



UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2017 – MARZO 2018

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

Ingeniería en Sistemas

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

ANALISIS COMPARATIVO DE LOS PROTOCOLOS DE RED IPV4 E IPV6 EN LA RED DE FAFI

EGRESADO:

María Eugenia Portero Pino

TUTOR:

Mgs. Wellington Isaac Maliza Cruz

AÑO 2018

TEMA:

ANALISIS COMPARATIVO DE LOS PROTOCOLOS DE RED IPV4 E IPV6 EN LA RED DE FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA

1. INTRODUCCIÓN

La evaluación institucional de universidades y escuelas politécnicas realizadas por el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES), tiene como objetivo determinar el grado de cumplimiento de los estándares de calidad definidos en el modelo de evaluación vigente. La acreditación es obligatoria y necesaria para que una institución pertenezca al Sistema de Educación Superior Ecuatoriano, por lo que la Facultad de Administración Finanzas, e Informática de la Universidad Técnica de Babahoyo desea brindar, mejorar y optimizar recursos ya que la Facultad solo cuenta con protocolo de red Ipv4.

El siguiente caso de estudio surge por la necesidad de obtener una mejor información en cuanto al número de usuarios que utilizan internet, ya que ha ido creciendo de una manera excesiva y esto hace que el número de direcciones IP sea cada vez menor. Los dispositivos utilizados actualmente para cubrir el problema de escasez de direcciones pronto dejarán de ser funcionales.

Agregado a ello, la meta de lograr conectividad a Internet a través de artefactos distintos de una computadora no es posible realizarla con el protocolo IP en la versión cuatro. Esto se logrará si se cuenta con un protocolo que garantice una cantidad infinita de direcciones.

Por tales razones, el estudio del protocolo IP en su versión seis y su adopción por parte de las organizaciones merece especial atención, ya que permitirá conocer cuáles son los componentes involucrados en la transición, la forma de proceder en la transición y su coexistencia con el protocolo en su cuarta versión para la obtención de los beneficios brindados por ambos protocolos.

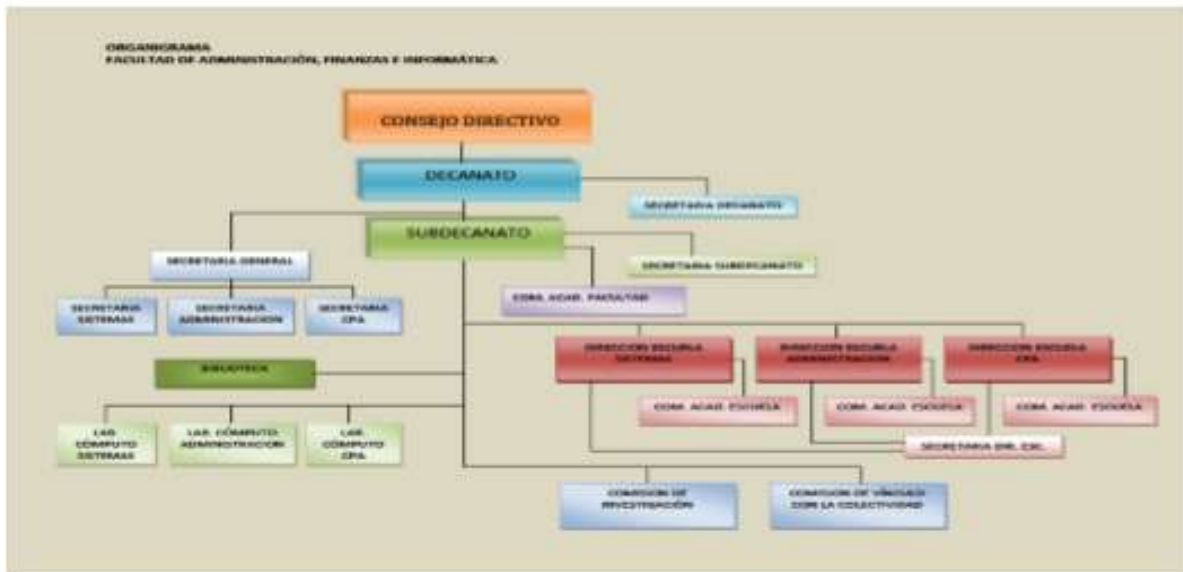
Al conocer la forma de proceder y los diferentes mecanismos de transición, consiste en brindar las soluciones que puede adoptar la Facultad de Administración, Finanzas e Informática en el corto, mediano y largo plazo para permitir la coexistencia de ambos protocolos, y así, poder obtener la mayor cantidad de beneficios de ambos protocolos.

2. DESARROLLO

La Facultad de Administración Finanzas e Informática es una Unidad Académica Superior de la Universidad Técnica de Babahoyo, cuyo gobierno se estructura conforme lo determina el vigente Estatuto Universitario, a fin de que puedan afrontar con total rectitud y eficiencia los retos que imponen el avance y desarrollo de la sociedad moderna. (FAFI-RESEÑA HISTORICA,, s.f.)

A través del Análisis Comparativo de los protocolos de Red Ipv4 e Ipv6 en la Red de la Facultad de Administración, Finanzas e Informática de acuerdo a los lineamientos de los Procesos de datos y telecomunicaciones. La facultad tiene un departamento de la red cableada Ipv4 que brinda el servicio de internet con 233 puntos de red a los diferentes laboratorios, oficinas y aulas donde poseen numerosas extensiones inalámbricas que permiten al personal administrativo, docentes y estudiantes conectarse a los diferentes puntos de red. La metodología que se emplea en el presente estudio de caso es la investigativa.

ORGANIGRAMA DE LA FAFI



FUENTE: (GALARZA, 2017)

Las redes IP usuales se conectan a lugares de grandes distancias y satisfacen las necesidades de conectividad de sus usuarios. Para realizar cada una de estos procedimientos cada paquete tiene que pasar por routers, switches, firewalls y demás elementos los cuales toman decisiones individuales de enrutamiento que hacen difícil la diligencia monopolizada de la red. («ANÁLISIS COMPARATIVO DE PRESTACIONES ENTRE SDN Y REDES CONVENCIONALES.PDF», S. F.) .

Dentro de las características que existen en cuanto a dirección en Ipv4 se compone de una red y una parte sistema principal y la longitud es de 32 bits (4 bytes). En Ipv6 su longitud es de 128 bits (8 grupos de 16 bytes). Al ser direcciones más grandes son más difíciles de representar, ya que en Ipv4 no es demasiado práctico para crear direcciones mucho más grandes. La arquitectura principal es de 64 bits para el número de red y 64 bits para el sistema principal. Es por esto que Ipv6 tiene una arquitectura más complicada que Ipv4.

Si bien el agotamiento de las direcciones de Ipv4 es la razón por lo que se ha disparado todo este cambio, en cuanto Ipv6 es algo más que un espacio de direcciones más amplio ya

que propone para el soporte de movilidad, seguridad y calidad de servicio un alcance de madurez importante.

