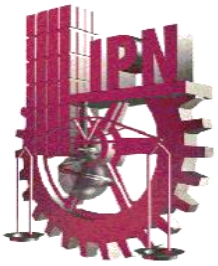


INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

Propuesta del despliegue del protocolo IPv6 en la red de telecomunicaciones de la ESIME Zacatenco.

TESIS

QUE PARA OBTENER EL GRADO DE

Maestro en Ciencias en Ingeniería de Telecomunicaciones

PRESENTA:

Ing. Octavio Eduardo García Barragán

Director de Tesis

Dr. Salvador Álvarez Ballesteros

Ciudad de México

Diciembre, 2019

RESUMEN

En este trabajo de tesis, se busca la implementación del protocolo IPv6 en la red de datos de la ESIME Zacatenco (ESIMEZ) con el fin de que se realice una metodología que agilice la migración en cualquier otra dependencia del Instituto Politécnico Nacional (IPN) y de esta manera todo el Instituto migré a esta versión (IPv6).

Antes de comenzar con el análisis de la Red de datos de la ESIMEZ, es necesario conocer el protocolo IPv6, es decir, sus principales características y ventajas con respecto a IPv4; Se sabe que la principal característica es el amplio espacio de direcciones, pero no es la única, en este trabajo se analizan todos los detalles que tiene IPv6 y se realiza una comparación entre ambos protocolos de Internet (IPv4 e IPv6).

Se realiza un estudio del estado del arte actual acerca de la Implementación del protocolo IPv6 en México y en el Mundo; Se estudian casos de éxito llevados a cabo por algunos Proveedores de Servicio de Internet (ISPs) en Latinoamérica.

El estudio de la estructura de la red de telecomunicaciones del Instituto Politécnico Nacional (a la cuál, nos referiremos como Red Politécnica a lo largo del documento), es fundamental para el desarrollo de este trabajo, aquí se conoce como es la gestión de la red Politécnica, cuáles son los protocolos de ruteo empleados, la clasificación de la red, los modelos de dispositivos que se tienen en producción, etc. Esta información es indispensable para plantear cualquier servicio o mejora a la red.

Luego se centra el trabajo en el análisis y diagnóstico de la red de datos de la ESIMEZ, destacando cuales son los principales problemas en la red, y determinando si los equipos son capaces de soportar IPv6.

Finalmente se realizan pruebas creando escenarios con dispositivos de red semejantes o iguales a los que se emplean dentro de la red de la ESIMEZ para definir si es viable o no la implementación del protocolo IPv6 en convivencia con IPv4.

ABSTRACT

In this thesis, the implementation of the IPv6 protocol in the data network of the ESIME Zacatenco (ESIMEZ) is sought in order to make a methodology that expedites migration in any other dependency of the National Polytechnic Institute and of this way the entire Institute migrates to this version (IPv6).

Before beginning with the analysis of the Telecommunications Network in ESIME-Zac, it is necessary to know the IPv6 protocol, that is, its main characteristics and advantages with respect to IPv4; It is known that the main feature is the large address space, but it is not the only one, in this work all the details that IPv6 has are analyzed and a comparison is made between both Internet protocols (IPv4 and IPv6).

A study of the current state of the art about the implementation of the IPv6 protocol in Mexico and in the World is carried out; We study success cases carried out by some Internet Service Providers (ISPs) in Latin America.

The study of the structure of the Telecommunications network of the National Polytechnic Institute (Polytechnic Network), is fundamental for the development of this work, here we present the management of the IPN network, which are the routing protocols used, the classification of the network, the models of devices that they are in production, etc. This information is essential to propose any service or improvement to the network.

Then the work is landed in the analysis and diagnosis of the ESIME-Zac data network, highlighting which are the main problems in the network, and determining if the equipment is capable of supporting IPv6.

Finally, tests are performed creating scenarios with network devices similar or equal to those used within the ESIMEZ network to define whether the implementation of the IPv6 protocol in coexistence with IPv4 is viable or not.

AGRADECIMIENTOS

En este apartado aprovecho la oportunidad de expresar mis agradecimientos a quienes me acompañaron y contribuyeron positivamente en esta etapa de mi vida.

Antes que nada, quiero agradecer a mi asesor, el Dr. Salvador Álvarez Ballesteros, quien siempre estuvo ahí para solucionar mis dudas y para guiarme en todo este proceso; Compartiendo experiencias profesionales y personales.

Al M. en C. José Rodrigo Espinoza Bautista, quien estuvo al tanto de mi proyecto a lo largo de todo este proceso, y quien compartió conmigo su conocimiento para cumplir este logro, y siempre estuvo a disposición para solucionar mis dudas.

El principal agradecimiento que tengo es para mi familia. A mis padres, principales promotores de mis sueños quienes hicieron todo lo posible para que me enfocara completamente en mis estudios. A mi Papá, Eduardo García Toriz, quien siempre ha estado al pendiente de mi desarrollo integral, buscando desarrollar mi carácter. A mi Mamá, Graciela Barragán Villanueva, quien además de estar al pendiente de mí, me enseñó a darle prioridad a lo verdaderamente importante. A mi hermano Isaac, quien siempre estuvo a mi lado demostrando su cariño. A todos ellos por siempre demostrarme su amor incondicional en todo momento.

A mis compañeros de la Maestría, quienes hicieron de este un proceso ameno, y que fueron personas de las que aprendí diferentes maneras de enfrentar los problemas.

Al departamento de conectividad de la Dirección de Cómputo y Comunicaciones del IPN por su apoyo en el desarrollo de este proyecto, especialmente al Ingeniero Martín quien estuvo al pendiente de mi trabajo.

A la Unidad de Informática de la ESIMEZ, especialmente al Ingeniero Raymundo, quien me dio la oportunidad de conocer toda la red de datos de la escuela.

Al Instituto Politécnico Nacional y a la Escuela Superior de Ingeniería Mecánica y Eléctrica donde estuve más de seis años, y donde se me brindaron todas las herramientas posibles para formarme profesionalmente.

Índice

ÍNDICE TABLAS Y FIGURAS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El crecimiento del uso del internet ha aumentado de manera exponencial los últimos 15 años, en un principio las capacidades de los equipos no permitían el intercambio veloz de archivos multimedia (videos, audio, imágenes, etc.); Hoy en día, esto se ha convertido en una necesidad, pues gracias al desarrollo de nuevas tecnologías, se han logrado crear dispositivos con altas capacidades de procesamiento, además de gran espacio de memoria.

Este crecimiento, sin embargo, no ha sido proporcional al despliegue del Protocolo IPv6, lo cual es un problema, específicamente en Latinoamérica, solo cuatro personas de cada 100 cuentan con esta versión. Especialistas afirman que cuanto más esperen las empresas y proveedores en actualizar poco a poco su infraestructura, mayor será el gasto cuando deban de actualizarla por completo. La forma en la que existe coexistencia entre el Protocolo IPv4 e IPv6, ha sido mediante las técnicas de transición empleadas (Doble Pila, Traducción y Túneles); Estas técnicas con una solución a mediano plazo, pues involucra mayores gastos de operación (OPEX). [1] [2]

El Protocolo IPv6, cuenta con un espacio de direcciones bastante amplio, 340 trillones de trillones de direcciones IP, las cuales ayudaran al desarrollo de aplicaciones como son el Internet de las Cosas (IoT), donde la mayoría de los objetos que usamos de manera cotidiana estarán conectados a internet.

En este proyecto se planea cambiar la infraestructura del núcleo de la red Politécnica, la cual consta de tres nodos (Zacatenco, Casco de Santo Tomas y UPIICSA). E iniciar el despliegue del protocolo IPv6 en todas sus capas, siguiendo el esquema jerárquico de CISCO (Capa de Acceso, Capa de Distribución y Capa de Núcleo).

Para el inicio del despliegue, en la capa de acceso, se analizará la red de datos de la ESIMEZ, que servirá como guía para cada una de las dependencias del IPN.

PLANTEAMIENTO DEL PROBLEMA

La red Politécnica siempre se ha tratado de mantener actualizada, con el fin de que siempre se cubran las necesidades de todos sus usuarios; Hoy en día, cualquier organización necesita de una red de datos, pues una de las principales características de las redes es mejorar y facilitar los procesos con tal de obtener una mejor productividad.

A pesar de que el Instituto siempre se ha actualizado, no se ha realizado un proceso de planeación en su crecimiento y su actualización. La Dirección de Cómputo y Comunicaciones (DCyC) se ha encargado de mantener la red Politécnica.

La red Politécnica, actualmente brinda diferentes servicios como Internet, Correo Electrónico Institucional, Portal Web, DNS, Cursos en Línea, Telefonía IP, Videoconferencias, El Sistema de Administración Escolar (SAES), entre otros. Todos estos servicios, se brindan bajo el protocolo de Internet versión 4 (IPv4), el cual está llegando a su fin.

La red Politécnica cuenta con equipo capaz de soportar IPv4 e IPv6, por lo que es posible iniciar el proceso de transición sin que se tenga que invertir en infraestructura. Uno de los problemas principales, según la DCyC, es que no hay mucha iniciativa por parte de las Escuelas para iniciar con el despliegue.

En ESIME Zacatenco no existe un diagrama de la topología física y lógica de la red de telecomunicaciones, también se tienen los siguientes problemas:

- Crecimiento Sin Control.
- Duplicidad de IP’s.
- Interferencias (Puntos de Acceso Wi-Fi).
- Problemas de Diseño en la última actualización de la Red (año 2016).
- No hay certeza de donde se ubican ciertos nodos.
- Equipo no explotado al máximo (Puertos sin conectar).

Todos estos problemas se deben a los cambios de administración en la Unidad de Informática (UDI), la cual, es encargada de gestionar la red de datos de la ESIMEZ, y aunque el objetivo de los encargados sea brindar un servicio de calidad; El detener los procesos, cambiando a los encargados, resulta perjudicial para la red.

En el presente trabajo se realizará un análisis general de la capa de núcleo y distribución de la red Politécnica, y posteriormente un diagnóstico más detallado de la Red de datos de la ESIMEZ para determinar si se cuenta con equipo capaz de soportar IPv6 y decidir que técnicas de transición serán viables para cada uno de los escenarios. Además, será posible proponer un rediseño en la red de datos de la ESIMEZ con la información obtenida con el diagnóstico.

JUSTIFICACIÓN

Hoy en día, la Red Politécnica no tiene las facilidades de agregar nuevos dispositivos para su acceso a internet, pues no cuenta con direcciones IP públicas suficientes; Razón fundamental por la cual la red se encuentra limitada.

Desde sus inicios, el IPN se ha destacado por mantenerse a la Vanguardia actualizando su infraestructura Tecnológica, por lo tanto, es muy importante que inicie la migración al Protocolo IPv6 para que continúe el crecimiento de la red con una mejor calidad y desempeño para todos los usuarios garantizando la retrocompatibilidad con IPv4.

La importancia de iniciar el despliegue de IPv6 es muy importante para el desarrollo de nuevos proyectos académicos, que involucran temas como Internet en las cosas (IoT) e Internet en Todo (IoE); donde cualquier objeto de uso cotidiano se podrá conectar con otro mediante Internet.

En mayo del presente año (2018), entraron en producción nuevos equipos de red en el núcleo de la Red Politécnica; Equipo que tiene la capacidad de soportar ambos protocolos (IPv4 e IPv6); El Instituto ya cuenta con un espacio de direcciones IPv6 asignado por IAR México (Internet Addresses and Resources Mexico). Por lo tanto, se justifica el desarrollo de este trabajo pues se tienen las condiciones necesarias para iniciar con el despliegue de IPv6.

En colaboración con el Ing. Manuel de la Cruz Cruz, encargado del Departamento de Conectividad y Transmisiones del IPN, se definió un plan a mediano plazo, en el que se iniciará formalmente la transición a IPv6 en todas las capas de la red (Núcleo, Distribución y Acceso). De esta manera se optó por la ESIME Zacatenco para comenzar con este proceso en la capa de Acceso mientras se realizan pruebas en la capa del núcleo.

OBJETIVOS

OBJETIVO GENERAL. –

Diseñar una propuesta de Implementación del Protocolo Ipv6 en la Capa De Acceso en ESIME Zacatenco.

OBJETIVOS ESPECÍFICOS. –

- Analizar y Definir la topología física Actual de la ESIME Zacatenco.
- Determinar si la Topología Física cumple con las demandas de las diferentes áreas de la escuela según su importancia.
- Determinar si los equipos de la ESIME Zacatenco cumplen los requisitos necesarios para iniciar la migración a IPv6.
- Definir una Metodología para la Implementación del Protocolo IPv6 en la capa de Acceso de la Red Politécnica.
- Determinar que mecanismo de transición (Túnel, Doble Pila y Traducción) es el adecuado para implementar IPv6 en ESIME.
- Propuesta de adquisición de equipo para mejorar la eficiencia de la red con IPv6.

CAPÍTULO I: MARCO CONTEXTUAL

Antecedentes

A principios de los 90s la IETF (Internet Engineering Task Force – Grupo de Trabajo de Ingeniería de Internet) notó un agotamiento acelerado de direcciones IPv4, de las 3700 millones de direcciones IPv4, ya estaba ocupada una octava parte; y fue duplicándose cada 5 años, por lo tanto, las proyecciones indicaban que la última dirección se agotaría en el año 2005.

Este problema llevó al IETF, a trabajar en la siguiente generación de IP (IPng, IP next generation), que finalmente llevó la creación del estándar IPv6. El primer RFC sobre IPv6 se publicó en 1995.

Al ya haber equipo existente en funcionamiento con el protocolo IPv4, era necesario seguir aprovechando sus capacidades; Más adelante, surgieron equipos capaces de trabajar bajo ambos protocolos (que soporten ambas versiones). Por lo tanto, surgieron técnicas que permitieran disminuir el rápido agotamiento de direcciones IPv4 públicas, entre estas técnicas se encuentra NAT (Traducción de Direcciones de Red), la cual sirve para conectarse a Internet.

Esta técnica permite que varios hosts puedan acceder a internet usando únicamente una sola dirección IP pública, aunque NAT interviene con varias aplicaciones, especialmente en las que no se adhieren a un modelo simple cliente/servidor. [3]

En el Capítulo II se mencionan las características más importantes de IPv6 como son, el espacio de direcciones, capacidad de autoconfiguración de computadoras y ruteadores, soporte a seguridad con IPsec, además de calidad de servicio, etc.

6Bone

Para el despliegue de IPv6 era importante que se involucraran tanto empresas de desarrollo tecnológico, como centros de investigación y universidades, y por este motivo, en el año 1996 inicia 6Bone, la cuál era una red experimental en la que participaron 47 países.

Este proyecto sirvió como banco de pruebas de IPv6, con el fin de ayudar a la transición, y sirvió para que los desarrolladores e implementadores hicieran experimentos de ruteo, desarrollo de aplicaciones e implementaciones. Las direcciones asignadas a los participantes solo eran temporales

La red se componía de nodos que soportaban directamente paquetes IPv6, y estos nodos se vinculaban con enlaces virtuales (Túneles), y para esto los equipos en los extremos del túnel debían soportar IPv6 en su sistema operativo. Solo participaron siete países Latinoamericanos, entre ellos, México.

Las Universidades de México que participaron en este proyecto fueron la UNAM (Universidad Nacional Autónoma de México), La UDG (Universidad de Guadalajara) y el ITESM (Instituto Tecnológico de Estudios Superiores de Monterrey) a quienes se les delegaron bloques con fines experimentales.

6Bone concluye en junio del 2006, cuando finalmente todos estos bloques temporales se devolvieron. [4] [5]

En 1999, el foro IPv6 es fundado por el IETF con el fin de fomentar el despliegue de IPv6; En los siguientes años ocurrieron algunos acontecimientos que influyeron en el despliegue del protocolo IPv6 y su disponibilidad:

- En marzo del año 2000 Microsoft hace el lanzamiento de la versión de vista previa de tecnología IPv6 para Windows 2000.
- En el 2001 la empresa Cisco Systems presenta dispositivos (Enrutadores y Switches) compatibles con IPv6.
- El 4 de febrero de 2008 la IANA agrega registros AAAA para las direcciones IPv6 para la resolución de nombres de dominio (DNS) usando solo IPv6.
- El 8 de junio de 2011, la sociedad de Internet, celebra el Día Mundial de IPv6 con una prueba global de 24 horas de IPv6.
- El 6 de junio del 2012 se celebra el Día Mundial del Lanzamiento de IPv6, donde se desplego IPv6 de forma permanente en todos las empresas y organizaciones que formaban parte de la sociedad de internet.

Despliegue IPv6 a nivel Mundial

A pesar de que IPv6 lleva más de 10 años desde su creación, el protocolo de internet versión cuatro sigue siendo el más popular en el mundo; el despliegue de IPv6 no ha sido proporcional al crecimiento de internet, y por eso han surgido técnicas para atrasar el agotamiento de direcciones IPv4.

Los siguientes datos fueron obtenidos de Google, y en la siguiente tabla (Tabla 1) podemos ver qué países van más avanzados en cuanto a su despliegue IPv6.

GLOBAL	
PAÍS	**ADOPCIÓN (%)**
Bélgica	52.58
Alemania	40.72
Grecia	36.52
USA	33.82
Uruguay	32.57
India	32.38
Malasia	28.54

Tabla 1 Porcentaje de Adopción de IPv6 a nivel global según Google [6]

Según estadísticas de Google a nivel mundial, solamente el 24.23% de usuarios acceden a su página mediante IPv6.

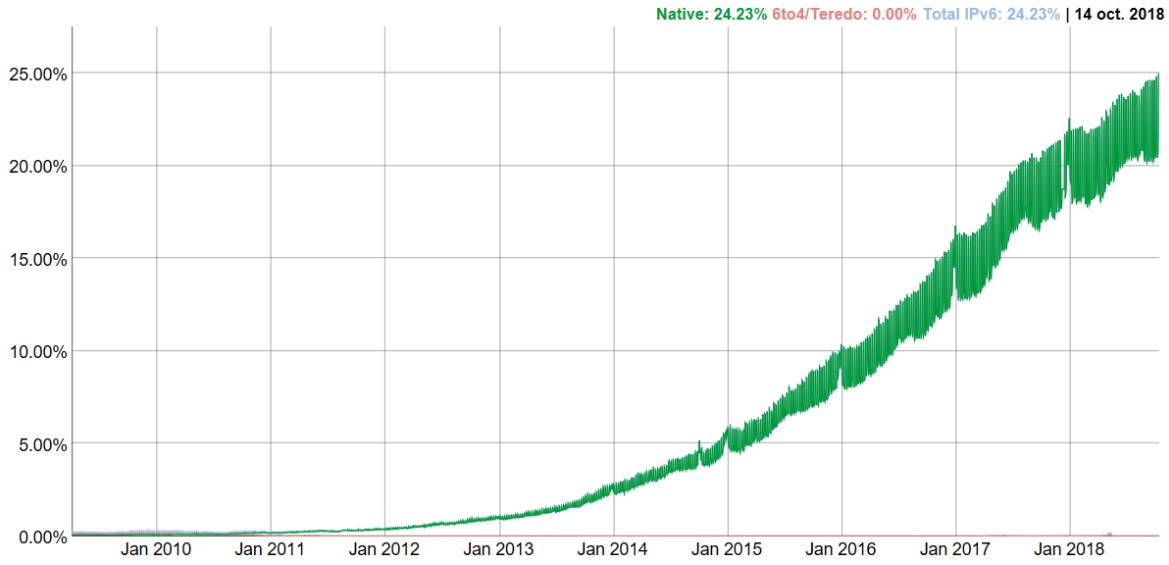


Figura 1. Acceso a Google mediante IPv6 a nivel Mundial [6]

El único país latinoamericano que se encuentra en este ranking es Uruguay; México, al igual que Uruguay, pertenece a LACNIC (Registro Regional de Internet para América Latina y el Caribe) quien es el encargado de administrar y delegar los recursos de internet en Latinoamérica y el Caribe.

El despliegue de IPv6 en México ha sido bajo. En la tabla (Tabla 2) se pueden observar los países de nuestra región más avanzados en cuanto al despliegue de IPv6 (Estadísticas de Google consultadas el 09 de octubre del 2018).

LACNIC	
PAÍS	**ADOPCIÓN (%)**
Uruguay	32.57
Brasil	25.59
T & Tobago	19.34
Perú	16.28
Ecuador	15.38
Puerto Rico	12.32
México	12.31
Bolivia	8.42

Tabla 2 Porcentaje de Adopción de IPv6 en la región LACNIC según Google [6]

La IANA es la entidad que se encarga de supervisar y administrar globalmente la asignación de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio, entre otros recursos; Y ésta a su vez se divide en los RIR (Registro Regional de Internet), los cuales son:

- American Registry for Internet Numbers (ARIN)1 para América Anglosajona.
- RIPE Network Coordination Centre (RIPE NCC)2 para Europa, el Oriente Medio y Asia Central.
- Asia-Pacific Network Information Centre (APNIC)3 para Asia y la Región Pacífica.
- Latin American and Caribbean Internet Address Registry (LACNIC)4 para América Latina y el Caribe.
- African Network Information Centre (AfriNIC) para África

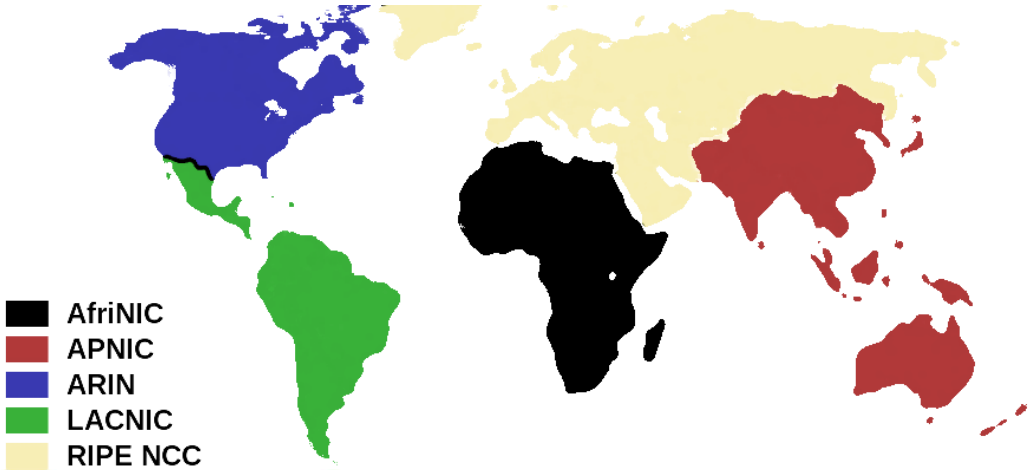


Figura 2. Distribución de los Registros Regionales de Internet (RIR)

Como se mencionó previamente, México pertenece a LACNIC, y en LACNIC se han tenido diferentes casos de éxito en toda la región, lo que ha significado el crecimiento en cuanto al despliegue de los países listados en la Tabla 2**.**

El bajo crecimiento se debe a la poca iniciativa que han tenido las diferentes empresas, pero no se les puede obligar a que inicien con el despliegue de IPv6, por esta razón las escuelas o universidades juegan un papel muy importante, pues ellas si tienen la iniciativa, además de que son capaces de preparar y capacitar a las personas interesadas.

Sin embargo, si los ISPs (Proveedores de Servicio de Internet) no se interesan en iniciar con la transición, el despliegue será más lento, y en cierto punto, costoso.

CASOS DE ÉXITO (LACNIC)

COMTECO (Cooperativa de Telecomunicaciones Cochabamba) es la empresa de telecomunicaciones responsable del despliegue masivo en Bolivia. Es prestador de servicios de televisión por cable, telefonía móvil, larga distancia, internet satelital, etc.

En el año 2012 solicitó un prefijo IPv6 a LACNIC, y el siguiente año levanto un enlace BGP (Protocolo de Puerta de Enlace de Frontera) con su proveedor de tránsito, publicando así su prefijo (2803:9400::/32), finalmente se inició el despliegue al cliente el 22 de agosto del 2014 mediante dual stack, pues invirtieron en el núcleo de su plataforma para su compatibilidad con IPv6.

Es el primer Operador Boliviano en migrar a IPv6, después lo hicieron Huracán Electric y Entel SA. Hoy en día todos los tipos de direcciones IPv6 conectados en Bolivia son de tipo nativa, y hasta inicios del presente año (2018) todavía existía un bajo porcentaje en tipos de direcciones para técnicas de tuneleo como Teredo y 6to4. [7]

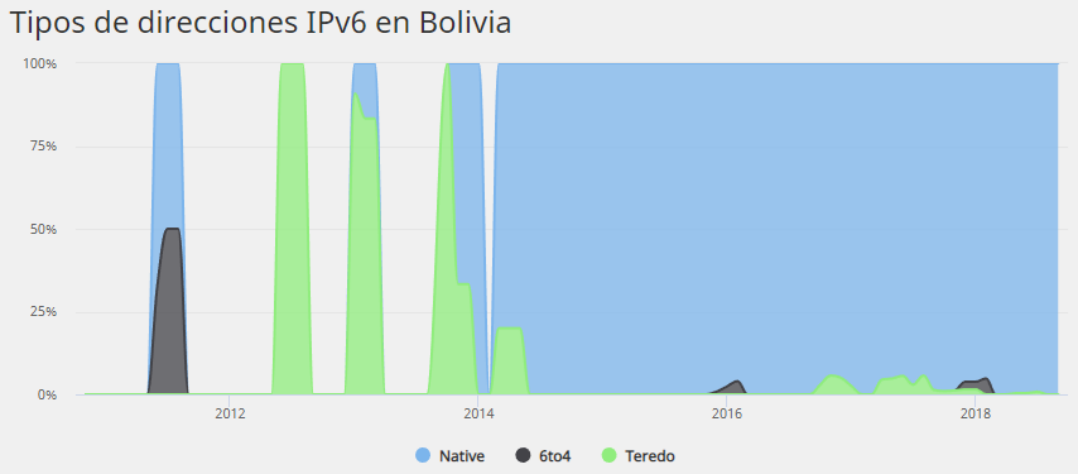


Figura 3. Porcentaje tipo de Direcciones IPv6 en Bolivia [8]

En Brasil son varios los operadores que iniciaron el despliegue de IPv6; Estos son Oi, GVT y Vivo. Actualmente ya hay 25 empresas u operadores que ya brindan este servicio. Actualmente, aún existen tipos de direcciones para tuneleo con Teredo y 6to4; aunque en un porcentaje menor a uno.

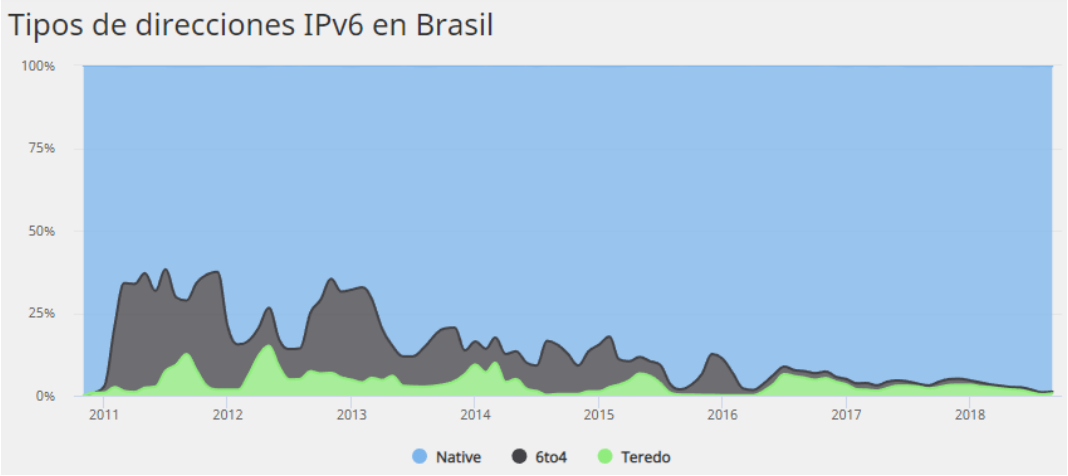


Figura 4. Porcentaje tipo de Direcciones IPv6 en Brasil [8]

En Ecuador la Corporación Nacional de Telecomunicaciones ha jugado un papel muy importante en cuanto al despliegue de IPv6, pues paso de un 1% a un 14.8% de despliegue en un año. Su éxito radica en la decisión temprana para el despliegue de IPv6. El despliegue se realizó con la técnica Dual Stack y CGNAT en la red fija.

Hoy en día, sigue siendo el ISP más importante, aunque empresas como Huracán Electric y Transtelco SA también brindan este servicio en Ecuador. Actualmente todos los tipos de direcciones son nativas.

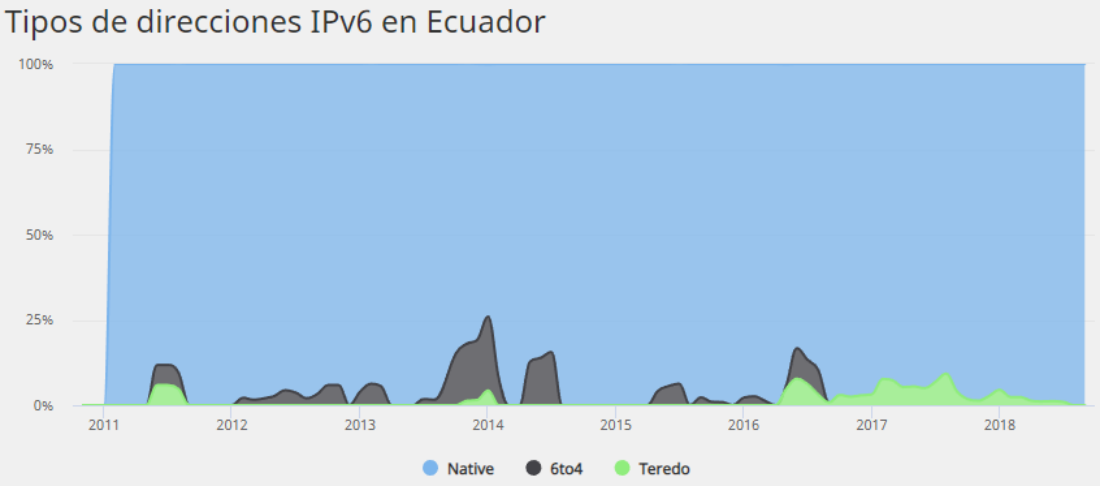


Figura 5. Porcentaje tipo de Direcciones IPv6 en Ecuador [8]

El operador que ha impulsado el despliegue de IPv6 en Perú es Telefónica del Perú, quien desarrolló una estrategia de despliegue desde el 2008, aplicando acciones de culturización con sesiones para empresas e instituciones importantes en el desarrollo. Iniciaron sus pruebas en el 2010. Su estrategia consistió en usar Dual Stack con CGNAT, Mantener los clientes de alto valor con direcciones IPv4 Públicas, y ofrecimiento de servicios IPv6 a los prestadores de contenido que lo solicitaran. En la Figura 6 se puede observar el plan de transición desarrollado.

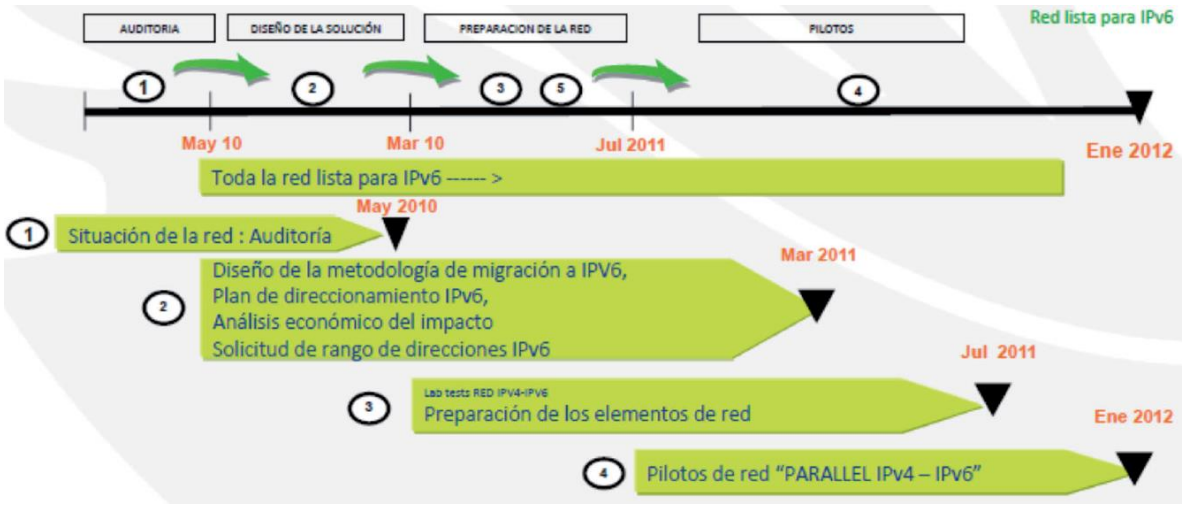


Figura 6. Plan de Transición Telefónica del Perú [7]

En la Figura 7 se puede apreciar el porcentaje del tipo de direcciones (nativa, teredo y 6to4).

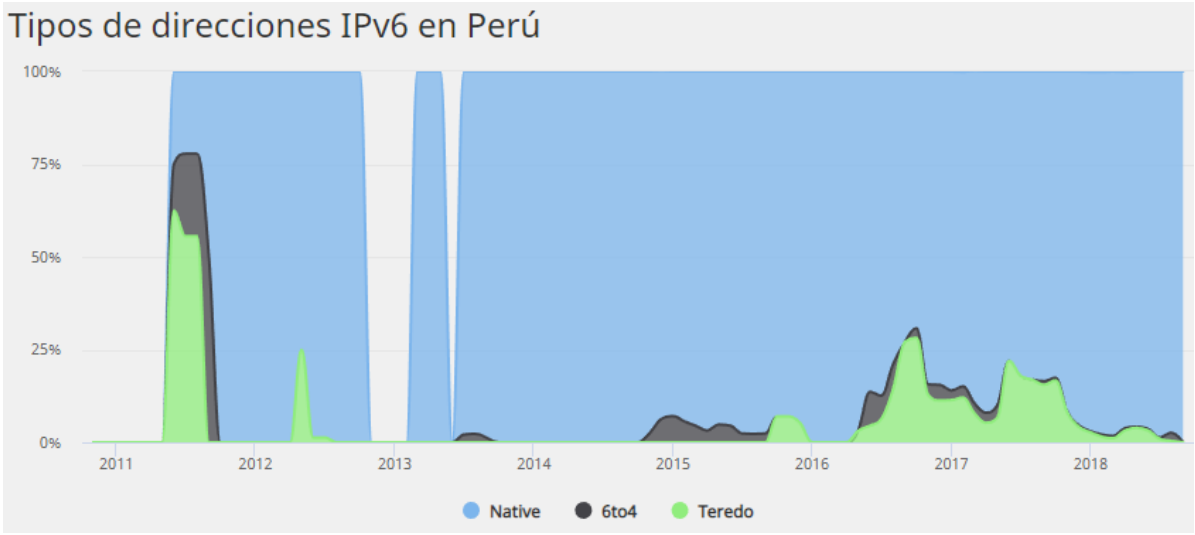


Figura 7. Porcentaje tipo de Direcciones IPv6 en Perú [8]

Uruguay se encuentra en el top cinco mundial, el ISP responsable de este despliegue es ANTEL (Administración Nacional de Telecomunicaciones), principal proveedor de internet local, quienes fueron renovando continuamente los equipos de las redes fijas y móviles. Actualmente todas las conexiones son de tipo nativas.

[8] [9]

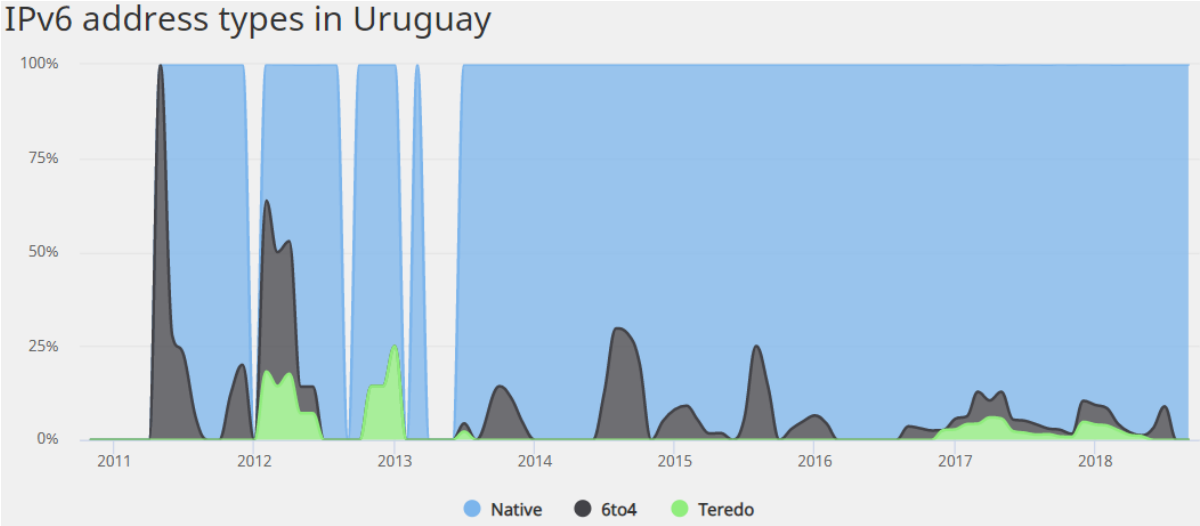


Figura 8. Porcentaje tipo de Direcciones IPv6 en Uruguay [8]

IPv6 en México

La Universidad Nacional Autónoma de México inició investigaciones sobre IPv6 desde diciembre de 1998, después se constituye su proyecto en donde se establece un amplio programa de pruebas y trabajos.

Las primeras pruebas realizadas se hicieron con el proyecto 6Bone, con el fin de probar conceptos y realizar prácticas del protocolo IPv6, y la puesta en operación de IPv6; En este proyecto participaron 47 países, la UNAM fue el primer nodo en México, registrándose en junio de 1999. Dicho proyecto finalizó en el 2006; Consistió en una red virtual compuesta por “islas” que soportaban IPv6.

En septiembre de 1999 la UNAM se convirtió en un Nodo de backbone de 6Bone. Además, la UNAM ha delegado direcciones y configurado túneles a otras instituciones en México que quisieran hacer pruebas con IPv6. De esta manera consiguió un rango de direcciones tipo pTLA (3ffe:8070::/28), que posteriormente adquirieron otras dos universidades: La Universidad de Guadalajara (UDG) y el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM), por lo que dichas instituciones pudieron delegar direcciones y configurar túneles con más de 16 instituciones en México y otras fuera del país con el fin de que realizaran pruebas de IPv6. En 1999 y 2000 se realizaron dos seminarios nacionales de IPv6.

La red IPv6 de la UNAM fue la primera bajo este protocolo, inició operaciones en agosto de 1999, contaba con varios túneles hacia otros nodos de Backbone de

6Bone como son SPRINT, FIBERTEL, MERIT, BAY NETWORKS, JANET e ISI-LAP y hacia los hosts de la UNAM.

La UNAM brindaba servicios de IPv6 mediante túneles IPv6 sobre IPv4 a otras Instituciones como el IPN, la ITAM, CUDI, entre otros. Tal como se puede apreciar en la Figura 9.

Figura 9. Conexión a 6Bone en México

Para contar con una red de pruebas en una primera etapa, y posteriormente con una red de producción, se instaló la Red IPv6 de la UNAM, la primera red IPv6 instalada en México y que inició operaciones en agosto de 1999. Esta red contó con varios túneles hacia otros nodos de Backbone de 6Bone: SPRINT, FIBERTEL, MERIT, BAY NETWORKS, JANET e ISI-LAP, y hacia los hosts que ha tenido la UNAM corriendo con distintos sistemas operativos como Windows 2000, 2003, Vista y 7, Solaris, así como varias distribuciones de Linux y de BSD.

Hoy en día, la UNAM trabaja con otras instituciones (de México y Latinoamérica) para su conexión IPv6; Las Instituciones más destacadas son el Instituto Politécnico Nacional, La Universidad Autónoma Metropolitana, el Instituto Tecnológico de Estudios Superiores de Monterrey, PEMEX, entre otras.

El primer túnel de IPv6 sobre IPv4 entre las redes académicas de México y Estados Unidos se realizó en el 2001 cuando se integró el Grupo de Trabajo de IPv6

en CUDI (Corporación Universitaria para el Desarrollo de Internet), la cual coordina la red académica de México. A finales de ese mismo año, la UNAM obtuvo un bloque de direcciones tipo sTLA (2007:0448::/35), el primero en México para servicios de Producción, posteriormente otras Universidades como la UDG y el ITESM también obtuvieron sus respectivos bloques, además de los primeros Proveedores de Servicios de Internet (ISP).

En el 2002, la primera conexión IPv6 nativa entre México y Estados Unidos entra en Operación.

El porcentaje de adopción en México es del 12.86% (consultado el 16 de octubre del 2018). [6] [10] [11]

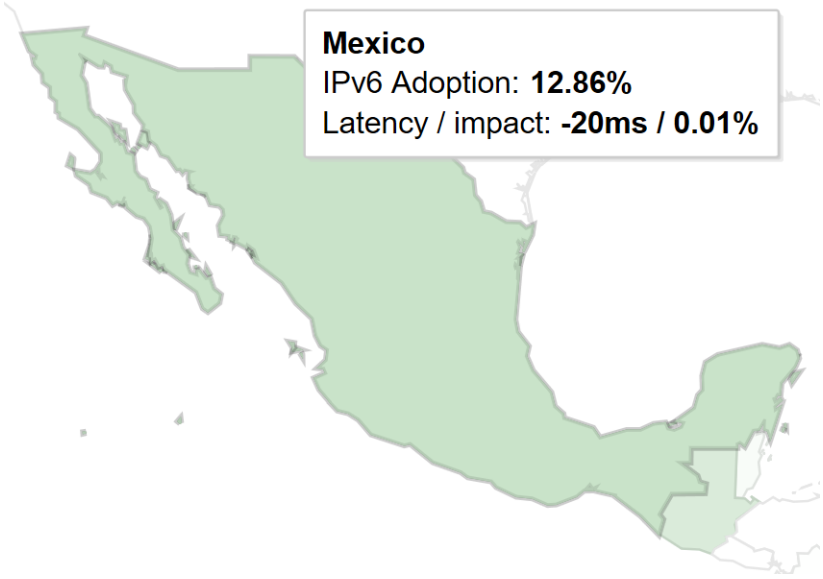


Figura 10. Porcentaje de Adopción de IPv6 en México según Google [6]

El siguiente diagrama (Figura 11) muestra el número de asignaciones de IPv4 e IPv6 en México al 16 de abril del 2013 según NIC México.

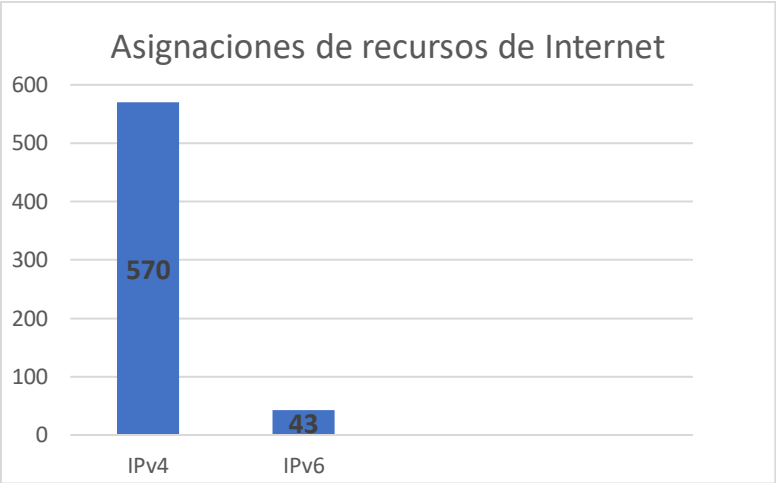


Figura 11. Asignación de los recursos de Internet IPv4 e IPv6 [12]

Evidentemente, la iniciativa de las empresas no ha sido la esperada, sin embargo, el hecho de que algunos proveedores de servicios ya se hayan involucrado en el despliegue de IPv6 en su propia red, genera un ambiente de competencia en el cual sus adversarios se tendrán que preocupar por el despliegue del nuevo protocolo en su infraestructura.

En la siguiente tabla (3) se pueden observar todas las asignaciones realizadas en México al 16 de abril del 2013.

PREFIJO	EMPRESA	GIRO	TIPO DE CONEXIÓN
2001:1248::/32	Alestra	ISP	Túnel
2806::/28	Axtel	ISP	Nativa
2801:f0::/48	Banco de México	Finanzas	----------
2806:2e0::/32	BTU Comunicación	ISP	----------
2806:250::/32	Cablemas	ISP	Nativa
2806:310::/32	Cablevisión Red	ISP	----------
2806:2a0::/32	Cablevisión	ISP	----------
2801:f0:20::/48	Centros Culturales de México	Educación	Túnel
2806:300::/32	Computadoras y Servicios Especiales	ISP	----------
2001:1228::/32	CUDI	Educación	Nativa
2806:220::/32	GSAT Com.	ISP	Túnel
2801:c4:10::/48	IJALTI	Educación	----------
2801:c4:20::/48	INAOE	Educación	----------
2801:f0:28::/48	INEC	Gobierno	----------

2001:1230::/32	INFOTEC	ISP	?
2801:c4:60::/48	**IPN**	**Educación**	**----------**
2001:1220::/32	ITESM	Educación	Túnel
2806:2f0::/32	Iusacell	ISP	----------
2001:1238::/32	Maxcom	ISP	Túnel
2806:260::/32	Mega Cable	ISP	----------
2806:240::/32	Megacable	ISP	Túnel
2806:320::/32	Metro Net SAPI	ISP	----------
2001:1260::/32	Metrored	ISP	Túnel
2001:1240::/32	Micronet	ISP	Túnel
2001:1250::/32	NIC México	Otro	Nativa
2801:c4:20::/48	Operbes (Bestel)	ISP	----------
2806:200::/32	Pegaso PCS (Telefónica)	ISP	Nativa
2001:1200::/32	Protel-I Next	ISP	Túnel
2001:1270::/32	Sixsigma	ISP	----------
2806:290::/32	TelNor	ISP	----------
2806:230::/32	Televisión Internacional (Multimedios)	ISP	----------
2806:270::/32	Triara	ISP	----------
2806:1000::/24	Uninet	ISP	Nativa
2801:c0::/32	UA Baja California	Educación	----------
2801:c4::/48	UA Cd. Juárez	Educación	----------
2801:c4:50::/48	UA de Guadalajara	Educación	----------
2801:c4:40::/48	UA de Guerrero	Educación	----------
2001:13a8::/32	UA Hidalgo	Educación	----------
2801:f0:16::/48	UA Querétaro	Educación	----------
2801:d0::/32	UA SLP	Educación	----------
2001:1218::/32	UNAM	Educación	Nativa
2001:1210::/32	U de Guadalajara	Educación	Túnel
2801:c4:30::/48	U de Guanajuato	Educación	----------

Tabla 3 Asignación de Bloques IPv6 al 16 de abril del 2013 [12]

Aunque ya se han delegado o asignado direcciones IPv6 a más de 40 organizaciones, solamente se ha detectado la conexión de 16 de ellas, algunas lo hacen de manera nativa y otras mediante túnel.

Actualmente solo existen tres escuelas que ya se conectan a IPv6, las cuales son la Universidad Nacional Autónoma de México (UNAM), la Universidad de Guadalajara (UDG) y el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM). El ITESM se conecta mediante el uso de túneles. [12]

RedUNAM

La red de la UNAM (RedUNAM) como se explicó anteriormente, cuenta con IPv6 en algunos segmentos desde 1999, y también brinda servicios a otras escuelas mediante túneles. El proyecto de despliegue fue bastante amplio, con muchos trabajos que involucraban temas como Doble Pila, túneles, servidores Web, servidores DNS, aplicaciones multimedia, Internet2, e incluso conexiones con redes internacionales de IPv6 que entonces era mediante la red experimental 6Bone.

En las principales pruebas realizadas en RedUNAM para el despliegue de IPv6 se llevaron temas como:

- Métodos de conexión como “6to4”, Teredo, ISATAP, Tunnel Broker, etcétera.
- Software de Conexión como Trumpet Winsock, Freenet6, etcétera.
- Acceso a páginas Web con navegadores modificados que soportan IPv6.
- Servidores Web IPv6 para los distintos sistemas operativos.
- Diferentes tipos de autoconfiguración con ruteadores y switches de las marcas mencionadas, computadoras bajo los diferentes sistemas operativos.
- Softwares traductores IPv4/IPv6 para Windows (Toolnet6 y MSR) y Linux.
- Análisis de tráfico en IPv6.
- Pruebas de desempeño de IPv6 vs. IPv4 y de conexiones seguras (IPSec6).
- IPv6 sobre ATM, PPP, WDM, etcétera

En el año 2012 su conexión a IPv6 se hizo de manera nativa gracias a un ISP, además se instalaron equipos nuevos con soporte a IPv6. [10]

Universidad de Guadalajara (UDG)

Desplegada desde el año 2001, dentro de la comunidad universitaria. El 90% de la red institucional cuenta con el direccionamiento IPv6 y salida a Internet de manera nativa. El consumo diario de Internet IPv6 aproximadamente es de 1Gbps, que es más del 40% del tráfico total de la Universidad de Guadalajara arriba de 1Gbps.

Los servicios de IPv6 se brindan a toda la comunidad en coexistencia con IPv4 mediante doble pila, el sitio web World IPv6 la ubica en el lugar 96 en el ranking mundial con un despliegue del 31.59%.

Una de sus aportaciones se hizo durante el evento Internet Gobernance Forum 2016 en el documento titulado “Best Practice Forum on IPv6”, donde se hace referencia a la Universidad de Guadalajara como un caso exitoso en México. [13]

Situación Actual del Despliegue IPv6 en el Instituto Politécnico Nacional

La red Politécnica, combina diferentes tipos de red, es decir, tiene componentes de red de Área Amplia, de área Metropolitana, de Área Local, enlaces de Microondas, redes inalámbricas, etc. Tiene una extensión geográfica muy grande, y para tener una gestión no tan compleja, se basan en un modelo jerárquico de capas desarrollado por la marca CISCO. [14]

En el Capítulo IV se verá detalladamente la estructura de la red, sin embargo, es posible señalar que bajo el modelo jerárquico que consta de tres capas (Núcleo, Distribución y Acceso) el IPN ha actualizado gran parte de la infraestructura en muchos segmentos de su red. Actualmente la capa de Núcleo ya cuenta con equipo que soporta IPv6 e IPv4, y gran parte de los equipos en la capa de Distribución también, el problema se encuentra en la capa de acceso, donde se encuentra el usuario. Y no se ha realizado un análisis a profundidad en esta capa; Por esta razón, se decidió iniciar en ESIME Zacatenco.

El IPN ya cuenta con un bloque de direcciones IPv6 (2801:c4:60:: /48), y su proveedor de servicios de Internet (ISP) también cuenta con este servicio, por lo que es obligación del Instituto iniciar con el despliegue.

CAPÍTULO II: MARCO TEÓRICO

Redes de Datos

En los últimos años, las redes de comunicaciones han tenido un gran impacto en la sociedad, pues su uso ha aumentado de manera exponencial. Muchas empresas, organizaciones e instituciones han utilizado esta herramienta para mejorar la productividad y eficiencia de trabajo; Sin mencionar a los usuarios que acuden a sus computadoras para realizar diferentes funciones, tales como, realizar movimientos bancarios, reservar habitaciones, realizar compras, etc. Muchas de estas diferentes funciones que tiene un ordenador se deben al desarrollo exponencial de aplicaciones los años recientes; Esto se debe principalmente las capacidades que los dispositivos tienen hoy en día.

El punto clave de contar con una red de computadoras es muy simple, y se basa en la compartición de recursos, por ejemplo, una impresora, información en una página web, espacios disponibles en el disco duro de un servidor, etc. Para que una red opere de manera adecuada, existen dispositivos tales como hubs, conmutadores, enrutadores, entre otros; Que facilitan el acceso a los servicios de la red consistentemente, además de controlar que los servicios se usen de manera correcta y por las personas adecuadas.

Una Red de datos es el conjunto de máquinas o dispositivos (host) que se encuentran interconectados por un medio físico. Para considerar a un dispositivo como un nodo, éste debe ser capaz de intercambiar la información (datos) producida por otros nodos. La función de una red es el intercambio de información (datos) entre ordenadores; Y gracias a este intercambio de información es que surgen las diferentes tareas o servicios que se pueden realizar.

Una red de computadoras también se puede definir como el grupo de dispositivos o host interconectados con el fin de cumplir algún objetivo o tarea específica, los dispositivos pueden ser ordenadores, impresoras, servidores, o cualquier dispositivo capaz de conectarse a la red.

Una característica primordial en las redes de datos, es la forma en la que se procesa la información, que en este caso se realiza de manera distribuida, es decir, no es necesario que una sola máquina se haga cargo de todas los pasos o tareas para realizar un proceso.

Un término muy importante cuando se habla de redes de comunicaciones es el Protocolo; éstos rigen el control de la información de la red, es decir, constan de un conjunto de reglas entre dos o más dispositivos para el intercambio de información.

El rendimiento es un concepto muy importante cuando se habla de Redes, pues sirve para determinar si una Red es eficiente o no; Para medir el Rendimiento de una Red, es posible hacerlo de varias maneras: Tomando en cuenta el tiempo de transmisión, que se refiere al tiempo que tarda un mensaje en llegar desde un dispositivo a otro; Y tomando en cuenta el tiempo de respuesta, que es el tiempo que pasa entre una petición y su respectiva respuesta.

La cantidad de usuarios, el medio de transmisión, la capacidad de los dispositivos conectados (hardware), y también de la capacidad del software; Son factores que influyen en el rendimiento de la Red.

El ancho de banda y la latencia son términos muy usados para medir el rendimiento, regularmente se busca tener mayor ancho de banda y menor latencia. Al enviar más información a través de la red, incrementa el ancho de banda, y lo mismo ocurre con la latencia, pues aumenta el tráfico en la Red (mayor congestión).

Otro concepto que se debe comprender cuando se habla de una Red es la fiabilidad, que se refiere al éxito en la entrega de datos, donde se llevan a cabo diferentes mediciones tales como la frecuencia de fallo de la Red, el tiempo de recuperación de un enlace cuando hubo un fallo, y su robustez ante problemas de alto impacto.

Modos de Comunicación

Existen tres modos de comunicación básicos; estos son Simplex, Half-Duplex y Full-Duplex.

El primero consiste en la transmisión de información en un sentido; Algunos ejemplos claros de este modo son: El escuchar una estación de Radio, es decir, los datos van de la antena transmisora de dicha estación a la antena receptora del radio, y no se puede transmitir en sentido contrario.

En el caso de Half-Duplex, se comparte un mismo canal de comunicación, por lo tanto, no se lleva a cabo una comunicación simultánea, es decir, Si un dispositivo A envía información a un dispositivo B, el dispositivo B no puede enviar información a la vez. El flujo de información es en un solo sentido en un tiempo determinado. Un ejemplo de este modo de comunicación son los walky-talkies.

Finalmente, tenemos el modo Full-Duplex, en este caso se requieren dos canales físicos de transmisión y recepción; Por lo tanto, la información puede fluir en ambos sentidos a la vez (de manera simultánea). El ejemplo más conocido por la mayoría de este modo de comunicación es el teléfono. [15]

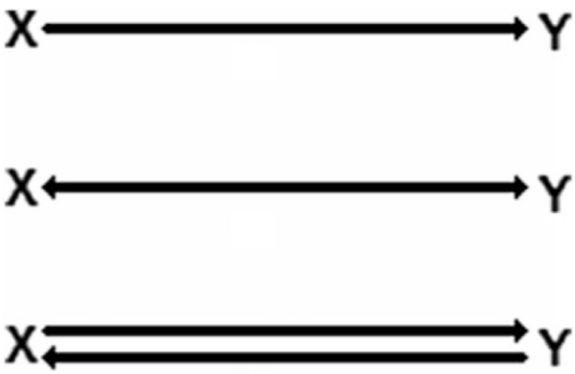


Figura 12. Modos de Comunicación (Simplex, Half Duplex y Full Duplex)

Modelo OSI

Este modelo se adoptó como estándar por la ISO (Organización Internacional de Normalización) en 1979, la necesidad de este estándar surgió debido a la incompatibilidad que existía entre dispositivos. [16]

Consiste de siete capas, y los dispositivos encargados del control de la red que se mencionaron anteriormente actúan en las primeras tres capas (Física, Enlace de Datos, Red); Cada una de las siete capas maneja la información de diferente manera, y la unidad en que se maneja la información se llama PDU (Unidad de Datos de Protocolo), algunas capas agregan cierta información a los datos debido a los protocolos que se encuentran involucrados; Esta información se puede agregar en forma de Cabeceras y Colas (Una al principio del PDU y otra al final respectivamente). De esta manera, si un host desea transmitir información, la cabecera que se le agregue en la Capa de Red será la utilizada en el host receptor, así que esta compatibilidad debe ser extremo a extremo para que el intercambio de información sea correcto. [17]

Es necesario hablar de los modos de transferencia de datos, estos son: Orientado a Conexión y No Orientado a Conexión.

En el Orientado a Conexión, se debe establecer un camino (conexión) para el flujo de datos entre el transmisor y el receptor antes de iniciar con la transmisión de información, un ejemplo son las llamadas telefónicas donde es imposible comunicarse antes de que ya exista una conexión, en este caso el camino para el flujo de datos se establece una vez que se contesta la llamada.

Por otro lado, existe el No Orientado a Conexión, y en este caso no se requiere establecer un camino o trayectoria para el flujo de datos, el control de la

información se agrega a los datos que son transmitidos; Un ejemplo son los mensajes de correo electrónico.

Capa Física

Esta capa maneja bits sin formato como Unidad de Datos del Protocolo (PDU), consiste en transmitir los bits desde la capa de Enlace de Datos transmisora a la capa de Enlace de Datos receptora.

Aquí se definen los medios mecánicos, eléctricos, funcionales y de procedimiento que sirven para activar, desactivar o mantener algún enlace físico entre dos entidades de enlace de datos. En esta capa la señal puede ser transmitida mediante un cable (tensión eléctrica), luz a través de fibra óptica, o electromagnética por medio del aire.

Entre las tareas que se llevan a cabo en esta capa se encuentra la de activación de conexiones físicas a petición de la capa superior (Enlace de Datos), otra de las funciones es la transmisión de los bits (PDU) de la fuente al destino. También es posible que se requieran compartir canales físicos mediante multiplexación en el emisor y demultiplexación en el receptor.

Se debe asegurar que los bits lleguen en orden al receptor, esto mediante la secuenciación. [18]

Capa de Enlace de Datos

En esta capa la unidad de datos de protocolo es la Trama (frame), pueden variar en cuanto a su tamaño de cientos a miles de bytes, el control de información se anexa en un encabezado y en una cola. Las funciones de esta capa dependen del tipo de comunicación (Orientado a Conexión y No Orientado a Conexión). Por ejemplo, para comunicación Orientada a Conexión es posible establecer la conexión entre las entidades que se comunican entre sí; Y un ejemplo de una función de comunicación no Orientada a Conexión puede ser la retransmisión.

Capa de Red

La PDU en esta capa son los Paquetes, en esta capa se controla el enrutamiento de datos entre redes, además del control de subredes, a continuación, se muestran las principales tareas involucradas en esta Capa.

Seleccionar el mejor camino que seguirá el flujo de información de origen a destino es el principal objetivo del Enrutamiento.

La segmentación consiste en hacer los paquetes más pequeños, lo cual es muy importante cuando la información viaja a través de diferentes redes con diferentes estándares en la capa de enlace de datos.

También se emplea el Mapeo de Dirección de Red a Dirección de Enlace de Datos. El direccionamiento de Red es jerárquico y brinda una dirección única a cada Host.

Capa de Transporte

Los Segmentos son la Unidad de Datos de Protocolo correspondientes a esta capa.

Comunicación Orientada a Conexión. Aquí se establecen y liberan las conexiones; Se realiza un control de Secuencia para que la información llegue en el mismo orden que fueron transmitidos; En esta capa se Detectan y Corrigen errores. También puede monitorear la Calidad de Servicio (QoS) de los Parámetros de comunicación.

Comunicación No Orientada a Conexión. Detección de Errores (Sin Corrección), también es posible monitorear la Calidad de Servicio (QoS).

Capa de Sesión

Establece el inicio y finalización de sesiones; También se lleva a cabo la Administración del Token, el cual se relaciona con el modo de comunicación (simplex, half-duplex y full-duplex). Se puede decir que aquí se controlan los diálogos entre aplicaciones. Aquí se ven involucrados los Protocolos RPC (Llamada de Procedimiento Remoto), SCP (Protocolo de Comunicación Simple) y ASP (Protocolo de Sesión APPLE TALK).

Capa de Presentación

Esencialmente es responsable de la forma en la que se presentan los datos en la Aplicación, brinda servicios de compresión, encriptación y traducción o formateo de datos.

Capa de Aplicación

Finalmente, la última capa del modelo OSI, se encarga de definir los servicios presentados al usuario final, aquí se definen los parámetros de calidad de servicio, así como los aspectos de seguridad; Entre los servicios que existen encontramos el Protocolo de Transferencia de Archivos (FTP), el Sistema de Nombres de Dominio (DNS), Protocolo Seguro de Transferencia de Hipertexto (HTTPS) para acceso a páginas web, entre otros.

A continuación, se puede observar en la Figura 13 un esquema del Modelo OSI, con los PDUs correspondientes a cada capa y sus estructuras.

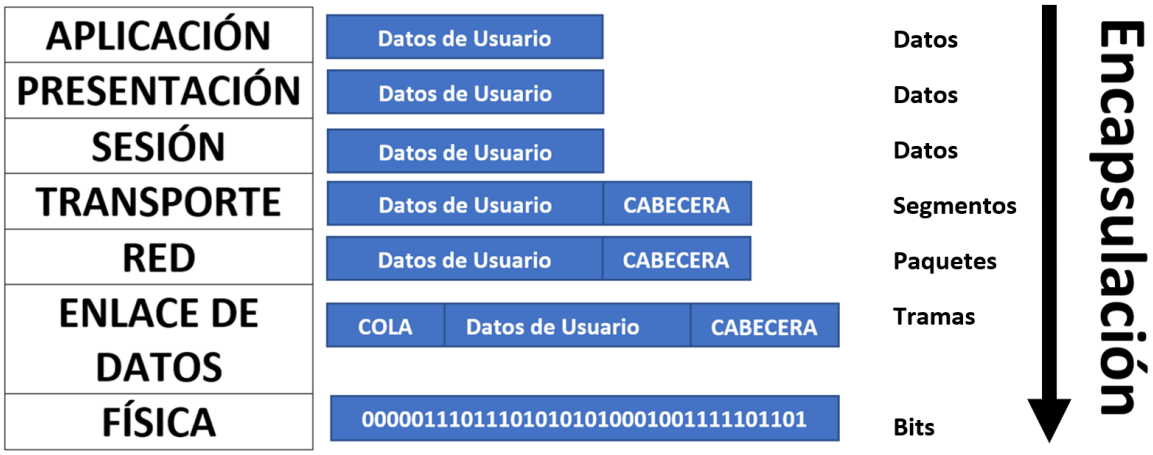


Figura 13. Encapsulación en Modelo OSI

En la Figura 14 se puede apreciar como el Enrutador (dispositivo de red) se ubica en la capa de red.

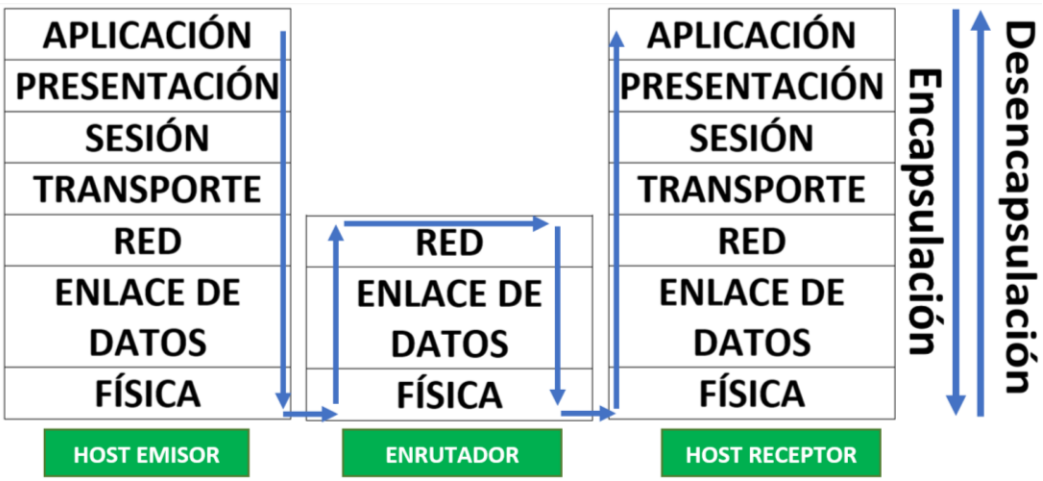


Figura 14. Capas que cubre el Enrutador

Modelo TCP/IP

Este modelo desciende de un proyecto del Departamento de Defensa de Estados Unidos, titulado “Red de la Agencia de Proyectos de Investigación Avanzada” (ARPANET, Por sus siglas en ingles), creado con el fin de mantener comunicación ante una pérdida de comunicaciones. A diferencia del Modelo OSI, el cual fue un modelo para que los protocolos se desarrollaran basándose en él; Este modelo se basa su funcionamiento en los protocolos TCP/IP ya existentes.

Este modelo se adoptó de manera amplia debido a que ARPANET ya estaba ahí por lo tanto adopto este modelo. Algunos beneficios del modelo TCP/IP son la independencia de Hardware y Software, el esquema de direccionamiento amplio y flexible; Además de ser un sistema abierto, donde su definición y sus implementaciones son públicos.

Está formado por cuatro capas: Acceso a la Red, Internet, Transporte y Aplicación como se observa en la Figura 15.

Figura 15. Capas Modelo TCP/IP

Se puede notar que no existen capas de sesión ni de presentación como en el Modelo OSI, y la capa de enlace de datos y la capa física se reducen a una sola (Capa de Acceso a la Red).

Capa de Acceso a la Red: Se encarga de que los paquetes provenientes de la capa de Internet se entreguen a un enlace físico y viceversa; Sin importar el tipo de Red (WAN, LAN, etc.) o el medio, siempre y cuando la red sea capaz de entregar los paquetes IP; Por lo tanto, estos medios y tipos de red se pueden usar en la capa de Internet. Los protocolos correspondientes a esta capa definen los procedimientos para el acceso al medio de transmisión y también para la interacción con el Hardware de la Red.

Esta capa es la encargada de mapear las Direcciones IP (Empleadas en la capa de Internet) con las direcciones de Hardware (Dirección MAC), además

determina la conexión de medios físicos dependiendo de la interfaz de Red y del tipo de Hardware.

Capa de Internet: La selección de la mejor ruta o trayectoria para que los datos fluyan desde el emisor hasta el receptor es el propósito principal de esta capa; El protocolo IP es el principal en esta capa; Y los protocolos que soportan a IP son el Protocolo de Control de Mensajes de Internet (ICMP), el Protocolo de Resolución de Direcciones (ARP) y el Protocolo de Resolución de Direcciones Invertido (RARP). El protocolo IP se encarga definir los paquetes y el esquema de direccionamiento, también transportar los datos de la Capa de Acceso a la red a la Capa de Transporte.

Uno de los dispositivos de Red usados en esta capa es el Enrutador, y es el que se encarga de seleccionar la mejor ruta para la transmisión de información.

