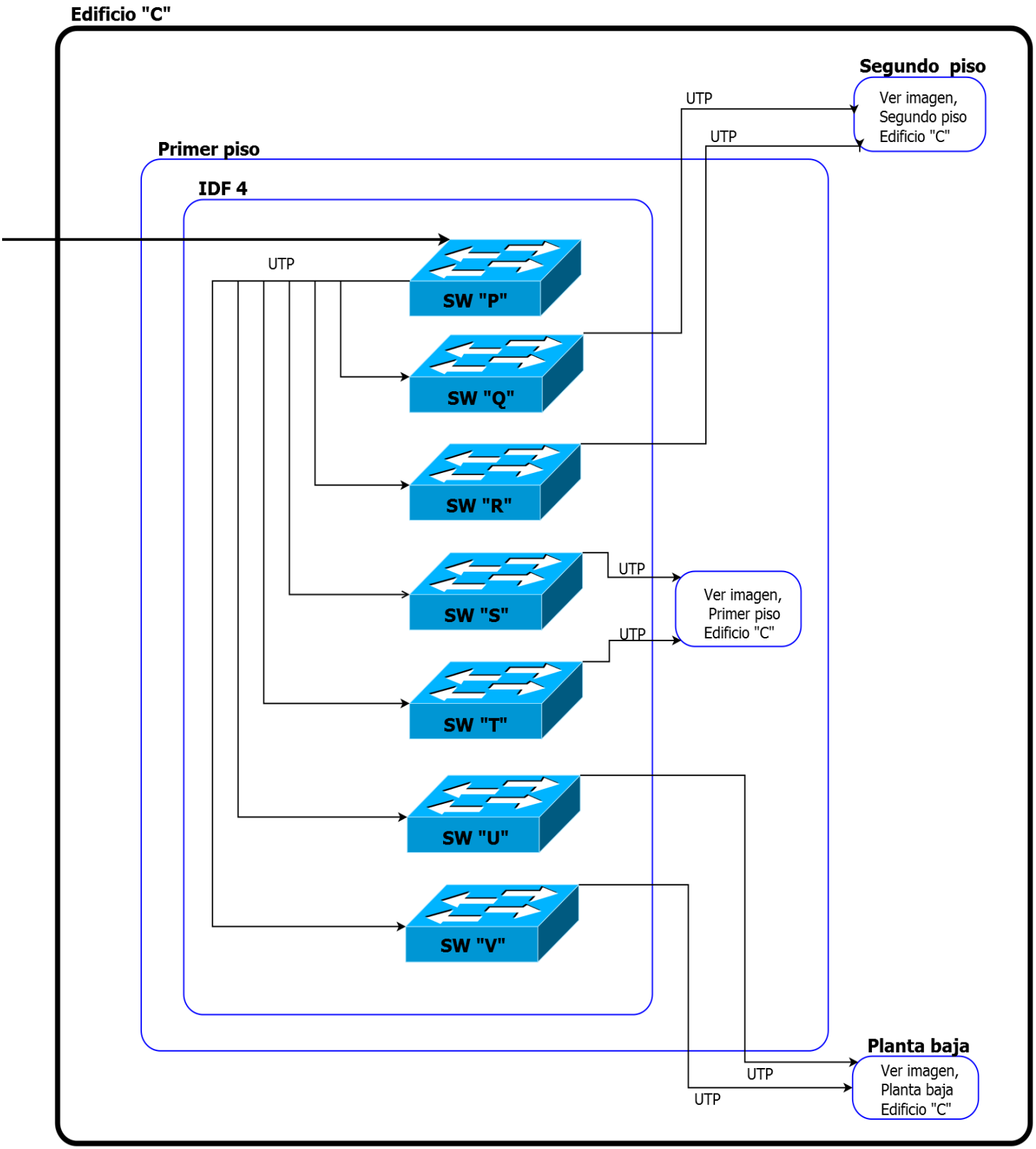
Topología lógica Edificio “A”:



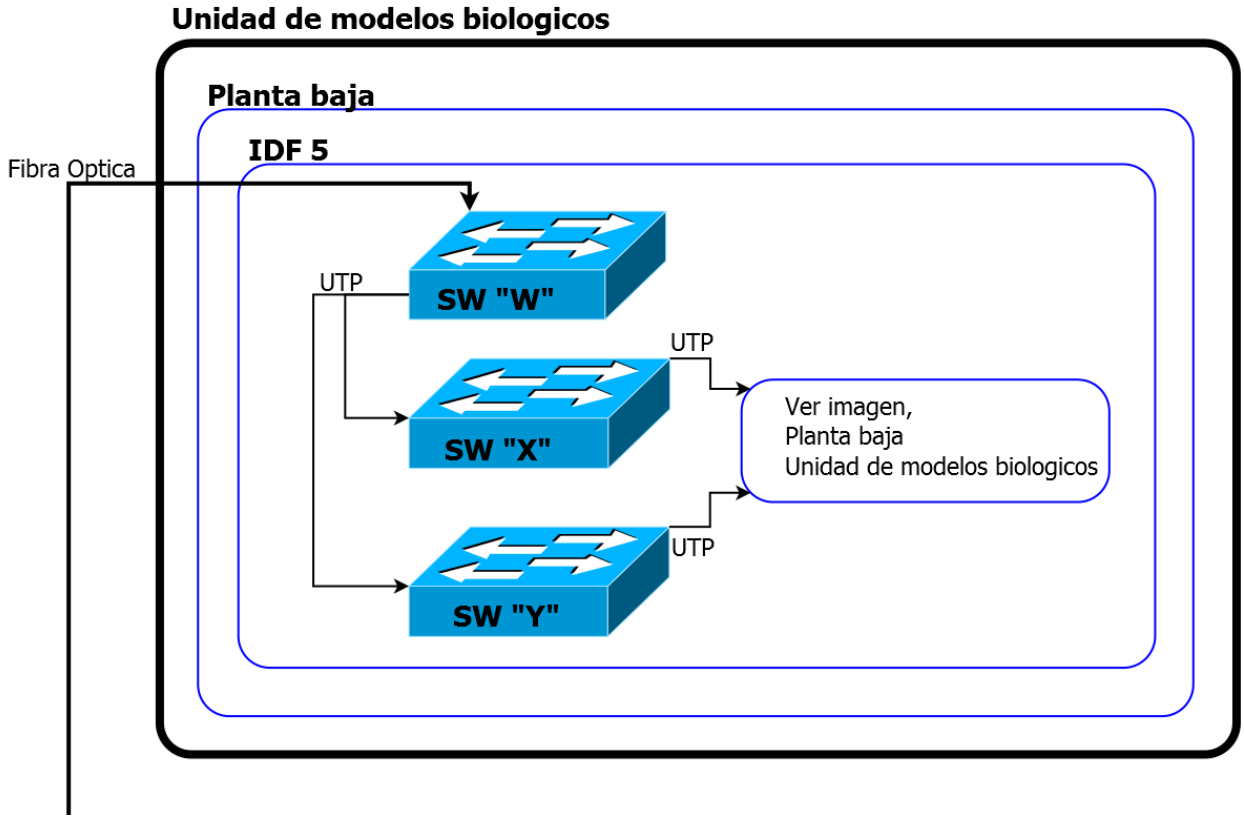
Topología lógica Edificio “B”:



Topología lógica Edificio “C”:



Topología lógica de la Unidad De Modelos Biológicos:



3.5 Distribución general de IP en los segmentos de red

Instituto de Investigaciones Biomédicas de la nueva sede				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	132.248.116.0/24	Edificio "A": -Servidores -WAN del FW/NAT/GW	IP pública	6
VLAN 1	192.168.2.0/24	Edificio "C": -Comunidad académica -Ruteadores -Impresoras en red	IP privada	178
VLAN 1	192.168.3.0/24	Edificio "A": -Servidores internos -Comunidad académica -Ruteadores -Impresoras en red	IP privada	97
VLAN 1	192.168.4.0/24	Edificio "B": -Comunidad académica -Ruteadores -Impresoras en red Unidad de Modelos Biológicos: -Comunidad académica -Ruteadores -Impresoras en red	IP privada	175
VLAN 1	192.168.199.0/24		IP privada	17
VLAN 1	192.168.6.0/24	Edificio "B" y "C": -Investigadores	IP privada	30
VLAN 1	192.168.7.0/24	Edificio "B" y "C": -Investigadores	IP privada	15
VLAN 1	192.168.8.0/24	Edificio "B" y "C": -Investigadores	IP privada	26
VLAN 1	192.168.169.0/24	Edificio "A", "B", "C" y Unidad de Modelos Biológicos: -Secretaria técnica y CCTV	IP privada	27
VLAN 1	192.168.200.0/24	Edificio "A", "B", "C" y Unidad de Modelos Biológicos: -Administración de SW	IP privada	25

Haciendo un total de 596 IP privadas e IP públicas registradas.

3.6 Lista general de los SW instalados en los MDF e IDF y sus características

Edificio	Antigüedad	Marca	Modelo	FIRMWARE	IP	No. De puertos ocupados	No. de puertos libres	Tipo	Identificador	Ubicación
"A", Planta Baja	4 años	Enterasys	G3-Series	06.61.07.0010	192.168.200.1	7 sfp FO 1000, 1 sfp utp 1000	16 sfp	Core	SW "A"	MDF1
	9 años	3com	SuperStack 4 5500G	V3.02.00.s56	192.168.200.2	24 ethernet 1000, 1 sfp ethernet 1000	3 sfp	Distribucion y Acceso	SW "B"	MDF1
	9 años	3com	SuperStack 4 5500 - EI 52 port SuperStack 4 5500 - EI 52 port	V3.01.04.s56	192.168.200.5	43 ethernet 100, 1 sfp utp 1000	5 ethernet 100, 3 sfp	Acceso	SW "C"	MDF1
	9 años	3com		V3.01.04.s56	192.168.200.4	44 ethernet 100, 1 sfp utp 1000	4 ethernet 100, 3 sfp	Acceso	SW "D"	MDF1

Edificio	Antigüedad	Marca	Modelo	FIRMWARE	IP	No. De puertos ocupados	No. de puertos libres	Tipo	Identificador	Ubicación
"A", Segundo Piso	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.13	36 ethernet 1000	12 ethernet 1000, 4 sfp	Acceso	SW "E"	IDF2, Cluster
	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.12	37 ethernet 1000	11 ethernet 1000, 4 sfp	Acceso	SW "F"	IDF2, Cluster
	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.11	35 ethernet 1000, 1 sfp FO 1000	13 ethernet 1000, 3 spf	Distribucion y Acceso	SW "G"	IDF2, Cluster

Edificio	Antigüedad	Marca	Modelo	FIRMWARE	IP	No. De puertos ocupados	No. de puertos libres	Tipo	Identificador	Ubicación
"A", Cómputo	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.19	17 ethernet 1000, 1 sfp 1000	31 ethernet 1000, 3 sfp	Acceso	SW "H"	IDF1

Edificio	Antigüedad	Marca	Modelo	FIRMWARE	IP	No. De puertos ocupados	No. de puertos libres	Tipo	Identificador	Ubicación
"B", Primer Piso	4 años	Enterasys	B5G124-48	06.42.06.0008	192.168.200.31	10 ethernet 1000, 1 sfp 1000 FO	38 Ethernet 1000, 3 sfp libres	Distribución	SW "I"	IDF3
	9 años	3com	SuperStack 4 5500 - EI 52 port	V3.03.02s168ep22	192.168.200.32	45 ethernet 100, 1 sfp utp 1000	3 ethernet 10/100, 3 sfp 1000	Acceso	SW "J"	IDF3
	9 años	3com	SuperStack 4 5500 - EI 52 port	V3.01.12.s56	192.168.200.33	21 ethernet 100, 1 sfp utp 1000	27 ethernet 10/100, 3 sfp	Acceso	SW "K"	IDF3
	9 años	3com	SuperStack 4 5500 - EI 52 port	V3.01.12.s56	192.168.200.34	48 ethernet 10/100	4 sfp	Acceso	SW "L"	IDF3
	9 años	3com	SuperStack 4 5500 - EI 52 port	V3.01.12.s56	192.168.200.35	25 ethernet 10/100	23 ethernet 10/100, 4 sfp	Acceso	SW "M"	IDF3
	9 años	3com	SuperStack 4 5500 - EI 52 port	V3.01.12.s56	192.168.200.36	44 ethernet 10/100, 1 sfp utp 1000	4 ethernet 10/100, 3 sfp	Acceso	SW "N"	IDF3
	9 años	3com	SuperStack 4 5500 - EI 52 port	V3.01.12.s56	192.168.200.37	39 ethernet 10/100	9 ethernet 10/100, 4 sfp	Acceso	SW "O"	IDF3

Edificio	Antigüedad	Marca	Modelo	FIRMWARE	IP	No. De puertos ocupados	No. de puertos libres	Tipo	Identificador	Ubicación
"C", Primer Piso	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.41	8 ethernet 1000, 1 sfp FO 1000	40 Ethernet 1000, 3 sfp	Distribución	SW "P"	IDF4
	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.42	48 ethernet 1000	4 sfp	Acceso	SW "Q"	IDF4
	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.43	11 ethernet 1000	37 ethernet 1000, 4 sfp	Acceso	SW "R"	IDF4
	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.44	41 ethernet 1000	7 ethernet 1000, 4 sfp	Acceso	SW "S"	IDF4
	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.45	26 ethernet 1000	22 ethernet, 4 sfp	Acceso	SW "T"	IDF4
	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.46	30 ethernet 1000	18 ethernet 1000, 4 sfp	Acceso	SW "U"	IDF4
	4 años	Enterasys	B5G124-48	06.81.01.0027	192.168.200.47	43 ethernet 1000	5 ethernet 1000, 4 sfp	Acceso	SW "V"	IDF4

Edificio	Antigüedad	Marca	Modelo	FIRMWARE	IP	No. De puertos ocupados	No. de puertos libres	Tipo	Identificador	Ubicación
Unidad de Modelos Biologicos, Planta Baja	6 años	HP	HP A5120 JE072Q	139	192.168.200.51	48 ethernet 10/100, 1 sfp FO 1000	3 sfp	Distribución y Acceso	SW "Y"	IDF5
	6 años	HP	HP A5120 JE072Q	139	192.168.200.52	16 ethernet 10/100	4 sfp, 32 ethernet 10/100	Acceso	SW "X"	IDF5
	6 años	HP	HP A5120 JG236A	607	192.168.200.53	14 ethernet 10/100	4 sfp, 10 ethernet 10/100	Acceso	SW "Y"	IDF5

Haciendo un total de 25 SW.

3.7 Distribución de IP y asignación de SW en cada edificio

Las IP registradas se encuentran distribuidas en cada segmento de red en cada edificio de la siguiente manera:
En el Edificio “A” del Instituto se tiene contemplado un total de 124 IP registradas, mismos que se encuentran distribuidos de la siguiente manera:

Edificio “A”, Planta baja, 40 IP registradas:

Edificio "A", Planta Baja				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	192.168.3.0/24	-Comunidad académica -Ruteadores -Impresoras en red	IP privada	29
VLAN 1	192.168.169.0/24	-Secretaria técnica y CCTV	IP privada	7
VLAN 1	192.168.200.0/24	-Administración de SW	IP privada	4

-Conectados al SW “C” y “D”:

Tipo	Identificador	Ubicación
Acceso	SW "C"	MDF1
Acceso	SW "D"	MDF1

-Edificio “A”, Primer Piso, 12 IP registradas:

Edificio "A", Primer Piso				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	192.168.3.0/24	-Servidores internos -Comunidad académica -Ruteadores -Impresoras en red	IP privada	8
VLAN 1	192.168.169.0/24	-CCTV	IP privada	4

-Conectados al SW “B”:

Tipo	Identificador	Ubicación
Distribución y Acceso	SW "B"	MDF1

-Edificio “A”, Segundo Piso, 72 IP registradas:

Edificio "A", Segundo Piso				
VLAN	**Segmento de red**	**Área**	**Tipo IP**	**IP registradas**
VLAN 1	132.248.116.0/24	-Servidores -WAN del FW/NAT/GW	IP pública	6
VLAN 1	192.168.3.0/24	-Servidores internos -Comunidad académica -Ruteadores -Impresoras en red	IP privada	60
VLAN 1	192.168.169.0/24	-CCTV	IP privada	2
VLAN 1	192.168.200.0/24	-Administración de SW	IP privada	4

-Conectados al SW “E”, “F”, “G” y “H”:

Tipo	Identificador	Ubicación
Acceso	SW "E"	IDF2, Cluster
Acceso	SW "F"	IDF2, Cluster
Distribución y Acceso	SW "G"	IDF2, Cluster
Acceso	SW "H"	IDF1

En el Edificio “B” del Instituto se tiene contemplado un total de 221 IP registradas, mismos que se encuentran distribuidos de la siguiente manera:

-Edificio “B”, Planta Baja, 75 IP registradas:

Edificio "B", Planta Baja				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	192.168.4.0/24	-Comunidad académica -Ruteadores	IP privada	50

		-Impresoras en red		
VLAN 1	192.168.6.0/24	-Investigadores	IP privada	2
VLAN 1	192.168.7.0/24	-Investigadores	IP privada	5
VLAN 1	192.168.8.0/24	-Investigadores	IP privada	4
VLAN 1	192.168.169.0/24	- CCTV	IP privada	2

-Conectados al SW “J” y “K”:

Tipo	Identificador	Ubicación
Acceso	SW "J"	IDF3
Acceso	SW "K"	IDF3

-Edificio “B”, Primer Piso, 75 IP registradas:

Edificio "B", Primer Piso				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	192.168.4.0/24	-Comunidad académica -Ruteadores -Impresoras en red	IP privada	62
VLAN 1	192.168.6.0/24	-Investigadores	IP privada	4
VLAN 1	192.168.7.0/24	-Investigadores	IP privada	4
VLAN 1	192.168.8.0/24	-Investigadores	IP privada	3
VLAN 1	192.168.169.0/24	- CCTV	IP privada	2
VLAN 1	192.168.200.0/24	-Administración de SW	IP privada	7

-Conectados al SW “L” y “M”:

Tipo	Identificador	Ubicación
Acceso	SW "L"	IDF3
Acceso	SW "M"	IDF3

-Edificio “B”, Segundo Piso, 71 IP registradas:

Edificio "B", Segundo Piso				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	192.168.4.0/24	-Comunidad académica -Ruteadores -Impresoras en red	IP privada	63
VLAN 1	192.168.6.0/24	-Investigadores	IP privada	4
VLAN 1	192.168.7.0/24	-Investigadores	IP privada	5
VLAN 1	192.168.8.0/24	-Investigadores	IP privada	2
VLAN 1	192.168.169.0/24	- CCTV	IP privada	2

-Conectados al SW “N” y “O”:

Tipo	Identificador	Ubicación
Acceso	SW "N"	IDF3
Acceso	SW "O"	IDF3

En el Edificio “C” del Instituto se tiene contemplado un total de 229 IP registradas, mismos que se encuentran distribuidos de la siguiente manera:

-Edificio “C”, Planta Baja, 79 IP registradas:

Edificio "C", Planta Baja				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	192.168.4.0/24	-Comunidad académica -Ruteadores -Impresoras en red	IP privada	64
VLAN 1	192.168.6.0/24	-Investigadores	IP privada	4
VLAN 1	192.168.7.0/24	-Investigadores	IP privada	5
VLAN 1	192.168.8.0/24	-Investigadores	IP privada	4
VLAN 1	192.168.169.0/24	- CCTV	IP privada	2

-Conectados al SW “Q” y “R”:

Tipo	Identificador	Ubicación
Acceso	SW "Q"	IDF4
Acceso	SW "R"	IDF4

-Edificio “C”, Primer Piso, 76 IP registradas:

Edificio "C", Primer Piso				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	192.168.4.0/24	-Comunidad académica -Ruteadores -Impresoras en red	IP privada	56
VLAN 1	192.168.6.0/24	-Investigadores	IP privada	4
VLAN 1	192.168.7.0/24	-Investigadores	IP privada	4
VLAN 1	192.168.8.0/24	-Investigadores	IP privada	3
VLAN 1	192.168.169.0/24	- CCTV	IP privada	2
VLAN 1	192.168.200.0/24	-Administración de SW	IP privada	7

-Conectados al SW “S” y “T”:

Tipo	Identificador	Ubicación
Acceso	SW "S"	IDF4
Acceso	SW "T"	IDF4

-Edificio “C”, Segundo Piso, 74 IP registradas:

Edificio "B", Segundo Piso				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	192.168.4.0/24	-Comunidad académica -Ruteadores -Impresoras en red	IP privada	61
VLAN 1	192.168.6.0/24	-Investigadores	IP privada	4
VLAN 1	192.168.7.0/24	-Investigadores	IP privada	5
VLAN 1	192.168.8.0/24	-Investigadores	IP privada	2
VLAN 1	192.168.169.0/24	- CCTV	IP privada	2

-Conectados al SW “U” y “V”:

Tipo	Identificador	Ubicación
Acceso	SW "U"	IDF4
Acceso	SW "V"	IDF4

En la Unidad De Modelos Biológicos del Instituto se tiene contemplado un total de 22 IP registradas, mismos que se encuentran distribuidos de la siguiente manera:

- Unidad De Modelos Biológicos, Planta Baja, 22 IP registradas:

Unidad de Modelos Biológicos, Planta Baja				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	192.168.199.0/24	-Comunidad académica -Ruteadores -Impresoras en red	IP privada	17

VLAN 1	192.168.169.0/24	- CCTV	IP privada	2
VLAN 1	192.168.200.0/24	-Administración de SW	IP privada	3

-Conectados al SW “Q” y “R”:

Tipo	Identificador	Ubicación
Acceso	SW "X"	IDF5
Acceso	SW "Y"	IDF5

3.8 Grupos de usuarios basados en funciones

Todos los grupos de usuarios dentro de la comunidad académica actualmente utilizan direcciones IP de clase C con máscara de red de clase C asignados por grupos:

Instituto de Investigaciones Biomédicas de la nueva sede				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	132.248.116.0/24	Edificio "A": -Servidores -WAN del FW/NAT/GW	IP pública	6
VLAN 1	192.168.2.0/24	Edificio “C”: -Comunidad académica -Ruteadores -Impresoras en red	IP privada	178
VLAN 1	192.168.3.0/24	Edificio “A” : -Servidores internos -Comunidad académica -Ruteadores -Impresoras en red	IP privada	97
VLAN 1	192.168.4.0/24	Edificio “B”: -Comunidad académica -Ruteadores -Impresoras en red	IP privada	175
VLAN 1	192.168.199.0/24	Unidad de Modelos Biológicos: -Comunidad académica -Ruteadores -Impresoras en red	IP privada	17
VLAN 1	192.168.6.0/24	Edificio "B" y "C": -Investigadores	IP privada	30
VLAN 1	192.168.7.0/24	Edificio "B" y "C": -Investigadores	IP privada	15

VLAN 1	192.168.8.0/24	Edificio "B" y "C": -Investigadores	IP privada	26
VLAN 1	192.168.169.0/24	Edificio "A", "B", "C" y Unidad de Modelos Biológicos: -Secretaria técnica y CCTV	IP privada	27
VLAN 1	192.168.200.0/24	Edificio "A", "B", "C" y Unidad de Modelos Biológicos: -Administración de SW	IP privada	25

Se utilizaron direcciones IP de clase C ya que las 254direcciones IP utilizables que proporcionaba por red cubrían la demanda de host, límite que está a punto de llegar a su máxima capacidad, por lo que se planea migrar a direcciones IP clase B; sabiendo que las direcciones IP de clase B permiten 65534 host y 16384 redes que a mediano o largo plazo no se espera que se utilicen en su totalidad.
Para el direccionamiento IP de los servidores se utilizó el segmento de red 192.168.3.0/24 que permite asignar hasta 254 direcciones IP por segmento más que suficientes para tener una segmentación de red ordenada.
Se asignó el segmento de red 192.168.200.0/24 para la administración de los dispositivos de telecomunicación que son:
25 SW (Core, distribución y de acceso)
La administración del FW/NAT/GW es a través de una IP pública.

3.9 Equipos instalados en el MDF e IDF

Actualmente la infraestructura de red de la nueva sede está basada en su mayoría en dispositivos de telecomunicaciones *Enterasys* seguido de *3com-HP* en un ambiente mixto, dentro de la institución la sección de computo tiene instalado un total de 25 SW (distribuidos entre: Core, distribución y de acceso) y 1 FW/NAT/GW (la administración del 1 FW/NAT/GW es a través de una IP pública), la institución cuenta con 1 MDF y 5 IDF distribuidos de la siguiente manera:
-Los equipos instalados en el MDF1 son los siguientes:

Antigüedad	Marca	Modelo	IP	Tipo	Identificador
4 años	Enterasys	G3-Series	192.168.200.1	Core	SW "A"
9 años	3com	SuperStack 4 5500G	192.168.200.2	Distribución y Acceso	SW "B"
9 años	3com	SuperStack 4 5500 - EI 52 port	192.168.200.5	Acceso	SW "C"
9 años	3com	SuperStack 4 5500 - EI 52 port	192.168.200.4	Acceso	SW "D"

-Los equipos instalados en el IDF1 son los siguientes:

Antigüedad	Marca	Modelo	IP	Tipo	Identificador
4 años	Enterasys	B5G124-48	192.168.200.19	Acceso	SW "H"

-Los equipos instalados en el IDF2 son los siguientes:

Antigüedad	Marca	Modelo	IP	Tipo	Identificador
4 años	Enterasys	B5G124-48	192.168.200.13	Acceso	SW "E"
4 años	Enterasys	B5G124-48	192.168.200.12	Acceso	SW "F"
4 años	Enterasys	B5G124-48	192.168.200.11	Distribución y Acceso	SW "G"

-Los equipos instalados en el IDF3 son los siguientes:

Antigüedad	Marca	Modelo	IP	Tipo	Identificador
4 años	Enterasys	B5G124-48	192.168.200.31	Distribución	SW "I"
9 años	3com	SuperStack 4 5500 - EI 52 port	192.168.200.32	Acceso	SW "J"
9 años	3com	SuperStack 4 5500 - EI 52 port	192.168.200.33	Acceso	SW "K"
9 años	3com	SuperStack 4 5500 - EI 52 port	192.168.200.34	Acceso	SW "L"
9 años	3com	SuperStack 4 5500 - EI 52 port	192.168.200.35	Acceso	SW "M"
9 años	3com	SuperStack 4 5500 - EI 52 port	192.168.200.36	Acceso	SW "N"
9 años	3com	SuperStack 4 5500 - EI 52 port	192.168.200.37	Acceso	SW "O"

-Los equipos instalados en el IDF4 son los siguientes:

Antigüedad	Marca	Modelo	IP	Tipo	Identificador
4 años	Enterasys	B5G124-48	192.168.200.41	Distribución	SW "P"
4 años	Enterasys	B5G124-48	192.168.200.42	Acceso	SW "Q"
4 años	Enterasys	B5G124-48	192.168.200.43	Acceso	SW "R"
4 años	Enterasys	B5G124-48	192.168.200.44	Acceso	SW "S"

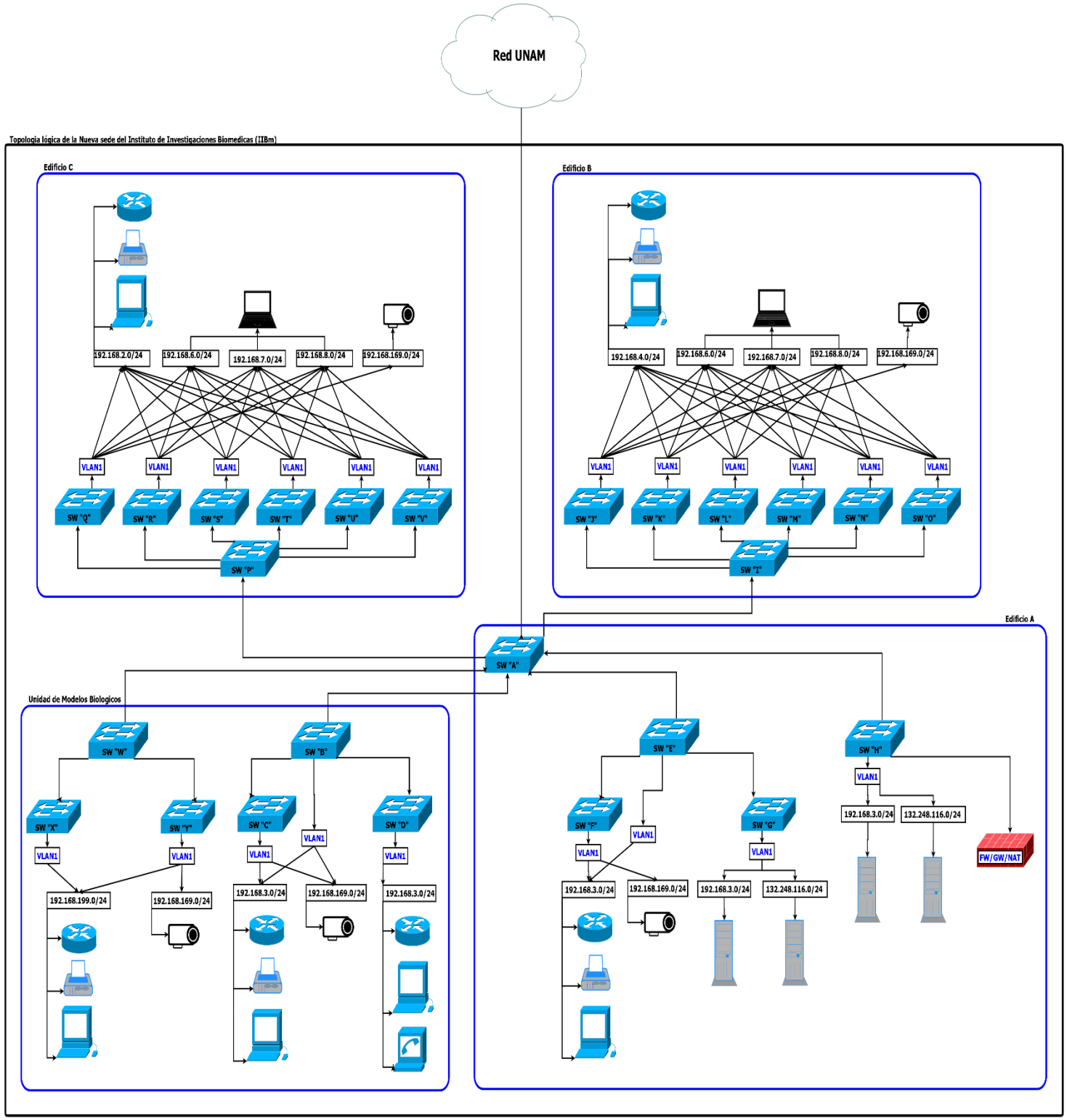
4 años	Enterasys	B5G124-48	192.168.200.45	Acceso	SW "T"
4 años	Enterasys	B5G124-48	192.168.200.46	Acceso	SW "U"
4 años	Enterasys	B5G124-48	192.168.200.47	Acceso	SW "V"

-Los equipos instalados en el IDF5 son los siguientes:

Antigüedad	Marca	Modelo	IP	Tipo	Identificador
6 años	HP	HP A5120 JE072Q	192.168.200.51	Distribución y Acceso	SW "W"
6 años	HP	HP A5120 JE072Q	192.168.200.52	Acceso	SW "X"
6 años	HP	HP A5120 JG236A	192.168.200.53	Acceso	SW "Y"

3.10 Configuración actual de los SW

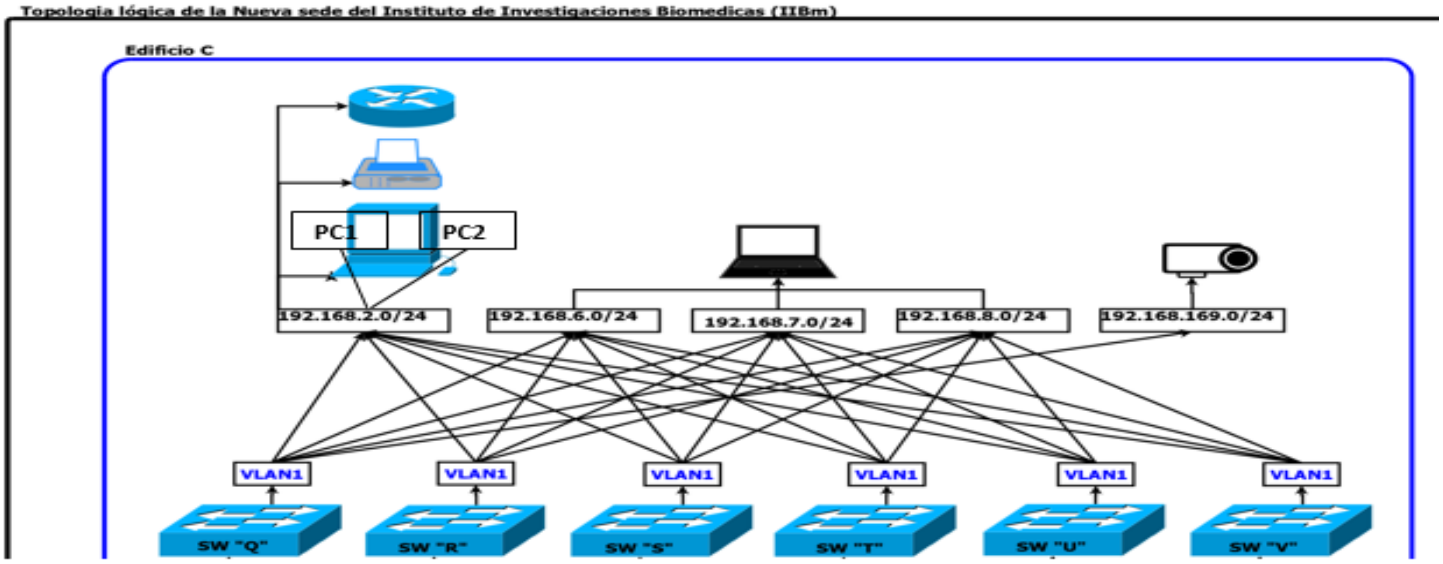
Todos los SW instalados en cada uno de los MDF e IDF se encuentran en red plana, utilizan la VLAN1 (VLAN predeterminada), es decir, todos los puertos del SW se convierten en miembros de la VLAN1 en el momento que estos se conectan al dispositivo haciendo que todos los dispositivos formen parte del mismo dominio de Broadcast.