“Los dispositivos propuestos para el despliegue de Ipv6 implica la convivencia con Ipv4 por un tiempo determinado, y esto presenta como un desafío importante para lograr la transición efectiva, sin perder los servicios ya desplegados en Ipv4, pero a la vez sin desaprovechar las bondades que trae Ipv6". («ANÁLISIS COMPARATIVO DE PRESTACIONES ENTRE SDN Y REDES CONVENCIONALES.PDF», S. F.) .

La dirección IP es una regla numérica que identifica a equipos o dispositivos de una red se usa en redes que utilizan el "idioma" (protocolo) de Internet, ya sea una red privada o la propia Internet. La IP de un dispositivo hace que la red lo distinga de los otros y sea capaz de hacerle llegar datos o recibirlos. **(ABOUT ESPAÑOL, 2016)**

DIRECTRICES DE DIRECCIONAMIENTO

Debemos tener en cuenta algunas instrucciones sobre los números utilizados para el ID de red y el ID de host cuando al establecer una dirección IP se utilizan clases.

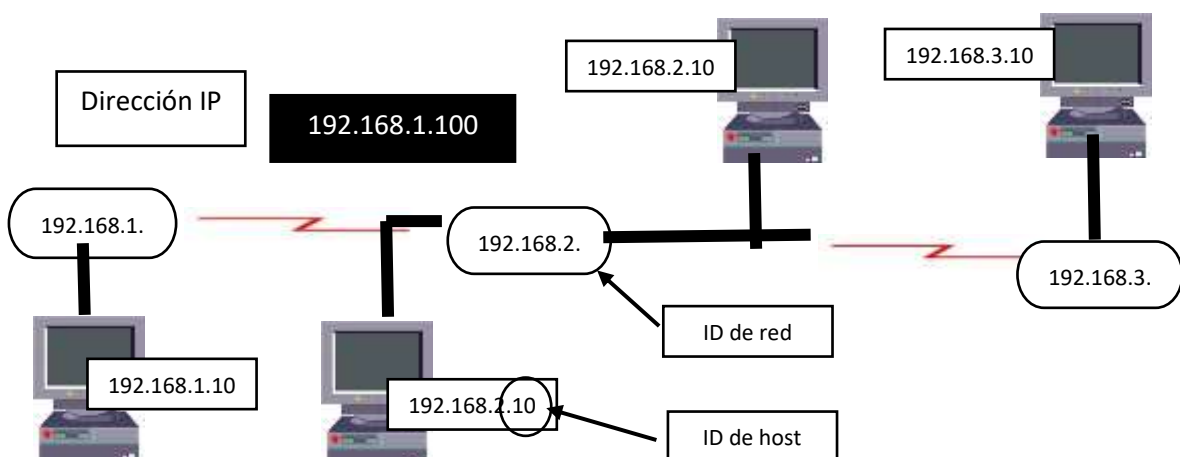
- El primer número del ID de red no puede ser 127. Este número de ID está guardada para pruebas de conexión, como realizar un bucle local.
- El número del ID de host no pueden ser solo 255, ya que esta dirección se utiliza como guía de difusión IP, no puede ser solo ceros, ya que esta dirección es beneficiada para indicar una ID de red y debe ser exclusivo para el ID de red local. **(EDSEL ENRIQUE UREÑA LEON, 2013)**

DIRECCIONAMIENTO DE RED IPV4

Ipv4 hace referencia a la cuarta versión del Protocolo de Internet IP y es un protocolo sin conexión el cual es implementado en redes que hacen uso de permutación de paquetes que al utilizar este protocolo cada día va siendo más limitado ya que requiere varios complementos adicionales para funcionar como el protocolo de mensajes de control de internet y protocolo de resolución de direcciones. (SOLVETIC, 2017)

Para poder comunicarse cada equipo debe tener una dirección IP exclusiva. En el direccionamiento IP en clases, el tamaño y tipo de la red determinara la clase de dirección IP que habitaremos cuando proporcionaremos direcciones IP a los equipos y otros hosts de nuestra red.

La dirección IP es el único identificador que diferencia un equipo de otro en una red y ayuda a localizar donde radica ese equipo. Se necesita una dirección IP para cada equipo y componente de router, que se comuniquen mediante TCP/IP. (ESEL ENRIQUE UREÑA LEON, 2013),



Realizado por: María Eugenia Portero Pino

La dirección IP está formada por: el ID de Host y el ID de red. ID de red que identifica el segmento de red en el que está ubicado el equipo, y el ID de host que registra un equipo, otro dispositivo de una clase. (GARCÍA JESÚS, SERVICIOS DE RED E INTERNET, MOLINILLO)

CLASE	RANGO	MASCARA DE RED
A	1.0.0.0 – 126.255. 255. 255	255.0.0.0
B	128.0.0.0 – 191. 255.255.255	255.255.0.0
C	192.0.0.0 – 223. 255.255.255	255.255.255.0
D	224. 255.255.255 – 239. 255.255.255	-----
E	240.0.0.0 – 255.255.255.255	-----

Realizado por: María Eugenia Portero Pino

(JULIAN CAMILO SOMBREDERO ALFONSO, 2014)

DIRECCIONES IP CLASE A, B, C, D Y E

Para implementar en redes de diferentes tamaños, las direcciones IP se integran de conjuntos llamados clases. Identificado como direccionamiento classful (que no transmiten la mascara de subred en sus actualizaciones). La dirección IP consta de 32 bits dividido en parte de red y host. La secuencia de bits inicial instauro su clase (Cisco. (s.f.)).

CLASE A	RED	HOST		
Octeto	1	2	3	4
CLASE B	RED		HOST	
Octeto	1	2	3	4
CLASE C	RED			HOST
Octeto	1	2	3	4

CLASE D	HOST			
Octeto	1	2	3	4

Realizado por: María Eugenia Portero Pino

Direccionamiento de red Ipv6

IPv6, es el protocolo más reciente de IP se posiciona como la modernización de Ipv4 en términos de capacidad, cubrimiento y seguridad, utiliza el sistema hexadecimal, están basadas en 128 bits y está combinado por ocho octetos de un tamaño de 16 bits, separadas por dos puntos seguidos (:). **(SOLVETIC, 2017)**

Ipv6 es la nueva generación del protocolo de comunicaciones de internet y gran parte de los sistemas operativos actuales están ya preparados para utilizarlo. En esta entrada se explican de forma sencilla las características más importantes de las direcciones Ipv6 y se muestra una conexión elemental entre dos equipos a través de Ipv6. **(GARCÍA JESÚS, SERVICIOS DE RED E INTERNET, MOLINILLO)**

A nivel general, podemos clasificar las direcciones IPv6 en tres grandes categorías:

- Las direcciones **Unicast**, al igual que en IPv4, son las más usuales y empleadas. Estas son concedidas a una interface o nodo permitiendo la comunicación directa entre dos nodos de la red. Esta técnica de comunicación es conocida como uno a uno (one-to-one).
- Las direcciones **Multicast** permiten identificar múltiples interfaces o nodos en una red. Con este tipo de direcciones podemos comunicarnos con varios nodos de manera sincronizada. Esta técnica de comunicación es conocida como uno a mucho (one-to-many).
- Las direcciones **Anycast** son un nuevo tipo de dirección en IPv6. Una dirección Anycast establece diversas interfaces, sin embargo, mientras que los paquetes de Multicast son

aceptados por varios equipos, los paquetes Anycast sólo se entregan a una interfaz o nodo.
(CISCO CCNA, 2013)

En informática y telecomunicación, un protocolo de comunicaciones es un conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos

El protocolo define, entre otros:

- El formato y orden de los mensajes a intercambiar.
- Las acciones a realizar en cada caso.