Capa de Transporte: De manera similar al Modelo OSI, esta capa busca que exista conversación de extremo a extremo, Dos protocolos que corresponden a esta capa son TCP y UDP, los cuales buscan crear comunicación en el modo Orientado a Conexión y No Orientado a Conexión.

El Protocolo TCP proporciona secuenciación; Lo que significa que en caso de que algunos segmentos de datos lleguen a su destino en secuencias diferentes a la que se envió, es posible reorganizarse. Este protocolo proporciona la confiabilidad que el Protocolo IP carece, pues aquí se puede verificar que la información llegue sana y salva. Divide la información en Datagramas, los ordena en secuencia, y le agrega cierta información para control de errores.

Capa de Aplicación: Maneja la representación de datos, la codificación y el control de diálogo, su función es por un lado entregar los datos de las aplicaciones a la capa de Transporte y por el otro recabar información de la capa de transporte y entregarlos a las capas correctas. Algunos de los Protocolos que cubren varias aplicaciones son HTTP (Protocolo de Transferencia de Hipertexto), FTP (Protocolo de Transferencia de Archivos), SMTP (Protocolo Simple de Transferencia de Correo), POP3 (Protocolo de Oficina Postal 3), Telnet y DNS (Servicio de Nombres de Dominio).

Muchos protocolos de esta capa son conversaciones que usan el Código ASCII (Código Estándar Americano para el Intercambio de Información), y por lo tanto pueden pasar a través cualquier tipo de puertas de enlace, hosts, y enrutadores; Debido a que se pueden usar conversaciones de texto, no resulta ser tan seguro, y surgen versiones seguras de algunos protocolos mencionados anteriormente como HTTPS y SSL. [19]

PROTOCOLO DE INTERNET (IP)

El protocolo IP (Internet Protocol) surgió en inicios de la década de los 80s junto al Protocolo de Control de Transmisión (Transmition Control Protocol); Tenía el propósito de que todas las computadoras conectadas a Internet contaran con un lenguaje en común. La dirección IP es necesaria en un dispositivo para que este pueda ser localizado, y pueda recibir información a través de la red. Este es un Protocolo no Orientado a Conexión, por lo tanto, no se requiere establecer una conexión antes de transmitir la información, además no verifica si los datos llegaron de manera correcta (mejor esfuerzo), los protocolos que se encargan de esto se encuentran en capas superiores como TCP. Este protocolo es exclusivo de la capa de Internet, además de ICMP y ARP.

Es un protocolo de conmutación de paquetes definido por el IETF RFC971 y fue modificado por los RFC 950, 919 y 922. Diseñado para trabajar en sistemas interconectados de redes de comunicación por computadora con conmutación de paquetes. Su función es entregar paquetes de un host a otro, que se encuentre o no en la misma red anexando una cabecera o encabezado que contiene información de direccionamiento y control.

Su funcionamiento es básicamente de la siguiente manera; En la capa de transporte se toman flujos de datos, mismos que son divididos para enviarse como paquetes IP; Aunque estos paquetes tienen una capacidad de 64 Kbytes, normalmente son menores a 1.5 Kbytes, pues se transmiten mediante una trama ethernet; Después estos paquetes viajan a través de internet con ayuda de los enrutadores, los cuales determinan las rutas a seguir entre enrutadores para llegar al destino. Finalmente, cuando todos los paquetes son entregados al receptor, la capa de red se encarga de reensamblarlos y subsecuentemente entregarlos a la capa de transporte.

Una característica muy útil del Protocolo IP es la segmentación y el reensamblaje de paquetes largos a paquetes pequeños, pues existen redes que tienen diferentes reglas en la longitud máxima; Cada paquete se trata como una unidad independiente, no se establece ningún circuito lógico. [20]

IPv4

Es la cuarta versión del Protocolo de Internet, implementado por primera vez en ARPANET (Red Experimental) en 1983. Está definido en el RFC 791. Debido a que era un protocolo experimental, no se analizó el crecimiento de su uso, y el espacio de direcciones es de 32 bits.

Encabezado IPv4

El datagrama IPv4 se divide en encabezado y la carga útil; donde el encabezado se forma por una parte de 20 bytes y una opcional de longitud variable, en la Figura 16 se puede observar la cabecera; en esta los bits se transmiten de izquierda a derecha y de arriba hacia abajo.

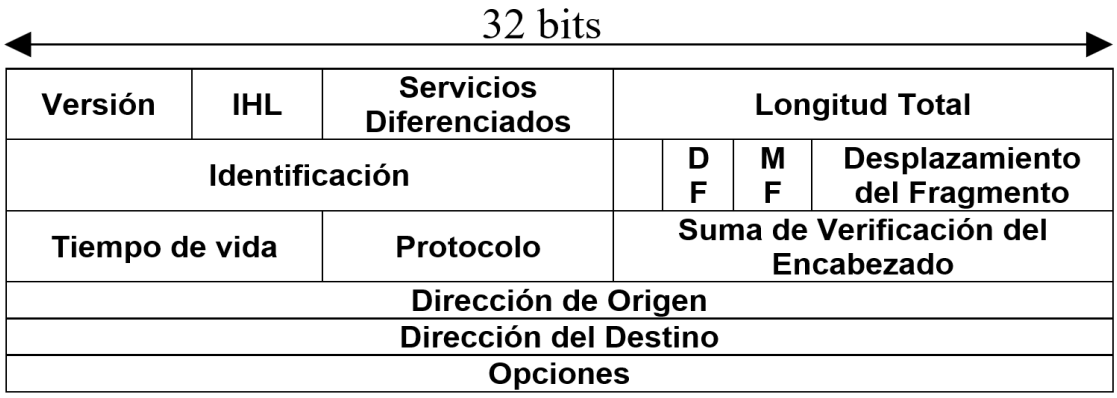


Figura 16. Encabezado IPv4 [15]

El Campo Versión indica, como su nombre lo dice, la versión del protocolo del datagrama para este caso la versión número 4. Aunque ya existe el protocolo IPv6 desde hace más de diez años, la versión 4 sigue siendo más utilizada hoy en día.

El siguiente campo IHL contiene la longitud de la cabecera que puede variar entre 20 y 60 bytes; Por obvias razones es importante, pues cada host que recibe un paquete IPv4 debe identificar el tamaño de la cabecera.

El campo Servicio Diferenciado determina la calidad del servicio, por ejemplo, para la voz se requiere velocidad, y para la transferencia de archivos que no haya errores.

En el campo de Longitud Total se incluye todo el datagrama, es decir, tanto la cabecera como los datos, y la longitud máxima es de 65535 bytes.

El campo Identificación sirve para que el host destino determine a que datagrama pertenece un fragmento recién llegado, todos los fragmentos de un paquete tienen el mismo valor.

El campo DF (No fragmentar) define si se fragmenta o no el paquete, de esta forma es posible conocer el paquete más grande que se transmite sin necesidad de fragmentarse; Si este campo se encuentra activo, el emisor da por hecho que se enviara el paquete en un solo fragmento.

Por otra parte, MF (Mas fragmentos) está activo en todos los fragmentos a excepción del ultimo, con el fin de saber cuándo se han entregado todos los fragmentos.

El campo de Desplazamiento del fragmento funciona como una secuenciación, para identificar a que parte del paquete pertenece cada fragmento; es importante señalar que es posible dividir un datagrama en hasta 8152 fragmentos.

La cantidad de saltos que puede dar un datagrama en la red se define en el campo Tiempo de Vida. El campo Protocolo hace referencia al Protocolo superior (TCP/UDP).

En el campo Suma de Verificación (Checksum) se verifica si el paquete no fue alterado o dañado en el camino. Los campos de direcciones origen y destino que constan de 32 bits.

En los campos Dirección de origen y Dirección de destino se indica la dirección IP del emisor y el receptor.

Finalmente, el campo de opciones contiene funciones no tan comunes como marcas de tiempo, seguridad e incluso necesidades de enrutamiento (Enrutamiento de Origen y grabación de ruta). [21]

Formato de Dirección IPv4

Cada computadora tiene asignada una dirección lógica de 32 bits que se divide en dos partes, una de ellas se refiere al grupo de red o subredes y la otra a un grupo de host, característica que vuelve a las direcciones IP jerárquicas. Una dirección IP no se refiere específicamente a un host; se trata de una interfaz de red;

Por lo tanto, es posible tener un host en dos redes que contará con dos direcciones IP.

La porción de red de una dirección IP tendrá el mismo valor para todos los hosts de dicha red, y el prefijo de una dirección IP es el bloque que abarca un espacio contiguo de direcciones.

Las direcciones IP constan de 4 segmentos de 8 bits separados por puntos escritos en forma decimal, por ejemplo: 148.134.79.2

El prefijo se escribe con una diagonal al final de la dirección IP seguido de la longitud en bits de la porción de red, es decir, si se tiene un /16, 16 bits corresponden a la parte de red y 16 a la de host. En la práctica, los enrutadores no son capaces de determinar el prefijo solo teniendo la dirección IP, por lo tanto, estos prefijos se transmiten en los protocolos de enrutamiento.

El prefijo se expresa con 1s en los bloques de la dirección IP que correspondan a la red, a esto se le conoce como “máscara de subred”, en la siguiente Figura (17) se puede apreciar este concepto de manera gráfica para una dirección /16.

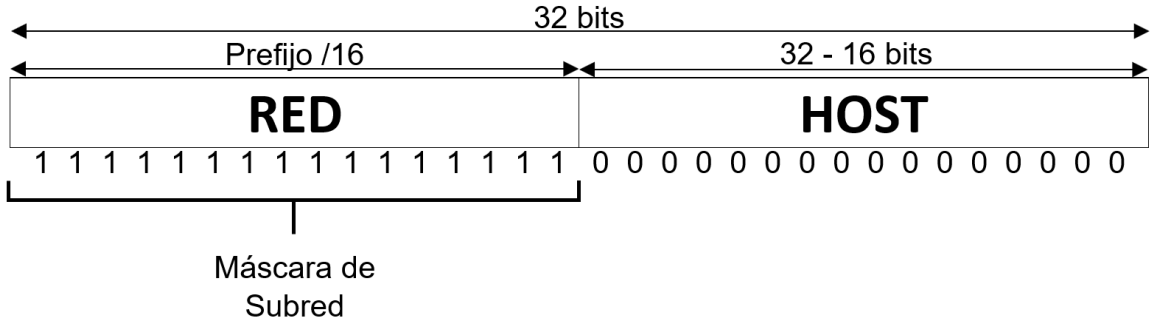


Figura 17. Máscara de Subred

Las direcciones del protocolo de Internet se han vuelto de suma importancia, pues son un recurso para el funcionamiento de Internet; Estas direcciones son asignadas a diferentes interfaces de red de dispositivos que se conecten a la red; Ya sean, computadoras, teléfonos inteligentes, enrutadores, impresoras, televisiones inteligentes, servidores, sensores, entre otros. [22]

Hoy en día cada uno de los dispositivos conectados a internet tienen una dirección IP y como se ha mencionado anteriormente, el crecimiento de dispositivos conectados a internet ha sido exponencial, por lo que ha surgido la necesidad de un gran número de direcciones IP. El protocolo de internet IPv4 cuenta con 4,294,967,296 direcciones, y según LACNIC (Registro de Direcciones de Internet

para América Latina y Caribe) quienes son los encargados de la asignación y administración de los recursos de numeración de Internet en la región, se dispone de menos del 5%.

La jerarquía tiene una desventaja, y es que conlleva al desperdicio de direcciones si no se gestionan adecuadamente, es decir, si se realiza una asignación de bloques grandes de direcciones es muy probable que no todas se utilicen.

Los números de red son administrados por ICANN (Corporación de Internet para la Asignación de Nombres y Números) quien a su vez divide el espacio de direcciones y las delega a autoridades regionales quienes se encargan de repartir las direcciones IP a Proveedores de Servicios de Internet (ISP) o a compañías. [23]

Clases de red IPv4

En un principio, las direcciones IP se clasificaban en grupos, como se puede ver a continuación (Figura 18), la clase E fue reservada para uso futuro.

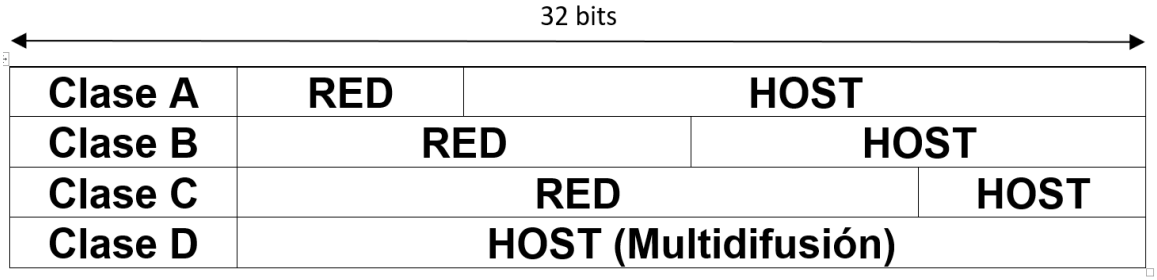


Figura 18. Clases de Red

Para la clase A, el rango de direcciones es de 1.0.0.0 – 127.255.255.255, equivalente a 128 redes con 16 millones de host por red; El rango de direcciones para la clase B va de 128.0.0.0 – 191.255.255.255, con 16384 redes con 65536 host por red. La clase C comúnmente usada para redes de área local (LAN) permite 2 millones de redes con 256 hosts en cada una, su rango va desde 192.0.0.0 – 223.255.255.255. Finalmente, la clase D soporta multidifusión y su rango es de 224.0.0.0 – 239.255.255.255.

El problema de esta jerarquía era notable, pues una red clase A era demasiado grande mientras que una red clase C podía ser demasiado pequeña, por este motivo hubo muchas compañías a las que se les asignaron bloques de clase B, y en muchos casos, este espacio de direcciones no se usó por completo. Con el

paso de los años surgieron nuevas técnicas para cubrir este problema, por ejemplo, el Enrutamiento Inter dominio sin Clases (CIDR).

Agotamiento IPv4

Es un hecho que el Internet se ha vuelto de uso cotidiano, algo que no era esperado en sus inicios, y por este motivo no se contempló su crecimiento exponencial; IPv4 sigue siendo el protocolo más usado en el mundo. Los últimos cinco bloques de direcciones IPv4 con 16,777,216 direcciones por bloque (/8) fueron asignados en febrero del año 2011 por la IANA para cada uno de los RIRs, lo cual se conoció como “el principio del fin”. [24] [25]

Ante los primeros estudios sobre la escasez de IPv4, surgieron diferentes técnicas para atrasar la fecha en que las direcciones IPv4 se agotaran por completo.

La primera medida que tomó la IANA fue comenzar a asignar bloques de direcciones sin clases (CIDR, Ruteo Inter dominio Sin Clases), pues con la asignación por clases (A, B y C) se desperdiciaban muchas direcciones IP; Esta medida se estandarizó en 1993 (RFC 1518 y RFC 1519) aunque solo sirvió para disminuir el agotamiento exponencial que se estaba dando. [26]

Otra de las técnicas empleadas, es la **asignación dinámica de direcciones IP**, este proceso consiste en asignar una dirección IP a una computadora cuando esta se enciende y consecuentemente entra en la red; Cuando la computadora sale de la red, o se apagaba, la dirección IP que tenia se reasigna a otro dispositivo que entre a la red en ese momento. El problema de usar esta técnica surge en redes comerciales, donde los equipos se mantienen conectados a la red.

NAT (Traducción de Direcciones de Red)

Otra técnica que es muy usada actualmente es NAT (Traducción de Direcciones de Red, del inglés Network Address Translation); Esta técnica es principalmente empleada por los ISP quienes le asignan una sola dirección IP pública a cada casa o negocio para acceder a internet. El procedimiento para acceder a Internet con NAT inicia con la traducción de una de las direcciones IP de la red interna de la casa o negocio a una dirección IP pública, de esta manera varios equipos de una red local comparten una dirección IP pública. NAT se estandarizó en 1994 en el RFC 1631. [27] [28]

Este método se ha usado como una solución temporal ante el agotamiento de direcciones IPv4, y aunque ha sido de gran ayuda, muchos expertos no están de acuerdo con el uso de NAT por varias razones:

- No cumple el modelo arquitectónico de IP, cada máquina debe estar identificada con una dirección IP mundialmente.
- No cumple el esquema de conexión extremo a extremo (end-to-end).
- Se pierde la esencia de una red sin conexión a una red orientada a conexión, pues NAT debe mantener las asignaciones de cada conexión.
- Con NAT se pierde la independencia de capas (Red y Transporte).

Estos son los inconvenientes del uso de NAT, de cualquier forma, sigue siendo muy utilizado en negocios y hogares. [29][30]

Actualmente el Registro de Direcciones de Internet para América Latina y Caribe (LACNIC) al que México Pertenece se encuentra en la tercera fase de agotamiento de direcciones IPv4, esta fase inició el 15 de febrero del 2017, en la que no se le asignaran más recursos IPv4 a Organizaciones que ya tengan estos recursos asignados por LACNIC; Ya se está hablando de un agotamiento lo que promueve el uso de la nueva versión del Protocolo de Internet (IPv6). En LACNIC se ha hecho una proyección del fin de esta cuarta fase de agotamiento, la cual apunta a diciembre del 2019, tal como se puede observar en la Figura 19 obtenida de la página de LACNIC; Como se puede apreciar hasta el 16 de septiembre del 2018 quedan disponibles 1,899,008 direcciones IP. [31] [32]

Figura 19. Proyección Agotamiento de IPv4 en LACNIC (Consultado el 16/Sep/2018) [32]

IPv6

Es el protocolo de Internet versión 6, definido en el RFC 2460 en diciembre de 1998; Ya existía una versión número cinco que había sido diseñada con fines experimentales y nunca fue más allá. Los estudios sobre un nuevo protocolo surgen ante el agotamiento de IPv4 en 1990, es entonces que la IEFT (Grupo de Trabajo de Ingeniería de Internet) comienza a trabajar buscando resolver diferentes problemas además del agotamiento de direcciones, por ejemplo, el proporcionar más seguridad, realizar un protocolo con una cabecera más simple y que ayude a tener un procesamiento rápido, que fuera posible que pueda coexistir con IPv4, etc.

Después de muchas propuestas y reuniones de discusión se llegó en 1993 a lo que hoy conocemos como IPv6, logrando cumplir los objetivos que la IETF se propuso al inicio de su investigación. [33] [34]

- Las direcciones en IPv6 son más largas (128 bits), con 8 bloques de 16 bits separados por "**:**", es compatible con protocolos como TCP, UDP, ICMP, IGMP, BGP y DNS.
- IPv6 cuenta con una cabecera más eficiente y simple que IPv4, característica que permite un procesamiento más rápido en los enrutadores.
- Con esta nueva versión se tiene autenticación y privacidad.
- Mejora en cuanto a calidad de servicio (QoS) debido al amplio contenido de multimedia en internet.

Con el espacio de direcciones que cuenta IPv6 es equivalente a cubrir toda la superficie de la Tierra con $7x10^{23}$ direcciones IP por metro cuadrado, lo cual hace muy poco previsible el agotamiento de estas.

Historia IPV6

El protocolo IPv6 surgió debido a que la tasa de asignación de direcciones IPv4 era tan alta que Internet se quedaría sin más direcciones IPv4 en aproximadamente 5 años; Esto fue reconocido por Frank Solensky en agosto de 1990. Debido a esto se tomaron las siguientes cuatro medidas de forma inmediata:

- Los Registros Regionales de Internet (RIR) dejaron de asignar direcciones Con Clase, y comenzaron a asignar direcciones de tipo Enrutamiento Inter dominio Sin Clases (CIDR), esto disminuyó inmediatamente el agotamiento que se preveía.
- Se buscó recuperar las direcciones ya alocadas pero que no eran usadas.

- La IETF invitó a los expertos a trabajar en una siguiente generación del protocolo IPv4.
- Se plantearon los principales fundamentos detrás del funcionamiento de NAT (Traducción de Direcciones de Red).

En ese entonces no fue posible hacer una proyección de cuánto tiempo se alargaría el uso del protocolo IPv4. Hoy sabemos que NAT es el principal responsable de extender el tiempo de IPv4 por más de 20 años. [35]

IPv6 fue propuesto por Bob Hinden y Steve Deering con su respectiva especificación en 1998. En los siguientes diez años surgieron trabajos relacionados (DHCPv6, DNS AAAA, modificación de cabeceras TCP/UDP, implementación en Linux, MacOS y Windows). [36]

En el año 2011 iniciaron las fases de agotamiento de direcciones IPv4 para la Región de Asia y Pacífico (APNIC), en el 2012 para la región de Europa y Medio Oriente (NCC), en Latino América y el Caribe (LACNIC) en el 2014, en Norte América (ARIN) en el año 2015 y en la Región correspondiente a África (AfriNIC) en el año 2017. [37]

Encabezado IPv6

Como se puede apreciar en la Figura 20, la cabecera IPv6 es más simple en comparación con IPv4, ahora solo se tienen ocho campos, mientras que con IPv4 eran 14, teniendo un espacio de 40 bytes (No variable como en IPv4).

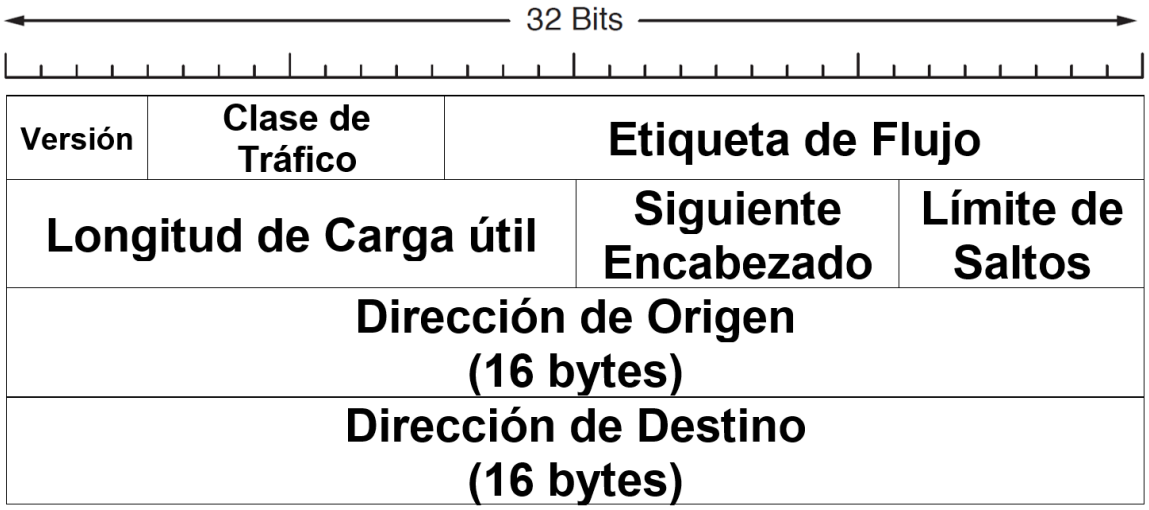


Figura 20. Encabezado IPv6 [38]

El campo versión indica la versión del protocolo en cuestión, en este caso es seis (IPv6); En el campo Clase de Tráfico se definen los servicios diferenciados con fines de calidad y servicio.

Después sigue el campo Etiqueta de Flujo, si este campo tiene un valor diferente de cero quiere decir que se requiere un tratamiento específico, pueden ser requisitos de retardo, esto se establece por adelantado, y así los enrutadores verifican en sus tablas el tipo de tratamiento que se le debe dar a los paquetes.

La tarea de identificar cuántos bytes hay después del encabezado es específica del campo Longitud de Carga Útil.

El siguiente campo es el responsable de poder simplificar la cabecera, este es el campo Siguiente Encabezado, cuenta con seis encabezados adicionales de extensión (Autenticación, Fragmentación, Enrutamiento, entre otros). Si él se trata del último encabezado, entonces el siguiente será el protocolo de transporte.

El campo Límite de saltos es similar a IPv4 (Tiempo de vida), donde se busca que los paquetes no duren por siempre.

Por último, se tienen los campos de Dirección de Origen y Destino, aquí se indican las direcciones IP de las interfaces de la red de origen y destino ahora con un espacio de direcciones mucho mayor ($2^{128}\ direcciones$). [39]

Comparando las cabeceras de ambos protocolos (IPv4 e IPv6) es posible determinar porqué se eliminaron algunos campos, por ejemplo, El campo de longitud de cabecera (IHL) no era necesario pues ahora con IPv6 es un tamaño constante; El campo Siguiente Encabezado reemplazo al campo Protocolo adicionando mejoras como seguridad, autenticación, etc.

Los campos encargados de la fragmentación fueron eliminados, pues con IPv6 los hosts determinan el tamaño de paquete a usar de manera dinámica, dependiendo de la MTU (Unidad Máxima de Transferencia) de las diferentes rutas. En IPv4 la fragmentación se daba en cada enrutador; Y en IPv6, la fragmentación se define al principio, por ejemplo, si al llegar un paquete a un enrutador, este rebasa la MTU, manda un mensaje de error al emisor solicitando que divida los paquetes futuros para ese destino; De esta manera (enviando los paquetes de tamaño adecuado al principio) se vuelve más eficiente el sistema. El tamaño mínimo de los paquetes aumento de 576 a 1280 bytes.

Se eliminó el campo de suma de verificación, el cual también implicaba un gran costo, pues esta suma de verificación también se realiza en la capa de enlace de datos y de transporte.

Encabezados de Extensión

Hay seis tipos de encabezados de extensión, son opcionales, en caso de que exista más de uno, van después del encabezado fijo y en el siguiente orden.

- Opciones salto por salto
- Opciones de Destino
- Enrutamiento
- Fragmentación
- Autenticación
- Carga útil de seguridad cifrada

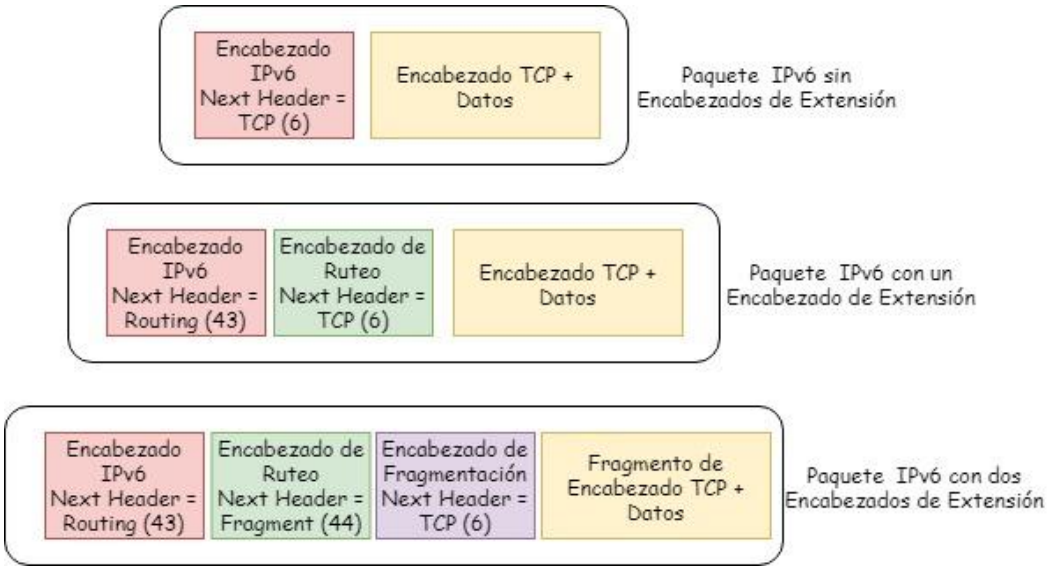


Figura 21. Encabezados de Extensión Agregados

Opciones Salto por Salto. – Usado para llevar información opcional que sea examinada en cada nodo a través de la ruta del paquete. Se identifica con un valor de 0 en Siguiente encabezado. Tiene el siguiente formato.

Siguiente Cabecera	Hdr Ext Len
Opciones	

Opciones de Destino. – Llevan información que solo el nodo destino podrá examinar. Se identifica con un valor de 60 en Siguiente encabezado.

Siguiente Cabecera	Hdr Ext Len	
Opciones		

Enrutamiento. – Se da una lista de los nodos por los que debe pasar un paquete para llegar a su destino. Se identifica con un valor de 43 en Siguiente encabezado.

Siguiente Cabecera	Hdr Ext Len	Tipo de Ruteo	Segmentos
Especificación de Tipo de Datos			

El campo Next Header (Encabezado Siguiente) Identifica el tipo de cabecera después del encabezado de enrutamiento. Hdr Ext Len determina la longitud del encabezado. Routing Type (Tipo de Enrutamiento) identifica el tipo de enrutamiento. El campo Segments Left (Segmentos) determina los segmentos de ruta restantes, o los nodos intermedios que no se han visitado. [40]

Fragmentación. – En IPv4, cada enrutador realizaba esta función dependiendo de la Unidad Máxima de Transferencia del segmento en el que estaban conectados, en IPv6 ya no, cuando un enrutador recibe un datagrama de tamaño mayor a la MTU, se envía un mensaje al emisor mediante ICMP, para que la fragmentación se haga desde el inicio (end-to-end). Se identifica con un valor de 44 en Siguiente encabezado. Su formato es el siguiente, y funciona de manera similar a IPv4.

Siguiente Cabecera	Reservado	Fragmento Offset	Res	M
Identificación				

El campo Siguiente Cabecera define el tipo de cabecera inicial de la parte a fragmentar. El siguiente campo (Reservado), es para usos futuros es inicializado a

cero para transmisión e ignorado para recepción. Fragmento Offset se refiere al inicio de la parte a fragmentar del paquete original. El campo Res es otro campo reservado para usos futuros. La bandera M define si se deben realizar más fragmentos o si es el último fragmento.

Finalmente, el campo Identificación debe identificar los fragmentos para poder ser reensamblados en el destino de forma correcta.

Autenticación. – Brinda Integridad, sin conexión y Autenticación a los paquetes de datos IP. Se identifica con un valor de 51 en Siguiente encabezado. [41]

Siguiente Cabecera	Longitud de Carga de Datos	RESERVADO
Índice de Parámetros de Seguridad (SPI)		
Numero de Secuencia		
Valor de Verificación de Integridad		

Carga útil de Seguridad Cifrada. – Encargado de la Autenticidad de Origen, integridad y protección de confidencialidad de los paquetes.

Índice de Parámetros de Seguridad (SPI)		
Numero de Secuencia		
Carga de Datos (Variable)		
Relleno (0 a 255 Bytes)		
	Longitud de Relleno	Siguiente Cabecera
Valor de Verificación de Integridad		

El campo Índice de parámetro de seguridad o SPI es de 32 bits, y se encarga de asociar el paquete con una determinada asociación de seguridad; El campo Número de secuencia es de 32 bits.

Luego en el campo Datos de carga útil (variable) para el caso de modo transporte, incluye el segmento de la capa de transporte, mientras que si está en modo túnel incluye un paquete IP; Este campo se encuentra cifrado.

En la sección de Relleno (0-255 bits) se deja espacio para completar hasta el múltiplo de octetos necesario; El campo Longitud del relleno es de 8 bits.

El campo Siguiente cabecera (8 bits), identifica el tipo de datos que se encuentra la sección datos de carga útil.

Finalmente, en Datos de autenticación (variable), contiene el valor de comprobación de integridad calculado sobre el paquete.

Las cabeceras de Extensión llevan un orden de ejecución, es decir, si no se identifica el valor que contiene el campo “siguiente cabecera” el paquete se descarta y mediante ICMPv6 (Protocolo de Mensajes de Control de Internet) se notifica al emisor. [42]

1. Cabecera IPv6.
2. Cabecera de Opciones Hop-by-Hop.
3. Cabecera de opciones de destino.
4. Cabecera de enrutamiento
5. Cabecera de Fragmento.
6. Cabecera de autenticación.
7. Cabecera de carga útil de seguridad encapsulada.
8. Cabecera de Opciones de Destino (para opciones a ser procesadas solo por el destino final del paquete).
9. Cabecera de capa superior.

Direccionamiento

En IPv6 existen tres clases de direcciones: Unidifusión (Unicast), Multidifusión (Multicast) y Difusión por proximidad (Anycast). [43]

1. Unidifusión. - Se identifica una interfaz de un solo nodo, en esta clasificación se tienen otros tipos de direcciones; entre ellas están, Link local, Unique Local, Global, Loopback, No especificada y Mapeada.
    - **Link Local:** No se enrutan fuera del segmento local, su función principal consiste en brindar direccionamiento automático cuando no exista un servidor DHCP. Este tipo de direcciones tienen el prefijo FE80::/64.
      El segmento que corresponde al ID de interfaz se hace con el formato EUI-64, en el cual se toman 48 bits de la dirección MAC y se agregan 16 bits predefinidos (FFFE).

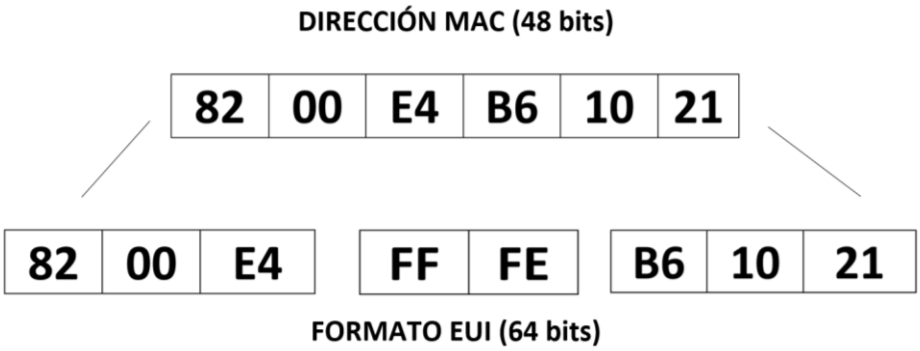


Figura 22. Formato EUI (64 bits)

- Unique Local: Se usan para enlaces locales, y son únicas, su enrutamiento es limitado (No Internet), se definen con el prefijo FC::/7. Siempre que sea local, el octavo bit del prefijo lo indica, cambiando a FD::/8.
- Global: Son las direcciones públicas, es decir, las que son enrutables en internet; El prefijo es 2000::/3.
- Loopback: Este tipo de dirección permanece dentro del host, es decir, los enrutadores no transmiten paquetes con esta dirección. La dirección es ::1/128.
- No especificada: Indican que no hay una dirección IPv6 presente; Aunque es posible que el host la use como dirección de origen hasta que reciba una dirección IPv6 sin que se envíe entre los enrutadores. Está definida como ::/128.
- Mapeada: Representan la transmisión o recepción de paquetes IPv4, después del prefijo se agrega la dirección IPv4 (::FFFF:198.162.12.2).

2. Multidifusión. - La cual consiste en identificar a grupos de interfaces de nodos distintos y de esta manera el paquete enviado lo reciban los miembros del grupo de multidifusión. Su prefijo es FF00:/8. (NOTA: En IPv6 no existe Broadcast).
3. Difusión por proximidad. - donde se definen por la cercanía del remitente, además de que también identifican grupos de interfaces de nodos diferentes. [44]

Como se ha mencionado anteriormente, una dirección IPv6 tiene un tamaño de 128 bits, y se divide en 8 segmentos de 16 bits separados por dos puntos. [38]

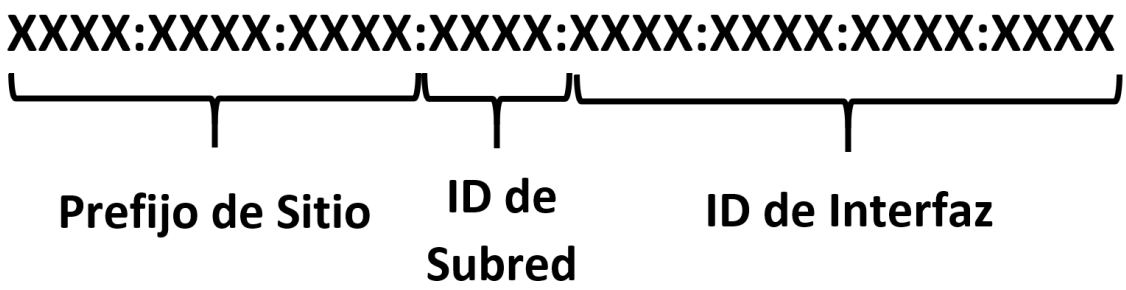


Figura 23. Definición de Direcciones IPv6

Los primeros 48 bits determinan el prefijo de sitio, el cual define la topología pública que el ISP o el Registro Regional de Internet suelen asignar al sitio. Los siguientes 16 bits corresponden al ID de subred que el administrador asigna al sitio, pues es parte de la topología privada o interna.

Los últimos 64 bits conforman al ID de la interfaz o token, el cual puede configurarse automáticamente desde la dirección MAC de la interfaz. [45]

La notación de las direcciones IPv6 se divide en ocho bloques de 16 bits separados por "**:**" y cada uno de los bloques se escribe en forma hexadecimal tal y como la siguiente dirección:

5000:0000:0000:0000:0243:332D:ABCD:EF30

Como se puede apreciar, las direcciones son muy largas, y en este caso con muchos ceros; Existen algunas reglas para reescribir estas direcciones como omitir ceros a la izquierda dentro de cada bloque y reemplazar los bloques de ceros que sean consecuentes con "**::**". Y siguiendo el ejemplo anterior, la dirección se reescribiría así:

5000::243:332D:ABCD:EF30

Protocolo ICMPv6

Funciona de manera similar a IPv4, para enviar mensajes entre diferentes equipos de red, entre las mejoras que se agregaron está el protocolo de Descubrimiento de Vecinos (ND) que usa los mensajes de ICMPv6 para definir las direcciones de los dispositivos vecinos en la capa de enlace además del soporte a IPv6 móvil.

El protocolo ND puede usarse tanto en un enrutador o nodo como en un host. Si se utiliza en un enrutador se puede indicar al host cual es el nodo adecuado para dar un salto siguiente (next hop) para el destino del paquete fuera del área local. Al efectuarse en un host, se descubren los enrutadores vecinos. [46]

Existen cuatro tipos de mensajes de error en ICMPv6:

- Destino Inalcanzable (tipo 1)
- Paquete demasiado grande (tipo 2)
- Tiempo Excedido (tipo 3)
- Problema de Parámetro (tipo 4)

En la siguiente tabla (4) se pueden apreciar los códigos de cada mensaje de error y su significado.

Número de Mensaje	**Tipo de Mensaje**	**Campo de Código**
1	Destino Inalcanzable	0 = No hay ruta al destino. 1 = La comunicación con el destino es administrativamente prohibida. 2 = Más allá del alcance de la dirección de origen. 3 = dirección inalcanzable. 4 = puerto inalcanzable. 5 = Dirección de origen fallida. 6 = Rechazar ruta al destino.
2	Paquete demasiado Grande	Campo de código establecido en 0 por el remitente e ignorado por el receptor
3	Tiempo Excedido	0 = Límite de saltos excedido en tránsito. 1 = tiempo de reensamblado del fragmento excedido.
4	Problema de Parámetro	0 = campo de encabezado erróneo encontrado. 1 = Siguiente tipo de cabecera no reconocido encontrado. 2 = Opción IPv6 no reconocida encontrada.

Tabla 4 Códigos Mensaje de Error ICMPv6

Protocolos de Ruteo

El ruteo es exclusivo de la capa de red, y el dispositivo que se encarga de transmitir los datagramas de datos es el enrutador; Su función es comparar la dirección destino del datagrama en cuestión para que posteriormente se compare con los prefijos que el enrutador contiene en la tabla de enrutamiento y finalmente reenviar el datagrama. La tabla de enrutamiento aloja información que sirve para intercomunicar los hosts. El enrutador después de comparar la dirección destino con la información en la tabla de enrutamiento puede descartar el paquete, reenviarlo a través de una de las interfaces de red a las que está conectado, o pasar el paquete al nivel superior en el host local.

Los protocolos se pueden clasificar por cómo funcionan y por la zona de la red donde se implementan. Si nos basamos en la zona por un lado están los Protocolos de Ruteo Interior (IGP), que son usados dentro de un sistema autónomo; Y por el otro los Protocolos de Ruteo Exterior (EGP) encargados de la comunicación entre una red local con redes remotas (Internet).

En cuanto a su funcionamiento (método para calcular y encontrar rutas) están los Protocolos Vector Distancia que determinan la dirección y numero de saltos hacia un enlace en Internet. Los protocolos Estado de Enlace usan el algoritmo SPF (Camino Corto Primero, Shortest Path Fist) con el fin de formar la topología del segmento donde se encuentra el enrutador del destino. Y finalmente los Protocolos Híbridos balanceados que combinan a los dos anteriores. [47]

RIPng (Protocolo de Información de Ruteo)

Este protocolo es usado dentro de los sistemas autónomos (IGP), y usa el método vector distancia, el cual arroja una métrica que define la dirección y ruta más rápida automáticamente. Las actualizaciones y los tiempos de expiración para las rutas que hayan sido desconectadas se mantuvieron con respecto a IPv4 (30 y 180 segundos respectivamente). El algoritmo que usa es vector distancia Bellman-Ford (Al igual que en IPv4).

En la tabla 5 se muestran los cambios y características nuevas que surgieron para enrutar a IPv6.

Propiedad	Explicación
Protocolo de Transporte	Uso de UDP para RIPng
Número de Puerto	El puerto para UDP es el 521
Salto Siguiente (Next Hop)	Es la dirección de enlace local (link-local) IPv6 de la interfaz del enrutador que anuncia el prefijo de red
Límite de Saltos (Hop Limit)	El límite de saltos de paquete está configurado en 255 para las actualizaciones RIP.
Anuncio de rutas	Se hacen con longitud y métrica.
Número de Rutas	Depende de la Unidad Máxima de Transferencia

Tabla 5 Características nuevas RIPng [48]

OSPFv3 (Primer Camino Más Corto)

Es un protocolo de estado de enlace, es decir, cada enrutador identifica cuáles son sus vecinos y a que distancia (Saltos) se encuentra de ellos. Entre sus características principales encontramos que es un protocolo abierto, es decir que brinda interoperabilidad para redes en las que existen diferentes marcas.

Otra característica bastante importante es que es un protocolo de convergencia rápida, esto quiere decir que cuando exista algún cambio en la red las tablas de enrutamiento se actualizan rápidamente para generar nuevas rutas. La convergencia rápida se debe a que los segmentos de red se pueden separar en diferentes Áreas, de esta manera, un cambio en una subred no implicaría una actualización de todos los enrutadores. [49]

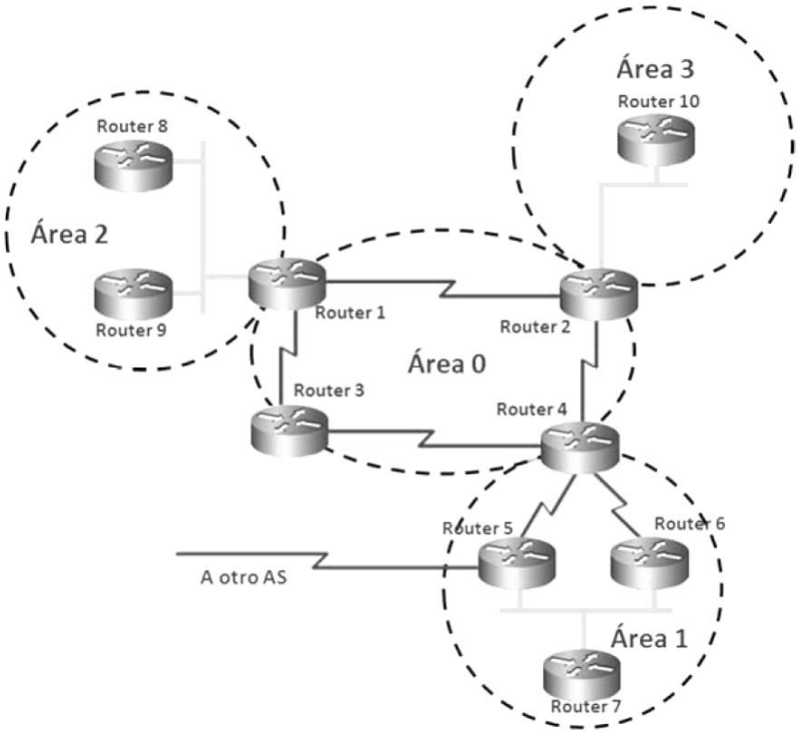


Figura 24. Áreas en OSPFv3

Es un protocolo al que se le puede aplicar el algoritmo MD5 para tener autenticación, lo que lo vuelve seguro.

Otra característica muy importante en OSPF es el uso de métricas, pues se toma en cuenta el ancho de banda para llegar más rápido a un destino en lugar de solo los saltos entre enrutadores.

Mecanismos de Transición

Existen diferentes escenarios que nos permiten lograr coexistencia entre la versión 4 y la versión 6 del Protocolo de Internet; La razón fundamental de llevar a cabo estos mecanismos es simple y son los costos de inversión; si alguna organización o empresa quiere actualizarse a IPv6 puede hacerlo de manera gradual, sin que se deba realizar un gasto sustancial en infraestructura. Los mecanismos de transición permiten que exista una transición suave. Es necesario que el despliegue del protocolo IPv6 sea proporcional al crecimiento del internet. [50] [51]

Esta transición representa un gran desafío, y existen varias soluciones o técnicas, como son: Túneles (Tunneling), Doble Pila (Dual Stack) y Traducción (Translation).

Túneles

Soportan la conexión igual a igual a través de una red diferente; es decir, mantienen el modelo extremo a extremo en el que se basa Internet. Los Túneles tienen la capacidad de habilitar la conectividad IPv6 en una red IPv4 y viceversa.

Las operaciones de un Túnel son la encapsulación, des encapsulación y señalización del punto final del Túnel, sin que sea requerida alguna operación en capa superior. Para llevar a cabo esta técnica es necesario que los nodos de los extremos soporten tanto IPv4 como IPv6 tal y como se expresa en la Figura 25.

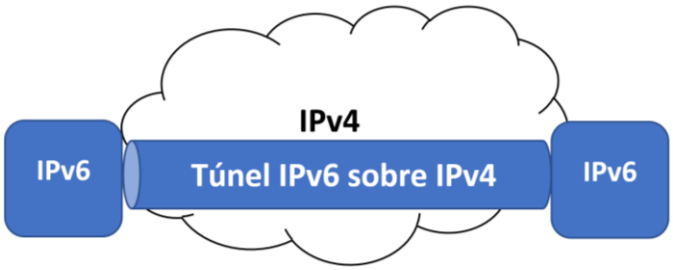


Figura 25. Esquema Túnel IPv6 sobre IPv4

Para hacer un Túnel IPv6 a través de una red IPv4 se agrega una cabecera IPv4 antes del paquete IPv6 formando un paquete resultante, el cual se envía a la dirección destino indicada en la cabecera IPv4, en el destino (IPv6) se elimina el encabezado IPv4 y se procesa el paquete como si se hubiera recibido a través de una interfaz normal habilitada para IPv6. Existen dos tipos de túneles, los configurados de manera manual y los automáticos. [52]

Los configurados de forma manual tienen la desventaja de que deben configurarse en ambos extremos, aunque sean más simples y la ruta del túnel es predecible. Por otra parte, los túneles automáticos son más complejos, existen varios mecanismos de túnel automático de IPv6 sobre IPv4 como son: 6over4, ISATAP, 6to4, Teredo, entre otros. [53]

6over4. –

Maneja a la red IPv4 como un "Ethernet virtual" para el propósito de la comunicación IPv6. Los paquetes no pasan a través de NAT, pues la dirección IPv4 se cambia con el protocolo de descubrimiento de vecinos. [54]

ISATAP. –

Transporta los paquetes IPv6 donde no existe infraestructura IPv6 nativa; ISATAP consigue que los hosts que soporten ambos protocolos (doble pila), se comuniquen con otros hosts con las mismas características, obteniendo así una red IPv6 virtual, dentro de la infraestructura IPv4. Su uso está enfocado dentro de los sitios, es decir, no comunica sitios entre sí. [55]

El formato que usa ISATAP puede obtenerse de cualquier prefijo de unidifusión (/64), de esta forma es posible el enrutamiento de IPv6 local o en Internet. La dirección IPv4 se codifica en los últimos 32 bits de la dirección IPv6. [56]

6to4. –

Una diferencia entre los túneles manuales y los automáticos es que los primeros son punto a punto, y los segundos punto a multipunto. Los túneles automáticos 6to4 no se deben configurar en dos enrutadores, sino que utilizan la infraestructura IPv4 como enlace virtual de multiacceso sin difusión (broadcast).

La dirección IPv4 embebida en la dirección IPv6 es usada para encontrar el otro extremo del túnel automático. El túnel es configurado en un enrutador de frontera en una red IPv6, donde se crea el túnel por paquete que es enviado a otro enrutador de frontera en otra red IPv6. El enrutador extrae la dirección destino IPv4 de la dirección IPv6, la cual debe comenzar con el prefijo 2001::/16, el formato es:

2002:**border-router-ipv4-address**::/48

Los enrutadores de frontera de cada extremo del túnel configurado deben soportar ambos protocolos, también se puede configurar el túnel entre un enrutador de frontera y un host. [57]

Teredo. –

La característica principal de esta tecnología de transición es que funciona detrás de los traductores de direcciones de red (NAT) IPv4, logrando cruzar uno o varios dispositivos NAT. Aquí los paquetes se envían como mensajes UDP (Protocolo de Datagramas de Usuario). De esta manera se permite que los clientes Teredo accedan a host IPv6 y hosts Teredo IPv4. [58]

Doble Pila (Dual Stack)

En esta técnica de transición, todos los componentes de la red deben soportar ambos protocolos (IPv4 e IPv6), y las aplicaciones deciden que versión utilizar. La arquitectura en doble pila es el despliegue preferido para una red con aplicaciones de ambos protocolos. El problema de implementar este mecanismo es principalmente la inversión en equipo que soporte ambos protocolos. Es simple de configurar, principalmente para cada nodo que soporte IPv4 e IPv6. [59]

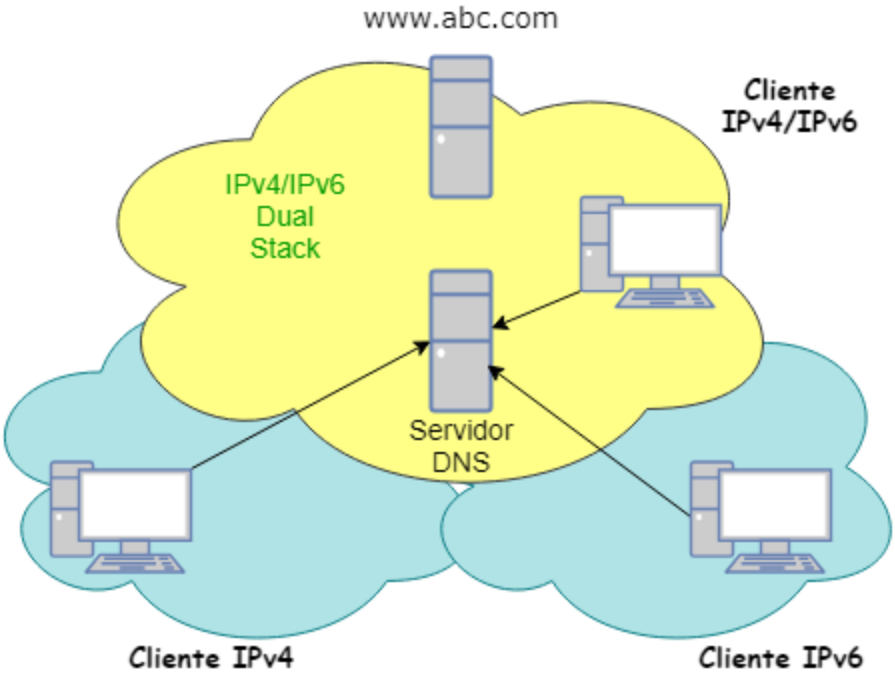


Figura 26. Mecanismo de Transición Doble Pila (Dual Stack)

Traducción

En esta técnica de traducción se utilizan dispositivos que conviertan los paquetes IPv4 a IPv6 o en sentido contrario; Uno de los problemas del uso de esta técnica es que rompe con el modelo extremo a extremo (end-to-end) e implica traducción en la capa de aplicación. Este tipo de técnicas son muy utilizadas por los proveedores de servicio de internet (ISP). Suelen emplearse en redes que utilizan un protocolo, pero quieren mantener el soporte a servicios para otro protocolo (Soporte a servicios IPv4 en hosts IPv6). [60]

NAT64/DNS64

Una de las más empleadas es NAT64/DNS64 donde para el usuario final aparece como si todos los sitios de internet fueran IPv6, y para el servidor de Internet como si las conexiones se realizaran desde un usuario IPv4 con IP compartida. Los usuarios reciben direcciones IPv6 del proveedor y eso no impide que se conecten a otros dispositivos IPv4 vía Internet.

Se usa un prefijo /96 definido para mapear las direcciones IPv4 a IPv6, este prefijo es el siguiente: 64:FF9B::/96. Aunque es posible usar cualquier prefijo, éste ya es exclusivo para este fin.

Cabe señalar que para usar este método es necesario que los usuarios cuenten con IPv6 de manera nativa. Cuando el usuario requiera acceder a contenido o dispositivos IPv4, se realiza una consulta DNS (Sistema de Nombres de Dominio); Para este caso DNS64 agrega un registro AAAA (IPv6) a la respuesta.

La ventaja de NAT64/DNS64 es que por su funcionamiento impulsa a los proveedores a actualizar la infraestructura de sus usuarios; Además de que el tráfico migrará automáticamente a IPv6 cuando todo el contenido y los servicios de internet migren a IPv6 cuenten con su registro AAAA. [61] [62]

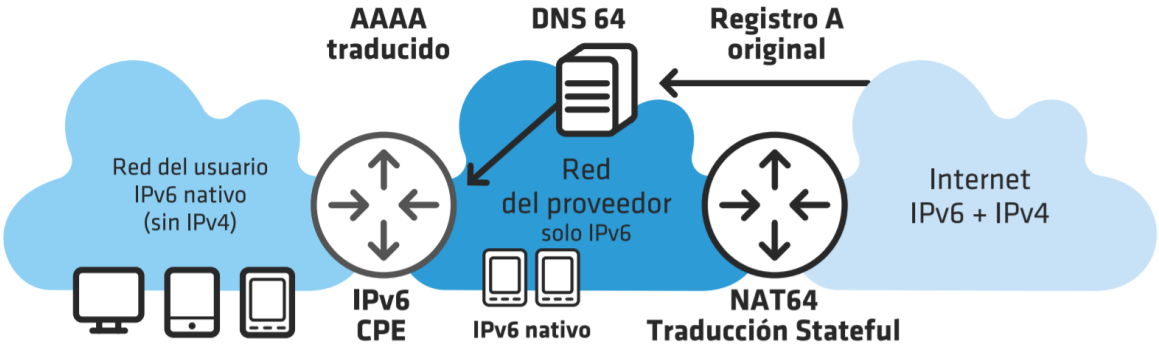


Figura 27. Esquema de NAT64/DNS64 [7]

Según estudios de LACNIC sobre el uso de NAT (Traducción de direcciones de red), en las redes IPv4 el 94% de los clientes se encuentran detrás de un dispositivo NAT. En IPv6 esto no es así, solo el 0.6% se halla detrás de un dispositivo NAT IPv6, pues el objetivo de IPv6 es que todos los dispositivos cuenten con una dirección IP pública.

Comparación entre IPv4 e IPv6

La principal característica que define al protocolo IPv6 es el amplio espacio de direcciones; pues fue lo que motivó su desarrollo, sin embargo, no es la única característica que lo define. En la Tabla 6 se muestran las principales diferencias entre el Protocolo de Internet versión 4 y versión 6.

Característica	IPv4	IPv6
Espacio de Direcciones	32 bits	128 bits
Soporte a encabezado Ipsec	Opcional	Requerido
Fragmentación	En Hosts y Routers	Solo en Hosts
Tamaño de Paquete	576 bytes	1280 bytes
Suma de Verificación en Encabezado	Si	No
Opciones en Encabezado	Si	No
Resolución de Direcciones en capa de Enlace	ARP	Mensajes de Descubrimiento de Vecinos Multidifusión
Afiliación Multidifusión	IGMP	MLD
Descubrimiento de Router	Opcional	Requerido
Uso de Broadcast	Si	No
Configuración	Manual, DHCP	Automático, DHCPv6
Consulta de nombres DNS	Usa registros A	Usa registros AAAA
Cumplimiento Modelo Arquitectónico de IP	No (Uso de NAT)	Si

Tabla 6 Diferencias IPv4 e IPv6

Uno de los problemas más significativos en cuanto al desempeño del protocolo IPv6 se debe al uso de túneles pues se forma una red superpuesta muy diferente de la red inferior y provoca diferencias en el enrutamiento; Debido a esto se considera un riesgo potencial de seguridad cuando cruzan los límites de la red. Hoy en día APNIC ha notado que IPv6 tiene mejor desempeño. En pruebas realizadas por Facebook determinaron que IPv6 es más veloz en un 15% para dispositivos móviles en Estados Unidos. [37] [63]

CAPÍTULO III: MARCO METODOLÓGICO

El método científico se tomó como base para este proyecto de investigación, y mediante éste, fue posible definir una metodología acorde a los fines del proyecto de investigación, que buscan el desarrollo de una propuesta de implementación. De esta manera se definió el Marco Metodológico que se describe a lo largo de este capítulo.

En este capítulo se presenta la metodología utilizada para el desarrollo del proyecto de investigación, con el fin de que este procedimiento pueda ser utilizado en todos los segmentos correspondientes a la capa de acceso de la red Politécnica.

Esta metodología se realizó en tres pasos, como se puede apreciar en la Figura 28.

Figura 28. Etapas de la Metodología del proyecto de investigación.

El llevar a cabo una metodología implica que exista mayor rendimiento y productividad en el desarrollo de un proyecto de investigación, además permite que las tareas se realicen con menor esfuerzo y de manera rápida; Todo esto con el fin de cumplir los objetivos establecidos. De esta manera el definir una metodología resulta imprescindible para cualquier proyecto de investigación que involucre una implementación en un sistema ya establecido. Cada una de las etapas se definen a continuación.

Diagnóstico

En esta etapa se podrán definir las problemáticas de la red de datos de la ESIMEZ, así como, establecer objetivos preliminares para el diseño de la implementación de IPv6 en la capa de acceso correspondiente al segmento de la ESIMEZ.

Para realizar el diagnóstico de la investigación, se dividió en dos pasos que se observan en la figura 29.

Figura 29. Pasos de la etapa de Diagnóstico

Al finalizar el diagnóstico, se tendrá una visión total de la problemática encontrada en la red de datos de la ESIMEZ, lo cual, permitirá el inicio del desarrollo del diseño de la implementación. A continuación, se describen cada uno de los pasos que forman parte de la etapa del diagnóstico.

Observación

En primera instancia se realiza la observación del sistema bajo investigación, a partir de ella se pueden hacer diagnósticos preliminares para definir la problemática, este es un paso importante dentro de una investigación, ya sea, exploratoria y experimental.

Para esta investigación la observación será una constante a lo largo del desarrollo del proyecto de investigación, sin embargo, esta será útil en esta etapa

que consiste en la detección de problemas superficiales de la red de datos de la ESIMEZ y así poder definir como está estructurada su topología física.

Cabe señalar que esta etapa es la que demanda más tiempo, pues no existe una documentación previa de la red de datos de la ESIMEZ, por lo tanto, se tendrá que hacer la observación de la red completa.

Durante la etapa de observación se obtendrá la información de la red, así como, sus interconexiones, parámetros y mediciones, para posteriormente ser analizadas.

Esta etapa consiste esencialmente en la captura de datos de toda la red, desde información superficial, hasta la problemática señalada por los administradores de la red. Todos los datos adquiridos son importantes para su análisis.

Análisis

A partir de la información recabada durante la observación, el siguiente paso es el análisis de ésta. El análisis de la información permitirá conocer el estado actual y las características de la red de datos de la ESIMEZ.

Entre las características más importantes de la red que se desean conocer encontramos las siguientes:

- Topología de Red Actual
- Equipos
    - Compatibilidad
    - Configuración
    - Características y Propiedades
- Gestión
- Lineamientos, Estándares y Normatividad

Una vez obtenida esta información se detectarán deficiencias, incongruencias y problemas de diseño para realizar la propuesta de rediseño de la red de datos de la ESIMEZ para poder implementar IPv6.

Una vez finalizado el análisis de la red y haber identificado las carencias para implementar IPv6 en ella, será momento de comenzar con el desarrollo del rediseño de la red y la propuesta de implementación de IPv6 en ESIMEZ; Pues ya será posible proponer esta propuesta y rediseño con una base de argumentos sólidos.

Desarrollo

Una vez definida la problemática de la red para implementar IPv6, es tiempo de formular una propuesta con base en la información obtenida en la etapa del diagnóstico.

Durante esta etapa se analizarán las posibilidades existentes para implementar IPv6 en la red de datos de la ESIMEZ, para posteriormente proponer escenarios viables y realizar pruebas con ellos, de esta manera, se determinará cual es la mejor opción y a partir de ella hacer un diseño y una propuesta de implementación óptima de acuerdo con los equipos y las necesidades de la red.

Esta etapa de desarrollo se divide en dos (Análisis de posibilidades y Diseño y Propuesta) como se observa en la Figura 30.

Figura 30. Pasos de la etapa de Desarrollo

Análisis de Posibilidades

Es común que un problema no tenga una sola solución posible, por esta razón es necesaria la exploración de distintas soluciones, para determinar cuál es la mejor entre ellas.

En este caso, las soluciones para este proyecto de investigación son múltiples, ya que esto dependerá de distintos factores, como son:

- Administradores de la Red
- Personal Técnico
- Equipos
- Mecanismos de Transición
- Estructura y Topología de la Red
- Presupuesto
- Entre Otros.

Al realizar el análisis de las diferentes soluciones, se podrá determinar cuál o cuáles son las más viables.

Al finalizar esta etapa se tendrá que haber elegido la mejor opción para que a partir de ella se haga una propuesta formal para la implementación de IPv6 en la red de datos de la ESIMEZ.

Diseño y Propuesta

Una vez determinada la opción más viable para implementar IPv6 dentro de la red de datos de la ESIMEZ, solo queda realizar el diseño y la propuesta que permitirá esto.

De la opción elegida será necesario plantear escenarios de implementación, con esto, se podrá definir cuál es la mejor estrategia para la implementación de IPv6 en la red de datos de la ESIMEZ, los escenarios podrán ser: Modelos, Maquetas, Simulaciones, etc.

Estos escenarios permitirán conocer si es necesario adquirir nuevos equipos, cambiar la topología de red, reconfigurar equipos, entre otras acciones que modifiquen el estado actual de la red.

Al finalizar el diseño de la mejor opción para la implementación de IPv6, se tiene que realizar la propuesta formal a los administradores de la red para que aprueben o propongan modificaciones antes de ser implementado.

Implementación

En esta etapa se realizará un plan o programa de implementación, dado que, es muy difícil o imposible cambiar una red de telecomunicaciones por completo al mismo tiempo. Por lo que se requiere que se creen fases de implementación que no comprometan el funcionamiento de la red, ya que, la red se encontrará en

servicio mientras se realizan los trabajos de implementación. Las etapas de Implementación se observan en la Figura 31.

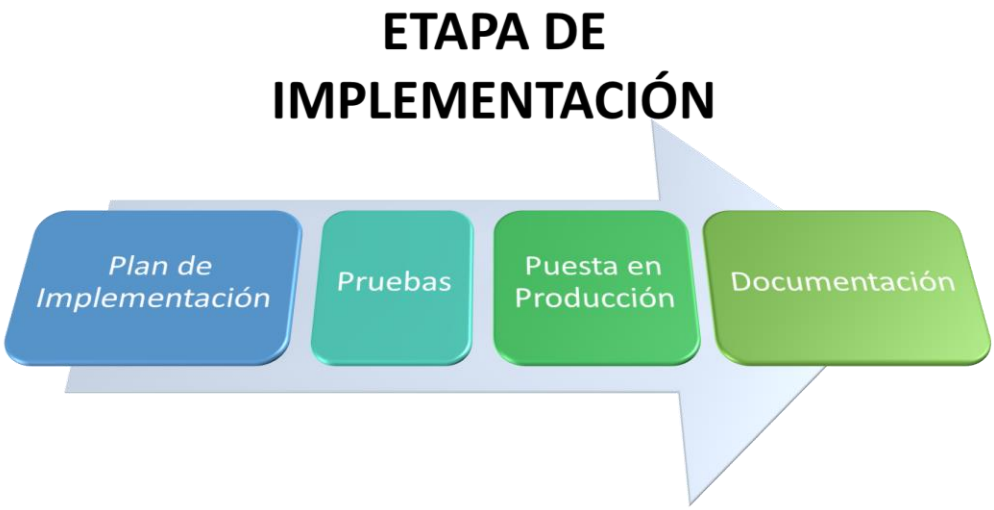


Figura 31. Pasos de la etapa de Implementación.

Plan de Implementación

En esta etapa es necesario llevar a cabo un plan para integrar gradualmente la propuesta realizada previamente, este plan debe contemplar la menor afectación a los usuarios de la red, por esto, es crítico el seccionamiento de la propuesta.

Este plan debe detallar los lugares donde se realizarán los trabajos de implementación y las personas que se encargaran de ella, así como los pasos a seguir en caso de contingencia, es decir, que la implementación no tenga éxito.

Finalmente, el plan debe ser revisado y autorizado por los administradores de la red, dado que ellos junto con el equipo de transición estarán encargados de auditar cada una de las etapas del plan, y dar a conocer si existe algún problema para continuar con la implementación.

Pruebas

Este paso es muy importante, y es en el cual se evalúa el funcionamiento de los escenarios propuestos ya instalados físicamente en los segmentos definidos en la etapa de Desarrollo. De esta manera es posible verificar el correcto o, en su caso, incorrecto funcionamiento de los escenarios. Aquí se analizan diferentes

parámetros y se detectan ciertas fallas con el fin de asegurar un servicio optimo en la red de datos de la ESIMEZ para su posterior puesta en producción

Puesta en Producción

Una vez comprobado el funcionamiento adecuado de cada uno de los escenarios es necesaria la revisión y autorización de los administradores de la red, quienes deben estar al tanto de cada cambio que se presente en la red y no tengan ningún inconveniente en cuanto a la implementación. De esta manera será posible hacer cambios en la red poniendo en producción los escenarios propuestos para que afecten positiva y directamente al usuario final.

Finalmente, si las conclusiones obtenidas al haber puesto en producción los escenarios de implementación son positivas; Es posible replicar esta metodología en cada uno de los segmentos que conforman la capa de Acceso de la red Politécnica, con el fin de agilizar dicha implementación para los administradores de la red.

Documentación

Debido a que no existía documentación sobre la estructura de la red y su estado se debe documentar todo lo realizado en cada una de las Etapas de la Metodología, es decir, los procedimientos que se llevaron durante el diagnóstico de la red, el análisis de los escenarios de implementación, el análisis de las especificaciones de los equipos, el análisis de las normas y estándares, las configuraciones de los equipos, etc.

Esto será muy útil cuando en el futuro se proponga algún rediseño, y los encargados de la gestión de la red cuenten con toda esta información necesaria para definir un plan de implementación siguiendo los pasos de cada una de las etapas mencionadas anteriormente.

CAPÍTULO IV: DESARROLLO DE LA PROPUESTA

El procedimiento para el desarrollo de la propuesta, esta detallado en este capítulo; Aquí se siguen los pasos planteados en el Marco Metodológico definido previamente con el fin de implementar la versión 6 del Protocolo de Internet.