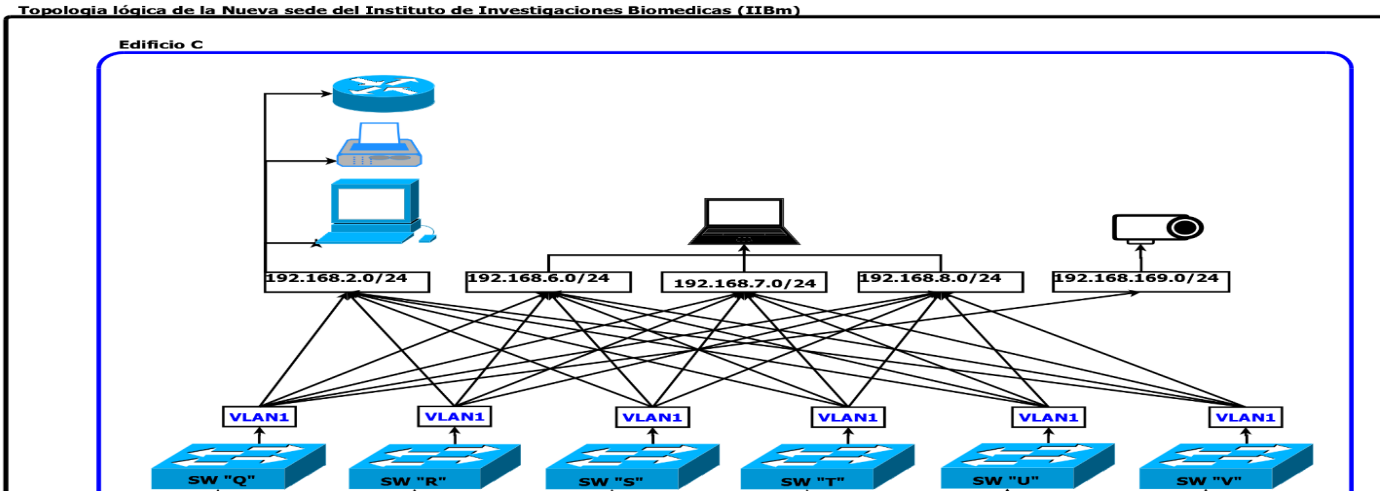
En esta configuración cualquier dispositivo conectado a cualquier puerto del SW puede comunicarse con otro dispositivo conectado a un puerto del SW (si están en el mismo segmento de red). Cuando un dispositivo en la red plan envía una trama de Broadcast el SW envía esa trama de Broadcast a todos sus puertos que pertenezcan a la misma VLAN esperando recibir una trama Unicast de respuesta.
Es decir, cuando la PC1 de la VLAN1 del SW “Q” envía una trama de Broadcast el SW “Q” envía esta trama de Broadcast a todos sus puertos dentro de la VLAN1, luego envía la trama de Broadcast al SW “P” que a su vez la envíat a todos sus puertos troncales configurados para aceptar la VLAN1 y estos nuevos SW harán lo mismo por tos todos sus puertos dentro de la VLAN1.
Luego el SW “P” enviara la trama de Broadcast al SW “A” y se repetirá lo del párrafo anterior generando una fenómeno conocido como tormenta de Broadcast, la cuál es perjudicial para el buen desempeño de la red..
Cada vez que dispositivos en diferentes redes de capa 3 (capa de red del modelo OSI) necesiten comunicarse es necesario un router, en este caso el servidor FW/NAT/GW cubre esta función (la configuración actual del FW/NAT/GW no se puede hacer pública por políticas de seguridad).

3.11 Red plana

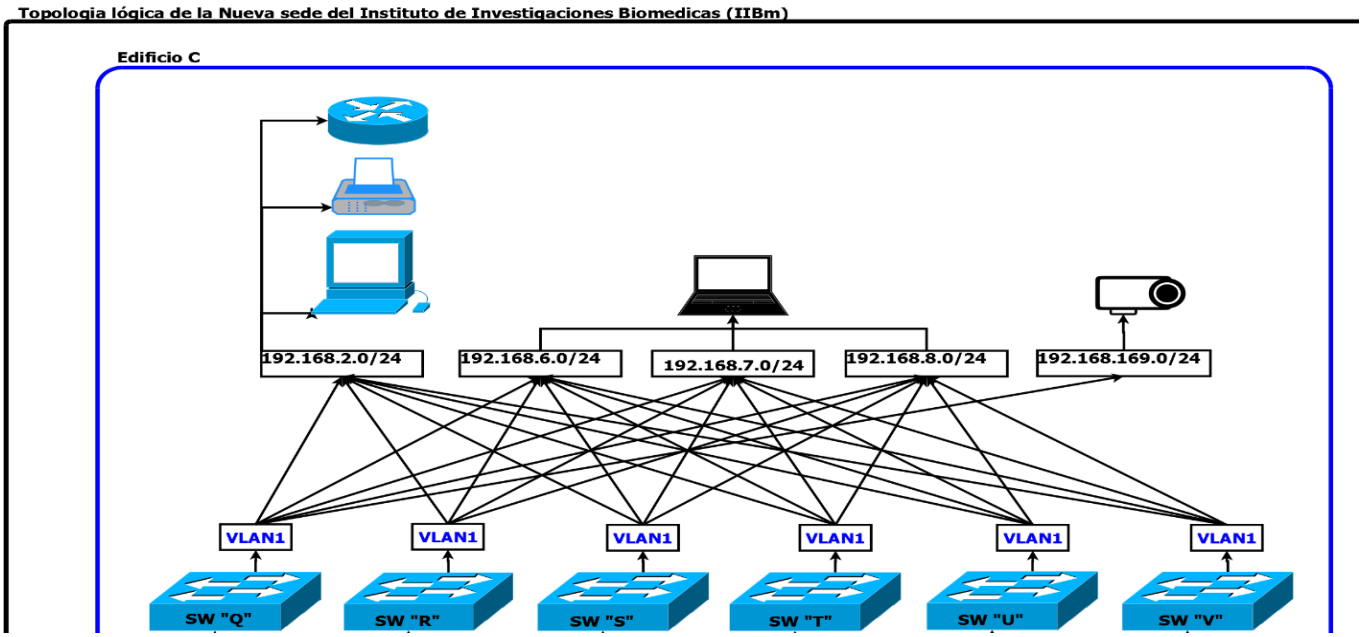
Cuando un dispositivo (PC1) conectado al SW “Q” en VLAN1 quiere comunicarse con otro dispositivo (PC2) conectado al SW “Q” en VLAN1 dentro de la red sigue los siguientes pasos:
1.- La (PC1) conectado al SW “Q” en VLAN1 envía una trama de Broadcast al SW “Q”



2.- El SW “Q” envía esta trama de Broadcast a los puertos dentro de la VLAN1 esperando recibir una trama Unicast de respuesta.

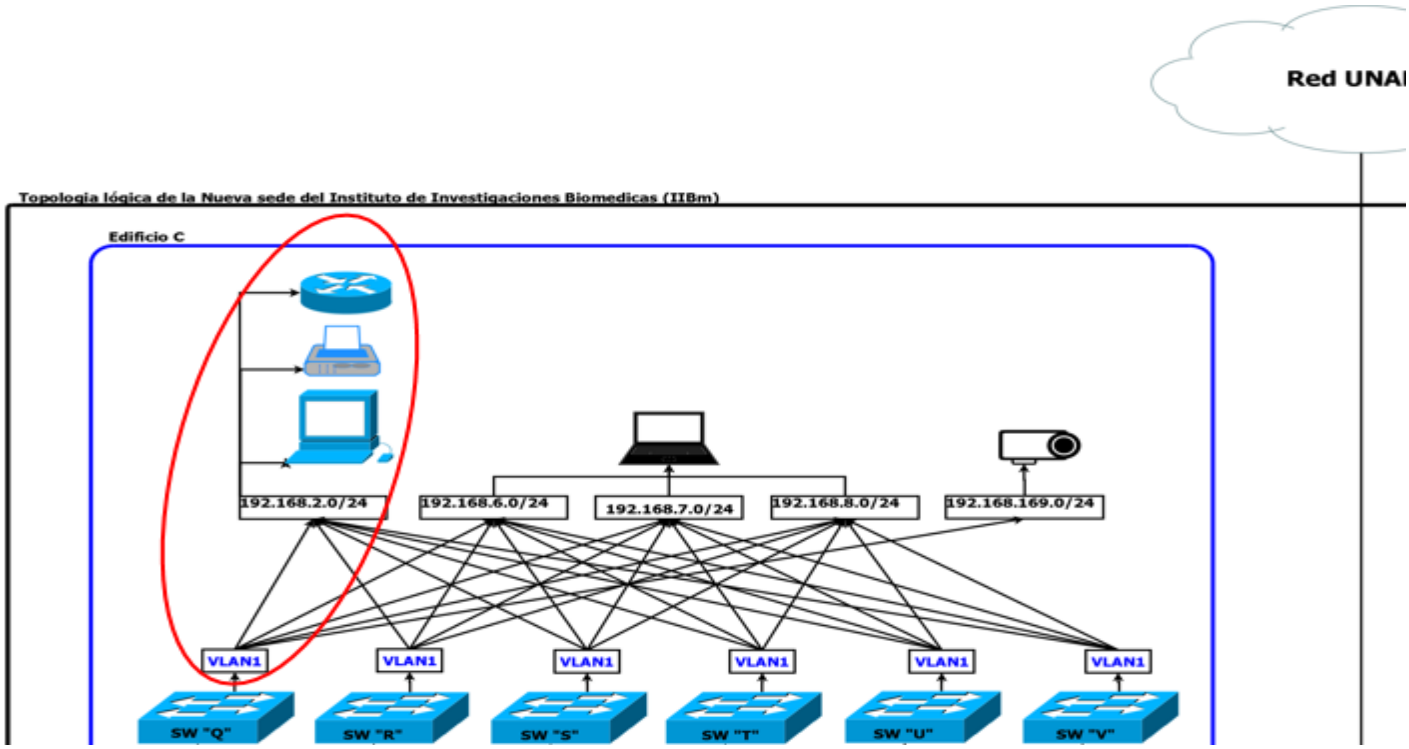


3.- Si la PC1 y la PC2 están configurados dentro del mismo segmento de red, la PC2 enviara una trama de respuesta Unicast al SW “R”, la trama de respuesta contiene la dirección MAC de destino de la PC2.



4.-El switch “Q” construye su tabla MAC y toma decisiones de conmutación de tramas basado en direcciones MAC y puertos.

5.- La PC1 mediante la invocación del protocolo ARP obtiene la dirección MAC de la PC2 y la utiliza para crear una trama Unicast que envía al SW “Q”, quien finalmente conmuta la trama al puerto especifico al que se conecta a la PC2.



3.12 Comunicación inter VLAN

Cuando la (PC1) conectada al SW “Q” en VLAN1 quiere establecer comunicación con la (PC2) conectado al SW “R” en VLAN1, sigue el siguiente procedimiento:

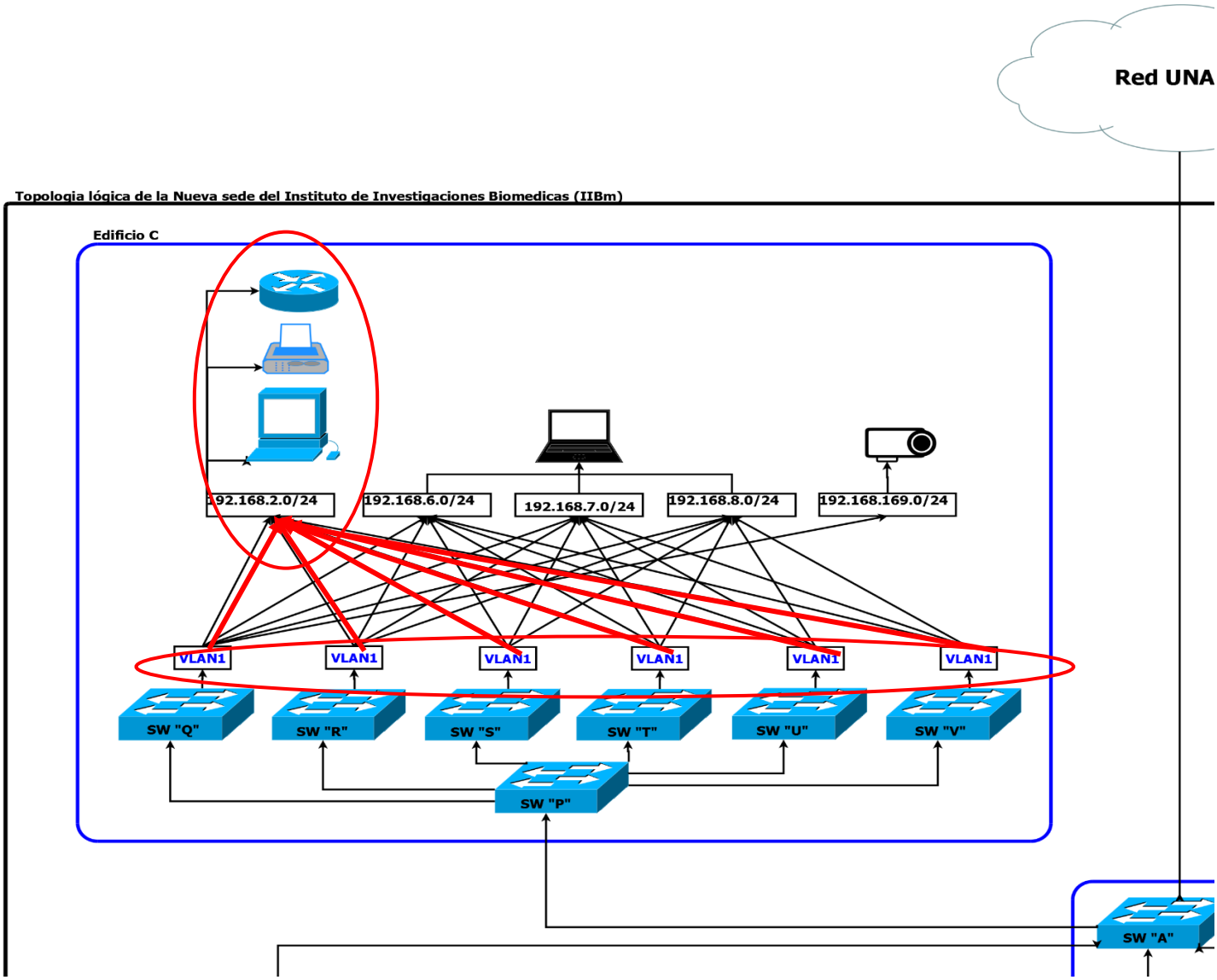
1.-La (PC1) conectada al SW “Q” en VLAN1 enviara la trama de petición ARP (Broadcast) al SW “Q”.

2.-El SW “Q” enviara a través del puerto troncal“1)” la trama de petición ARP al SW “P”.

3.-El SW “Q” y SW “P” enviaran la trama de petición ARP a todos los puertos en la VLAN1 a través de los puertos troncales configurados para admitir VLAN1(en este caso todos los enlaces troncales están configurados para aceptar todas las VLAN en la red, es decir, los puertos troncales “1)”, “2)”, “3)”, “4)”, “5)”, “6)” y “7)” mandaran la trama de petición ARP a los SW “Q”, “R”,SW “S”,SW “T”,SW “U” y SW “V”).

4.-La PC2 enviara una trama de respuesta ARP (Unicast) al SW “R”, este enviara la trama de respuesta ARP por todos los puertos troncales configurados para aceptar la VLAN1 hasta llegar a la PC1 que recibe la respuesta que contiene la dirección MAC de destino de la PC2.

5.-Ahora la PC1 tiene la dirección MAC de destino de la PC2 y la utiliza para crear una trama Unicast con la dirección MAC de la PC2 como destino, el SW “Q”, “P” y “R” envían la trama a la PC2.



CAPÍTULO IV
SOLUCIÓN PROPUESTA

4.1 Planteamiento del diseño de la red

Habiendo evaluado la distribución y diseño de la red actual del Instituto de Investigaciones Biomédicas de la nueva sede se buscó satisfacer las necesidades que tenía utilizando el equipo con el que se contaba por parte de la sección de computo en los diferentes MDF e IDF abarcando varios puntos esenciales para su buen funcionamiento.

Después de haber evaluado las diferentes posibilidades se seguirá conservando el diseño jerárquico actual con las implementaciones de las nuevas mejoras ya que aumentaba notablemente las posibilidades de escalabilidad de la red a futuro.

Se espera a mediano plazo poder cambiar los equipos a la marca de *CISCO,* la red jerárquica es más fácil de administrar y aislar posibles incidencias en el funcionamiento de la red.

Un diseño de red jerárquico brinda la posibilidad de dividir la red en capas independientes (módulos), cada capa pertenece a un edificio y piso especifico con un rol de grupo específico, el modelo de diseño jerárquico estará dividido en tres capaz:

- Core
- Distribución
- Acceso

Haciéndose mayor énfasis en la capa 1 (capara física) y capa 2 (capa de enlace) del modelo OSI ya que en estas capas se concentra el diseño de una red LAN.

Se actualizará el diagrama de topología lógica y física de acuerdo a los cambios planteados.

Se planea optimizar las virtudes que ofrecen las VLAN así como otras herramientas como IPTABLES para solucionar los problemas ya detectados en la red:

Saturación del ancho de banda
Colisiones
Perdida de información
Problemas de enrutamiento
Seguridad en la red
Duplicidad de IP

Entre otros tantos problemas estos son los de mayor relevancia para la institución.