(MÓDULO PROFESIONAL DE SERVICIOS DE RED E INTERNET (IESSANJUANBOSCO, 2016)).

La transición a IPv6 no será un proceso inmediato ni tan simple como pulsar un botón que conmute al nuevo protocolo, la idea es que convivan ambos protocolos durante algunos años y que la implantación de IPv6 sea gradual. Para esto se han desarrollado mecanismos que permitirán la coexistencia y migración progresiva tanto de las redes como de los equipos de usuario. Estos mecanismos de transición son los siguientes:

Doble pila.- Esta solución implementa las pilas de ambos protocolos, IPv4 e IPv6, en cada nodo de la red. Cada nodo con doble pila en la red tendrá dos direcciones de red, una IPv4 y otra IPv6. Este procedimiento es fácil de desplegar y está ampliamente soportado. Sin embargo, tiene la desventaja de que la topología de la red requiere dos tablas de encaminamiento y dos procesos de enrutamiento.

Túneles.- Aquí la conexión se logra encapsulando los paquetes IPv6 en paquetes IPv4. De esta manera, se pueden enviar paquetes IPv6 sobre una infraestructura IPv4. Hay muchas tecnologías de túneles disponibles, éstas difieren en el método que usan los nodos encapsuladores para determinar la dirección a la salida del túnel (el destino).

Traducción.- Este método es necesario cuando un nodo que solo soporta IPv4 intenta comunicar con un nodo que únicamente soporta IPv6. Se traducen las cabeceras de los paquetes entre IPv4 e IPv6 (sólo los campos comunes). Una de las técnicas usadas es TRT (Transport Relay Translator) que traduce a nivel de la capa de transporte (donde se realiza la transferencia de datos libre de errores entre emisor y receptor). Se podrían migrar fácilmente al uso de pilas duales, y la mayoría de los sistemas operativos admiten IPv6 en la actualidad.

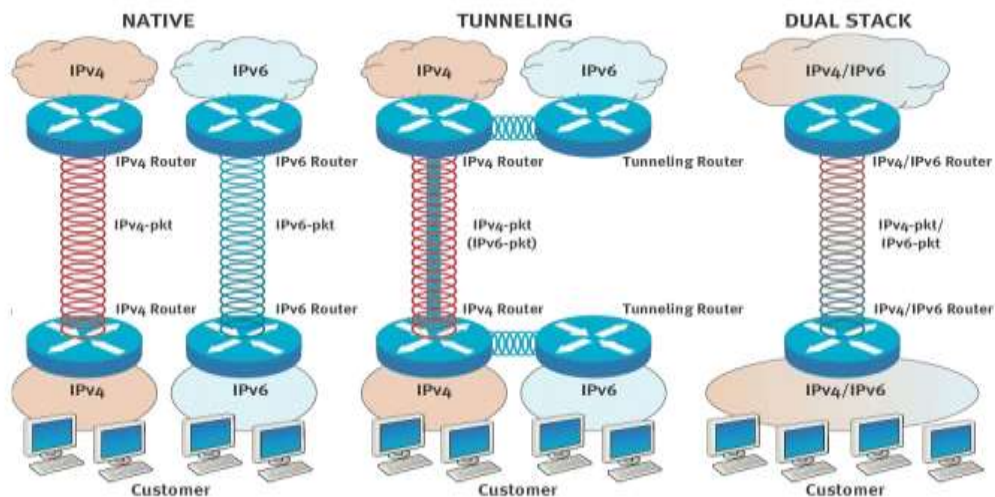
La principal desventaja de este método es una disminución del rendimiento de los equipos de red, ya que tienen que mantener tablas de encaminamiento y rutas independientes para cada uno de los protocolos. **(Ávila Mejía O, 2011)**

Las mejores prácticas de seguridad en IPV6 busca definir una estrategia de seguridad adecuada en IPV6, a fin de minimizar las amenazas que atenten contra la confidencialidad, la integridad y la disponibilidad de la información de la empresa; así como prevenir los posibles ataques a la misma. A continuación se mencionan tres de las mejores prácticas de seguridad:

VLAN: Son la manera más sencilla de brindar seguridad en capa 2, ya que permiten dividir la red en segmentos más pequeños independientes lógicamente.

Listas de Control de Acceso: Son filtros que permiten o deniegan el acceso a los recursos de la red. El filtro puede definirse en base a: las direcciones IP, los protocolos de capa superior y los puertos. IPv6 solo tiene soporte para las ACL (Access Control List) extendidas nombradas.

Acceso Remoto Seguro: SSH (Secure Shell) permite el acceso remoto a dispositivos a través de la red, haciendo uso de conexiones seguras, implementando autenticación y proporcionando terminales con sesiones cifradas. (AGUIRRE L, JULIO 2013)



Los diferentes procedimientos para alargar la vida de IPv4 se han instaurado, como NAT (Traducción de direcciones Privadas a Públicas), pero debido a los problemas en la conexión que presentan, la transición a IPv6 llegó.

IPv4 tiene una cantidad aproximada de 4300 millones de direcciones pero IPv6 tiene alrededor de 340 sextillones de direcciones, es decir, casi la misma cantidad que el total de direcciones IPv4 para cada ser humano sobre la Tierra! además en el momento de la creación de IPv6 se eliminaron ciertos defectos en la estructura de las direcciones IPv4 y se incluyeron mejoras tanto en seguridad como eficiencia. (CISCO SUPPORT COMMUNITY, 2016)