Como se expresó en el capítulo anterior, es necesario realizar un Diagnóstico, que consiste en la observación donde se capturan datos de la red, se investiga la estructura y gestión, y se analiza la problemática en la red. Después se debe realizar un análisis de toda la información recabada, por ejemplo, si los dispositivos son compatibles con IPv6, si la topología física cumple con las expectativas de los encargados, etc.

Es importante que en el desarrollo se analicen las propuestas y diseños para su futura implementación, porque en esta etapa se definen los escenarios posibles para el despliegue de IPv6, y también se proponen los cambios a la red.

Finalmente, se requiere hacer un plan de implementación donde se realicen pruebas con los escenarios planteados sin que se afecte al servicio de la red; Para que posteriormente se implemente.

Diagnóstico

Esta etapa del proyecto, tal como se menciona en el capítulo sobre el Marco Metodológico, es la que requiere mayor tiempo, debido a que es muy importante documentarse sobre la estructura de la red Politécnica; Se debe conocer la problemática, los servicios que se brindan a los usuarios, las características que tienen los dispositivos de red, la administración de la red, etc. De esta manera, se pueden proponer cambios bien argumentados que no afecten al funcionamiento actual de la red.

Red de Telecomunicaciones Instituto Politécnico Nacional

Debido al gran tamaño de la red, y su distribución geográfica, la Red Politécnica no entra en una clasificación simple de redes pues tiene componentes LAN (Redes de Área Local), MAN (Redes de Área Metropolitana), WAN (Redes de Área Amplia), entre otros. Y para que su gestión no sea tan compleja, se adoptó el modelo jerárquico de tres capas de CISCO (Núcleo o Backbone, Distribución y Acceso) que permite que la red sea escalable, confiable y eficiente.

La capa de Núcleo es la de mayor jerarquía, se encarga de transmitir grandes cantidades de trafico de manera confiable y rápida. Cualquier error en esta capa

puede afectar a cualquier usuario de toda la red, por lo tanto, debe ser de baja tolerancia a fallos. Debido a las grandes cantidades de tráfico que se manejan en esta capa, la latencia y la velocidad son las principales preocupaciones aquí. Esta capa debe ser de alta confiabilidad. baja Latencia, redundante, además de bajos tiempos de convergencia.

La capa de Distribución se encarga principalmente del ruteo, filtrado y el acceso WAN (Wide Area Network, en español Red de Área Amplia). Determina la forma más rápida en que las solicitudes de servicio de red se manejen. En la capa de distribución se instauran las políticas de la red, en esta capa se Implementan Listas de Acceso, Filtrado de Paquetes y Puesta en fila (Cola).

Por último, la capa de Acceso es donde los usuarios finales se conectan a la red, la mayoría de los recursos que el usuario necesita son disponibles localmente. El uso de switches es muy frecuente en esta capa.

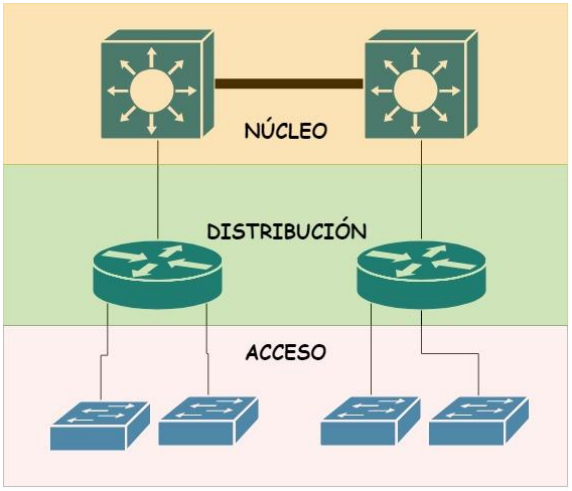


Figura 32. Modelo Jerárquico de Capas de Cisco Systems.

Núcleo Red Politécnica

El Núcleo de la Red Politécnica está formado por tres nodos, formando una delta; Cada uno de los nodos se ubica en los principales campus de la Ciudad de México (Zacatenco, UPIICSA y Santo Tomás). El nodo principal se encuentra en Zacatenco en la Dirección de Cómputo y Comunicaciones.

Estos nodos se encuentran interconectados mediante fibra óptica monomodo, la cual permite mantener velocidades de transmisión altas y grandes distancias, ideales para la capa de backbone. Estos cables son de 18 hilos y están instalados en los túneles del Sistema de Transporte Colectivo de la Ciudad de México. Las distancias de los enlaces son:

- Zacatenco-UPIICSA: 19.9 Km.
- Santo Tomás-UPIICSA: 18.1 Km.
- Zacatenco-Santo Tomás: 13.5 Km.

Como medio de redundancia, el Núcleo de la Red también tiene conexiones con Microondas; Además, también existen enlaces de microondas a determinadas unidades del Instituto debido a su ubicación Geográfica. En total hay 21 enlaces de microondas:

- Zacatenco -> COFAA, Santo Tomás y UPIICSA.
- Santo Tomás -> CECyT 2, ESIA Tecamachalco, CICATA Legaria, CEDICyT Tezozómoc, CECyT 6, CECyT 12, UPIICSA y Zacatenco.
- UPIICSA -> CECyT 1, CECyT 3, CET 1, CECyT 10, CECyT 7, CECyT 15, ESIME Culhuacán, CECyT 13, CECyT 14, ESCA Tepepan, Santo Tomás y Zacatenco.

Las antenas empleadas son de tipo tambor, y los equipos cuentan con un modem y el radio; Alcanzando un ancho de banda de 465 Mbps.

El 10 de mayo del año en curso (2018) entro en producción equipo nuevo en el núcleo de la red. En cada nodo se instalaron dos Switches Multicapa de la Marca CISCO, el Modelo es NEXUS 9508. Actualmente el equipo solo está configurado direccionamiento IPv4, aunque también soporta IPv6 en Doble Pila (Dual Stack). En la figura 33 se puede observar cómo se conectó el equipo. [64]

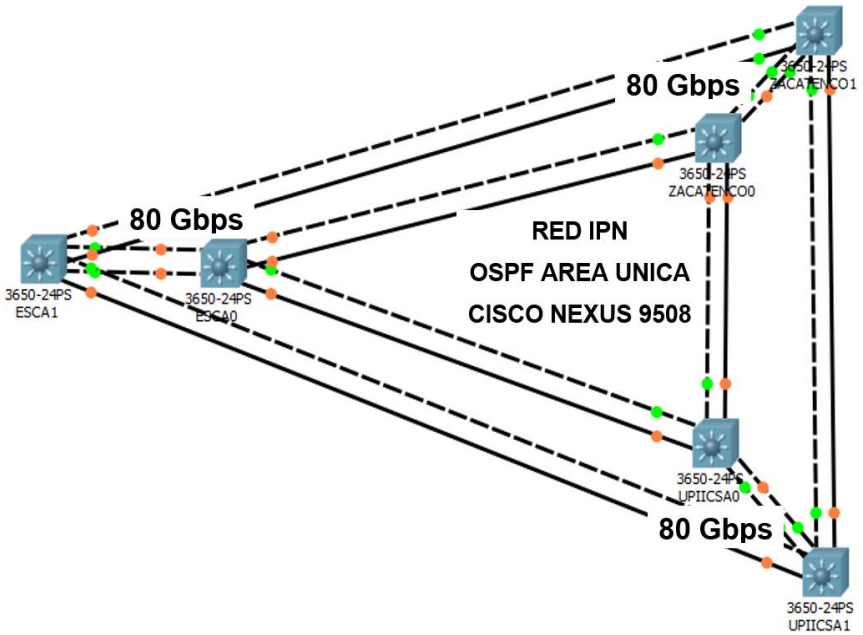


Figura 33. Equipos Nexus 9508 Instalados en la Capa del Núcleo de la Red del IPN.

Zacatenco

Como se mencionó anteriormente, Zacatenco es el nodo principal y está ubicado en la DCyC, su importancia radica en que aquí se encuentran sistemas de monitoreo y administración central de la red. Además de que aquí se mantienen servicios como el correo institucional, Páginas Web, Bases de Datos, etc.

En Zacatenco se ubican Secretarías, Áreas Administrativas y de Gobierno, Centros de Investigación

Los dos switches multicapa que se instalaron en el núcleo de la red son los principales en Zacatenco (CISCO Nexus 9508), a partir de estos se conectan los equipos de la capa de distribución donde se cuenta con switches multicapa de la marca Brocade, modelo ICX-7250, el cual también cuenta con soporte Dual Stack (IPv4/IPv6).

Este Nodo tiene un enlace a Internet de 3Gbps, y cuenta con los dispositivos de red que se encargan del ruteo en la frontera, además de los equipos de seguridad (firewall, sistema de protección contra intrusos y sistema de administración de contenidos). También cuenta con salida a Internet 2 con un enlace de 1Gbps.

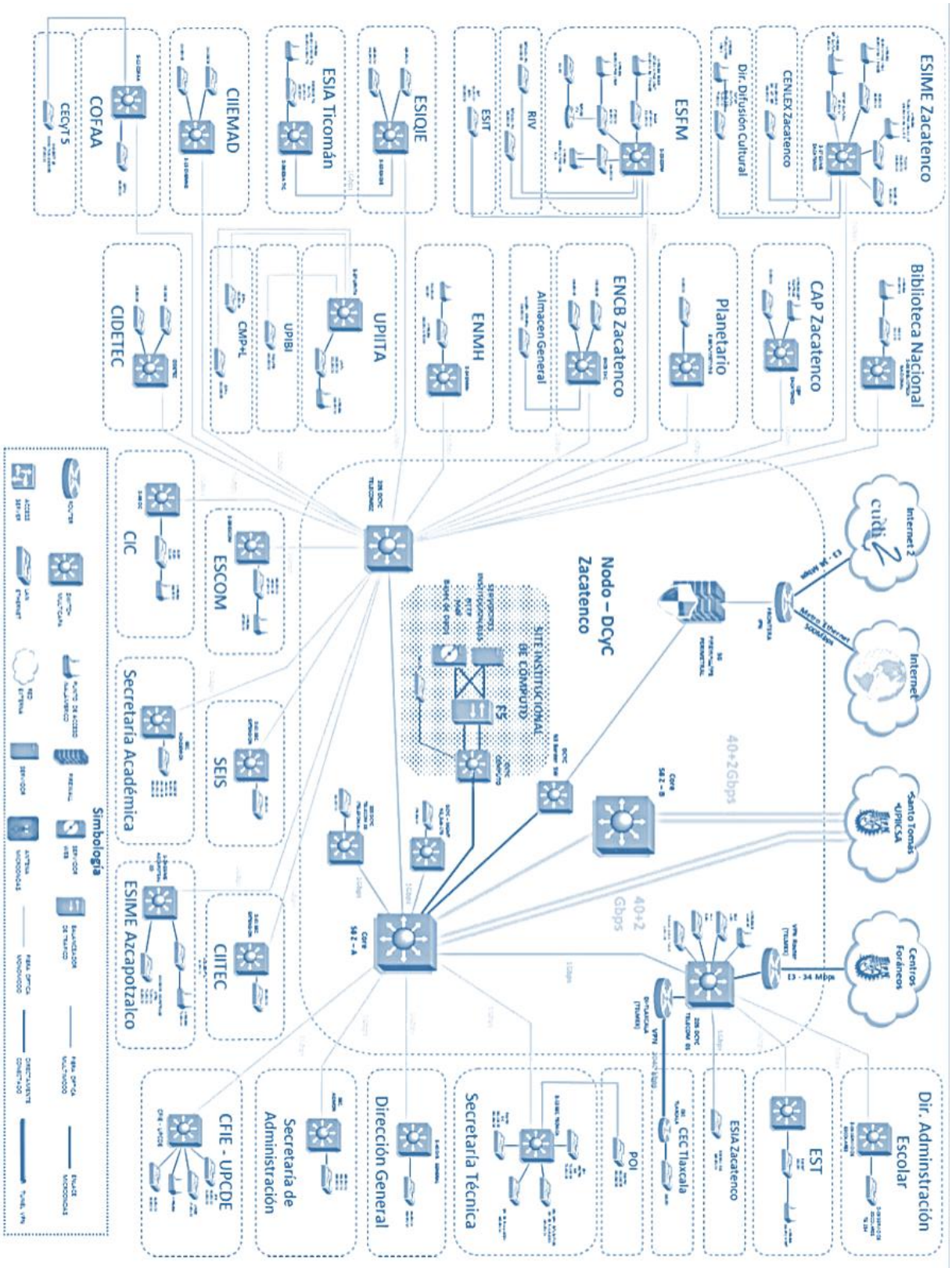


Figura 34. Diagrama de Red del Nodo Zacatenco.

Santo Tomás

En este nodo hay dos switches multicapa de los 6 que fueron instalados en el backbone (CISCO Nexus 9508), Los dispositivos de distribución son de la marca Enterasys de la serie N3 ubicados en la ESCA, ENCB, CAP Sto. Tomás y el CECyT 11.

En este nodo se tienen varios enlaces de microondas a escuelas donde no era económicamente viable instalar cable de fibra óptica. Los enlaces manejan un ancho de banda de 155Mbps.

Al igual que Zacatenco, cuenta con un enlace de salida hacia Internet de 3Gbps y con sus dispositivos de seguridad correspondientes.

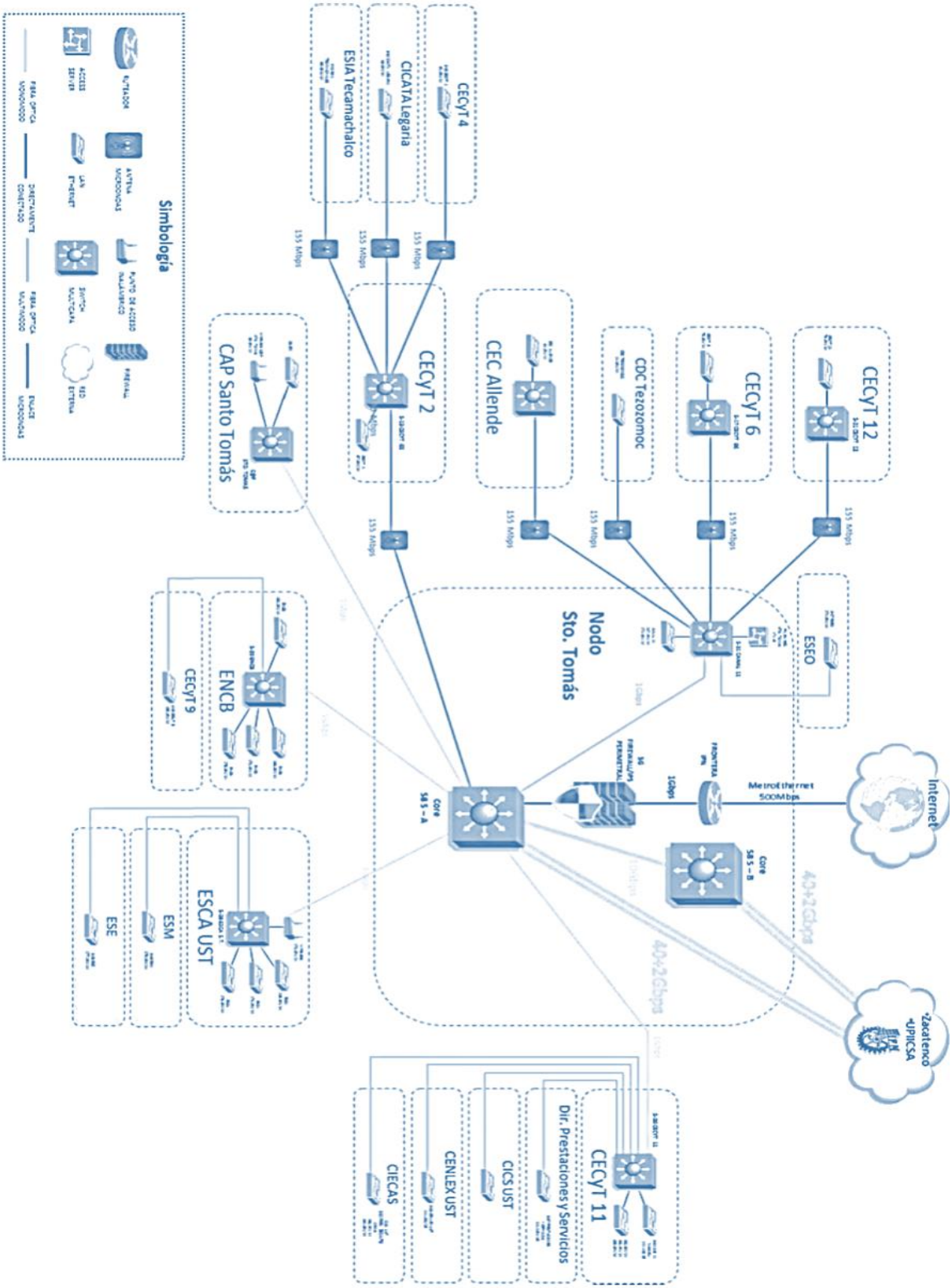


Figura 35. Diagrama de Red del Nodo Santo Tomás.

UPIICSA

De los tres campus que conforman la delta del núcleo de la red, UPIICSA es la de menor tamaño, el equipo de distribución que se conecta hacia las demás instalaciones de esta unidad es de la marca Enterasys S4. También cuenta con salida hacia Internet en un enlace de 3Gbps. A través de enlaces de microondas y con otro switch multicapa S4 conecta a otras escuelas.

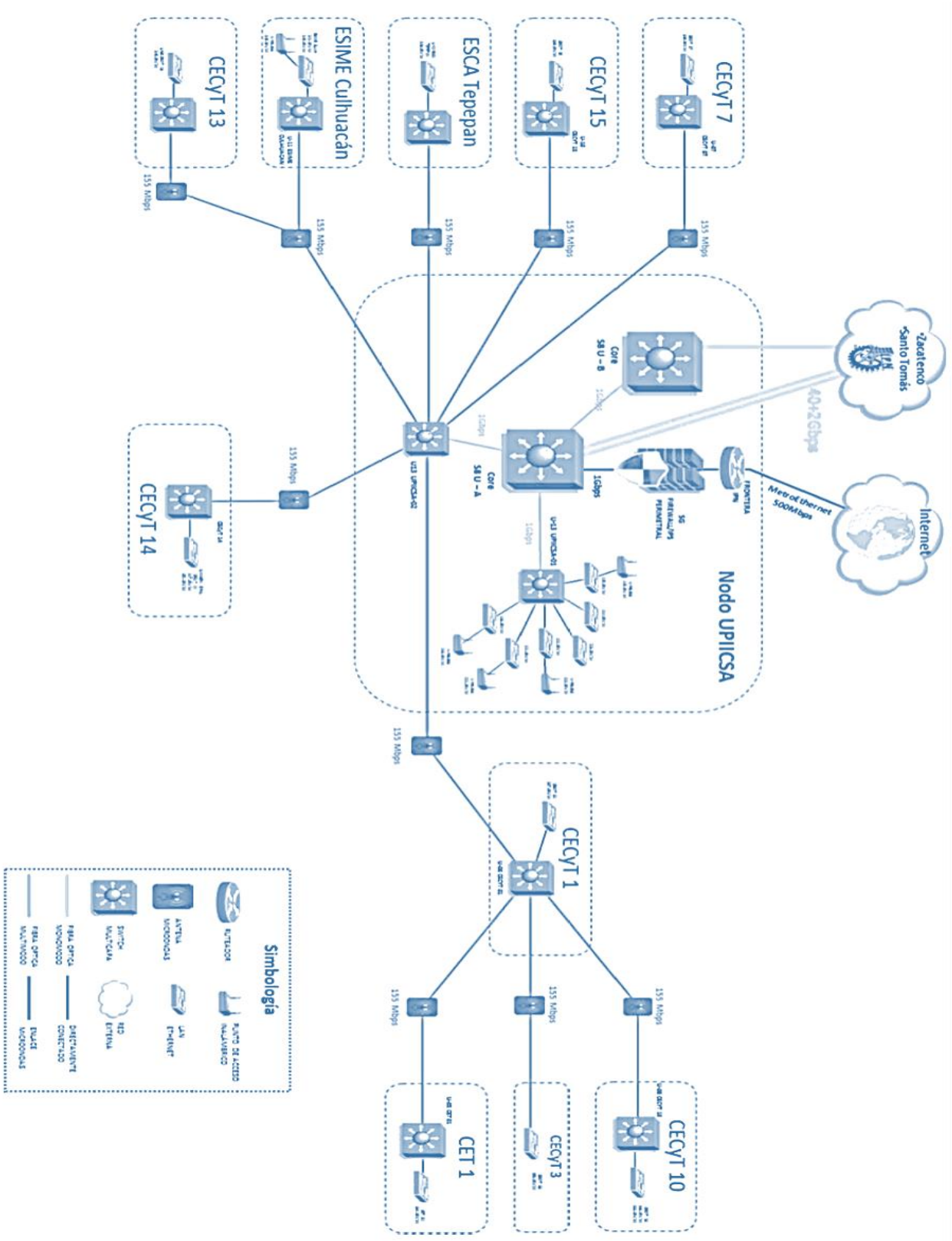


Figura 36. Diagrama de Red del Nodo UPIICSA

Diagnóstico Red de Datos de la ESIMEZ

La primera etapa de este proyecto definida en el Marco Metodológico consiste en realizar el diagnóstico de la red, Para esto es necesario conocer los problemas que existen en la red.

Actualmente (septiembre 2018) no existe un diagrama de la topología física de la red de telecomunicaciones. Ha crecido descontroladamente debido a los cambios de administración y al desconocimiento del reglamento que establece la unidad de informática (UDI), quienes se encargan de toda la gestión de la red de datos de la ESIMEZ.

Como se mencionó anteriormente, el problema principal son los cambios de administración, sin importar la capacidad y las buenas intenciones de los que toman el cargo, los procesos se cortan. Y muchas veces quedan proyectos a la mitad.

Otro gran problema, es que no hay un diagrama de la topología física; Y cuando hay cambios de administración, se pierde tiempo en el reconocimiento de la red; Cuando es algo esencial para proponer mejoras a la red.

Como los usuarios desconocen las normas, surgen muchos problemas en la capa de acceso; Por ejemplo: Duplicidad de direcciones IP (Se han descubierto ordenadores con la dirección IP de un dispositivo de capa 3), Instalación no autorizada de Puntos de Acceso Inalámbricos (Interferencias con los AP de la escuela), Crecimiento sin control.

Otros problemas más específicos que se han informado son ciertos problemas de diseño en la última actualización de la red (Año 2016), Certeza de la ubicación de ciertos nodos y equipo reciente no conectado.

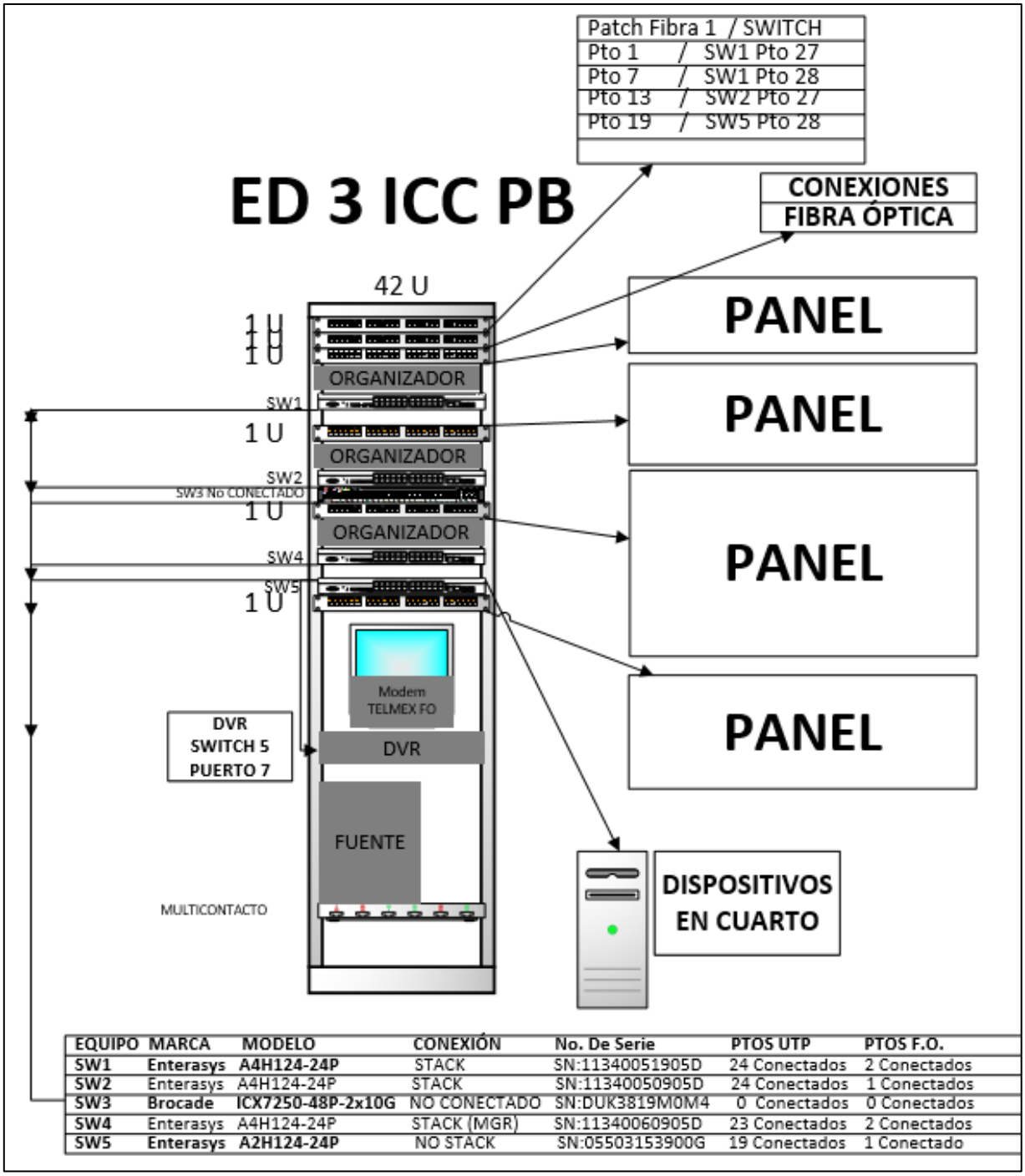
Tomando en cuenta los problemas ya mencionados, el siguiente paso es levantar la topología física de la ESIME Zacatenco; Para esto, se requiere iniciar con la subetapa de Observación (definida en el Capítulo III); La cual consiste en extraer toda la información posible observando cada uno de los cuartos de telecomunicaciones (TR, por sus siglas en inglés Telecommunications Room) en ESIMEZ y su interconexión. Para esto se propuso extraer la siguiente información:

- Marca, Modelo y No. de Serie de los Equipos.
- Señalar si se trata de un Punto de Conexión Principal (MCC), un Punto de Conexión Intermedia (ICC) o de Conexión Horizontal (Norma TIA/EIA-568-B).
- Señalar si hay equipos desconectados.
- Puertos Libres.

- Señalar si los equipos están en modo Stack (Apilados).
- Conexiones de Fibra Óptica.

Para realizar el diagrama de la topología física de la red se empleó Microsoft Visio, el cual es un software de dibujo vectorial que te permite realizar diagramas de bases de datos, diagramas de redes, diagramas de flujo, etc.

En la Figura 37 se pueden observar los datos que se extrajeron de cada TR.



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	Enterasys	A4H124-24P	STACK	SN:11340051905D	24 Conectados	2 Conectados
SW2	Enterasys	A4H124-24P	STACK	SN:11340050905D	24 Conectados	1 Conectados
SW3	Brocade	ICX7250-48P-2x10G	NO CONECTADO	SN:DUK3819M0M4	0 Conectados	0 Conectados
SW4	Enterasys	A4H124-24P	STACK (MGR)	SN:11340060905D	23 Conectados	2 Conectados
SW5	Enterasys	A2H124-24P	NO STACK	SN:05503153900G	19 Conectados	1 Conectado

Figura 37. Plantilla de Datos extraídos de cada Cuarto de Telecomunicaciones usando Visio

El nombre de cada uno de los TR tiene el siguiente formato:

EDIFICIO-PUNTO DE CONEXIÓN-PISO-OFICINA(OPCIONAL)

La Figura 37 representa un ICC (Punto de Conexión Intermedia) ubicado en la Planta Baja del Edificio 3, donde se encuentra un laboratorio para los alumnos

con más de 30 computadoras; Cabe señalar que dicho TR estaba nombrado EDIFICIO 3 IDF, pero como la Norma ya ha sido actualizada, ahora se tienen los Puntos de Conexión Principal (MCC), De Conexión Intermedia (ICC) y Conexión Horizontal (HCC).

Los Swithes o Conmutadores se enumeraron de arriba hacia abajo, como se puede apreciar, En la parte inferior hay una tabla que indica la Marca, Modelo, No. de Serie, Si se encuentra en modo Stack (Apilado), los puertos UTP conectados y los puertos de Fibra Óptica conectados.

En la parte superior derecha se aprecia un recuadro que representa las conexiones que hay en el Panel de fibra óptica (En caso de que exista), y se relacionan con los puertos de los Switches.

En los recuadros que tienen por nombre "PANEL", se menciona cuantos puertos de los paneles UTP se encuentran conectados, y si estos mismos están conectorizados (coloquialmente hablando, se dice que están Ponchados).

Normalmente, los conectores de los Paneles UTP que se encuentran ponchados van a un nodo para su respectiva conexión con el Usuario; Aunque existen algunos casos donde el cable UTP, sale directo del Switch por el plafón a la canaleta y llega directamente a un Ordenador.

También se representan otros dispositivos dentro del TR, puede que haya Puntos de Acceso (AP), DVRs, Monitores, CPUs, etc.

La Figura 38 representa las conexiones de cada Switch (De acuerdo con su numeración), es decir, si van conectados a los paneles, si salen directamente del switch, si están usándose los puertos para la conexión en modo Stack, los puertos de Fibra Óptica y otros dispositivos conectados.

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)	SWITCH 3 (PANEL/PUERTO)	SW 4 BROCA DE	SWITCH 5 (PANEL/PUERTO)
1	P1/1	P2/25	P3/49		UNTAGLE
2	P1/2	COLGADO	P3/50		UNTAGLE
3	P1/3	P2/27	P3/51		NO CONECTADO
4	P1/4	P2/28	P3/52		NO CONECTADO
5	P1/5	P2/29	P3/53		NO CONECTADO
6	P1/6	P2/30	P3/54		NO CONECTADO
7	P1/7	P2/31	P3/55		P2/26
8	P1/8	P2/32	P3/56		NO CONECTADO
9	P1/9	P2/33	P3/57		P3/68
10	P1/10	P2/34	P3/58		P3/67
11	P1/11	P2/35	P3/59		P3/70
12	P1/12	P2/36	P3/60		P3/69
13	P1/13	P2/37	P3/61		NO CONECTADO
14	P1/14	P2/38	P3/62		NO CONECTADO
15	P1/15	P2/39	P3/63		NO CONECTADO
16	P1/16	P2/40	NO CONECTADO		NO CONECTADO
17	P1/17	P2/41	P3/64		COLGADO
18	P1/18	P2/42	NO CONECTADO		NO CONECTADO
19	P1/19	P2/43	P4/73		NO CONECTADO
20	P1/20	P2/44	P3/66		ACCESS POINT
21	P1/21	P2/45	P4/74		NO CONECTADO
22	P1/22	P2/46	COLGADO		NO CONECTADO
23	P1/23	P2/47	DVR		P3/65
24	P1/24	P2/48	SW5/PTO 24		SW3/PTO24
25 STACK UP	CONECTADO	CONECTADO	CONECTADO		NO CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO	CONECTADO		NO CONECTADO
27 F.O.	CONECTADO Panel F.O. Pto. 7	CONECTADO Panel FO Pto 13	CONECTADO Panel FO Pto 19		CONECTADO Panel FO Pto 4
28 F.O.	CONECTADO Panel F.O. Pto. 1	CONECTADO Panel FO Pto 16	CONECTADO Panel FO Pto 22		NO CONECTADO

Figura 38. Ejemplo de Tabla de Conexiones de Dispositivos de Red.

El procedimiento se fue realizando por Edificio, para Identificar si los TR estaban Interconectados entre sí. En la Figura 39, se logra apreciar el diagrama general del Edificio 3.

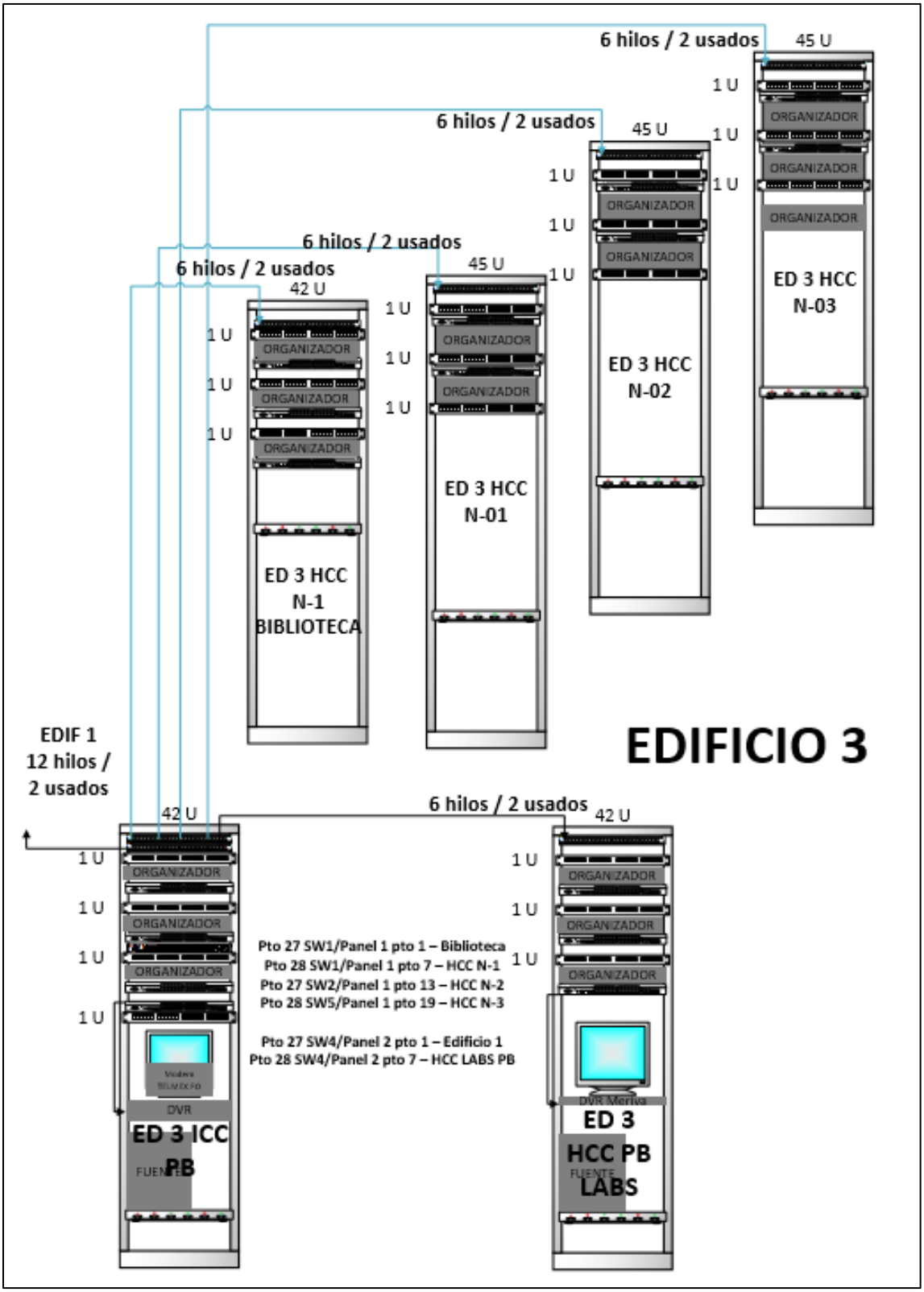


Figura 39. Diagrama de Interconexiones EDIFICIO 3 usando Visio

Como se puede apreciar, en este edificio vienen más detalles sobre la conexión de Fibra Óptica (según el caso); Se mencionan los hilos disponibles, los hilos ocupados, y con que Switches del ICC están conectados.

Existen Casos como el Edificio 5, donde hay conexiones mediante UTP, los cuáles no fueron posibles de identificar a simple vista.

El siguiente Diagrama (Figura 40) se puede observar como es el diagrama de la Topología Física en ESIMEZ.

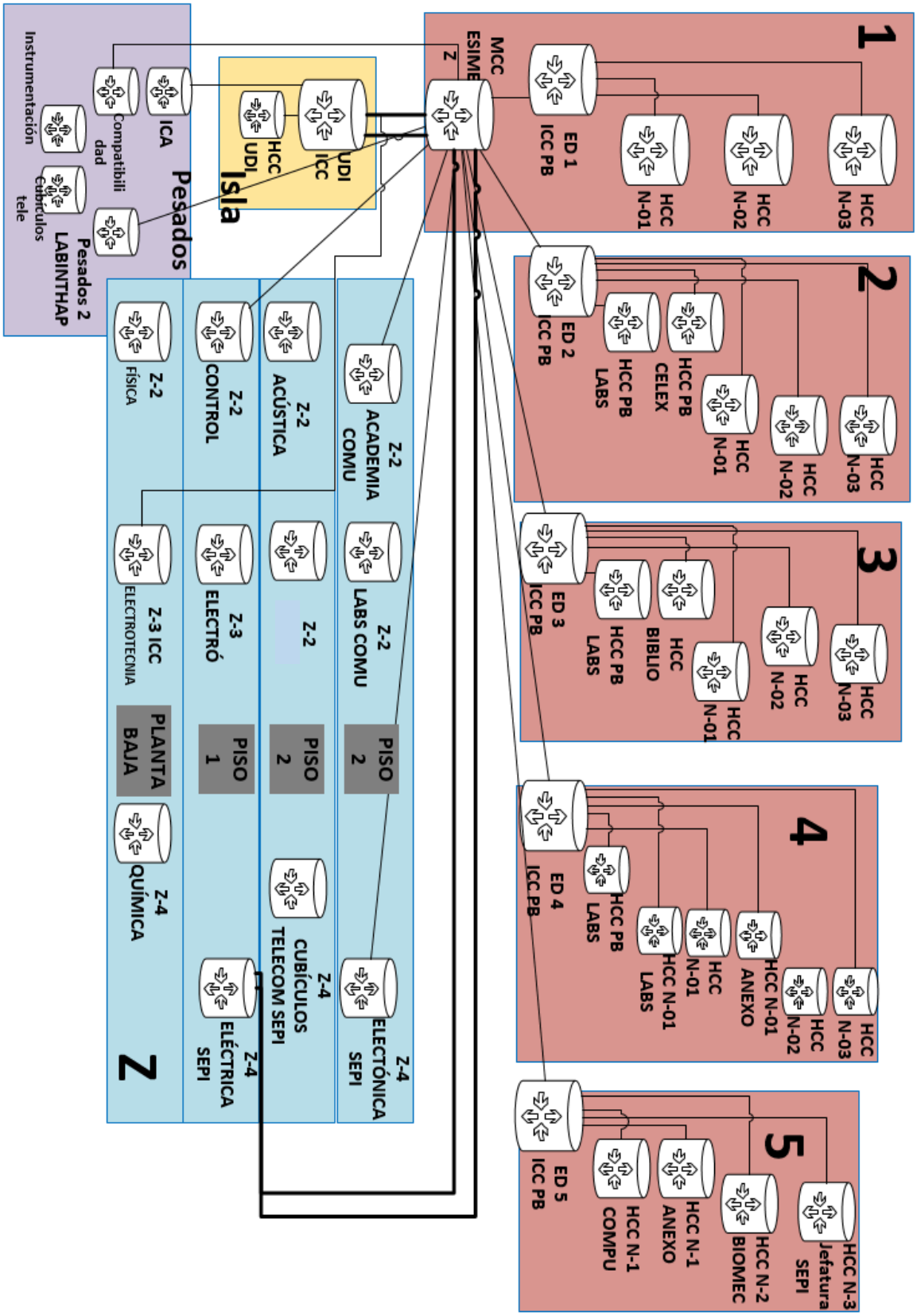


Figura 40. Topología de Red de ESIME Zacatenco usando Visio

Se realizó el diagnóstico de los Edificios 1, 2, 3, 4, 5, Z y la Unidad de Informática, pues es donde se tienen los laboratorios con más nodos, y donde se establece la mayor parte de la comunidad estudiantil.

Con esta información, es posible determinar en la subetapa de Análisis si la red puede iniciar con el despliegue de IPv6. (NOTA: Todos los Diagramas se encuentran en el apartado "ANEXOS").

Aplicaciones de la Red Politécnica

Además de conocer físicamente la topología de la red de datos de la ESIMEZ, es necesario saber cuáles son las aplicaciones y servicios que brinda.

El uso cada vez más frecuente de las redes, se debe principalmente a las Tecnologías de Información en las Comunicaciones (TICs), y en el ámbito educacional, se han empleado como una herramienta que facilite la investigación de los alumnos y docentes; A continuación, se mencionan algunos servicios y aplicaciones que ofrece la red Politécnica.

Sistema Institucional de Información (SII)

Como se mencionó anteriormente, hoy en día el uso de las TICs en cualquier ambiente organizacional trae muchas ventajas, y una de ellas es mejorar la eficiencia de ciertos procesos.

El objetivo del SII consiste en analizar, procesar, proteger y preservar la información que generen las diferentes dependencias en el instituto; Con el fin de impulsar los sistemas de información en el IPN. Se compone de 29 subsistemas de gestión institucional, y genera 168 indicadores en diferentes ámbitos como capital humano, evaluación y planeación.

Estos sistemas integran los datos que se generan en todas las escuelas y dependencias del IPN para que se lleve a cabo una mejor gestión y toma de decisiones.

Actualmente existen diferentes sistemas; y la Coordinación del Sistema Institucional de Información se encarga de su administración, como son: Sistema Institucional de Información (SII), Sistema Institucional de Información de Investigación y Posgrado (SIIIP), Sistema Institucional del Programa Integral del Fortalecimiento de la Estructura Física Educativa (SIPIFIFE), Sistema de Administración para el Control de Documentos (SACDOC), Intranet de la Secretaría de Gestión Estratégica (Intranet SGE); Entre otros.

Campus Virtual Politécnico (Polivirtual)

Uno de los propósitos en el IPN es la educación a distancia mediante entornos virtuales, el campus virtual politécnico es una plataforma que contribuye al desarrollo de los alumnos, sin necesidad de que la comunidad se deba presentar en un aula para recibir asesoría. En esta plataforma se brinda soporte en la operación del modelo educativo de educación a distancia; Se administra el acceso a los recursos, la interacción entre docente-alumno. Actualmente este servicio da atención a carreras de Bachillerato, Licenciatura y posgrado como son:

Bachillerato. - Administración, Comercio Internacional, Computación, Telecomunicaciones, Informática, Diseño Gráfico Digital, Etc.

Licenciatura. – Contador Público, Negocios Internacionales, Turismo, Comercio Internacional, Administración y Desarrollo Empresarial, Etc.

Posgrado. – En Matemática Educativa y en Ciencias en Física Educativa.

Está conformado por alumnos, autores, tutores, asesores, coordinadores, directivos y funcionarios de las unidades académicas. Esta plataforma se rige por el marco legal del Instituto, y tiene la finalidad de brindar educación de calidad.

En la red Politécnica se brindan servicios fundamentales para los usuarios que se conectan a la red todos los días, esto es lo que la convierte en la principal plataforma de comunicación del Instituto; Aquí se brindan diferentes servicios que son imprescindibles para algunas áreas; Éstos se clasifican de acuerdo con su importancia en: **Aplicaciones de Misión Crítica, Aplicaciones Importantes y Aplicaciones Ordinarias.**

Aplicaciones de Misión Crítica

Internet es el servicio que dispone de la mayor parte del tráfico de la red Politécnica (80 % del tráfico total), pues es una gran herramienta, en la que se pueden encontrar innumerables aplicaciones e información.

La **Telefonía bajo IP** que integra las comunicaciones de voz y datos en una misma red; Este esquema es un ejemplo de las redes convergentes, donde se busca que se integren comunicaciones como voz, datos, video, entre otros, en la misma red. En el segundo capítulo se menciona que campo de la cabecera IPv4 e IPv6 define la calidad de servicio para Voz, Datos o Video.

El **Sistema de Nombres de Dominio (DNS)** se encarga de convertir los números de la dirección IP a la que están hospedadas las páginas web en el nombre de dominio (La dirección de la página web); esto facilita al usuario el memorizar

fácilmente los nombres de las páginas en lugar de números de las direcciones IP.

El **Correo Electrónico Institucional** con dominio @ipn.mx para la comunidad. Existen varias ventajas de tener una cuenta institucional, Google Drive y Microsoft One Drive te brindan espacio de 1 Terabyte en la nube. Además, Microsoft te da licencia para instalar Office 365.

El **aula polivirtual** forma parte del Campus Virtual Politécnico; en esta plataforma se desarrollan cursos en línea, y está basada en Moodle (Aplicación de distribución Libre de Ambiente Educativo Virtual).

El **Portal Web Institucional** (www.ipn.mx) es el sitio web del Instituto Politécnico Nacional.

El **Sistema de Administración Escolar (SAES)** Es una herramienta utilizada por docentes y alumnos con el fin de agilizar procesos, también se realizan consultas de horarios y de calificaciones en las escuelas.

El servicio de **Videoconferencia** para transmisión y recepción de eventos con el fin de apoyar a las actividades académicas, de investigación y gestión que requieran las dependencias del Instituto.

Aplicaciones Importantes

Antivirus Institucional. Es un factor esencial para protección a equipos de cómputo ante amenazas de programas maliciosos, además cuenta con análisis y detección de amenazas en la infraestructura y red. Este servicio se ofrece en la Dirección de Cómputo y Comunicaciones mediante el Departamento de Seguridad e Informática. Se ofrecen capacitaciones de detección de malware, desinfección de equipos y el uso de herramientas antimalware, así como asesoría en cuanto a la instalación de clientes antivirus.

Sistemas de Seguridad Informática. Dispositivos instalados en la red que se encargan de detectar y evitar anomalías o amenazas informáticas.

Sitios Web de Escuelas y Unidades. Todas las Unidades del Instituto cuentan con una página web, donde se encuentra información de la unidad en cuestión, así como ciertas herramientas y servicios que ésta proporcione.

Sistema Institucional de Bibliotecas y Servicios de Información. Herramienta que facilita la búsqueda de la información, donde es posible encontrar tesis, libros electrónicos, o la ubicación de algunos libros en las bibliotecas.

Sistema de Administración de la Red de Datos. Sirve para llevar a cabo

una gestión y monitoreo en la plataforma de datos con el fin de tener control y operación de las telecomunicaciones; También se implementa automatización, visibilidad e integración de los equipos en la red.

Sistema Institucional de Gestión Administrativa (SIGA). Se llevan a cabo procesos de gestión administrativa, además brinda los mecanismos de seguimiento y control.

Sistema Institucional de Información de Integración Social. Encargada de sistematizar procesos que se relacionan con el registro y la revisión de proyectos que las dependencias Politécnicas fomentan con el sector productivo, con el fin de agilizar su seguimiento y autorización.

Aplicaciones Ordinarias

Repositorio Digital Institucional (RDI). Aquí se guarda en formato digital todo el material científico o académico de una institución; Hoy en día es la principal forma de publicar información digital soportada en software libre. Dentro de los repositorios es posible encontrar Tesis doctorales, artículos científicos, ponencias, revistas científicas, etc. Este repositorio forma parte de la iniciativa Open Access, que fue un movimiento internacional para contribuir al sistema de comunicación científica y que sea de acceso abierto al conocimiento.

Sistema Institucional de Servicio Médico Integral (SISMI). El fin de este sistema es funcionar como una herramienta de soporte en el servicio de salud para la comunidad politécnica; Se divide en seis módulos para llevar un seguimiento integral en el paciente (Historial clínico, Medicina general, Optometría, Odontología, Nutrición, Epidemiología, IMSS y Seguro).

Sistema Institucional de Información Jurídica. Mediante este sistema se brinda asesoría y consulta a la comunidad politécnica y al público en general sobre el marco normativo del IPN, además de los servicios que se dan en la Oficina del Abogado General; De esta manera se promueve una eficiente realización de tareas administrativas y académicas en cumplimiento con los requisitos legales que se establecen en el marco jurídico y administrativo.

Sistema de Alerta Sísmica. Desarrollado en la Escuela Superior de Física y Matemáticas (ESFM), que se activa cuando el sistema detecta ondas primarias de un sismo llamadas ondas P, 50 segundos antes de que ocurra un movimiento telúrico. A diferencia de la Alarma de la Ciudad de México, La Alerta Sísmica del IPN detecta sismos en cualquier parte del país, aunque con una anticipación de tiempo menor.

El Centro Nacional de Cálculo (CeNaC) también se encarga de realizar aplicaciones dentro del Instituto:

- **Sistema Institucional de Control Patrimonial**. Diseñado con el fin de que los Bienes muebles del instituto se encuentren registrados de manera adecuada. Cuenta con una base de datos confiable y mediante este sistema es posible donar, registrar y dar de baja. Con este sistema se pretende: Describir los Bienes de cada Unidad Responsable, Conocer el estado físico de los Bienes, así como la naturaleza de sus fallas y Definir la función del Bien.
- **Sistema de Control de Gestión Institucional (SCGI).** Administración de documentos elaborados dentro de las escuelas, unidades y centros en el IPN.
- **Sistema de Control de Relaciones de Servicio Social (SICORESS).** Se encarga del control de registro y liberación de servicio social en nivel medio superior y superior.
- **Sistema de Información de Integrador de Trámites (SIINTRA).** Herramienta de automatización a servicios del Departamento de Prestaciones y Servicios para empleados del IPN.
- **Sistema Institucional de Servicio Social (SISS).** En este sistema se gestiona la actividad del alumno durante su servicio (reportes mensuales, horas cumplidas), se lleva el registro dependiendo el perfil del estudiante con los respectivos prestatarios registrados en el sistema.
- **Sistema Institucional de Alumnos Consejeros (SIAC).** Seguimiento de oficios de alumnos consejeros.
- **Sistema Institucional de Seguimiento y Actualización de Egresados (SISAE).** Maneja información de los egresados para contactarlos a través de Servicio Social y la Dirección de Egresados.
- **Encuentro de Tutorías (e-Tutorías).**

Dispositivos de la Red Politécnica y sus Características

A Continuación, se dará una breve explicación de los equipos que actualmente forman parte del segmento de Red que se analizó, el cual va desde el Nodo Principal ubicado en la Dirección de Cómputo y Comunicaciones correspondiente a la Capa de Núcleo, el Switch o Conmutador de Distribución Ubicado en el Edificio 1 de ESIMEZ (Capa de Distribución), y todos los equipos de la Red de datos de la ESIMEZ (Capa de Acceso).

Cisco Nexus 9508 (DCyC)

Equipo con gran capacidad de recuperación, con puertos de 1/10/40 Gigabit, ideal para formar parte del Núcleo de la Red. Orientado a centros de datos de grandes empresas, Proveedores de Servicio, e incluso en la Nube.

La serie Cisco Nexus 9500 puede operar en dos modos, Cisco ACI y Cisco NX-OS. El primero va orientado la implementación de una estructura basada en políticas de automatización, además del diseño y administración de la estructura de los centros de datos. El segundo (NX-OS), el switch ofrece capacidades multicapa (2 y 3) básicas, y también nuevas tecnologías como son VXLAN, plano de control VPN Ethernet (BGP-EVPN) de Protocolo de Puerta de Enlace de Frontera (BGP) y Conmutación de Etiquetas multiprotocolo (MPLS).

Figura 41. Switch Multicapa Modelo Cisco Nexus 9500 Series fuente: [65]

Esta serie tiene la capacidad de un Ancho de banda máximo de 172.8 Tbps dependiendo las tarjetas de línea 1, 10, 25, 40, 50 y 100 Interfaces Ethernet Gigabit.

Usando estas tarjetas, es posible configurar el equipo de la siguiente manera:

- 576 puertos Ethernet de 100 Gbit
- 576 puertos Ethernet de 40 Gbit
- 2304 puertos Ethernet de 25 Gbit
- 2304 puertos Ethernet de 10 Gbit

Los Switches Cisco de la serie Nexus 9500 impulsan la transición de las redes de las Empresas de 1 y 10 Gbit a 50 y 100 Gbit. Tienen supervisores redundantes, controladores del sistema, fuentes de alimentación, y bandejas de ventiladores, por lo tanto, son dispositivos de Alta disponibilidad, fiabilidad y escalabilidad.

Brocade ICX-7750-48F (ESIMEZ Edificio 1)

Las redes organizacionales están creciendo rápidamente, y hoy en día están aumentando sus velocidades de conmutación a 10 y 40 Gbit Ethernet, y esto se debe a que cada vez se usan más ciertas aplicaciones como videos de alta definición (HD), Infraestructura de escritorio Virtual (VDI); O nuevos modelos de negocio donde los usuarios de la organización se comunican dentro de la empresa con sus propios dispositivos (BYOD).

Este dispositivo tiene capacidades avanzadas de ata disponibilidad y una arquitectura de apilamiento flexible (12 unidades y hasta 5.76 Tbps de Ancho de Banda en apilamiento agregado), orientado para LAN empresariales.

Otra de sus características principales es el apilamiento de larga distancia, que permite una administración en un punto único; También cuenta con características avanzadas como BGP (Protocolo de Puerta de Enlace de Frontera), Enrutamiento, Multi-Chassis Trunking (MCT), reenvío virtual (VRF).

Compatible con OpenFlow en modo puerto híbrido, habilitando la función de Red definida por Software (SDN) que permite facilitar la implementación de servicios de red.

Figura 42. Switch Multicapa Marca Brocade Modelo ICX-7750-48F fuente: [66]

Brocade ICX-7250-48P (Acceso)

Capaz de conmutar hasta 256 Gbps, cuenta con 48 puertos con PoE (Power Over Ethernet); Tiene la capacidad de enrutamiento bajo IPv4 e IPv6 (RIP y OSPF); A continuación, se pueden observar sus características principales:

- 4095 VLANs
- Autenticación 802.1x
- Asignación Dinámica de VLANs
- Máximo 254 STP (Spanning Tree Protocol)
- Rutas estáticas IPv4/IPv6
- Interfaces Virtuales
- Rutas Dinámicas IPv4/IPv6
- OSPFv2, OSPFv3, RIPv1/v2, RIPng.
- Túneles IPv6 sobre IPv4
- Redes Definidas por Software con soporte a OpenFlow v1.0 y v1.3

Diseñado para pequeñas y medianas empresas, son switches escalables de alto desempeño y confiabilidad.

Figura 43. Switch Multicapa Marca Brocade Modelo ICX-7250-48P fuente: [67]

Enterasys Serie A4 (Acceso)

Es un Switch de alto rendimiento y escalable, con soporte a latencias. Tiene clasificación de paquetes en múltiples capas, cuenta con 4 puertos Gigabit Ethernet de enlace ascendente aprovechando el apilamiento.

Entrega características de clase empresarial en apilamiento, garantizando alta conectividad y rendimiento; Soporta 16000 direcciones MAC. Para medianas y grandes empresas. Los mecanismos de cola inteligente aseguran que las aplicaciones de misión crítica reciban prioridad de acceso a los recursos de la red.

Características:

- Se pueden apilar hasta 8 switches, brindando capacidad de 140.8 Gbps.
- Capacidad de conmutación de 17.6 Gbps
- Dependiendo el equipo soporta hasta 48 Puertos Ethernet 10/100, así como 2 puertos Gigabit Ethernet y 2 10/100/10000 modulares.
- En cuanto a calidad de servicio, el switch A4 soporta VoIP y Video IP, además de todo tipo de aplicaciones.

Figura 44. Switch Multicapa Marca Enterasys Serie A4 fuente: [68]

Enterasys Serie A2 (Acceso)

Es un switch de frontera Fast Ethernet de Alto rendimiento y escalable. Ideal para entornos que requieren soporte de alta densidad de puertos Ethernet. Cuenta con clasificación de paquetes para servicios diferenciados (QoS). A Continuación, se muestran algunas características principales del equipo.

- Conmutación de 17.6 Gbps.
- Soporte de 8000 direcciones MAC.
- Para redes 100 Mbps
- Capacidad de apilamiento de hasta 8 equipos A2.
- 8 colas de prioridad basadas en hardware por puerto Ethernet.
- Soporte a multimedia (Video, VoIP, etc.)
- Autenticación y Seguridad
- Un solo usuario/dispositivo por puerto, que se puede autenticar mediante IEEE 802.1X o dirección MAC.

Figura 45. Switch Multicapa Marca Enterasys Serie A2 fuente: [69]

Enterasys Serie B5 (Acceso)

Switch Gigabit Ethernet escalable, con soporte para alta demanda y latencia. Soporte de puertos de alta densidad 10/100/1000, Gestión IPv4/IPv6, enrutamiento IPv4.

- 32000 direcciones MAC.
- Soporte Multimedia para identificación de servicios de VoIP.
- 8 colas de prioridad basadas en hardware por puerto Ethernet.
- Capacidad de conmutación de 184 Gbps.
- Apilamiento de hasta 8 equipos de la serie B5, consiguiendo hasta 384 Puertos Ethernet 10/100/1000.
- Enrutamiento IPv4 (RIPv1/v2).
- Power Over Ethernet (PoE).

Figura 46. Switch Multicapa Marca Enterasys Serie B5 fuente: [70]

Desarrollo

Con toda la información obtenida en el Diagnóstico de la red es posible definir los escenarios que se asemejen al segmento de red que distribuye servicio a la red de datos de la ESIMEZ, y también los cambios que se pueden realizar a la topología física para una mejor administración de ésta con el fin de realizar las pruebas correspondientes y finalmente se implementen o entren en producción.

Estos escenarios buscan asemejarse a las condiciones actuales de la red de datos de la ESIMEZ para verificar si ambos protocolos de internet pueden convivir.

Los escenarios que se proponen siguen el mismo esquema que se tiene en la red Politécnica, es decir, bajo el modelo jerárquico de capas de Cisco Systems.

Despliegue IPv6

Conociendo la estructura de la red y los modelos de los equipos que la conforman, se realizó el Análisis planteado en el segundo paso correspondiente a la etapa del Diagnóstico, para poder crear escenarios que se asemejen a lo que existe en ESIMEZ; Actualmente el protocolo de enrutamiento que se emplea en todo el instituto es OSPF, se utiliza este protocolo debido a que es un estándar y todos

los dispositivos de red cuentan con él. Hay marcas que desarrollan sus propios protocolos de enrutamiento, sin embargo, solo se limitan a los dispositivos de la marca en específico. Para IPv6 también existe OSPF en la versión número tres (OSPFv3), y el primer escenario consiste en probar este protocolo de enrutamiento en el router ICX-7750-48F, que es con el que cuenta la ESIMEZ, y otro router de la marca Enterasys serie S4 que simule al router de la capa de distribución aunque en esta capa actualmente se cuenta con un router ICX-7750-48F, pero para fines de experimentación solo se cuenta con uno.

Es necesario analizar las posibles soluciones para la implementación (Planteado en la primera subetapa del Desarrollo), es decir, tomar en cuenta las prioridades de los administradores de la red, el personal técnico con el que se puede contar, los equipos que se podrán usar para realizar las maquetas (escenarios) y el presupuesto. Para el desarrollo de las maquetas de redes, se utilizó equipo muy similar al que se ocupa en la red de datos de la ESIMEZ; Con el administrador de la red se tuvo que consultar el sitio donde se podrá iniciar con la implementación, y así poder desarrollar las maquetas o escenarios de acuerdo con sus preferencias. Finalmente, como se requiere llevar a cabo una migración suave a IPv6, se deben aprovechar los recursos que se tienen sin que se hagan grandes gastos de inversión, por tal motivo los mecanismos de transición son fundamentales en este proyecto de investigación.

A continuación, se describen los escenarios propuestos para la implementación de IPv6 en ESIMEZ.

El diseño de este escenario debe tener un segmento de red configurado con ambos protocolos IPv4 e IPv6 (Doble Pila), que sería la forma en la que ESIME conviviría con IPv6. Y el resto de los segmentos solo con IPv6 para que se compruebe el funcionamiento del protocolo OSPFv3.

El segundo escenario es de capa 2, es decir, involucra a los switches conectados directamente al router de ESIMEZ, que cuando ya se encuentre enrutando las direcciones IPv6, se deben configurar los hosts con una dirección IPv6 además de la dirección IPv4 con la que ya cuentan. Y finalmente a los dispositivos que tengan capacidad de administración IPv6 también asignarles una dirección para que se puedan configurar de forma remota.

Por último, se realizó un escenario para comprobar el funcionamiento del servidor DHCPv6; Es importante mencionar que este servicio es el que le brinda acceso a la red a todos los usuarios de la red inalámbrica; Actualmente se asignan direcciones IPv4 privadas que salen a Internet mediante NAT (Traducción de Direcciones de Red). Al habilitar el servicio DHCPv6, no será necesario utilizar NAT para los dispositivos finales que soporten IPv6. Por lo tanto, se eliminarán las

desventajas que implica el uso de NAT, como son, la independencia de capas, el aumento de los retrasos de conmutación para aplicaciones en tiempo real como VoIP (Voz sobre IP), el modelo extremo a extremo, etc.

Estos escenarios pueden funcionar como una guía para las demás dependencias del Instituto, pues cada escuela cuenta con un Enrutador, y para el caso donde se cuente con un enrutador que no soporte IPv6 es posible la comunicación mediante túneles.

El primer paso es que toda la red tenga conectividad IPv6 para que posteriormente se pueda solicitar el servicio de Internet (Más Utilizado) al Proveedor bajo ambos Protocolos (IPv4 e IPv6).

NOTA: Los escenarios planteados se encuentran en el capítulo V (pruebas y resultados).

Rediseño Topología ESIMEZ

Conociendo las condiciones de la red, y las capacidades de los equipos, el diseño y la propuesta (definidos en el Marco Metodológico), son el siguiente paso, pues ya se cuenta con toda la información necesaria para proponer cambios que beneficien a la red de datos de la ESIMEZ. Ya han sido definidos los escenarios en la subetapa anterior sobre el Análisis de Posibilidades.

Ya se mencionó la problemática que existe en la red de datos de la ESIMEZ, por lo que se tuvo que levantar la topología física de la red para tener información suficiente y así proponer cambios en la red. La red Politécnica cuenta mínimo con un Enrutador (Router) en cada una de las diferentes Escuelas y Dependencias (Capa Acceso), el cual distribuye los servicios que se generan desde la capa del núcleo.

En ESIME Zacatenco se cuenta un Router Brocade ICX-4750-48F desde el año 2016, en esta actualización también se instalaron Switches de la misma marca en todos los edificios; Aunque especialmente en el edificio 1, donde todos los switches son del mismo modelo ICX-7250-48P. En los demás edificios solo se instalaron estos mismos en los puntos de conexión Intermedia (ICC) como se puede observar en la Figura 47. Este modelo aún no se conecta a la red, aunque ya está instalado en cada uno de los cuartos de telecomunicaciones correspondientes a los ICCs, de acuerdo con el diagnóstico realizado, ya se conocen las capacidades de este modelo y se busca explotarlo dentro de la red.

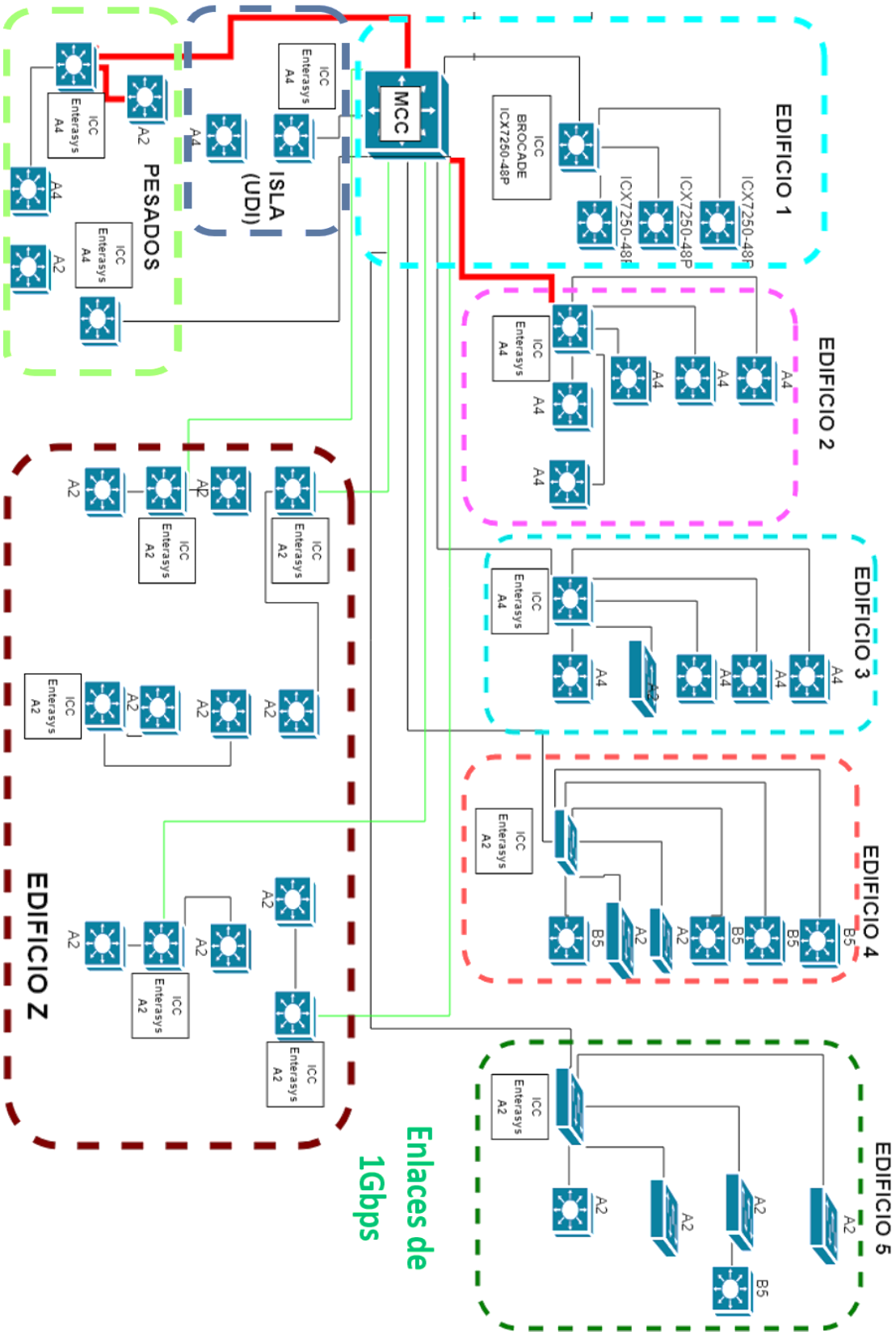


Figura 47. Diagrama General red de datos ESIME Zacatenco Actual (enlaces 1Gbps).

El Modelo ICX-7250-48P es compatible con los demás switches que están en ESIMEZ, pero con capacidades de procesamiento mayores. En ESIMEZ existen varios modelos de equipos, que se pueden apreciar en la siguiente tabla, en la que también se señala si soportan IPv6 o no.