4.2 Planteamiento para el desarrollo de una red segmentada

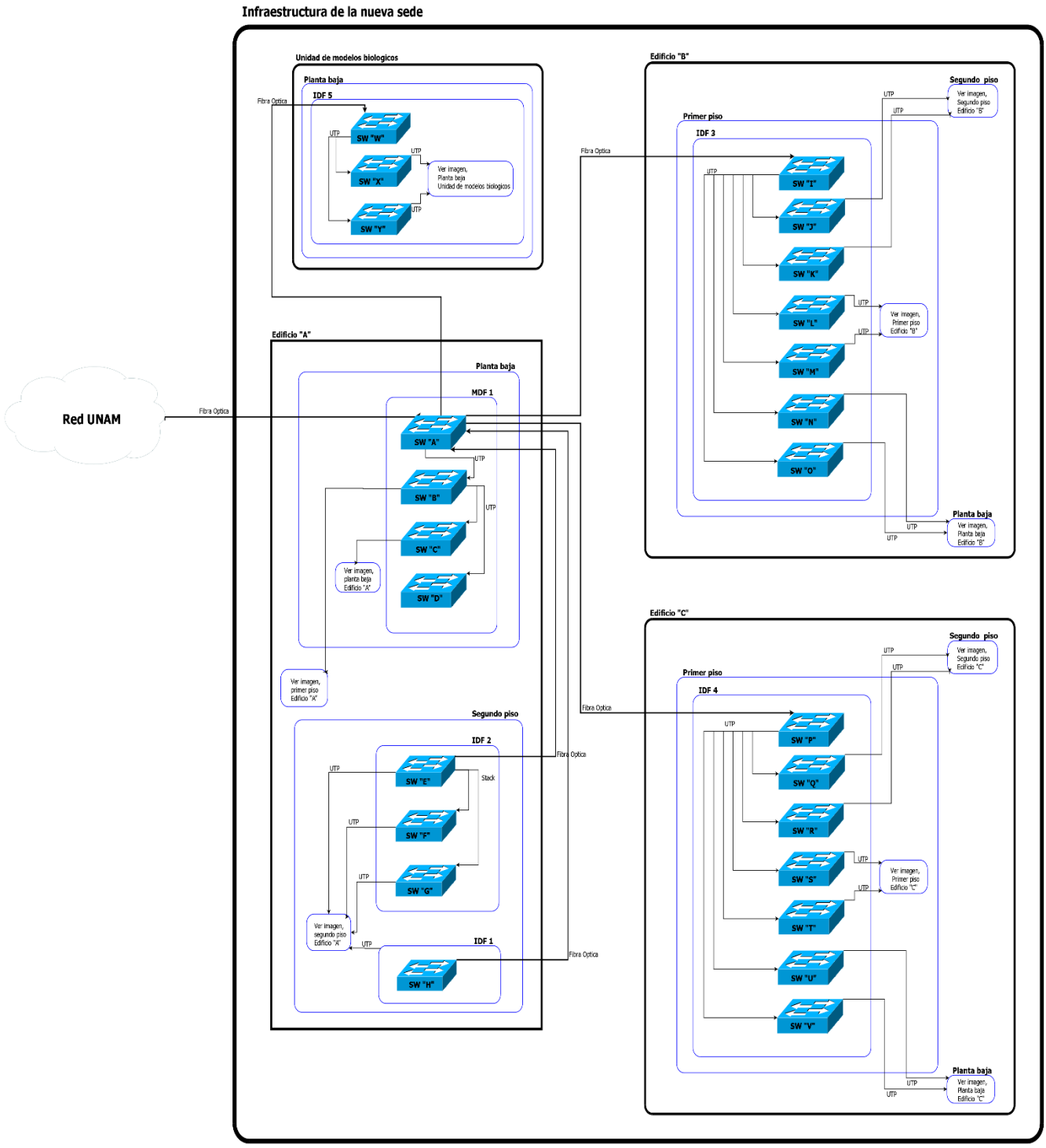
En el diseño de la nueva red segmentada utilizando tecnología VLAN toma en consideración el crecimiento de la comunidad académica y la demanda de acceso y servicios de la red.

Los SW que están instalados en los MDF e IDF no soportan el uso de múltiples VLAN problema que se resolverá con la actualización del Firmware del mismo.

Se espera separar el tráfico de los diferentes servicios y miembros de la comunidad académica que se tiene dentro de la institución para lograr:

- Mejorarla administración de la red
- Limitar las posibilidades de duplicidad de IP
- Aislamiento de problemas en el tráfico de red sin comprometer a toda la red
- Asignación de recursos y acceso de servicios por función (rol) de usuario

4.3 Topología lógica propuesta



La arquitectura de red actual será conservada dado que da el rendimiento requerido y su reubicación sería muy complicada.

4.4 Segmentación de la red empleando VLAN

La propuesta planteada contempla implementar tecnología VLAN para segmentar la red, todos los grupos de usuarios dentro de la comunidad académica utilizan actualmente direcciones IP de clase C con mascara de red de clase C asignados por grupos:

Instituto de Investigaciones Biomédicas de la nueva sede				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	132.248.116.0/24	Edificio "A": -Servidores -WAN del FW/NAT/GW	IP pública	6
VLAN 1	192.168.2.0/24	Edificio "C": -Comunidad académica -Ruteadores -Impresoras en red	IP privada	178
VLAN 1	192.168.3.0/24	Edificio "A": -Servidores internos -Comunidad académica -Ruteadores -Impresoras en red	IP privada	97
VLAN 1	192.168.4.0/24	Edificio "B": -Comunidad académica -Ruteadores -Impresoras en red	IP privada	175
VLAN 1	192.168.199.0/24	Unidad de Modelos Biológicos: -Comunidad académica -Ruteadores -Impresoras en red	IP privada	17
VLAN 1	192.168.6.0/24	Edificio "B" y "C": -Investigadores	IP privada	30
VLAN 1	192.168.7.0/24	Edificio "B" y "C": -Investigadores	IP privada	15
VLAN 1	192.168.8.0/24	Edificio "B" y "C": -Investigadores	IP privada	26
VLAN 1	192.168.169.0/24	Edificio "A", "B", "C" y Unidad de Modelos Biológicos: -Secretaria técnica y CCTV	IP privada	27
VLAN 1	192.168.200.0/24	Edificio "A", "B", "C" y Unidad de Modelos Biológicos: -Administración de SW	IP privada	25

Se plantea migrar a los usuarios dentro de la comunidad académica utilizando direcciones IP de clase B con mascara de red de clase C asignados por grupos:

Situacion futura

Instituto de Investigaciones Biomédicas de la nueva sede				
VLAN	Segmento de red	Área	Tipo IP	IP registradas
VLAN 1	132.248.116.0/24	Edificio "A": -Servidores con IP pública -WAN del FW/NAT/GW	IP pública	6
VLAN 2	172.16.2.0/24	Edificio "A": -Comunidad académica -Impresoras en red -Equipo de videoconferencia	IP privada	85
VLAN 3	172.16.3.0/24	Edificio "B": -Comunidad académica -Impresoras en red	IP privada	163
VLAN 4	172.16.4.0/24	Edificio "C": -Comunidad académica -Impresoras en red	IP privada	166
VLAN 5	172.16.5.0/24	"Unidad de Modelos Biológicos": -Comunidad académica -Impresoras en red	IP privada	16
VLAN 6	172.16.6.0/24	Edificio "A", "B", "C" y Unidad de Modelos Biológicos: -Routers	IP privada	57
VLAN 7	172.16.7.0/24	Edificio "A": -Servores internos	IP privada	5
VLAN 8	172.16.8.0/24	Edificio "B", "C" y Unidad de Modelos Biológicos: -Investigadores	IP privada	71
VLAN 9	172.16.169.0/24	Edificio "A", "B", "C" y Unidad de Modelos Biológicos: -CCTV y secretaria técnica	IP privada	27
VLAN 1	172.16.200.0/24	Edificio "A", "B", "C" y Unidad de Modelos Biológicos: -Administración de SW	IP privada	25

4.5 Las virtudes de implementar VLAN

La utilización de VLAN proporciona beneficios importantes para la administración de las redes dentro de la institución, como son:

Una mejor administración de la red: se puede llevar un mejor control de las VLAN creadas aislando cualquier posible incidencia dentro de la red o realizar configuraciones de una VLAN específica sin afectar al resto. Las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos de la red similares serán asignados a una misma VLAN haciendo que el nuevo dispositivo adquiera las políticas y procedimientos que ya se configuraron para la VLAN. La asignación de nombre de VLAN será igual al segmento de red correspondiente facilitando la identificación.

Aumento de la seguridad: existen grupos de usuarios que tienen datos sensibles, separando a cada tipo de usuario de la red en una VLAN con mayores políticas de seguridad disminuyendo las posibilidades de que existan violaciones a la información.

Reducción de costos: se reutiliza el equipo existente para mejorar la red sin la necesidad de comprar equipo nuevo haciendo un uso más eficiente de los enlaces y ancho de banda existente.

Limitar posibilidades de duplicidad de IP: si algún usuario se conecta a una red plana puede duplicar la IP de otro usuario provocando que el usuario legítimo de la IP privada asignada se quede sin servicio de red, con la segmentación de la red se limita la posibilidad de duplicidad de IP ya se por error o intencionado.

Mejor rendimiento: la división de las redes planas de capa 2 en múltiples segmentos de red (dominios de Broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.

Separación de funciones: hay usuarios que tienen necesidades diferentes de la red, dependiendo del tipo de usuario se le asigna un segmento de red con determinados privilegios o servicios.

Fragmentación de un gran dominio de Broadcast en varios dominios de Broadcast más pequeños: esto reduce el tráfico de Broadcast y mejora el rendimiento de la red.

4.6 Preparación del entorno para el servidor FW/NAT/GW

Se configurará un servidor como FW/NAT/GW empleando tecnologías Open Sourse:

S.O. GNU/Linux de la distribución Debían

Herramienta IPTABLES

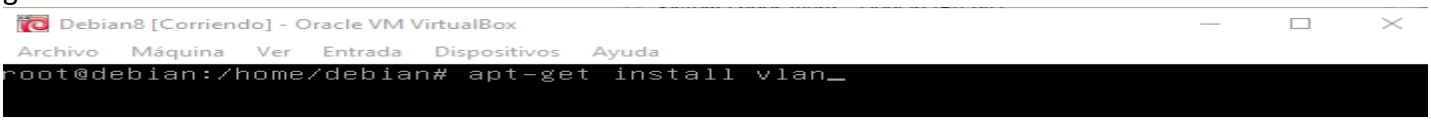
También se emplearon metodologías renovadas para la segmentación de red empleando VLAN's, implementación de políticas de seguridad más estrictas dentro del FW/NAT/GW, asignación de roles para los usuarios de la red de la comunidad académica por cuestiones de seguridad ya que cada usuario tiene una necesidad diferente y tener un registro más preciso de la estructura de la red del Instituto de Investigaciones Biomédicas.

El servidor FW/NAT/GW cumple la función de FW para el control de accesos y salidas de una red a otra, la función de GW como el siguiente punto de acceso a la red para la comunicación de redes distintas y la función de NAT para economizar la cantidad de IP públicas disponibles por parte de la institución permitiendo que múltiples direcciones IP privadas compartan una sola dirección IP publica de internet.

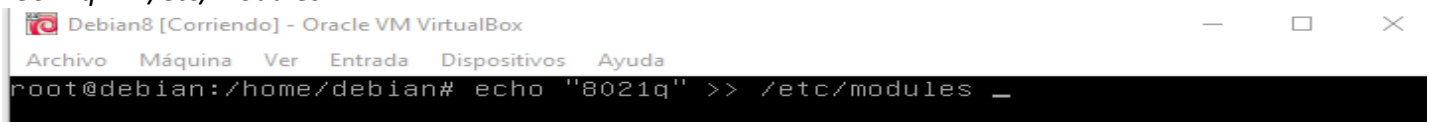
Usaremos un sistema operativo Debian 8, se deben tener dos interfaces de red físicas en el FW/NAT/GW, una funcionara como red LAN (gateway) y la otra funcionara como red WAN (salida al internet).

Para la preparación del entorno de servidor FW/NAT/GW se realizó lo siguiente:

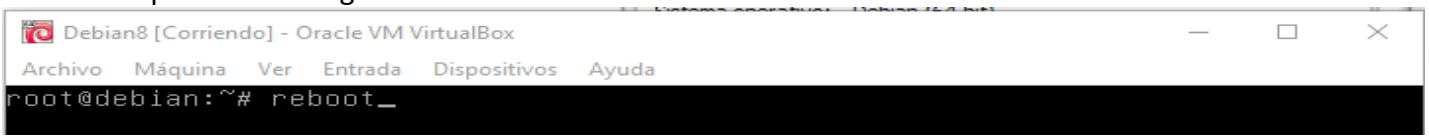
1.-Para activar el soporte de VLAN's en el S.O. GNU/Linux de la distribución Debianes necesario instalar el paquete "vlan" a través del gestor de paquetes incluido en la distribución debían, usando el comando "apt-getinstallvlan"



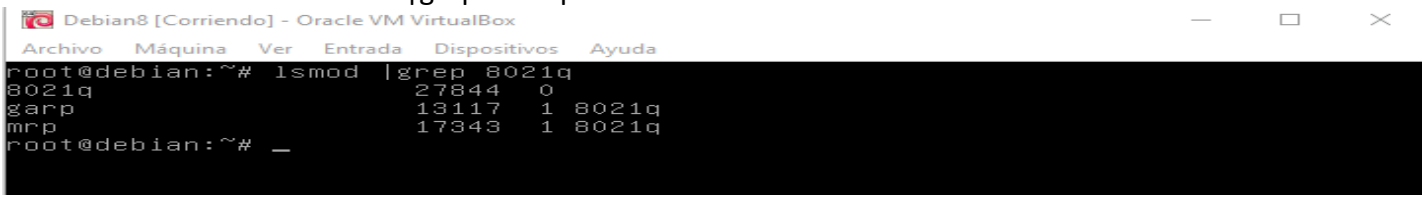
1.1.-Cargar el módulo encargado de implementar “vlan” en el sistema operativo mediante el comando: *“echo “8021q”>> /etc/modules”*



1.1.1.-Para probar la configuración anterior es necesario reiniciar el S.O. con el comando “reboot”



1.1.2.-Para comprobar que el modulo se encuentra activo en el kernel listamos los módulos cargados en el kernel con el comando “lsmod |grep 8021q”



2.-Configurarlos segmentos LAN y WAN en las interfaces de red,
editando el archivo de configuración “nano /etc/network/interfaces”
NOTA: interfaz WAN- eth0
interfaz LAN - eth1
Configurar cada interfaz de red utilizando los siguientes parámetros:

This file describes thenetwork interfaces availableonyoursystem
andhowtoactivatethem. For more information, seeinterfaces(5).

source /etc/network/interfaces.d/*

Theloopbacknetwork interface
auto lo
iface lo inetloopback

Theprimarynetwork interface

#levantar interfaz fisica
auto eth0

#WAN1
auto eth0:1
iface eth0:1 inetstatic
address 132.248.116.7
netmask 255.255.255.0
network 132.248.116.0
broadcast 132.248.116.255

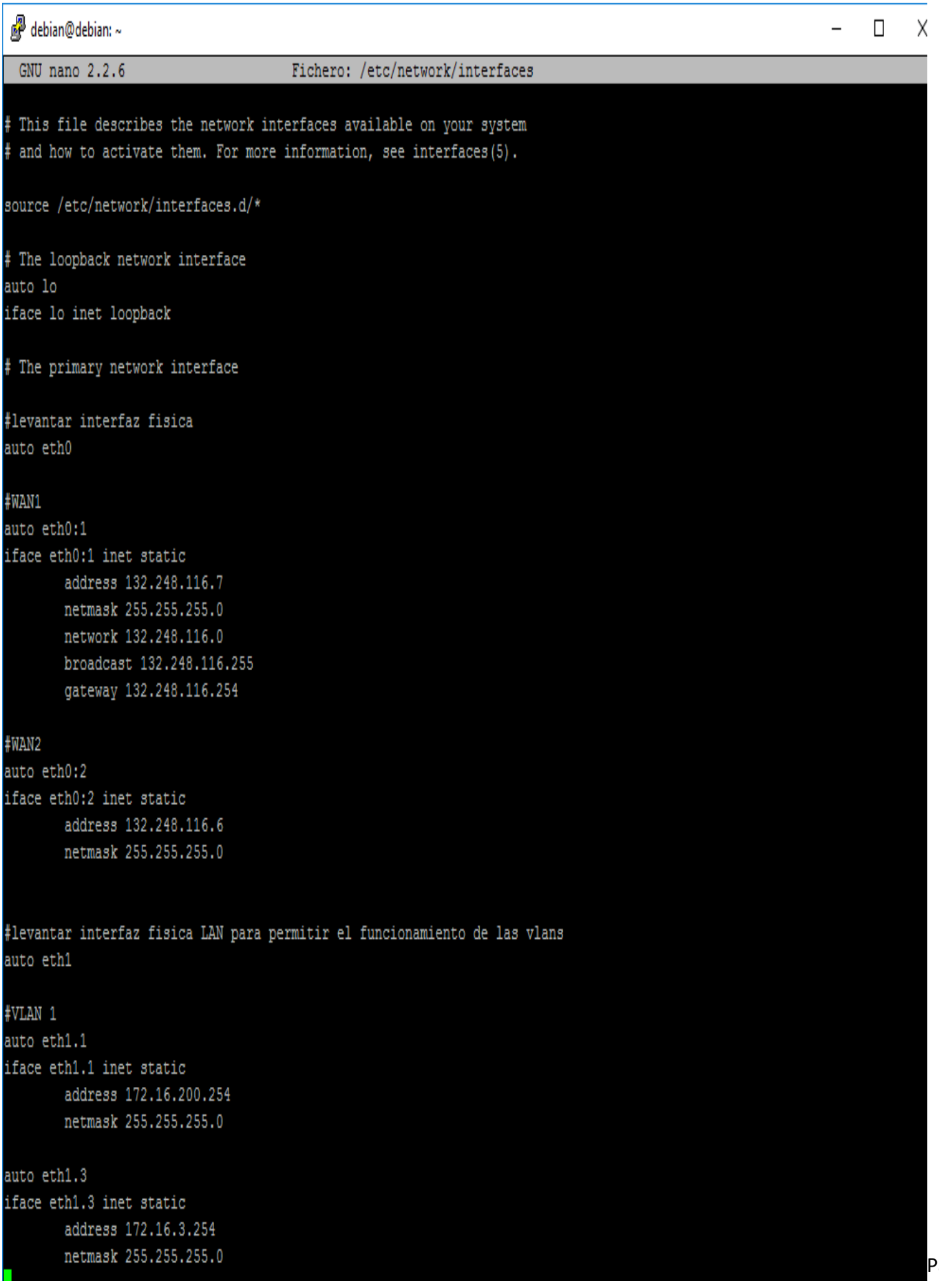
gateway 132.248.116.254

#WAN2
auto eth0:2
iface eth0:2inetstatic
address 132.248.116.6
netmask 255.255.255.0

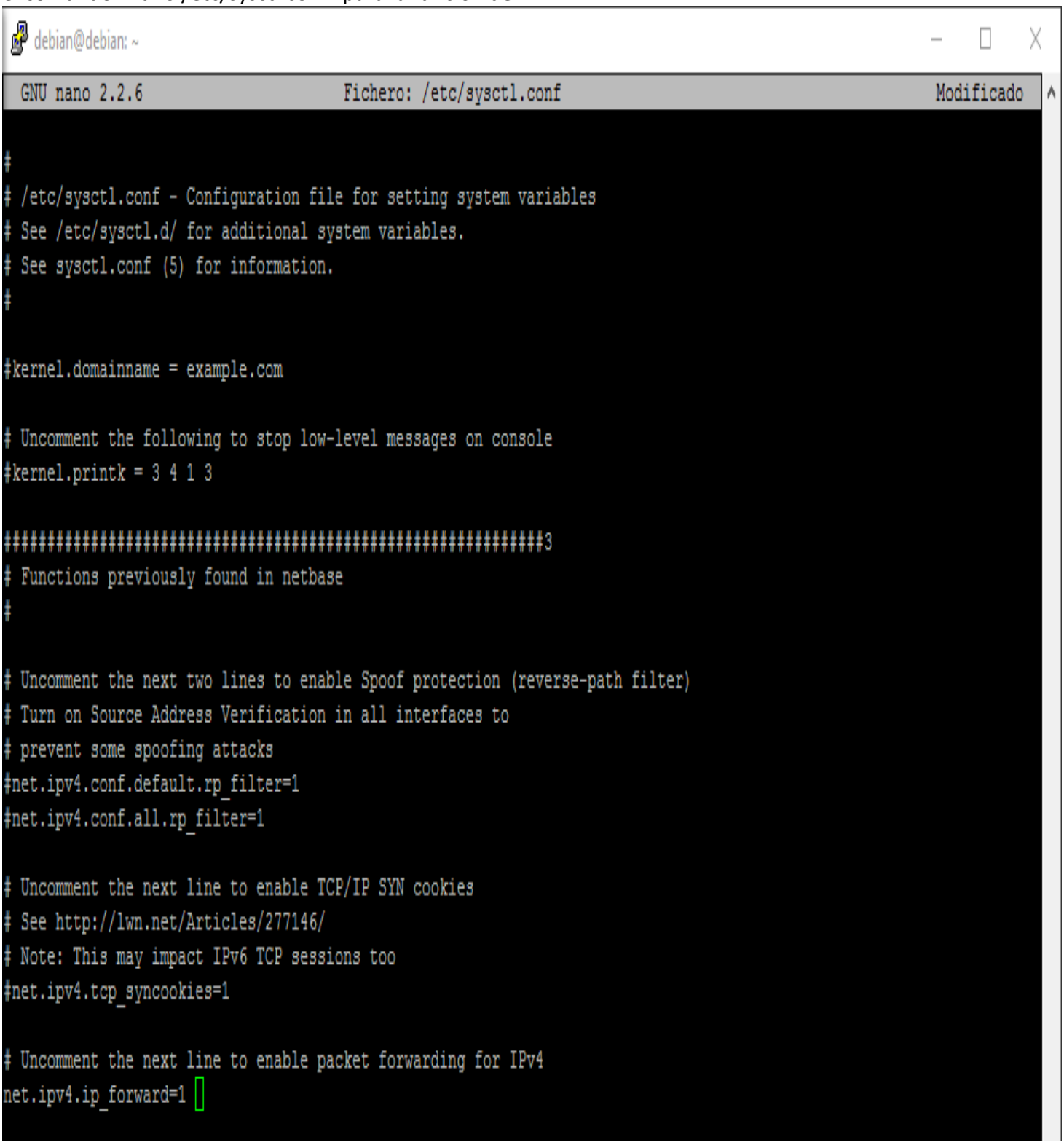
#levantar interfaz fisica LAN para permitir el funcionamiento de las vlans
auto eth1

#VLAN 1
auto eth1.1
iface eth1.1 inetstatic
address 172.16.200.254
netmask 255.255.255.0

auto eth1.3
iface eth1.3 inetstatic
address 172.16.3.254
netmask 255.255.255.0
.
.
.
auto eth1.10
iface eth1.10inetstatic
address 172.16.10.254
netmask 255.255.255.0
(Describiendo así cada una de las VLAN permitidas o registradas)

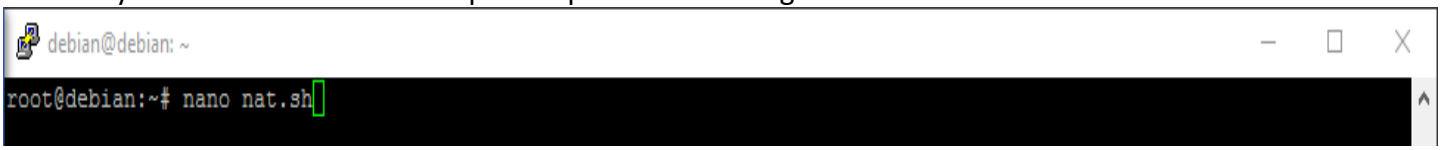

debian@debian: ~
GNU nano 2.2.6 Fichero: /etc/network/interfaces
This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*
The loopback network interface
auto lo
iface lo inet loopback
The primary network interface
#levantar interfaz fisica
auto eth0
#WAN1
auto eth0:1
iface eth0:1 inet static
address 132.248.116.7
netmask 255.255.255.0
network 132.248.116.0
broadcast 132.248.116.255
gateway 132.248.116.254
#WAN2
auto eth0:2
iface eth0:2 inet static
address 132.248.116.6
netmask 255.255.255.0
#levantar interfaz fisica LAN para permitir el funcionamiento de las vlans
auto eth1
#VLAN 1
auto eth1.1
iface eth1.1 inet static
address 172.16.200.254
netmask 255.255.255.0
auto eth1.3
iface eth1.3 inet static
address 172.16.3.254
netmask 255.255.255.0

3.-Permitir paso de paquetes de una interfaz de red a otra en el kernel, habilitar “net.ipv4.ip_forward=1” con el comando “nano /etc/sysctl.conf” para la función de NAT



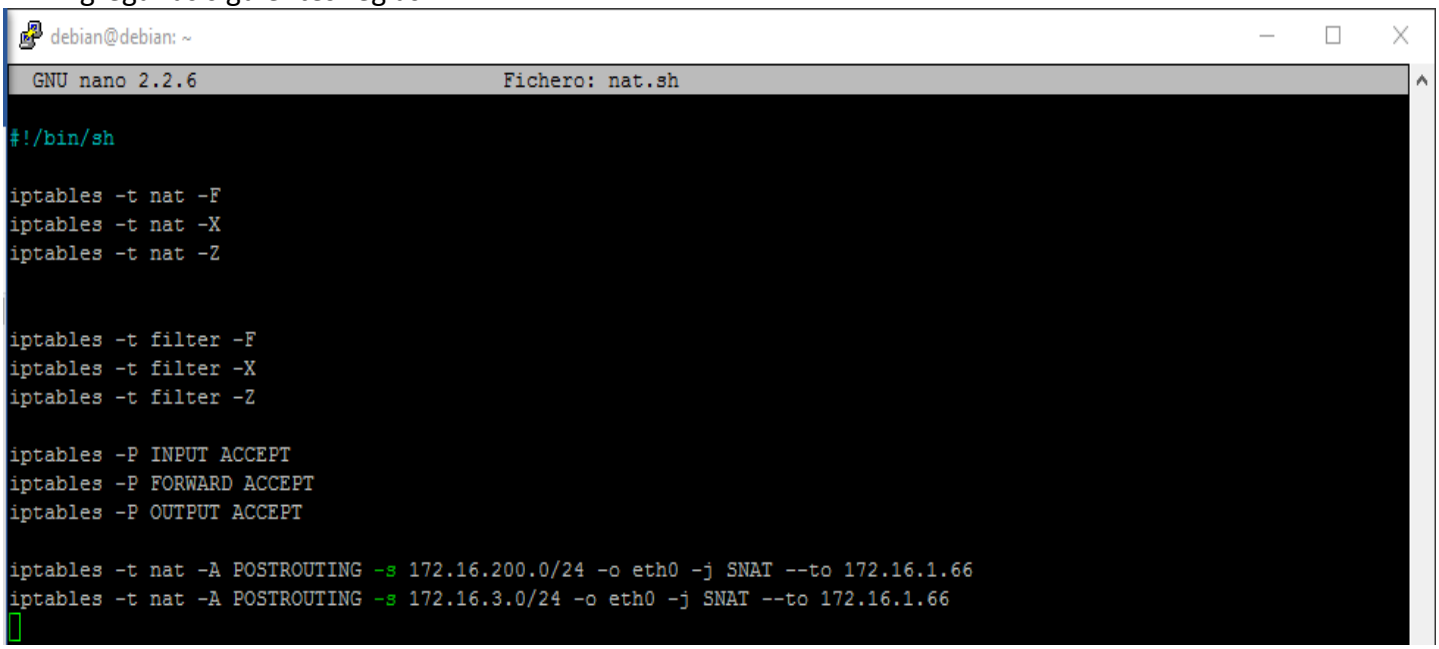
En principio un equipo con GNU/Linux no permite que pasen paquetes de una interfaz de red a otra, para que se permita esto y por tanto pueda funcionar el equipo como router, o más concretamente en este caso como dispositivo de NAT, hay que activar (dar valor 1) lo que se denomina bit de forward.

4.-Crear y editar el archivo “nat.sh” para implementar las reglas de IPTABLES relacionadas con la función NAT.



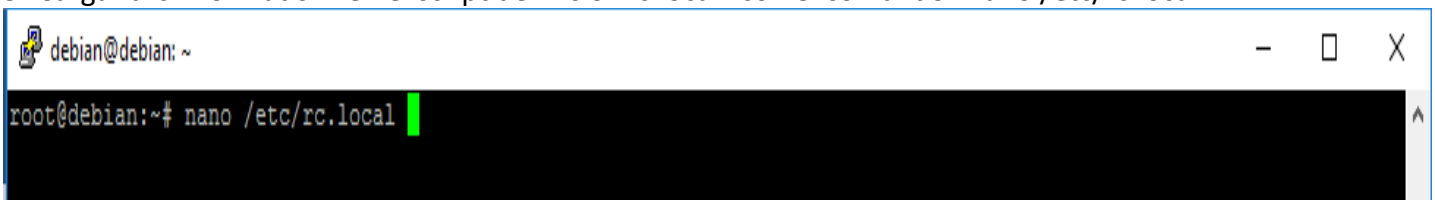
El archivo nat.sh será interpretado por el sistema al iniciarse

4.1.-Agregarlas siguientes reglas.



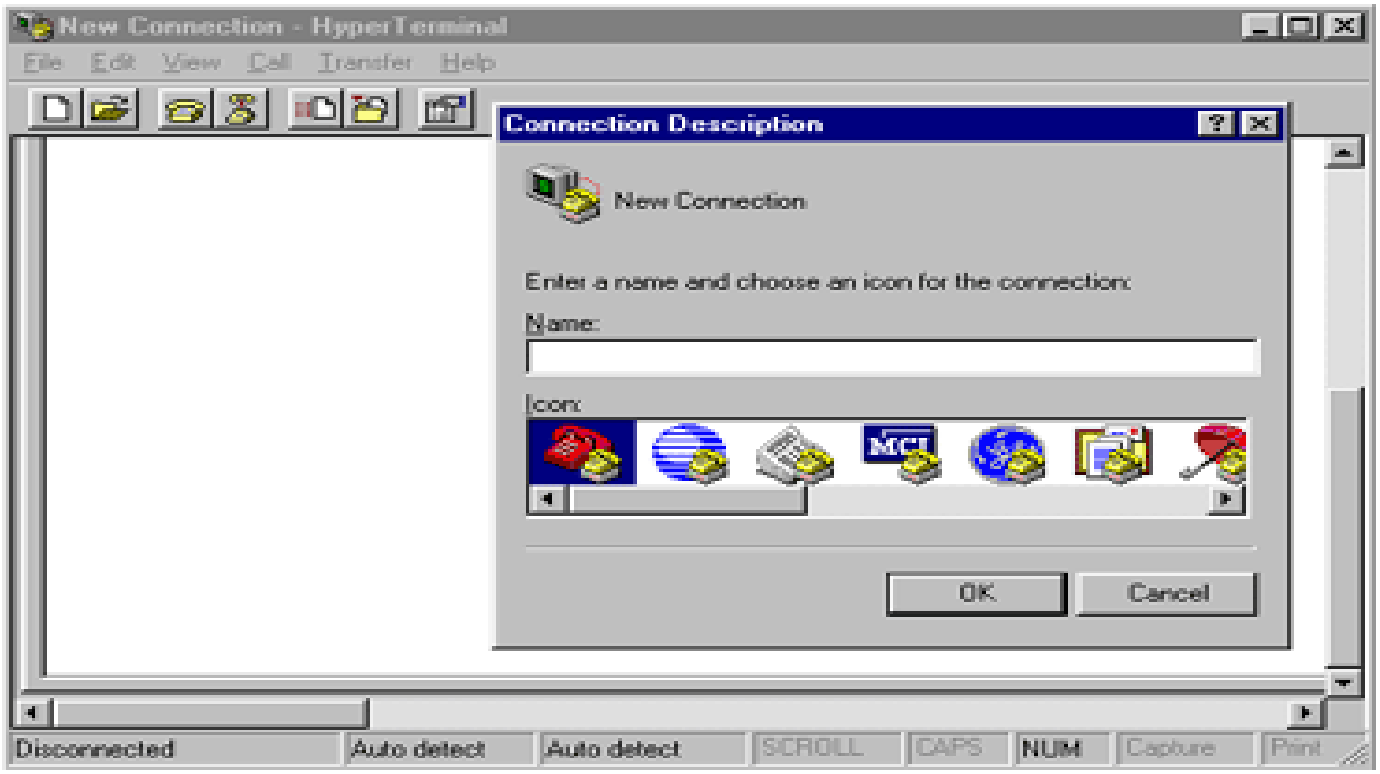
Antes de establecer las nuevas reglas para IPTABLES es una buena práctica limpiar todo el contenido para evitar riesgos residuales de alguna configuración que pueda entrar en conflicto con las nuevas reglas que se van a establecer.
Al implementar IPTABLES se tiene un mejor control en el tráfico de red, estableciendo las reglas sobre que segmentos de red tendrán acceso a los recursos de la red y que políticas de seguridad seguirán.

5.-Cargar archivo “nat.sh” en el script de inicio “rc.local” con el comando “nano /etc/rc.local”



4.7 Implementación de VLAN en capa 2

Para la implementación de la tecnología VLAN se emplearan dispositivos capa 2 los modelos de los SW instalados en los MDF e IDF son:
-G3-Series
-SuperStack 4 5500G
-B5G124-48
-HP A5120 JE072Q
Para comunicarnos con el SW utilizaremos la interfaz de *HyperTerminal*



4.7.1 Creación de las VLAN en el SW

Inicialmente los SW suelen tener solo la VLAN1 (default) de fábrica

```
<5500-EI>system
<5500-EI>system-view
System View: return to User View with Ctrl+Z.
[5500-EI]
[5500-EI]
[5500-EI]
[5500-EI]display vlan
 The following VLANs exist:
  1(default)
[5500-EI]_
```

Para crear una VLAN realizamos lo siguiente

```
[5500-EI]
[5500-EI]
[5500-EI]
[5500-EI]vlan 3
[5500-EI-vlan3]_
```

Se podrá visualizar la nueva VLAN creada

```
[5500-EI]
[5500-EI]display vlan
 The following VLANs exist:
  1(default), 3
[5500-EI]_
```

Este proceso se repetirá para todas las VLAN

4.7.2 Asignación de puerto a VLAN

Para asignar un puerto a una VLAN hay que acceder a la VLAN a la que se quiere asignar el puerto

```
[5500-EI]
[5500-EI]
[5500-EI]vlan 3
[5500-EI-vlan3]_
```

Procedemos con la asignación del puerto a la VLAN

```
[5500-EI-vlan3]
[5500-EI-vlan3]
[5500-EI-vlan3]port Ethernet 1/0/8
[5500-EI-vlan3]q
[5500-EI]save
The configuration will be written to the device.
Are you sure?[Y/N]y
Please input the file name(*.cfg)(To leave the existing filename
 unchanged press the enter key):
```

Ahora podemos ver que el puerto está asignado correctamente a la VLAN3 para este ejemplo

```
#
vlan 3
#
interface Aux1/0/0
#
interface Ethernet1/0/1
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
#
interface Ethernet1/0/6
#
interface Ethernet1/0/7
#
interface Ethernet1/0/8
 port access vlan 3
#
interface Ethernet1/0/9
  ---- More ----_
```

Este proceso se repetirá para la asignación de todos los puertos a las VLAN

4.7.3 Crear puerto troncal

Accedemos al número de puerto que se asignara como puerto tipo TRUNK

```
[5500-EI]
[5500-EI]interface Ethernet 1/0/24
[5500-EI-Ethernet1/0/24]_
```

Se estable la asignación de puerto tipo TRUNK

```
[5500-EI-Ethernet1/0/24]
[5500-EI-Ethernet1/0/24]port link-type trunk
[5500-EI-Ethernet1/0/24]
```

Asignamos las VLAN permitidas en el puerto TRUNK

```
[5500-EI-Ethernet1/0/24]
[5500-EI-Ethernet1/0/24]port trunk permit vlan 3
 Please wait... Done.
[5500-EI-Ethernet1/0/24]_
```

Guardaremos la configuración en un archivo asignándole un nombre propio

```
Are you sure?[Y/N]n
[5500-EI]save asignacion_VLAN3
 Invalid file name!
[5500-EI]save asignacionvlan
 Invalid file name!
[5500-EI]save ?
  STRING  The name of specific file(*.cfg)[unit][drive]filename<5-56>
  backup  backup config file
  main    main config file
  safely  Save current configuration safely
  <cr>

[5500-EI]save asignacion_VLAN3.sfg
 Invalid file name!
[5500-EI]save asignacion_VLAN3.cfg
The current configuration will be saved to flash:/asignacion_VLAN3.cfg [Y/N]:y
Now saving current configuration to the device.
Saving configuration. Please wait...
......
 Unit1 save configuration flash:/asignacion_VLAN3.cfg successfully

[5500-EI]
%Apr  2 00:04:25:233 2000 5500-EI CFM/3/CFM_LOG:- 1 -Unit1 save configuration su
ccessfully.
```

4.7.4 Asignación IP de administración

Cada SW tendrá asignada una IP de administración, para ello se accede al SW a través de la interfaz HYPERTERMINAL con el siguiente comando

```
[5500-EI]
[5500-EI]
[5500-EI]interface vlan 1
[5500-EI-Vlan-interface1]_
```

Una vez dentro se asignara la IP de administración

```
[5500-EI-Vlan-interface1]
[5500-EI-Vlan-interface1]
[5500-EI-Vlan-interface1]
[5500-EI-Vlan-interface1]
[5500-EI-Vlan-interface1]
[5500-EI-Vlan-interface1]ip addres
[5500-EI-Vlan-interface1]ip address 172.16.200.3
                                                 ^
 % Incomplete command found at '^' position.
[5500-EI-Vlan-interface1]
[5500-EI-Vlan-interface1]ip address 172.16.200.3?
   X.X.X.X

[5500-EI-Vlan-interface1]ip address 172.16.200.3 255.255.255.0
[5500-EI-Vlan-interface1]
%Apr  2 00:09:20:344 2000 5500-EI IFNET/5/UPDOWN:- 1 -Line protocol on the inter
face Vlan-interface1 is UP

[5500-EI-Vlan-interface1]
```

Este proceso se repetirá para la asignación de IP de administración de todos los SW

CONCLUSIONES

Dado el análisis que se hizo de la situación actual y solución propuesta de la infraestructura de red de biomédicas no se puede dejar pasar por alto la necesidad de que la infraestructura contara con un enlace redundante de internet proveniente de la DGTIC dado que si este enlace llegara a fallar dejaría sin servicio de internet a toda la institución de biomédicas causando problemas a los investigadores y académicos ya que varios de sus tareas y trabajos diarios dependen de su conexión a internet para poder llevarlas a cabo.

Se reutilizo el equipo de la infraestructura con el que ya se contaba aprovechando las mejoras posibles de actualización de software, firmware, VLAN y utilización de tecnologías OPEN SOURCE para poder satisfacer la nueva demanda que requería la comunidad académica de la institución, logrando alcanzar el objetivo planteado.

Se mitigaron gran parte de los problemas detectados en la infraestructura de red, se elaboró un manual e inventario de los equipos con los que cuenta la sección de cómputo distribuidos en el MDF e IDF de cada edificio logrando así una notable mejor administración del equipo y su localización física y lógica en la red.

Se mejoró la seguridad en la red, se optimizo la segmentación de la red utilizando VLAN lo cual podrá ayudar a largo plazo a mantener, mejorar y administrar los equipos conectador en la red cabe.

RECOMENDACIONES

La sección de computo ha hecho un gran trabajo manteniendo la red de biomédicas con el equipo con el que se cuenta en stack, no obstante, se hace evidente la necesidad de tener un manual de contingencia en caso de que el enlace de internet proveniente de la DGETIC falle, esto se puede solucionar teniendo un enlace redundante que pudiera garantizar de cierta medida que si un enlace llegara a fallar el otro estaría disponible para tener continuidad de servicio.

Se necesita realizar una renovación de los equipos que cuenta la red, algunos de ellos ya se encuentran en end-life o están a punto de llegar a su tiempo de vida útil, no se cuenta con equipo de reserva, por lo que si un SW llega a fallar es sustituido por otro que no tenga máxima prioridad en alguna otra parte de la red.

El instituto llego a crecer rápidamente a lo largo del tiempo, ampliando consigo la necesidad de acceso al medio, se plantearía no solo cambiar el equipo, si no que rediseñar la estructura que se tiene para que tenga mayor escalabilidad en base a la demanda del servicio que la comunidad académica requiere.

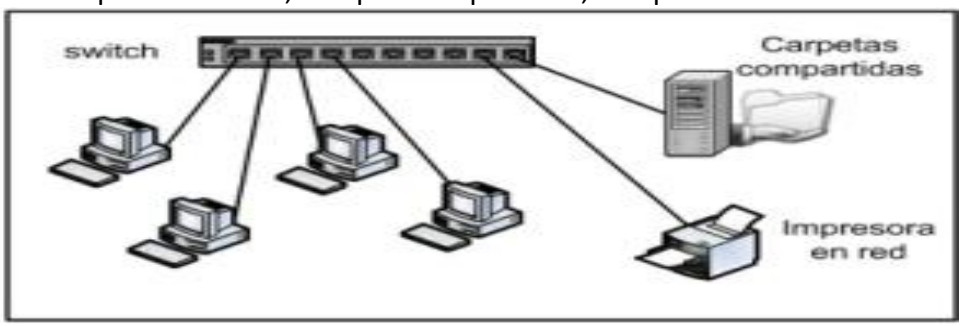
ANEXOS

Anexo1.- Clasificación de redes de datos

Una red de datos puede clasificarse de acuerdo a la arquitectura física, el tamaño y la distancia cubierta.
De acuerdo a alcance que tenga la red de datos se puede clasificar en:

LAN (Red de Área Local, Local Area Network):

Las redes de área local son un conjunto de dispositivos que pertenecen a la misma organización (una vivienda, un edificio, la mayoría de propiedad privada) y están conectados dentro de un área geográfica pequeña mediante una red cableada. La velocidad de transferencia de datos en una red de área local alcanza los 10 Mbps (en una red Ethernet) y 1Gbps (en Gigabit Ethernet), una red LAN suele proveer de 100 a 1000 usuarios, una red LAN permite: compartir archivos, compartir impresoras, compartir la conexión a Internet, etc.



Esquema de una red LAN[32]

MAN (Red de Área Metropolitana, Metropolitan Area Network)
WAN (Red de Área Amplia, Wide Area Network)
WLAN (Red de Área Local Inalámbrica, Wireless Local Area Network)

Anexo2.- Capaz del modelo OSI

El modelo consta de 7 capas que definen las diferentes fases por las que deben pasar los datos para ser transmitidos de un dispositivo a otro sobre una red de comunicaciones, este modelo ofrece ventajas en el diseño y análisis de procesos de comunicaciones mediante la división de cada fase de la comunicación, haciéndolos menos complejos, organizados e independientes entre sí en el tratamiento de problemas de red. En el modelo de referencia OSI las funciones definidas se complementen unas a otras, algunas funciones pueden ejecutarse de manera sucesiva precediendo a otras, cuando se envía la información el emisor agrega un identificador desde la capa superior a la inferior de manera sucesiva y cuando recibe la información el receptor éste va interpretando los identificadores de la capa inferior a la superior.

Nivel 1, capa física (señal y transmisión binaria):

Es la capa más baja del modelo OSI, define las características físicas de una red, la tarea primordial de esta capa es la transmisión bit a bit entre el emisor y el receptor utilizando señales eléctricas codificados en datos digitales (0 o 1). Ejemplo; el cable coaxial, cable de par trenzado, fibra óptica.

Nivel 2, capa de enlace de datos (direccionamiento físico):

Esta capa toma los datos digitales y los transforma en señales, los bits de datos se organizan en tramas, se crea un encabezamiento en el que se puede identificar al emisor y al destinatario por su dirección física, es decir garantiza la conexión y transmisión de datos a través de los enlaces físicos que utiliza el ordenador para conectarse a la red. Utiliza protocolos como LLC, la MAC address, ethernet y dispositivos como switch.

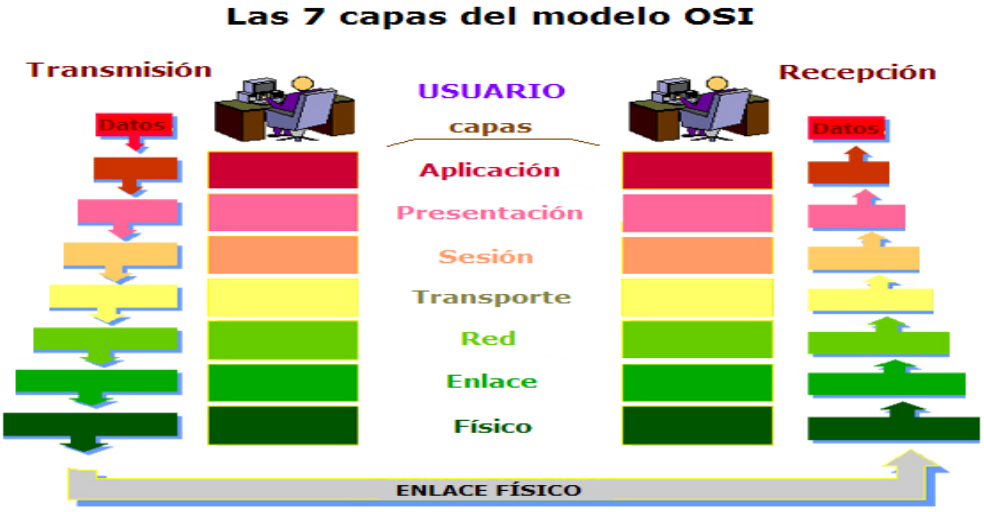
Nivel 3, capa de red (Determinación de ruta e IP):

Esta capa se encarga de interconectar redes y encaminar los paquetes del origen al destino decidiendo que ruta de acceso físico deberán tomar los datos en función de las condiciones de la red, prioridad de servicio y

[32] http://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

otros factores. Utiliza protocolos IP, IPX y dispositivos como router y switch (algunos switch trabajan en el nivel 3).

Nivel 4, capa de transporte (Conexión extremo a extremo y fiabilidad de los datos)
Nivel 5, capa de sesión (comunicación entre dispositivos de la red)
Nivel 6, capa de presentación (representación de los datos)
Nivel 7, capa de aplicación (servicio de red a aplicaciones)

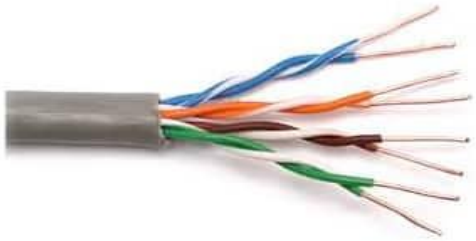


Interacción de las capas del modelo OSI[33]

Anexo3.- Tipo de cables de red

El cable de red es el medio físico por el cual podemos conectar un dispositivo con otro, una terminal de red con otra y es por este medio por el cual se transmiten y/o transfieren los datos.

Cables UTP (Unshielded twisted pair): son cables de pares trenzados de cobre, comúnmente aislados con plástico PVC como su única protección, esto los hace propensos a ser afectados por las interferencias electromagnéticas, después de los 100 metros empiezan a tener perdida de información, son los más usados para el cableado de la LAN.



Cable UTP común[34]

El cable UTP se puede dividir en siete categorías y algunas variantes:

Categoría 1
Categoría 2
Categoría 3
Categoría 4
Categoría 5

[33] http://superinformacionweb.blogspot.mx/2014/03/modelo-osi-ventajas-y-desventajas.html
[34] http://www.tektel.com/b1/faq/ethernet-cable-faqs/utp-vs-stp-cable-image/

Categoría 5e (enhanced, mejorado): es una variante mejorada de la categoría 5, tiene una velocidad de transmisión máxima de 1000Mb/s o "1000 Base-T" o "Gigabit Ethernet", haciéndolo hasta 10 veces más rápido y es retro compatible con sus versiones anteriores.
Categoría 6: Tiene una velocidad de transmisión máxima de 1Gb/s, puede transmitir a distancias de 100 metros antes de sufrir pérdidas de información, resiste muy bien el ruido de interferencias de señal gracias a su blindaje.
Categoría 6a (aumentado): es una variante mejorada de la categoría 6, esta nueva especificación mitiga los efectos de la diafonía o crosstalk (ruido), tiene una velocidad de transmisión máxima de 10 Gb/s.
Categoría 7: Transmisión máxima de 10Gb/s, puede transmitir a distancias de 100metros antes de sufrir pérdidas de información, resiste muy bien el ruido de interferencias de señal gracias a que posee blindaje para cada par de cable individualmente.
Cable FTP (Foiled Twisted Pair): son cables muy similares al UTP con la diferencia de estar protegido con una malla metálica global que cubre a todos los cables, resiste mejor las perturbaciones externas.

Cable FTP común [35]

Cables STP (Shielded twisted pair): son cables muy similares al UTP con la diferencia de estar protegido con una malla metálica individual por cada par de cables, esto le ayuda a resistir mucho más las perturbaciones externas y radiaciones electromagnéticas permitiendo mantener una mejor calidad en los datos transmitidos y menor perdida de información.

Cable STP común [36]

Cable de fibra óptica: Estos medios transportan las señales digitales de datos en forma de pulsos modulados de luz, está formado por un par de cables de fibra de vidrio, cada uno consta de un delgado cilindro de vidrio que constituye el núcleo, cubierto por un revestimiento de vidrio con un índice de refracción menor y sobre este se encuentra un forro de goma o plástico. Un hilo de vidrio solo puede transmitir señales en una dirección haciendo que cada cable tenga dos hilos de vidrio para que uno se encargue de transmitir y el otro de recibir las señales.

[35] https://pondalpar113.wordpress.com/tipos-de-cable/
[36] http://www.tektel.com/b1/faq/ethernet-cable-faqs/utp-vs-stp-cable-image/

Tipos de conectores para fibra óptica:

Tipos de conectores de Fibra óptica[37]

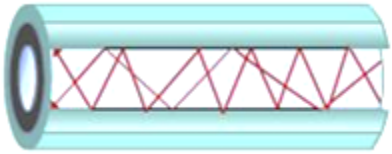
FC: se usa en la transmisión de datos y en las telecomunicaciones.
FDDI: se usa para redes de fibra óptica.
LC y MT-Array: se utiliza para la transmisión de alta densidad de datos.
SC y SC-Dúplex: se utilizan para la transmisión de datos.
ST o BFOC: se usa en redes de edificios y en sistemas de seguridad.
El conector LC y el SC son los más utilizados.

Modos de propagación en fibra óptica:

Monomodo: El haz de luz dentro del núcleo viaja sin rebotar en sus paredes permitiéndole mantener velocidades de transferencia más altas, los datos se transfieren trazando una línea donde solo se propaga un modo de luz permitiéndole viajar mayores distancias de hasta 400km, el diámetro de la fibra de vidrio es de 8,3 a 10 µm, puede alcanzar velocidades de hasta varias decenas de Gbit/s.

Fibra óptica Monomodo[38]

Multimodo: Los haces de luz pueden circular por más de un modo, es comúnmente usado para distancias máximas de 2km, el núcleo de una fibra multimodo tiene un índice de refracción superior, el diámetro de la fibra de vidrio es de 50 a 125 µm, puede alcanzar velocidades de hasta 10 Gbit/s.



Fibra óptica Multimodo[39]

[37] http://www.china-cable-suppliers.com/
[38] http://www.ingenieriasystems.com/2013/02/redes-y-comunicaciones-i-medios-de_21.html
[39] http://www.ingenieriasystems.com/2013/02/redes-y-comunicaciones-i-medios-de_21.html

Anexo4.- Interfaz de red

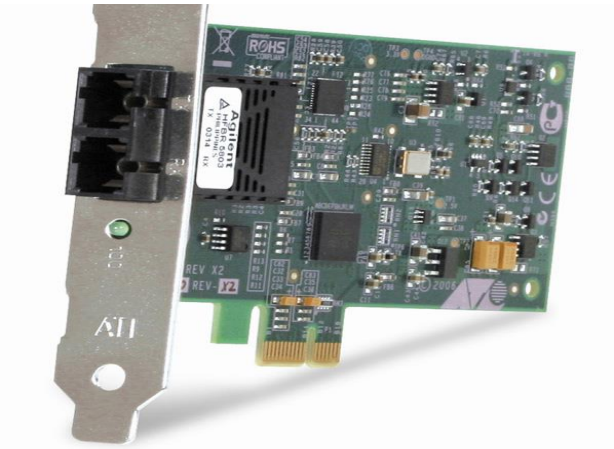
La interfaz de red, Network Interface Card (NIC) o adaptador de red sirve de intermediario entre el ordenador y la red permitiendo compartir recursos o acceder a una red, convierte los datos enviados por el ordenador a un formato que pueda ser interpretado por la red y también a la inversa traduce los datos que ingresan de la red para que el ordenador pueda leerlos. Los adaptadores de red se pueden clasificar en Token Ring y ARCNET que son para redes especiales, las WIFI y las ETHERNET son para redes más comunes, a su vez cada tarjeta de red se puede clasificar por el tipo de cable que utiliza (cable de par trenzado, fibra óptica, etc.) y por el tipo de conexión que tiene (PCI, USB PCMIA), las tarjetas de red pueden estar integradas a la placa base o ser añadidas. Cada tarjeta de red puede ser identificada por su dirección única MAC de 48 bits regulada por el estándar IEEE y se le puede asignar una IP. La interfaz de red puede estar conectado a la red de manera física o inalámbrica, opera en la capa dos y tres del modelo OSI.

Existen diferentes tipos de tarjetas de red

Tarjeta de red Token Ring

Tarjeta de red ARCNET

Tarjeta de red Ethernet: Utilizan conectores RJ-45, BNC, UIA, etc. El caso más habitual de tipo de conector para esta NIC es el RJ-45, su velocidad de transmisión de información puede ir dese los 10Mb/s hasta los 10Gb/s, en algunos casos se utilizan cables de par trenzado de categoría 6 y 7 que trabajan a frecuencias más altas. Las velocidades especificadas en la NIC son teóricas, por ejemplo, una tarjeta que tenga 100Mb/s de velocidad de transmisión realmente solo transmitirá 78 Mb/s, este tipo de conexión ya sea de tarjeta o cable permite unir ordenadores, servidores, etc. de diversos modelos o marcas, este tipo de tarjetas de red son las más utilizadas en la actualidad.



NIC Ethernet[40]

Tarjeta de red inalámbrica: la tarjeta de red inalámbrica o Wireless también se les consideran NIC, vienen en diferentes versiones dependiendo de las normas a la cual se ajustan, las más populares son la 802.11b (es el estándar definido por la IEEE para determinar la frecuencia y velocidad de una señal WIFI), su ventaja evidente es la flexibilidad que tiene de no requerir cables para poder establecer una conexión entre un dispositivo y la tarjeta inalámbrica, este tipo de tarjetas suelen estar provistas por una antena, este tipo de tarjetas han empezado a caer en desuso por la aparición de las tarjetas USB adaptadas a WIFI.

[40] http://yovanyck.blogspot.mx/

Tarjeta de red inalámbrica[41]

Tarjetas de fibra óptica: envían y reciben información por medio del uso de fibra óptica en la red, tiene comúnmente puertos SFP, los conectores más usados para este tipo de tarjetas son los LC y SC, actualmente son las NIC con mayos velocidad de transmisión de datos.

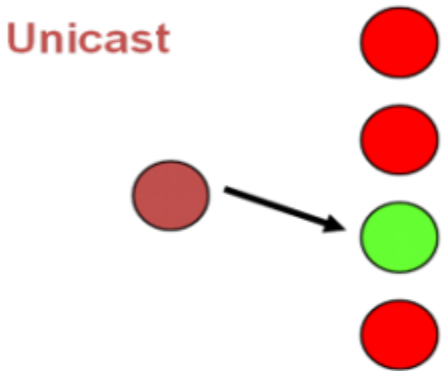
Tarjeta de fibra óptica[42]

Anexo5.- Método de transmisión de información Unicast, Multicast y Broadcast

Unicast: Es un método de transmisión uno a uno (one-to-one), en este método él envió de datos se realiza desde un único nodo emisor a un único nodo receptor, en un entorno unicast aunque varios usuarios puedan solicitar la misma información al servidor al mismo tiempo, el servidor responderá a las peticiones de los usuarios enviando la información a cada usuario, el método unicast envía por separado el tráfico de los datos a cada equipo que ha solicitado los datos, la desventaja de este método es que puede provocar la inundación (flooding) de la red por la cantidad de tráfico que se puede llegar a generar, un ejemplo del uso del método unicast sería una llamada telefónica o los protocolos: http, smtp, ftp, etc.

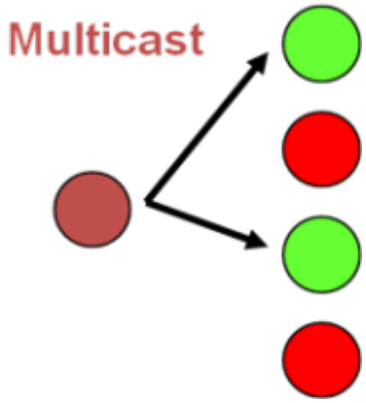
[41] http://yovanyck.blogspot.mx/

[42] https://www.startech.com/mx/Industriales-ES/Adaptadores-Red/tarjeta-de-red-pcie-gigabit-ethernet-fibra-optica-sfp-abierto~PEX1000SFP2



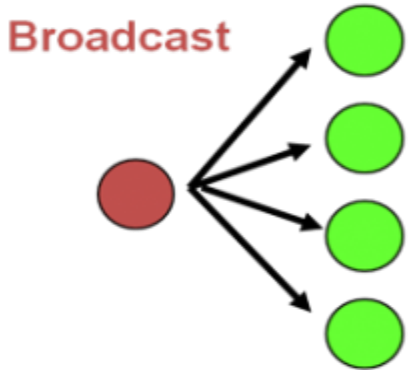
Método de transmisión unicast[43]

Multicast: Es un método de transmisión de uno a muchos (one-to-many), en este método él envió de datos se realiza desde un nodo emisor a multiples nodos receptores de manera simultánea, este modo de transmisión es similar al broadcast excepto que el multicast solo envía la información a un grupo específico y el broadcast envía la información a todos los nodos de la red, se basa en un único proceso de envió independientemente del número de nodos receptores, desde el origen hacia todos los nodos receptores que posean al menos un miembro de una determinada dirección multicast, un ejemplo del uso del método multicast en internet es un IRC (Internet Relay Chat).



Método de transmisión Multicast[44]

Broadcast: Es un método de transmisión de uno a todos (one-to-all), en este método el envío de datos se realiza de un nodo emisor a todos los nodos receptores de manera simultánea.

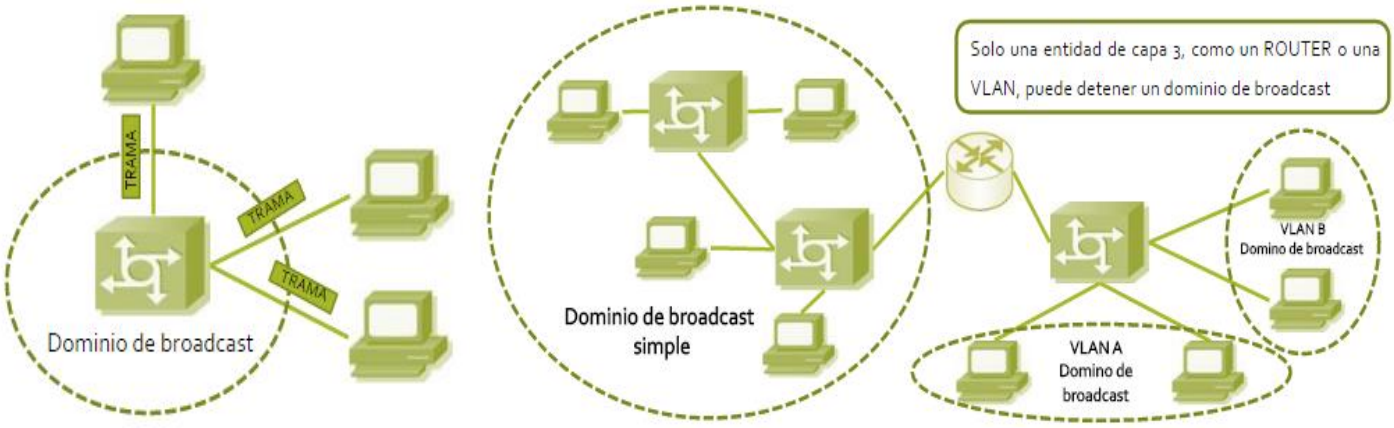


Método de transmisión broadcast[45]

[43] http://forum.huawei.com/enterprise/thread-224239-1.html
[44] http://forum.huawei.com/enterprise/thread-224239-1.html
[45] http://forum.huawei.com/enterprise/thread-224239-1.html

Anexo6.- Dominio de Broadcast y dominio de colisión

Dominio de Broadcast: es el conjunto de todos los dispositivos debajo del router que reciben una trama de Broadcast, solo un router o una VLAN pueden detener un dominio de Broadcast.



Ejemplo de dominio de Broadcast por VLAN[46]

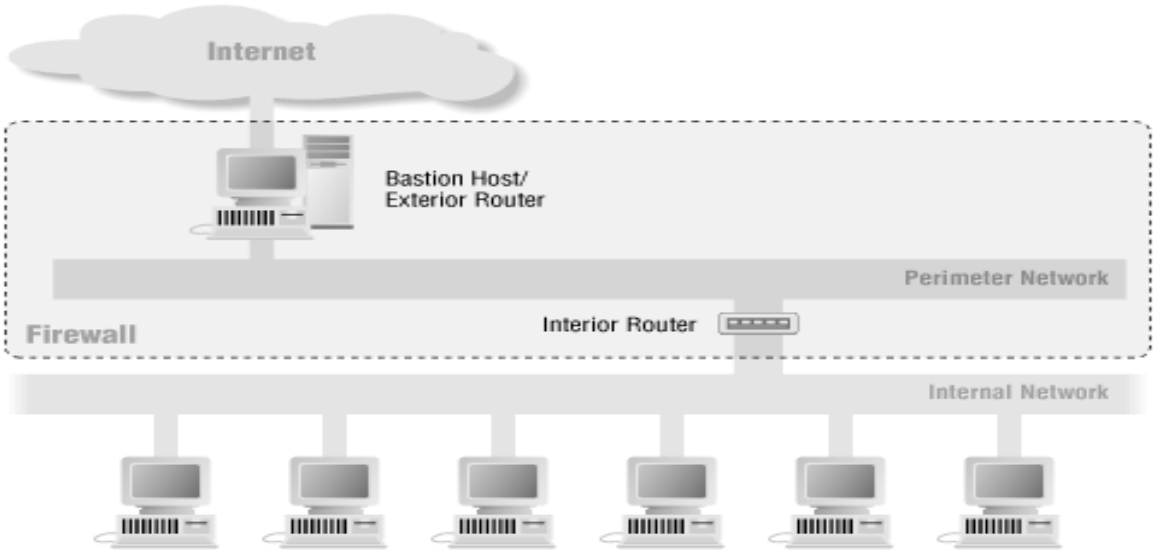
Dominio de colisión: son todos los dispositivos que se encuentran dentro de un mismo segmento de red y será el área que se verá afectada cuando ocurre una colisión, una colisión ocurre cuando dos nodos transmiten tramas de forma simultanea chocando y dañándose cuando se encuentran en el medio físico, se puede considerar a cada host conectado a un puerto de SW como un dominio de colisión individual ya que se mantiene separado del resto de dominios de colisión, los SW y los router's reducen los dominios de colisión ya que segmentan la red.

Dominio de colisión[47]

Anexo7.- Bastión host

También llamado servidor bastion, es un sistema identificado por el administrador del firewall para la recepción y mitigación de posibles ataques externos, actúa como punto de contacto o intermediario entre la red interna y la red externa, filtra el trafico entrante y saliente escondiendo la configuración de la red interna, generalmente proveen un solo servicio e implementa técnicas de hardening desactiva o elimina todas las aplicaciones, servicios, programas, protocolos y puertos innecesarios para el servicio que ofrece, se pueden tener varios bastion host con el fin de aumentar la seguridad en la red interna, esto con el fin de que si la integridad de un bastion host se ve comprometida no afecte más allá del servicio que proveía, el uso de un bastion host se puede extender a web server, DNS server, SMTP server, FTP server, proxy server, VPN server, etc.

[46] http://slideplayer.es/slide/3395931/
[47] http://slideplayer.es/slide/3395931/



Representación de la ubicación del bastión host en la red[48]

Anexo8.- Iptables

Iptables es una herramienta del módulo de Netfilter, se encuentra incluido en el kernel del sistema operativo LINUX, con Netfilter usando iptables podemos filtrar paquetes, traducir direcciones y puertos NAT, mantener registros de logs, permite definir las políticas de filtrado de paquetes y módulos NAT para decir que paquetes aceptar, rechazar, omitir, cuando y como actuar sobre determinados paquetes, iptables emplea:

Cadenas

Son un conjunto de reglas que se aplican a los paquetes cuando cumplen determinadas condiciones

```
iptables [-t table] COMANDO CADENA condición acción [opciones]
    1       2       3      4       5       6       7

iptables -t filter -A INPUT -p tcp --dport 23 -j DROP
    1       2      3  4          5              6
```

Composición básica de una cadena [49]

algunas de estas cadenas pueden ser:

-INPUT: filtra el tráfico entrante, define la acción a realizar cuando un paquete coincide con la regla de entrada de la interfaz**,** se aplica a los paquetes destinados a la propia máquina**.**

-OUTPUT: filtra el tráfico saliente, define la acción a realizar cuando un paquete coincide con la regla de salida de la interfaz, se aplica a los paquetes originados en la propia máquina.

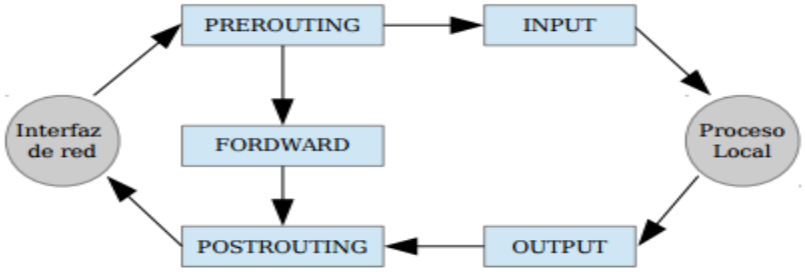
-FORWARD: define la acción a tomar cuando se reenvía un paquete de una interfaz a otra, FORWARD se encuentra PREROUTING y POSTROUTING.

-PREROUTING: Define la primera acción a tomar antes de que el paquete entre en el sistema, permite establecer la comunicación desde la red externa a la red interna.

-POSTROUTING: Determina la acción a tomar justo antes de enviar el paquete a la interfaz destino, permite establecer la comunicación desde la red interna a la red externa.

[48] https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch06_05.htm

[49] https://www.dte.us.es/docencia/etsii/gii-ti/tecnologias-avanzadas-de-la-informacion/Laboratorio-2-Netfilter.pdf



Esquema del procesamiento de Netfilter utilizando la herramienta Iptables[50]

Comandos:
-A : append, agrega una regla a una cadena
-D : delete, borra una regla de una cadena especifica
-R : remplace, remplaza una regla
-I : insert: inserta una regla en lugar de una cadena
-L : list, muestra las reglas que contiene la cadena a la que le pasemos este argumento
-F : flush, borra todas las reglas de una cadena
-Z : zero, pone en cero a todos los contadores de una cadena
-N : new-chain, borra la cadena especificada
-X : delete-chain, borra la cadena especificada
-P : policy, explica al kernel que hacer con los paquetes que no coincidan con ninguna regla
-E : rename-chain, cambia el orden de una cadena

Condiciones:
-p : protocol, la regla se aplica a un protocolo
-s : source, la regla se aplica a una dirección IP de origen
-d : destination, la regla se aplica a una dirección IP destino
-i : in-interface, la regla se aplica a una interfaz origen
-o : out-interface, la regla se aplica a una interfaz destino
-j : indica la acción a realizar con determinado tráfico cuando cumple las reglas de la cadena, que puede ser ACCEPT, DROP, REJECT , etc.
-m : la regla se aplica si hay una coincidencia especifica
-t : especifica la tabla a utilizar, puede ser NAT, FILTER, MANGLE o RAW

Tablas:
FILTER: se usa para el filtrado general de paquetes, es decir, decide que paquetes entran y cuáles no, está compuesta por las cadenas INPUT, OUTPUT y FORWARD, la tabla FILTER es la predeterminada de Netfilter, cuando no se especifica la tabla a utilizar en una cadena se utilizara por defecto la tabla FILTER.
NAT: Se encarga de las traducciones de direcciones, permite alterar la dirección de origen y destino de un paquete, está compuesta por las cadenas PREROUTING, POSTROUTING y OUTPUT, comúnmente NAT se utiliza para SNAT y DNAT.
MANGLE: Se usa para modificar paquetes enteros o algún parámetro del paquete, cuando un paquete cumple ciertas características recibirá un tratamiento específico como puede ser diferenciar tráfico en función de los servicios, etc., está compuesto por las cadenas INPUT, OUTPUT, FORWARD; PREROUTING y POSTROUTING

[50] https://www.dte.us.es/docencia/etsii/gii-ti/tecnologias-avanzadas-de-la-informacion/Laboratorio-2-Netfilter.pdf

RAW: Se usa para configurar excepciones en el seguimiento de paquetes, está compuesto por las cadenas PREROUTING y OUTPUT

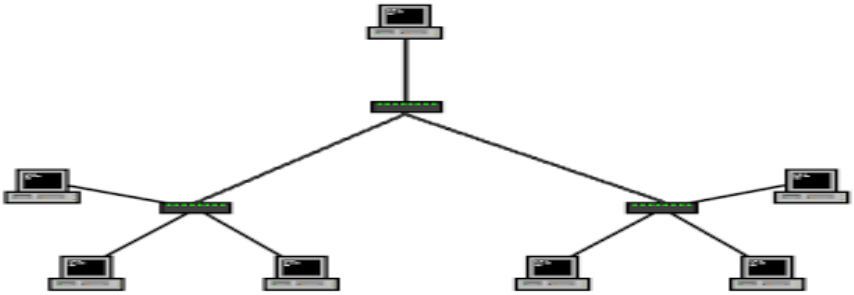
Condiciones de estado:
-state : permite seleccionar paquetes de acuerdo al estado de su conexión, que pueden ser:
ESTABLISHED: el paquete es parte de una conexión existente que manda paquetes en ambas direcciones
NEW: el paquete iniciara una conexión nueva o es asociada a una conexión a la que todavía no se le ha visto paquetes en ambas direcciones
RELATED: el paquete está creando una nueva conexión asociada a otra existente conocida
INVALID: las reglas de la cadena no permiten asociar el paquete a ninguna conexión (con este tipo de paquetes generalmente se usa DROP)

Condiciones TCP/UDP:
-sport : source-port, selecciona o excluye paquetes de un puerto o rango de puertos origen
-dport : destination-port, selecciona o excluye paquetes de un puerto o rango de puertos destino

Reglas de destino del tráfico:
Indica la acción a realizar cuando se cumplan las condiciones establecidas
-ACCEPT: Acepta el paquete
-DROP: Rechaza el paquete, sin avisar al emisor que el paquete fue rechazado
-REJECT: Rechaza el paquete, avisando al emisor que el paquete fue rechazado
-LOG: registra el tráfico
-MASQUERADE [dirección IP]: enmascara la dirección IP origen de forma dinámica, esta acción solo puede ser usada en la tabla NAT en la cadena POSTROUTING
-DNAT --to [dirección IP][:puerto]: enmascara la dirección IP destino, comúnmente usando para el enrutamiento de paquetes, proxy, balanceo de cargas, etc.
-SNAT --to [dirección IP][:puerto]: enmascara la dirección IP origen de forma fija, también se le conoce como IP Masquerading.

Anexo9.- Tipos de topologías de red

La topología de red es el arreglo físico o lógico en el cual los dispositivos o nodos de una red se interconectan entre sí, es decir, es la forma en la cual está diseñada la red, la topología de red puede ser:
Topología física: es la disposición física de los dispositivos o nodos de la red.
Topología lógica: es la trayectoria lógica de una señal por los nodos de una red física.
Existen varias estructuras de topología de red:
Topología de bus
Topología de estrella
Topología de anillo
Topología de malla
Topología de Árbol: es similar a la topología de estrella y la topología de bus, en este tipo de topología existen varios concentradores secundarios los cuales se comunican con un concentrado central, esto permite ramificar y expandir la red tanto como queramos.



Ejemplo de topología en árbol[51]

Pueden utilizarse más de una topología a la vez formando topologías hibridas.

[51] http://1.bp.blogspot.com/_oIVNwpBarhc/SclxtwuyfuI/AAAAAAAAAAU/xeikHDv6Zb8/s320/Netzwerktopologie_Baum.png

GLOSARIO

Dominio de colisión: es el área que se ve afectada cuando ocurre una colisión dentro de un dominio de broadcast
Dominio de broadcast: es el conjunto de todos los dispositivos que reciben tramas de broadcast, solo los dispositivos que trabajen en capa 3 del modelo OSI como un router o una VLAN pueden detener un dominio de broadcast.
Broadcast address: Dirección de difusión, es una dirección IP especificada que se usa para recibir o difundir un mensaje a todos los nodos de una red, se basa en la dirección de la red y la máscara de subred.
Tormenta de broadcast: es un evento no desea donde varios broadcast se envían simultáneamente a todos los segmentos de red, utiliza una cantidad importante del ancho de banda de la red haciendo que la transmisión en la red se alenté, también hace que el TTL de los paquetes se agote y sean descartados.
TTL: Tiempo de vida de un paquete antes de ser desechado
ID: identificador
MAC: control de acceso al medio o Media Access Control, es la subcapa de Ethernet inferior de la capa de direccionamiento físico del modelo OSI, el hardware implementa el MAC generalmente en la NIC, tiene dos funciones principales:
A.-Encapsulación de datos (delimitación de trama, direccionamiento y detección de errores)
B.-Colocar las tramas en los medios y el retiro de las tramas de los medios, es decir, administra el control de acceso al medio
MAC Address: dirección mac, es un identificar único de 48 bits para identificar todos los dispositivos de red como las tarjetas de red Ethernet, Switch, routers, etc.
CSMA/CD: Carrier Sense Multiple Access with Collision Detection o acceso múltiple con escucha de portadora y detección de colisiones, es un protocolo de acceso al medio compartido donde los dispositivos de red escuchan el medio antes de transmitir, determinando si el canal y sus recursos se encuentran disponibles para realizar una transmisión, si detecta una colisión finaliza él envió.
10/100/1000: es la velocidad de transmisión de datos, que puede estar dada en: 10Mb/s Ethernet, 100Mb/s FastEthernet, 1Gb/s GigaEthernet.
Cable UTP: Unshielded Twisted Pair o par trenzado no blindado
Cable FTP: Foiled Twisted Pair o par trenzado con pantalla global
Cable STP: Shielded Twisted Pair o par trenzado blindado
Cable de F.O./f.o.: Fiber Optic o Fibra óptica
µm: micrómetro, es una unidad de longitud equivalente a una milésima parte de un milímetro.
Estándar: Es un conjunto de reglas o normas establecidas que sirven de modelo o referencia.
Protocolo IEEE 802.1Q: es el estándar utilizado en las VLAN's, para mayor información consultar la siguiente URL https://www.ietf.org/meeting/86/tutorials/86-IEEE-8021-Thaler.pdf
Protocolo IEEE 802.2: es el estándar utilizado en la capa de direccionamiento físico del modelo OSI, para mayor información consultar la siguiente URL
http://www.signallake.com/publications/1998802.2LogicalLinkControl.pdf
Protocolo IEEE 802.3: es el estándar utilizado en la capa física del modelo OSI, para mayor información consultar la siguiente URL
http://people.ee.duke.edu/~mbrooke/EE164.02/Spring_2004/group_2/index_files/8023.pdf
Peer to peer (P2P): es una arquitectura de red que permite el intercambio de información entre dispositivos sin necesidad de un servidor central
SSID: Service Set Identifier, es el nombre que identifica a una red inalámbrica.
Roaming: es la capacidad de cambiar de un área de cobertura a otra sin interrupciones en el servicio o perdida en conectividad.

TIA: Telecommunications Industry Association o asociación de la industria de telecomunicaciones, desarrolla normas de cableado, es la principal asociación comercial que desarrolla estándares relacionados con las tecnologías de información y comunicaciones (TIC).
EIA: Electronics Industry Alliance o alianza de industria electrónicas, antes era conocido como Electronics Industry Association, es una organización formada por compañías electrónicas y de tecnologías en los Estados Unidos, su propósito es promover el desarrollo de mercado y la competitividad de la industria.
IEEE: Intitute of Electrical and Electronics Engineers o Intituto de ingeniería eléctrica y electrónica, es la mayor asociación mundial sin fines de lucro formada por profesionales de las tecnologías, se dedicada a la estandarización, desarrollo tecnológico, etc.
ISO: Internacional Organization for Standardization u organización internacional de estandarización, es una organización que promueve y desarrolla estándares a nivel mundial.
ANSI: American National Standards Institute o instituto nacional americano de estandares, es una organización sin ánimos de lucro que supervisa el desarrollo de los estándares para productos, servicios, procesos y sistemas en los Estados Unidos.
NIC: tarjeta de interfaz de red (Network Interfaces Card).
Subred: es una serie de redes contenidas en una red, se pueden dividir en red clase A, B o C.
Mascara de subred: es un patrón de 32 bits (de 1 y 0) que describe que parte de una dirección le pertenece a la subred y cual al host.
Host: también conocido como anfitrión, es un dispositivo que funciona como el punto de inicio y final de las transferencias de datos.
PVID: Puerto VLAN Identificador, cuanto un puerto recibe una trama sin etiquetar utiliza la ID de la VLAN nativa.
Access link: Puerto de acceso, es cualquier puerto de un switch que pertenece a una VLAN
Trunk link: Puerto troncal, es un puerto en un switch que sirve de enlace entre switches para la transmisión de tráfico de varias VLAN.
Trama: Es un paquete de información (bits) ordenada, consta de cabecera, datos y cola, transporta información y permite al receptor extraer esta información.
DNS: Domain Name Service, es un sistema de nomenclatura jerárquica que traduce un nombre de dominio en una dirección IP y vice-versa
Tag: etiqueta, es un identificador, también se puede utilizar el término Taggear que significa etiquetar.
IPsec: Internet Protocol Security, es un protocolo de capa 3 del modelo OSI que puede enviar los datos cifrados para redes IP, permite mejorar la seguridad usando algoritmos de cifrado más complejos y un sistema de autenticación más exhaustivo, soporta cifrados de 56bits y 168bits.
PPTP/MPPE: Point to Point Tunneling Protocol/ Microsoft Point to Point Encryption, es un protocolo capa 3 del modelo OSI desarrollada por varias empresas, PPTP soporta varios protocolos VPN con cifrado de 40bits y 128bits utilizando el protocolo MPPE, PPTP por sí solo no cifra información.
L2TP/IPsec: Layer 2 Tunneling Protocol, es un protocolo capa 2 del modelo OSI capaz de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP, por si solo L2TP no puede cifrar la información.
Man-in-the-middle: hombre en el medio, es cuando un atacante intercepta una comunicación legítima asumiendo el roll de un intermediario y simulando una conexión segura.
tunneling: túnel, es un término utilizado para simbolizar el hecho de que los datos son cifrados desde el momento en que entran a la VPN hasta que salen de ella, siendo incomprensibles para cualquiera que no esté en uno de los extremos de la VPN, como si los datos viajaran a través de un tunel.
Dirección IP: Es un identificador numérico único en una red que se le asigna a un host o interfaz de red.

Protocolo IP: Internet Protocol, es un protocolo de la capa 3 del modelo OSI, o capa 2 del modelo OSI en TCP/IP, el protocolo IP se encarga del transporte de paquetes desde el origen hasta el destino en una comunicación.
Protocolo TCP: Transmision Control Protocol, es un protocolo orientado a las comunicaciones y ofrece una transmisión de datos lenta y confiable, asegurándose de que la transferencia de datos se realice correctamente, usada en correo electrónico, buscadores web, etc.
Protocolo TCP/IP: es el conjunto del protocolo IP y TCP, por medio de este protocolo se logra la transmisión de información entre computadoras pertenecientes a una red, es la base para los servicios más utilizados en internet como transferencia de ficheros, correo electrónico, login remoto, etc.
Protocolo UDP: User Datagram Protocol, es un protocolo destinado a aquellas comunicaciones que ofrece una transmisión rápida y poco confiable, usado en streaming, VoIP, etc.
Protocolo HTTP: HyperText Transfer Protocol, es un protocolo de comunicación en la WWW.
Protocolo FTP: File Transfer Protocol o protocolo de transferencia de archivos, es un protocolo de transferencia de archivos que define la manera en que los datos deben ser transferidos a través de una red TCP/IP.
WWW: World Wide Web o red informática mundial, es un servicio de internet utilizado para búsqueda y acceso a la información de las páginas web.
Protocolo SSH: Secure Shell, es un protocolo que sirve para acceder de manera remota a un host a través de la red y es más segura al cifrar la información.
Protocolo SMTP: Simple Mail Transfer Protocol, es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre host.
RIP: Routing Information Protocol.
OSPF: Open Shortest Path Firts.
EIGRP: Enhanced Interior Gateway Routing Protocol.
Datagrama: Es un fragmento de un paquete de datos.
IRC: Internet Relay Chat, es un protocolo de comunicación en tiempo real basado en texto, permite que dos o más personas que se encuentran en un canal puedan comunicarse entre sí.
FW: Firewall o cortafuegos, actúa de intermediario entre dos redes o un ordenado y una red, examina los paquetes de información que trata de entrar y/o salir y en función de reglas establecidas permite la entrada o salida de los paquetes por medio de hardware (un equipo), software (un programa) o ambas.
Web: es una red informática diseñada para compartir recursos en internet
Log en firewall: Es un registro detallado de actividades en el firewall, como intentos de conexión o control de tráfico.
S.O.: Sistema Operativo, es el software principal o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software.
Patch Panel: panel de conexiones, es un panel físico que recibe todos los cables del cableado de la estructura.
Framework: es un entorno o conjunto de herramientas necesarias para el desarrollo de una actividad especifica
NAT: Network Address Translation o traducción de direcciones de red,
Gateway: puerta de enlace, es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes, traduce la información del protocolo utilizado en una red al protocolo usado en la red destino.
Protocolo IPv4: es el protocolo actual de internet, es un sistema de identificación utilizado para enviar información entre dispositivos, las direcciones IPv4 están basadas en 32bits formado por cuatro octetos (números de 8bits que van desde 0 hasta 256), puede ser IP publica o IP privada dependiendo del tipo de red a la que pertenezca.

Protocolo IPv6: es un protocolo de internet diseñado para mejorar a IPv4, es un sistema de identificación utilizado para enviar información entre dispositivos, las direcciones IPv6 están basadas en 128bits formado por ocho secciones de 16 bits (números de 16 bits que van desde 0 hasta 65,536), puede ser IP fija o IP dinámica en función del modo en que se asignan.

IP publica: son direcciones IP utilizadas en internet que pertenecen a un único host, estas IP's son reconocidas y validas por el IANA
IANA: Internet Assigned Numbers Authority,
IP privada: son direcciones IP reutilizables que se reservan para ser utilizadas en redes locales y se llaman privadas o no enrutables porque no pueden ser utilizadas en internet
Mapea/Mapear: asigna/asignar
Pool: en las TIC's se le denomina pool a un grupo o conjunto de recursos
TIC: Tecnologías de la información y comunicación, engloba las tecnologías de la información y las tecnologías de la comunicación, las TIC's son el estudio, diseño, desarrollo, mantenimiento y gestión de la información por medio de tecnologías y sistemas informáticos, es decir, las TIC's son todas aquellas tecnologías o técnicas que permiten transmitir, recibir, procesar y gestionar la información, las TIC's se pueden dividir en:
redes: telefonía fija, banda ancha, telefonía móvil, redes de televisión, redes en el hogar, etc.
terminales: ordenadores personales, navegador web, televisor, etc.
servicios: correo electrónico, educación, comercio electrónico, etc.
Hardening: Es el proceso por el cual se aumenta la seguridad de un sistema reduciendo las vulnerabilidades, esto se logra eliminando servicios, protocolos y puertos innecesarios en el sistema.
Kernel: es el núcleo de un sistema operativo
Netfilter: es un framework en el kernel de Linux que intercepta y manipula el tráfico de red, su herramienta más conocida es iptables.
Puerto troncal: es una conexión punto a punto que permite interconectar varias VLAN
Backbone: columna vertebral, es el enlace principal de una red
Conmutar: establecer comunicación entre dos o más puntos
Concentrador: centraliza el cableado de varios dispositivos para repetirla por sus diferentes puertos.
Repetidor: retransmite o amplifica una señal.
Token: es un identificador
SW: switch, es un dispositivo que interconecta redes o dispositivos en la capa 2 del modelo OSI

BIBLIOGRAFÍA

https://books.google.com.mx/books?id=Mgvm3AYIT64C&pg=PA150&dq=que+es+una+vlan&hl=es&sa=X&redir_esc=y#v=onepage&q=que%20es%20una%20vlan&f=false
https://books.google.com.mx/books?id=QAxAJEBgUWYC&pg=PA263&dq=que+es+una+vlan&hl=es&sa=X&redir_esc=y#v=onepage&q&f=false
https://books.google.com.mx/books?id=0gpdAgAAQBAJ&pg=PA45&dq=que+es+una+vlan&hl=es&sa=X&redir_esc=y#v=onepage&q=que%20es%20una%20vlan&f=false
https://books.google.com.mx/books?id=oFqEYC9THfEC&pg=PA94&dq=mdi-x&hl=es&sa=X&redir_esc=y#v=onepage&q=mdi-x&f=false
https://books.google.com.mx/books?id=WEfnGbAwM0kC&pg=PA125&dq=que+es+una+vlan&hl=es&sa=X&redir_esc=y#v=onepage&q=que%20es%20una%20vlan&f=false
https://books.google.com.mx/books?id=joMlAU4seLYC&pg=PA263&dq=que+es+una+vlan&hl=es&sa=X&redir_esc=y#v=onepage&q&f=false
https://es.scribd.com/doc/162120756/DIFERENCIAS-ENTRE-CABLE-UTP-CAT6-Y-CABLE-UTP-CAT6A-docx
http://redestelematicas.com/tipos-de-switches/
http://uhu.es/antonio.barragan/content/protocolo-csmacd
https://informaticaesp.wordpress.com/2012/02/11/que-es-una-tarjeta-de-red-y-para-que-sirve/
http://carlosredes23.blogspot.mx/2013/05/vlan_3028.html
https://sites.google.com/site/modulovlan/3-1-presentacion-de-las-vlan/3-1-1-presentacion-de-las-vlan
https://www.ecured.cu/index.php/Ethernet
http://www.c3comunicaciones.es/Documentacion/Alcance%20fo.pdf
http://es.ccm.net/contents/258-vpn-redes-privadas-virtuales
http://es.ccm.net/faq/2757-que-es-un-router
http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Firewall-y-como-funciona.php
http://www.seguridad.unam.mx/descarga.dsc?arch=422
http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
http://www.adslayuda.com/generico-nat.html
http://es.ccm.net/contents/271-nat-conversion-de-direcciones-de-red-habilitacion-de-puertos-y
http://www.mikroways.net/2010/06/06/tipos-de-nat-y-configuracion-en-cisco/
http://www.omnisecu.com/cisco-certified-network-associate-ccna/static-nat-dynamic-nat-and-pat.php
https://www.dte.us.es/docencia/etsii/gii-ti/tecnologias-avanzadas-de-la-informacion/Laboratorio-2-Netfilter.pdf
http://www.redeszone.net/gnu-linux/iptables-configuracion-del-firewall-en-linux-con-iptables/
http://www.eveliux.com/mx/Topologias-de-red.html
http://www.delfirosales.com/2009/06/metodos-de-transmision-unicast.html
http://ecovi.uagro.mx/ccna1/course/module5/5.3.1.2/5.3.1.2.html
https://wiki.ubuntu.com/vlan
https://sites.google.com/site/modulovlan/3-1-presentacion-de-las-vlan/3-1-4-control-de-los-dominios-de-broadcast-con-las-vlan