Descripción	IPv4	IPv6
Dirección	<p>32 bits de longitud (4 bytes). La dirección se compone de una red y una parte de sistema principal, que dependen de la clase de dirección. Existen varias clases de dirección: A, B, C, D o E, según los bits iniciales. El número total de direcciones IPv4 es 4 294 967 296.</p> <p>El formato de texto de las direcciones IPv4 es $nnn.nnn.nnn.nnn$, donde $0 \leq nnn \leq 255$, y cada n es un dígito decimal. Los ceros iniciales pueden omitirse. El número máximo de caracteres de impresión es 15, sin contar una máscara.</p>	<p>128 bits de longitud (16 bytes). La arquitectura básica es 64 bits para el número de red y 64 bits para el número de sistema principal. Con frecuencia, la parte de sistema principal de una dirección IPv6 (o parte de la misma) se obtendrá de una dirección MAC u otro identificador de interfaz.</p> <p>Según el prefijo de subred, IPv6 tiene una arquitectura más complicada que IPv4. El número de direcciones IPv6 es de 1028 (79 228 162 514 264 337 593 543 950 336) veces mayor que el número de direcciones IPv4. El formato de texto de la dirección IPv6 es $2001:0db8:1234:0000:0000:0000:0000/48$, donde cada grupo es un dígito hexadecimal que representa 4 bits. Los ceros iniciales pueden omitirse. Pueden utilizarse dos signos de dos puntos (::) una vez en el formato de texto de una dirección para designar cualquier número de 0 bits. Por ejemplo, $::ffff:10.120.78.40$ es una dirección IPv6 correlacionada con IPv4.</p>
Asignación de direcciones	<p>Originariamente, las direcciones se asignaban por clase de red. A medida que se agota el espacio de direcciones, se efectúan asignaciones más pequeñas mediante CIDR (direccionamiento interdominio sin clase). La asignación no está equilibrada entre instituciones y naciones.</p>	<p>La asignación está en las primeras fases. El grupo IETF (Internet Engineering Task Force) y el grupo IAB (Internet Architecture Board) han recomendado asignar una longitud de prefijo de subred /48 a prácticamente cada organización, domicilio privado o entidad. Ello dejará 16 bits para división en subredes para la organización. El espacio de direcciones es suficientemente extenso para asignar a cada persona del mundo su propia longitud de prefijo de subred /48.</p>
Tiempo de vida máximo de la dirección	<p>Por regla general, no se trata de un concepto pertinente para direcciones IPv4, excepto en las direcciones asignadas mediante DHCP.</p>	<p>Las direcciones IPv6 tienen dos tiempos de vida: el preferido y el válido. El tiempo de vida preferido siempre es \leq válido.</p> <p>Si ha expirado el tiempo de vida preferido, la dirección no debe utilizarse como dirección IP de origen para las conexiones nuevas si existe una dirección preferida igualmente buena. Si ha expirado el tiempo de vida válido, la dirección no se utilizará (reconocerá) como dirección IP de destino válida para paquetes entrantes ni se utilizará como dirección IP de origen.</p> <p>Algunas direcciones IPv6 tienen, por definición, tiempos de vida preferidos y válidos infinitos, como la de enlace local.</p>
Máscara de dirección	<p>Se utiliza para designar la red desde la parte del sistema principal.</p>	<p>No se utiliza.</p>
Prefijo de dirección	<p>Algunas veces se utiliza para designar la red desde la parte del sistema principal. Puede escribirse como sufijo /nn en el formato de presentación de la dirección.</p>	<p>Se utiliza para designar el prefijo de subred en una dirección. Se escribe como sufijo /nnn (hasta 3 dígitos decimales, $0 \leq nnn \leq 128$) tras el formato de impresión. Por ejemplo: $fe80::982:2a5c/10$, donde los primeros 10 bits engloban el prefijo de subred.</p>
ARP (Protocolo de Resolución de Dirección)	<p>IPv4 utiliza el ARP para encontrar una dirección física, como la dirección MAC o de enlace, asociada con una dirección IPv4.</p>	<p>IPv6 incrusta estas funciones dentro del propio IP como parte de los algoritmos para autoconfiguración sin estado y descubrimiento de vecino, utilizando ICMPv6 (Internet Control Message Protocol version 6). Por lo tanto, no hay nada igual a ARP6.</p>

Ámbito de la dirección	Este concepto no es válido para las direcciones de difusión simple. Existen rangos de direcciones privadas designados y bucles de retorno. Por lo demás, se presupone que las direcciones son globales.	En IPv6 , el ámbito de la dirección forma parte de la arquitectura. Las direcciones de difusión simple tienen dos ámbitos definidos (de enlace local y global), mientras que las direcciones de difusión múltiple tienen 14 ámbitos. La selección de direcciones por omisión para el origen y para el destino tiene en cuenta el ámbito. Una zona de ámbito es una instancia de un ámbito en una red específica. Como consecuencia, las direcciones IPv6 a veces deben entrarse o asociarse con un ID de zona. La sintaxis es %zid donde zid es un número (normalmente pequeño) o un nombre. El ID de zona se escribe después de la dirección y antes del prefijo. Por ejemplo, 2ba::1:2:14e:9a9b:c%3/48.
Tipos de dirección	Las direcciones IPv4 se agrupan en tres tipos básicos de categorías: dirección de difusión única, dirección de difusión múltiple y dirección de difusión.	Las direcciones IPv6 se agrupan en tres tipos básicos de categorías: dirección de difusión única, dirección de difusión múltiple y dirección de difusión indiferente.
ARPING	ARPING es una herramienta de TCP/IP para probar si es posible acceder a sistemas en la LAN local.	Hay un soporte parecido para IPv6 disponible con la herramienta NDPING.
Rastreo de comunicaciones	Un rastreo de comunicaciones es una herramienta para recoger un rastreo detallado de los paquetes TCP/IP (y otros) que entran y salen del sistema.	Se da el mismo soporte a IPv6 .
Configuración	Debe configurar un sistema recién instalado para que pueda comunicarse con otros sistemas; es decir, deben asignarse rutas y direcciones IP.	La configuración es opcional, según las funciones requeridas. IPv6 puede utilizarse con cualquier adaptador Ethernet y puede ejecutarse a través de la interfaz de bucle de retorno. Las interfaces IPv6 pueden configurarse automáticamente utilizando la autoconfiguración sin estado de IPv6 . También se puede configurar manualmente la interfaz IPv6 . Por lo tanto, el sistema podrá comunicarse con otros sistemas IPv6 locales y remotos, según el tipo de red o según si existe un direccionador IPv6 .
DNS (sistema de nombres de dominio)	Las aplicaciones aceptan nombres de sistema principal y utilizan DNS para obtener una dirección IP, utilizando la API de socket gethostbyname(). Las aplicaciones también aceptan direcciones IP y luego utilizan DNS para obtener nombres de sistema principal con gethostbyaddr(). Para IPv4, el dominio para búsquedas inversas es in-addr.arpa.	Se da el mismo soporte a IPv6 con el tipo de registro AAAA (A cuádruple) y la búsqueda inversa (IP-a-nombre). Una aplicación puede aceptar (o no) direcciones IPv6 de DNS y seguidamente utilizar (o no) IPv6 para la comunicación. La API de socket gethostbyname() sólo soporta IPv4 . Para IPv6 , se utiliza una nueva API getaddrinfo() para obtener (a elección de la aplicación) sólo direcciones IPv6 o direcciones IPv4 e IPv6 . Para IPv6 , el dominio que se utiliza para las búsquedas inversas es ip6.arpa y, si no se encuentran, se utiliza ip6.int.
DHCP (Protocolo de Configuración Dinámica de Sistemas Principales)	El protocolo DHCP se utiliza para obtener dinámicamente una dirección IP y más información de configuración. IBM y soporta un servidor DHCP para IPv4 .	La implementación IBM y de DHCP no da soporte a IPv6 . Sin embargo, puede utilizarse la implementación del servidor DHCP ISC.