EQUIPO	Marca	Modelo	Compatibilidad IPv6
Switch	Enterasys	A2H124-24	NO
Switch	Enterasys	A2H124-24P	NO
Switch	Enterasys	A4H124-24P	SI
Switch	Enterasys	B5G124-24P2	SI
Switch	Brocade	ICX7250-48P	SI
Router	Brocade	ICX7750-48F	SI

Tabla 7. Compatibilidad de Dispositivos en ESIMEZ con IPv6

Los switches son equipos de capa 2, para estos la implementación del protocolo IPv6 es transparente (solo se configura la dirección IPv6 a los hosts), se puede observar en la tabla anterior que algunos tienen compatibilidad con IPv6; esto quiere decir que al dispositivo se le puede asignar una dirección IPv6 con fines de administración, con tal de que se pueda acceder a estos equipos de forma remota a través de diferentes protocolos; La Dirección de Cómputo y Comunicaciones accede a los equipos de capa 2 y capa 3 a través del protocolo SSH (Secure SHell) con el fin de resolver los problemas sin tener que presentarse donde se requieran realizar cambios. Debido a esto, es necesario que se actualicen los equipos que no soportan IPv6, como son los del modelo de la serie A2; Para un mejor funcionamiento se propone que se adquieran equipos que tengan capacidades de 10Gbps en cada puerto, de esta manera mejorarían notablemente los servicios en tiempo real para los usuarios.

Ahora es posible aumentar el ancho de banda en los medios que se encuentran entre el Router de la ESIME-Zac (ICX-7750-48P) y los Switches Brocade ICX-7250-48P, pues estos equipos pueden manejar en cada puerto un

ancho de Banda de hasta 10Gbps; De esta manera esta manera mejoran los servicios de voz sobre IP (conexión en tiempo real), streaming, y multimedia entre el Switch Principal de ESIME-Zac (MCC) y los puntos de conexión intermedios (ICC) como se aprecia en la Figura 48.

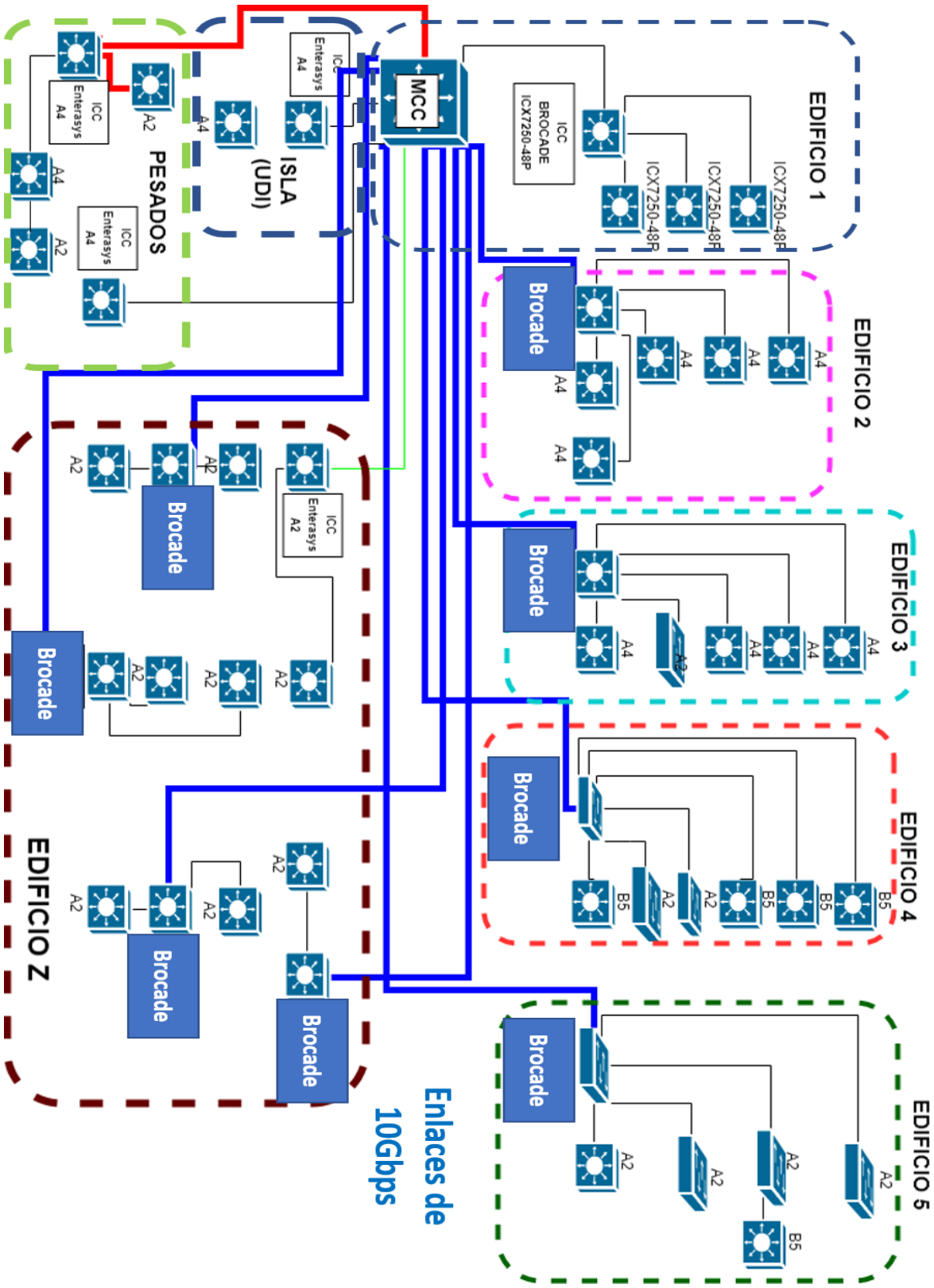


Figura 48. Diagrama General Red de datos ESIME Zacatenco Rediseño (Configurando Equipo Brocade).

Finalmente, se requiere que se adquieran equipos más recientes que cuenten por lo menos con soporte a IPv6 de administración, para que los encargados del Departamento de Conectividad de la DCyC puedan acceder a ellos de forma remota y los configuren cuando se presenten fallas o se deba dar mantenimiento.

Los equipos señalados en el siguiente diagrama (Figura 49) no cuentan con esta característica.

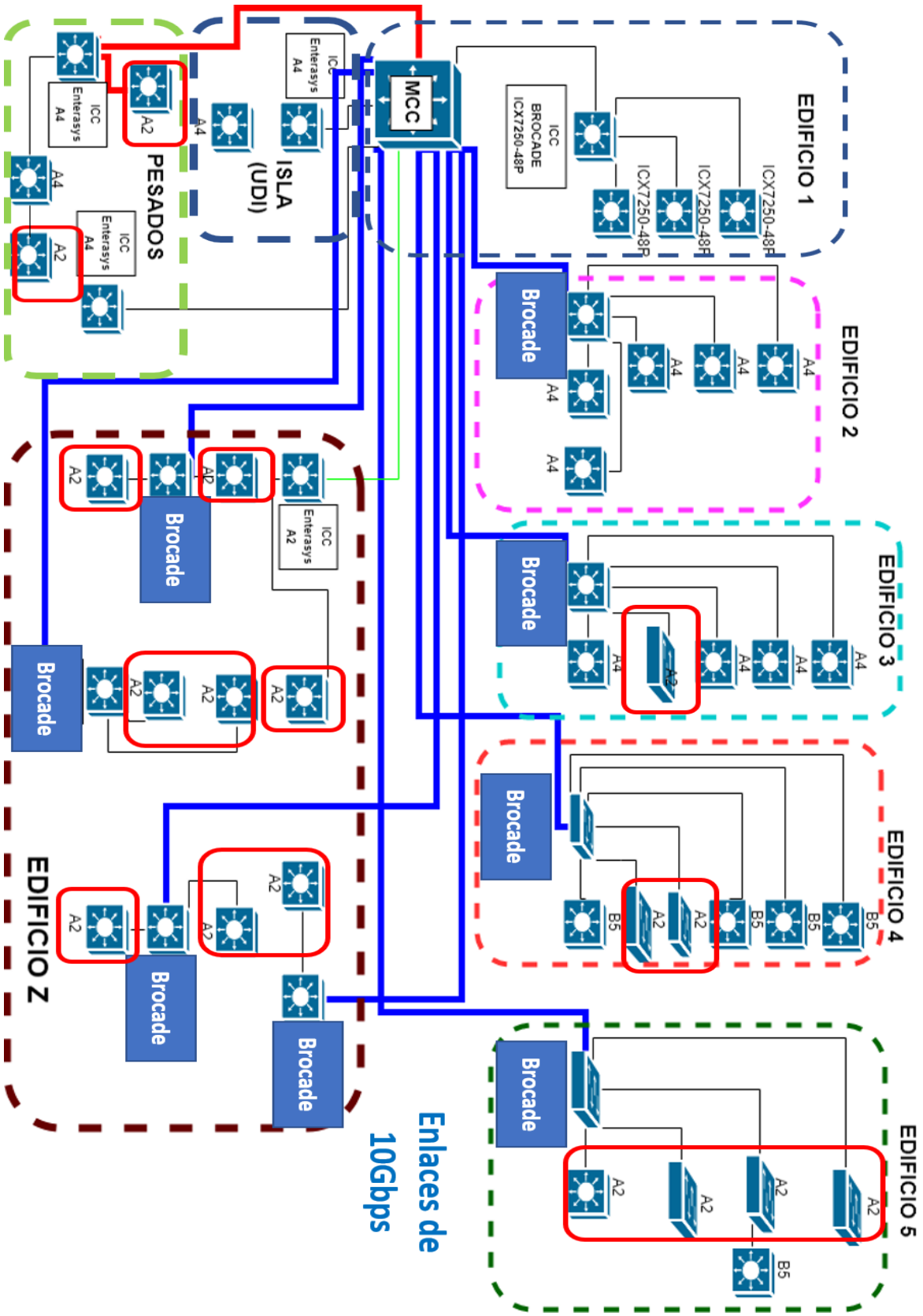


Figura 49. Dispositivos sin soporte a IPv6 ESIME Zacatenco

Implementación

Para la etapa de implementación es necesario llevar a cabo un plan en el que se aplique este procedimiento en cada una de las escuelas, centros de investigación y edificios de gobierno que forman parte de la red (Plan de implementación). En este plan se debe priorizar el correcto funcionamiento de la red de datos de la ESIMEZ durante las pruebas que se realicen, para que no se afecte el servicio a los usuarios de la red.

Se debe aplicar la etapa de diagnóstico a cada dependencia, se deben proponer escenarios semejantes a las diferentes topologías, conectar los escenarios en paralelo con la red que se encuentre en producción. Es muy importante llevar a cabo las Pruebas necesarias para que se puedan medir ciertos parámetros importantes para los administradores de red, y cuando los encargados lo autoricen, comenzar con la puesta en producción en todos los dispositivos de la red en cuestión.

La documentación es necesaria para que las dependencias que quieran realizar cualquier cambio a su red puedan basarse en proyectos de implementación previos. Sin necesidad de realizar nuevamente un diagnóstico detallado de su red.

CAPÍTULO V: PRUEBAS Y RESULTADOS

Se crearon diferentes escenarios de prueba con modelos de dispositivos de red que abundan en la red Politécnica. Dichas pruebas se realizaron en el departamento de Conectividad en la Dirección de Cómputo y Comunicaciones en el edificio inteligente.

Escenario 1 (Experimental)

En la Figura 50 se plantea un escenario para probar el funcionamiento de IPv6 en convivencia con IPv4 en una red ya en producción. Este escenario se asemeja a la conexión que existe entre el Enrutador Principal en la ESIMEZ (Brocade ICX-7750-48F) de la capa de acceso con el Enrutador de la capa de Distribución (Enterasys S4 para este experimento) que les brinda servicio a varias escuelas de Zacatenco. Como se puede observar, la parte derecha del diagrama correspondería a la ESIME-Zac con direccionamiento IPv4 e IPv6. En esta prueba se habilita OSPFv3, que es el protocolo de enrutamiento estándar para IPv6. Actualmente se utiliza OSPF para IPv4 debido a las diferentes marcas de dispositivos de red con los que cuenta el Instituto, y este protocolo de enrutamiento es un estándar que tienen todos los dispositivos de capa 3. En el apartado "ANEXOS" se pueden encontrar las configuraciones con los comandos correspondientes para cada uno de los escenarios.

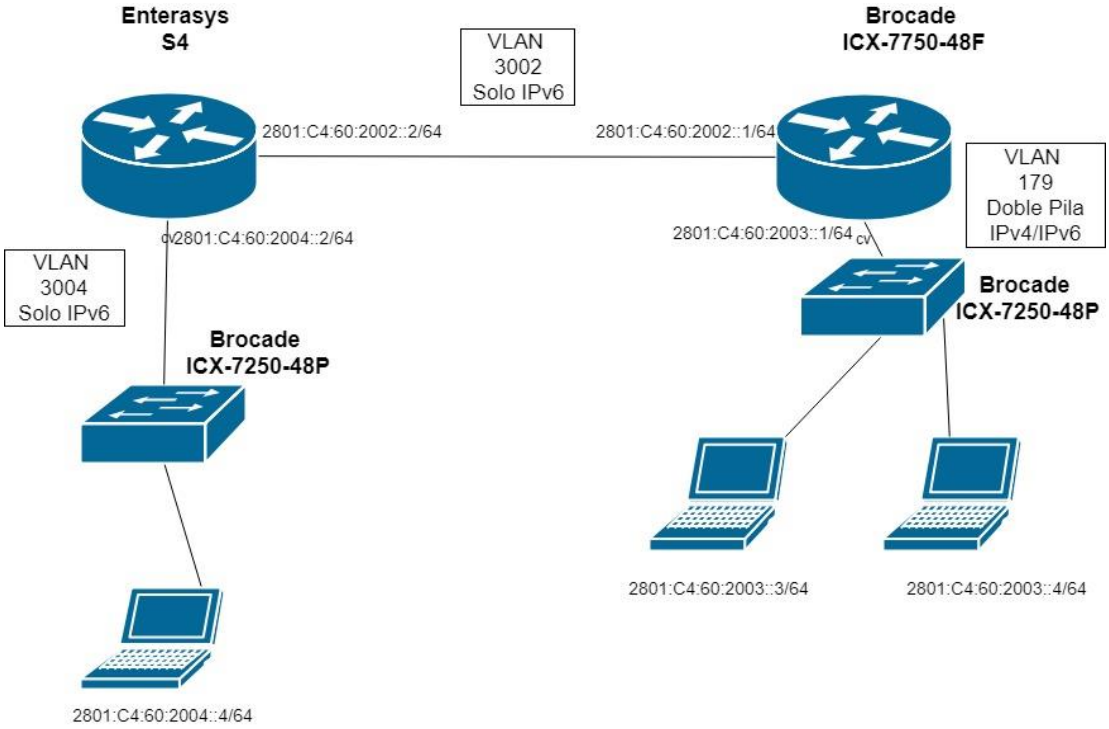


Figura 50. Escenario 1 Propuesto (Capa de acceso y distribución)

En este escenario la topología se divide en tres prefijos de red:

1. 2801:c4:60:**2004**::/64
2. 2801:c4:60:**2002**::/64
3. 2801:c4:60:**2003**::/64

En los segmentos correspondientes a los prefijos 2801:c4:60:**2004**::/64 y 2801:c4:60:**2002**::/64 se configuró únicamente el protocolo IPv6 (IPv6 Only); La configuración de los equipos fue en doble pila (dual stack) para el segmento que corresponde al prefijo 2801:c4:60:**2003**::/64, por lo tanto, conviven IPv4 e IPv6 pues en este segmento ya se tenía configurada una subred en producción IPv4 en el Switch ICX-7750-48F.

Los modelos de los dispositivos de red empleados en éste primer escenario fueron los siguientes:

- Enterasys Serie S4 (Router)
- Brocade ICX-7750-48F (Router)
- Brocade ICX.7250-48P (Switch capa 2)

CONFIGURACIÓN DE DISPOSITIVOS

El procedimiento para crear esta topología consistió en conectar equipo por equipo, mientras se verificaba su respectiva conexión a nivel IP con el comando PING después de haber asignado las direcciones IPv6 estáticas correspondientes a los segmentos de red en los ordenadores. Después se configuró el protocolo de enrutamiento dinámico OSPFv3.

De acuerdo con la Figura 50, el desarrollo de esta topología comenzó por el equipo Enterasys S4 hacia la derecha. El cliente informático utilizado para la configuración de los dispositivos fue Putty dentro de un sistema operativo Windows 10.

ENTERASYS S4

Primero se realizaron las configuraciones al **Router Enterasys Serie S4**, para esto fue necesario conectarse al dispositivo con el cable de consola.

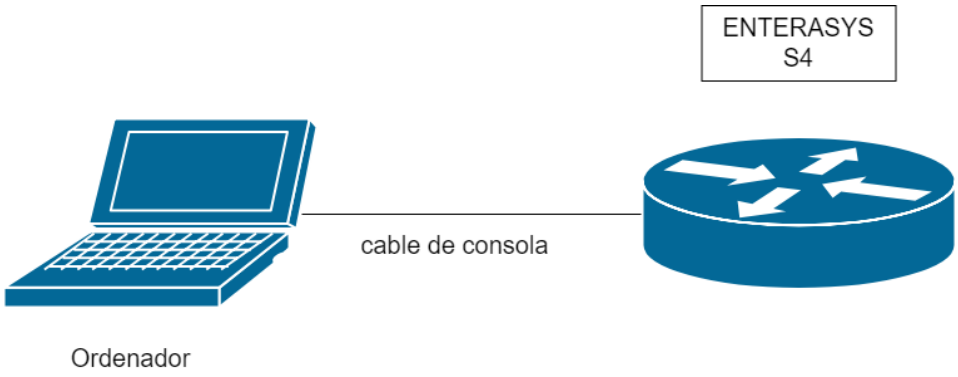


Figura 51. Conexión al Router Enterasys Serie S4.

Después, mediante la aplicación del cliente informático Putty se accedió al dispositivo ingresando las credenciales de seguridad correspondientes y se configuró la VLAN 3004 y la VLAN 3002 en los puertos correspondientes (Figura 50). Después se activó el protocolo de enrutamiento para IPv6 (OSPFv3), se debe asignar el ID de proceso para OSPF (10.220.255.81) en las interfaces que estarán involucradas con el protocolo. Se le asignó una dirección IPv6 a las interfaces VLAN 3002 (2801:c4:60:2002::2/64) dentro del modo de ruteo y se activó el protocolo OSPFv3 indicando el área correspondiente (0.0.0.0), se debe especificar el mismo ID del proceso creado anteriormente (10.220.255.81).
Por último, se repite este proceso para el segmento 2801:c4:60:2004::/64 de la VLAN 3004.

BROCADE ICX-7250-48P

Para este proceso se conectó el ordenador a este dispositivo con el cable de consola, también se conectó al Router Enterasys S4.

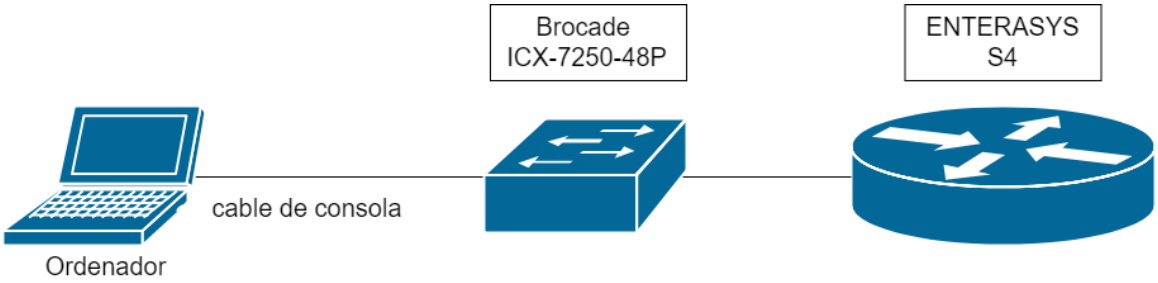


Figura 52. Conexión a Switch Brocade ICX-7250-48P para configuración de VLANs

Se configuró la VLAN 3004 en el segmento del prefijo 2801:c4:60:2004::/64 a todos los puertos switch Brocade ICX-7250-48P.

Por último, se configura una dirección IPv6 con fines de administración (2801:c4:60:2004::3/64).

NOTA: Esta configuración se realizó en ambos dispositivos ICX-7250-48P.

BROCADE ICX-7750-48F

Para este proceso se hizo la conexión del ordenador con el switch ICX-7750-48F usando el cable de consola, Y también hizo la interconexión con el Router Enterasys S4.

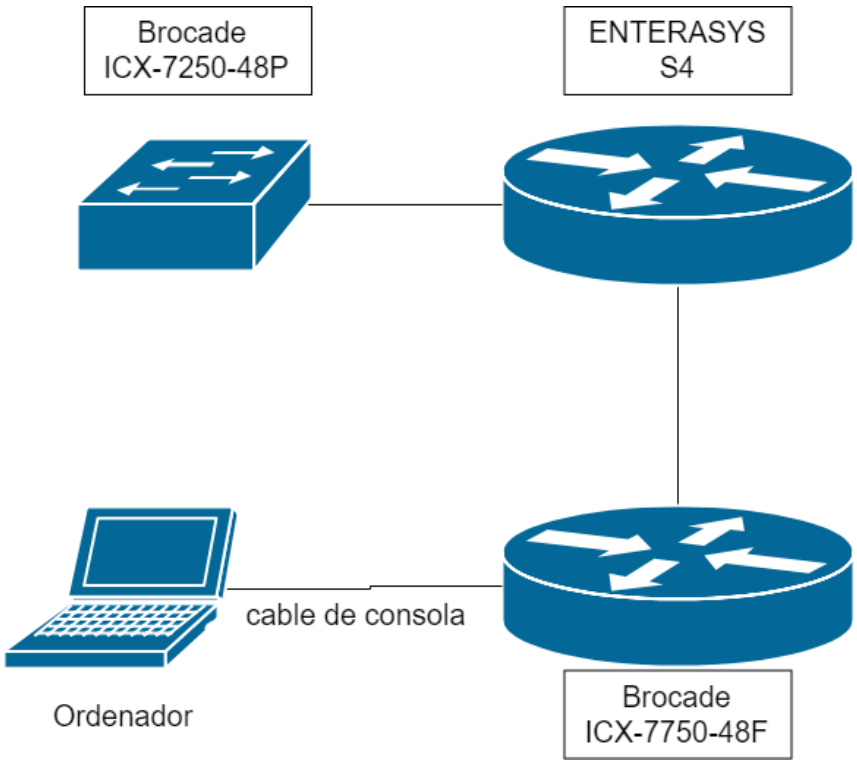


Figura 53. Conexión de Router ICX-7750-48F para su configuración.

Se configuró la VLAN 3002 para el segmento con el prefijo 2801:c4:60:**2002::**/64 al puerto 21. Después se asignó la dirección IPv6 2801:c4:60:**2002::1**/64 a la VLAN 3002 y la dirección IPv6 2801:c4:60:**2003::1**/64 a la VLAN 179 previamente configurada y bajo el protocolo OSPF (Siguiendo el esquema de la figura 50).

Se configuró el protocolo de ruteo OSPFv3 para IPv6 en la VLAN 179.

La VLAN 3002 se creó bajo el nombre “IPV6 7750 A S4” en el puerto 21 y posteriormente se le habilitó el protocolo OSPFv3 y se le asignó la dirección IPv6 de la interfaz.

La VLAN 179 ya estaba previamente configurada en el dispositivo, con su respectiva dirección IPv4 asignada y el protocolo de enrutamiento OSPF para IPv4.

En la misma VLAN 179 se habilitó IPv6, se asignó la dirección IPv6 a la interfaz y se configuró el protocolo OSPFv3.

Configuración de direcciones IP en Hosts

Las direcciones configuradas para este escenario son estáticas, en la Figura 54 se puede apreciar la interfaz gráfica de conexiones de red en Windows 10 para configurar la dirección IPv6 correspondiente, para que posteriormente se realicen las pruebas de conexión entre los dispositivos que conforman el escenario.

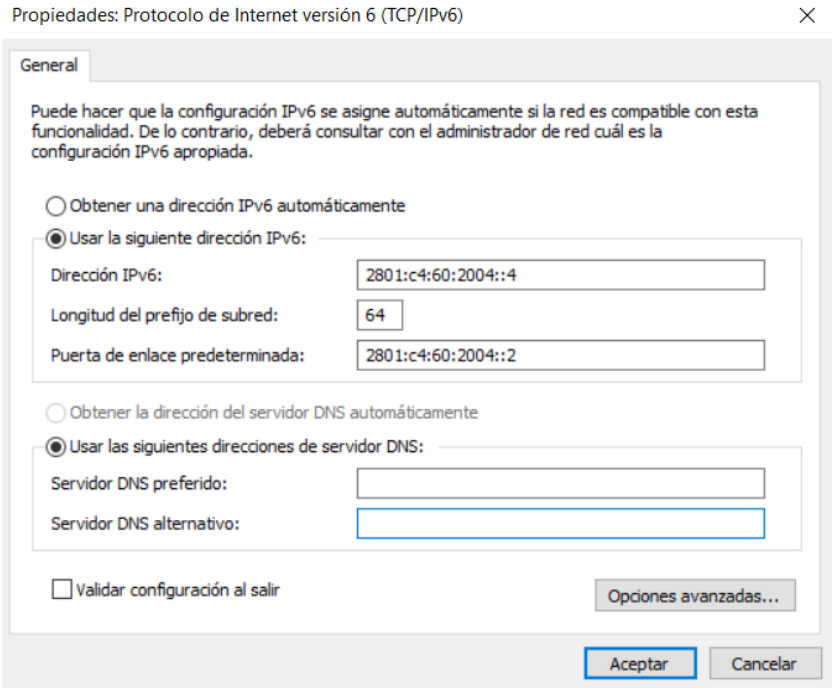


Figura 54. Configuración de Dirección IPv6 2801:c4:60:2004::4/64 (PC1)

Este ordenador (PC1) corresponde al segmento de red 2801:c4:60:**2004**::/64, y se le asignó la dirección 2801:c4:60:2004::4/64 y la puerta de enlace predeterminada (Default Gateway) 2801:c4:60:2004::2/64, correspondiente a la interfaz en el router S4.

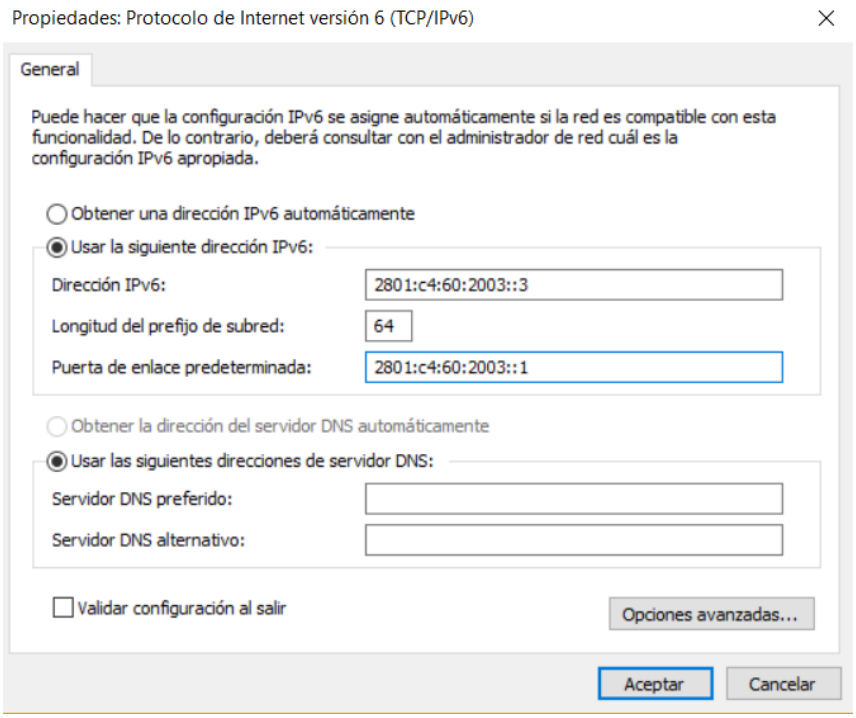


Figura 55. Configuración de Dirección IPv6 2801:c4:60:2003::3/64 (PC2)

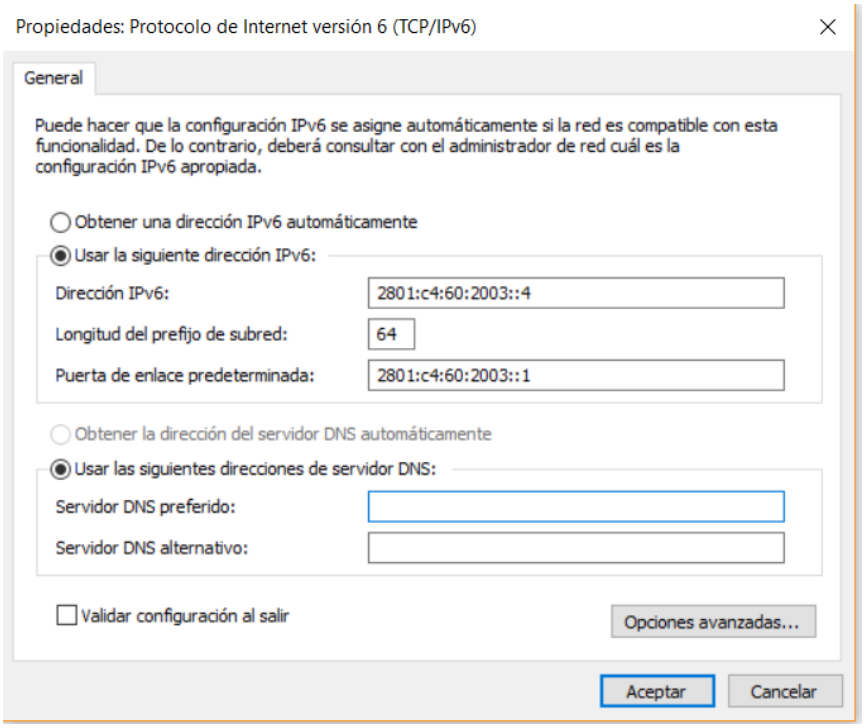


Figura 56. Configuración de Dirección IPv6 2801:c4:60:2003::4/64 (PC3)

Las figuras anteriores (Figura 55 y Figura 56), corresponden a la configuración de la dirección IP en la PC2 y PC3, como se puede observar, ambos ordenadores forman parte de la misma red 2801:c4:60:2003::/64.

En estos ordenadores ya se disponía de direcciones IPv4 estáticas dentro de la VLAN 179, la cual ya se encontraba en producción bajo IPv4, a esta misma VLAN se le asignó la dirección IPv6 2801:c4:60:2003::1/64 (Puerta de enlace predeterminada). De esta forma, en este segmento de red ambos protocolos de internet convivían sin ningún problema.

Se hizo un ping a la PC1 (2801:c4:60:2004::4/64) desde la PC3 (2801:c4:60:2003::4/64) a través de la ventana de comandos del sistema operativo Windows 10 con el comando “ping -6 2801:c4:60:2004::4” como se puede apreciar en la Figura 57.

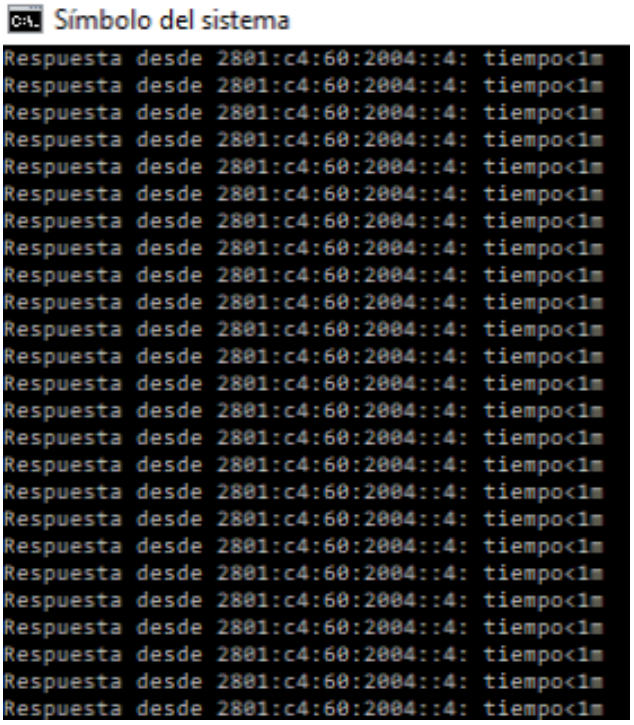


Figura 57. Ping a PC1 (2801:c4:60:2004::4/64) desde PC3 (2801:c4:60:2003::4/64).

Para verificar la ruta del paquete se utilizó el comando “tracert”, como se puede apreciar en la siguiente captura (Figura 58) se muestran los saltos a las diferentes puertas de enlace configuradas en cada router: Primero sale por la puerta de enlace correspondiente al segmento 2801:c4:60:2003::1, después al 2801:c4:60:2002::2 para finalmente llegar al host con la dirección IPv6 2801:c4:60:2004::4.

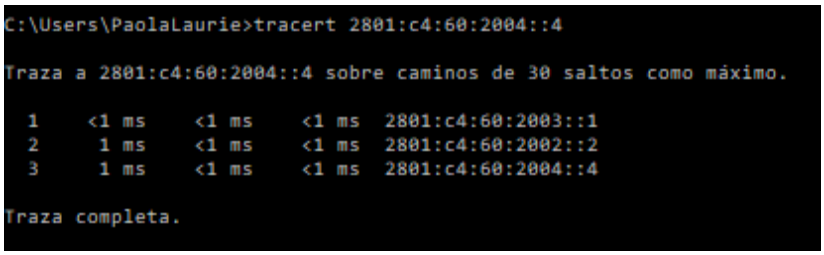


Figura 58. Ruta del Paquete desde PC1 a PC3 usando el comando "tracert"

Como se mencionó anteriormente, este escenario se asemeja a la conexión entre capa de distribución y acceso, y habilitando el protocolo OSPFv3 cada usuario que cuente con una dirección IPv6 tendrá acceso a los servicios de la red Politécnica una vez que estos se migren a IPv6.

Escenario 2 (Modelos ESIMEZ)

En esta maqueta (Figura 59) se hizo una representación de cómo se deberían configurar los switches en los edificios de ESIME-Zac con el fin de que se aproveche el equipo de la marca Brocade que actualmente no se utiliza (ICX-4250-48P); Cabe señalar que debido a que estos dispositivos son de capa dos (Enlace de Datos), simplemente basta con configurar las IPs estáticas (v4 y v6) con el mismo prefijo de red en cada host; Aunque es posible configurar una dirección IPv6 de administración a los switches que lo soporten, lo cual permite emplear el protocolo SSH (Secure SHell) que es muy utilizado en la DCyC para conectarse de manera segura a los equipos de capa 2 y capa 3 remotamente.

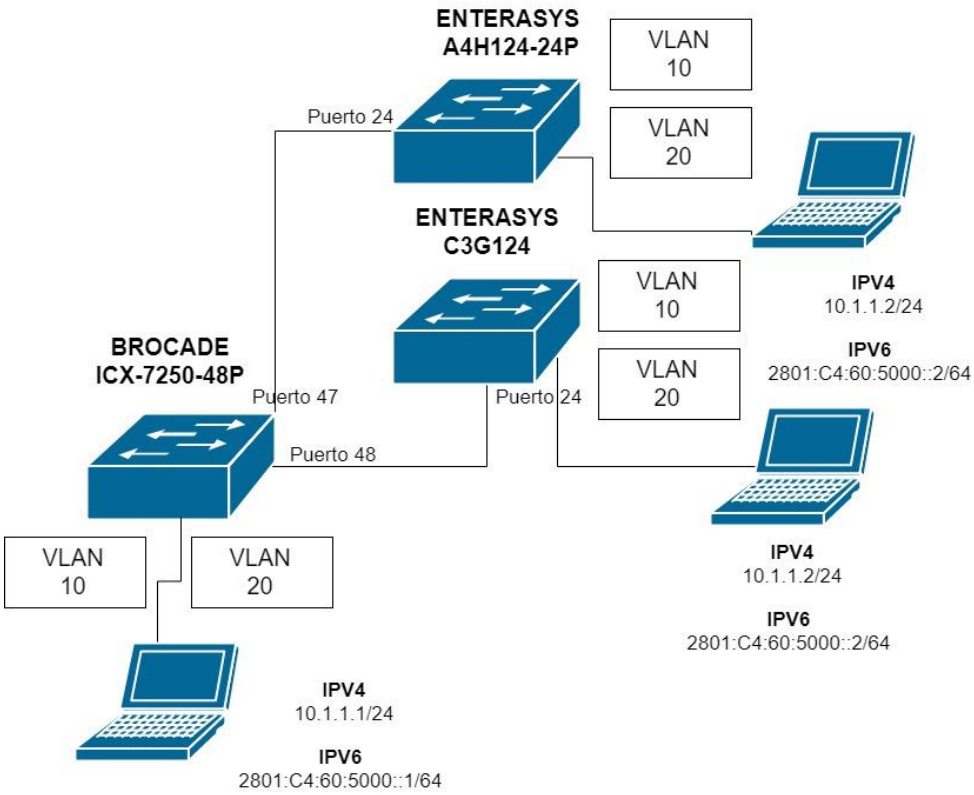


Figura 59. Escenario 2 Propuesto (Modelos ESIMEZ)

Para esta prueba se configuraron tres computadoras con el prefijo de red 10.1.1.0/24 para IPv4 y 2801:c4:60:5000::/64 para IPv6. De esta manera ambos protocolos conviven mediante el mecanismo de transición Doble Pila (Dual Stack).

Los modelos de los dispositivos de red empleados en este escenario fueron los siguientes:

- Brocade ICX.7250-48P
- Enterasys Serie C3G124
- Enterasys Serie A4H124-24P

CONFIGURACIÓN DE DISPOSITIVOS

El procedimiento para crear esta topología consistió en conectar equipo por equipo, mientras se verificaba su respectiva conexión con el comando PING después de haber asignado las direcciones IPv6 estáticas e IPv4 correspondientes a los equipos.

De acuerdo con la figura 59 el desarrollo de esta topología comenzó por el equipo de la marca Brocade (ICX-7250-48P) hacia la derecha. El cliente informático utilizado para la configuración de los dispositivos fue Putty dentro de un sistema operativo Windows 10.

BROCADE ICX-7250-48P

Con el cable de consola se accedió al dispositivo para su configuración.

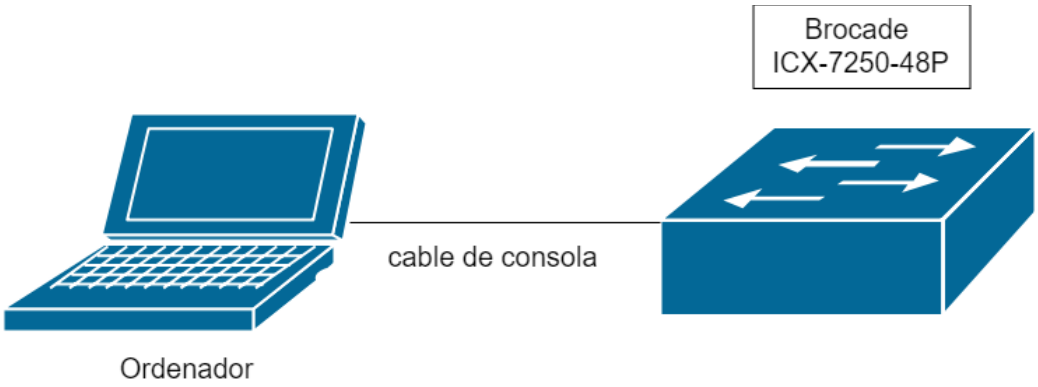


Figura 60. Conexión al Switch Brocade ICX-7250-48P.

Se accedió al dispositivo a través de la aplicación del cliente informático Putty; Se crearon las VLANs propuestas en el escenario de la figura 59 y se asociaron a los puertos (VLAN 10 puertos 1 – 24 y VLAN 20 puertos 25 - 46). Se definieron los Puertos Troncales para hacer la conexión con otros switches que tengan las mismas VLANs.

Después se configuraron las direcciones IP al switch con fines de administración para configurarlo remotamente mediante el protocolo SSH; 10.1.1.100/24 para IPv4 y 2801:c4:60:5000::100/64 para IPv6.

Finalmente se activa el protocolo Secure Shell (SSH) en el switch para la configuración remota definiendo usuario y contraseña; Y también las direcciones IP de los hosts que podrán acceder al dispositivo mediante SSH.

ENTERASYS C3G124-24

El puerto 48 (troncal) del Switch ICX-7250-48P se conectó al puerto 24 (troncal) del Switch Enterasys C3G124-24 mediante UTP. Y se accedió a éste a través del cable de consola.

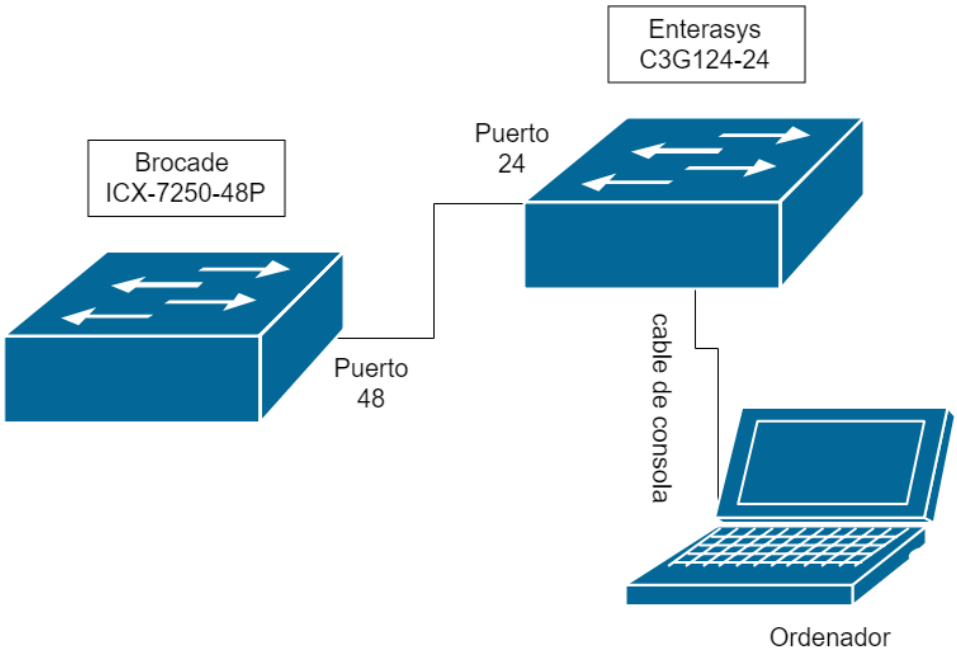


Figura 61. Conexión de Switch Enterasys C3G124-24 para configuración

Se crearon las VLANs propuestas en el escenario de la figura 59 y se asociaron a los puertos correspondientes (VLAN 10 puertos 1 - 12, VLAN 20 puertos 12 - 23).

Después se configuraron los puertos troncales (puerto 24).

Finalmente se asignaron las direcciones IP para administración 10.1.1.200/24 para IPv4 y 2801:c4:60:5000::101/64 para IPv6.

ENTERASYS A4H124-24P

El puerto 47 (troncal) del Switch ICX-7250-48P se conectó al puerto 24 (troncal) del Switch Enterasys A4H124-24P mediante UTP. Y se accedió a éste a través del cable de consola.

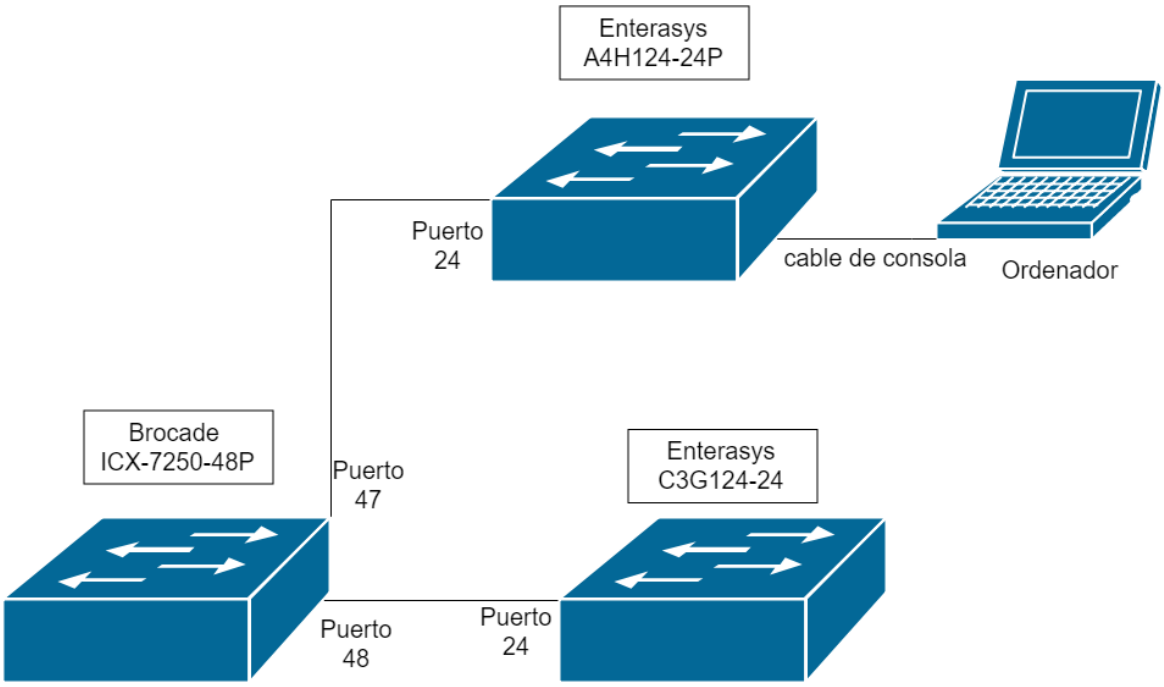


Figura 62. Conexión de Switch Enterasys A4H124-24P para configuración

Se crearon las VLANs propuestas en el escenario de la figura 59 y se asociaron a los puertos correspondientes (VLAN 10 puertos 1 - 12, VLAN 20 puertos 12 - 23).

Después se configuraron los puertos troncales (puerto 24).

Finalmente se asignaron las direcciones IP para administración 10.1.1.3/24 para IPv4 y 2801:c4:60:5000::102/64 para IPv6.

Configuración de direcciones IP en Hosts

Las direcciones configuradas para este escenario son estáticas, en las Figuras 64 y 66 se puede apreciar la interfaz gráfica de conexiones de red en Windows 10 para configurar la dirección IPv6 correspondiente. Se utilizaron dos ordenadores, uno se mantuvo conectado en el Switch Brocade simulando los Puntos de Interconexión Intermedios (ICCs) ubicados en ESIME-Zac, donde actualmente existen equipos de esta marca sin utilizarse.

Se utilizo el prefijo de red 10.1.1.0/24 para IPv4 y el prefijo 2801:c4:60:5000::/64 en todo el escenario, tal y como se administra la red de datos

de la ESIMEZ, donde cada segmento de las interfaces del Router que se encuentra en la ESIMEZ se asocia a una subred por edificio, conectándose a cada ICC.

En el ordenador conectado en el Switch de la marca Brocade (PC1) se configuró la dirección 10.1.1.1/24 para IPv4 y 2801:c4:60:5000::1/64 para IPv6 tal y como se puede apreciar en las Figuras 63 y 64.

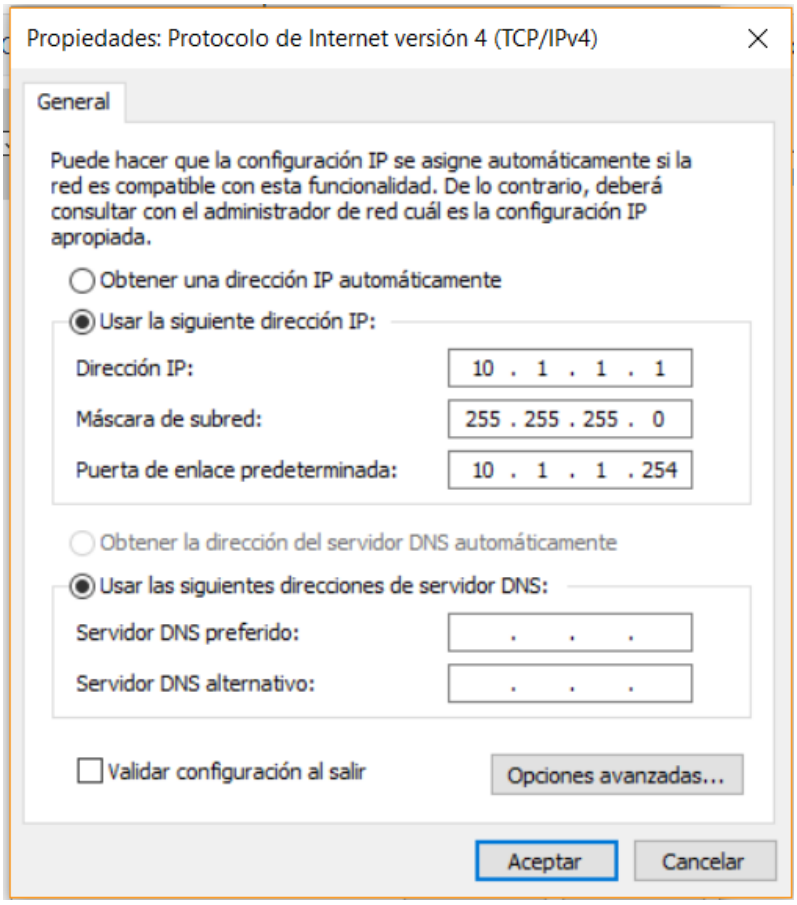


Figura 63. Configuración Dirección IPv4 en PC1.

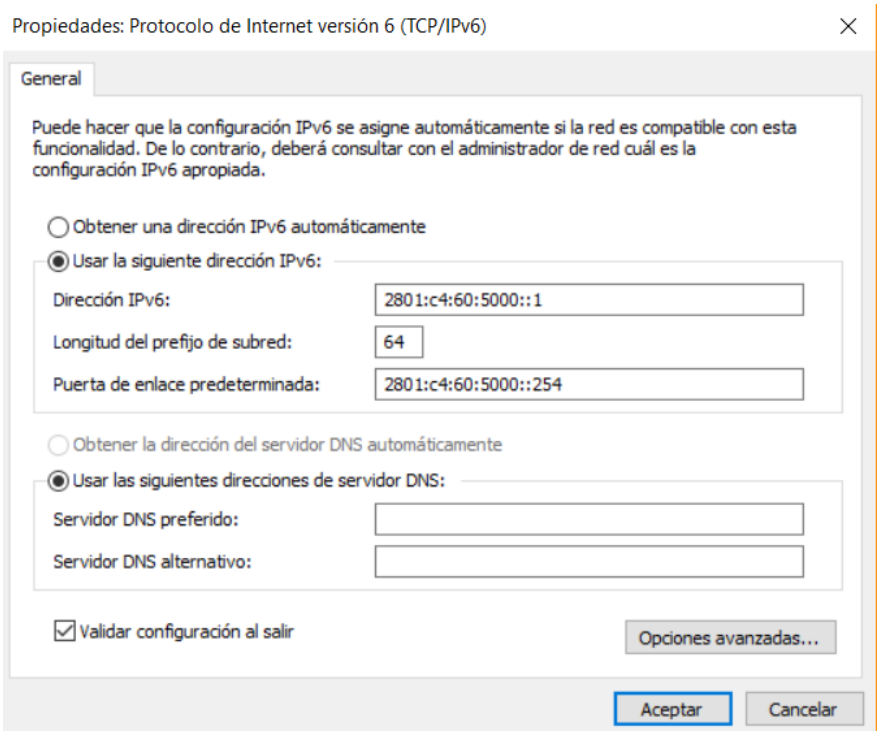


Figura 64. Configuración Dirección IPv6 en PC1.

En el segundo ordenador (PC2) se conectó en los switches restantes y se le asignó la dirección IPv4 10.1.1.2/24 y la dirección IPv6 2801:c4:60:5000::2/64 tal y como se aprecia en las Figuras 65 y 66.

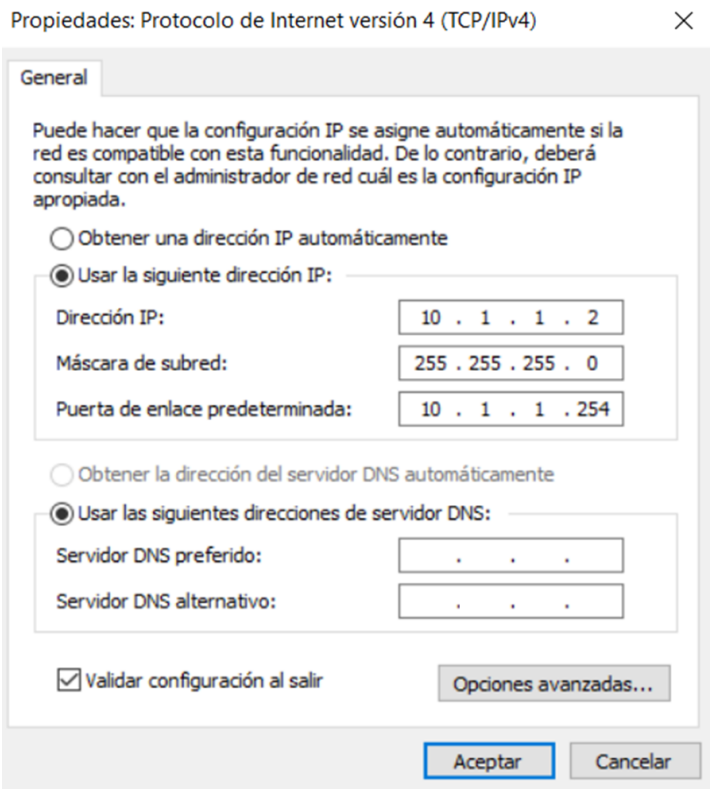


Figura 65. Configuración Dirección IPv4 en PC2.

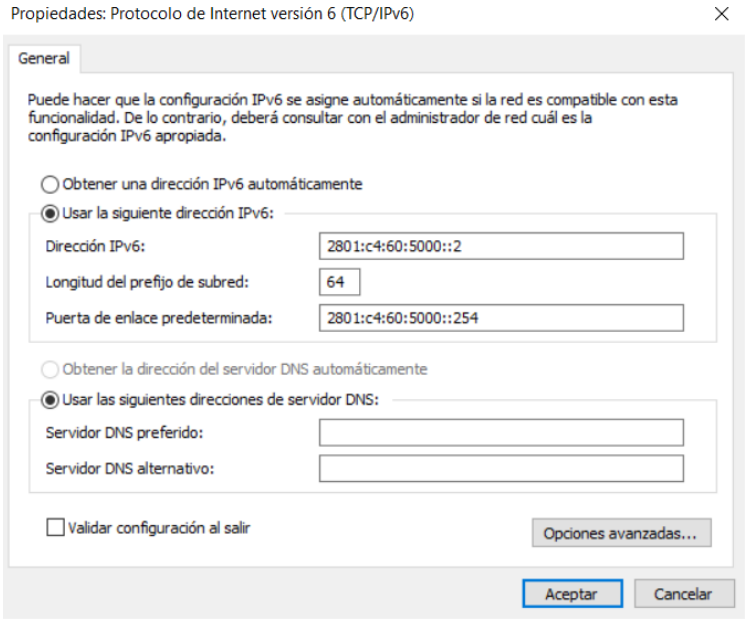


Figura 66. Configuración Dirección IPv6 en PC2.

En las Figuras 67 y 68 se comprueba la conexión mediante SSH utilizando PuTTY con IPv6.

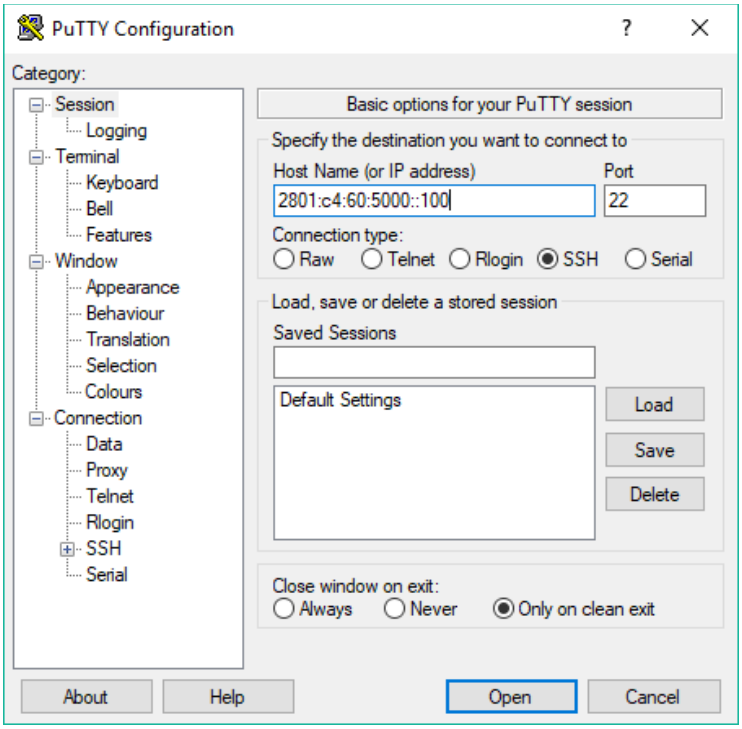


Figura 67. Conexión a través de SSH mediante IPv6 usando el cliente informático PuTTY

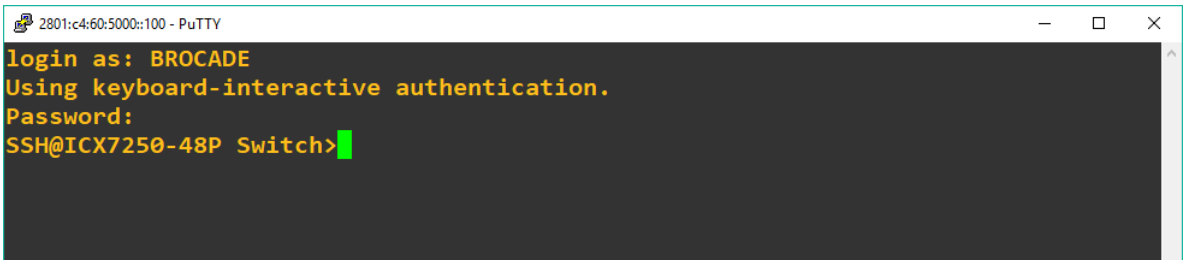


Figura 68. Accediendo a la Línea de Comandos con IPv6 usando PuTTY.

Se hizo un ping desde la PC2 conectada al switch A4H124-24P al switch Brocade por ambos protocolos, y la conexión se realizó sin ningún inconveniente; Comprobando de esta manera la compatibilidad de ambos protocolos mediante Doble Pila.

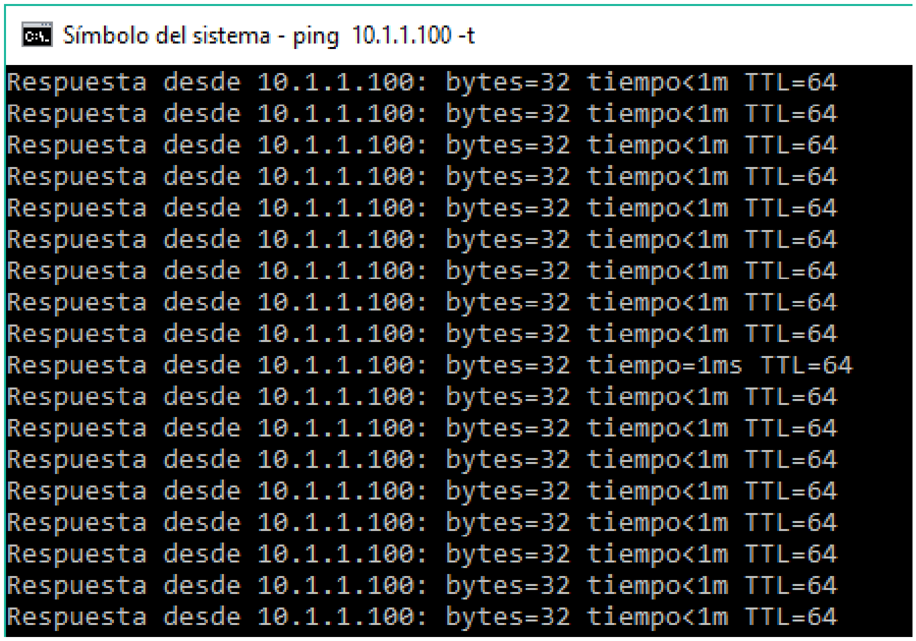


Figura 69. Ping IPv4 a Switch Brocade ICX-7250-48P desde PC2

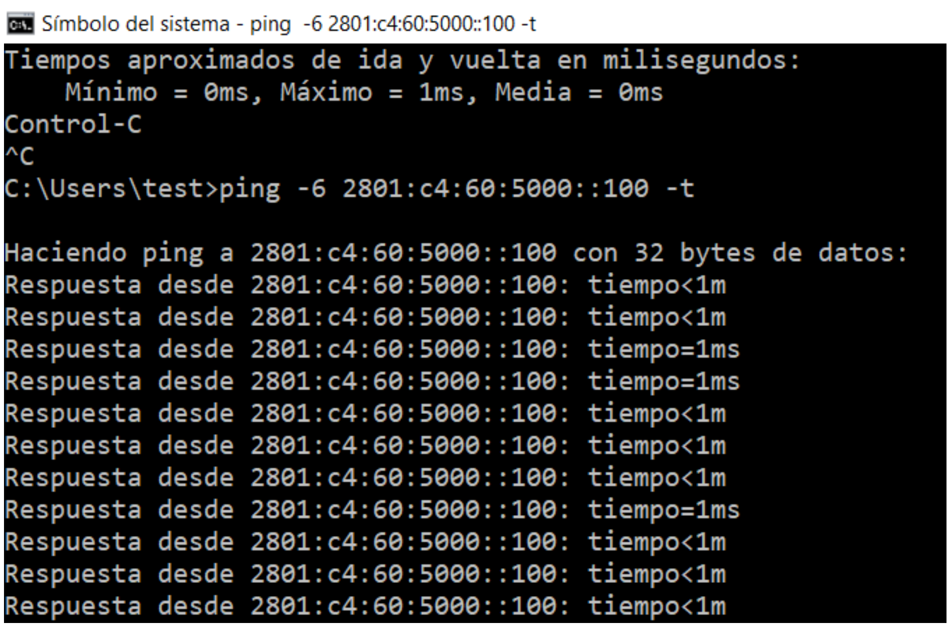


Figura 70. Ping IPv6 a Switch Brocade ICX-7250-48P desde PC2

En este escenario se pudo comprobar el funcionamiento de ambos protocolos en doble pila, lo cual es recomendado para el comienzo de cualquier migración a IPv6, hablando específicamente de ESIME Zacatenco no fue necesario utilizar la técnica de tuneleo, pues los enrutadores que forman la trayectoria desde la capa de acceso hasta el núcleo de la red en la Dirección de Cómputo y Comunicaciones cuentan con soporte a IPv6.

Escenario 3 (DHCPv6)

Como se mencionó anteriormente, los usuarios de la red inalámbrica del IPN se conectan de forma dinámica con DHCP, con direcciones IPv4 privadas, que posteriormente salen a internet empleando NAT. En la Figura 71 se puede apreciar el escenario establecido para el direccionamiento dinámico de IPv6.

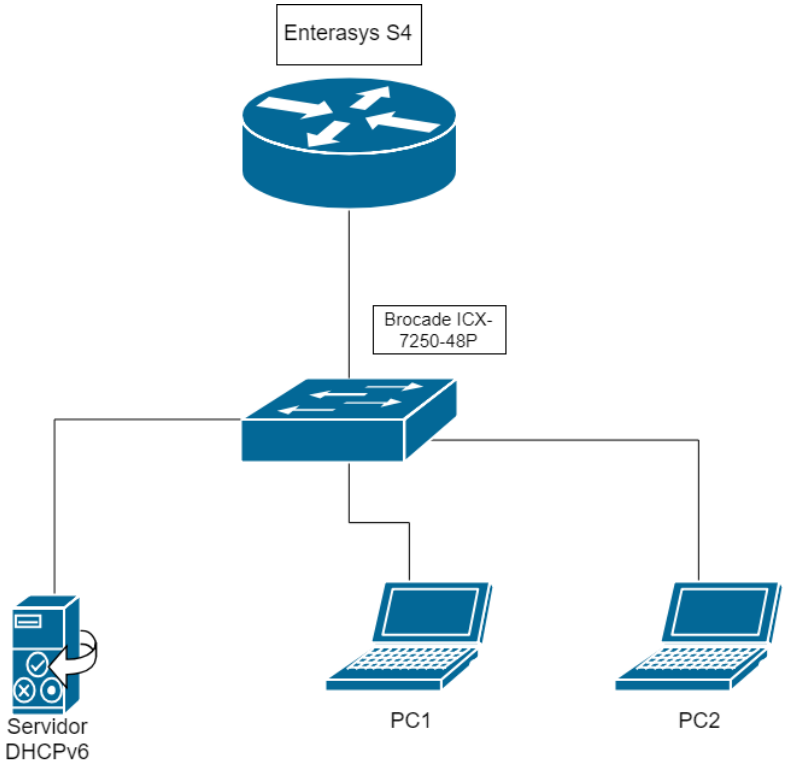


Figura 71. Diagrama Escenario 3 (DHCPv6)

Actualmente el servidor DHCP para IPv4 se encuentra en la capa de núcleo de la red Politécnica, y es administrado por el departamento de conectividad en la DCyC. El escenario que aquí se presenta es para comprobar el funcionamiento de DHCPv6.

Como se puede apreciar, se utilizó un Enrutador Enterasys S4 y un Switch Brocade ICX-7250-48P.

El Enrutador debe tener configurado un protocolo de enrutamiento, para este caso es el que se había configurado en el Escenario 1, es decir, OSPFv3. Para este caso se utilizó el segmento 2801:c4:60:**2004**::/64 del primer escenario.

El switch debe tener configuradas las VLANs que los administradores señalen; para este caso se les asignó la misma VLAN a todos los puertos.

El ordenador donde se instaló el servidor DHCPv6 tiene el Sistema Operativo Linux Debian; El servidor instalado es el ISC-DHCP-server, y el rango que se configuró para el segmento 2801:c4:60:**2004**::/64 fue desde 2801:c4:60:2004::6 hasta 2801:c4:60:2004::10 tal como se observa en la Figura 72.