FTP (Protocolo de Transferencia de Archivos)	FTP le permite enviar y recibir archivos a través de redes.	Se da el mismo soporte a IPv6 .
Fragmentos	Cuando un paquete es demasiado grande para el siguiente enlace por el que debe viajar, puede ser fragmentado por el remitente (sistema principal o direccionador).	Para IPv6 , la fragmentación sólo puede producirse en el nodo de origen y el re-ensamblado sólo se efectúa en el nodo de destino. Se utiliza la cabecera de extensión de fragmentación.
Tabla de sistemas principales	Tabla configurable que asocia una dirección de Internet con un nombre de sistema principal (por ejemplo, 127.0.0.1 para un bucle inverso). El resolvidor de nombres de sockets utiliza esta tabla, bien sea antes de una búsqueda de DNS o cuando ha fallado una búsqueda de DNS (según la prioridad de búsqueda del nombre de sistema principal).	Se da el mismo soporte a IPv6 .
Soporte de IBM Navigator for i	IBM Navigator for i proporciona una solución de configuración completa para TCP/IP.	Se da el mismo soporte a IPv6 .
Interfaz	La entidad conceptual o lógica que utiliza TCP/IP para enviar y recibir paquetes y siempre asociada íntimamente con una dirección IPv4 , si no denominada con una dirección IPv4 . También se denomina interfaz lógica. Las interfaces IPv4 pueden iniciarse y detenerse independientemente entre sí e independientemente de TCP/IP utilizando los mandatos STRTCPIFC y ENDTCPIFC y utilizando IBM Navigator for i.	Se da el mismo soporte a IPv6 .
ICMP (Internet Control Message Protocol)	IPv4 lo utiliza para comunicar información de red.	Para IPv6 , se utiliza de un modo similar; sin embargo, ICMPv6 (Protocolo de mensajes de control de Internet, versión 6) proporciona algunos atributos nuevos. Siguen existiendo los tipos de error básicos, como "no puede alcanzarse el destino", "petición y respuesta de eco". Se añaden tipos y códigos nuevos para dar soporte al descubrimiento de vecino y funciones relacionadas.
IGMP (Internet Group Management Protocol)	Los direccionadores IPv4 utilizan IGMP para buscar sistemas principales que aceptan tráfico para un determinado grupo de difusión múltiple, y los sistemas principales IPv4 utilizan IGMP para informar a los direccionadores IPv4 sobre la existencia de escuchadores de grupo de difusión múltiple (en el sistema principal).	El protocolo MLD para IPv6 (Descubrimiento de escucha de difusión múltiple) sustituye a IGMP. MLD, esencialmente, es similar a IGMP para IPv4, pero utiliza ICMPv6 añadiendo unos valores de tipo ICMPv6 específicos de MLD.
Cabecera IP	Longitud variable de 20-60 bytes, según las opciones IP existentes.	Longitud fija de 40 bytes. No existen opciones de cabecera IP. En general, la cabecera IPv6 es más sencilla que la cabecera IPv4 .
	Varias opciones que pueden acompañar a una cabecera IP	La cabecera IPv6 no tiene opciones. Por el contrario, IPv6 añade cabeceras

Opciones de cabecera IP	(antes de cualquier cabecera de transporte).	adicionales de extensión (opcionales). Las cabeceras de extensión son AH y ESP (inalteradas desde IPv4), salto-a-salto, direccionamiento, fragmento y destino. Actualmente, IPv6 da soporte a algunas cabeceras de extensión.
Byte de protocolo de cabecera IP	Código de protocolo de la capa de transporte o carga útil de paquete (por ejemplo, 'Protocolo de Mensajes de Control de Internet' o ICMP).	El tipo de cabecera que sigue inmediatamente a la cabecera IPv6 . Utiliza los mismos valores que el campo de protocolo IPv4 . Aunque el efecto arquitectónico es permitir un rango definido actualmente de cabeceras siguientes, y se amplía fácilmente. La cabecera siguiente será una cabecera de transporte, una cabecera de extensión o ICMPv6.
Byte tipo de servicio de cabecera IP	Utilizado por QoS y servicios diferenciados para designar una clase de tráfico.	Utiliza códigos diferentes para designar una clase de tráfico IPv6 . Actualmente, IPv6 no da soporte a TOS.
Conexión LAN	La interfaz IP utiliza la conexión de LAN para acceder a la red física. Existen muchos tipos diferentes; por ejemplo Ethernet. También se conoce como la interfaz, enlace o línea física.	IPv6 puede utilizarse con cualquier adaptador Ethernet y también se soporta a través de Ethernet virtual entre particiones lógicas.
L2TP (Layer Two Tunnel Protocol)	L2TP puede considerarse un PPP virtual, y funciona a través de todos los tipos de línea a los que se da soporte.	Se da el mismo soporte a IPv6 .
Dirección de bucle de retorno	Una dirección de bucle de retorno es una interfaz con una dirección 127.*.* (normalmente 127.0.0.1) que un nodo sólo puede utilizar para enviarse paquetes a sí mismo. La interfaz física (descripción de línea) se denomina *LOOPBACK.	El concepto es el mismo que en IPv4 . La dirección de bucle de retorno individual es 0000:0000:0000:0000:0000:0000:0000:0001 o ::1 (versión abreviada). La interfaz física virtual se denomina *LOOPBACK.
MTU (Unidad máxima de transmisión)	La unidad máxima de transmisión de un enlace es el número máximo de bytes que soporta un tipo de enlace determinado, como una Ethernet o un módem. Para IPv4 , 576 es el mínimo habitual.	IPv6 tiene un límite inferior en MTU de 1280 bytes. Es decir, IPv6 no fragmenta los paquetes por debajo de este límite. Para enviar IPv6 a través de un enlace con una MTU de menos de 1280 bytes, la capa de enlace debe fragmentar y desfragmentar con transparencia los paquetes IPv6 .
NDPING	Hay un soporte parecido para IPv4 disponible con la herramienta ARPING.	NDPING es una herramienta TCP/IP para probar si es posible acceder a sistemas vecinos en interfaces de IPv6 .
NETSTAT	Netstat es una herramienta que se usa para ver el estado de las conexiones, interfaces o rutas TCP/IP. Disponible utilizando IBM Navigator for i y la interfaz basada en caracteres.	Se da el mismo soporte a IPv6 .
NAT (Conversión de direcciones de red)	Funciones básicas de cortafuegos integradas en TCP/IP, configuradas con IBM Navigator for i.	Actualmente, NAT no da soporte a IPv6 . Por regla general, IPv6 no requiere NAT. El mayor espacio de direcciones de IPv6 soluciona el problema de escasez de direcciones y permite una remuneración más sencilla.
Tabla de red	En IBM Navigator for i, una tabla configurable que asocia un nombre de red con una dirección IP sin máscara. Por ejemplo, la red de sistema principal 14 y la dirección IP 1.2.3.4.	Actualmente, no se efectúan cambios en esta tabla para IPv6 .
Petición de información de nodo	No existe.	Una herramienta de red simple y cómoda que debe funcionar como ping, pero con contenido: un nodo IPv6 puede consultar a otro nodo IPv6 el nombre DNS del destino, la dirección de difusión simple IPv6 , o la dirección IPv4 . Actualmente, no se

		soporta.
OSPF (Open Shortest Path First)	OSPF es un protocolo de direccionador que se utiliza, preferentemente a RIP, en redes de sistema autónomas y amplias.	Se da el mismo soporte a IPv6 .
Filtrado de paquetes	El filtrado de paquetes es un conjunto de funciones básicas de cortafuegos integradas en TCP/IP. Se configura utilizando IBM Navigator for i.	El filtrado de paquetes no da soporte a IPv6.
Reenvío de paquetes	La pila TCP/IP de IBM i puede configurarse para reenviar los paquetes IP que recibe para direcciones IP no locales. Normalmente, la interfaz de entrada y la interfaz de salida se conectan a LAN diferentes.	El reenvío de paquetes da soporte de forma limitada a IPv6. La pila TCP/IP de IBM i no da soporte al descubrimiento de vecinos como direccionador.
PING	PING es una herramienta básica de TCP/IP para comprobar si puede accederse a un elemento. Disponible utilizando IBM Navigator for i y la interfaz basada en caracteres.	Se da el mismo soporte a IPv6 .
PPP (Protocolo de Punto a Punto)	PPP da soporte a interfaces de marcación a través de varios tipos de líneas y módem.	Se da el mismo soporte a IPv6 .
Restricciones de puerto	IBM Navigator for i permite a un cliente configurar el número de puertos seleccionados para TCP o protocolo de datagramas de usuario (UDP), de forma que sólo están disponibles para un perfil específico.	Las restricciones de puerto para IPv6 son idénticas a las que están disponibles en IPv4 .
Puertos	TCP y UDP tienen espacios de puerto separados, identificados mediante números de puerto en el rango 1-65535.	Para IPv6 , los puertos funcionan igual que para IPv4 . Puesto que se encuentran en una nueva familia de direcciones, ahora existen cuatro espacios de puerto separados. Por ejemplo, existen dos espacios de puerto TCP 80 a los que puede enlazarse una aplicación, uno en AF_INET y uno en AF_INET6.
Direcciones privadas y públicas	Todas las direcciones IPv4 son públicas, excepto tres intervalos de direcciones que IETF RFC 1918 ha designado como privados: 10.*.* (10/8), 172.16.0.0a 172.31.255.255 (172.16/12), y 192.168.*.* (192.168/16). Los dominios de direcciones privados normalmente se utilizan en organizaciones. Las direcciones privadas no pueden direccionarse a través de Internet.	IPv6 tiene un concepto similar, pero con diferencias importantes. Las direcciones son públicas o temporales (anteriormente denominadas anónimas). Véase RFC 3041. A diferencia de las direcciones privadas de IPv4 , las direcciones temporales pueden direccionarse globalmente. La motivación también es diferente; las direcciones temporales de IPv6 pretenden proteger la identidad de un cliente cuando establece una comunicación (asuntos de privacidad). Las direcciones temporales tienen un tiempo de vida limitado, y no contienen un identificador de interfaz que sea una dirección de enlace (MAC). Generalmente no pueden distinguirse de las direcciones públicas. IPv6 tiene el concepto de ámbito de direcciones limitado utilizando sus designaciones de ámbito diseñado.
Tabla de protocolos	En IBM Navigator for i, una tabla de protocolos es una tabla configurable que asocia un nombre de protocolo con su número de protocolo asignado; por ejemplo, UDP, 17. El sistema se envía con un número pequeño de entradas: IP,	La tabla puede utilizarse con IPv6 sin cambios.

	TCP, UDP, ICMP.	
QoS (Calidad de servicio)	La calidad de servicio le permite solicitar la prioridad de paquetes y la anchura de banda para las aplicaciones TCP/IP.	Se da el mismo soporte a IPv6 .
Cambio de numeración	El cambio de numeración se efectúa mediante una nueva configuración manual, con la posible excepción de DHCP. Generalmente, para una ubicación u organización, el cambio de numeración es un proceso difícil y problemático que debe evitarse siempre que sea posible.	El cambio de numeración es un elemento arquitectónico importante de IPv6 , y es en gran parte automático, especialmente en el prefijo /48.
Ruta	Lógicamente, se trata de una correlación de un conjunto de direcciones IP (podría contener sólo una) a una interfaz física y una sola dirección IP de salto siguiente. Los paquetes IP cuya dirección de destino se define como parte del conjunto se reenvían al salto siguiente utilizando la línea. Las rutas IPv4 se asocian con una interfaz IPv4 , por consiguiente, una dirección IPv4 . La ruta por omisión es *DFROUTE.	Conceptualmente, es similar a IPv4 . Una diferencia importante: las rutas IPv6 se asocian (vinculan) con una interfaz física (un enlace, como por ejemplo ETH03), y no con una interfaz. Un motivo por el que una ruta está asociada con una interfaz física es que la selección de la dirección de origen funciona de un modo distinto para IPv6 y para IPv4 . Consulte la sección Selección de dirección de origen.
RIP2 (protocolo de información de direccionamiento)	RIP es un protocolo de direccionamiento al que da soporte el daemon direccionado.	Actualmente, RIP no da soporte a IPv6 .
Tabla de servicios	En IBM i, se trata de una tabla configurable que asocia un nombre de servicio con un puerto y protocolo; por ejemplo, FPT de nombre de servicio, puerto 21, TCP y protocolo de datagramas de usuario (UDP). En la tabla de servicios aparece un número elevado de servicios muy conocidos. Muchas aplicaciones utilizan esta tabla para determinar qué puerto utilizar.	Para IPv6 , no se efectúa ningún cambio en esta tabla.
SNMP (Simple Network Management Protocol)	SNMP es un protocolo para la administración de sistemas.	Se da el mismo soporte a IPv6 .
API de sockets	Estas API son la forma en que las aplicaciones utilizan TCP/IP. Las aplicaciones que no necesitan IPv6 no se ven afectadas por los cambios de sockets para dar soporte a IPv6 .	IPv6 mejora los sockets de forma que ahora las aplicaciones pueden utilizar IPv6, con una familia de direcciones nueva: AF_INET6. Las mejoras han sido diseñadas de forma que las aplicaciones IPv4 existentes no se ven afectadas de ningún modo por IPv6 y los cambios de API. Se da cabida a las aplicaciones que quieren dar soporte al tráfico IPv4 e IPv6 concurrente, o sólo al tráfico IPv6 , utilizando direcciones IPv6 correlacionadas con IPv4 con el formato::ffff:a.b.c.d, donde a.b.c.d es la dirección IPv4 del cliente. Las nuevas API también incluyen soporte para la conversión de direcciones IPv6 de texto a binario y de binario a texto.