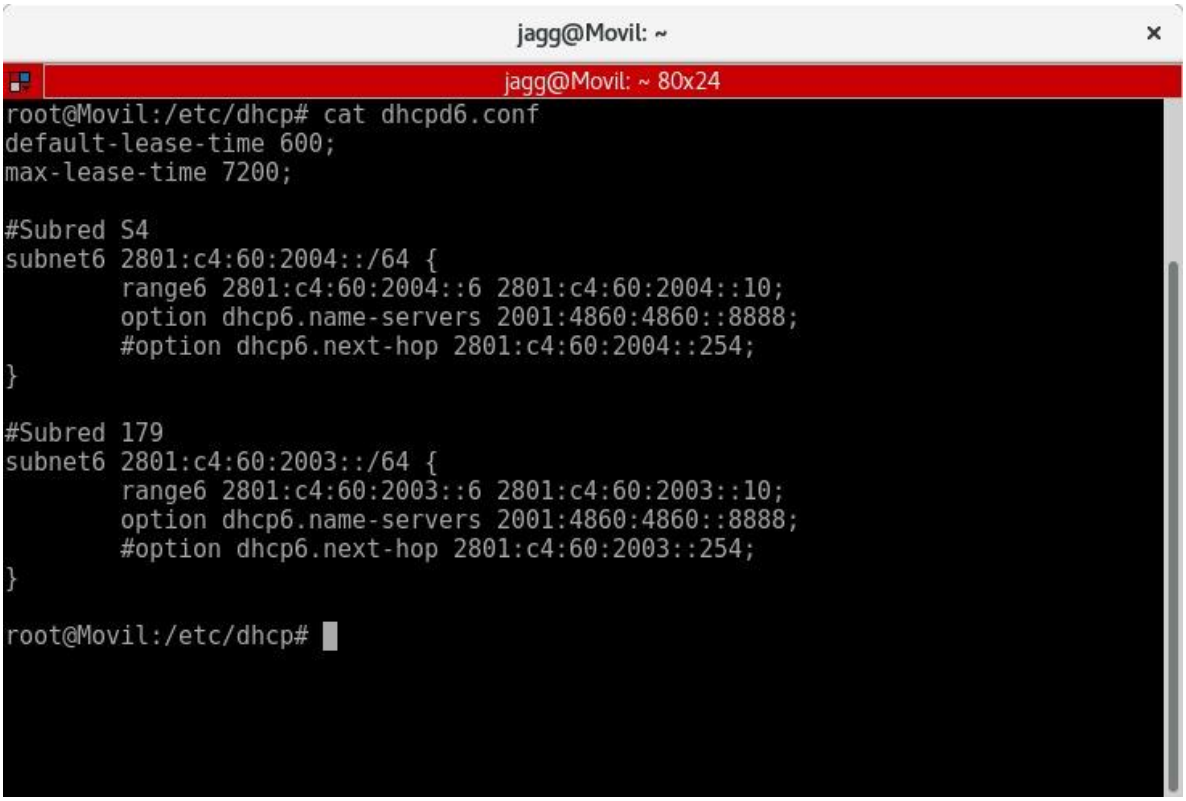


Figura 72. Configuración Servidor DHCPv6

Fue necesario ingresar un comando a la interfaz del segmento para que éste no se autoconfigurara y asignará direcciones IPv6 a los hosts; pues sin desactivar esta característica se asignaban dos direcciones a los hosts.

En la Figura 73 se puede apreciar la dirección asignada a uno de los hosts conectados en el switch, la dirección del servidor de nombres de dominio (DNS) y La dirección de la puerta de enlace predeterminada (Default Gateway) en IPv6.

Figura 73. Captura dirección IPv6 asignada a Host con DHCPv6

Como se puede apreciar, la dirección IPv6 asignada es 2801:c4:60:2004::10 está dentro del rango configurado en la Figura 72; También se observa la dirección del servidor de nombres de dominio (DNS) 2001:4860:4860::8888.

De esta manera es posible configurar un servidor DHCPv6 sin ningún problema. El uso de IPv6 permitirá dejar de usar NAT para la conexión de los usuarios de la red inalámbrica con IPv4.

CAPITULO VI: CONCLUSIONES Y TRABAJOS FUTUROS

Después realizar el diagnóstico propuesto en la primera etapa del Marco Metodológico IV en cada uno de los cuartos de telecomunicaciones de la ESIMEZ, se observó que la Topología no cumplía con ciertos estándares en algunas secciones de la red, por lo cual, Se realizó el levantamiento de la topología física en ESIME Zacatenco, documentando electrónicamente la topología existente. De esta manera será más eficiente la gestión de la red, pues no se perderá tiempo en el reconocimiento de esta; Además los encargados del departamento de la Unidad de Informática podrán identificar segmentos de red de manera más rápida. Después de realizar el levantamiento de la topología y su documentación es posible proponer cambios para que cumpla con el estándar TIA/EIA-568b.

De acuerdo con el análisis realizado, siguiendo la Metodología propuesta, La última actualización que se hizo a la red de datos de la ESIMEZ, fue en el año 2016, en ese proyecto se actualizaron los equipos que brindan servicios a las áreas administrativas ubicadas en el Edificio 1, por lo tanto, cubren perfectamente las necesidades de estas áreas, que son las más importantes de la red para llevar el control escolar, becas, servicio social, etc. Sin embargo, continuando con la exploración de los cuartos de telecomunicaciones en ESIMEZ, se detectó que en los demás edificios los dispositivos de red, aunque la mayoría son compatibles con IPv6, están trabajando a su máxima capacidad; Y se requiere de equipo más reciente para que la red sea escalable.

En cuanto al despliegue de IPv6, la estructura de la red permite que se inicie la migración en cualquier momento, pues basta con que se configure el router ubicado en el edificio 1 para OSPFv3 y a los ordenadores se les asigne una dirección IPv6 estática o dinámica (DHCPv6); Para los switches es transparente, pues solo conmutan de acuerdo con las direcciones MAC.

De acuerdo con las actividades desarrolladas para la obtención de datos de la red de datos de la ESIMEZ, y todo el proceso de análisis, desarrollo y propuesta; Basado en el Método Científico. Se definió una metodología que agilizará la implementación del Protocolo IPv6 en cada una de las dependencias que formen parte de la capa de acceso de la red Politécnica. De esta manera se aprovecha el tiempo y se prioriza una mayor eficiencia en cada una de las redes correspondientes a cada dependencia.

Después de realizar el análisis de los equipos instalados en la red de datos de la ESIMEZ, fue posible definir qué mecanismo de transición implementar, en este caso fue Doble Pila; Lo cual se recomienda en la primera etapa de despliegue de IPv6 en la capa de acceso donde sea posible, y para los casos en los cuales los enrutadores no soporten IPv6 (Solo IPv4) se propone la configuración de túneles. La traducción es principalmente utilizada por los Proveedores de Servicio de Internet

(ISPs) que ya cuentan con una Red Solo IPv6 donde se realiza la traducción para el contenido IPv4.

Aunque los dispositivos de red cumplen con los estándares que permiten su compatibilidad, aún hay equipo que no soporta IPv6 para administración y que estos puedan ser monitoreados y configurados de manera remota a través del Protocolo SSH (Secure SHell), el cual es el utilizado por la Dirección de Cómputo y Comunicaciones. Por lo tanto, es necesaria la adquisición de nuevo equipo que cumpla como mínimo con estas características.

El siguiente paso es aplicar este procedimiento en cada una de las dependencias del IPN (Escuelas, Centros de Investigación, Edificios de Gobierno, Etc.) mientras se migran los servicios que son indispensables (DHCP, DNS, Servidores Web, Correo Electrónico, etc.) para que finalmente se solicite la conexión IPv6 con el Proveedor de Servicios de Internet.

Trabajos Futuros

Se propone realizar un manual que pueda ser utilizado en cualquier dependencia del Instituto Politécnico Nacional que se interese por implementar IPv6 en sus respectivas redes de telecomunicaciones.

La puesta en producción requiere de la autorización de los encargados de la red, quienes se propusieron como objetivo desplegar el protocolo IPv6 el siguiente año (2019).

Se debe trabajar seriamente en la difusión del reglamento y los lineamientos que la Unidad de Informática (Encargada de la Gestión de la Red de datos de la ESIMEZ) tiene, pues por el desconocimiento de esta información, es que la red tiene muchos problemas.

Es conveniente realizar el etiquetado en el cableado en varias secciones de la red para facilitar el trabajo técnico cuando se requiera hacer mantenimiento o solucionar algún problema físico. El etiquetado actual solo cubre el edificio 1 y las conexiones entre el MCC y los ICCs.

ANEXOS

Configuración de Dispositivos
ESCENARIO 1

ENTERASYS SERIE S4

1. Conectar el ordenador al dispositivo mediante cable de consola.
2. Abrir la aplicación del cliente informático Putty y acceder al dispositivo ingresando las credenciales.
3. Creación de las VLANs propuestas en el escenario de la figura 50.

```
S4->set vlan create 3002
```

```
S4->set vlan create 3004
```

4. Asignar VLAN a puertos

```
S4->set port vlan ge.1.2 3002
```

```
S4->set port vlan ge.1.3 3004
```

5. Crear el proceso OSPFv3

```
S4->router
```

```
S4-router->configure terminal
```

```
S4-router-config->ipv6 router ospf 3
```

```
S4-router-config-ospfv3->router-id 10.220.255.81
```

6. Definir un ID al router a manera de dirección IPv4

```
S4-router-config-ospfv3->redistribute connected
```

Pese a que en la topología se considera el uso únicamente de OSPFv3, este comando permite redistribuir rutas estáticas o rutas aprendidas desde otro protocolo de red

```
S4-router-config-ospfv3->log-adjacency
```

7. Activando el registro de las adyacencias OSPF con otros routers

```
S4-router-config-ospfv3->exit
```

8. Salir de modo de configuración

9. Configurar interfaz como ruteo y asignar dirección IPv6

S4->router

S4-router->configure terminal

S4-router-config->interface vlan 3002

10. Configurar interfaz en modo ruteo

S4-router-config-intf-Vlan-3002->ipv6 address 2801:c4:60:2002::2/64

11. Asignar dirección IPv6 a la interfaz VLAN que ya se encuentra en modo ruteo. se mantiene un prefijo de red 64 y la configuración de la dirección es estática

S4-router-config-intf-Vlan-3002->ipv6 ospf 3 area 0.0.0.0

A diferencia de la configuración del protocolo de enrutamiento sobre IPv4, dentro de IPv6 las áreas se declaran dentro de la configuración de la interfaz. Es importante especificar el mismo ID del proceso ospf que fue creado previamente y el área OSPF a la que se encuentra conectada la interfaz

S4-router-config-intf-Vlan-3002->ipv6 enable

S4-router-config-intf-Vlan-3002->ipv6 nd prefix 2801:c4:60:2002::/64 2592000 604800

S4-router-config-intf-Vlan-3002->ipv6 forwarding

12. Habilitando enrutamiento de paquetes IPv6, en este dispositivo, por defecto se encuentra apagado, por lo que no escribir este comando significa que el protocolo no funcionará.

S4-router-config-intf-Vlan-3002->no shutdown

S4-router-config-intf-Vlan-3002->exit

13. Repetir proceso para configura al segmento de red 2801:c4:60:2004::/64

S4->router

S4-router->configure terminal

S4-router-config->interface vlan 3004

S4-router-config-intf-Vlan-3004->ipv6 address 2801:c4:60:2004::2/64

S4-router-config-intf-Vlan-3004->ipv6 ospf 3 area 0.0.0.0

S4-router-config-intf-Vlan-3004->ipv6 enable

S4-router-config-intf-Vlan-3004->ipv6 nd prefix 2801:c4:60:2004::/64 2592000 604800

S4-router-config-intf-Vlan-3004->ipv6 forwarding

```
S4-router-config-intf-Vlan-3004->no shutdown

S4-router-config-intf-Vlan-3004->exit
```

BROCADE ICX-7250-48P

Se configuró la VLAN 3002 en el segmento del prefijo 2801:c4:60:2004::/64 a todos los puertos switch Brocade ICX-7250-48P con los siguientes comandos.

1. Se crea la VLAN 3004 y se asigna a todos los puertos sin etiquetar (pues no se requiere de enlaces troncales).

```
ICX7250-48P Switch(config)#vlan 3004

ICX7250-48P Switch(config-vlan-3004)#untagged ethernet 1/1/1 to 1/1/48
```

2. Con el comando “show vlan 3004” se verifica la creación de la VLAN y su asignación a los puertos.

```
ICX7250-48P Switch(config-vlan-3004)#show vlan 3004

PORT-VLAN 3004, Name [None], Priority level0, in single spanning tree domain

 Untagged Ports: (U1/M1)  1  2  3  4  5  6  7  8  9 10 11 12

 Untagged Ports: (U1/M1)  13  14  15  16  17  18  19  20  21  22  23  24

 Untagged Ports: (U1/M1)  25  26  27  28  29  30  31  32  33  34  35  36

 Untagged Ports: (U1/M1)  37  38  39  40  41  42  43  44  45  46  47  48
```

3. Se configura la dirección IPv6 con fines de administración.

```
ICX7250-48P Switch(config)#ipv6 enable

ICX7250-48P Switch(config)#ipv6 address 2801:c4:60:2004::3/64
```

BROCADE ICX-7750-48F

Se configuró la VLAN 3002 para el segmento con el prefijo 2801:c4:60:**2002::**/64 al puerto 21. Después se asignó la dirección IPv6 2801:c4:60:**2002::1**/64 a la VLAN 3002 y la dirección IPv6 2801:c4:60:**2003::1**/64 a la VLAN 179 previamente configurada y bajo el protocolo OSPF.

A la VLAN 179 también se le configuró el protocolo de ruteo OSPFv3 para IPv6.

1. Crear la VLAN 3002 bajo el nombre IPV6 7750 A S4 en el puerto 21.

```
ICX7250-48P Switch(config)#vlan 3002 name "IPV6 7750 A S4" by port

ICX7250-48P Switch(config)#untagged ethe 1/1/21
```

2. Habilitar el protocolo OSPFv3 en la interfaz correspondiente a la VLAN 3002 y asignar la dirección IPv6 de dicha interfaz.

```
ICX7250-48P Switch(config)#interface ve 3002

ICX7250-48P Switch(config)#ipv6 address 2801:c4:60:2002::1/64

ICX7250-48P Switch(config)#ipv6 enable

ICX7250-48P Switch(config)#ipv6 ospf area 0
```

3. La VLAN 179 ya estaba configurada en el dispositivo, con su respectiva dirección IPv4 asignada y el protocolo de enrutamiento OSPF.

```
interface ve 179

port-name Red Conectividad

ip address 192.168.1.254 255.255.255.0

ip ospf area 0
```

4. Dentro de la VLAN 179 se habilitó IPv6, se asignó la dirección IPv6 a la interfaz y se configuró el protocolo OSPFv3

```
ICX7250-48P Switch(config)#ipv6 address 2801:c4:60:2003::1/64

ICX7250-48P Switch(config)#ipv6 enable

ICX7250-48P Switch(config)#ipv6 ospf area 0
```

ESCENARIO 2

BROCADE ICX-7250-48P

1. Conectar el ordenador al dispositivo mediante cable de consola.
2. Abrir la aplicación del cliente informático Putty y acceder al dispositivo ingresando las credenciales.
3. Creación de las VLANs propuestas en el escenario de la figura 59 y asociarlas a los puertos.

```
ICX7250-48P Switch(config)#vlan 10

ICX7250-48P Switch(config-vlan-10)#untagged ethernet 1/1/1 to 1/1/24

ICX7250-48P Switch(config-vlan-10)#vlan 20

ICX7250-48P Switch(config-vlan-20)#untagged ethernet 1/1/25 to 1/1/46
```

4. Definir los Puertos Troncales con el comando “tagged” para hacer la conexión con otros switches que tengan las mismas VLAN-

```
ICX7250-48P Switch(config-vlan-20)#tagged ethernet 1/1/47 to 1/1/48

ICX7250-48P Switch(config-vlan-20)#vlan 10

ICX7250-48P Switch(config-vlan-10)#tagged ethernet 1/1/47 to 1/1/48
```

5. Con el comando “show vlan” es posible verificar si hemos creado las VLAN y asociado a los puertos “tagged ports” para los troncales y “untagged ports” para los que van a host.

```
ICX7250-48P Switch(config-vlan-10)#sh vlan
```

6. El siguiente paso es configurar las direcciones IP al switch con fines de administración (de esta manera es posible conectarse al equipo para configurarlo remotamente mediante el protocolo SSH).

```
ICX7250-48P Switch(config)#ip address 10.1.1.100 255.255.255.0
```

7. Para configurar la dirección IPv6 de administración en el switch primero se habilita IPv6.

```
ICX7250-48P Switch(config)#ipv6 enable

ICX7250-48P Switch(config)#ipv6 address 2801:c4:60:5000::100/64
```

8. Con los siguientes comandos se realiza el ping a la dirección IP de algún host que se encuentre conectado en el switch.

```
ICX7250-48P Switch#ping 10.1.1.2

ICX7250-48P Switch#ping ipv6 2801:c4:60:5000::2
```

9. OPCIONALMENTE se puede definir alguna VLAN para que sea de administración, de lo contrario cualquier host conectado al switch que cuente con las credenciales podrá acceder mediante SSH.

```
ICX7250-48P Switch(config)#vlan 10

ICX7250-48P Switch(config-vlan-10)#management-vlan
```

10. Secure Shell (SSH) se habilita en en el switch de la siguiente manera.

```
ICX7250-48P Switch(config)#crypto key generate dsa
```

11. Se crea un usuario y una contraseña.

```
ICX7250-48P Switch(config)#enable user password-masking

ICX7250-48P Switch(config)#username OCTAVIO password

Enter password: *******
```

12. Con el siguiente comando se habilita el uso local para SSH.

```
ICX7250-48P Switch(config)#aaa authe login default local
```

13. En este paso se definen las direcciones de los hosts que podrán conectarse al switch de manera remota.

```
ICX7250-48P Switch(config)#ip ssh client 10.1.1.2

ICX7250-48P Switch(config)#ip ssh client ipv6 2801:c4:60:5000::2
```

ENTERASYS C3G124-24

1. Conectar el ordenador al dispositivo mediante cable de consola.
2. Abrir la aplicación del cliente informático Putty y acceder al dispositivo ingresando las credenciales.
3. Creación de las VLANs propuestas en el escenario de la figura 59 y asociarlas a los puertos.

```
C3(su)->set vlan create 10

C3(su)->set port vlan ge.1.1-12 10 modify-egress

C3(su)->set vlan create 20

C3(su)->set port vlan ge.1.13-23 20 modify-egress

C3(su)->set vlan egress 10 ge.1.1-12 untagged

C3(su)->set vlan egress 20 ge.1.12-23 untagged
```

4. Se definen los puertos “tagged” para los enlaces troncales

```
C3(su)->set vlan egress 10 ge.1.24 tagged

C3(su)->set vlan egress 20 ge.1.24 tagged
```

5. Para verificar la creación de las VLAN y sus puertos se utiliza el comando “show vlan port”

C3(su)->show vlan port

Port	VLAN	Ingress Filter	Egress Vlan
ge.1.1	10	N	untagged: 10
ge.1.2	10	N	untagged: 10
ge.1.3	10	N	untagged: 10
ge.1.4	10	N	untagged: 10
ge.1.5	10	N	untagged: 10
ge.1.6	10	N	untagged: 10
ge.1.7	10	N	untagged: 10
ge.1.8	10	N	untagged: 10
ge.1.9	10	N	untagged: 10
ge.1.10	10	N	untagged: 10
ge.1.11	10	N	untagged: 10
ge.1.12	10	N	untagged: 10
ge.1.13	20	N	untagged: 20
ge.1.14	20	N	untagged: 20
ge.1.15	20	N	untagged: 20
ge.1.16	20	N	untagged: 20
ge.1.17	20	N	untagged: 20
ge.1.18	20	N	untagged: 20
ge.1.19	20	N	untagged: 20
ge.1.20	20	N	untagged: 20
ge.1.21	20	N	untagged: 20
ge.1.22	20	N	untagged: 20
ge.1.23	20	N	untagged: 20
ge.1.24	20	N	tagged: 10,20

```
lag.0.1     1       N       untagged: 1

lag.0.2     1       N       untagged: 1

lag.0.3     1       N       untagged: 1

lag.0.4     1       N       untagged: 1

lag.0.5     1       N       untagged: 1

lag.0.6     1       N       untagged: 1
```

6. Se asigna una dirección IPv4 al dispositivo para administración.

```
C3(su)->set ip address 10.1.1.200 mask 255.255.255.0 gateway 10.1.1.254
```

7. Se habilita IPv6 en el dispositivo para posteriormente asignar la dirección IPv6 y la puerta de enlace predeterminada (gateway) con fines de administración, en este dispositivo se puede habilitar una VLAN para que sea de administración.

```
C3(su)->set ipv6 enable

C3(su)->set ipv6 address 2801:c4:60:5000::101/64

C3(su)->set ipv6 gateway 2801:c4:60:5000:254

C3(su)->set host vlan 10
```

ENTERASYS A4H124-24P

1. Conectar el ordenador al dispositivo mediante cable de consola.
2. Abrir la aplicación del cliente informático Putty y acceder al dispositivo ingresando las credenciales.
3. Creación de las VLANs propuestas en el escenario de la figura 59 y asociarlas a los puertos.

```
A4(su)->set vlan create 10

A4(su)->set port vlan ge.1.1-12 10 modify-egress

A4(su)->set vlan create 20

A4(su)->set port vlan ge.1.13-23 20 modify-egress

A4(su)->set vlan egress 10 ge.1.1-12 untagged

A4(su)->set vlan egress 20 ge.1.12-23 untagged
```

4. Se asigna una dirección IPv4 al dispositivo para administración.

```
A4(su)->set ip address 10.1.1.3 mask 255.255.255.0 gateway 10.1.1.254
```

5. Se habilita IPv6 en el dispositivo para posteriormente asignar la dirección IPv6 y la puerta de enlace predeterminada (gateway) con fines de administración.

```
A4(su)->set ipv6 enable

A4(su)->set ipv6 address 2801:c4:60:5000::102/64

A4(su)->set ipv6 gateway 2801:c4:60:5000::254
```

ESCENARIO 3

Para probar el funcionamiento de DHCPv6 se realizaron las mismas configuraciones del primer escenario donde ya se tenía un Protocolo de enrutamiento definido (OSPFv3).

ENTERASYS SERIE S4

1. Conectar el ordenador al dispositivo mediante cable de consola.
2. Abrir la aplicación del cliente informático Putty y acceder al dispositivo ingresando las credenciales.
3. Creación de las VLANs.

```
S4->set vlan create 3002

S4->set vlan create 3004
```

4. Asignar VLAN a puertos

```
S4->set port vlan ge.1.2 3002

S4->set port vlan ge.1.3 3004
```

5. Crear el proceso OSPFv3

```
S4->router

S4-router->configure terminal

S4-router-config->ipv6 router ospf 3

S4-router-config-ospfv3->router-id 10.220.255.81
```

6. Definir un ID al router a manera de dirección IPv4

```
S4-router-config-ospfv3->redistribute connected

S4-router-config-ospfv3->log-adjacency
```

7. Activando el registro de las adyacencias OSPF con otros routers

```
S4-router-config-ospfv3->exit
```

8. Salir de modo de configuración

9. Configurar interfaz como ruteo y asignar dirección IPv6

```
S4->router
```

```
S4-router->configure terminal
```

```
S4-router-config->interface vlan 3002
```

10. Configurar interfaz en modo ruteo

```
S4-router-config-intf-Vlan-3002->ipv6 address 2801:c4:60:2002::2/64
```

11. Asignar dirección IPv6 a la interfaz VLAN que ya se encuentra en modo ruteo. se mantiene un prefijo de red 64 y la configuración de la dirección es estática

```
S4-router-config-intf-Vlan-3002->ipv6 ospf 3 area 0.0.0.0
```

```
S4-router-config-intf-Vlan-3002->ipv6 enable
```

```
S4-router-config-intf-Vlan-3002->ipv6 nd prefix 2801:c4:60:2002::/64 2592000 604800
```

```
S4-router-config-intf-Vlan-3002->ipv6 forwarding
```

12. Habilitando enrutamiento de paquetes IPv6, en este dispositivo, por defecto se encuentra apagado, por lo que no escribir este comando significa que el protocolo no funcionará.

```
S4-router-config-intf-Vlan-3002->no shutdown
```

```
S4-router-config-intf-Vlan-3002->exit
```

13. Repetir proceso para configura al segmento de red 2801:c4:60:2004::/64

```
S4->router
```

```
S4-router->configure terminal
```

```
S4-router-config->interface vlan 3004
```

```
S4-router-config-intf-Vlan-3004->ipv6 address 2801:c4:60:2004::2/64
```

```
S4-router-config-intf-Vlan-3004->ipv6 ospf 3 area 0.0.0.0
```

```
S4-router-config-intf-Vlan-3004->ipv6 enable
```

S4-router-config-intf-Vlan-3004->ipv6 nd prefix 2801:c4:60:2004::/64 2592000 604800

S4-router-config-intf-Vlan-3004->ipv6 forwarding

S4-router-config-intf-Vlan-3004->no shutdown

S4-router-config-intf-Vlan-3004->exit

14. Es necesario desactivar la autoconfiguración de direcciones IPv6 con el siguiente comando; con el fin de que no exista doble direccionamiento IPv6 (Por el Enrutador y por el Servidor)

S4-router-config-intf-Vlan-3004->ipv6 nd prefix 2801:c4:60:2004::/64 2592000 604800 no-autoconfig

BROCADE ICX-7250-48P

1. Se crea la VLAN 3004 y se asigna a todos los puertos sin etiquetar (pues no se requiere de enlaces troncales).

ICX7250-48P Switch(config)#vlan 3004

ICX7250-48P Switch(config-vlan-3004)#untagged ethernet 1/1/1 to 1/1/48

2. Con el comando “show vlan 3004” se verifica la creación de la VLAN y su asignación a los puertos.

ICX7250-48P Switch(config-vlan-3004)#show vlan 3004

PORT-VLAN 3004, Name [None], Priority level0, in single spanning tree domain

Untagged Ports: (U1/M1) 1 2 3 4 5 6 7 8 9 10 11 12

Untagged Ports: (U1/M1) 13 14 15 16 17 18 19 20 21 22 23 24

Untagged Ports: (U1/M1) 25 26 27 28 29 30 31 32 33 34 35 36

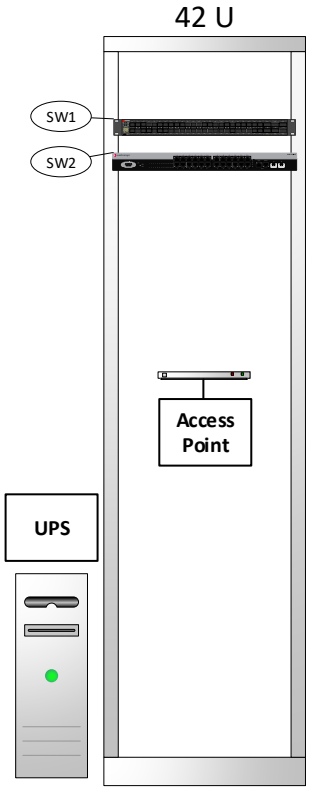
Untagged Ports: (U1/M1) 37 38 39 40 41 42 43 44 45 46 47 48

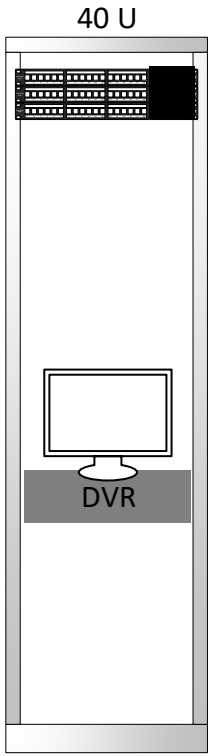
Diagrama Topología Física ESIMEZ (Herramienta de Microsoft Office Visio)

}

EDIFICIO 1

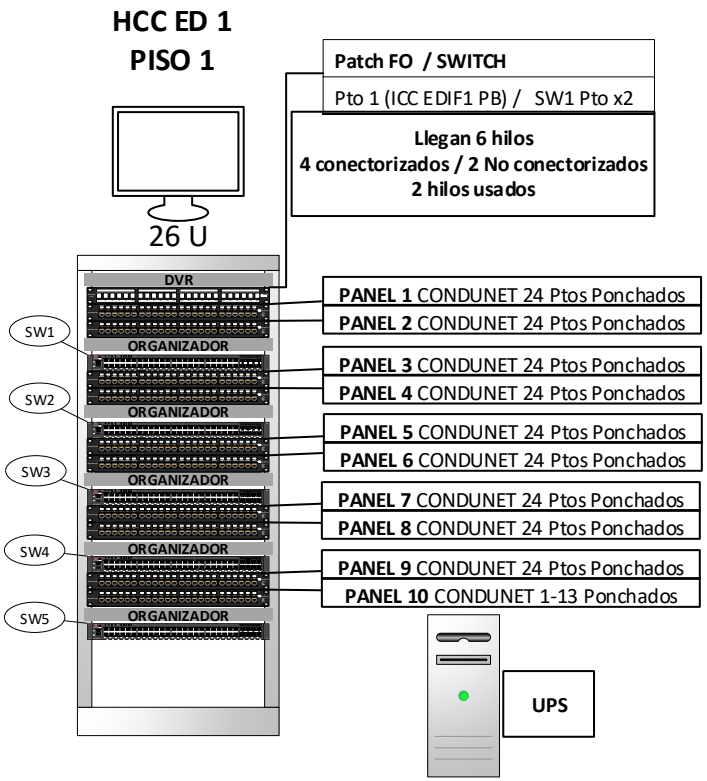
MCC ESIME
EDIF 1 PB



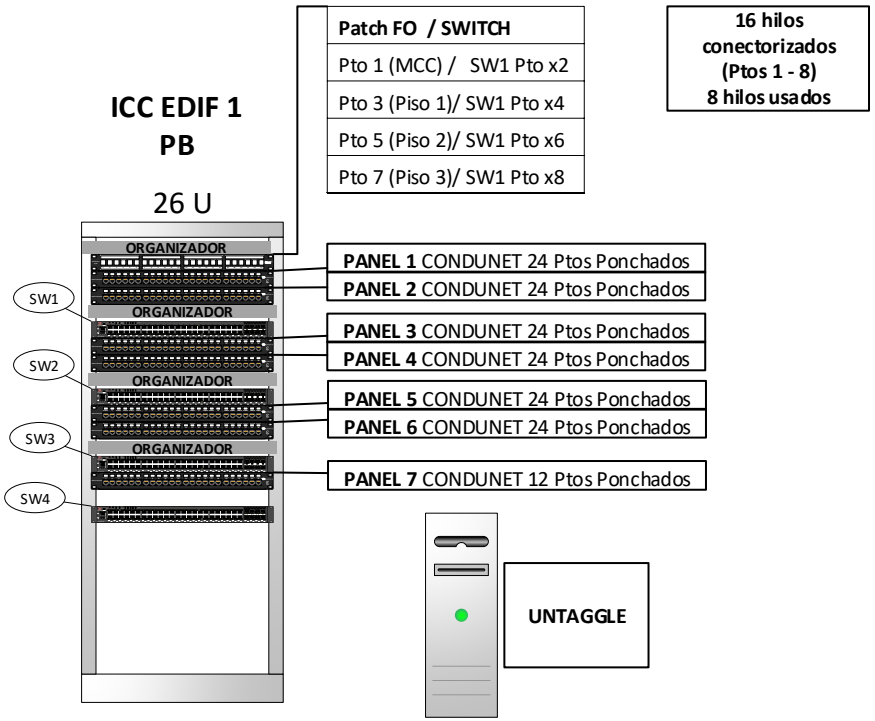


PANEL 1 (Pto 1 y 3 ponchados) Pto 1 ICC Ed1 PB Pto 3 Ed5
PANEL 2 (1-12 ponchados) Pto 2 Compatibilidad (et1/1/5) Pto 4 UDI (SW1 et1/1/1) Pto 6 Control (SW1 et1/1/7) Pto 8 SEPI eléctrica (SW1 et1/1/9) Pto 12 Edificio 4 (SW1 et1/1/3)
PANEL 3 (1-12 ponchados) Ningún Puerto conectado

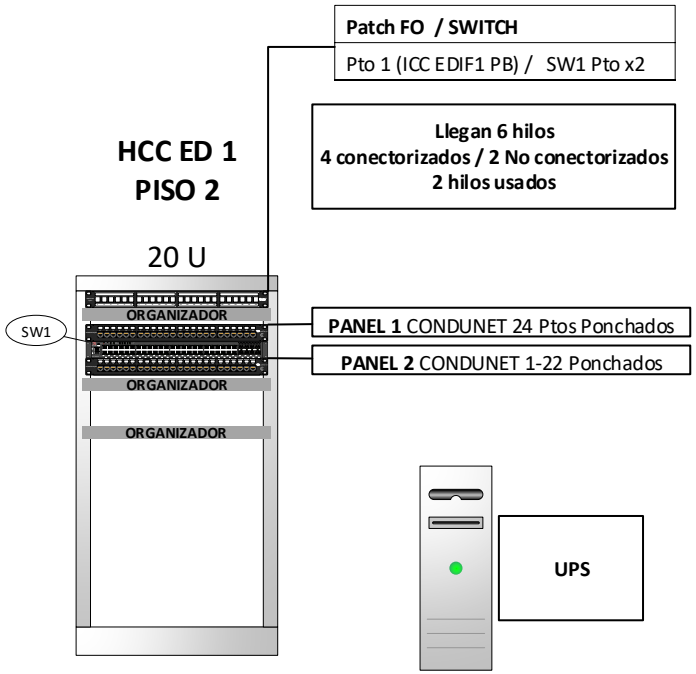
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO.	Ptos UTP
SW1	BROCADE	ICX7750-48F	----------	CRH3315M01J	23 conectados	----------
SW2	ENTERASYS	A2H124-24P	----------	08073165225E	----------	5 conectados



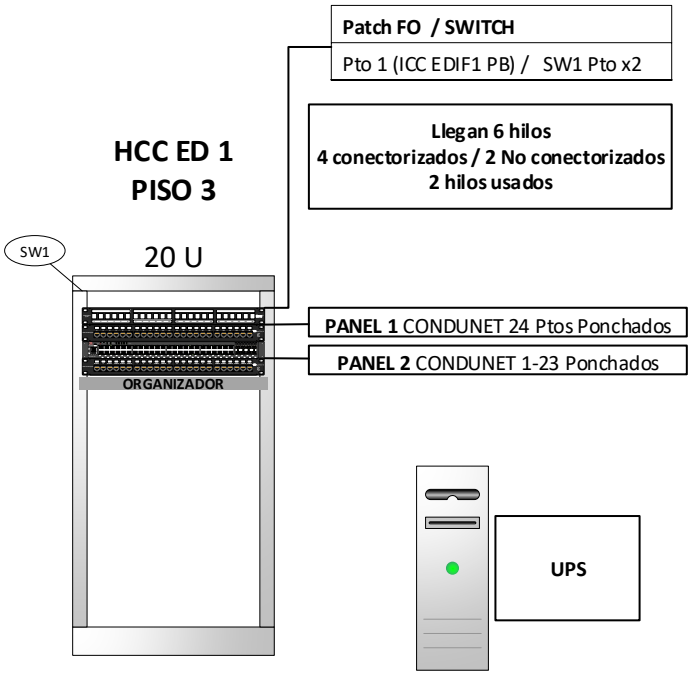
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos UTP	Ptos FO.
SW1	BROCADE	ICX7250-48P	STACK (MGR)	DUK3819M0ME	47 conectados	1 conectado
SW2	BROCADE	ICX7250-48P	STACK	DUK3819M0LF	48 conectados	----------
SW3	BROCADE	ICX7250-48P	STACK	DUK3819M0M7	48 conectados	----------
SW4	BROCADE	ICX7250-48P	STACK	DUK3819M0M8	48 conectados	----------
SW5	BROCADE	ICX7250-48P	STACK	DUK3819M0MH	43 conectados	----------



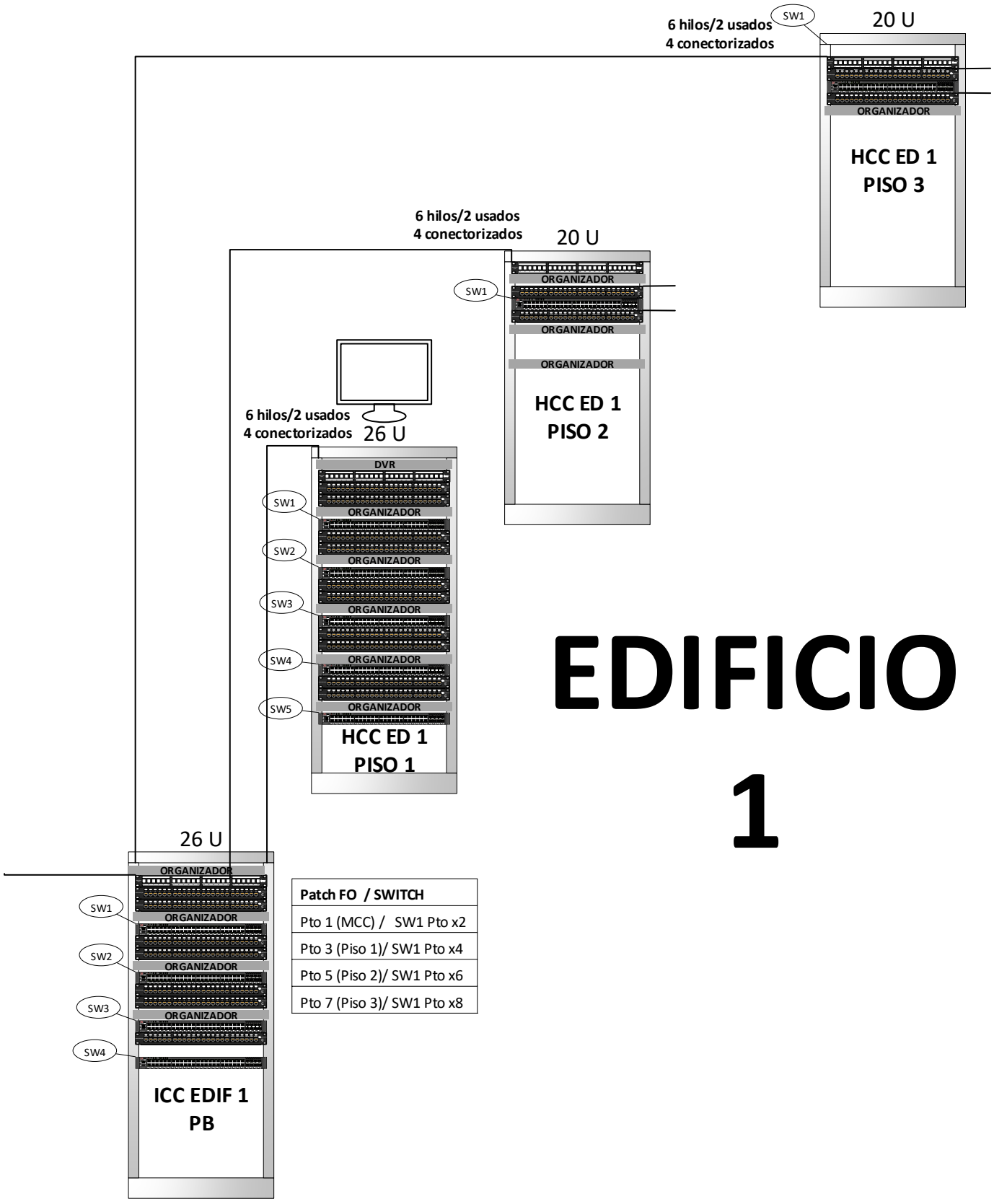
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos UTP	Ptos FO.
SW1	BROCADE	ICX7250-48P	STACK (MGR)	DUK3819M0M2	48 conectados	4 conectados
SW2	BROCADE	ICX7250-48P	STACK	DUK3819M0MJ	48 conectados	----------
SW3	BROCADE	ICX7250-48P	STACK	DUK3819M0LC	48 conectados	----------
SW4	BROCADE	ICX7250-48P	--------	DUK3819M0LM	27 conectados	----------



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos UTP	Ptos FO.
SW1	BROCADE	ICX7250-48P	----------	DUK3819M0M5	46 conectados	1 conectado



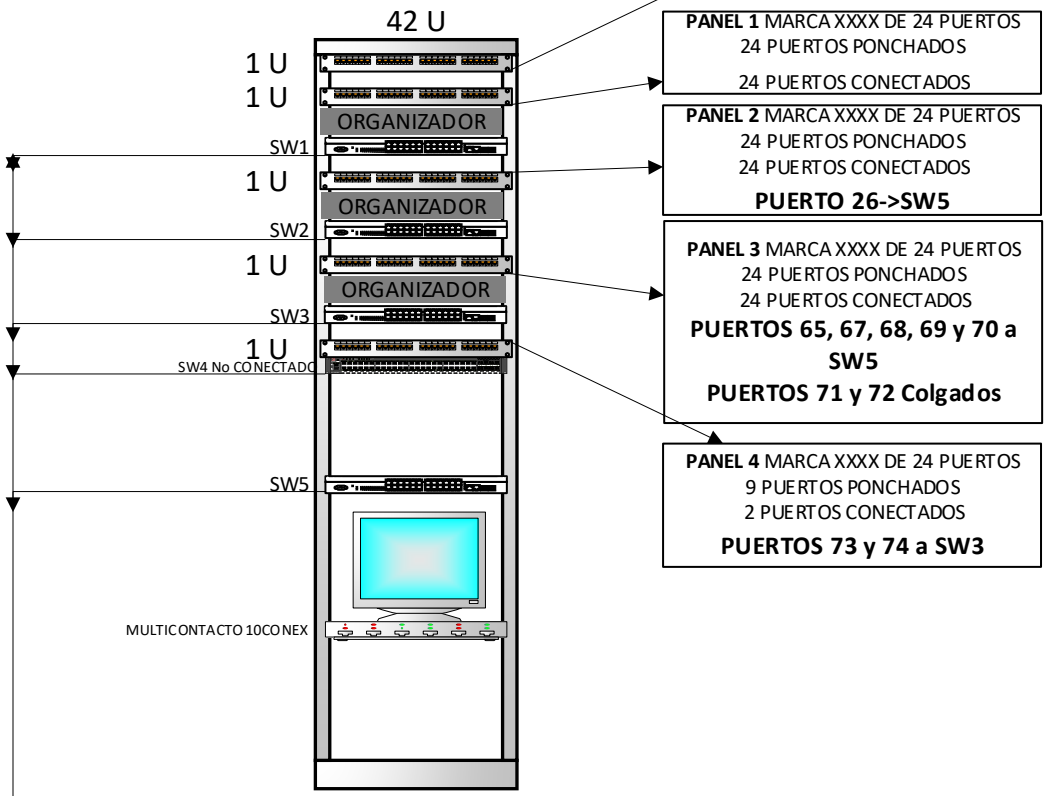
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos UTP	Ptos FO.
SW1	BROCADE	ICX7250-48P	----------	DUK3819M0LJ	47 conectados	1 conectado



Patch FO / SWITCH
Pto 1 (MCC) / SW1 Pto x2
Pto 3 (Piso 1)/ SW1 Pto x4
Pto 5 (Piso 2)/ SW1 Pto x6
Pto 7 (Piso 3)/ SW1 Pto x8

EDIFICIO 2

ED 2 ICC PB



Patch Fibra	/ SWITCH
Pto 1	/ SW1 Pto 28
Pto 4	/ SW4 Pto 27
Pto 7	/ SW1 Pto 27
Pto 13	/ SW2 Pto 27
Pto 16	/ SW2 Pto 28
Pto 19	/ SW3 Pto 27
Pto 22	/ SW3 Pto 28

PANEL 1 MARCA XXXX DE 24 PUERTOS
24 PUERTOS PONCHADOS
24 PUERTOS CONECTADOS

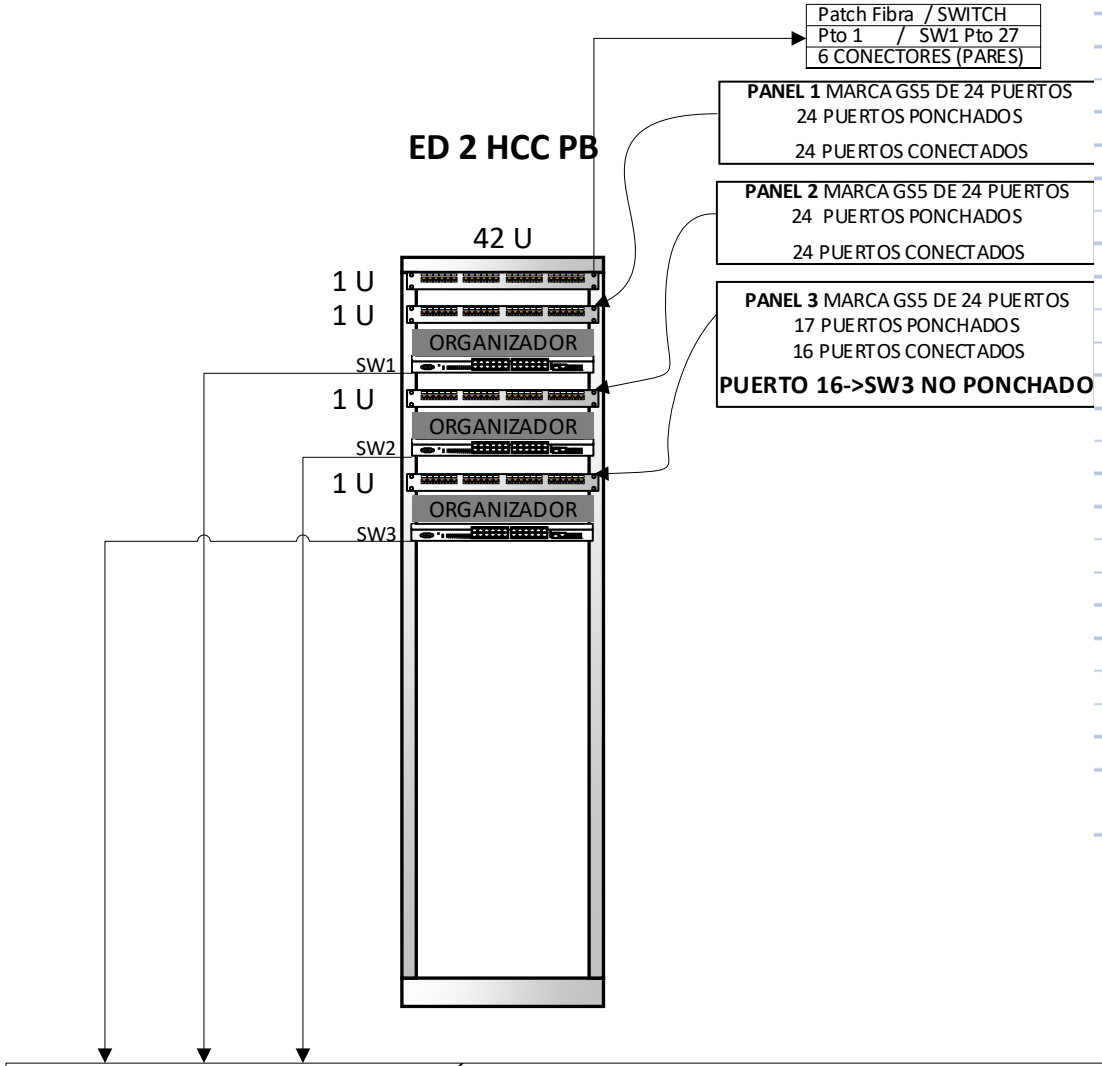
PANEL 2 MARCA XXXX DE 24 PUERTOS
24 PUERTOS PONCHADOS
24 PUERTOS CONECTADOS
PUERTO 26->SW5

PANEL 3 MARCA XXXX DE 24 PUERTOS
24 PUERTOS PONCHADOS
24 PUERTOS CONECTADOS
PUERTOS 65, 67, 68, 69 y 70 a SW5
PUERTOS 71 y 72 Colgados

PANEL 4 MARCA XXXX DE 24 PUERTOS
9 PUERTOS PONCHADOS
2 PUERTOS CONECTADOS
PUERTOS 73 y 74 a SW3

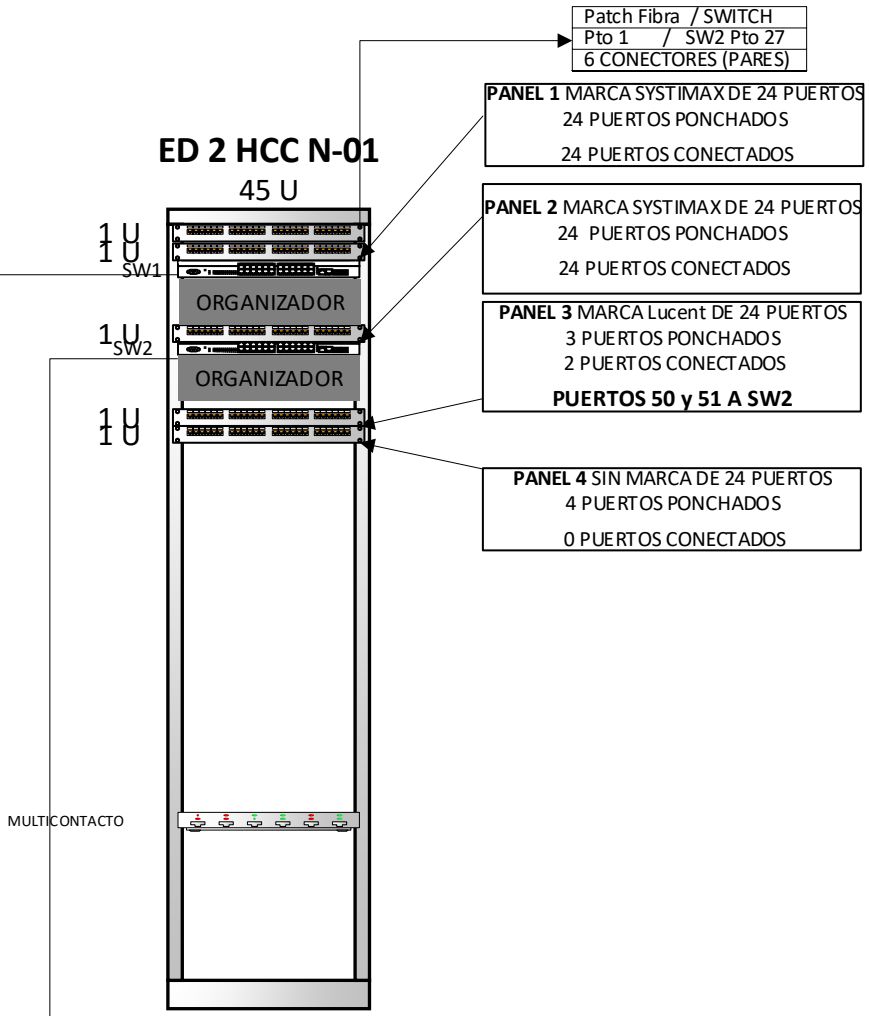
PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)	SWITCH 3 (PANEL/PUERTO)	SW 4 BROCADE	SWITCH 5 (PANEL/PUERTO)
1	P1/1	P2/25	P3/49		UNTAGLE
2	P1/2	COLGADO	P3/50		UNTAGLE
3	P1/3	P2/27	P3/51		NO CONECTADO
4	P1/4	P2/28	P3/52		NO CONECTADO
5	P1/5	P2/29	P3/53		NO CONECTADO
6	P1/6	P2/30	P3/54		NO CONECTADO
7	P1/7	P2/31	P3/55		P2/26
8	P1/8	P2/32	P3/56		NO CONECTADO
9	P1/9	P2/33	P3/57		P3/68
10	P1/10	P2/34	P3/58		P3/67
11	P1/11	P2/35	P3/59		P3/70
12	P1/12	P2/36	P3/60		P3/69
13	P1/13	P2/37	P3/61		NO CONECTADO
14	P1/14	P2/38	P3/62		NO CONECTADO
15	P1/15	P2/39	P3/63		NO CONECTADO
16	P1/16	P2/40	NO CONECTADO		NO CONECTADO
17	P1/17	P2/41	P3/64		COLGADO
18	P1/18	P2/42	NO CONECTADO		NO CONECTADO
19	P1/19	P2/43	P4/73		NO CONECTADO
20	P1/20	P2/44	P3/66		ACCESS POINT
21	P1/21	P2/45	P4/74		NO CONECTADO
22	P1/22	P2/46	COLGADO		NO CONECTADO
23	P1/23	P2/47	DVR		P3/65
24	P1/24	P2/48	SW5/PTO 24		SW3/PTO24
25 STACK UP	CONECTADO	CONECTADO	CONECTADO		NO CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO	CONECTADO		NO CONECTADO
27 F.O.	CONECTADO Panel F.O. Pto. 7	CONECTADO Panel FO Pto 13	CONECTADO Panel FO Pto 19		CONECTADO Panel FO Pto 4
28 F.O.	CONECTADO Panel F.O. Pto. 1	CONECTADO Panel FO Pto 16	CONECTADO Panel FO Pto 22		NO CONECTADO

EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A4H124-24P**	STACK	SN:11340054905D	24 Conectados	2 Conectados
SW2	Enterasys	A4H124-24P	STACK (MGR)	SN:11340052905D	24 Conectados	2 Conectados
SW3	Enterasys	A4H124-24P	STACK	SN:11340053905D	24 Conectados	2 Conectados
SW4	**Brocade**	**ICX7250-48P-2x10G**	NO CONECTADO	SN:DUK3819M0LT	0 Conectados	0 Conectados
SW5	Enterasys	A4H124-24P	NO STACK	SN:11410596905F	11 Conectados	1 Conectado



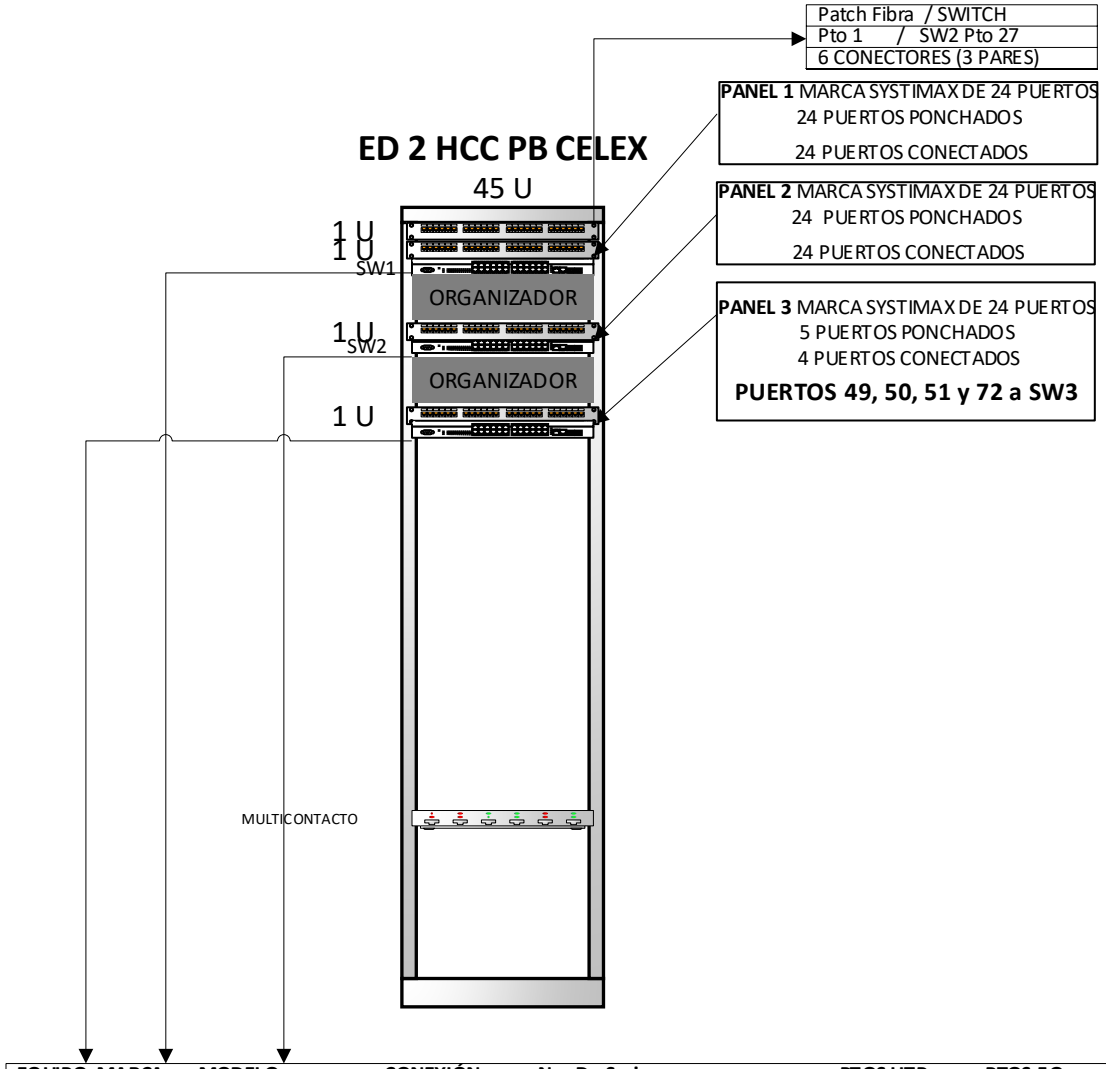
PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)	SWITCH 3 (PANEL/PUERTO)
1	P1/1	P2/1	P3/1
2	P1/2	P2/2	P3/2
3	P1/3	P2/3	P3/3
4	P1/4	P2/4	P3/4
5	P1/5	P2/5	P3/5
6	P1/6	P2/6	P3/6
7	P1/7	P2/7	P3/7
8	P1/8	P2/8	P3/8
9	P1/9	P2/9	P3/9
10	P1/10	P2/10	P3/10
11	P1/11	P2/11	P3/11
12	P1/12	P2/12	P3/12
13	P1/13	P2/13	P3/13
14	P1/14	P2/14	P3/14
15	P1/15	P2/15	P3/15
16	P1/16	P2/16	P3/16
17	P1/17	P2/17	NO CONECTADO
18	P1/18	P2/18	NO CONECTADO
19	P1/19	P2/19	NO CONECTADO
20	P1/20	P2/20	COLGADO
21	P1/21	P2/21	COLGADO (PLAFÓN)
22	P1/22	P2/22	NO CONECTADO
23	P1/23	P2/23	ACCESS POINT
24	P1/24	P2/24	NO CONECTADO
25 STACK UP	CONECTADO	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO	CONECTADO
27 F.O.	CONECTADO Panel 1 F.O.	NO CONECTADO	NO CONECTADO
28 F.O.	NO CONECTADO	NO CONECTADO	NO CONECTADO

EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A4H124-24P**	STACK	SN:11340082905D	24 Conectados	1 Conectados
SW2	Enterasys	A4H124-24P	STACK (MGR)	SN:11340056905D	24 Conectados	0 Conectados
SW3	Enterasys	A4H124-24P	STACK	SN:11340049905D	19 Conectados	0 Conectados



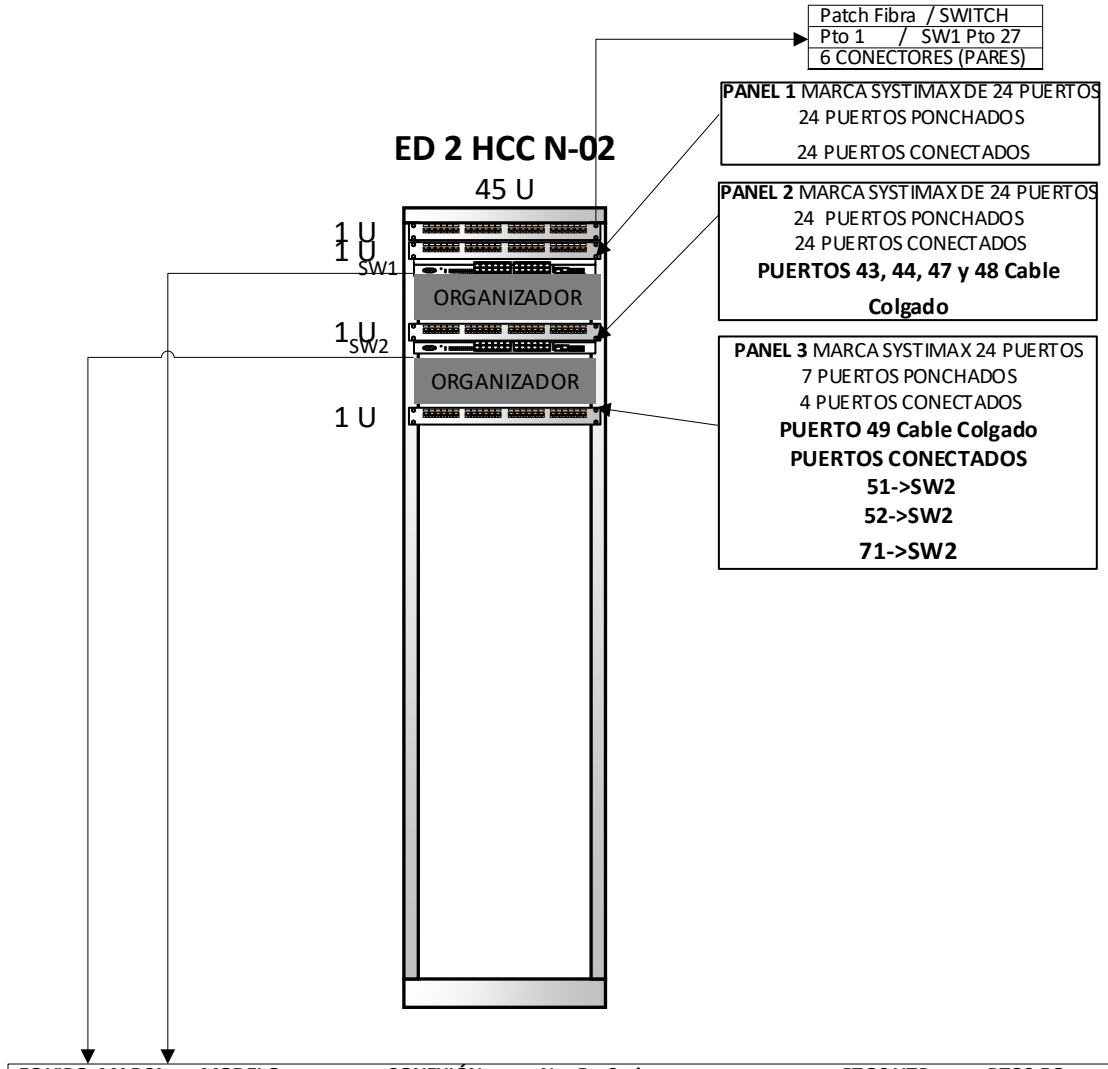
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A4H124-24P**	STACK (MGR)	SN:11510537905G **(VERIFICAR)**	24 Conectados	0 Conectados
SW2	Enterasys	A4H124-24P	STACK	SN:11510536905G **(VERIFICAR)**	24 Conectados	1 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)
1	P1/1	P2/25
2	P1/2	P2/26
3	P1/3	P2/27
4	P1/4	P2/28
5	P1/5	P2/29
6	P1/6	P2/30
7	P1/7	P2/31
8	P1/8	P2/32
9	P1/9	P2/33
10	P1/10	P2/34
11	P1/11	P2/35
12	P1/12	P2/36
13	P1/13	P2/37
14	P1/14	P3/51
15	P1/15	P3/50
16	P1/16	P2/40
17	P1/17	P2/41
18	P1/18	P2/42
19	P1/19	P2/43
20	P1/20	P2/44
21	P1/21	P2/45
22	P1/22	P2/46
23	P1/23	P2/47
24	P1/24	P2/48
25 STACK UP	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO
27 F.O.	NO CONECTADO	CONECTADO Panel 1 F.O.
28 F.O.	NO CONECTADO	NO CONECTADO



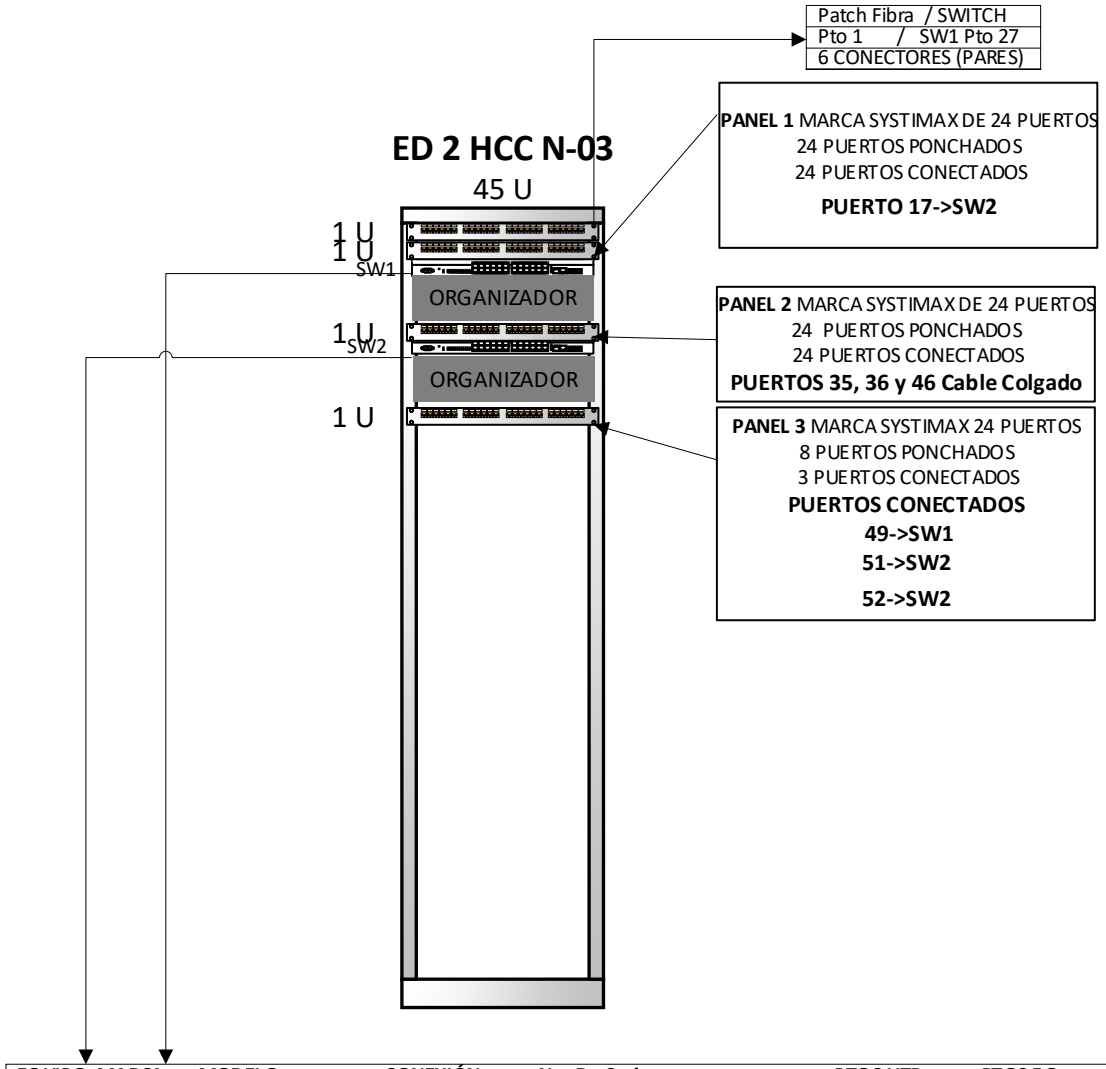
PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)	SWITCH 3 (PANEL/PUERTO)
1	P1/1	P2/25	P3/49
2	P1/2	P2/26	P3/50
3	P1/3	P2/27	P3/51
4	P1/4	P2/28	Directo al Plafón
5	P1/5	P2/29	Directo al Plafón
6	P1/6	P2/30	NO CONECTADO
7	P1/7	P2/31	Directo al Plafón CAT5E
8	P1/8	P2/32	NO CONECTADO
9	P1/9	P2/33	Directo al Plafón
10	P1/10	P2/34	Directo al Plafón CAT5E
11	P1/11	P2/35	Directo al Plafón
12	P1/12	P2/36	NO CONECTADO
13	P1/13	P2/37	Directo al Plafón
14	P1/14	P2/38	NO CONECTADO
15	P1/15	P2/39	Directo al Plafón
16	P1/16	P2/40	Directo al Plafón
17	P1/17	P2/41	NO CONECTADO
18	P1/18	P2/42	NO CONECTADO
19	P1/19	P2/43	NO CONECTADO
20	P1/20	P2/44	NO CONECTADO
21	P1/21	P2/45	NO CONECTADO
22	P1/22	P2/46	NO CONECTADO
23	P1/23	P2/47	NO CONECTADO
24	P1/24	P2/48	P3/72
25 STACK UP	CONECTADO	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO	CONECTADO
27 F.O.	NO CONECTADO	CONECTADO Panel 1 F.O.	NO CONECTADO
28 F.O.	NO CONECTADO	NO CONECTADO	NO CONECTADO

EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A4H124-24P**	STACK (MGR)	SN:11510530905G **(VERIFICAR)**	24 Conectados	0 Conectados
SW2	Enterasys	A4H124-24P	STACK	SN:11510519905G **(VERIFICAR)**	24 Conectados	1 Conectados
SW3	Enterasys	A4H124-24P	STACK	SN:11510229905G **(VERIFICAR)**	13 Conectados	0 Conectados



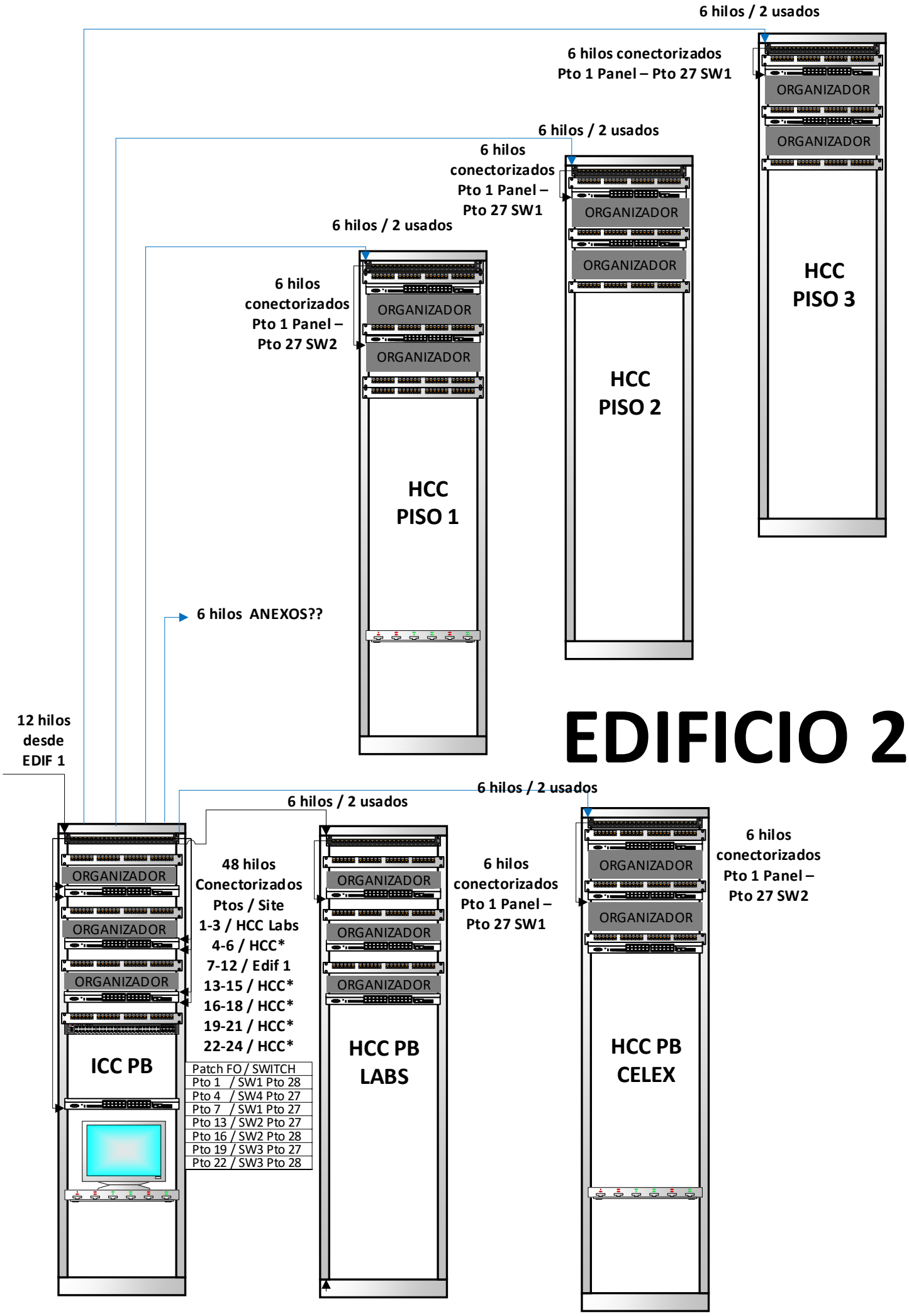
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A4H124-24P**	STACK (MGR)	SN:11510527905G **(VERIFICAR)**	24 Conectados	1 Conectados
SW2	Enterasys	A4H124-24P	STACK	SN:11510526905G **(VERIFICAR)**	23 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)
1	P1/1	P2/25
2	P1/2	P2/26
3	P1/3	P2/27
4	P1/4	P2/28
5	P1/5	P2/29
6	P1/6	P2/30
7	P1/7	P2/31
8	P1/8	P2/32
9	P1/9	P2/33
10	P1/10	P2/34
11	P1/11	P2/35
12	P1/12	P2/36
13	P1/13	P2/37
14	P1/14	P2/38
15	P1/15	P2/39
16	P1/16	P2/40
17	P1/17	P2/41
18	P1/18	P2/42
19	P1/19	**P3/71**
20	P1/20	**Sin Conexión**
21	P1/21	P2/45
22	P1/22	P2/46
23	P1/23	**P3/51**
24	P1/24	**P3/52**
25 STACK UP	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO
27 F.O.	CONECTADO Panel 1 F.O.	NO CONECTADO
28 F.O.	NO CONECTADO	NO CONECTADO

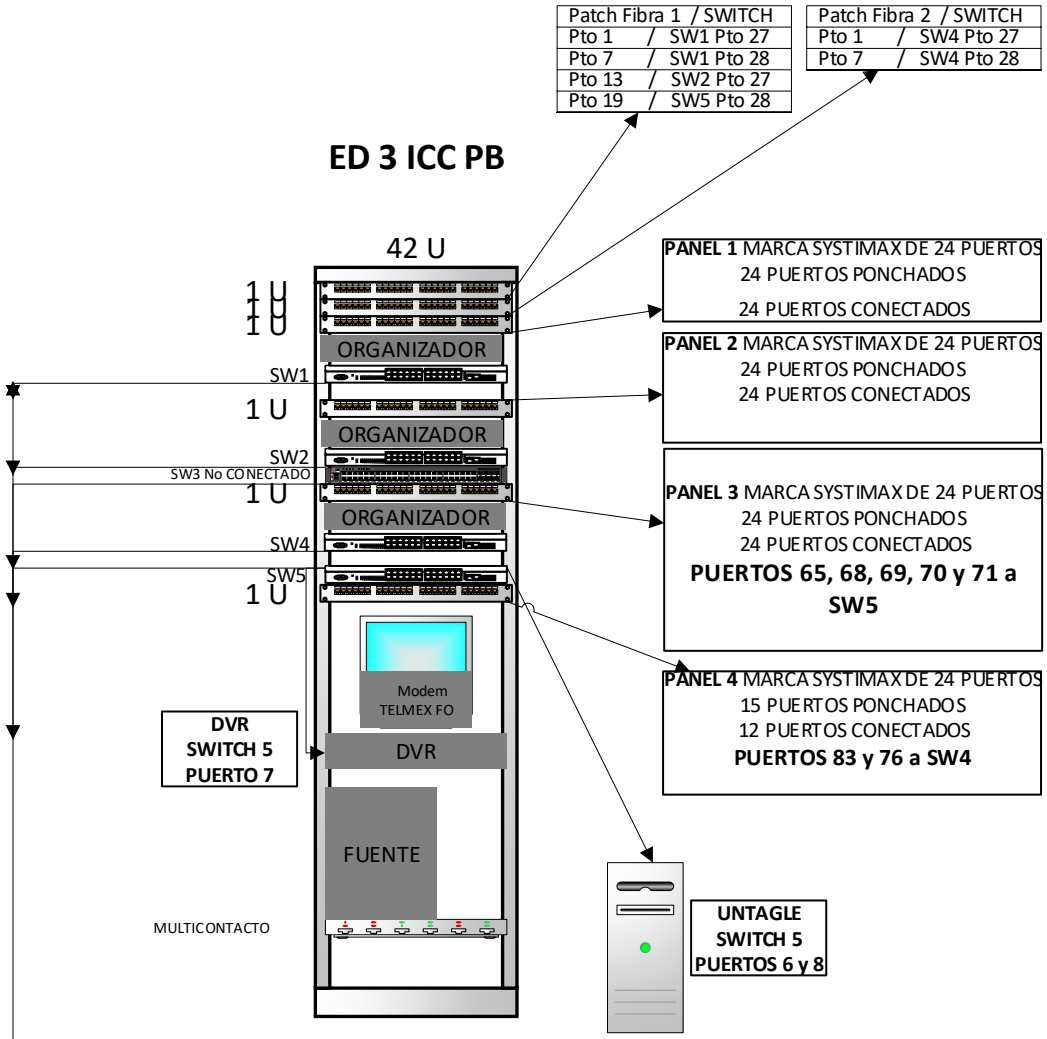


EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A4H124-24P**	STACK (MGR)	SN:11510535905G **(VERIFICAR)**	24 Conectados	1 Conectados
SW2	Enterasys	A4H124-24P	STACK	SN:11510531905G **(VERIFICAR)**	24 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)
1	P1/1	P2/25
2	P1/2	P2/26
3	P1/3	P2/27
4	P1/4	P2/28
5	P1/5	**P2/48**
6	P1/6	P2/30
7	P1/7	P2/31
8	P1/8	P2/32
9	P1/9	P2/33
10	P1/10	**P2/38**
11	P1/11	**P2/34**
12	P1/12	**P2/37**
13	P1/13	**P1/17**
14	P1/14	**P2/29**
15	**P3/49**	P2/39
16	P1/16	P2/40
17	**P1/15**	P2/41
18	P1/18	P2/42
19	P1/19	P2/43
20	P1/20	P2/44
21	P1/21	P2/45
22	P1/22	**P2/47**
23	P1/23	**P3/51**
24	P1/24	**P3/52**
25 STACK UP	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO
27 F.O.	CONECTADO Panel 1 F.O.	NO CONECTADO
28 F.O.	NO CONECTADO	NO CONECTADO

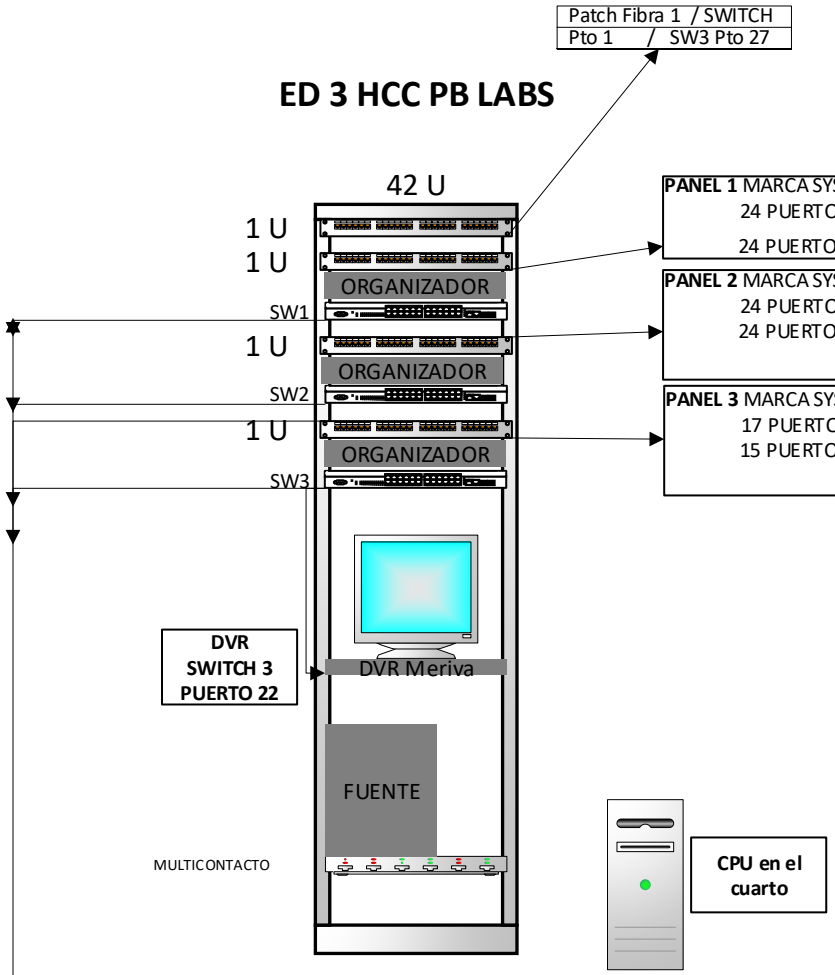

6 hilos / 2 usados
6 hilos conectorizados
Pto 1 Panel – Pto 27 SW1
ORGANIZADOR
ORGANIZADOR
HCC
PISO 3
6 hilos / 2 usados
6 hilos
conectorizados
Pto 1 Panel –
Pto 27 SW1
ORGANIZADOR
ORGANIZADOR
HCC
PISO 2
6 hilos / 2 usados
6 hilos
conectorizados
Pto 1 Panel –
Pto 27 SW2
ORGANIZADOR
ORGANIZADOR
HCC
PISO 1
6 hilos ANEXOS??
12 hilos
desde
EDIF 1
EDIFICIO 2
6 hilos / 2 usados
6 hilos / 2 usados
ORGANIZADOR
ORGANIZADOR
ORGANIZADOR
ICC PB
48 hilos
Conectorizados
Ptos / Site
1-3 / HCC Labs
4-6 / HCC*
7-12 / Edif 1
13-15 / HCC*
16-18 / HCC*
19-21 / HCC*
22-24 / HCC*
Patch FO / SWITCH
Pto 1 / SW1 Pto 28
Pto 4 / SW4 Pto 27
Pto 7 / SW1 Pto 27
Pto 13 / SW2 Pto 27
Pto 16 / SW2 Pto 28
Pto 19 / SW3 Pto 27
Pto 22 / SW3 Pto 28
ORGANIZADOR
ORGANIZADOR
ORGANIZADOR
ORGANIZADOR
HCC PB
LABS
6 hilos
conectorizados
Pto 1 Panel –
Pto 27 SW1
ORGANIZADOR
ORGANIZADOR
HCC PB
CELEX
6 hilos
conectorizados
Pto 1 Panel –
Pto 27 SW2

EDIFICIO 3



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A4H124-24P**	STACK	SN:11340051905D	24 Conectados	2 Conectados
SW2	Enterasys	A4H124-24P	STACK	SN:11340050905D	24 Conectados	1 Conectados
SW3	**Brocade**	**ICX7250-48P-2x10G**	NO CONECTADO	SN:DUK3819M0M4	0 Conectados	0 Conectados
SW4	Enterasys	A4H124-24P	STACK (MGR)	SN:11340060905D	23 Conectados	2 Conectados
SW5	**Enterasys**	**A2H124-24P**	NO STACK	SN:05503153900G	19 Conectados	1 Conectado

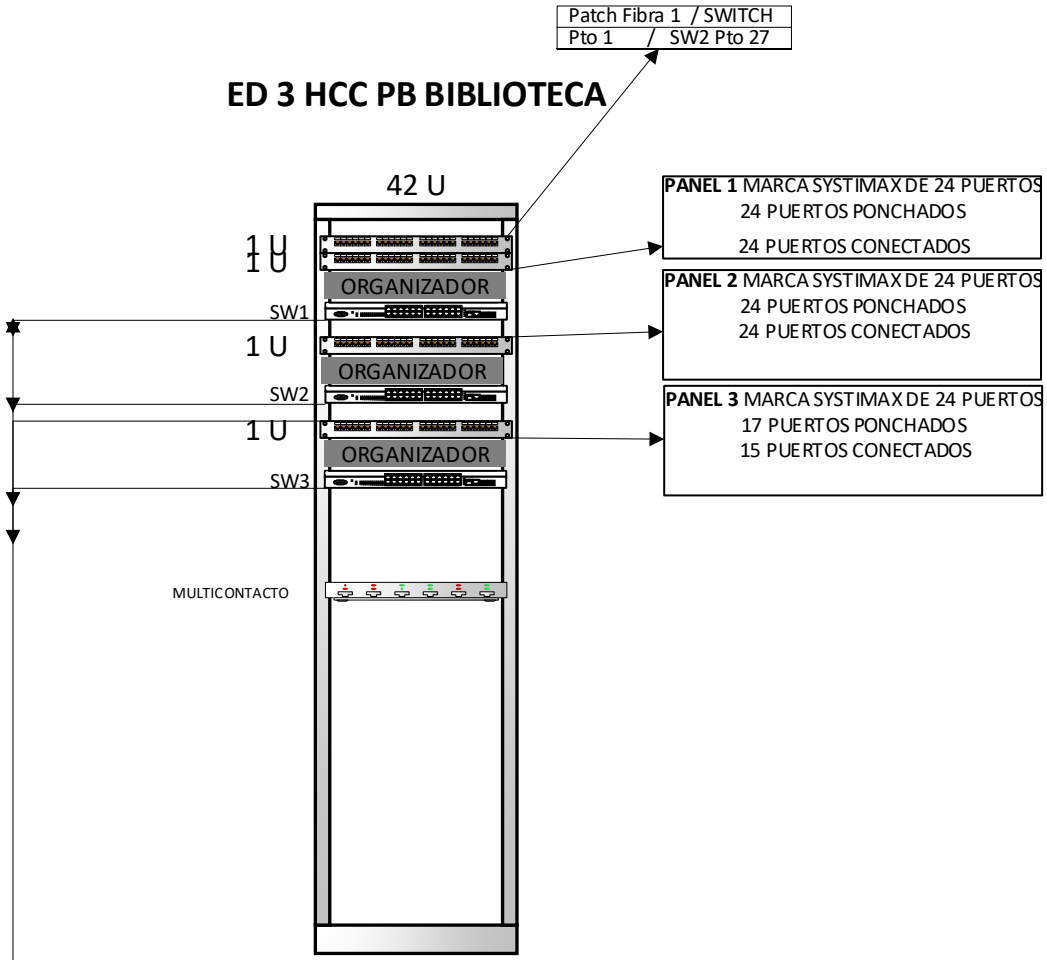
PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)	SW3 BROCADE	SWITCH 4 (PANEL/PUERTO)	SWITCH 5 (PANEL/PUERTO)
1	P1/1	P2/25		P3/49	P4/73
2	P1/2	P2/26		P3/50	P4/74
3	P1/3	P2/27		P3/51	P4/75
4	P1/4	P2/28		P3/52	P4/78
5	P1/5	P2/29		P3/53	P4/77
6	P1/6	P2/30		P3/54	Untagle
7	P1/7	P2/31		P3/55	DVR
8	P1/8	P2/32		P3/56	Untagle
9	P1/9	P2/33		P3/57	NO CONECTADO
10	P1/10	P2/34		P3/58	NO CONECTADO
11	P1/11	P2/35		P3/59	P4/79
12	P1/12	P2/36		P3/60	NO CONECTADO
13	P1/13	P2/37		P3/61	P4/93
14	P1/14	P2/38		P3/62	P4/94
15	P1/15	P2/39		P3/63	P4/95
16	P1/16	P2/40		P3/64	P4/96
17	P1/17	P2/41		COLGADO	P3/65
18	P1/18	P2/42		P3/66	NO CONECTADO
19	P1/19	P2/43		P4/83	P3/69
20	P1/20	P2/44		P3/67	P3/68
21	P1/21	P2/45		P3/72	P3/71
22	P1/22	P2/46		P4/76	P3/70
23	P1/23	P2/47		NO CONECTADO	NO CONECTADO
24	P1/24	P2/48		SW5/PTO24	SW4/PTO24
25 SU	CONECTADO	CONECTADO		CONECTADO	NO CONECTADO
26 SD	CONECTADO	CONECTADO		CONECTADO	NO CONECTADO
27 F.O.	CONECTADO Panel 1 F.O. Pto. 1	CONECTADO Panel 1 FO Pto 13		CONECTADO Panel 2 FO Pto 1	NO CONECTADO
28 F.O.	CONECTADO Panel 1	NO CONECTADO		CONECTADO	CONECTADO



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A4H124-24P**	STACK	SN:11340059905D	24 Conectados	0 Conectados
SW2	Enterasys	A4H124-24P	STACK **(MGR)**	SN:11340055905D	24 Conectados	0 Conectados
SW3	Enterasys	A4H124-24P	STACK	SN:11340058905D	17 Conectados	1 Conectados

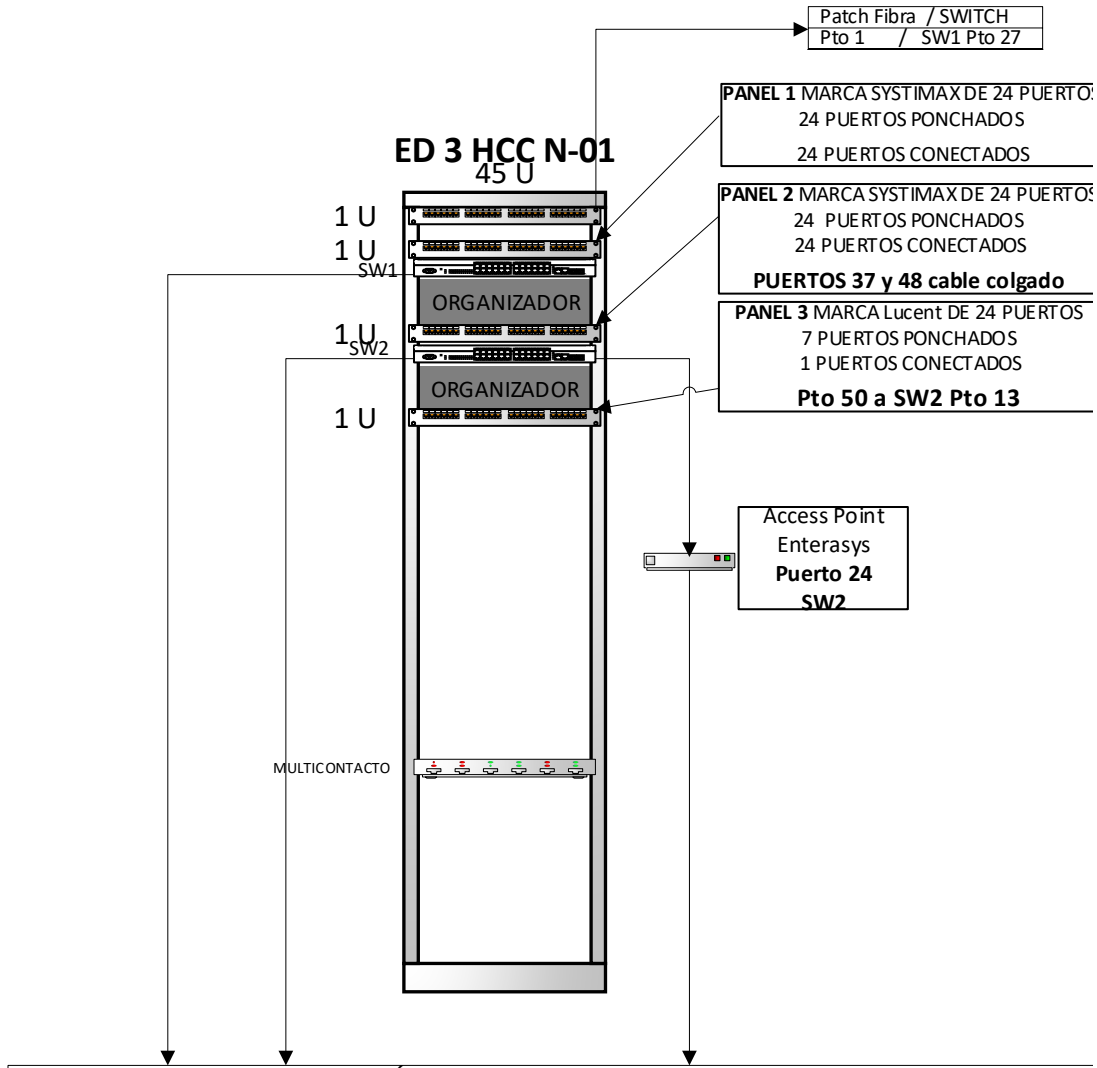
PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)	SWITCH 3 (PANEL/PUERTO)
1	P1/1	P2/25	P3/49
2	P1/2	P2/26	P3/50
3	P1/3	P2/27	P3/51
4	P1/4	P2/28	P3/52
5	P1/5	P2/29	P3/53
6	P1/6	P2/30	P3/54
7	P1/7	P2/31	P3/55
8	P1/8	P2/32	P3/56
9	P1/9	P2/33	P3/57
10	P1/10	P2/34	P3/58
11	P1/11	P2/35	P3/59
12	P1/12	P2/36	P3/60
13	P1/13	P2/37	P3/61
14	P1/14	P2/38	P3/62
15	P1/15	P2/39	P3/63
16	P1/16	P2/40	NO CONECTADO
17	P1/17	P2/41	NO CONECTADO
18	P1/18	P2/42	NO CONECTADO
19	P1/19	P2/43	NO CONECTADO
20	P1/20	P2/44	NO CONECTADO
21	P1/21	P2/45	NO CONECTADO
22	P1/22	P2/46	DVR
23	P1/23	P2/47	NO CONECTADO
24	P1/24	P2/48	COLGADO
25 STACK UP	CONECTADO	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO	CONECTADO
27 F.O.	NO CONECTADO	NO CONECTADO	CONECTADO Panel F.O. Pto. 1
28 F.O.	NO CONECTADO	NO CONECTADO	NO CONECTADO

ED 3 HCC PB BIBLIOTECA



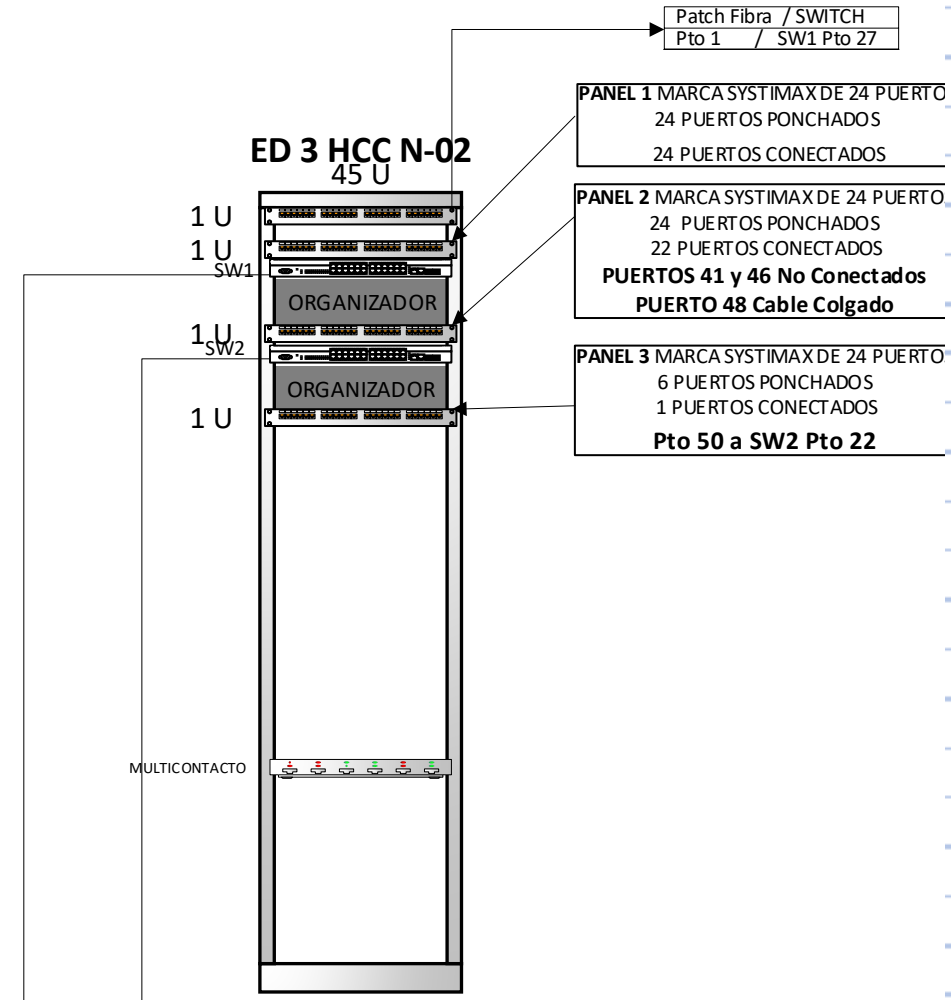
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A2H124-24**	STACK	SN:10420956225P	24 Conectados	0 Conectados
SW2	Enterasys	A2H124-24P	STACK **(MGR)**	SN:10420999225P	19 Conectados	1 Conectados
SW3	**Enterasys**	**A2H124-24P**	STACK	SN:08073120225E	23 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)	SWITCH 3 (PANEL/PUERTO)
1	P1/1	P2/25	P3/49
2	P1/2	P2/26	P3/50
3	P1/3	P2/27	P3/51
4	P1/4	P2/28	P3/52
5	P1/5	P2/29	P3/53
6	P1/6	P2/30	P3/54
7	P1/7	P2/31	P3/55
8	P1/8	P2/32	P3/56
9	P1/9	P2/33	P3/57
10	P1/10	P2/34	P3/58
11	P1/11	P2/35	P3/59
12	P1/12	P2/36	P3/60
13	P1/13	P2/37	P2/43
14	P1/14	P2/38	P2/44
15	P1/15	NO CONECTADO	P2/48
16	P1/16	NO CONECTADO	P2/46
17	P1/17	P2/41	P3/69
18	P1/18	P2/42	P2/39
19	P1/19	NO CONECTADO	P3/72
20	P1/20	NO CONECTADO	P2/47
21	P1/21	P2/45	P3/71
22	P1/22	NO CONECTADO	NO CONECTADO
23	P1/23	COLGADO	PLAFÓN
24	P1/24	COLGADO	PLAFÓN
25 STACK UP	CONECTADO	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO	CONECTADO
27 F.O.	NO CONECTADO	CONECTADO Panel 1 F.O.	NO CONECTADO
28 F.O.	NO CONECTADO	NO CONECTADO	NO CONECTADO



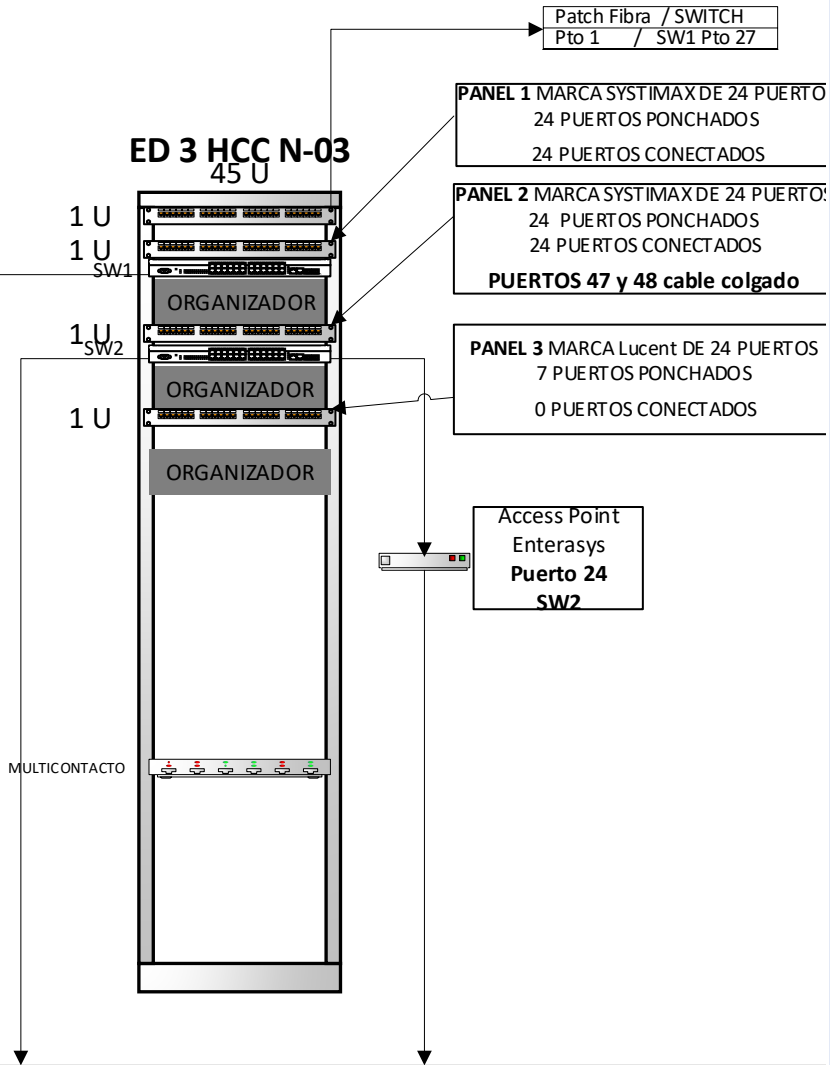
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	Enterasys	A4H124-24P	STACK (MGR)	SN:11510513905G	24 Conectados	1 Conectados
SW2	Enterasys	A4H124-24P	STACK	SN:11510512905G	24 Conectados	0 Conectados
AP	Enterasys	WS-AP3610	----------	S/N:11531162235T0000		

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)
1	P1/1	P2/25
2	P1/2	P2/26
3	P1/3	P2/27
4	P1/4	P2/28
5	P1/5	P2/29
6	P1/6	P2/30
7	P1/7	P2/31
8	P1/8	P2/32
9	P1/9	P2/33
10	P1/10	P2/34
11	P1/11	P2/35
12	P1/12	P2/36
13	P1/13	P3/50
14	P1/14	P2/38
15	P1/15	P2/39
16	P1/16	P2/40
17	P1/17	P2/41
18	P1/18	P2/42
19	P1/19	P2/43
20	P1/20	P2/44
21	P1/21	P2/45
22	P1/22	P2/46
23	P1/23	P2/47
24	P1/24	AP
25 STACK UP	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO
27 F.O.	CONECTADO Panel F.O. PTO 1	NO CONECTADO
28 F.O.	NO CONECTADO	NO CONECTADO



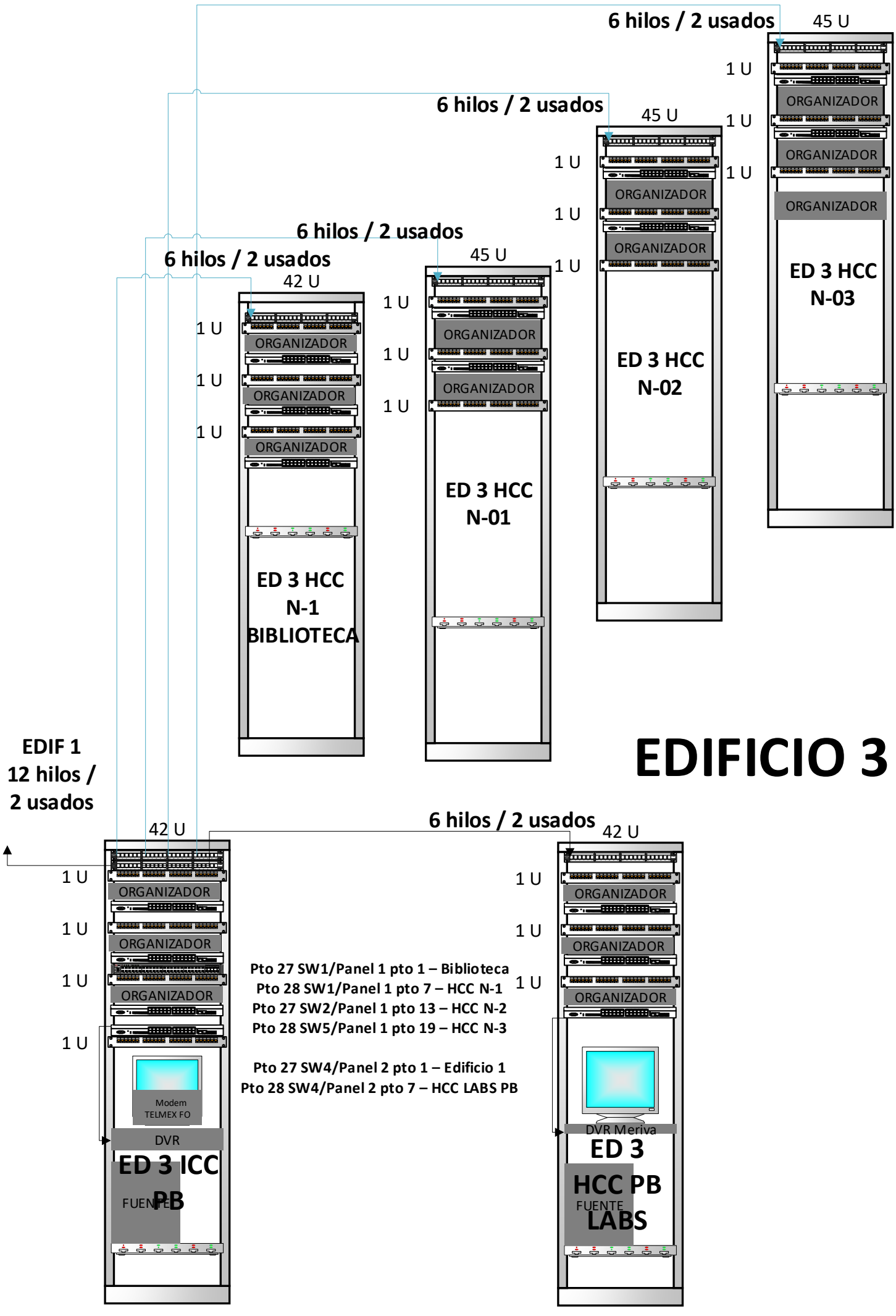
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	Enterasys	A4H124-24P	STACK (MGR)	SN:11510522905G	24 Conectados	1 Conectados
SW2	Enterasys	A4H124-24P	STACK	SN:11510521905G	23 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)
1	P1/1	P2/25
2	P1/2	P2/26
3	P1/3	P2/27
4	P1/4	P2/28
5	P1/5	P2/29
6	P1/6	P2/30
7	P1/7	P2/31
8	P1/8	P2/32
9	P1/9	P2/33
10	P1/10	P2/34
11	P1/11	P2/35
12	P1/12	P2/36
13	P1/13	P2/37
14	P1/14	P2/38
15	P1/15	P2/39
16	P1/16	P2/40
17	P1/17	NO CONECTADO
18	P1/18	P2/42
19	P1/19	P2/43
20	P1/20	P2/44
21	P1/21	P2/45
22	P1/22	P3/50
23	P1/23	P2/47
24	P1/24	COLGADO
25 STACK UP	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO
27 F.O.	CONECTADO Panel 1 F.O. Pto. 1	NO CONECTADO
28 F.O.	NO CONECTADO	NO CONECTADO

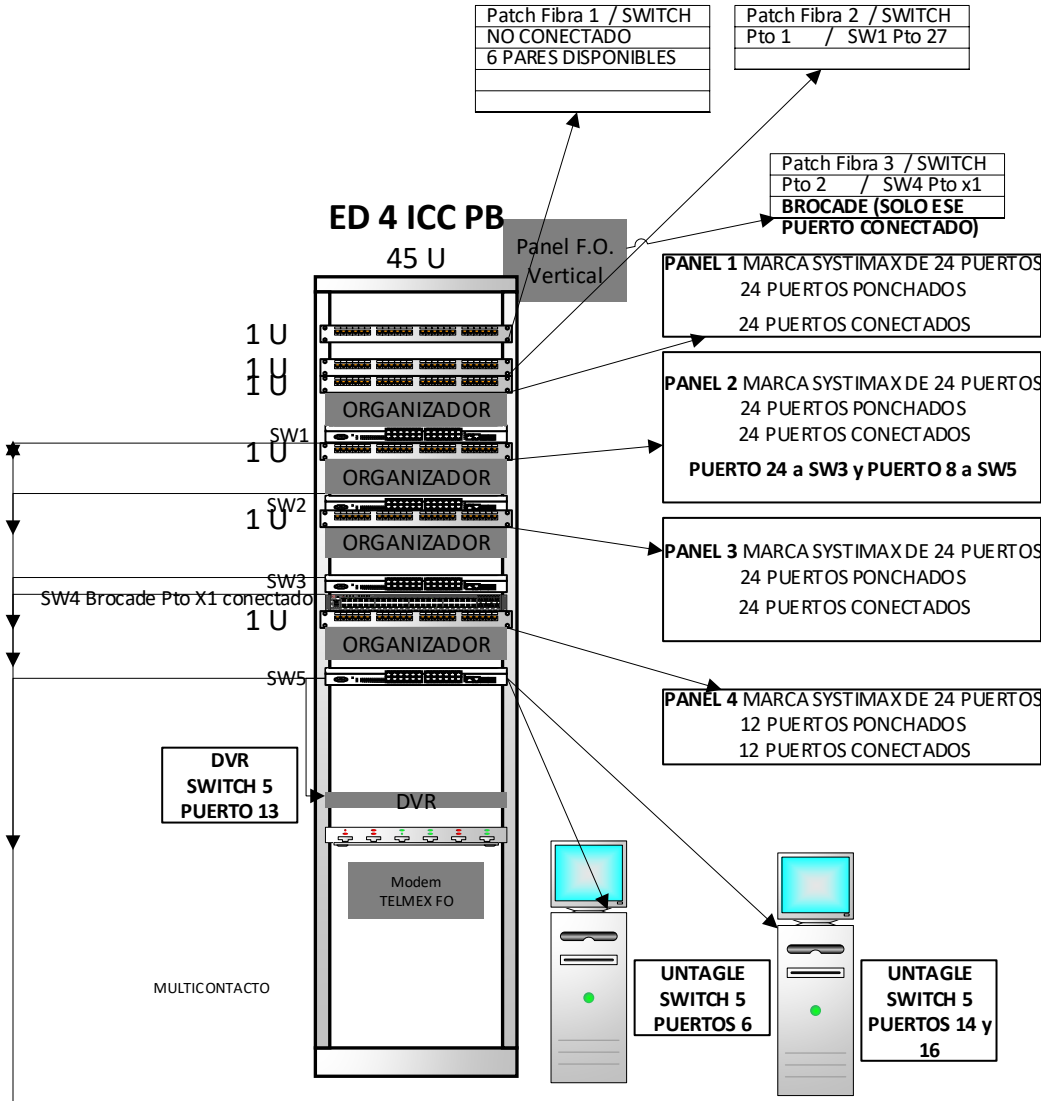


EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	Enterasys	A4H124-24P	STACK	SN:11510511905G	24 Conectados	1 Conectados
SW2	Enterasys	A4H124-24P	STACK (MGR)	SN:11510520905G	23 Conectados	0 Conectados
AP	Enterasys	WS-AP3610	----------	S/N:115326412351T0000		

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)
1	P1/1	P2/25
2	P1/2	P2/26
3	P1/3	P2/27
4	P1/4	P2/28
5	P1/5	P2/29
6	P1/6	P2/30
7	P1/7	P2/31
8	P1/8	P2/32
9	P1/9	P2/33
10	P1/10	P2/34
11	P1/11	P2/35
12	P1/12	P2/36
13	P1/13	P2/37
14	P1/14	P2/38
15	P1/15	P2/39
16	P1/16	P2/40
17	P1/17	P2/41
18	P1/18	P2/42
19	P1/19	P2/43
20	P1/20	P2/44
21	P1/21	P2/45
22	P1/22	P2/46
23	P1/23	NO CONECTADO
24	P1/24	AP
25 STACK UP	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO
27 F.O.	CONECTADO Panel 1 F.O. Pto.1	NO CONECTADO
28 F.O.	NO CONECTADO	NO CONECTADO


6 hilos / 2 usados
45 U
1 U
ORGANIZADOR
ED 3 HCC N-03
6 hilos / 2 usados
45 U
ED 3 HCC N-02
6 hilos / 2 usados
45 U
ED 3 HCC N-01
6 hilos / 2 usados
42 U
ED 3 HCC N-1 BIBLIOTECA
EDIF 1
12 hilos /
2 usados
42 U
Modem TELMEX FO
DVR
ED 3 ICC PB
FUENTE
6 hilos / 2 usados
42 U
DVR Meriva
ED 3 HCC PB
FUENTE
LABS
Pto 27 SW1/Panel 1 pto 1 – Biblioteca
Pto 28 SW1/Panel 1 pto 7 – HCC N-1
Pto 27 SW2/Panel 1 pto 13 – HCC N-2
Pto 28 SW5/Panel 1 pto 19 – HCC N-3
Pto 27 SW4/Panel 2 pto 1 – Edificio 1
Pto 28 SW4/Panel 2 pto 7 – HCC LABS PB
EDIFICIO 3

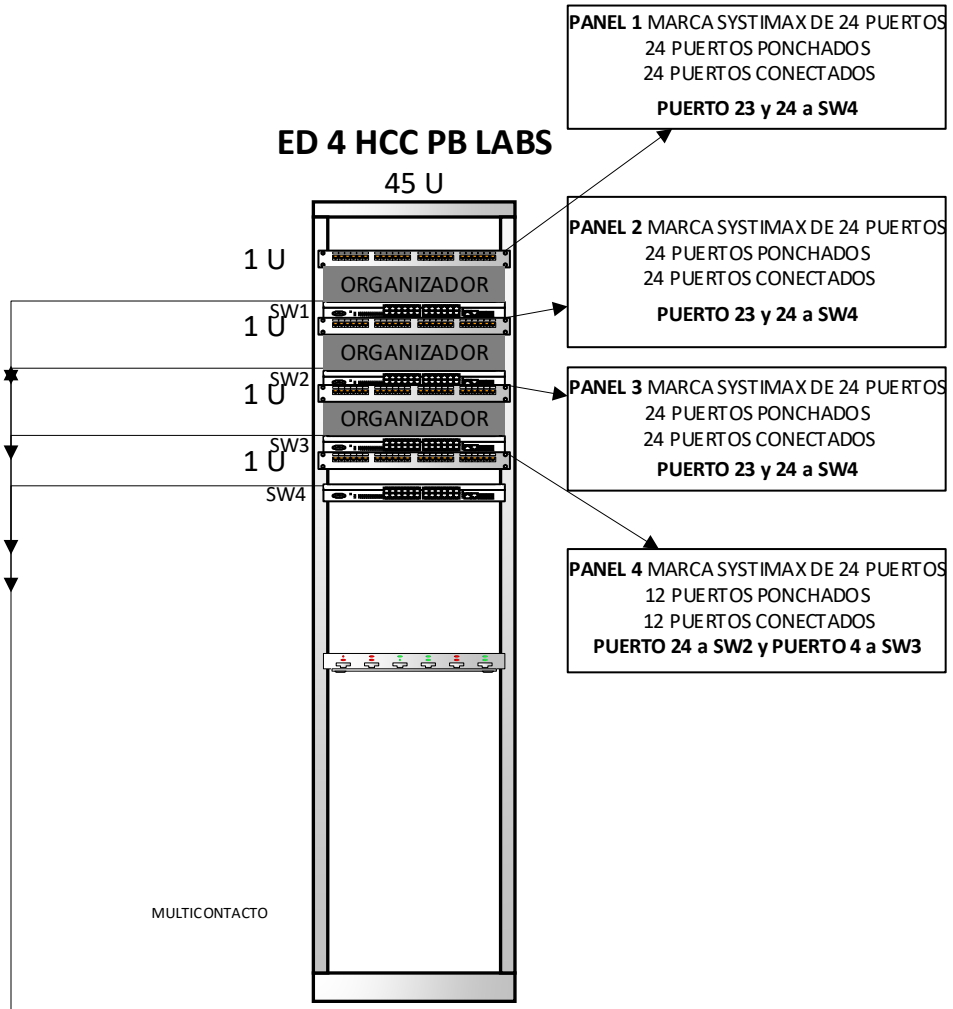
EDIFICIO 4



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A2H124-24P**	**STACK (MGR)**	SN:10300191225M	24 Conectados	1 Conectados
SW2	Enterasys	A2H124-24P	NO STACK	SN:11121112225P	24 Conectados	0 Conectados
SW3	Enterasys	A2H124-24P	STACK	SN:08013188225E	24 Conectados	0 Conectados
SW4	**Brocade**	**ICX7250-48P-2x10G**	NO CONECTADO	SN:DUK3819M0LV	0 Conectados	**1 Conectados**
SW5	Enterasys	A2H124-24P	STACK	SN:08013192225E	18 Conectados	0 Conectado

PUERTOS SWITCHES	SWITCH 1 (PANEL/ PUERTO)	SW 2 (P/PTO)	SW 3 (P/PTO)	Brocade	SW 5 (P/PTO)
1	P1/1	P2/1	P3/1		P4/1
2	P1/2	P2/2	P3/2		P4/2
3	P1/3	P2/3	P3/3		P4/3
4	P1/4	P2/4	P3/4		P4/4
5	P1/5	P2/5	P3/5		**P2/8**
6	P1/6	P2/6	P3/6		**UNTAGLE**
7	P1/7	P2/7	P3/7		
8	P1/8	P2/8	**P2/24**		
9	P1/9	P2/9	P3/9		**P4/20**
10	P1/10	P2/10	P3/10		**P4/18**
11	P1/11	P2/11	P3/11		**P4/5**
12	P1/12	P2/12	P3/12		**P4/19**
13	P1/13	P2/13	P3/13		**DVR**
14	P1/14	P2/14	P3/14		**UNTAGLE**
15	P1/15	P2/15	P3/15		
16	P1/16	P2/16	P3/16		**UNTAGLE**
17	P1/17	P2/17	P3/17		**SW2/24**
18	P1/18	P2/18	P3/18		
19	P1/19	P2/19	P3/19		
20	P1/20	P2/20	P3/20		
21	P1/21	P2/21	P3/21		P4/21
22	P1/22	P2/22	P3/22		P4/22
23	P1/23	P2/23	P3/23		P4/23
24	P1/24	**SW5/17**	P3/24		P4/24
25 SU	**CONECTADO**		**CONECTADO**		**CONECTADO**
26 SD	**CONECTADO**		**CONECTADO**		**CONECTADO**
27 F.O.	**CONECTADO Panel 2 F.O. Pto. 1**			**PTO x1**	
28 F.O.					

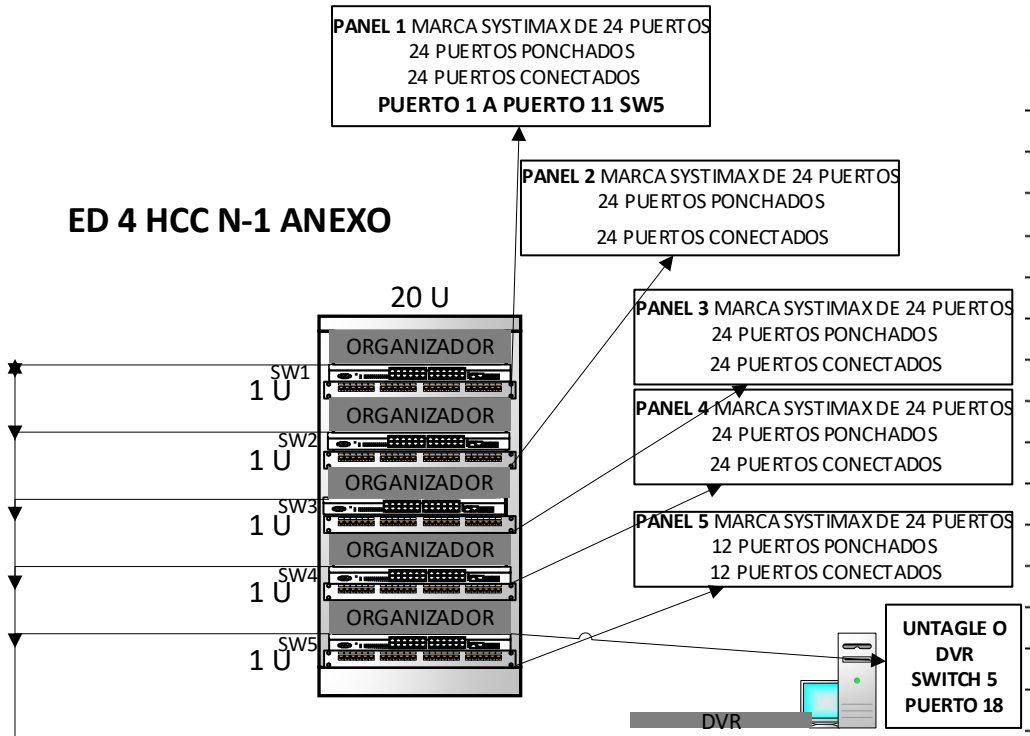
ED 4 HCC PB LABS



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**B5G124-24P2**	NO STACK	SN:11360263225K	24 Conectados	0 Conectados
SW2	Enterasys	B5G124-24P2	NO STACK	SN:12020667225L	24 Conectados	0 Conectados
SW3	Enterasys	B5G124-24P2	NO STACK	SN:11370402225k	24 Conectados	0 Conectados
SW4	Enterasys	B5G124-24P2	NO STACK	SN:11370403225k	14 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/ PUERTO)	SWITCH 2 (P/PTO)	SWITCH 3 (P/PTO)	SWITCH 4 (P/PTO)
1	P1/1	P2/1	P3/1	P4/1
2	P1/2	P2/2	P3/2	P4/2
3	P1/3	P2/3	P3/3	P4/3
4	P1/4	P2/4	P3/4	P4/4
5	P1/5	P2/5	P3/5	P4/5
6	P1/6	P2/6	P3/6	P4/6
7	P1/7	P2/7	P3/7	
8	P1/8	P2/8	P3/8	
9	P1/9	P2/9	P3/9	**COLGADO**
10	P1/10	P2/10	P3/10	
11	P1/11	P2/11	P3/11	
12	P1/12	P2/12	P3/12	
13	P1/13	P2/13	P3/13	
14	P1/14	P2/14	P3/14	
15	P1/15	P2/15	P3/15	
16	P1/16	P2/16	P3/16	
17	P1/17	P2/17	P3/17	**P3/23**
18	P1/18	P2/18	P3/18	**P3/24**
19	P1/19	P2/19	P3/19	**P2/23**
20	P1/20	P2/20	P3/20	**P2/24**
21	P1/21	P2/21	P3/21	**P1/23**
22	P1/22	P2/22	P3/22	**P1/24**
23	**SW3/23**	**SW1/24**	**SW1/23**	
24	**SW2/23**	**P4/24**	**SW4/24**	**SW3/24**
25 ST UP				
26 ST DOWN				
27 F.O.				
28 F.O.				

ED 4 HCC N-1 ANEXO

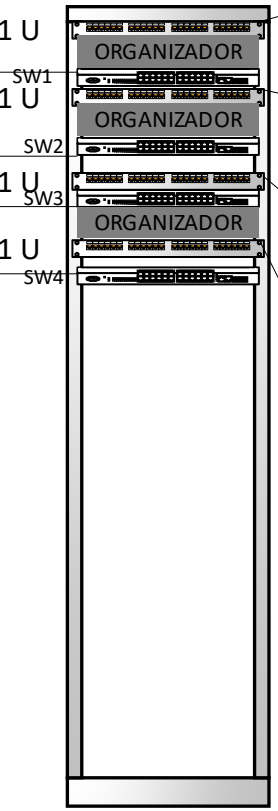


EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A2H124-24**	STACK	SN:10421017225P	24 Conectados	0 Conectados
SW2	**Enterasys**	**A2H124-24P**	STACK	SN:08073172225E	24 Conectados	0 Conectados
SW3	Enterasys	A2H124-24P	**STACK (MGR)**	SN:08073130225E	24 Conectados	0 Conectados
SW4	Enterasys	A2H124-24P	STACK	SN:08013231225E	24 Conectados	0 Conectado
SW5	Enterasys	A2H124-24P	STACK	SN:08073174225E	18 Conectados	0 Conectado

PUERTOS SWITCHES	SWITCH 1 (PANEL/ PUERTO)	SW2 (P/PTO)	SW3 (P/PTO)	SW4 (P/PTO)	SW 5 (P/PTO)
1	**COLGADO**	P2/25	P3/49	P4/73	P5/1
2	P1/2	P2/26	P3/50	P4/74	P5/2
3	P1/3	P2/27	P3/51	P4/75	P5/3
4	P1/4	P2/28	P3/52	P4/76	P5/4
5	P1/5	P2/29	P3/53	P4/77	P5/5
6	P1/6	P2/30	P3/54	P4/78	P5/6
7	P1/7	P2/31	P3/55	P4/79	P5/7
8	P1/8	P2/32	P3/56	P4/80	P5/8
9	P1/9	P2/33	P3/57	P4/81	P5/9
10	P1/10	P2/34	P3/58	P4/82	P5/10
11	P1/11	P2/35	P3/59	P4/83	**P1/1**
12	P1/12	P2/36	P3/60	P4/84	
13	P1/13	P2/37	P3/61	P4/85	**P5/22**
14	P1/14	P2/38	P3/62	P4/86	
15	P1/15	P2/39	P3/63	P4/87	
16	P1/16	P2/40	P3/64	P4/88	
17	P1/17	P2/41	P3/65	P4/89	
18	P1/18	P2/42	P3/66	P4/90	**DVR ó Untagle**
19	P1/19	P2/43	P3/67	P4/91	
20	P1/20	P2/44	P3/68	P4/92	**PLAFÓN**
21	P1/21	P2/45	P3/69	P4/93	**PLAFÓN**
22	P1/22	P2/46	P3/70	P4/94	**PLAFÓN**
23	P1/23	P2/47	P3/71	P4/95	**PLAFÓN**
24	P1/24	P2/48	P3/72	P4/96	**P5/23**
25 ST UP	**CONECTADO**	**CONECTADO**	**CONECTADO**	**CONECTADO**	**CONECTADO**
26 ST DOWN	**CONECTADO**	**CONECTADO**	**CONECTADO**	**CONECTADO**	**CONECTADO**
27 F.O.					
28 F.O.					

ED 4 HCC N-1 LABS

45 U



PANEL 1 MARCA SYSTIMAX DE 24 PUERTOS
24 PUERTOS PONCHADOS
24 PUERTOS CONECTADOS

PANEL 2 MARCA SYSTIMAX DE 24 PUERTOS
24 PUERTOS PONCHADOS
24 PUERTOS CONECTADOS

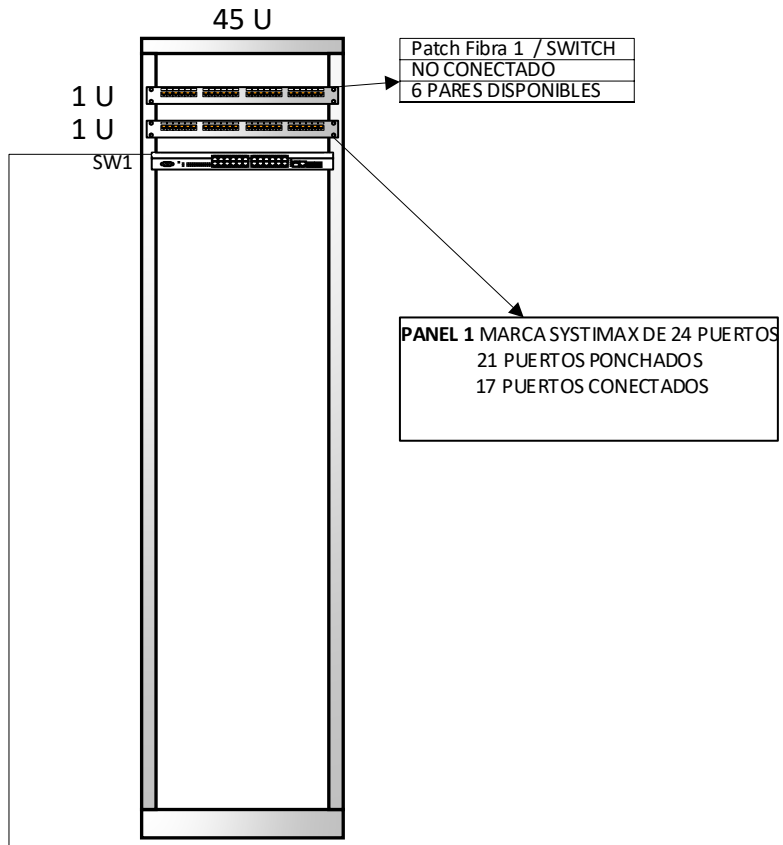
PANEL 3 MARCA SYSTIMAX DE 24 PUERTOS
24 PUERTOS PONCHADOS
24 PUERTOS CONECTADOS

PANEL 4 MARCA SYSTIMAX DE 24 PUERTOS
24 PUERTOS PONCHADOS
24 PUERTOS CONECTADOS

EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A2H124-24P**	STACK	SN:NO VISIBLE	24 Conectados	0 Conectados
SW2	Enterasys	A2H124-24P	STACK	SN:08013159225E	24 Conectados	0 Conectados
SW3	Enterasys	A2H124-24P	STACK	SN:08073144225E	24 Conectados	0 Conectados
SW4	Enterasys	A2H124-24P	STACK **(MGR)**	SN:10300068225M	24 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/ PUERTO)	SW2 (P/PTO)	SW3 (P/PTO)	SW4 (P/PTO)
1	P1/1	P2/1	P3/1	P4/1
2	P1/2	P2/2	P3/2	P4/2
3	P1/3	P2/3	P3/3	P4/3
4	P1/4	P2/4	P3/4	P4/4
5	P1/5	P2/5	P3/5	P4/5
6	P1/6	P2/6	P3/6	P4/6
7	P1/7	P2/7	P3/7	P4/7
8	P1/8	P2/8	P3/8	P4/8
9	P1/9	P2/9	P3/9	P4/9
10	P1/10	P2/10	P3/10	P4/10
11	P1/11	P2/11	P3/11	P4/11
12	P1/12	P2/12	P3/12	P4/12
13	P1/13	P2/13	P3/13	P4/13
14	P1/14	P2/14	P3/14	P4/14
15	P1/15	P2/15	P3/15	P4/15
16	P1/16	P2/16	P3/16	P4/16
17	P1/17	P2/17	P3/17	P4/17
18	P1/18	P2/18	P3/18	P4/18
19	P1/19	P2/19	P3/19	P4/19
20	P1/20	P2/20	P3/20	P4/20
21	P1/21	P2/21	P3/21	P4/21
22	P1/22	P2/22	P3/22	P4/22
23	P1/23	P2/23	P3/23	P4/23
24	P1/24	P2/24	P3/24	P4/24
25 ST UP	**CONECTADO**	**CONECTADO**	**CONECTADO**	**CONECTADO**
26 ST DOWN	**CONECTADO**	**CONECTADO**	**CONECTADO**	**CONECTADO**
27 F.O.				
28 F.O.				

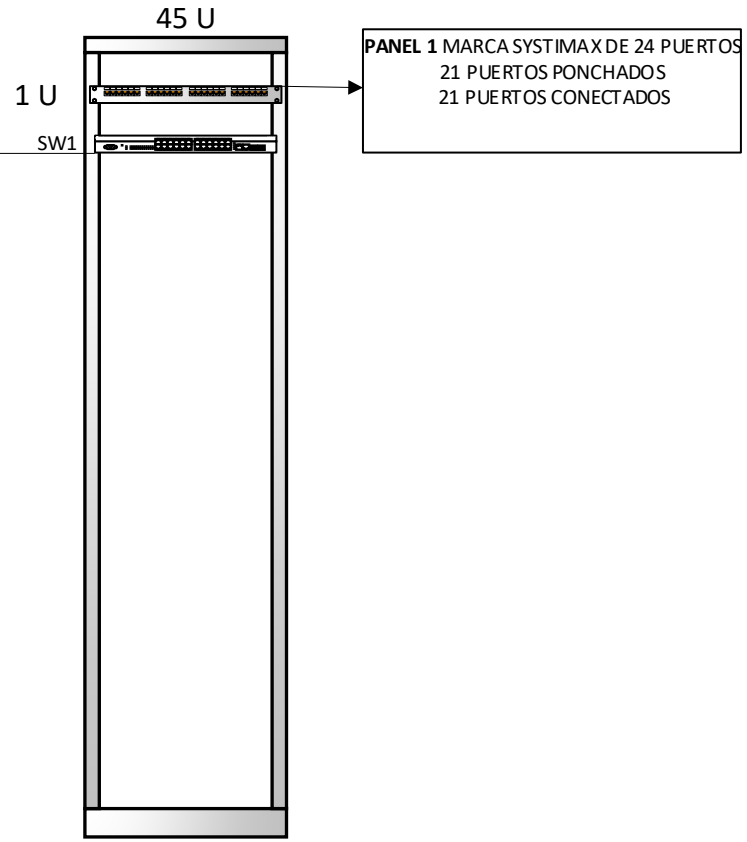
ED 4 HCC N-1 Pasillo



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	Enterasys	B5G124-24P2	MGR	SN:11370404225K	17 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)
1	P1/1
2	P1/2
3	P1/3
4	P1/4
5	P1/5
6	P1/6
7	P1/7
8	P1/8
9	P1/9
10	P1/10
11	P1/11
12	P1/12
13	P1/13
14	P1/14
15	
16	
17	
18	
19	
20	
21	
22	P1/22
23	P1/23
24	P1/24
25 STACK UP	
26 STACK DOWN	
27 F.O.	
28 F.O.	

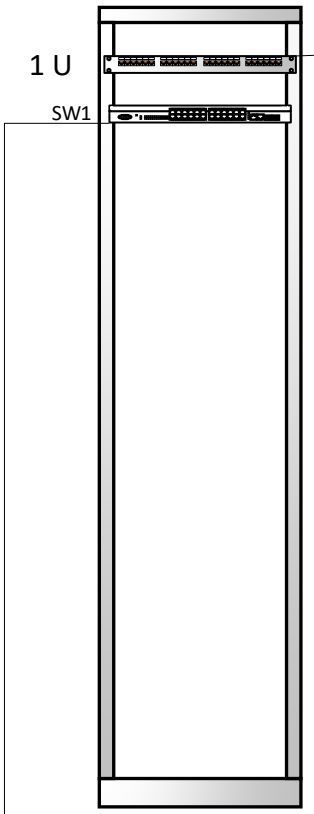
ED 4 HCC N-2



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**B5G124-24P2**	MGR	SN:10340925906D	21 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)
1	P1/1
2	P1/2
3	P1/3
4	P1/4
5	P1/5
6	P1/6
7	P1/7
8	P1/8
9	P1/9
10	P1/10
11	P1/11
12	P1/12
13	P1/13
14	P1/14
15	P1/15
16	P1/16
17	P1/17
18	P1/18
19	P1/19
20	P1/20
21	
22	
23	
24	P1/24
25 STACK UP	
26 STACK DOWN	
27 F.O.	
28 F.O.	