Selección de dirección de origen	Una aplicación puede designar un IP de origen (normalmente, mediante sockets bind()). Si se enlaza con INADDR_ANY, se selecciona un IP de origen basándose en la ruta.	Al igual que con IPv4, una aplicación puede designar una dirección IPv6 de origen utilizando bind(). Del mismo modo, puede dejar que el sistema seleccione una dirección de origen IPv6 utilizando in6addr_any. Sin embargo, puesto que las líneas IPv6 tienen muchas direcciones IPv6, el método interno de selección de un IP de origen es diferente.
Inicio y detención	Utilice el mandato STRTCP o ENDTCP para iniciar o detener IPv4 . Cuando ejecuta el mandato STRTCP para iniciar TCP/IP, siempre se inicia IPv4 .	Utilice el parámetro STRIP6 del mandato STRTCP o ENDTCP para iniciar o detener IPv6 . Es posible que no se inicie IPv6 cuando se inicia TCP/IP. IPv6 se puede iniciar de forma independiente más tarde. Las interfaces IPv6 se inician automáticamente cuando el parámetro AUTOSTART se establece con el valor *YES (el valor por omisión). IPv6 no puede utilizarse ni configurarse sin IPv4 . La interfaz de bucle de retorno IPv6::1 , se define y activa automáticamente cuando se inicie IPv6 .
Telnet	Telnet le permite iniciar la sesión y utilizar un ordenador remoto como si estuviera conectado al mismo directamente.	Se da el mismo soporte a IPv6 .
Rastrear ruta	La herramienta rastrear ruta es una herramienta básica de TCP/IP para efectuar determinaciones de ruta. Disponible utilizando IBM Navigator for i y la interfaz basada en caracteres.	Se da el mismo soporte a IPv6 .
Capas de transporte	TCP, UDP, RAW.	Existen los mismos transportes en IPv6 .
Dirección sin especificar	Aparentemente, no definida como tal. La programación de sockets utiliza 0.0.0.0 como INADDR_ANY.	Se define como ::128 (128 0 bits). Se utiliza como el IP de origen en algunos paquetes de descubrimiento de vecino, y otros contextos diferentes, como sockets. La programación de sockets utiliza ::128 como in6addr_any.
VPN (Redes privadas virtuales)	La herramienta Redes privadas virtuales (con IPsec) le permite extender una red privada segura a lo largo de una red pública existente.	Se da el mismo soporte a IPv6 .

(IBM.COM & SUPPORT, s.f.)

CONCLUSION

El caso de estudio me ha permitido establecer el grado de confidencialidad, en el cual se puede establecer un empate entre los dos protocolos y también lo es la manera en que la tecnología de seguridad implementada, en este caso la VPN, lo que nos permite una manera correcta de contrarrestar todo tipo de ataque en ambos protocolos.

En cuanto a la prueba de integridad en ambos casos se puede modificar y hacer llegar la misma cantidad de información al servidor, a su vez la seguridad en las redes de datos es de vital importancia sobre todo con protocolos que está en pleno auge como Ipv6 ya que permitirá fortalecer la red de la FAFI

En la actualidad la Facultad se ve en la necesidad de aumentar sus puntos de red, por lo cual, al realizar la tabla comparativa de protocolos, se hace necesario la utilización de Ipv6, que nos proporcione un mayor número de direcciones, como varias características adicionales que favorecería al aprendizaje y enseñanza por parte de los Docentes y Estudiantes.

BIBLIOGRAFÍAS

(«ANÁLISIS COMPARATIVO DE PRESTACIONES ENTRE SDN Y REDES CONVENCIONALES.PDF», S. F.)

(AVILA MEJIA O, 2011), Migración del Protocolo IPv4 a IPv6. Ciudad de México: Universidad Autónoma de México.

(ABOUT ESPAÑOL, 2016), <https://www.aboutespanol.com/que-es-la-direccion-ip-y-diferencia-entre-ipv4-e-ipv6-3507897>

(AGUIRRE L, JULIO 2013), Revista Politécnica - Julio 2013, Vol. 32, No. 2, P 45

CISCO. (S.F.). Cisco Networking Academy Program. CCNA 1 and 2. Version 3.1.

(CISCO CCNA, 2013), <http://blog.capacityacademy.com/2013/04/16/cisco-ccna-todo-sobre-ipv6-tipos-de-direcciones/>

(CISCO SUPPORT COMMUNITY, 2016), <https://supportforums.cisco.com/t5/routing-y-switching-blogs/direccionamiento-ipv6-bases-y-fundamentos/ba-p/3103703>

(EDSEL ENRIQUE UREÑA LEON, 2013),

<http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml>

(FAFI-RESEÑA HISTORICA,, s.f.), http://fafi.utb.edu.ec/resena_historica

(GARCÍA JESÚS, SERVICIOS DE RED E INTERNET, MOLINILLO)

(GROUPE FIGARO CCM BENCHMARK, 2017), a partir de <http://es.ccm.net/contents/257-tipos-de-redes>

(GALARZA, 2017), file:///E:/-E-UTB-FAFI-SIST-000033.pdf

(IBM.COM & SUPPORT, s.f.), a partir de

https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_73/rzai2/rzai2compipv4ipv6.htm

(JULIAN CAMILO SOMBREDERO ALFONSO, 2014), a partir de

<http://repository.usta.edu.co/bitstream/handle/11634/764/analisis%20comparativo%20de%20pres-taciones%20entre%20sdn%20y%20redes%20convencionales.pdf?sequence=1>

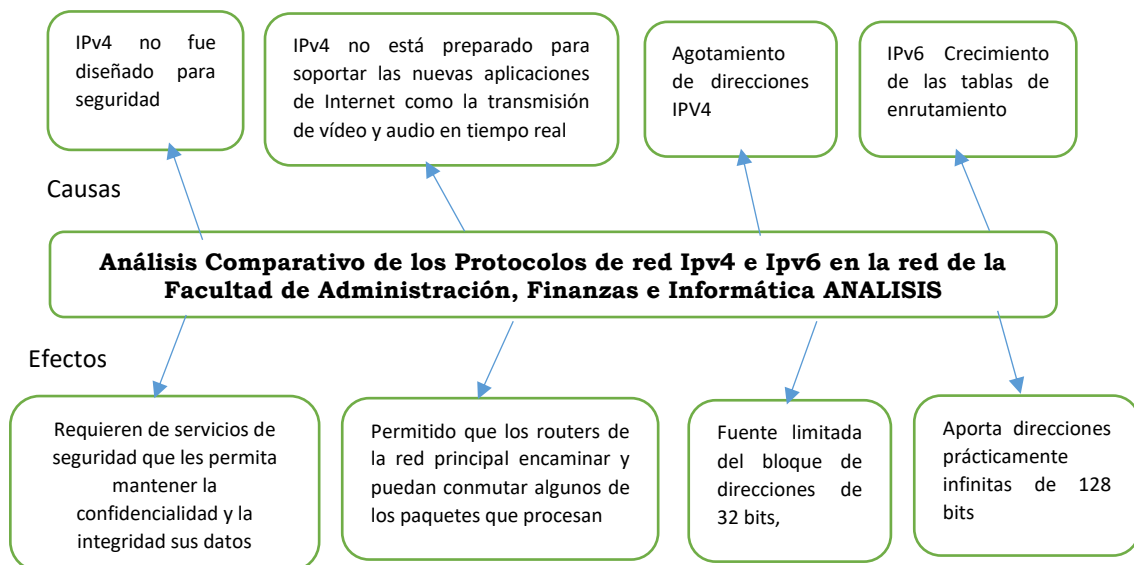
(MÓDULO PROFESIONAL DE SERVICIOS DE RED E INTERNET (IESSANJUANBOSCO, 2016)).