ED 4 HCC N-3

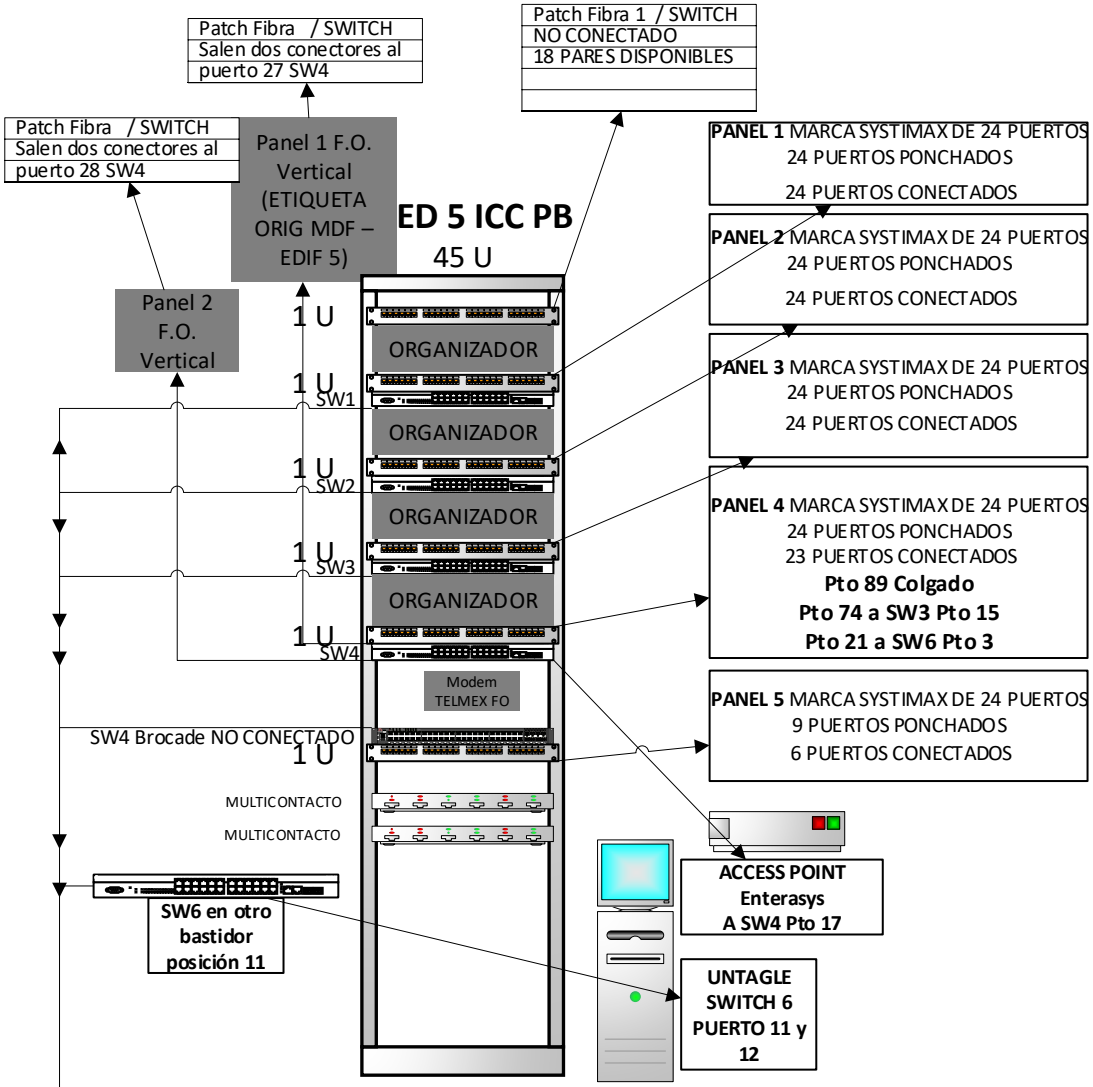


PANEL 1 MARCA SYSTIMAX DE 24 PUERTOS
21 PUERTOS PONCHADOS
22 PUERTOS CONECTADOS
PUERTO 19 A PTO 17 SW1 NO PONCHADO

EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**B5G124-24P2**	MGR	SN:12010457225K	24 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)
1	P1/1
2	P1/2
3	P1/3
4	P1/4
5	P1/5
6	P1/6
7	P1/7
8	P1/8
9	P1/9
10	P1/10
11	P1/11
12	P1/12
13	P1/13
14	P1/14
15	P1/15
16	P1/16
17	**P1/19**
18	**P1/20**
19	**P1/21**
20	**P1/22**
21	**PLAFÓN**
22	**PLAFÓN**
23	P1/23
24	P1/24
25 STACK UP	
26 STACK DOWN	
27 F.O.	
28 F.O.	

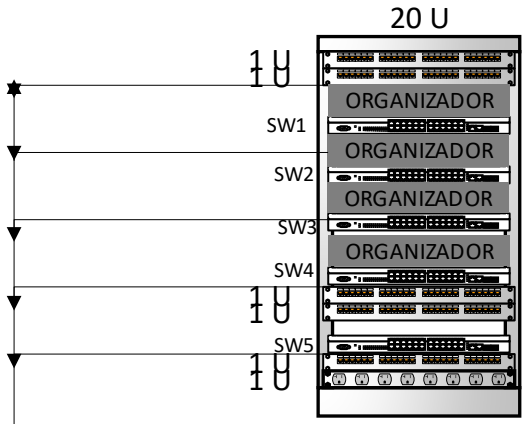
EDIFICIO 5



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A2H124-24P**	STACK	SN:10300049225M	24 Conectados	0 Conectados
SW2	Enterasys	A2H124-24P	**STACK (MGR)**	SN:10300100225M	24 Conectados	0 Conectados
SW3	Enterasys	A2H124-24P	STACK	SN:10300057225M	23 Conectados	0 Conectados
SW4	Enterasys	A2H124-24P	STACK	SN:10300194225M	23 Conectados	2 Conectados
SW5	**Brocade**	**ICX7250-48P-2x10G**	NO CONECTADO	SN:DUK3819M0LS	0 Conectados	0 Conectados
SW6	**Enterasys**	**A4H124-24P**	NO STACK	SN:11510518905G	13 Conectados	0 Conectados
AP	**Enterasys**	**WS-AP3620**	----------	**SN:10270336235J0000**		

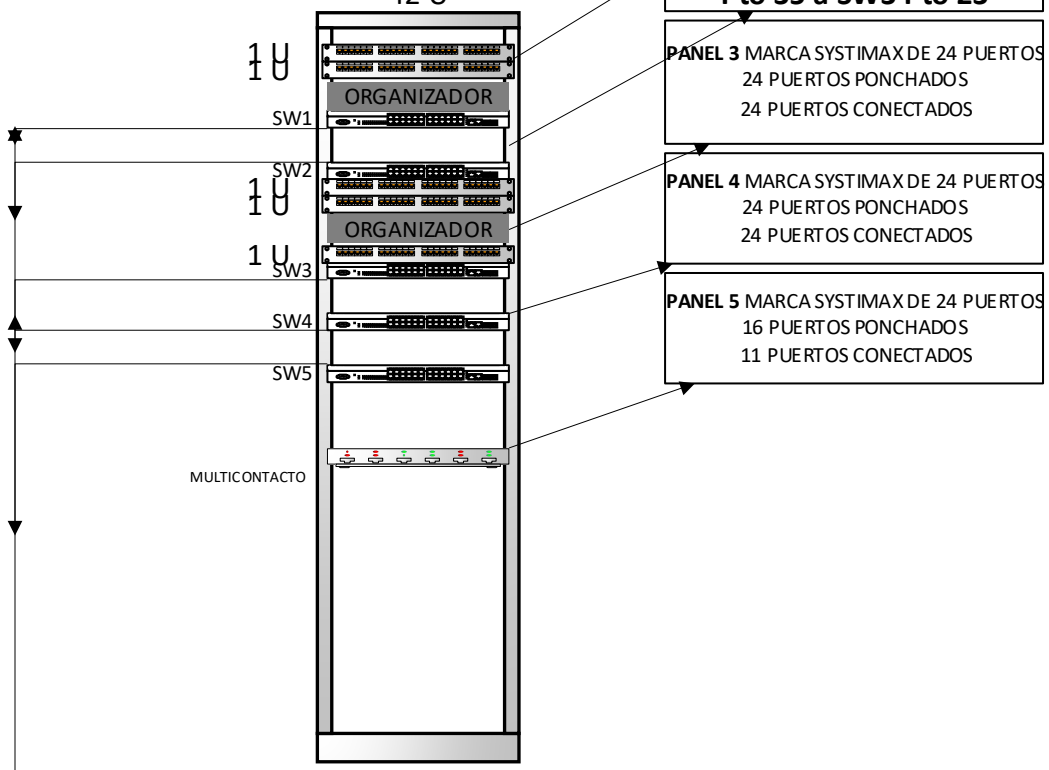
PUERTOS SWITCHES	SWITCH 1 (P/PTO)	SW2 (P/PTO)	SW3 (P/PTO)	SW4 (P/PTO)	SW5	SW6 (P/PTO)
1	P1/1	P2/25	P3/49	P4/73	B	SW4/21
2	P1/2	P2/26	P3/50	COLGADO	R	P5/2
3	P1/3	P2/27	P3/51	P4/75	O	P4/93
4	P1/4	P2/28	P3/52	P4/76	C	PLAFÓN
5	P1/5	P2/29	P3/53	P4/77	A	PLAFÓN
6	P1/6	P2/30	P3/54	P4/78	D	
7	P1/7	P2/31	P3/55	P4/79	E	PLAFÓN
8	P1/8	P2/32	P3/56	P4/80		
9	P1/9	P2/33	P3/57	P4/81		
10	P1/10	P2/34	P3/58	P4/82		
11	P1/11	P2/35	P3/59	P4/83		UNTAGLE
12	P1/12	P2/36	P3/60	P4/84		UNTAGLE
13	P1/13	P2/37	P3/61	P4/85		
14	P1/14	P2/38	P3/62	P4/86		
15	P1/15	P2/39	P4/74	P4/87		
16	P1/16	P2/40	P3/64	P4/88		
17	P1/17	P2/41	P3/65	AP		
18	P1/18	P2/42	P3/66	P4/90		
19	P1/19	P2/43	P3/67	P4/91		
20	P1/20	P2/44	P3/68	P4/92		P5/20
21	P1/21	P2/45	P3/69	SW6/1		P5/21
22	P1/22	P2/46	P3/70	P4/96		P5/22
23	P1/23	P2/47		P4/95		P5/23
24	P1/24	P2/48	P3/72			P5/24
25 ST UP	CONECTADO	CONECTADO	CONECTADO	CONECTADO		
26 ST DOWN	CONECTADO	CONECTADO	CONECTADO	CONECTADO		
27 F.O.				CONECTADO		
28 F.O.				CONECTADO		

ED 5 HCC N-1 ANEXO



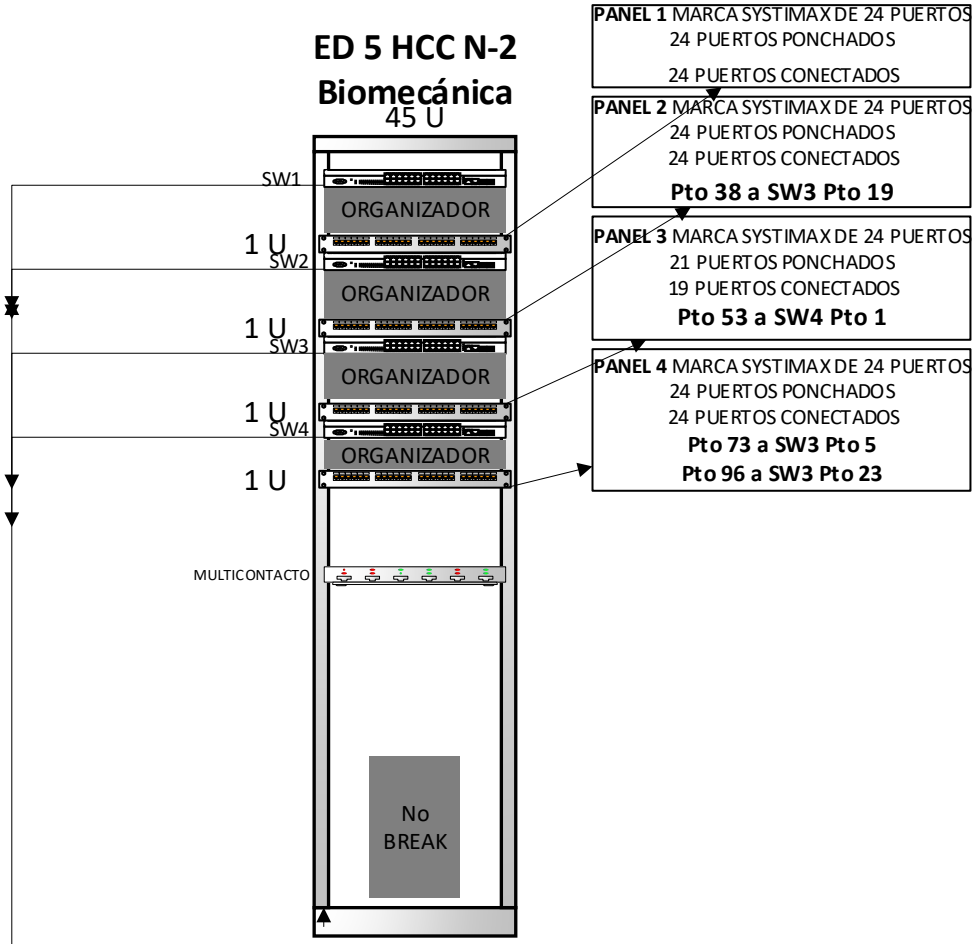
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A2H124-24**	**STACK (MGR)**	----------	23 Conectados	0 Conectados
SW2	**Enterasys**	**A2H124-24P**	STACK	----------	24 Conectados	0 Conectados
SW3	Enterasys	A2H124-24P	STACK	----------	24 Conectados	0 Conectados
SW4	Enterasys	A2H124-24P	**STACK (MGR)**	----------	22 Conectados	0 Conectado
SW5	Enterasys	A2H124-24	STACK	----------	21 Conectados	0 Conectado

ED 5 HCC N-1 Computación (Frente Anexo)



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A4H124-24P**	**STACK (MGR)**	SN:11510528905G	24 Conectados	0 Conectados
SW2	Enterasys	A4H124-24P	STACK	SN:11510517905G	24 Conectados	0 Conectados
SW3	Enterasys	A4H124-24P	STACK	SN:11510510905G	13 Conectados	0 Conectados
SW4	Enterasys	A4H124-24P	STACK	SN:11510509905G	24 Conectados	0 Conectados
SW5	Enterasys	A4H124-24P	STACK	SN:11510508905G	23 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SW2 (P/PTO)	SW3 (P/PTO)	SW4 (P/PTO)	SW 5 (P/PTO)
1	P1/1	P2/25	P5/97	P4/73	P3/49
2	P1/2	P2/26	P5/98	P4/74	P3/50
3	P1/3	P2/27	P5/99	P4/75	P3/51
4	P1/4	P2/28	P5/100	P4/76	P3/52
5	P1/5	P2/29	P5/101	P4/77	P3/53
6	P1/6	P2/30	P5/102	P4/78	P3/54
7	P1/7	P2/31	P5/103	P4/79	P3/55
8	P1/8	P2/32	P5/104	P4/80	P3/56
9	P1/9	P2/33	P5/105	P4/81	P3/57
10	P1/10	P2/34		P4/82	P3/58
11	P1/11	COLGADO		P4/83	P3/59
12	P1/12	P2/36		P4/84	P3/60
13	P1/13	P2/37		P4/85	P3/61
14	P1/14	P2/38		P4/86	P3/62
15	P1/15	P2/39		P4/87	P3/63
16	P1/16	P2/40		P4/88	P3/64
17	P1/17	P2/41	P5/117	P4/89	P3/65
18	P1/18	P2/42		P4/90	P3/66
19	P1/19	P2/43		P4/91	P3/67
20	P1/20	P2/44		P4/92	P3/68
21	P1/21	P2/45		P4/93	P3/69
22	P1/22	P2/46	PLAFÓN	P4/94	P3/70
23	P1/23	P2/47	P2/35	P4/95	P3/71
24	P1/24	P2/48	P5/120	P4/96	
25 ST UP	CONECTADO	CONECTADO	CONECTADO	CONECTADO	CONECTADO
26 ST DOWN	CONECTADO	CONECTADO	CONECTADO	CONECTADO	CONECTADO
27 F.O.					
28 F.O.					



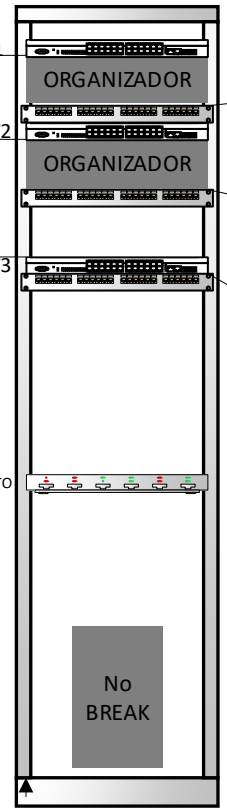
EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A2H124-24P**	**STACK (MGR)**	SN:08073160225E	24 Conectados	0 Conectados
SW2	Enterasys	A2H124-24P	STACK	SN:08013227225E	23 Conectados	0 Conectados
SW3	Enterasys	A2H124-24P	STACK	SN:08013225225E	24 Conectados	0 Conectados
SW4	**Enterasys**	**B5G124-24P2**	NO STACK	SN:10450421905F	24 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SW2 (P/PTO)	SW3 (P/PTO)	SW4 (P/PTO)
1	P1/1	P2/25	P3/49	P3/53
2	P1/2	P2/26	P3/50	P4/74
3	P1/3	P2/27	P3/51	P4/75
4	P1/4	P2/28	P3/52	P4/76
5	P1/5	P2/29		P4/77
6	P1/6	P2/30	P3/54	P4/78
7	P1/7	P2/31	P3/55	P4/79
8	P1/8	P2/32	P3/56	P4/80
9	P1/9	P2/33	P3/57	P4/81
10	P1/10	P2/34	P3/58	P4/82
11	P1/11	P2/35	P3/59	P4/83
12	P1/12	P2/36	P3/60	P4/84
13	P1/13	P2/37	P3/61	P4/85
14	P1/14		P3/62	P4/86
15	P1/15	P2/39	P3/63	P4/87
16	P1/16	P2/40	P3/64	P4/88
17	P1/17	P2/41	P3/65	P4/89
18	P1/18	P2/42	P3/66	P4/90
19	P1/19	P2/43	**P2/38**	P4/91
20	P1/20	P2/44	PLAFÓN	P4/92
21	P1/21	P2/45	**SW4/24**	P4/93
22	P1/22	P2/46	COLGADO	P4/94
23	P1/23	P2/47	**P4/96**	P4/95
24	P1/24	P2/48	P3/72	**SW3/21**
25 ST UP	CONECTADO	CONECTADO	CONECTADO	N/A
26 ST DOWN	CONECTADO	CONECTADO	CONECTADO	N/A
27 F.O.				
28 F.O.				

Patch Fibra / SWITCH
Salen dos conectores al puerto 27 SW2 (1 PAR)
Proveniente del ICC PB (VERIFICAR)

ED 5 HCC N-3 Jefatura SEPI

Panel F.O. Vertical



PANEL 1 MARCA SYSTIMAX DE 24 PUERTOS
24 PUERTOS PONCHADOS
24 PUERTOS CONECTADOS

PANEL 2 MARCA SYSTIMAX DE 24 PUERTOS
24 PUERTOS PONCHADOS
24 PUERTOS CONECTADOS
Pto 48 a SW2 Pto 24 Viene del suelo
Ptos 25-33 a SW3

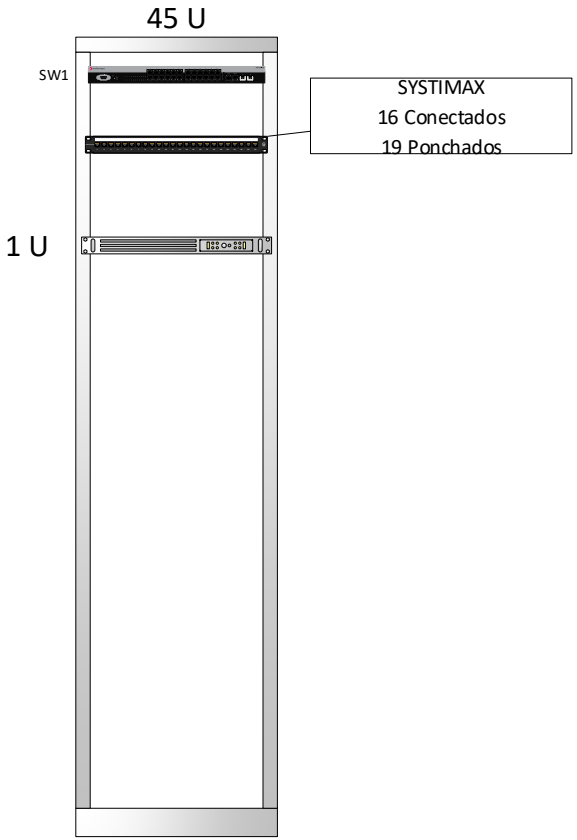
PANEL 3 MARCA SYSTIMAX DE 24 PUERTOS
7 PUERTOS PONCHADOS
0 PUERTOS CONECTADOS

EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	PTOS UTP	PTOS F.O.
SW1	**Enterasys**	**A2H124-24P**	STACK	SN:10300039225M	24 Conectados	0 Conectados
SW2	Enterasys	A2H124-24P	**STACK (MGR)**	SN:10300040225M	20 Conectados	1 Conectados
SW3	Enterasys	A2H124-24P	STACK	SN:08073162225E	11 Conectados	0 Conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/ PUERTO)	SW2 (P/PTO)	SW3 (P/PTO)
1	P1/1	PLAFÓN	P2/25
2	P1/2		P2/32
3	P1/3	PLAFON	P2/27
4	P1/4	PLAFÓN	P2/28
5	P1/5	PLAFÓN	P2/29
6	P1/6	PLAFON	P2/26
7	P1/7		COLGADO
8	P1/8		
9	P1/9	P2/43	P2/33
10	P1/10	P2/34	
11	P1/11	P2/35	P2/30
12	P1/12	P2/36	
13	P1/13	P2/37	PLAFON
14	P1/14	P2/38	
15	P1/15	P2/39	
16	P1/16	P2/40	
17	P1/17	P2/41	P2/31
18	P1/18	P2/42	
19	P1/19	P2/44	
20	P1/20	P2/45	
21	P1/21	P2/46	
22	P1/22		
23	P1/23	P2/47	
24	P1/24	P2/48	
25 ST UP	CONECTADO	CONECTADO	CONECTADO
26 ST DOWN	CONECTADO	CONECTADO	CONECTADO
27 F.O.		CONECTADO	
28 F.O.			

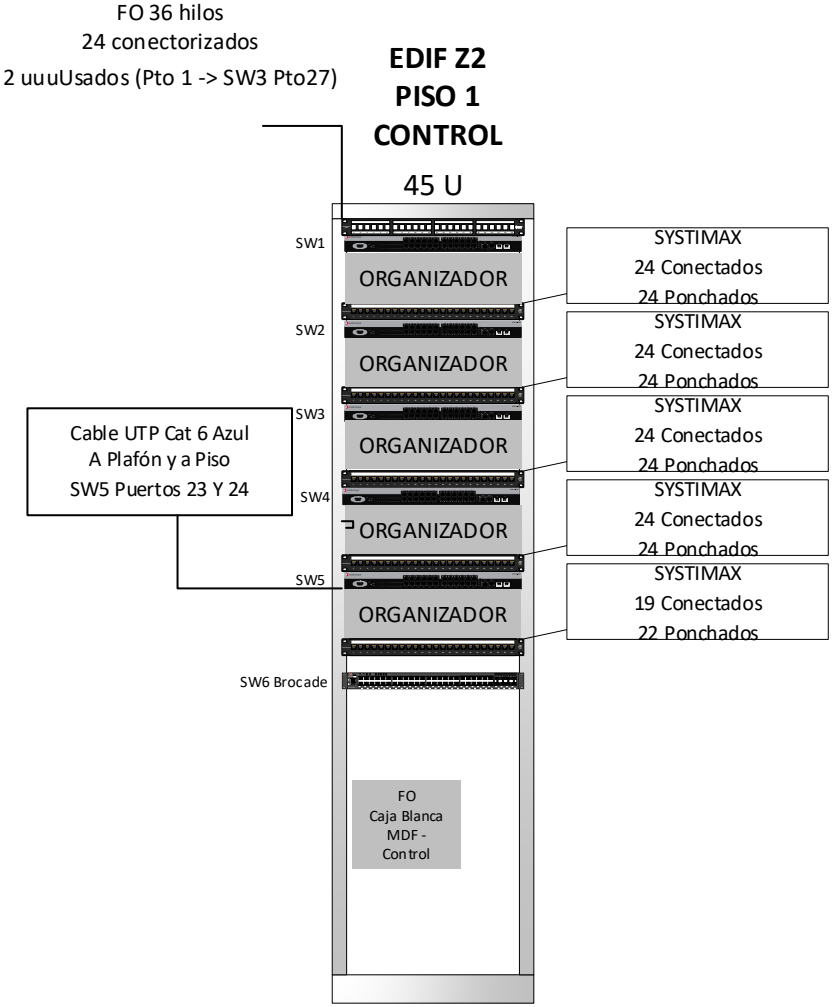
EDIFICIO Z

EDIF Z2 PB
FÍSICA



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	----------	10300166225M	----------	23 conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)
1	P1/1
2	P1/2
3	P1/3
4	P1/4
5	P1/5
6	P1/6
7	P1/7
8	P1/8
9	P1/9
10	P1/10
11	P1/11
12	P1/12
13	P1/13
14	P1/14
15	P1/15
16	P1/16
17	Cat 5E Pared
18	Cat 5E Pared
19	Cat 5E Pared
20	PLAFÓN
21	Cat 5E Pared
22	NO CONECTADO
23	PLAFÓN
24	AZUL PLAFÓN
25 STACK UP	----------
26 STACK DOWN	----------
27 F.O.	----------
28 F.O.	----------

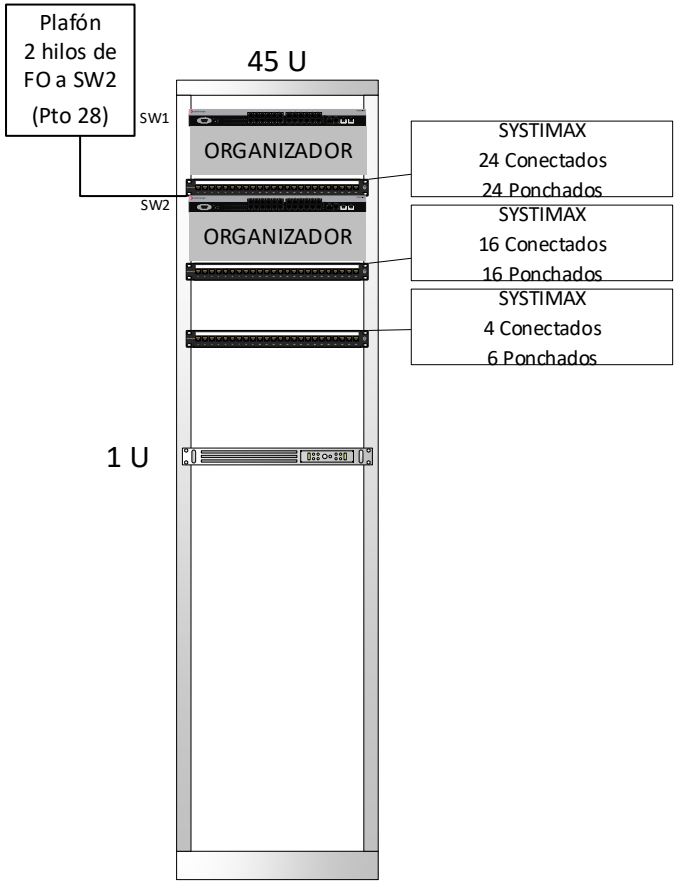


EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	STACK	10300045225M	----------	24 conectados
SW2	ENTERASYS	A2H124-24P	STACK	10300043225M	----------	24 conectados
SW3	ENTERASYS	A2H124-24P	STACK	10300067225M	1 conec	24 conectados
SW4	ENTERASYS	A2H124-24P	STACK (MGR)	10300059225M	----------	24 conectados
SW5	ENTERASYS	A2H124-24P	STACK	10300211225M	----------	21 conectados
SW6	BROCADE	ICX7250-48P	----------	DUK3819M0M3	----------	0 conectados

PUERTOS SWITCHES	SWITCH 1 (P/PTO)	SW 2 (P/PTO)	SW 3 (P/PTO)	SW 4 (P/PTO)	SW 5 (P/PTO)	SW 6 BROCADE
1	P1/1	P2/25	P3/49	P4/73	P5/97	
2	P1/2	COLGADO	P3/50	P4/74	P5/98	
3	P1/3	P2/27	P3/51	P4/75	P5/99	
4	P1/4	P2/28	P3/52	P4/76	P5/100	
5	P1/5	P2/29	P3/53	P4/77	P5/101	
6	P1/6	P2/30	P3/54	P4/78	P5/102	
7	P1/7	P2/31	P3/55	P4/79	P5/103	
8	P1/8	P2/32	P3/56	P4/80	P5/104	
9	P1/9	P2/33	P3/57	P4/81	P5/105	
10	P1/10	P2/34	P3/58	P4/82	P5/106	
11	P1/11	P2/35	P3/59	P4/83	P5/107	
12	P1/12	P2/36	P3/60	P4/84	P5/108	
13	P1/13	P2/37	P3/61	P4/85	P5/109	
14	P1/14	P2/38	P3/62	P4/86	P5/110	
15	P1/15	P2/39	P3/63	P4/87	P5/111	
16	P1/16	P2/40	P3/64	P4/88	P5/112	
17	P1/17	P2/41	P3/65	P4/89	P5/113	
18	P1/18	P2/42	P3/66	P4/90	P5/114	
19	P1/19	P2/43	P3/67	P4/91	N/C	
20	P1/20	P2/44	P3/68	P4/92	N/C	
21	P1/21	P2/45	P3/69	P4/93	N/C	
22	P1/22	P2/46	P3/70	P4/94	P5/115	
23	P1/23	P2/47	P3/71	P4/95	Cat 6 Plafón	
24	P1/24	P2/48	P3/72	P4/96	Cat 6 Suelo	
25 STACK UP	CONECTADO	CONEC	CONEC	CONEC	CONEC	
26 STACK DOWN	CONECTADO	CONEC	CONEC	CONEC	CONEC	
27 F.O.	----------	----------	CONECTADO Panel FO Pto 1	---------	---------	
28 F.O.	----------	----------	----------	---------	---------	

IMAX

EDIF Z2 PISO 2
ACÚSTICA

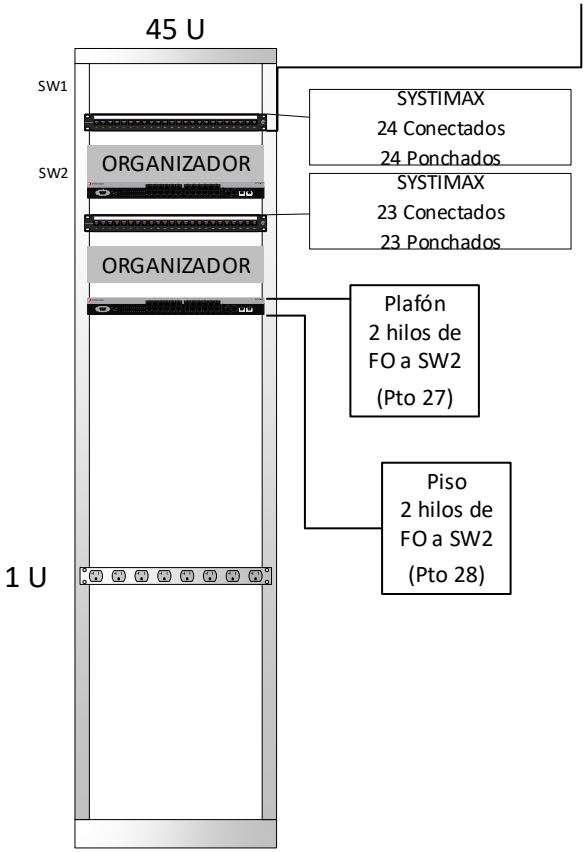


PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)
1	P1/1	P2/25
2	P1/2	P2/26
3	P1/3	P2/27
4	P1/4	P2/28
5	P1/5	P2/29
6	P1/6	P2/30
7	P1/7	P2/31
8	P1/8	P2/32
9	P1/9	P2/33
10	P1/10	P2/34
11	P1/11	P2/35
12	P1/12	P2/36
13	P1/13	P2/37
14	P1/14	P2/38
15	P1/15	P2/39
16	P1/16	P2/40
17	P1/17	**P3/1**
18	P1/18	**P3/2**
19	P1/19	**P3/3**
20	P1/20	**P3/4**
21	P1/21	**SIN CONEXIÓN**
22	P1/22	**SIN CONEXIÓN**
23	P1/23	**COLGADO**
24	P1/24	**SIN CONEXIÓN**
25 STACK UP	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO
27 F.O.	----------	----------
28 F.O.	----------	F.O. NARANJA PLAFÓN

EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	STACK (MGR)	10300058225M	----------	24 conectados
SW2	ENTERASYS	A2H124-24	STACK	08450006225F	1 conec	21 conectados

EDIF Z2 PISO 3
ACADEMIA
COMUNICACIONES

Llegan dos cables de FO
Uno de 6 hilos (conectorizados) SW1 – Pto 28 (2 usados)
Uno de 12 hilos (conectorizados) de MCC EDIF 1 a SW1 - Pto27 (2 usados)

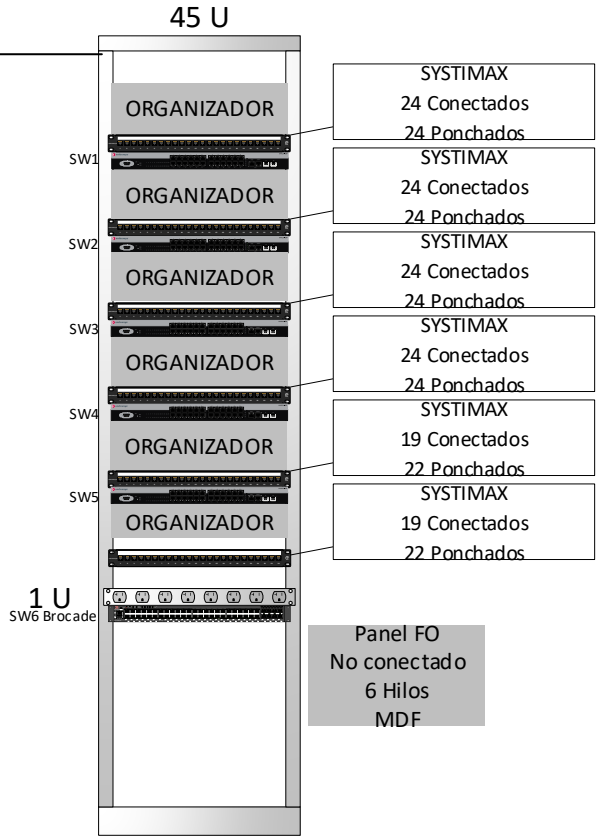


EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	STACK (MGR)	10300065225M	2 conec	24 conectados
SW2	ENTERASYS	A2H124-24P	STACK	10300208225M	2 conec	24 conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 (PANEL/PUERTO)
1	P1/1	P2/1
2	P1/2	P2/2
3	P1/3	P2/3
4	P1/4	P2/4
5	P1/5	P2/5
6	P1/6	P2/6
7	P1/7	P2/7
8	P1/8	P2/8
9	P1/9	P2/9
10	P1/10	P2/10
11	P1/11	P2/11
12	P1/12	P2/12
13	P1/13	P2/13
14	P1/14	P2/14
15	P1/15	P2/15
16	P1/16	P2/16
17	P1/17	P2/17
18	P1/18	P2/18
19	P1/19	P2/19
20	P1/20	P2/20
21	P1/21	P2/21
22	P1/22	**UNTAGLE**
23	P1/23	**UNTAGLE**
24	P1/24	P2/24
25 STACK UP	CONECTADO	CONECTADO
26 STACK DOWN	CONECTADO	CONECTADO
27 F.O.	MCC EDIF 1	F.O. NARANJA PLAFÓN
28 F.O.	NO CONECTADO	F.O. NARANJA PISO

FO 4 Hilos conectorizados
2 usados a SW4 Pto27

EDIF Z3 PB
ELECTROTECNIA

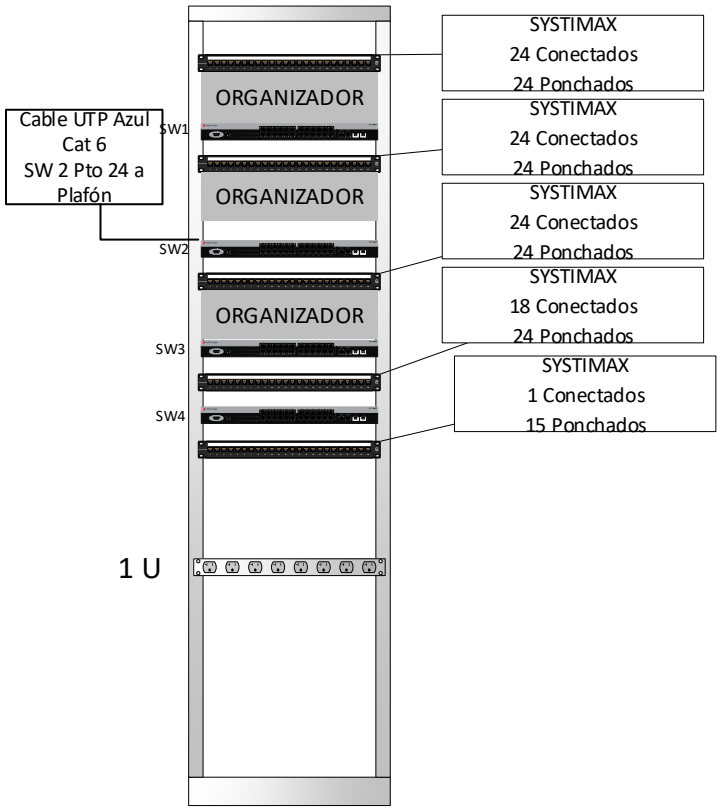


EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	STACK	10300097225M	----------	24 conectados
SW2	ENTERASYS	A2H124-24	STACK	10421009225P	----------	24 conectados
SW3	ENTERASYS	A2H124-24	STACK	10421011225P	----------	24 conectados
SW4	ENTERASYS	A2H124-24	STACK (MGR)	10421008225P	----------	23 conectados
SW5	ENTERASYS	A2H124-24	STACK	10421057225P	----------	19 conectados
SW6	BROCADE	ICX7250-48P	----------	DUK3819M0LR	----------	7 conectados

PUERTOS SWITCHES	SWITCH 1 (P/PTO)	SW 2 (P/PTO)	SW 3 (P/PTO)	SW 4 (P/PTO)	SW 5 (P/PTO)	SW 6 BROCADE
1	P1/1	P2/25	P3/49	P4/73	P5/97	P6/10
2	P1/2	COLGADO	P3/50	P4/74	P5/98	P6/12
3	P1/3	P2/27	P3/51	P4/75	P5/99	P6/13
4	P1/4	P2/28	P3/52	P4/76	P5/100	P6/15
5	P1/5	P2/29	P3/53	P4/77	P5/101	P6/16
6	P1/6	P2/30	P3/54	P4/78	P5/102	P6/20
7	P1/7	P2/31	P3/55	P4/79	P5/103	
8	P1/8	P2/32	P3/56	P4/80	P5/104	
9	P1/9	P2/33	P3/57	P4/81	P5/105	
10	P1/10	P2/34	P3/58	P4/82	P5/106	
11	P1/11	P2/35	P3/59	P4/83	P5/107	
12	P1/12	P2/36	P3/60	P4/84	P5/108	
13	P1/13	P2/37	P3/61	P4/85	P5/109	
14	P1/14	P2/38	P3/62	P4/86	P5/110	
15	P1/15	P2/39	P3/63	P4/87	P5/111	
16	P1/16	P2/40	P3/64	P4/88	N/C	
17	P1/17	P2/41	P3/65	P4/89	N/C	
18	P1/18	P2/42	P3/66	P4/90	PARED	
19	P1/19	P2/43	P3/67	P4/91	PTO 48/SW6	
20	P1/20	P2/44	P3/68	P4/92	PARED	
21	P1/21	P2/45	P3/69	P4/93	N/C	
22	P1/22	P2/46	P3/70	P4/94	PARED	
23	P1/23	P2/47	P3/71	P4/95	N/C	
24	P1/24	P2/48	P3/72	P4/96	N/C	PTO 19/SW5
25 STACK UP	CONEC	CONEC	CONEC	CONEC	CONEC	
26 STACK DOWN	CONEC	CONEC	CONEC	CONEC	CONEC	
27 F.O.	---------- -----	---------- ---	----------	CONECTADO Panel FO Pto 1 MCC	----------	
28 F.O.	---------- -----	---------- ---	----------	----------	----------	

IMAX

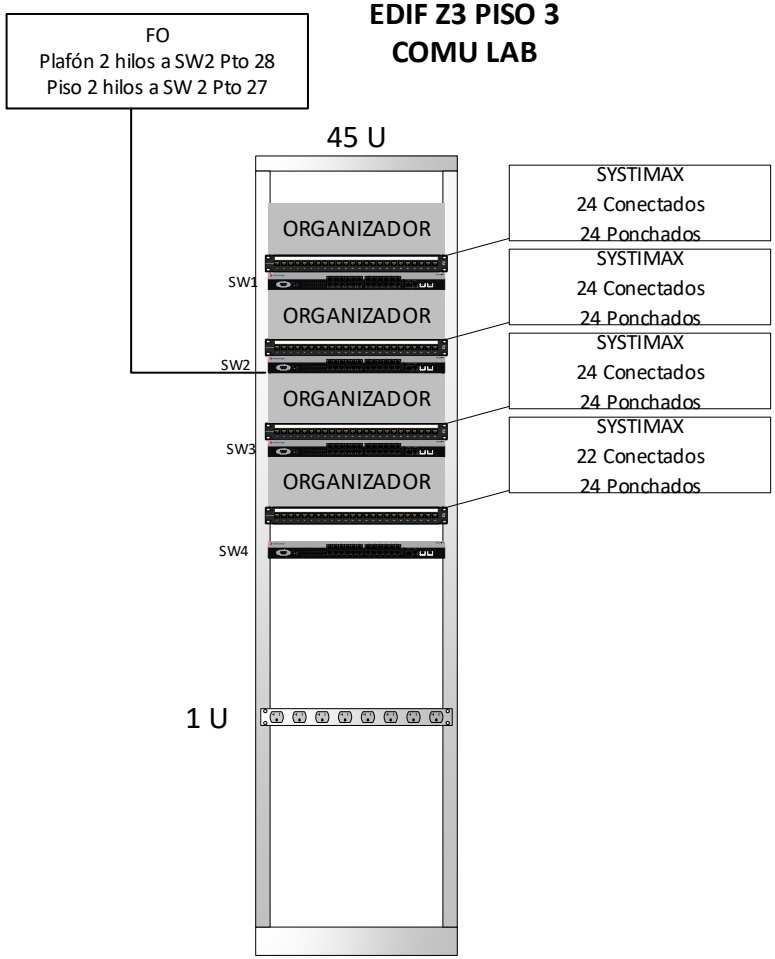
EDIF Z3
PISO 1
CIRCUITOS



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	STACK (MGR)	No Visible	----------	24 conectados
SW2	ENTERASYS	A2H124-24	STACK	No Visible	----------	24 conectados
SW3	ENTERASYS	A2H124-24	STACK	No Visible	----------	24 conectados
SW4	ENTERASYS	V2H124-24	----------	No Visible	----------	22 conectados

PUERTOS SWITCHES	SWITCH 1 (P/PTO)	SW 2 (P/PTO)	SW 3 (P/PTO)	SW 4 (P/PTO)
1	P1/1	P2/25	P3/49	P4/75
2	P1/2	**COLGADO**	P3/50	P4/76
3	P1/3	P2/27	P3/52	P4/77
4	P1/4	P2/28	P3/53	P4/78
5	P1/5	P2/29	**P3/54**	P4/79
6	P1/6	P2/30	**P3/55**	P4/80
7	P1/7	P2/31	**P3/56**	P4/81
8	P1/8	P2/32	**P3/57**	P4/82
9	P1/9	P2/33	**P3/58**	P4/83
10	P1/10	P2/34	**P3/59**	P4/84
11	P1/11	P2/35	**P3/60**	P4/85
12	P1/12	P2/36	**P3/61**	P4/86
13	P1/13	P2/37	**P3/62**	P4/87
14	P1/14	P2/38	**P3/63**	P4/88
15	P1/15	**P2/40**	**P3/64**	P4/89
16	P1/16	**P2/41**	**P3/65**	P4/90
17	P1/17	**P2/42**	**P3/66**	P4/91
18	P1/18	**P2/43**	**P3/67**	P4/92
19	P1/19	**P2/44**	**P3/68**	**N/C**
20	P1/20	**P2/45**	**P3/69**	**P1/22**
21	P1/21	**P2/46**	**P3/70**	**P1/23**
22	**P5/59**	**P2/47**	**P3/71**	**P1/24**
23	**P3/51**	**P2/48**	**P3/72**	N/C
24	**P2/39**	AZUL PLAFÓN	**SW4/PTO24**	**SW3/PTO24**
25 STACK UP	CONEC	CONEC	CONEC	**NA**
26 STACK DOWN	CONEC	CONEC	CONEC	NA
27 F.O.	----------	----------	----------	----------
28 F.O.	----------	----------	----------	----------

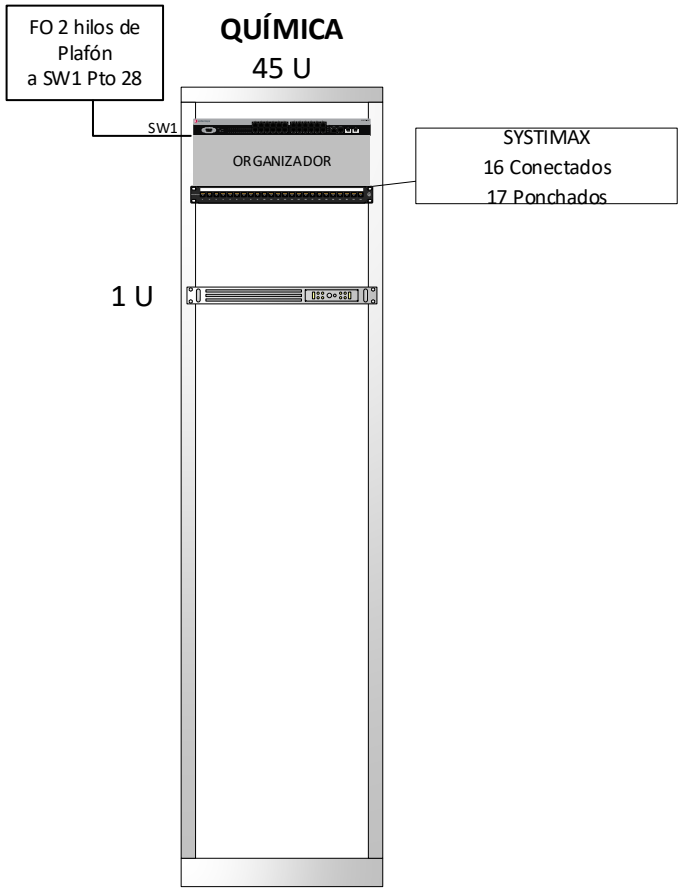
EDIF Z3 PISO 3
COMU LAB



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	STACK (MGR)	10300138225M	---------	24 conectados
SW2	ENTERASYS	A2H124-24P	STACK	10300046225M	2 conec	24 conectados
SW3	ENTERASYS	A2H124-24P	STACK	10300047225M	---------	24 conectados
SW4	ENTERASYS	A2H124-24P	STACK	10300066225M	---------	22 conectados

PUERTOS SWITCHES	SWITCH 1 (P/PTO)	SWITCH 2 (P/PTO)	SWITCH 3 (P/PTO)	SWITCH 4 (P/PTO)
1	P1/1	P2/25	P3/49	P4/73
2	P1/2	P2/26	P3/50	P4/74
3	P1/3	P2/27	P3/51	P4/75
4	P1/4	P2/28	P3/52	P4/76
5	P1/5	P2/29	P3/53	P4/77
6	P1/6	P2/30	P3/54	P4/78
7	P1/7	P2/31	P3/55	P4/79
8	P1/8	P2/32	P3/56	P4/80
9	P1/9	P2/33	P3/57	P4/81
10	P1/10	P2/34	P3/58	P4/82
11	P1/11	P2/35	P3/59	P4/83
12	P1/12	P2/36	P3/60	P4/84
13	P1/13	P2/37	P3/61	P4/85
14	P1/14	P2/38	P3/62	P4/86
15	P1/15	P2/39	P3/63	P4/87
16	P1/16	P2/40	P3/64	P4/88
17	P1/17	P2/41	P3/65	P4/89
18	P1/18	P2/42	P3/66	P4/90
19	P1/19	P2/43	P3/67	P4/91
20	P1/20	P2/44	P3/68	P4/92
21	P1/21	P2/45	P3/69	P4/93
22	P1/22	P2/46	P3/70	P4/94
23	P1/23	P2/47	P3/71	P4/95
24	P1/24	P2/48	P3/72	P4/96
25 STACK UP	CONEC	CONEC	CONEC	CONEC
26 STACK DOWN	CONEC	CONEC	CONEC	CONEC
27 F.O.	--------	2 hilos naranjas desde el piso	---------	---------
28 F.O.	---------	2 hilos naranjas desde plafón	---------	---------

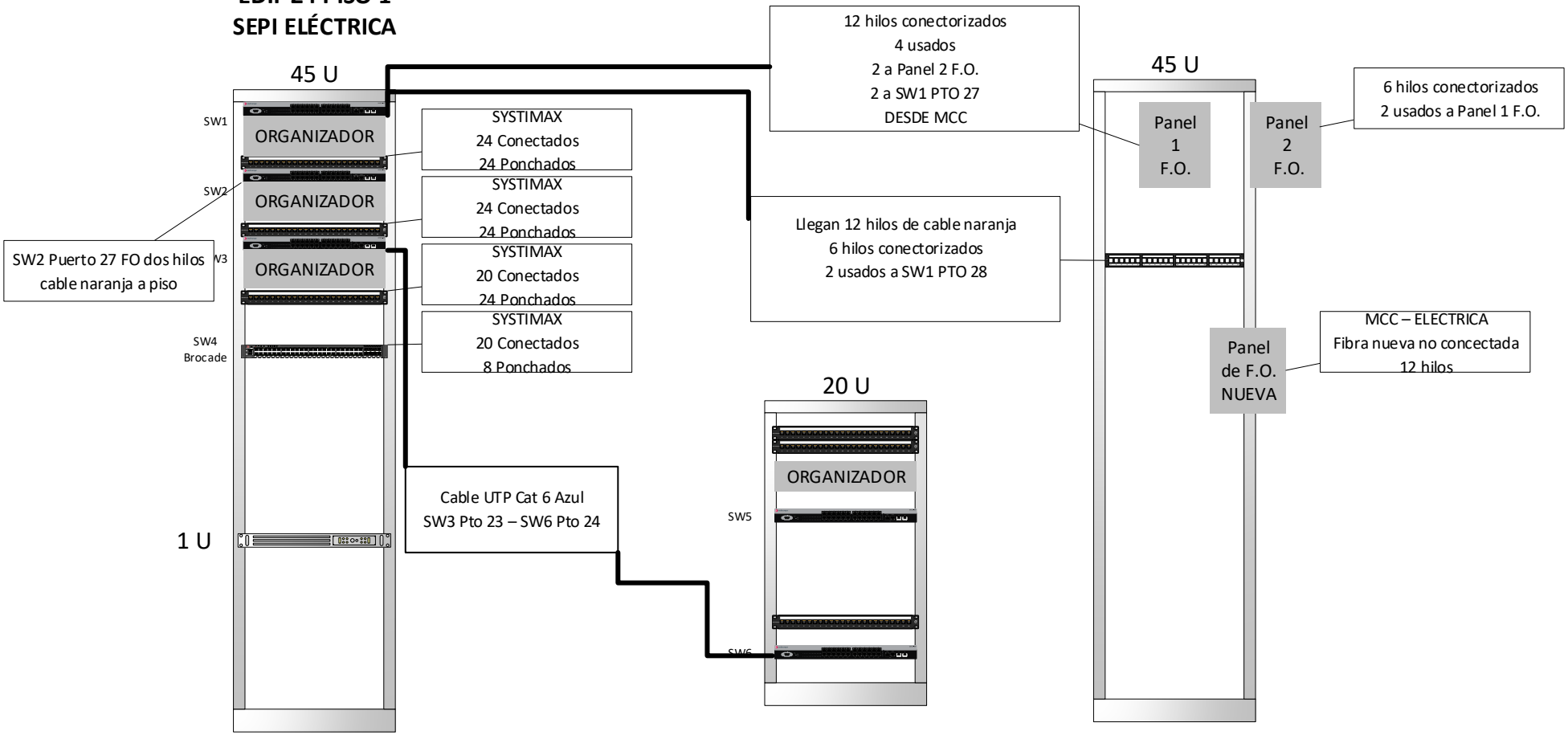
EDIF Z4
PB
QUÍMICA
45 U



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	----------	10300159225M	1 conec	20 conectados

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)
1	P1/1
2	P1/2
3	P1/3
4	P1/4
5	P1/5
6	P1/6
7	P1/7
8	P1/8
9	P1/9
10	P1/10
11	P1/11
12	P1/12
13	P1/13
14	P1/14
15	P1/15
16	P1/16
17	n/c
18	Pared
19	Pared
20	Pared
21	n/c
22	n/c
23	n/c
24	colgado
25 STACK UP	n/c
26 STACK DOWN	n/c
27 F.O.	n/c
28 F.O.	2 hilos naranjas desde plafón

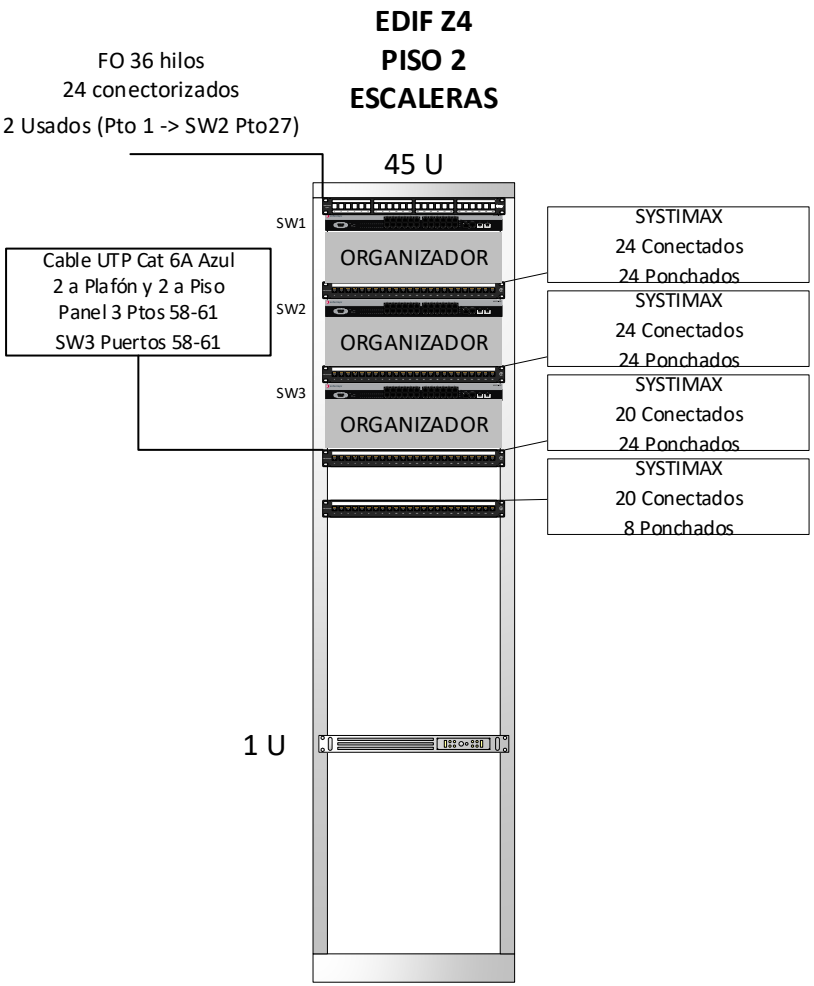
EDIF Z4 PISO 1
SEPI ELÉCTRICA



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	STACK (MGR)	10300192225M	----------	24 conectados
SW2	ENTERASYS	A2H124-24P	STACK	10300150225M	1 conec	24 conectados
SW3	ENTERASYS	A2H124-24P	STACK	10300087225M	----------	24 conectados
SW4	BROCADE	ICX7250 48P	----------	DUK3819MOMA	----------	----------
SW5	ENTERASYS	A2H124-24P	STACK (MGR)	No visible	----------	20 conectados
SW6	ENTERASYS	A2H124-24P	STACK	No visible	----------	23 conectados

EDIF Z4 PISO 1 SEPI
ELÉCTRICA
TABLA DE CONEXIONES

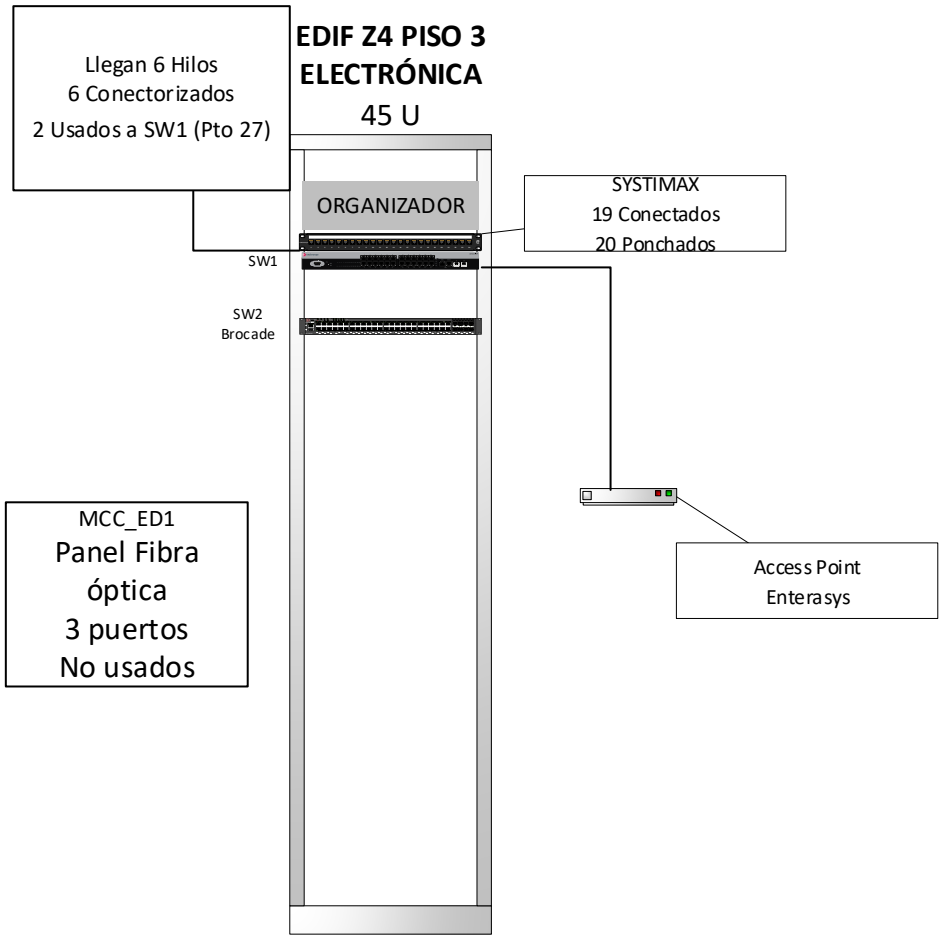
PUERTOS SWITCHES	SWITCH 1 (P/PTO)	SWITCH 2 (P/PTO)	SWITCH 3 (P/PTO)	SWITCH 4 BROCADE
1	P1/1	P2/25	P3/49	
2	P1/2	P2/26	P3/50	
3	P1/3	P2/27	P3/51	
4	P1/4	P2/28	P3/52	
5	P1/5	P2/29	P3/53	
6	P1/6	P2/30	P3/54	
7	P1/7	P2/31	P3/55	
8	P1/8	P2/32	P3/56	
9	P1/9	P2/33	P3/57	
10	P1/10	P2/34	P3/58	
11	P1/11	P2/35	P3/59	
12	P1/12	P2/36	P3/60	
13	P1/13	P2/37	P3/61	
14	P1/14	P2/38	P3/62	
15	P1/15	P2/39	P3/63	
16	P1/16	P2/40	P3/64	
17	**CPU (server)**	P2/41	P3/65	
18	P1/18	P2/42	P3/66	
19	P1/19	P2/43	P3/67	
20	P1/20	P2/44	P3/68	
21	P1/21	P2/45	P3/69	
22	P1/22	P2/46	P3/70	
23	P1/23	**n/c**	**Rack 2 SW 2**	
24	**CPU (server)**	P2/48	P3/72	
25 STACK UP	CONEC	CONEC	CONEC	
26 STACK DOWN	CONEC	CONEC	CONEC	
27 F.O.	Patch Panel FO cuadrado PTO 1 (MCC)	2 hilos naranjas desde el piso (Prob. Química)	--------	
28 F.O.	Patch Panel FO Horizontal PTO 1	----------	--------	



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	STACK	10300042225M	----------	24 conectados
SW2	ENTERASYS	A2H124-24P	STACK (MGR)	10300162225M	1 conec	24 conectados
SW3	ENTERASYS	A2H124-24P	STACK	10300063225M	----------	24 conectados

PUERTOS SWITCHES	SWITCH 1 (P/PTO)	SWITCH 2 (P/PTO)	SWITCH 3 (P/PTO)
1	P1/1	P2/25	P3/49
2	P1/2	P2/26	P3/50
3	P1/3	P2/27	P3/51
4	P1/4	P2/28	P3/52
5	P1/5	P2/29	P3/53
6	P1/6	P2/30	P3/54
7	P1/7	P2/31	P3/55
8	P1/8	P2/32	P3/56
9	P1/9	P2/33	P3/57
10	P1/10	P2/34	P3/58
11	P1/11	P2/35	P3/59
12	P1/12	P2/36	P3/60
13	P1/13	P2/37	P3/61
14	P1/14	P2/38	**P3/68**
15	P1/15	P2/39	Cat 5E Azul Plafón
16	P1/16	P2/40	**P3/70**
17	P1/17	P2/41	**P3/62**
18	P1/18	P2/42	**P3/72**
19	P1/19	P2/43	**P3/64**
20	P1/20	P2/44	**P4/2**
21	P1/21	P2/45	**P4/23**
22	P1/22	P2/46	**P4/4**
23	**P3/63**	P2/47	**Untagle**
24	P1/24	P2/48	**Untagle**
25 STACK UP	CONEC	CONEC	CONEC
26 STACK DOWN	CONEC	CONEC	CONEC
27 F.O.	----------	Patch Panel FO Pto 1	--------
28 F.O.	----------	----------	--------

IMAX



EQUIPO	MARCA	MODELO	CONEXIÓN	No. De Serie	Ptos FO	Ptos UTP
SW1	ENTERASYS	A2H124-24P	STACK (MGR)	10300142225M	1 conec	21 conectados
SW2	BROCADE	ICX-7250-48P	STACK	DUK3819M0LG	---------	----------
AP	ENTERASYS					

PUERTOS SWITCHES	SWITCH 1 (PANEL/PUERTO)	SWITCH 2 BOCADE
1	N/C	
2	P1/1	
3	P1/2	
4	P1/3	
5	P1/4	
6	P1/5	
7	P1/6	
8	P1/7	
9	P1/8	
10	P1/9	
11	P1/10	
12	PLAFÓN	
13	P1/11	
14	P1/12	
15	P1/13	
16	P1/14	
17	N/C	
18	P1/15	
19	P1/16	
20	P1/17	
21	P1/18	
22	P1/19	
23	N/C	
24	AP	
25 STACK UP	n/c	
26 STACK DOWN	n/c	
27 F.O.	PUERTO 3 PATCH PANEL FO	
28 F.O.	---------	

Especificaciones de dos Dispositivos de Red

Cisco Nexus 9500 Series Switches

Product overview

Application architectures and deployment modes are rapidly evolving. Modern applications are multinode, highly modular, and deployed over a combination of bare-metal, virtual, and cloud data center environments. In addition to that, individual departments within an organization have varying infrastructure and networking needs. These factors require that data center networks be simple, programmable, extensible, scalable, and shareable to meet the demands of applications.

The Cisco Nexus® 9000 Series Switches operate in one of two modes – Cisco Application Centric Infrastructure (Cisco ACI™) or Cisco NX-OS. In Cisco ACI mode, these switches provide a turnkey, fully automated, policy-based architecture to design and manage data center fabrics. In Cisco NX-OS mode, these switches provide the capability to use foundational layer 2/3 technologies, as well as modern technologies such as VXLAN, with a Border Gateway Protocol–Ethernet VPN (BGP-EVPN) control plane, segment routing, Multiprotocol Label Switching (MPLS), and automation via NX-APIs.

The Cisco Nexus 9000 Series Switches include the Nexus 9500 Series modular switches and the Nexus 9200/9300 Series fixed switches.

Figure 1. Cisco Nexus 9000 Series Switch Chassis

The Cisco Nexus 9500 Series modular switches are capable of supporting a bandwidth of up to 172.8 Terabits per second (Tbps) with a comprehensive selection of line cards that provide 1-, 10-, 25-, 40-, 50-, and 100-Gigabit Ethernet interfaces. Using these line cards, the Cisco Nexus 9500 Series switches can be configured with up to

1. 576 100-Gigabit Ethernet ports (or)
2. 576 40-Gigabit Ethernet ports (or)
3. 2304 25-Gigabit Ethernet ports (or)
4. 2304 10-Gigabit Ethernet ports

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

The supervisor, system controller, power supplies, and line cards are common across all three switches. Each switch, however, has unique fabric modules and fan trays that plug in vertically in the rear of the chassis.

Table 1. Features and benefits

Feature	Benefit
High performance	The Cisco Nexus 9500 Series cloud-scale switch delivers up to 172.8 Tbps of nonblocking performance at a latency of 5 microseconds or less at 100-, 50-, 40-, 25-, 10-, and 1-Gigabit Ethernet speeds. This enables customers to build robust and scalable high-speed fabrics that can support several thousands of high-speed access ports.
Telemetry	The Cisco Nexus 9500 Series cloud-scale switches support extensive switch and flow telemetry capabilities that provide extensive real-time visibility into switch and fabric states.
High-density 1-, 10-, 25-, 40- and 50-Gigabit Ethernet access configuration	Organizations can transition from low-speed (100-Megabit Ethernet and 1-Gigabit Ethernet) server access designs to high-speed (1-, 10-, 25-, 40-, and 50-Gigabit Ethernet) server access designs with the same port density.
High-density 10-, 40-, and 100-Gigabit Ethernet aggregation and spine configuration	The Cisco Nexus 9500 Series Switches help organizations transition from 1- and 10-Gigabit Ethernet infrastructure to 10-, 40-, and 100-Gigabit Ethernet infrastructures to support the increased bandwidth demands of scale-out, multinode application environments. The compatibility of 100-Gigabit Ethernet QSFP28 modules with 40-Gigabit Ethernet QSFP+ modules enables the migration and coexistence of 40- and 100-Gigabit Ethernet ports in the fabric.
High availability, reliability, and scalability	The Cisco Nexus 9500 Series Switches are designed with redundant supervisors, system controllers, power supplies, and fan trays, which eliminate any single point of failure in the chassis. These switches also support up to 6 fabric modules, which provide redundancy and graceful degradation of switching capacity in the event of fabric module failures. All transceivers are pluggable to support the highest possible Mean Time Between Failure (MTBF) for the switch.
Designed for the future	The Cisco Nexus 9500 Series Switches are designed for future expansion with the capability to support higher speed ports and more bandwidth.
Power efficiency	The Cisco Nexus 9500 Series Switches are the first switch chassis designed without a midplane. The line cards and fabric modules connect directly. This revolutionary design provides optimal front-to-back airflow and helps the switch operate with less power. In addition, all Cisco Nexus 9500 Series switch power supplies are rated at or higher than 80PLUS Platinum for AC inputs and equivalent efficiency for DC inputs. The typical power consumption per 10-Gigabit Ethernet port is less than 3.5 watts (W). The typical power consumption per 40- and 100-Gigabit Ethernet port is less than 14W and 22W respectively.

Deployment scenarios

The Cisco Nexus 9500 Series Switches support various deployment scenarios:

- Spine nodes in a spine-leaf fabric
- Core or aggregation node in an L2/L3 network
- Border gateway in a L2/L3 network

Spine-leaf fabric architecture

The high port-density and ability to support multispeed ports on the same chassis make the Cisco Nexus 9500 Series Switches the ideal choice as a spine in spine-leaf fabric architectures. The Cisco Nexus 9500 Series Switches can function as a spine in either Cisco Application Centric Infrastructure (Cisco ACI) or Cisco NX-OS operating modes (Figure 1).

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

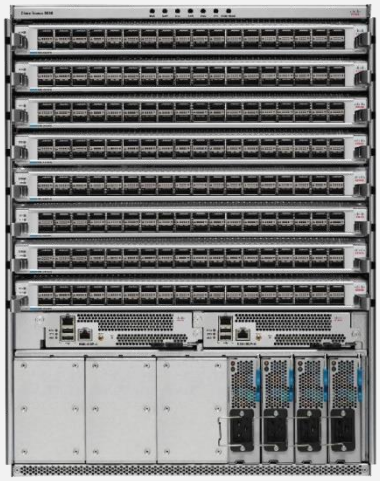
N9K-C9508: 8-Slot Chassis 	• Up to 8 line cards • Up to 8 power supplies • Up to 6 fabric modules of the same type • Up to 2 system controllers • Up to 2 supervisors of the same type • Up to 3 fan trays
N9K-C9516: 16-Slot Chassis 	• Up to 16 line cards • Up to 10 power supplies • Up to 6 fabric modules of the same type • Up to 2 system controllers • Up to 2 supervisors of the same type • Up to 3 fan trays

Table 2. Cisco Nexus 9500 Series Switch chassis specifications

	Cisco Nexus 9504 Chassis	Cisco Nexus 9508 Chassis	Cisco Nexus 9516 Chassis
Number of line card slots	4	8	16
Dimensions	12.25 x 17.50 x 33.15 in. (31.1 x 44.50 x 84.20 cm)	22.70 x 17.50 x 31.76 in. (57.78 x 44.50 x 80.67 cm)	36.70 x 17.50 x 31.76 in. (93.41 x 44.50 x 80.67 cm)
Weight	84 lb (38.2 kg)	150 lb (68.2 kg)	192 lb (87.3 kg)
Mean Time Between Failure (MTBF) Hours	1,038,080	928.910	680,000
Operating temperature	32 to 104°F (0 to 40°C)		
Nonoperating temperature	-40 to 158°F (-40 to 70°C)		
Humidity	5 to 95% (noncondensing)		
Altitude	0 to 13,123 ft (0 to 4,000m)		
Regulatory compliance	Products should comply with CE Markings according to directives 2004/108/EC and 2006/95/EC		

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

DATA SHEET

Brocade ICX 7750 Switch

HIGHLIGHTS

- Provides unprecedented stacking density and performance with up to 12 switches per stack and up to 5.76 Tbps of aggregated stacking bandwidth, limiting inter-switch bottlenecks and supporting large-scale distributed chassis deployments
- Enables single point of management across the campus through a distributed chassis architecture supporting long-distance stacking and new Brocade Campus Fabric technology
- Offers industry-leading 10/40 GbE port density and flexibility in a 1U form factor with up to 32×40 GbE or 96×10 GbE ports per unit, saving valuable rack space and power in wiring closets
- Provides chassis-class high availability with up to 12 full-duplex 40 Gbps stacking ports per switch, hitless stacking failover, and hot-swappable power supplies and fan assemblies
- Delivers superior value by incorporating enterprise-grade advanced features such as BGP, Multi-Chassis Trunking (MCT), and Virtual Routing and Forwarding (VRF)
- Provides OpenFlow support in true hybrid port mode, enabling Software-Defined Networking (SDN) for programmatic control of network data flows

10/40 GbE Distributed Chassis Switch for Campus Aggregation/Core

Today's enterprise network core and aggregation layers are quickly moving to 10 and 40 Gigabit Ethernet (GbE) switching as enterprises rapidly adopt applications such as High-Definition (HD) video, Bring Your Own Device (BYOD), and Virtual Desktop Infrastructure (VDI), which drive the need for resilient, high-bandwidth access networks. To meet these challenges, campus network solutions must provide better performance, port density, reliability, security, Quality of Service (QoS), and Total Cost of Ownership (TCO).

The Brocade® ICX® 7750 Switch delivers industry-leading 10/40 GbE port density, advanced high-availability capabilities, and flexible stacking architecture, making it the most robust Brocade aggregation and core distributed chassis switch offering for enterprise LANs. In addition to rich Layer 3 features, the Brocade ICX 7750 scales to 12-unit distributed-chassis stacking or Multi-Chassis Trunking (MCT) and is an integral part of Brocade Campus Fabric technology.

Today's data centers are also expanding as the demand for data and storage continues to grow exponentially. Moreover, requirements such as application convergence, non-stop operation, scalability, high availability, and power efficiency are placing even greater demands on the network infrastructure.

Part of the Brocade ICX family of Ethernet switches for campus LAN and classic Ethernet data center environments, the Brocade ICX 7750 Switch is a 1U high-performance, high-availability, and market-leading-density 10/40 GbE solution that meets the needs of business-sensitive campus deployments and classic Ethernet data center environments. With industry-leading price/performance and a low-latency, cut-through, non-blocking architecture, the Brocade ICX 7750 provides a cost-effective, robust solution for the most demanding deployments.

Brocade ICX 7750 Specifications

Specifications	
Connector options	• 100[1]/1000 Mbps, 10 Gbps 10GBASE-T ports: RJ-45 • 1 Gbps SFP ports: SX, LX, LHA, BXU, BXD • 10 Gbps SFP+ ports: USR, SR, LR, ER, ZR, direct-attached copper cables • 40 Gbps QSFP+ ports: SR4, LR4, LM4, AOC, direct-attached copper cables • Out-of-band Ethernet management: 10/100/1000 Mbps RJ-45 • Console management: mini-USB serial port (Mini-B plug) • Storage: USB port, standard-A plug For the latest information about supported optics, please visit www.brocade.com/optics.
Maximum MAC addresses	96,000 (switch image), 32,000 (router image)
Maximum VLANs	4,096
Maximum STP (spanning trees)	254
Maximum routes (in hardware)	IPv4 routes: up to 128,000 (shared resource) IPv6 routes: up to 7,000 (shared resource) Hosts: up to 32,000 (shared resource)
Trunking	Maximum ports per trunk: 16 Maximum trunk groups: 256 × 8 or 128 × 16
Maximum jumbo frame size	9,216 bytes
QoS priority queues	8 per port
Layer 2 switching	• 802.1s Multiple Spanning Tree • 802.1x Authentication • Auto MDI/MDIX • BPDU Guard, Root Guard • Dual-Mode VLANs • Dynamic VLAN Assignment • Dynamic Voice VLAN Assignment • Fast Port Span • GARP VLAN Registration Protocol • IGMP Snooping (v1/v2/v3) • IGMP Proxy for Static Groups • IGMP v2/v3 Fast Leave • IGMP Tracking • Inter-Packet Gap (IPG) adjustment • Link Fault Signaling (LFS) • MAC Address Locking; MAC Port Security • MAC-Layer Filtering • MAC Learning Disable • MLD Snooping (v1/v2) • Multi-device Authentication • Per-VLAN Spanning Tree (PVST/PVST+/PVRST) • Mirroring—Port-based, ACL-based, MAC Filter-based, and VLAN-based • Port Loop Detection • Private VLAN • Remote Fault Notification (RFN) • Single-instance Spanning Tree • Single-link LACP • Trunk Groups • Uni-Directional Link Detection (UDLD) • MCT (Brocade Multi-Chassis Trunking)

[1] 100 Mbps will be supported in a future software release.

Brocade ICX 7750 Specifications (Continued)

Base Layer 3 IP routing	• IPv4 and IPv6 static routes • ECMP • Port-based Access Control Lists • L3/L4 ACLs • Host routes	• Virtual Interfaces • Routed Interfaces • Route-only Support • Routing Between Directly Connected Subnets
Premium Layer 3 IP routing (with software license)	• IPv4 and IPv6 dynamic routes • RIP v1/v2, RIPng (IPv6) • OSPF v2, OSPF v3 (IPv6) • PIM-SM, PIM-SSM, PIM-DM, PIM passive (IPv4/IPv6 multicast routing functionality) • PBR • Virtual Route Redundancy Protocol (VRRP)	• VRRP-E, VRRP-E (IPv6) • VRRPv3 (IPv6) • BGP4, BGP4+ (IPv6) • GRE • IPv6 over IPv4 tunnels • VRF (IPv4 and IPv6)
SDN features	• Support for OpenFlow v1.0 and v1.3 • OpenFlow support with true hybrid port mode • Operates seamlessly under the Brocade SDN Controller • Metro-Ring Protocol (MRP) (v1, v2)	• Virtual Switch Redundancy Protocol (VSRP) • VLAN Stacking (Q-in-Q) • VRRP • Topology Groups
Metro features	• Metro-Ring Protocol (MRP) (v1, v2) • Virtual Switch Redundancy Protocol (VSRP) • VLAN Stacking (Q-in-Q) • VRRP • Topology Groups	
Quality of Service (QoS)	• ACL Mapping and Marking of ToS/DSCP • ACL Mapping and Marking of 802.1p • ACL Mapping to Priority Queue • ACL Mapping to ToS/DSCP • Classifying and Limiting Flows Based on TCP Flags • DHCP Relay	• DiffServ Support • Honoring DSCP and 802.1p • MAC Address Mapping to Priority Queue • Priority Queue Management using Weighted Round Robin (WRR), Strict Priority (SP), and a combination of WRR and SP
IEEE standards compliance	• 802.1AB LLDP/LLDP-MED • 802.1D-2004 MAC Bridging • 802.1p Mapping to Priority Queue • 802.1s Multiple Spanning Tree • 802.1w Rapid Spanning Tree (RSTP) • 802.1x Port-based Network Access Control • 802.3ab 1000Base-T • 802.3ad Link Aggregation (Dynamic and Static) • 802.3ae 10 Gigabit Ethernet	• 802.3u 100Base-TX • 802.3x Flow Control • 802.3z 1000Base-SX/LX • 802.3 MAU MIB (RFC 2239) • 802.3ba 40 Gbps Ethernet • 802.3az-2010 EEE • 802.1Q VLAN Tagging
RFC standards compliance	For a complete list of RFCs supported by the Brocade FastIron® software platform, please visit www.brocade.com/fastlronrfc.	

Brocade ICX 7750 Specifications (Continued)

Traffic management	• ACL-based inbound rate limiting and traffic policies • Broadcast, multicast, and unknown unicast rate limiting • Inbound rate limiting per port • Outbound rate limiting per port and per queue
High availability	• Redundant hot-swappable power supplies • Hot-swappable fan trays • L3 VRRP protocol redundancy • Real-time state synchronization across the stack • Hitless failover from master to standby stack controller • Hot insertion and removal of stacked units

Network and Device Management

Management	• Auto Configuration • Configuration Logging • Digital Optical Monitoring • Display Log Messages on Multiple Terminals • Embedded Web Management • Embedded DHCP Server • Industry-standard Command Line Interface (CLI) • Key-based activation of optional software features • Integration with HP OpenView for Sun Solaris, HP-UX, IBM AIX, and Windows • Brocade Network Advisor • MIB Support for MRP, Port Security, MAC Authentication, and MAC-based VLANs • Out-of-band Ethernet Management • ERSPAN support for remote troubleshooting and traffic monitoring • RFC 783 TFTP • RFC 854 TELNET Client and Server • RFC 951 Bootp • RFC 1157 SNMPv1/v2c • RFC 1213 MIB-II	• RFC 1493 Bridge MIB • RFC 1516 Repeater MIB • RFC 1573 SNMP MIB II • RFC 1643 Ethernet Interface MIB • RFC 1724 RIP v1/v2 MIB • RFC 1757 RMON MIB • RFC 2068 Embedded HTTP • RFC 2131 DHCP Server and DHCP Relay • RFC 2570 SNMPv3 Intro to Framework • RFC 2571 Architecture for Describing SNMP Framework • RFC 2572 SNMP Message Processing and Dispatching • RFC 2573 SNMPv3 Applications • RFC 2574 SNMPv3 User-based Security Model • RFC 2575 SNMP View-based Access Control Model SNMP • RFC 2818 Embedded HTTPS • RFC 3176 sFlow • SNTP Simple Network Time Protocol • Multiple Syslog Servers
Security	• 802.1X Accounting • MAC Authentication • DHCP snooping • Dynamic ARP inspection • Bi-level Access Mode (Standard and EXEC Level) • EAP pass-through support • IEEE 802.1X username export in sFlow • Protection against Denial of Service (DoS) attacks • Authentication, Authorization, and Accounting (AAA)	• Advanced Encryption Standard (AES) with SSHv2 • RADIUS/TACACS/TACACS+ • Secure Copy (SCP) • Secure Shell (SSHv2) • Username/Password • Web authentication • Change of Authorization (CoA) RFC 5176 • Flexible authentication

DATA SHEET

Brocade ICX 7250 Switch

HIGHLIGHTS

- Offers enterprise-class stackable switching at an entry-level price, allowing organizations to easily scale as demand grows and new technologies emerge
- Future-proofs campus networks via flexible stacking, software licensing of 1 GbE to 10 GbE ports, Brocade Campus Fabric technology, and OpenFlow support in true hybrid port mode, enabling Software-Defined Networking (SDN) for programmatic network control
- Enables enterprise-class manageability with up to 8×10 GbE ports for stacking or uplinks
- Delivers market-leading stacking scalability with up to 12 switches per stack, 80 Gbps of stacking bandwidth, and long-distance stacking using open standards
- Offers full Power over Ethernet (PoE+) to power wireless access points, video surveillance and video conferencing equipment, VDI terminals, and HD displays directly from the switch
- Includes the Brocade Assurance Limited Lifetime Warranty and three years of technical support

Enterprise-Class Stackable Switch with Future-Proof Expandability

The Brocade® ICX® 7250 Switch delivers the performance, flexibility, and scalability required for enterprise Gigabit Ethernet (GbE) access deployment. It raises the bar with up to 8×10 GbE ports for uplinks or stacking and market-leading stacking density with up to 12 switches (576×1 GbE) per stack. In addition, the Brocade ICX 7250 combines enterprise-class features, manageability, performance, and reliability with the flexibility, cost-effectiveness, and "pay as you grow" scalability of a stackable solution.

Premium Performance in an Entry-Level Switch

The Brocade ICX 7250 Switch provides enterprise-class stackable LAN switching solutions to meet the growing demands of campus networks. Designed for small to medium-size enterprises, branch offices, and distributed campuses, these intelligent, scalable edge switches deliver enterprise-class functionality at an affordable price—without compromising performance and reliability. The Brocade ICX 7250 delivers wire-speed, non-blocking performance across all ports to support latency-sensitive applications, such as real-time voice/video streaming and Virtual Desktop Infrastructure (VDI). The Brocade ICX 7250 is available in 24- and 48-port 10/100/1000 Mbps models with 1 GbE uplink or 10 GbE dual-purpose uplink/stacking ports (see Figure 1)—with or without PoE and PoE+—to support enterprise edge networking, wireless mobility, and IP communications without the need for additional power outlets or power injectors.

The new Brocade Campus Fabric technology maximizes the value of Brocade ICX 7250 Switches. It enables the Brocade ICX 7250 to extend ports in combination with Brocade ICX 7450 and 7750 Switches, creating a complete campus network solution with consolidated management across aggregation and core layers, shared network services—adding advanced Layer 3 capabilities to all switches—and scale-out flexibility to expand port density as needed (see Figure 2). The Brocade ICX 7250 with Campus Fabric technology provides an ideal network access solution for the campus network.

Brocade ICX 7250 Feature/Model Comparison (Continued)

	24 RJ-45 Ports	24 or 48 Ports Non-PoE		24 or 48 PoE+ Ports	
	Brocade ICX 7250-24G	Brocade ICX 7250-24	Brocade ICX 7250-48	Brocade ICX 7250-24P	Brocade ICX 7250-48P
Airflow	Front-to-back	Side-to-back	Side-to-back	Side-to-back	Side-to-back
Switch heat dissipation (25°C)[4] **Idle** (no PoE load) **10% traffic**[3] (full PoE load) **100% traffic**[3] (full PoE load)	114.6 BTU/hour 145.3 BTU/hour 151.4 BTU/hour	145.3 BTU/hour 176.06 BTU/hour 196.5 BTU/ hour	172.7 BTU/hour 216.8 BTU/hour 237.1 BTU/hour	170.6 BTU/hour 214.9 BTU/hour 249.08 BTU/hour	225.2 BTU/hour 286.6 BTU/hour 327.5 BTU/hour
Environment					
Weight (kg)	3.58	3.76	4.84	4.73	5.86
Dimensions	**48 port:** 440 mm (17.323 in.), W×370 mm (14.56 in.), D×43.7 mm (1.720 in.), H — 1U **24 port:** 440 mm (17.323 in.), W×280 mm (11.02 in.), D×43.7 mm (1.720 in.), H — 1U				
Acoustics (25°C)	40 dB	41.9 dB	44.5 dB	44.7 dB	45.9 dB
MTBF (hours) (25°C)	767,718	676,362	665,319	429,209	411,187

[2] 10 Gbps SFP+ ports are required for stacking.

[3] Traffic load on all ports connected with maximum possible PoE/PoE+ loads (if equipped). PoE power delivered to powered devices not included.

[4] PoE power not included in switch heat dissipation figures since the heat is not dissipated at the switch.

Brocade ICX 7250 Specifications

Specifications	
Connector options	• 10/100/1000 ports: RJ-45 • 1 Gbps SFP ports (Brocade ICX 7250-24G only) • 1/10 Gbps SFP+ ports (not available on Brocade ICX 7250-24G) • Out-of-band Ethernet management: 10/100/1000 Mbps RJ-45 • Console management: Mini-USB serial port (Mini-B plug) • File transfer: USB port (Standard-A plug) For the latest information about supported optics, please visit www.brocade.com/optics.
DRAM NVRAM (flash) Packet Buffer Size	2 GB (except for ICX 7250-24G: 1 GB) 2 GB (except for ICX 7250-24G: 1 GB) 24 port: 2 MB, 48 port: 4 MB
Maximum MAC addresses	16,384
Maximum VLANs Maximum PVLANs	4,096 32
Maximum STP (spanning trees)	254
Maximum VEs	255
Maximum routes (in hardware)	12,000 (IPv4) 2,048 (IPv6) 7000 (Next Hop Addresses)
Trunking	Maximum ports per trunk: 16 Maximum trunk groups: 128
Maximum jumbo frame size	9,216 bytes
Average latency	1.5 µs

Brocade ICX 7250 Specifications (Continued)

QoS Priority Queues	8 per port	
Multicast Groups	8,192 (Layer 2) 8,192 (Layer 3)	
Layer 2 switching	• 802.1s Multiple Spanning Tree • 802.1x Authentication • Auto MDI/MDIX • BPDU Guard, Root Guard • Dual-Mode VLANs • MAC-based VLANs, Dynamic MAC-based VLAN activation • Dynamic VLAN Assignment • Dynamic Voice VLAN Assignment • Fast Port Span • GVRP: GARP VLAN Registration Protocol • IGMP Snooping (v1/v2/v3) • IGMP Proxy for Static Groups • IGMP v2/v3 Fast Leave • IGMP Tracking • Inter-Packet Gap (IPG) adjustment • Link Fault Signaling (LFS) • MAC-Address Filtering	• MAC Learning Disable • MLD Snooping (v1/v2) • Multi-device Authentication • Per-VLAN Spanning Tree (PVST/PVST+/PVRST) • Mirroring—Port-based, ACL-based, MAC Filter-based, and VLAN-based • PIM-SM v2 Snooping • Port Loop Detection • Private VLAN • Remote Fault Notification (RFN) • Single-instance Spanning Tree • Single-link LACP • Trunk Groups (static, LACP) • Uni-Directional Link Detection (UDLD) • Metro-Ring Protocol MRP (v1, v2) • Virtual Switch Redundancy Protocol (VSRP) • Topology Groups • VLAN Stacking (Q-in-Q)
Base Layer 3 IP routing	• IPv4 and IPv6 static routes • RIP v1/v2, RIPng • ECMP • Port-based Access Control Lists • Layer 3/Layer 4 ACLs	• Host routes • Virtual interfaces • Routed interfaces • Route-only support • Routing between directly connected subnets
Premium Layer 3 IP routing	• IPv4 and IPv6 dynamic routes • OSPF v2, v3 • PIM-SM, PIM-SSM, PIM-DM, PIM passive (IPv4/IPv6 multicast routing functionality) • PBR	• Virtual Route Redundancy Protocol (VRRP) • VRRP-E (IPv4/IPv6) • VRRP v3 (IPv6) • IPv6 over IPv4 tunnels • VRF (IPv4 and IPv6)
Quality of Service (QoS)	• ACL Mapping and Marking of ToS/DSCP • ACL Mapping and Marking of 802.1p • ACL Mapping to Priority Queue • Classifying and Limiting Flows Based on TCP Flags • DiffServ Support • Honoring DSCP and 802.1p	• MAC Address Mapping to Priority Queue • Priority Queue Management using Weighted Round Robin (WRR), Strict Priority (SP), and a combination of WRR and SP • Priority Flow Control
Traffic management	• ACL-based inbound rate limiting and traffic policies • Broadcast, multicast, and unknown unicast rate limiting	• Inbound rate limiting per port • Outbound rate limiting per port and per queue

Brocade ICX 7250 Specifications (Continued)

Security	• 802.1X Accounting • MAC Authentication • Flexible authentication • Web authentication • DHCP snooping • Dynamic ARP inspection • ND Inspection (Neighbor Discovery) • Bi-level Access Mode (Standard and EXEC Level) • EAP pass-through support • IEEE 802.1X username export in sFlow	• Protection against Denial of Service (DoS) attacks • Authentication, Authorization, and Accounting (AAA) • MAC Address Locking; MAC Port Security • Advanced Encryption Standard (AES) with SSHv2 • RADIUS/TACACS/TACACS+ • Secure Copy (SCP) • Secure Shell (SSHv2) • Username/Password • Change of Authorization (CoA) RFC 5176
SDN features	• Support for OpenFlow v1.0 and v1.3 • OpenFlow support with true hybrid port mode	• Operates seamlessly under the Brocade SDN Controller
IEEE standards compliance	• 802.1AB LLDP/LLDP-MED • 802.1D-2004 MAC Bridging • 802.1p Mapping to Priority Queue • 802.1s Multiple Spanning Tree • 802.1w Rapid Reconfiguration of Spanning Tree (RSTP) • 802.1x Port-based Network Access Control (PNAC) • 802.3 Carrier Sense Multiple Access/Collision Detection (CSMA/CD) • 802.3ab 1000Base-T • 802.3 10Base-T • 802.3ad Link Aggregation (Dynamic and Static) – 802.1 AX-2008 Link Aggregation	• 802.3ae 10 GbE • 802.3af Power over Ethernet • 802.3at Power over Ethernet Plus • 802.3u 100Base-TX • 802.3x Flow Control • 802.3z 1000Base-SX/LX • 802.3 MAU MIB (RFC 2239) • 802.3az-2010 – Energy Efficient Ethernet (EEE) • 802.1Q VLAN Tagging • 802.1BR Bridge Port Extension
RFC standards compliance	For a complete list of RFCs supported by the Brocade ICX 7000 product family, please visit www.brocade.com/icx7rfc.	
Traffic management	• ACL-based inbound rate limiting and traffic policies • Broadcast, multicast, and unknown unicast rate limiting	• Inbound rate limiting per port • Outbound rate limiting per port and per queue
High availability	• Layer 3 VRRP protocol redundancy • Real-time state synchronization across the stack • Hitless failover from master to standby stack controller	• Hot insertion and removal of stacked units • Layer 2 VSRP switch redundancy • In-Service Software Update (ISSU)

DATA SHEET

B-Series B5

Gigabit Ethernet Stackable Edge Switchv

BUSINESS ALIGNMENT

- Aligns network resource utilization with business goals and priorities
- Reliable network operation for mission-critical applications

OPERATIONAL EFFICIENCY

- Management automation capabilities reduce network operational expenses
- Automatic discovery and deployment of VoIP services

SECURITY

- Ability to audit network for adherence to compliance regulations, such as PCI or HIPAA
- Network resources securely allocated according to user roles
- Network security maintained concurrently with user mobility

SUPPORT AND SERVICE

- Industry-leading customer satisfaction and first call resolution rates
- Personalized services, including site surveys, network design, installation, and training
- Comprehensive lifetime warranty, including feature upgrades and more

- Future-proofed with 802.3at high-power PoE support
- Automatic discovery and deployment of VoIP services
- High-availability stacking assures reliable network operations
- Automated management features reduce operational costs
- Investment protection via comprehensive lifetime warranty
- 1.47 Tbps capacity and 809.5 Mpps

Product Overview

The Extreme Networks B5 is a scalable, high-performance Gigabit Ethernet switch that provides support for the bandwidth-intensive and latency-sensitive requirements of today's demanding business applications. The B5 is an excellent choice for environments that require complete multi-layer switching capabilities and support for high density 10/100/1000 Ethernet ports, cost effective10GE uplinks, dual IPv4/IPv6 management, basic routing and policy-based automation capabilities for advanced edge deployments.

The B5 incorporates the new 802.3at high-power PoE on all ports, translating into increased power provisioning for power-hungry devices such as Pan/Tilt/Zoom (PTZ) IP surveillance cameras, IP videophones, third party 802.11n access points and virtual desktops. Built-in high-power PoE support is a cost effective alternative for customers in place of purchasing separate PoE midspans, which can take away valuable rack space, add cost and contribute more cabling to the wiring closet.

The B5 provides high port density in a 1U footprint and is environmentally friendly by design. The B5's overall energy efficiency is further enhanced by a low current draw and an extreme tolerance for high environmental temperatures. A highly-scalable architecture and a comprehensive lifetime warranty ensure that a B5 network investment will sustain a secure, feature-rich and cost-effective network well into the future.

Features / Standards and Protocols

MAC Address Table Size
32,000
VLANs
4,094 VLAN IDs
1,024 VLAN Entries per Stack

Switching Services
IEEE 802.1AB – LLDP
ANSI/TIA-1057 – LLDP-MED
IEEE 802.1D – MAC Bridges
IEEE 802.1s – Multiple Spanning Trees
IEEE 802.1t – 802.1D Maintenance
IEEE 802.1w – Rapid Spanning Tree Reconvergence
IEEE 802.3 – Ethernet
IEEE 802.3ab – GE over Twisted Pair
IEEE 802.3ad – Link Aggregation
IEEE 802.3ae – 10 Gigabit Ethernet (fiber)
IEEE 802.3af – PoE
IEEE 802.3at – High Power PoE (up to 30W per port)
IEEE 802.3i – 10Base-T
IEEE 802.3u – 100Base-T, 100Base-FX
IEEE 802.3z – GE over Fiber
Full/half duplex auto-sense support on all ports
IGMP Snooping v1/v2/v3
Jumbo Frame support (9,216 bytes)
Loop Protection
One-to-One and Many-to-One Port Mirroring
Port Description
Protected Ports
Selectable LAG Configuration (6 x 8, 12 x 4, 24 x 2)
Host CPUProtection – Broadcast/ Multicast/ Unknown Unicast Suppression
Spanning Tree Backup Root
STP Pass-Thru

VLAN Support
Generic Attribute Registration Protocol (GARP)
Generic VLAN Registration Protocol (GVRP)
IEEE 802.1p – Traffic classification
IEEE 802.1q – VLAN Tagging
Protocol-based VLANs with Extreme Networks Policy
IEEE 802.3ac – VLAN Tagging Extensions
Port-based VLAN (private port/private VLAN)
Tagged-based VLAN
VLAN Marking of Mirror Traffic
Standalone VLAN Association application for subnet, protocol and MAC based VLAN classification

Quality of Service
8 Priority Queues per Port
802.3x Flow Control
Class of Service (CoS)
Ingress Rate Limiting
IP ToS/DSCP Marking/Remarking
IP Precedence
IP Protocol
Layer 2/3/4 Classification
Multi-layer Packet Processing
Mixed Queuing Control – Strict and Weighted Round Robin
Source/Destination IP Address
Source/Destination MAC Address
RFC 2474 Definition of Differentiated Services Field

Security
ARP Spoof Protection
DHCP Spoof Protection
Dynamic and Static MAC Locking
EAP Pass Thru
Hybrid Mode
IEEE 802.1X Port Authentication
MAC-based Port Authentication
RADIUS Accounting for network access
RADIUS Client
IPsec for RADIUS transactions
RFC 3580 – IEEE 802.1X RADIUS Usage Guidelines
Multi-user Authentication
Pre-login banner
Password encrypted using a FIPS 1402 approved algorithm
Secure Networks Policy
Secured Shell (SSHv2)
Secured Socket Layer (SSL)
User and IP Phone Authentication
Web-based Port Authentication
Auto Console Disconnect
Security Log
Secure Directory

IPv4 Routing
Standard Access Control List (ACLs)
Extended ACLs
VLAN-based ACLs
Service ACLs
IPv6 ACLs - not simultaneously supported with policy
MAC-based ACLs - not simultaneously supported with policy
ARP & ARP Redirect
IP Helper Address
RFC 826 – Ethernet ARP
RFC 1058 – RIP v1
RFC 1256 – ICMP Router Discovery Messages
RFC 1519 Classless Inter-Domain Routing
RFC 1724 – RIPv2 MIB Extension
RFC 2236 – IGMPv2
RFC 2453 – RIP v2
RFC 3046 – DHCP/BootP Relay
RFC 3376 – IGMPv3
Static Routes

MIB Support
Enterasys Networks Entity MIB
Enterasys Networks Policy MIB
Enterasys Networks VLAN Authorization MIB
Enterasys Networks Spanning Tree Diagnostic MIB
ANSI/TIA-1057 – LLDP-MED MIB
IEEE 802.1AB – LLDP MIB
IEEE 802.1X MIB – Port Access
IEEE 802.3ad MIB – LAG MIB
RFC 826 – ARP and ARP Redirect
RFC 951, RFC 1542 – DHCP/BOOTP Relay
RFC 1213 – MIB/MIB II
RFC 1493 – BRIDGE-MIB
RFC 1643 – Ethernet-like MIB
RFC 2096 – IP Forwarding Table MIB
RFC 2131, RFC 3046 – DHCP Client/Relay
RFC 2571 – SNMP Framework MIB
RFC 2465 – IPv6 MIB
RFC 2466 – ICMPv6 MIB

Features / Standards and Protocols (cont.)

RFC 2613 – SMON MIB
RFC 2618 – RADIUS Authentication Client MIB
RFC 2620 – RADIUS Accounting Client MIB
RFC 2668 – Managed Object Definitions for 802.3 MAUs
RFC 2674 – P-BRIDGE-MIB
RFC 2674 – QBRIDGE-MIB VLAN Bridge MIB
RFC 2737 – Entity MIB (physical branch only)
RFC 2819 – RMON-MIB
RFC 2863 – IfMIB
RFC 2933 – IGMP MIB
RFC 3413 – SNMP v3 Applications MIB
RFC 3414 – SNMP v3 User-based Security Module (USM) MIB
RFC 3415 – View-based Access Control Model for SNMP
RFC 3584 – SNMP Community MIB
RFC 3621 – Power over Ethernet MIB

Management

Alias Port Naming Command Line Interface (CLI)
Configuration Upload/Download
Dual IPv4/IPv6 Management Support
Editable Text-based Configuration File
TFTP Client
Command Logging
Multi-configuration File Support
NMS Automated Security Manager
NMS Console
NMS Inventory Manager
NMS Policy Manager
Node/Alias Table
RFC 768 – UDP
RFC 783 – TFTP
RFC 791 – IP
RFC 792 – ICMP
RFC 793 – TCP
RFC 826 – ARP
RFC 854 – Telnet
RFC 951 – BootP
RFC 1157 – SNMP
RFC 1901 – Community-based SNMPv2
RFC 1981 – Path MTU for IPv6
RFC 2030 – Simple Network Time Protocol (SNTP)
RFC 2460 – IPv6 Protocol Specification
RFC 2461 – IPv6 Neighbor Discovery
RFC 2462 – Stateless Autoconfiguration
RFC 2463 – ICMPv6
RFC 2465 – IPv6 MIB
RFC 2933 – IGMP MIB
RFC 3176 – sFlow
RFC 3413 – SNMP Applications MIB
RFC 3414 – SNMP User-based Security Module (USM) MIB
RFC 3415 – View-based Access Control Model for SNMP
RFC 3587 – IPv6 Global Unicast Address Format
RFC 3826 – Advanced Encryption Standard (AES) for SNMP
RMON (Stats, History, Alarms, Events, Filters, Packet Capture)
RFC 4007 - IPv6 Scoped Address Architecture
RFC 4291 - IPv6 Addressing Architecture
Secure Copy (SCP)
Secure FTP (SFTP)
Simple Network Management Protocol (SNMP) v1/v2c/v3
SSHv2
RFC 3164 – The BSD Syslog Protocol
TACACS+ for Management Authentication, Authorization and Auditing
Web-based Management
Webview via SSL Interface

DATA SHEET

A-Series A4

Stackable L2/L3 Edge Switch

BENEFITS

BUSINESS ALIGNMENT

- Extreme Networks policy capabilities support converged multimedia networks
- Reliable network operation for mission-critical applications

OPERATIONAL EFFICIENCY

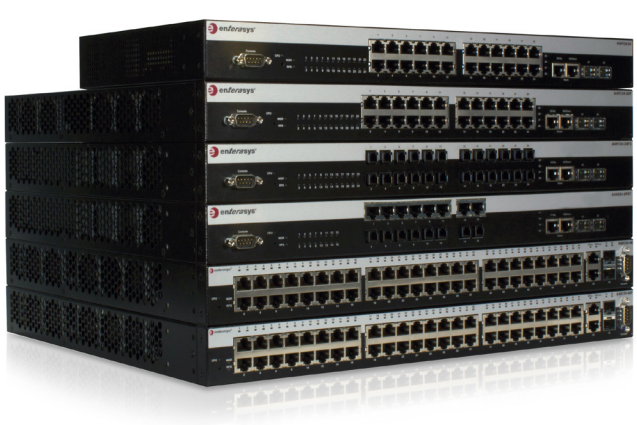
- Scalable architecture supports continued growth of network capacity
- Consolidated management capabilities reduce network operational expenses
- Highly available design ensures reliable network operations

OPERATIONAL EFFICIENCY

- Network access secured by 802.1x, MAC address and web-based authentication methods
- Extreme Networks policy provided enhanced network security that is maintained concurrently with user mobility
- Architecture designed with integral network security

SUPPORT AND SERVICE

- Industry-leading customer satisfaction and first call resolution rates
- Personalized services, including site surveys, network design, installation, and training
- Comprehensive lifetime warranty, including feature upgrades and more
- Release 6.61 adds policy and basic routing with support for two devices (PC and a phone) on a single port



- High-availability design assures reliable network operations
- Now with Extreme Networks policy and basic routing
- PoE supports a variety of network devices
- Investment protection via lifetime warranty
- 140.8 Gbps capacity and 104.8 Mpps

Product Overview

The Extreme Networks A4 is a highly reliable fast Ethernet edge switch that provides scalable, wire-rate performance in support of the bandwidth-intensive and delay-sensitive requirements of today's demanding applications. The A4 also provides multi-layer packet classification and priority queuing for differentiated services. Along with a switch capacity of 17.6 Gbps, the A4 provides up to 48 10/100 Ethernet ports as well as 4 Gigabit Ethernet uplink ports. Leveraging the A4's stacking capability, as many as 8 A4s can be interconnected in a single stack to create a virtual switch that provides 140.8 Gbps of capacity and up to 384 10/100 Ethernet ports as well as 16 Gigabit Ethernet uplink ports.

The A4 includes enterprise-class features in a 10/100 stackable switch that ensure seamless connectivity and application performance. With support for 16,000 MAC addresses, the A4 is an excellent choice for medium to large enterprises that need to support thousands of endpoints. Support for Extreme Networks policy enables strong support for integrated multimedia networks, including Voice over IP (VoIP) and IP video, as well as all types of data-intensive applications. With the 6.61 firmware release, all A4s can now deploy separate policies for both a personal computer and a VoIP phone on a single switch port. In conjunction with its non-blocking L2 switching architecture, the A4's intelligent queuing mechanisms ensure that mission-critical applications receive prioritized access to network resources.

Features / Standards and Protocols

MAC Address Table Size
16,000

VLANs
4,094 VLAN IDs
1,024 VLAN Entries per Stack

Switching Services
ANSI/TIA-1057 – LLDP-MED
IEEE 802.1AB – LLDP
IEEE 802.1D – MAC Bridges
IEEE 802.1s – Multiple Spanning Trees
IEEE 802.1t – 802.1D Maintenance
IEEE 802.1w – Rapid Spanning Tree Reconvergence
IEEE 802.3 – Ethernet
IEEE 802.3ab – GE over Twisted Pair
IEEE 802.3ad – Link Aggregation
IEEE 802.3af – PoE
IEEE 802.3i - 10Base-T
IEEE 802.3u - 100Base-T, 100Base-FX
IEEE 802.3z - GE over Fiber
Full/half duplex auto-sense support on all ports
IGMP Snooping v1/v2/v3
Jumbo Frame support (9,216 bytes)
Loop Protection
One-to-One and Many-to-One Port Mirroring
Port Description
Protected Ports
Selectable LAG Configuration (6 x 8, 12 x 4, 24 x 2)
CoS MIB based Broadcast/ Multicast/ Unknown Unicast Suppression
Spanning Tree Backup Root
STP Pass Thru

Security
ARP Spoof Protection
DHCP Spoof Protection
IEEE 802.1x Port Authentication
MAC-based Port Authentication
Password Protection (encryption)
Web-based Port Authentication
Dual User Authentication (PC + Phone)
Secure Networks Policy
RADIUS Accounting for network access
RADIUS Client
Secured Shell (SSHv2)
Secured Socket Layer (SSL)

IPv4 Routing
Standard Access Control List (ACLs)
Extended ACLs
VLAN-based ACLs
ARP & ARP Redirect
IP Helper Address
RFC 826 – Ethernet ARP
RFC 1058 – RIP v1
RFC 1256 – ICMP Router Discovery Messages
RFC 1519 Classless Inter-Domain Routing
RFC 1724 – RIPv2 MIB Extension
RFC 2236 – IGMPv2
RFC 2453 – RIP v2
RFC 3046 – DHCP/BootP Relay
RFC 3376 – IGMPv3
Static Routes

MIB Support
Enterasys Networks Entity MIB
Enterasys Networks Policy MIB
ANSI/TIA-1057 – LLDP-MED MIB
IEEE 802.1AB – LLDP MIB
Enterasys Networks VLAN Authorization MIB
IEEE 802.1X MIB – Port Access
IEEE 802.3ad MIB – LAG MIB
RFC 826 – ARP and ARP Redirect
RFC 951 – BOOTP
RFC 1213 – MIB/MIB II
RFC 1493 – BRIDGE-MIB
RFC 1542 – DHCP/BOOTP Relay
RFC 1643 – Ethernet-like MIB
RFC 2096 – IP Forwarding Table MIB
RFC 2131, RFC 3046 – DHCP Client/Relay
RFC 2233 – IF-MIB
RFC 2271 – SNMP Framework MIB
RFC 2466 – ICMPv6 MIB
RFC 2571 – SNMP Framework MIB
RFC 2613 – SMON MIB
RFC 2618 – RADIUS Authentication Client MIB
RFC 2620 – RADIUS Accounting Client MIB
RFC 2668 – Managed Object Definitions for 802.3 MAUs
RFC 2674 – P-BRIDGE-MIB
RFC 2674 – QBRIDGE-MIB VLAN Bridge MIB
RFC 2737 – Entity MIB (physical branch only)
RFC 2819 – RMON-MIB
RFC 2863 – IF-MIB
RFC 2933 – IGMP MIB
RFC 3413 – SNMP v3 Applications MIB
RFC 3414 – SNMP v3 User-based Security Module (USM) MIB
RFC 3415 – View-based Access Control Model for SNMP
RFC 3580 – IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
RFC 3584 – SNMP Community MIB
RFC 3621 – Power over Ethernet MIB

VLAN Support
Generic Attribute Registration Protocol (GARP)
Generic VLAN Registration Protocol (GVRP)
IEEE 802.1p – Traffic classification
IEEE 802.1q – VLAN Tagging
IEEE 802.1v – Protocol-based VLANs
IEEE 802.3ac – VLAN Tagging Extensions
Port-based VLAN (private port/private VLAN)
Tagged-based VLAN
VLAN Marking of Mirror Traffic

Management
Alias Port Naming
Command Line Interface (CLI)
Configuration Upload/Download
Dual IPv4/IPv6 Management Support
Editable Text-based Configuration File
FTP/TFTP Client
Multi-configuration File Support
NMS Automated Security Manager
NMS Console
NMS Inventory Manager
NMS Policy Manager
Node/Alias Table
RFC 768 – UDP
RFC 783 – TFTP
RFC 791 – IP
RFC 792 – ICMP
RFC 793 – TCP
RFC 826 – ARP
RFC 854 – Telnet
RFC 951 – BootP
RFC 1157 – SNMP
RFC 1901 – Community-based SNMPv2
RFC 2030 – Simple Network Time Protocol (SNTP)
RFC 2271 – SNMP Framework MIB
RFC 2465 – IPv6 MIB
RFC 2933 – IGMP MIB
RFC 3413 – SNMP Applications MIB
RFC 3414 – SNMP User-based Security Module (USM) MIB
RFC 3415 – View-based Access Control Model for SNMP
RFC 3826 – Advanced Encryption Standard (AES) for SNMP
RMON (Stats, History, Alarms, Events)
Secure Copy (SCP)
Secure FTP (SFTP)
Simple Network Management Protocol (SNMP) v1/v2c/v3
TACACS+ for Management Authentication, Authorization and Auditing
SSHv2
Syslog
Telnet
Text-based Configuration Upload /Downloand
Web-based Management
Webview via SSL Interface

Quality of Service
6 User Addressable Priority Queues per Port
802.3x Flow Control
Ingress Rate Limiting
IP ToS/DSCP Marking/Remarking
IP DSCP – Differentiated Services Code Point
IP Precedence
IP Protocol
Layer 2/3/4 Classification
Multi-layer Packet Processing
Mixed Queuing Control – Strict and Weighted Round Robin
Source/Destination IP Address
Source/Destination MAC Address

IPv6 Management
RFC 1981 - Path MTU for IPv6
RFC 2373 - IPv6 Addressing
RFC 2460 - IPv6 Protocol Specification
RFC 2461 - Neighbor Discovery
RFC 2462 - Stateless Autoconfiguration
RFC 2463 - ICMPv6
RFC 3587 - IPv6 Global Unicast Address Format
RFC 4007 - IPv6 Scoped Address Architecture
RFC 4291 - IP Version 6 Addressing Architecture

DATASHEET

Enterasys® SecureStack™ A2 Switch

Secure Fast Ethernet Stackable L2 Switch

High availability design assures reliable network operations

Granular QoS capabilities support converged multimedia networks

Power over Ethernet (PoE) supports a variety of network devices

Investment protection via Limited Lifetime Warranty

140.8Gbps capacity and 104.8Mpps

Product Overview

Enterasys' leadership position in the switching market is further enhanced by the Enterasys® SecureStack™ A2 stackable enterprise switch. The SecureStack A2 is a high-performance Fast Ethernet edge switch that provides scalable, wire-rate performance in support of the bandwidth-intensive and delay-sensitive requirements of today's demanding applications. With support for 8,000 MAC addresses, the A2 is an excellent choice for environments that require complete multilayer switching capabilities and support for high density (10/100Base-T, 100Base-FX) Ethernet ports. The A2 is well suited for 100Mb networks that may also require Gigabit Ethernet uplink connections. In addition to its complete multilayer switching capabilities, the A2 also provides multilayer packet classification and priority queuing for differentiated services. Along with a switch capacity of 17.6Gbps, the A2 provides up to 48 10/100Base-T or 24 100Base-FX Ethernet ports as well as 2 10/100/1000 Ethernet ports, which can be used as uplink or stacking connections. As many as 8 A2s can be interconnected in a single stack to create a virtual switch that provides 140.8Gbps of capacity and up to 384 10/100Base-T or 192 100Base-FX Ethernet ports as well as 32 10/100/1000 Ethernet ports for uplink or stacking connections.

Robust quality of service (QoS) features enable strong support for integrated multimedia networks, including Voice over IP, video, as well as all types of data-intensive applications. The A2 provides 8 hardware-based priority queues for each Ethernet port to support a suite of differentiated services with as many as 8 distinct priority levels. In conjunction with its non-blocking L2 switching architecture, the A2's intelligent queuing mechanisms ensure that mission-critical applications receive prioritized access to network resources.

The A2 provides a secure network by utilizing its authentication and security features, which can be applied at the port level or at the user level. The A2 supports a single user/device per port, which can be authenticated via IEEE 802.1X or MAC address.

The SecureStack product line provides high port density in a 1u footprint and is environmentally friendly by design. By maximizing port density within a given amount of rack space, the A2 minimizes its cooling requirements. The A2's overall electrical requirement is further reduced by a low current draw and an extreme tolerance for high environmental temperatures. A highly scalable architecture and a Limited Lifetime Warranty ensures that an A2 network investment will sustain a secure, feature rich and cost-effective network well into the future.

Benefits

Business Alignment

- Granular QoS capabilities support converged multimedia networks
- Reliable network operation for mission critical applications

Operational Efficiency

- Scalable architecture supports continued growth of network capacity
- Consolidated management capabilities reduce network operational expenses
- Security capabilities without the high overhead

Security

- Network access secured by 802.1x and MAC address authentication methods
- Network security maintained concurrently with user mobility
- Architecture designed with integral network security

Support and Service

- Industry leading customer satisfaction and first call resolution rates
- Personalized services
- Limited Lifetime Warranty

There is nothing more important than our customers.

Standards and Protocols

MAC Address Table Size
8,000

VLANs
4,096 VLAN IDs
1,024 VLAN entries per stack

Embedded Services
Ingress Rate Limiting
IP TOS Rewrite
Layer 2/3/4 classification
Multilayer Packet Processing

Switching Services
IEEE 802.1D – MAC Bridges
IEEE 802.1s – Multiple Spanning Trees
IEEE 802.1t – 802.1D Maintenance
IEEE 802.1w – Rapid Spanning Tree Reconvergence
IEEE 802.3ab – GE over Twisted Pair
IEEE 802.3ad – Link Aggregation
IEEE 802.3af – PoE
IEEE 802.3i - 10Base-T
IEEE 802.3u - 100Base-T, 100Base-FX
IEEE 802.3z - GE over fiber
Full/half duplex auto-sense support on all ports
IGMP Snooping v1/v2/v3
Jumbo Frame support (9,216 bytes)
Loop Protection
One-to-One and Many-to-One Port Mirroring
Port Description
Protected Ports
Per-Port Broadcast Suppression
Spanning Tree Backup Root
STP Pass Thru

VLAN Support
Generic Attribute Registration Protocol (GARP)
Generic VLAN Registration Protocol (GVRP)
IEEE 802.1p – Traffic Management/ Mapping to 8 queues
IEEE 802.1q – VLAN tagging
IEEE 802.1v – Protocol-based VLANs
IEEE 802.3ac – VLAN tagging extensions
Port-based VLAN (private port / private VLAN)
Tagged-based VLAN
VLAN Marking of Mirror Traffic

Quality of Service
8 priority queues per port
802.3x Flow Control
IP DSCP – Differentiated Services Code Point
IP precedence
IP protocol
Queuing Control – Strict and Weighted Round Robin
Source/Destination IP address
Source/Destination MAC address

Security
IEEE 802.1x Port Authentication
MAC-Based Port Authentication
Password Protection (encryption)
RADIUS Client
Secured Shell (SSHv2)
Secured Socket Layer (SSL)

RFC and MIB Support
Enterasys Entity MIB
Enterasys VLAN Authorization MIB

IEEE 802.1X MIB – Port Access
IEEE 802.3ad MIB – LAG MIB

RFC 826 – ARP and ARP Redirect
RFC 951, RFC 1542 – DHCP/BOOTP relay
RFC 1213 – RFC 1213-MIB/MIB II
RFC 1493 – BRIDGE-MIB
RFC 1643 – Ethernet-like MIB
RFC 2131, RFC 3046 – DHCP client//relay
RFC 2233 – IF-MIB
RFC 2271 – SNMP Framework MIB
RFC 2618 – RADIUS Authentication Client MIB
RFC 2620 – RADIUS Accounting Client MIB
RFC 2668 – Managed Object Definitions for 802.3 MAUs
RFC 2674 – P-BRIDGE-MIB
RFC 2674 – QBRIDGE-MIB VLAN Bridge MIB
RFC 2737 – Entity MIB (physical branch only)
RFC 2819 – RMON-MIB
RFC 2863 – IF-MIB
RFC 2933 – IGMP MIB
RFC 3289 – DiffServ MIB
RFC 3413 – SNMP Applications MIB
RFC 3414 – SNMP User-based Security Module (USM) MIB
RFC 3415 – View-based Access Control Model for SNMP
RFC 3580 – IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
RFC 3584 – SNMP Community MIB
RFC 3621 – Power over Ethernet MIB

Management
Alias Port Naming
Command Line Interface
Configuration Upload/Download
Editable Configuration File
FTP/TFTP client
Multi configuration File Support
NetSight Automated Security Manager
NetSight Console
NetSight Inventory Manager
NetSight Policy Manager
Node/Alias Table
RFC 854 – Telnet
RFC 1157 – SNMP
RFC 1901 – Community-based SNMPv2
RFC 2271 – SNMP Framework MIB
RFC 3413 – SNMPv3 Applications
RFC 3414 – User-based Security Model for SNMPv3
RFC 3415 – View-based Access Control Model for SNMP
RMON (Stats, History, Alarms, Events)
Simple Network Time Protocol (SNTP)
SSH
Syslog
Telnet
Text-based Configuration Upload/Download
Web-based Management
Webview via SSL Interface

GLOSARIO

AAAA

Registro que se utiliza en IPv6 para traducir nombres de hosts a direcciones IPv6.

ARP

Protocolo de Resolución de Direcciones. Es un protocolo de capa 2 (Enlace de Datos), para encontrar la dirección física (MAC).

ARPANET

Red de centros de investigación. Antecesor de Internet.

ASCII

American Standard Code for Information. Código que sirve para codificar combinaciones de caracteres y símbolos.

Backbone

Estructura que soporta una red compuesta principalmente de ruteo y acceso.

BGP-4

Border Gateway Protocol, protocolo de frontera que proporciona las reglas de comunicación entre los diferentes equipos de ruteo.

Bit

Es un digito del sistema de numeración binario.

Broadcast

Transmisión de información donde un nodo fuente envía información a muchos destinos de manera simultánea.

CGNAT

Carrier Grade NAT, NAT a gran escala donde se comparten pocas direcciones IP públicas entre muchos puntos finales.

CIDR

Classless Inter-Domain Routing, El grupo de trabajo de ingeniería de internet lo introdujo en el año 1993 para cambiar la arquitectura de direccionamiento, como medida ante el agotamiento de direcciones IPv4.

CUDI

Corporación Universitaria para el desarrollo de Internet, organismo que maneja la red Internet2 en México.

Datagrama

Conjunto estructurado de bytes que forma la unidad básica de comunicación del protocolo IP.

DHCP

Dynamic Host Configuration Protocol. Es un protocolo de red que permite a los clientes de una red obtener parámetros de configuración automáticamente.

DNS

Domain Name System. Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

Dual-stack

Método de transición de IPv4 a IPv6, donde un equipo puede tener ambos protocolos.

EGP

Exterior Gateway Protocol, es un protocolo estándar usado para intercambiar información de ruteo entre los diferentes equipos.

Enrutamiento

Procedimiento que consiste en conducir un datagrama hacia el destino a través de la red.

Encapsulamiento

Sistema basado en colocar una estructura de datagrama dentro de otra formando un nuevo paquete.

Firewall

Dispositivo que se encarga de filtrar el tráfico de Internet, basado en reglas de comportamiento, se ubica entre la Internet y la Intranet.

FTP

File Transfer Protocol, protocolo de transmisión de archivos por medio de una red.

Gateway

Equipo de distribución encargado de brindar los servicios a los usuarios.

Host

Dispositivo final que se conecta a una red.

HTML

Hiper Text Markup Language, lenguaje que manejan las páginas web actualmente.

HTTP

Protocolo de Transferencia de Hipertexto, para transmitir información en World

Wide Web.

IANA

Internet Assigned Numbers Authority, es la entidad que supervisa la asignación global de direcciones IP.

ICMP

Protocolo encargado de la comunicación de mensajes entre nodos conectados a la red.

IETF

Internet Engineering Task Force, es una organización internacional abierta de normalización, tiene como objetivos contribuir a la ingeniería de Internet, para diferentes áreas como transporte, encaminamiento, seguridad, etc.

IGP

Interior Gateway Protocol. Hace referencia a los protocolos de ruteo en el interior de una red.

Internet2

Red desarrollada por Universidades para brindar servicios de red para educación e investigación sin fines lucrativos.

IP

Internet Protocol. Protocolo de capa de red que facilita la entrega de datagramas sin garantía.

IPsec

Internet Protocol Security. Es un conjunto de protocolos cuya función es asegurar la comunicación sobre IP, autenticando o cifrando cada paquete en un flujo de datos.

IPv4

Abreviatura del Protocolo de Internet para identificar a la versión 4 de este protocolo.

IPv6

Abreviatura de la nueva versión del Protocolo de Internet para especificar que es la versión 6.

ISO

Organización Internacional de Estandarización, Encargada de crear estándares Internacionales.

LACNIC

Latin America & Caribbean Network Information Centre. Es el organismo que se

encarga de la asignación de direcciones IP a México y Latinoamérica.

LAN

Red local. Es una red de dimensiones pequeñas que interconecta equipos con distancias pequeñas.

MAC Address

Dirección única que lleva tarjetas de red grabadas en una ROM para identificar un dispositivo.

MAN

Red de Área Metropolitana. Red con cobertura en un área geográfica extensa.

Multicast

Es el envío de información en una red a múltiples destinos de forma simultánea.

NAT

Traducción de Direcciones de Red, técnica empleada ante el agotamiento de direcciones IPv4.

NIC México

Organización responsable de administrar los recursos de Internet en México.

OSPF

Open Shortest Path First, protocolo de frontera que proporciona el mecanismo de comunicación entre los equipos de distribución.

POP3

Protocolo de Oficina Postal 3. Obtiene mensajes de correo electrónico desde un servidor remoto para clientes locales.

QoS

Quality of Service, son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado.

RFC

Request For Comments. Documento de especificaciones que se muestra al público para discusión.

RIP

Routing Information Protocol, protocolo de frontera que proporciona un método de comunicación entre equipos de ruteo.

RIR

Registros Regionales de Internet. Organizaciones que supervisan la asignación de recursos de Internet en una Región en el Mundo (RIPE NCC, LACNIC, ARIN, APNIC y AfriNIC).

Router

Dispositivo físico que conecta dos o más redes, encargado de distribuir los distintos datagramas hacia su destino.

SMTP

Simple Mail Transfer Protocol. Protocolo que permite la transmisión de correos electrónicos en la red.

SSH

Secure Shell. Protocolo de comunicación segura entre dos sistemas para conexión a un host de forma remota.

Switch

Dispositivo físico que conecta los dispositivos de usuario con la red, se encarga de brindar acceso a los usuarios a la red.

TCP

Transmission Control Protocol. Protocolo de capa 4 que permite una conexión fiable y orientada a conexión junto con el protocolo de internet.

Telnet

Telecommunication Network. Protocolo de red para conexión a otro dispositivo de forma remota para su manejo.

Tunneling

Encapsulado de un paquete IPv6 dentro de un paquete IPv4.

UDP

User Datagram Protocol. Protocolo no fiable y sin conexión basado en IP, que trabaja en la capa 4.

Unicast

Envío de información desde un host fuente a un host destino.

VLAN

Red de área local virtual, es un método que permite crear redes lógicas independientes dentro de una red física.

WAN

Red de gran alcance. Este tipo de red se utiliza para conectar redes pequeñas, formando una red de grandes dimensiones que abraca diferentes áreas.

Wi-Fi

Wireless Fidelity. Redes de área local inalámbrica que cumplen la norma IEEE 802.11.

WWW

World Wide Web. Red informática mundial, para acceder y buscar información en Internet.

6Bone

Proyecto Internacional que sirvió como banco de pruebas para ayudar a la transición a IPv6.

REFERENCIAS

[1] Internet Society, “Adopción de IPv6: Un informe de la política pública de Internet Society (ISOC),” no. June 2015, pp. 1–8, 2016.

[2] G. Zhang, B. Quoitin, and S. Zhou, “Phase changes in the evolution of the IPv4 and IPv6 AS-Level Internet topologies,” *Comput. Commun.*, vol. 34, no. 5, pp. 649–657, 2011.

[3] I. Van Beijnum, “Running IPv6 2006.pdf.”

[4] F. R. and H. R., “6bone (IPv6 Testing Address Aloocation) Phaseout, RFC 3701,” 2006.

[5] B. Fink, “IPv6 Backbone (6bone).” [Online]. Available: https://www6.ietf.org/wg/concluded/6bone.html. [Accessed: 20-Sep-2018].

[6] “Google IPv6 Statistics,” 2018. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption. [Accessed: 16-Oct-2018].

[7] Omar de León, “Despliegue de IPV6 para el desarrollo socio económico en América Latina y el Caribe,” pp. 1–116, 2015.

[8] “IPv6 test.” [Online]. Available: http://ipv6-test.com/stats/. [Accessed: 02-Oct-2018].

[9] “Uruguay en el top 5 de IPv6 mundial,” *Lacnic News*, 2018. [Online]. Available: https://prensa.lacnic.net/news/ipv6/uruguay-en-el-top-5-de-ipv6-mundial. [Accessed: 30-Oct-2018].

[10] R. D. Universitaria, “Trece años de ipv6 en méxico. caso unam ©,” pp. 1–16, 2012.

[11] UNAM, “IPv6 en México Historia,” 2012. [Online]. Available: http://www.ipv6.unam.mx/. [Accessed: 10-Aug-2018].

[12] NIC México, “IPv6 en México,” 2013. [Online]. Available: http://www.cudi.edu.mx/primavera_2013/presentaciones/IPv6-Edmundo.pdf.

[13] LACNIC, “¿Quiénes implementan?,” *IPv6 Portal*, 2018. [Online]. Available: http://portalipv6.lacnic.net/quienes-implementan/.

[14] Cisco Systems, “Campus Resumen de diseño.” Cisco Systems, San José CA, 2013.

[15] M. M. Alani, *Guide to OSI and TCP/IP Models*. 2014.

[16] J. D. Day and H. Zimmermann, “The OSI Reference Model,” *Proc. IEEE*, vol. 71, no. 12, pp. 1334–1340, 1983.

[17] R. L. Miller, “The OSI Model: An Overview,” *SANS Inst. Read. Room site*, 2005.

[18] R. Denenberg, “Open Systems Interconnection,” *Libr. Hi Tech*, vol. 3, no. 1, pp. 15–26, 1985.

[19] L. Adrián and E. Corona, “Protocolos Tcp / Ip De Internet,” 2004.

[20] C. Liberatori, *Redes de Datos y sus Protocolos*. Mar del Plata, Argentina: EUDEM, 2018.

[21] R. Kaur, S. Kumar, and V. K. Patle, “Analysis of Tunneling Transition Mechanism in IPv6,” vol. 5, no. 3, pp. 313–318, 2013.

[22] S. L. Levin and S. Schmidt, “IPv4 to IPv6: Challenges, solutions, and lessons,” *Telecomm. Policy*, vol. 38, no. 11, pp. 1059–1068, 2014.

[23] D. López, N. Y. Gelvez García, and L. F. Pedraza, “Modelo para la integración de redes IPv4-IPv6 basado en Túneles,” vol. 3, pp. 1–8.

[24] G. Goth, “The end of IPv4 is nearly here - Really,” *IEEE Internet Comput.*, vol. 16, no. 2, pp. 7–10, 2012.

[25] D. Xu and T. Roemer, “News Briefs. What Happened to the IPv4 Address Shortage ?,” vol. 27, no. 4, pp. 342–344, 2009.

[26] P. Dell, “Two economic perspectives on the IPv6 transition,” *Info*, vol. 12, no. 4, pp. 3–14, 2010.

[27] D. Wing, “Network address translation: Extending the Internet address space,” *IEEE Internet Comput.*, vol. 14, no. 4, pp. 66–70, 2010.

[28] W. Chimiak, S. Janansky, and B. Chimiak, “LETTERS. IETF and IPv4,” no. MAY, pp. 15–17, 2014.

[29] R. Ando, B. Boguraev, R. Byrd, and M. Neff, “IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663,” *Nat. Lang. Eng.*, vol. 11, no. 1, pp. 67–86, 1999.

[30] L. Zhang, “A retrospective view of network address translation,” *IEEE Netw.*, vol. 22, no. 5, pp. 8–12, 2008.

[31] M. Daoudi, “Architectural Implications of NAT, RFC 2993,” *J. Vis. Lang. Comput.*, vol. 11, no. 3, pp. 287–301, 2000.

[32] LACNIC, “Fases de Agotamiento de IPv4,” 2017. [Online]. Available: http://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4. [Accessed: 16-Sep-2018].

[33] Union Internacional de Telecomunicaciones, “Cuestiones relativas a IPv4 e IPv6,” pp. 14–16, 2013.

[34] Y. Mun and H. Keren Lee, *Understanding IPv6*. Springer, 2005.

[35] B. Stockebrand, *IPv6 in Practice. A Unixer´s Guide to the Next Generation to the Next Generation Internet.* Berlin: Springer, 2007.

[36] Y. Cui, W. Wang, Q. Sun, L. Li, and X. Wang, “IPv4 Address Sharing and Allocation for IPv6 Transition,” *IEEE Internet Comput.*, vol. 19, no. 5, pp. 66–71, 2015.

[37] Google, “State of IPv6 Deployment Table of Contents,” 2017.

[38] S. Racherla and J. Daniel, “IPv6 Introduction and Configuration,” *Ibm*, p. 96, 2013.

[39] I. Forum, “Tutorial de IPv6,” *IPv6 Forum*, pp. 1–46, 2000.

[40] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification, RFC 2460,” pp.

1–39, 1998.

[41] S. Kent, “IP Authentication Header, RFC 4302,” pp. 1–34, 2005.

[42] C. Y. Lin, I. Y. Chen, and S. Y. Kuo, “Extension headers for IPv6 anycast,” *Comput. Commun.*, vol. 29, no. 16, pp. 3013–3019, 2006.

[43] T. Savolainen, J. Soininen, and B. Silverajan, “IPv6 addressing strategies for IoT,” *IEEE Sens. J.*, vol. 13, no. 10, pp. 3511–3519, 2013.

[44] E. Horley, “Pratical IPv6 for Windows Administrators,” *Apress*, 2013.

[45] Oracle Corporation, “Descripción General de las direcciones IPv6,” 2010. [Online]. Available: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/index.html. [Accessed: 10-Sep-2018].

[46] S. Hagen, *IPv6 Essentials*, Second Edi. O’ Reilly, 2006.

[47] M. Dunmore, “6NET: An IPv6 Deployment Guide,” *Management*, vol. 129, p. 2865, 2005.

[48] O. J. Salcedo Parra, C. Hernández, and H. C. Manta C., “Análisis y evaluación del routing information protocol RIP.” Revista Tecnura, 2010.

[49] D. Medhi and K. Ramasamy, *Network Routing. Algorithms, Protocols and Architectures*, Second. Cambridge: Elsevier, 2018.

[50] R. Cilileo, G. Gagliano, *Ipv6 para todos*, vol. 1. 2009.

[51] Y. Cui, Q. Sun, K. Xu, W. Wang, and T. Lemon, “Configuring IPv4 over IPv6 Networks: Transitioning with DHCP,” *IEEE Internet Comput.*, vol. 18, no. 3, pp. 84–88, 2014.

[52] Y. Cui, Y. Chen, J. Liu, Y. L. Lee, J. Wu, and X. Wang, “State management in IPv4 to IPv6 transition,” *IEEE Netw.*, vol. 29, no. 6, pp. 48–53, 2015.

[53] D. Larson, “Energizing the Transition to IPv6,” *Agenda*, no. June, pp. 138–148, 2002.

[54] S. Steffann, “A Comparison of IPv6-over-IPv4 Tunnel Mechanisms, RFC 7059,” *J. Vis. Lang. Comput.*, vol. 11, no. 3, pp. 287–301, 2013.

[55] P. Wu, Y. Cui, J. Wu, J. Liu, and C. Metz, “Transition from IPv4 to IPv6: A state-of-the-art survey,” *IEEE Commun. Surv. Tutorials*, vol. 15, no. 3, pp. 1407–1424, 2013.

[56] Cisco Systems, “ISATAP Tunnel Support for IPv6.” San José CA, pp. 1–8.

[57] Cisco Systems, “IPv6 Automatic 6to4 Tunnels.” San José CA, pp. 1–6.

[58] Microsoft, “Teredo Overview,” 2007. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457011(v=technet.10). [Accessed: 22-Jul-2018].

[59] I. J. C. Network, V. Jain, S. M. Tech, D. Tiwari, S. Singh, and S. Sharma, “Impact of IPv4 , IPv6 and Dual Stack Interface over Wireless Networks,” no. April, pp. 65–71, 2018.

[60] C. Bouras, P. Ganos, and A. Karaliotas, “The deployment of IPv6 in an IPv4 world and transition strategies,” *Internet Res.*, vol. 13, no. 2, pp. 86–93, 2003.

[61] A. C. de A. ISOC-Ar, *IPv6 para Operadores de Red*. 2014.

[62] A. Quintero, F. Sans, and E. Gamess, “Performance Evaluation of IPv4/IPv6 Transition Mechanisms,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 8, no. 2, pp. 1–14, 2016.

[63] W. Aftab, Z. A. Mir, and S. Irfan, “COMPARISON AND TRANSITION STUDY OF INTERNET PROTOCOL VERSION 4 & 6 (IPV4 & IPV6),” vol. 8, no. 7, pp. 2015–2018, 2017.

[64] Dirección de Cómputo y Comunicaciones IPN, “Medios de Transmisión. Red de Microondas,” 2010. [Online]. Available: http://www.virtual.ipn.mx/MediosTransmision/Paginas/Microondas.aspx. [Accessed: 19-Jun-2018].

[65] Cisco Systems, “Cisco Nexus 9500 Series Switches Data Sheet,” 2018. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-729404.html. [Accessed: 05-May-2018].

[66] Brocade Communications Systems, “Brocade ICX 7750 Switch,” 2016. [Online]. Available: www.brocade.com.

[67] Brocade Communications Systems, “Brocade ICX 7250 Switch,” p. 13, 2017.

[68] Extreme Networks Inc, “A-Series A4,” 2014. [Online]. Available: www.extremenetworks.com.

[69] Enterasys Networks Inc, “Enterasys SecureStack A2 Switch,” 2008. [Online]. Available: www.extremenetworks.com.

[70] Enterasys Networks Inc, “B-Series B5,” 2014. [Online]. Available: www.extremenetworks.com.