(SOLVETIC, 2017), a partir de

<https://www.solvetic.com/page/noticias/s/internet/caracteristicas-diferencias-protocolo-internet-ipv4-ipv6>

ANEXOS

Árbol del problema



Análisis FODA

Un análisis de las fortalezas, oportunidades, debilidades y amenazas del análisis comparativo entre las redes IPv4 e IPv6 en la red de la Facultad de Administración, Finanzas e Informática que nos permitirán centrarnos en el tipo de sistema que realizaremos para resolver el problema.

FORTALEZAS

- ✓ Apoyo del Departamento de Sistemas para la generación de ideas de oportunidades de mejora.
- ✓ Personal comprometido y efectivo en todas las áreas de trabajo, con capacidad técnica y experiencia profesional.

- ✓ Capacidad de innovación e integración de los sistemas de información.
- ✓ Plan de capacitación de acuerdo a necesidades del personal.

DEBILIDADES

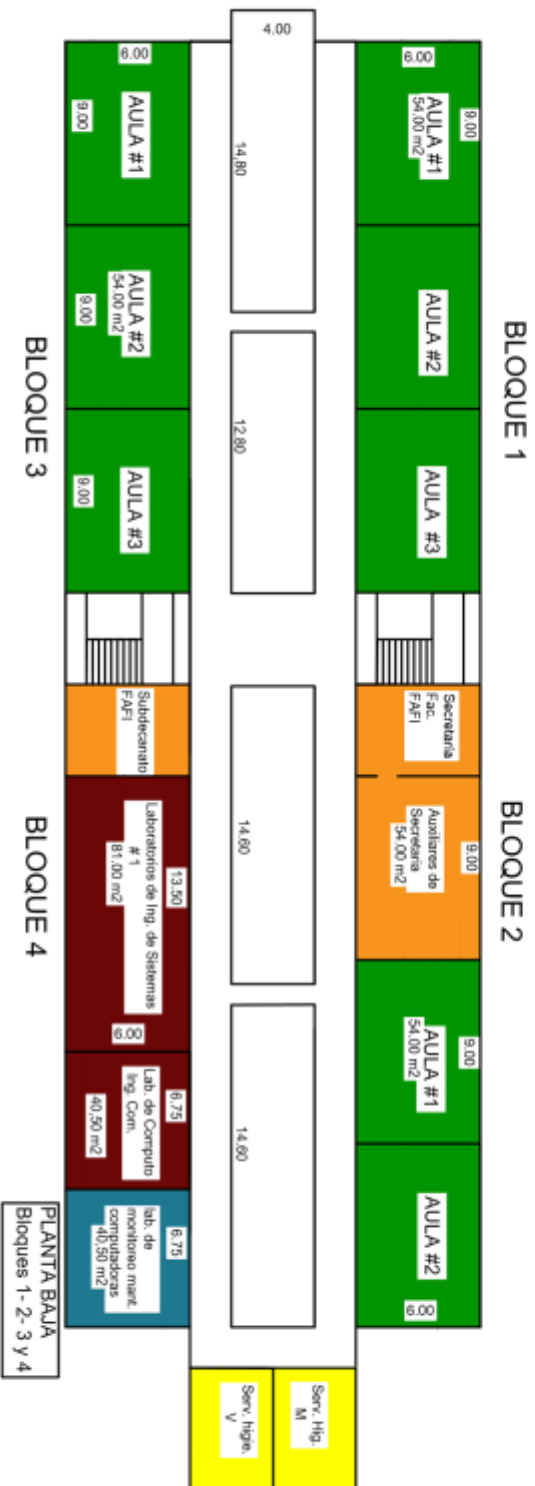
- ✓ Recursos y capacidades escasas
- ✓ Carece de niveles de seguridad.
- ✓ Las direcciones IP deben ser asignadas por un organismo encargado en cada facultad.

OPORTUNIDADES

- ✓ Políticas de Estado que apoyan a las Instituciones de Educación Superior para alcanzar la excelencia académica.
- ✓ Desarrollos de nuevas tecnologías y buenas prácticas de gestión enfocadas a los sistemas educativos.
- ✓ Capacidad de adaptación de las herramientas tecnológicas para generar soluciones a bajos costos con seguridad y fácil acceso a la información.
- ✓ Asignación de recursos que permiten soportar el crecimiento institucional.
- ✓ Tecnología actualizada que permite la interconexión entre los diferentes sistemas institucionales.

AMENAZAS

- ✓ Procedimientos administrativos burocráticos en las adquisiciones.
- ✓ Resistencia al cambio, falta de disposición y compromiso de las direcciones y mejora de los Protocolos de Red.
- ✓ Riesgo de ocurrencia de desastres naturales.

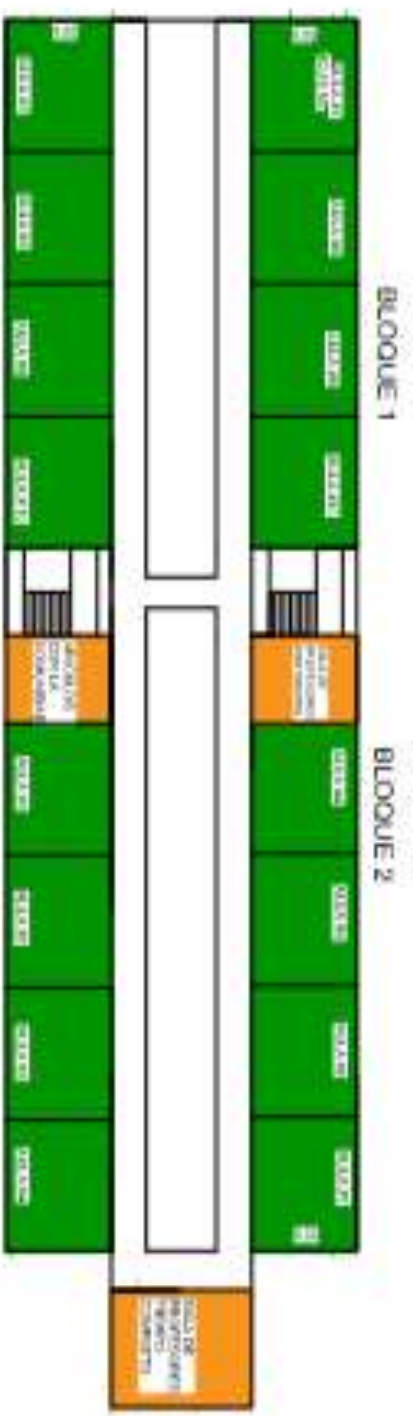


NOMENCLATURA

- AULAS = 432.00 M2
- OFICINAS = 108.00 M2
- LAB. COMP. = 162.00 M2
- SERV. HIGIE. = 48.00 M2
- Lab. Mant. Com. = 40.50 m2

UNIVERSIDAD TECNICA DE BABAHOYO

CONTIENE PLANTA BAJA BLOQUES FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA



- NOMENCLATURA
- AULAS = 675.00 M²
 - OFICINAS = 27.00 M²

2ª PLANTA ALTA
Bloques 1-2-3 y 4

UNIVERSIDAD TECNICA DE BABAHOYO	PLANO #3
CONTIENE: 2ª PLANTA ALTA BLOQUES FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA	