UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
POSGRADO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN
INSTITUTO DE INVESTIGACIONES EN MATEMÁTICAS APLICADAS Y EN SISTEMAS

ANÁLISIS Y PROPUESTAS DE ADOPCIÓN DE IPv6 EN RED UNAM CASO: INSTITUTO DE CIENCIAS NUCLEARES

TESIS
QUE PARA OPTAR POR EL GRADO DE
MAESTRÍA DE INGENIERÍA Y CIENCIAS DE LA COMPUTACIÓN

PRESENTA:
LETICIA ROJAS NAVA

TUTORES:
DR. LUKAS NELLEN FILLA
M. EN I. JUAN LUCIANO DÍAZ GONZÁLEZ
INSTITUTO DE CIENCIAS NUCLEARES

MIEMBROS DE COMITÉ:

DR. JAVIER GÓMEZ CASTELLANOS , FACULTAD DE INGENIERÍA
DR. LUKAS NELLEN FILA, INSTITUTO DE CIENCIAS NUCLEARES
DR. JOSÉ DAVID FLORES PEÑALOZA, FACULTAD DE CIENCIAS
DR. JOSÉ JAIME CAMACHO ESCOTO, FACULTAD DE INGENIERÍA
M. EN I. JUAN LUCIANO GÓNZALEZ DÍAZ, INSTITUTO DE CIENCIAS NUCLEARES

MÉXICO, D.F. JUNIO 2024

Resumen

El presente trabajo tiene como objetivo ser una referencia para otras instituciones educativas que han decidido iniciar el proceso de adopción de IPv6 en sus redes institucionales.

Para ello, se revisaron arquitecturas que permiten implementar estos mecanismos de transición que junto con buenas prácticas permitirán la integración de servicios IPv4 e IPv6.

Se realizó la comparativa de desempeño y rendimiento entre una solución técnica para un router de frontera desarrollado con software de código abierto versus una solución comercial que dependiendo del número de usuarios que se tengan en la red, puede ser una opción económica que apoye a las instituciones que cuentan con muy bajo presupuesto para incursionar en esta transición.

Agradecimientos:

Dr. Lukas Nellen Filla
Dra. Anaid Antaramian Salas
M.C. Enrique Palacios Boneta
M.C. Luciano Díaz Gonzalez
Ing. Iván Alejandro Aguilar Castillo
Ing. Azael Fernández Alcántara
Ing. Edgar López Ruiz
Ing. Armando Martínez Estrada

No alcanzan las palabras para agradecer, la experiencia y conocimientos que ofrece esta Universidad al contar con profesionales como ustedes, que impulsan y motivan a sus alumnos en el noble trabajo de la docencia.

Un enorme reconocimiento a este grupo de profesores que con paciencia y dedicación durante todos estos años han tenido el compromiso de conformar grupos de trabajo con excelencia a fin de formar líderes en el campo tecnológico.

Mi motivación más grande de seguir estudiando: el pequeño niño que estuvo a mi lado apoyándome durante el desarrollo de este trabajo… te amo Isaac.

Agradezco el apoyo de los proyectos de DGAPA PAPIIT IN110621 y IN114924.

ÍNDICE

Índice de Figuras

Índice de Tablas

Capítulo 1. Introducción

1.1 Planteamiento del problema

La LACNIC (Registro de Direcciones de Internet para América Latina y Caribe) ha anunciado que se encuentra en la fase 3 de agotamiento de IPv4, es decir, se inicia con la recuperación o devoluciones de direcciones y teniendo una reserva para infraestructura crítica, por tanto, está generando una lista de espera para dicha asignación, condicionada a demostrar que ya se tienen asignaciones de IPv6 [67].

Actualmente la adopción de IPv6 ofrece desafíos a las Instituciones para evaluar la renovación tecnológica y para las áreas técnicas no solo por tener que garantizar la compatibilidad con la infraestructura con la que se cuenta y con las aplicaciones, sino por superar la inercia y desconocimiento de los beneficios que ofrece IPv6.

RedUNAM cuenta desde el año 2000 con la asignación del Bloque de IPv6, es importante comenzar a generar tráfico con este protocolo, ya que la creciente demanda de dispositivos conectados a internet genera cada vez más la expansión de direcciones IP, aunado a la necesidad tiene la UNAM de la interconexión con otros países más avanzados que ya trabajan con redes IPv6 y que comparten contenidos pedagógicos y de investigación, esto provoca una brecha tecnológica que se puede superar al contar con la asignación del bloque IPv6.

1.2 Hipótesis

El presente trabajo pretende ofrecer al lector una guía y una referencia para gestionar la inversión y desmitificar la complejidad de la transición para la adopción de IPv6 a través del mecanismo Dual Stack. Adicionalmente se ofrece una solución de router de frontera económica basada en una solución de código abierto.

1.3 Objetivos

El principal objetivo es ofrecer una guía para adoptar IPv6 mostrando las mejores prácticas, con el menor costo para iniciar con este proceso, sin realizar muchas modificaciones al diseño de red actual.

Otro objetivo es desmitificar que el proceso de adopción de IPv6 es costoso y complejo, a través de la creación de manuales técnicos para que otras entidades educativas comiencen con el proceso de adopción.

Finalmente, se demostrará que la solución con código abierto puede ser viable para instituciones que cuenten con bajo presupuesto y el talento en las áreas TIC que puedan replicar esta propuesta.

1.4 Metodología

En el capítulo 10, se desarrolla una metodología para comenzar el proceso de adopción de IPv6 en donde se utilizó el mecanismo de transición Dual Stack en un laboratorio de pruebas. Se configuró un router con Shorewall y se crearon zonas para tener un ambiente de pruebas, que permitió capacitar al técnico, y logró replicar algunos ambientes de redes a fin de tener una matriz de pruebas de conectividad tanto para IPv4 e IPv6.
Las pruebas de rendimiento tienen como objetivo demostrar que el router que se configuró es capaz de soportar las conexiones de los usuarios concurrentes hasta para instituciones grandes, sin demandar muchos recursos en el hardware.

1.5 Importancia

Este trabajo permitirá tener como referencia al Instituto de Ciencias Nucleares el cual es un ejemplo de la coexistencia del protocolo IPv4-IPv6, también permitirá a otras dependencias que no tienen el personal técnico con la experiencia sobre el proceso de adopción de IPv6, poder consultar y tener estas guías.
Considerando que la universidad ya cuenta con la asignación de direccionamiento IPv6 es importante comenzar a utilizar y generar este tráfico para ayudar a crear y/o migrar servicios institucionales sobre este protocolo.
Podrán tenerse los beneficios de adoptar IPv6 en temas de rendimiento, seguridad y eficiencia en la red que todas las áreas TIC, las cuales pueden empezar a generar la mejora del servicio a la comunidad universitaria, dando una ventaja competitiva en el medio educativo y en el campo de la investigación.

Capítulo 2. IPv6

La IETF (Internet Engineering Task Force) crea IPv6 dado el crecimiento exponencial de la Internet. A partir de esta nueva versión se crea el proyecto 6Bone, el cual tuvo como objetivo tener un espacio en la red para pruebas y prácticas experimentales con esta versión, en donde se involucraron 47 países, entre ellos México [1].

LACNIC (Latino America Caribbean Network Information Center) es la entidad encargada de la distribución de los recursos de Internet para la región de Latinoamérica, como son las direcciones IPv4 e IPv6, los números de sistema autónomo (ASN), entre otros recursos. Actualmente ha reportado la fase 3 de la asignación de direccionamiento IPv4. Como se puede observar en la figura 1, se ha incrementado considerablemente la asignación de IP 's en los últimos meses y años, sobre todo en el año 2020 iniciada la pandemia de coronavirus [8].

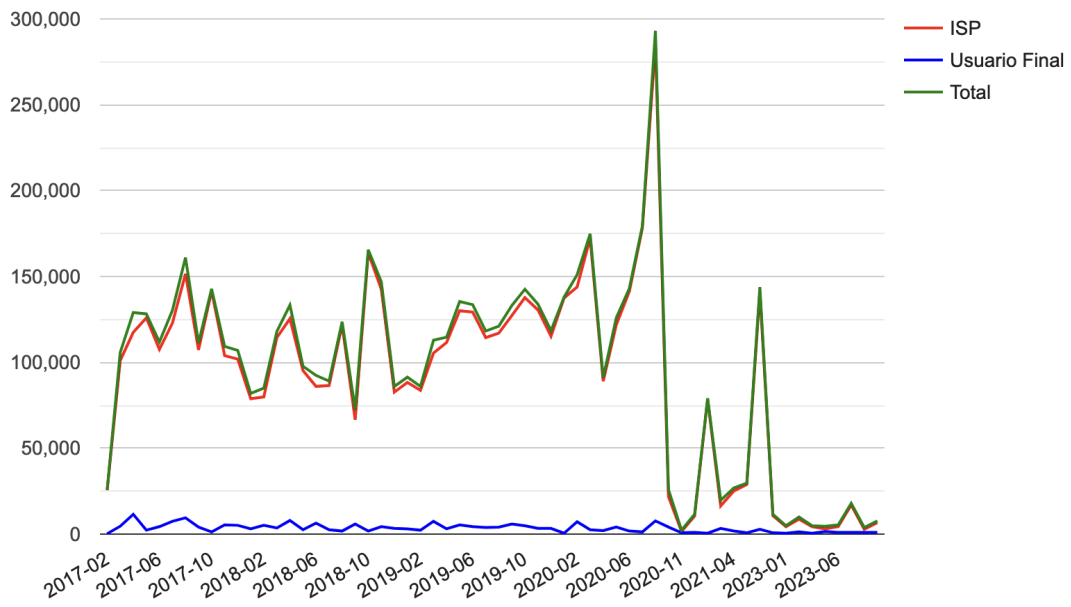


Figura 1.- Asignación de direcciones IPv4 en fase 3 por LACNIC

Fuente: https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4

Por otro lado, surge otra organización “IPv6 Forum” donde líderes ISP y fabricantes de telecomunicaciones se unen para promover y agilizar la adopción hacia el mercado de esta nueva versión, en donde participa México y de allí la UNAM, a través de la DGTIC (Dirección General de Cómputo y de Tecnologías de Información y Comunicación) logra ser el primer nodo en conexión IPv6 para red

de pruebas. Para el año 2000, la UNAM recibe su primer bloque de direcciones tipo TLA[4].

Figura 2.- Red UNAM IPv6

Fuente: http://www.ipv6.unam.mx/

LACNIC proporcionó un segundo bloque de direcciones IPv6 a la UNAM, que vino a sustituir el anteriormente asignado por ARIN, la cual ha comenzado a distribuir o asignar a las entidades y dependencias de la universidad para comenzar a integrar a las diferentes escuelas e institutos. Es por ello, que el Instituto de Ciencias Nucleares (ICN) (ver figura 4), ha comenzado a integrarse a la RedUNAMv6 y se le ha asignado un prefijo para adoptar un mecanismo de transición de IPv4 a IPv6.

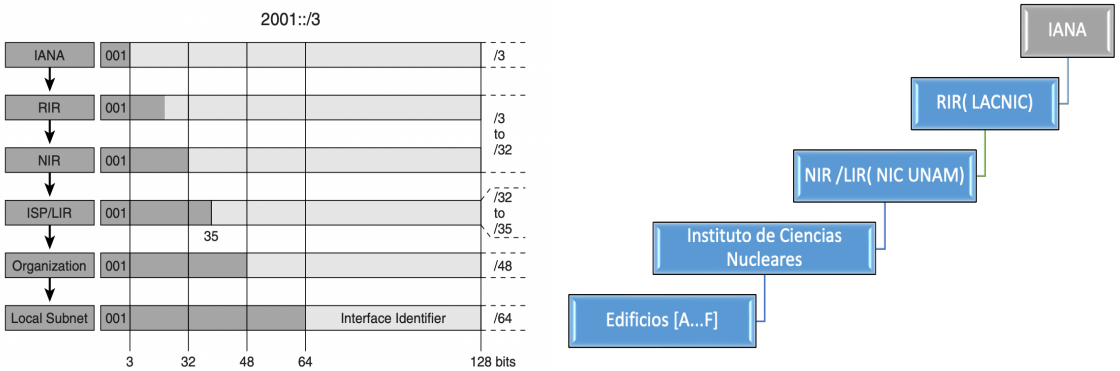


Figura 3.- Asignación de direcciones IANA.

Fuente: http://www.nodis-cisco.com/wp-content/download/Deploying%20IPv6%20Networks.pdf, pág. 65

Figura 4.-Jerarquía de direccionamiento en la UNAM

Fuente: Autor

2.1 IPv6

La cabecera de IP se modifica en la versión 6 y se establecen 40 bytes fijos; estos encabezados de IPv6 son estructuras de datos que permiten obtener información como :

- Versión (4 bits). Su valor es 6.
- Tipo de Servicio -Traffic Class (8 bits).
- Etiqueta del Flujo - Flow Label (20 bits). Marcar paquetes, se utiliza con QoS (Quality of Service).
- Tamaño de la carga -Payload Length (mínimo 16 bits - máximo 6557 bits, sin embargo se puede extender con el uso de jumbogramas).
- Cabecera siguiente - Next header (8 bits) .
    - 41 Header
    - 45 Interdomain Routing Protocol
    - 46 Resource Reservation Protocol
    - 58 IPv6 ICMP Packet
    - 0 Hop-by-Hop Options Header
    - 43 IPv6 Routing Header
    - 44 IPv6 Fragment Header
    - 50 Encapsulating Security Payload
    - 51 IPv6 Authentication Header
    - 59 No Next Header
    - 60 Destination Options Header
    - Tipo de protocolo (ver tabla 3)

- Límite de Saltos - Hop limits (8 bits). Tiempo que puede permanecer un paquete en red, decrementa en 1 cuando ingresa router y se descarta cuando llega a cero.
- Dirección Origen - Source IP address (128 bits) .
- Dirección destino - Destination IP address (128 bits). Unicast, anycast o multicast.

Tabla 1.Comparativa de IPv4 con IPv6[19]

Propiedad	IPv4	IPv6
Tamaño de la dirección	32 bits	128 bits
Tamaño de la red	8-30 bits	64 bits
Tamaño de los paquetes de las cabeceras	20 - 60 bytes	40 bytes

(headers)		
Extensión de cabeceras (headers)	número limitado a pequeñas opciones IP	número ilimitado de cabeceras de extensión de de IPv6
Fragmentación	el emisor o algún router intermedio está permitido fragmentar	solo el emisor puede fragmentar
Protocolos de Control	ARP, ICMP y otros	todos están basados en ICMPv6, NDP y MLD
Descubrimiento de camino MTU	opcional, no muy usado	altamente recomendado
Mínimo MTU permitido	576 bytes	1280 bytes
Path máximo PMTU	9001 bytes (jumbo frames)	4.2GB (datagrams)
Asignación de direcciones	usualmente una dirección por host	usualmente múltiples direcciones por interfaz
Tipo de direcciones	unicast, multicast, anycast y broadcast	unicast, multicast, anycast
Configuración de direcciones	configuración manual o por protocolos como DHCPv4	Configuración manual y automática utilizando SLAAC y/o DHCPv6

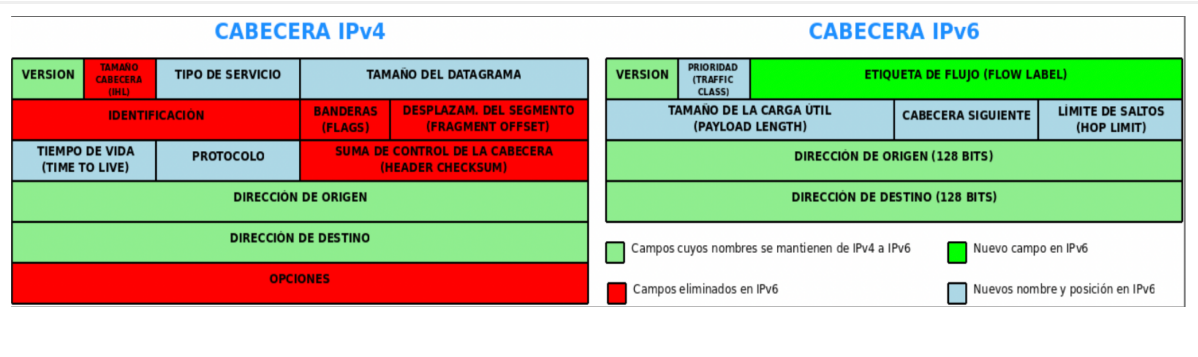


Figura 5. Comparativa de cabeceras IPv4 vs IPv6

Fuente: https://www.profesionalreview.com/2020/02/29/ipv4-vs-ipv6/

2.2 Cabeceras de Extensión IPv6.

Estas cabeceras se utilizan para mejorar los servicios y las funciones de IPv6 como son:

Tabla 2.- Cabeceras de Extensión IPv6[37]

Cabecera de Extensión	Tipo	Observación
Hop to Hop Options	NH=0	Usado para opciones que aplican routers intermedios
Capa superior TCP/ UDP	NH= 6/17	TCP=6 UDP=17 ICMPv6=58
Routing	NH=43	
Fragmentación	NH=44	Usado para enviar Path Maximum Transmission Unit (PMTU).
Autenticación (AH)	NH=51	Usado para opciones de integridad de IPSec
Encapsulating Security Payload (ESP)	NH=50	Usado para opciones de integridad y confidencialidad de IPSec.
Destination options header	NH=60	Usado para opciones que se aplican solo al destinatario.
movilidad (MIPv6)	NH=135	Utilizado para administrar enlaces móviles de IPv6

El campo “next header” (NH) permite introducir estas extensiones a través de un identificador hacia la siguiente extensión hasta llegar a los datos.

Tabla 3.- Tipo de Protocolos [27]

Protocolo	Tipo	Observaciones
TCP	NH=6	Transmission Control Protocol
UDP	NH=17	User Datagram Protocol
IPv6-in-IPv6	NH=41	Protocolo para Túneles de IPv6
GRE	NH=47	Protocolo para túneles de encapsulación de enrutamiento genérico.
ICMPv6	NH=58	Internet Control Message Protocol para IPv6
No next Header	NH=59	Paquetes generalmente usados en ESP

OSPF	NH=89	Open Shortest Path First version 3
PIM	NH=103	Protocol Independent Multicast routing
SCTP	NH=132	Stream Control Transmission Protocol

Orden de los encabezados en IPv6

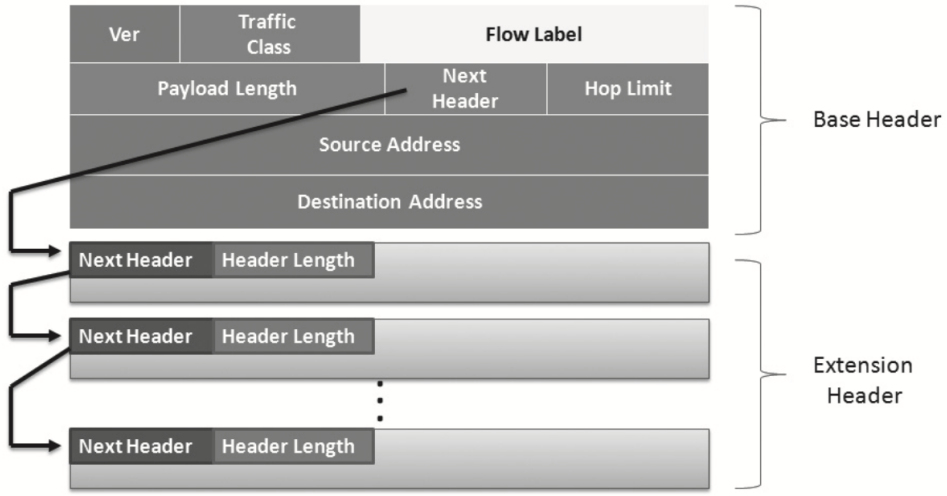


Figura 6. Orden de las Cabeceras IPv6, pág. 23

Fuente:https://scte-cms-resource-storage.s3.amazonaws.com/SCTE_IPv6DeploymentBestPractices-Fundamentals_OperationalPractice.pdf

2.3 Dirección en IPv6

Para el direccionamiento IP, existen varios documentos de buenas prácticas y solo un par de RFCs informativos que nos permiten definir el cambio y/o integración de IPv4 con IPv6.

- En IPv6 no existe tráfico ni direcciones de broadcast.
- Los encabezados tienen un tamaño fijo.
- No hay información redundante.
- *Unicast*: Identifica una interfaz en un solo nodo. Un paquete “unicast” es enviado para esa interfaz de red.
- *Multicast*: Es un identificador para un grupo de interfaces; un paquete con esta dirección es enviado a todas las interfaces del grupo. Otra funcionalidad en IPv6 es el descubrimientos de vecinos “*neighbor discovery*” (ND) y “*router discovery*” (RD). Permite una comunicación de uno a muchos y de muchos a muchos, estas direcciones solo son válidas como destinos.
- *Anycast*: Puede identificar algunas interfaces de red o uno o muchos nodos.
- Loopback: Se requiere y es asignada a una sola interfaz de red en un nodo.
- Link-Local Addresses (LLA): Se requiere en todas las interfaces en un enlace, es un segmento de red separado por routers, similar a el broadcast de dominio en IPv4.

- *Unique local anycast (ULA)*: Está destinada a un direccionamiento interno. Potencialmente ruteable entre subredes, no ruteable globalmente.
- Global: Aplica para el acceso a Internet; Son direcciones únicas ruteables para acceso a redes públicas.

Tabla 4.- Diferentes tipos de direcciones IPv6 [57]

Tipo de Dirección	Notación IPv6	Uso
Loopback	::1/128	Dirección Loopback de cada interfaz de red
Dirección IPv4 embebida	::FFFF/96	Prefijo para tener una dirección IPv4 en una dirección IPv6
Global unicast	2000::/3	Global unicast y anycast (asignada)
Global unicast	4000::/3 - FC00::/9	Global unicast y anycast (sin asignar)
Teredo	2001:0000::/ 32	Tunneling IPv6 sobre UDP sobre NAT
No ruteable	2001:DB8::/32	No ruteable. Para documentación
6to4	2002::/16	Mecanismo de transición 6to4
Link-local unicast	FE80::/10	Link local Unicast, no enrutable y no se reenvía el paquete fuera del enlace local. Unicast de enlace local
Local IPv6 address	FC00::/7	Espacio para dirección Unicast y anycast. Dirección local única
Multicast	FF00::/8	Dirección multicast
Global	2001::/16	
Site-local	FEC0::/10	reservada por IETF
No especificada	::/128	
Pruebas, experimental	3FFE::/16	Usada en 6Bone
	0:0:0:0:0:0::/96	(Reservada por IETF)

Capítulo 3. Protocolos auxiliares de IPv6

En el siguiente apartado se describirán brevemente algunos protocolos auxiliares como el ICMPv6 y el NDP que nos permitirán detectar y resolver direcciones IPv6.

3.1 Internet Control Message Protocol (ICMPv6)

RFC 2463. Es parte integral de la arquitectura de IPv6 y debe ser soportada por todas las arquitecturas de IPv6. Su principal propósito es transmitir la información de la conectividad sobre la red IP. Viaja directamente a través del datagrama IP, así como UDP.

El protocolo habilita el reporte de los mensajes de errores y funciones de control. Cuando el campo de “Next Header” tiene el valor de 58, se refiere a un dato de ICMPv6. El tipo de campo de los mensajes del 1 al 127 en este protocolo son reservados para errores, mientras que el tipo 128 es para control y generación de reportes.
Los errores que describe el protocolo son cuatro: Paquete muy grande, tiempo excedido, problema de parámetro y destino no alcanzable. En la tabla 5 se presentan algunos mensajes considerados en ICMPv6.

Tabla 5. Mensajes de ICMPv6[9]

Mensaje	Tipo	Descripción
Destino no alcanzado	1	Algunos paquetes son borrados en la trayectoria hacia el destino, por problemas de congestión o pérdida de conectividad.
Paquete muy grande	2	Se presenta en el proceso de fragmentación de paquetes que se realiza en el router. En el primer salto se define el PMTU para determinar si se requiere fragmentar.
Tiempo excedido	3	Podría presentarse un bucle en la red por una configuración en el router, si el paquete llega a cero en el campo de “hop limit”, se envía este mensaje.
problema con un parámetro	4	Proporciona mensajes para detectar

		problemas genéricos en el router.
Requerimiento Echo	128	Diagnóstico para la conectividad vía comando ping.
Repetición Echo	129	Diagnóstico para la conectividad vía comando ping.
Multicast Listener Query (MLQ)	130	Transmitir los mensajes para los miembros del grupo multicast o link-local.
Multicast Listener Report (MLR)	131	Reportes de los mensajes para los miembros del grupo multicast o link-local.
Multicast Listener Done (MLD)	132	Confirmación de mensajes para los miembros del grupo multicast o link-local.
Router Solicitation (RS)	133	Utilizado por los nodos cuando quieren configurar su IPv6 para solicitar un RA al router (prefijos de enlace).
Router Advertisement (RA)	134	Respuesta a un RS. Anuncia la presencia de prefijos para el enlace.
Neighbor Solicitation (NS)	135	Determina la capa de enlace de un vecino. Búsqueda en capa 2 de algún nodo. DAD (Duplicate Address Detection).
Neighbor Advertisement (NA)	136	Respuesta a un NS. cambio de dirección en la capa de enlace.
Redirect Message	137	Informa a los nodos que hay un mejor primer salto para el destino.
Router Renumbering (RR)	138	Se envían comandos RR a todos los routers multicast, link-local y anycast.
ICMP Node Information Query (NIQuery)	139	Mensaje de reenvío y reversa de nombre independiente del DNS.
ICMP Node Information Response (NIReplay)	140	Respuesta al mensaje de reenvío y reversa de nombre independiente del DNS.
Inverse Neighbor Discovery Solicitation Message (INDS)	141	Por cada solicitud IND se genera un respuesta y un anuncio sobre el enlace para el origen y el objetivo.
Inverse Neighbor Discovery Advertisement (INDA)	142	Permite a un nodo determinar y anunciar una dirección IPv6 en la capa de enlace.
Version 2 Multicast Listener Report	143	
Home Agent Address Discovery Request Message	144	Mensaje “anycast” usado por un nodo móvil para solicitar un prefijo al dueño de

		la red doméstica.
Home Agent Address Discovery Replay Message	145	Mensaje usado por un nodo móvil como respuesta de una solicitud de un prefijo al dueño de la red doméstica.
Mobile prefix solicitation	146	Mensaje para solicitar el prefijo de la red móvil.
Mobile prefix Advertisement	147	Mensaje para anunciar el prefijo de la red móvil.

Dado que IPv6 permite tener más de una dirección IP asignada a una interfaz de red con diferente alcance, existen dos algoritmos para definir el alcance de la conectividad: algoritmos SAS (Source Address Selection) y DAS (Destination Address Selection) que se usan antes de generar algún error de conexión.

3.2 Neighbor Discovery Protocol (NDP)

RFC: 4861. Proporciona funcionalidades para el router y el "host" cuando se conectan al mismo enlace. Algunas funcionalidades como la resolución de direcciones, redireccionamiento, descubrimiento de prefijos y detección de vecinos.

La búsqueda de vecinos es una función usada por los nodos para descubrir routers cercanos, direcciones, prefijos y otros parámetros de configuración. Se compone de cabeceras IPv6, cabeceras de ICMPv6, cabeceras y opciones propias del protocolo.NDP equivale a utilizar los protocolos ARP e ICMP para IPv4, ya que no se tiene forma alguna de detectar nuevos componentes en la red con IPv4.

El protocolo ND construye el conocimiento necesario para tomar decisiones con respecto al envío de los paquetes IPv6 hacia su vecino. Este conocimiento se construye a través de anuncios (solicitados o no) recibidos desde el router y los nodos.

Tabla 6 Características ND[19]

Tipo de Mensaje	Descripción
Router Discovery	Se habilitan los servidores para localizar a los routers con la conexión de los enlaces.
Prefix Discovery	Se habilitan los servidores para aprender prefijos usados en la conexión de los enlaces.
Parameter Discovery	Habilita los nodos para aprender los parámetros como el PMTU o el "hop limit"

Address Autoconfiguration	Habilita el hosts para configurar automáticamente una dirección
Address Resolution	Habilita a los servidores para determinar la dirección del enlace hacia los destinos.
Next-hop determination	Habilita los nodos para determinar el “next hop” para obtener un destino.
Neighbor unreachability detection	Habilita los nodos para detectar que un “neighbor” no es alcanzable.
Duplicate Address Detection	Permite a los nodos determinar si alguna dirección está en uso.
Redirect	Permite a los routers informar a los servidores un mejor “next hop” en el enlace para un particular destino.
Default router y selección específica de routers	Habilita a los routers para informar las rutas específicas a los servidores
Proxying Nodes	Acepta paquetes a nombre de otros nodos

Existen varios niveles de comunicación entre los diferentes componentes de red, para ello se tienen dos algoritmos que dependiendo qué dispositivos participan en la comunicación, es la tarea que pueden realizar. En la tabla 7, se describe qué funciones se cubren utilizando estos dos algoritmos.

Tabla 7.- Roles y Funciones en Protocolo ND[19]

Algoritmo	Comunicación entre servidor - servidor	Comunicación entre servidor y router	Comunicación entre nodo - nodo
Selección de Router por defecto	detección de “neighbor” indetectable	Descubrimiento del router	Resolución de dirección IPv6
		Selección del router por defecto	
Determinación del campo “next-hop”	Detección de Duplicidad de Dirección IPv6 (DAD)	Descubrimiento de prefijo	Redireccionamiento
		Descubrimiento de parámetros	
		Especificaciones del router	

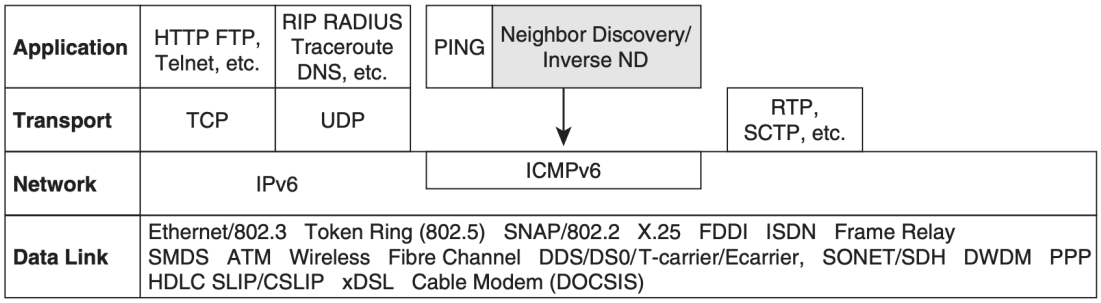


Figura 7.- Pila de Protocolo IPv6 y la ubicación de Neighbor Discovery Protocol

Fuente: Pág. 72 http://www.nodis-cisco.com/wp-content/download/Deploying%20IPv6%20Networks.pdf

Capítulo 4. Mecanismos de Autoconfiguración

En este capítulo se revisarán los mecanismos de autoconfiguración que se tiene para IPv6 que se tienen como los es SLAAC y DHCPv6 a fin de poder distribuir el direccionamiento IP de forma automática.

4.1 Stateless Address Autoconfiguration (SLAAC)

RFC4862: Es un mecanismo que permite la autoconfiguración de los componentes que se conectan a la red con IPv6. El proceso incluye la generación de la dirección local en la capa de enlace, la generación de la dirección global y el procedimiento para la detección de duplicidad de direcciones (DAD) para verificar la unicidad de una dirección IP dentro de un enlace.

Este método permite al dispositivo tener una dirección IPv6 sin tener un servicio DHCPv6, esto lo hace a través del protocolo ICMPv6 con mensajes de solicitud de router (RS) y con mensajes de anuncio de router (RA, indicador M=0 y el indicador O=0). Dado que es un servicio sin estado, no hay ningún servidor que mantenga la información de la dirección de red, es decir, cuales están en uso y cuales están disponibles.

Hay varias formas de generar un identificador de interfaz (IID) única de 64 bit, dos de ellas son:

- Proceso EUI-64.
- Generación aleatoria.

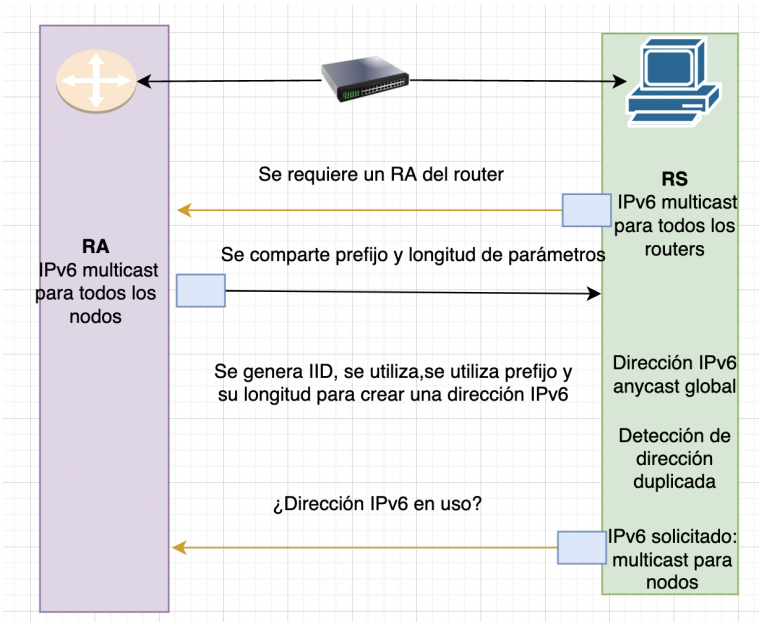


Figura 8.- SLAAC / DAD

Fuente: Autor

4.2 DAD (Duplicate Address Detection)

Se utiliza para verificar que una dirección IPv6 local es única sobre una red antes de ser asignada a un puerto de red. Es por ello, que antes de empezar a generar su IID se utiliza DAD (Detección de Direcciones Duplicadas).

4.3 DHCPv6

RFC 3315. Es el protocolo de red que proporciona de forma dinámica una dirección IP, existen dos tipos: sin estado(stateless) y con estado (stateful). La combinación de DHCPv6 con SLAAC existe para distribuir una red con todos los nodos con IPv6 o con una red “dual stack” con una combinación de IPv4 e IPv6.

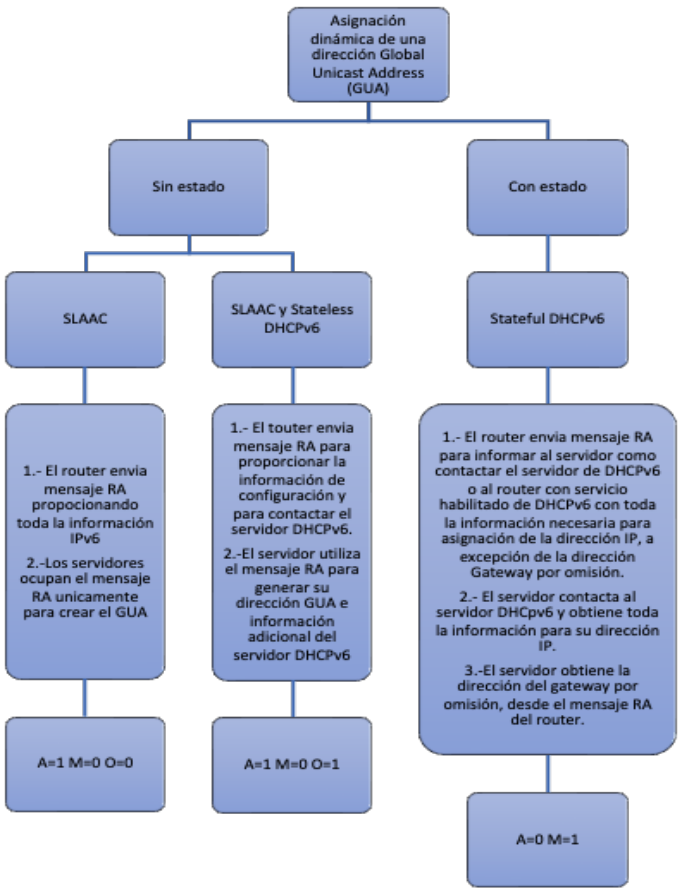


Figura 9.- DHCPv6

Fuente: Autor

Existen estrictas diferencias entre DHCPv4 (se utiliza MAC address) y DHCPv6 (se asigna IID) :

- El uso de DNS, son protocolos y servicios separados.
- El uso de SLAAC, ya que las direcciones IPv6 pueden ser configuradas sin el uso de un DHCPv6.
- DHCPv6 genera menor tráfico que DHCPv4, por el uso de broadcast en IPv4 y el uso de multicast en IPv6.
- En IPv6 existe la habilidad de asignar múltiples direcciones en una sola interfaz de red.

Tabla 8.- Comparación de mensajes entre DHCPv4 y DHCPv6 [34]

DHCPv4	DHCPv6
DISCOVER	SOLICIT
OFFER	ADVERTISE
REQUEST	REQUEST / RENEW
ACK	REPLY

Capítulo 5. Mecanismos de Transición

Existen tres técnicas para la transición de IPv4 a IPv6: Dual stack, Tunneling y traductores IPv4/IPv6; cada técnica presenta diferentes requisitos y condiciones, así como ventajas y desventajas. En la siguiente tabla se puede apreciar algunas características de cada uno así como su clasificación.

Tabla 9.- Comparativa de mecanismos de transición IPv6[7]

	Comparativa de mecanismos de Transición IPv6						
Técnica	**6RD**	**DS-Lite**	**Lw4o6**	**NAT64**	**464XLAT**	**MAP-E**	**MAP-T**
Clasificación	Tunnel (6in4)	Tunnel (4in6)	Tunnel (4in6)	Traductor	Tunnel	Traductor (4in6)	Traductor
Multicast IPv4	SI	No	No	No	No	No	No
Red de Acceso	IPv4	IPv6	IPv6	IPv6	IPv6	IPv6	IPv6
OverHead (bytes)	20	40	40	20	20	40	20
Escalabilidad	Alta	media	Alta	Alta	Alta	Alta	Alta
Soporte en Celular	No	No	No	Si	Si	No	No
Facilidad de HA	Alta	Baja	Alta	media	media	Alta	Alta
Soporte TCP/UDP/ICMP	SI	SI	SI	No	No	No	No
Mesh IPv4	Si	No	No	No	No	si	Si
Mesh IPv6	Si	Si	Si	Si	Si	Si	Si
Traduccion ISP (Estado)	-	-	-	CON	CON	SIN	SIN
Traduccion 46/64	-	-	-	ISP	ISP y/o CPE	-	ISP + CPE

5.1 Dual Stack

Este método de transición[7] permite tener IPv4 e IPv6 simultáneamente en la red, tanto aplicaciones como equipos tengan ambas pilas de comunicación activas ya sea por la misma interfaz de red o separadas. Las conexiones se harán sobre IPv4 o sobre IPv6 pero no de IPv4 a IPv6 o viceversa. Sus direcciones IP se mantienen separadas.

Tabla 10.- Tipo de direccionamiento soportado por Dual Stack[23]

Tipo de Direccionamiento soportado por Dual Stack	
IPv4	Link Local IPv4, PPoE, DHCPv4
IPv6	Link Local IPv6 fe80::/10, ULA, GUA, PoE, PPoE, SLAAC, Prefix+EUI-64, DHCPv6/DHCPv6-PD, DNSv6 y Privacy

Ventajas

- Es simple.
- Permite seguir usando IPv4.
- Coexistencia indefinida de IPv4 e IPv6.
- Los equipos pueden resolver con DNSv4 o DNSv6.

Desventajas

- Implica tener doble direccionamiento IP, no resuelve la escasez de direcciones sobre IPv4.
- No es óptimo para redes móviles de telefonía celular.
- No es óptimo para redes IoT.
- Se requiere la doble gestión para la operación y mantenimiento de la red.
- Es necesario tener sistema de protección para ambos direccionamientos de red.
- Aumenta la complejidad por el manejo y administración de dos redes.

5.2 SIIT-DC [8]

(Stateless IP/ICMP Translation for IPv6 Data Centers Environments)

Este mecanismo define un modelo de aprovisionamiento de red para sistemas que soportan únicamente IPv4 para que puedan conectarse hacia y desde redes con IPv6, es decir comunicaciones “single stack”. Está basado en el RFC 7755 y 7756.

Introduce un nuevo componente: SIIT-DC Border Relay (BR), es sin estado (stateless), el cual traduce IPv4 a IPv6 y viceversa usando un algoritmo de traslación (RFC 6052) y tablas de mapeo.

El SIIT-DC BR no mantiene ningún estado asociado con conexiones individuales, dispositivos o flujos. Opera muy similar al router, permite tráfico IPV4 para y hacia una interfaz IPv6, soporta arquitecturas de alta disponibilidad y ruteo asimétrico usando ECMP (Equal-cost multi-path routing).

En la traducción en SIIT-DC de IPv4 e IPv6, el BR traduce las dos direcciones origen y destino en un paquete con el algoritmo Explicit Address Mapping (EAM). Este algoritmo se basa en el uso de prefijos de IPv6 para mapear bloques de direcciones IPv4. La traducción realizada por el BR no modifica el TTL del paquete, solo modifica los encabezados de IPv4 e IPv6. Se puede combinar SIIT-DC con DNS64 para que las aplicaciones IPv6 inicien con servidores IPv4.

Ventajas

- Single Stack solo IPv6 permite construir escenarios futuros.
- Solución eficiente ante la falta de direcciones públicas IPv4.
- Evita la complejidad y la ineficiencia del despliegue de Dual Stack.

Desventajas

- Ciertos problemas con las fragmentación en IPv4 y uso limitado de la fragmentación en IPv6.
- Algunos protocolos como FTP o SIP presentan problemas con el uso de NAT64.

5.3 Tunneling [9]

Este mecanismo habilita la comunicación entre redes incompatibles para ser puenteadas pueden ser punto a punto, de forma secuencial o punto a multipunto. Existen tres mecanismos para esta técnica de transición:

- IPv6 *Tunnel Broke*r.- Proporciona un servicio de configuración automática para IPv6 sobre túneles de IPv4 para conectar usuarios a Internet con IPv4. La conectividad del usuario y el ISP es requerida en IPv4. Sin embargo presenta potenciales implicaciones de seguridad.

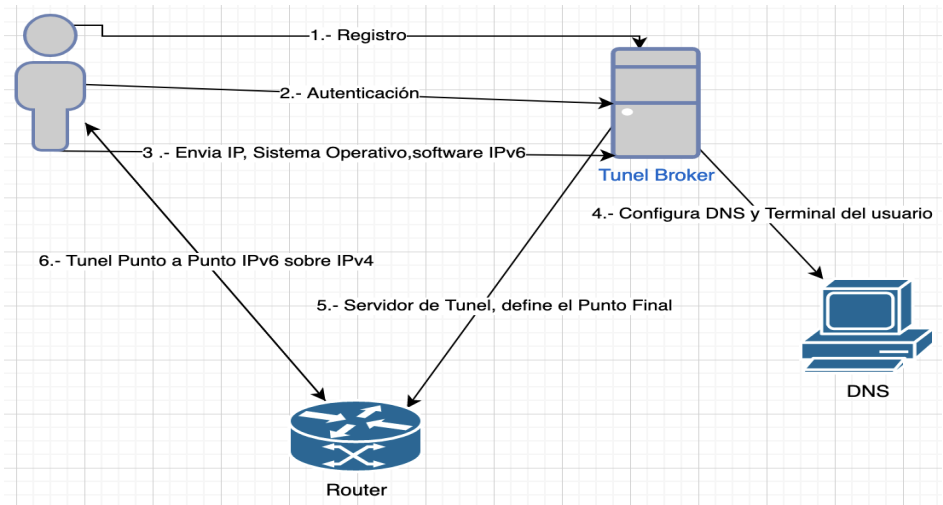


Figura 10.- IPv6 Tunnel Broker

Fuente: Autor

- *Tunnel Configure (Testbed*).- Depende de la configuración manual de ambos extremos de la comunicación, uno como cliente y otro como proveedor del túnel remoto. Una vez establecido el túnel, el proveedor establecerá la información de ruteo relevante para la red del cliente. Al final el cliente puede admitir una pila de IPv6 mientras que el router de frontera maneja el túnel y el encapsulado y desencapsulado de los paquetes IPv6 sobre la red de IPv4 (se requieren interfaces *Dual Stack*) en la puerta de enlace (*gateway*).

Se necesitan enlaces seguros y estableces para una buena comunicación, pero es indispensable un router que soporte "*dual stack*" y un proveedor de red IPv4.

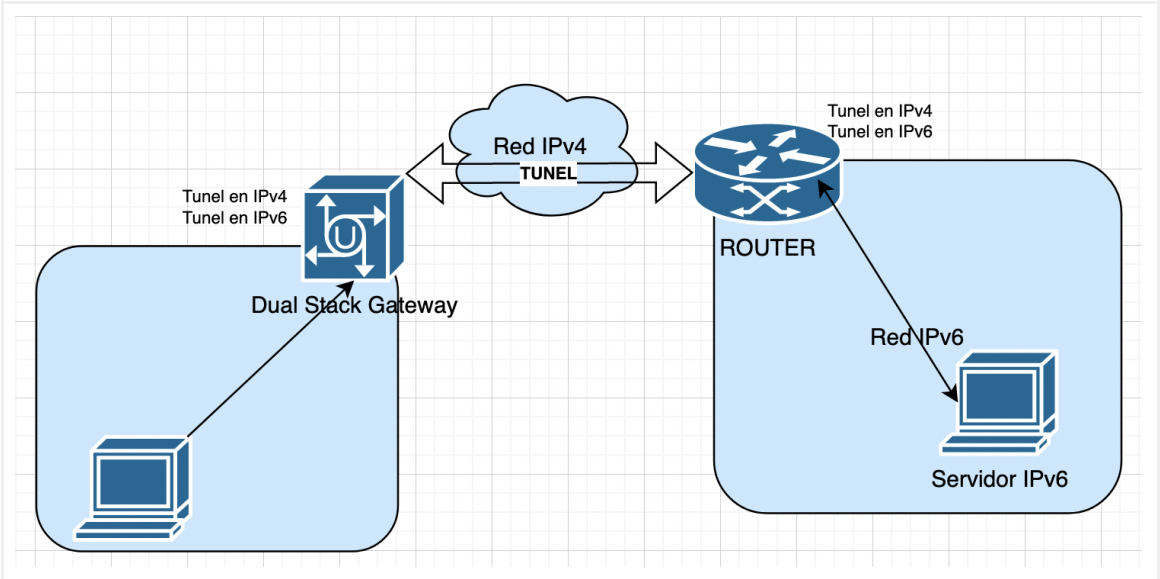


Figura 11.- Configuración manual del Túnel

Fuente: Autor

- *Automatic 6to4 Tunnel*.- Se refiere a una configuración del túnel que no requiere administración directa, el cual permite conectar un sitio aislado en IPv6 hacia una red IPv4 y hacia redes IPv6. Este mecanismo trata la red IPv4 como un enlace virtual sin transmisión (*nonbroadcast*), por lo que la dirección IPv4 embebida en la dirección IPv6 se usada para encontrar el otro extremo de la red. La dirección IPv4 es fácil de extraer del paquete de red de IPv6 y se entrega todo el paquete sobre la red IPv4, si son compatibles con *6to4* el cual es el más utilizado.

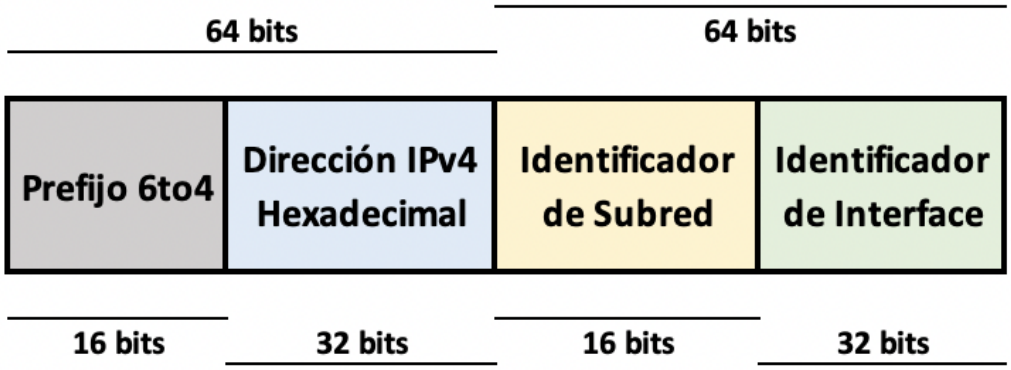


Figura 12.- Estructura de una dirección IPv6 con automatic 6to4 Tunneling

Fuente: Autor

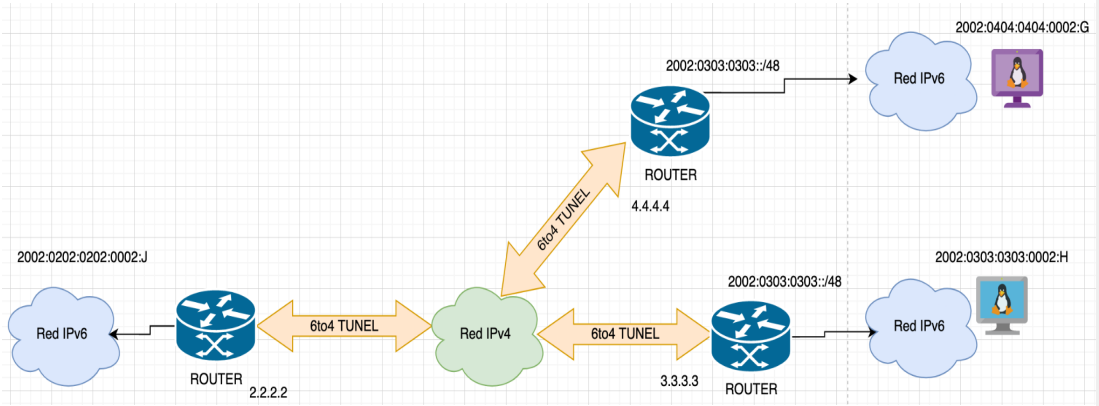


Figura 13.- Ejemplo de Automatic 6to4 Tunnel

Fuente: Autor

- 6RD (IPv6 Rapid Deployment) .- Desarrollado por un ISP francés, es un refinamiento de 6to4 Tunnel,ya que este cambia el formato de las direcciones.Requiere de dos componentes:
  - CPE 6RD.-Es la interfaz entre el operador y el usuario y necesita un software que soporte 6RD.
  - Relay 6RD.- Es la interface entre la red IPv4 y la red IPv6, encargado de encapsular y desencapsular paquetes

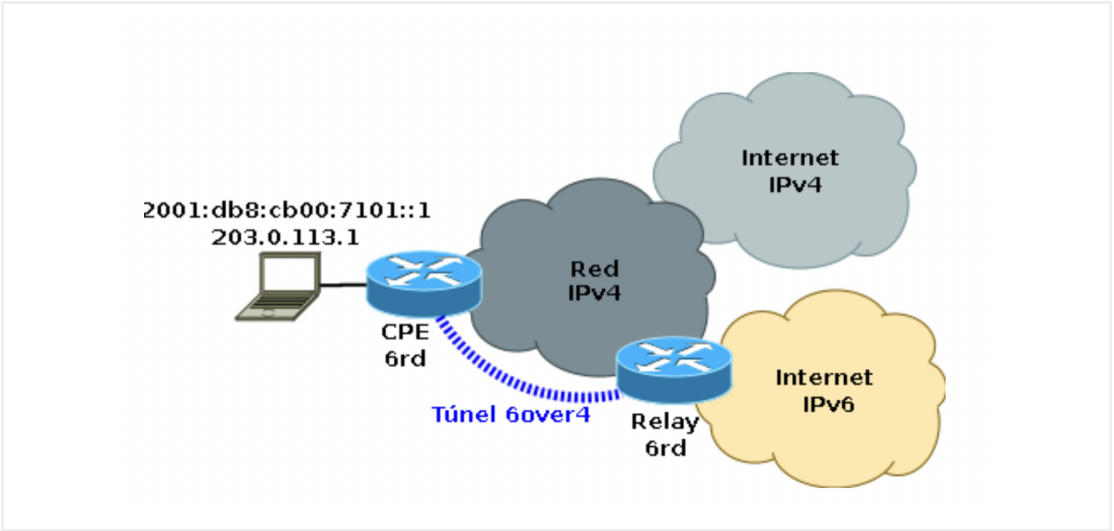


Figura 14.- Arquitectura 6RD

Fuente: https://www.lacnic.net/4012/1/lacnic/ipv6:-transition-mechanisms

5.4 Dual Stack-Lite[5]

Se centra en los servicios de internet para IPv4 obtengan sobre una red de transporte solo de IPv6 con un esquema de túnel de IPv4/IPv6; el tráfico IPv4 es encapsulado y enviado a un NAT (solo tiene un nivel) : CGN, LSN, AFTR (Address Familiy Transition Router), B4 (Basic Bridging BroadBand), por tanto, las direcciones IPv4 son compartidas. Por otro lado, la red IPv6 opera de forma nativa en la red del operador.

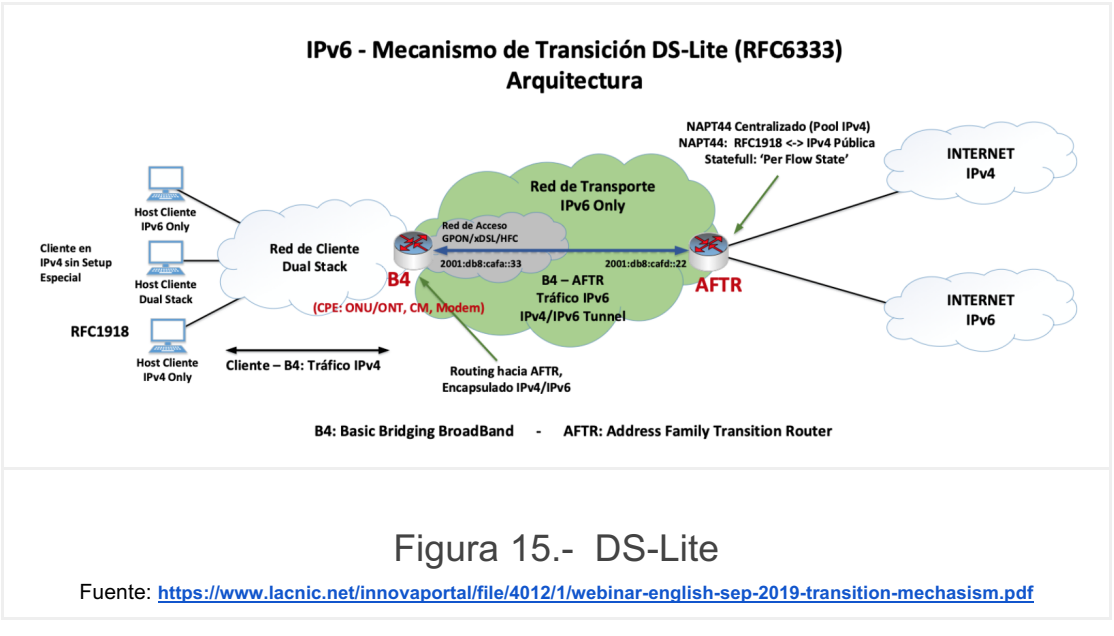


Figura 15.- DS-Lite

Fuente: https://www.lacnic.net/innovaportal/file/4012/1/webinar-english-sep-2019-transition-mechasism.pdf

En la figura 7, se observa un CPE/B4 el cual tiene el tráfico IPv4 a diferencia del AFTR el cual maneja la red IPv6. el CPE/B4 encapsula todo el tráfico IPv4 usando el

túnel IPv4/IPv6 y reenviarlo a AFTR (y viceversa). Este mecanismo admite tráfico *"unicast"* pero no admite tráfico *"multicast".*

Ventajas

- No se requiere ninguna modificación para los clientes IPv4 o los clientes Dual Stack.
- El tráfico IPv6 no se encapsula, haciendo más eficiente la red.
- Soporte de todo tipo de protocolo con tráfico "*unicast*".
- Adopción de este mecanismo sin impacto en la red IPv6.
- Aprovisionamiento de B4 con opciones de DHCPv6.

Desventajas

- Sobrecarga en la red de transporte derivado el encapsulado del túnel IPv4/IPv6.
- No soporta tráfico multicast.
- No resuelve el problema de la falta de direcciones IPv4.
- No es compatible con el IPv4 Mesh en la red de transporte del ISP.
- Con el manejo del túnel se agrega complejidad al *(Deep Packet Inspection*) DPI.

5.5 Lw4o6 (LightWeight 4o6)[22]

Es una extensión de la versión de DS-Lite, el cambio radica en que el NAT se ubica del lado del cliente del túnel IPv4/IPv6. Existen dos componentes principales:

- Lw4o6 .- Lightweight Basic Bridging BroadBand.
- LwAFTR .- Lightweight Address Family Translation Router.

El NAT44 es distribuido en los CPEs, por lo tanto el LwAFTR disminuye la información de estado, ya que usa un modelo *"per subscriber"* y una tabla *"Restricted Port Set ID"* para el encapsulado de los paquetes enviados por el LwB4

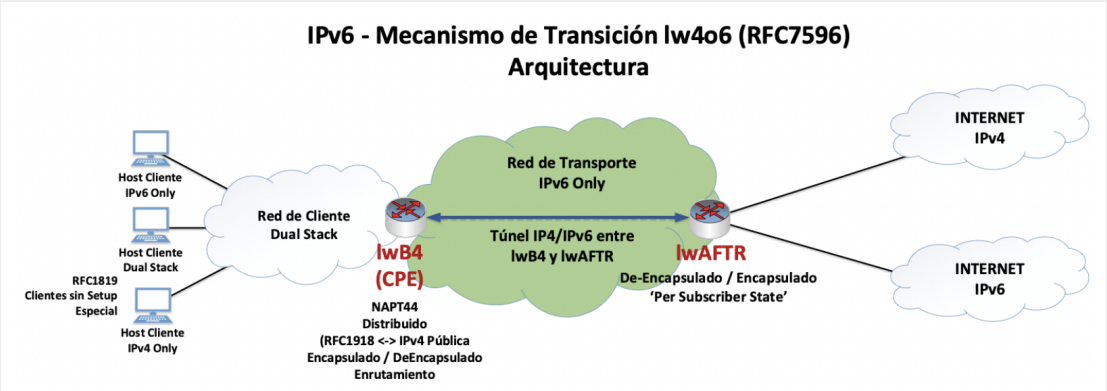


Figura 16.- Lw4o6

Fuente: https://www.lacnic.net/innovaportal/file/5495/1/el-mecanismo-de-transicion-lw4o6.pdf

Ventajas

- Además de tener las mismas ventajas que DS-Lite.
- Aprovisionamiento automático de lwB4 con DHCPv6 options.
- No se requiere ahora de CGNAT en el lwAFTR.
- Mejor desempeño que DS-Lite, ya que el NAPT es distribuido.

Desventajas

- El “overhead” en la red de transporte por el encapsulado de túnel IPv4/IPv6 entre lvB4 y lwAFTR.
- No soporta tráfico multicast.
- Puede requerir alguna actualización de CPE para soporte de funcionalidad de lwB4.
- No soluciona el problema de agotamiento de direcciones IPv4.
- No está ideado para redes móviles celulares.
- El encapsulado IPv4/IPv6 en la red de transporte IPv6 Only agrega cierta complejidad al DPI en la red del operador.

5.6 Traductores de Versión

Esta técnica consiste en utilizar algún dispositivo que convierte los paquetes de IPv4 a IPv6 y viceversa.

5.6.1 NAT64 (RFC 6146)

Network Address Translation-Protocol. - Los nodos NAT son los que se encuentran en la frontera entre la red IPv6 e IPv4. Cada nodo contiene un grupo de direcciones IP enrutables de IPv4, las cuales son dinámicamente asignadas a nodos con dirección IPv6, esto no es simétrico, es decir, no se puede mapear una dirección IPv6 hacia una dirección IPv4 (se mantiene un estado). Todos los servicios, aplicaciones, clientes dentro de las redes que usa NAT64 del usuario deberán soportar IPv6. Es absolutamente necesario usar DNS64 con esta solución.

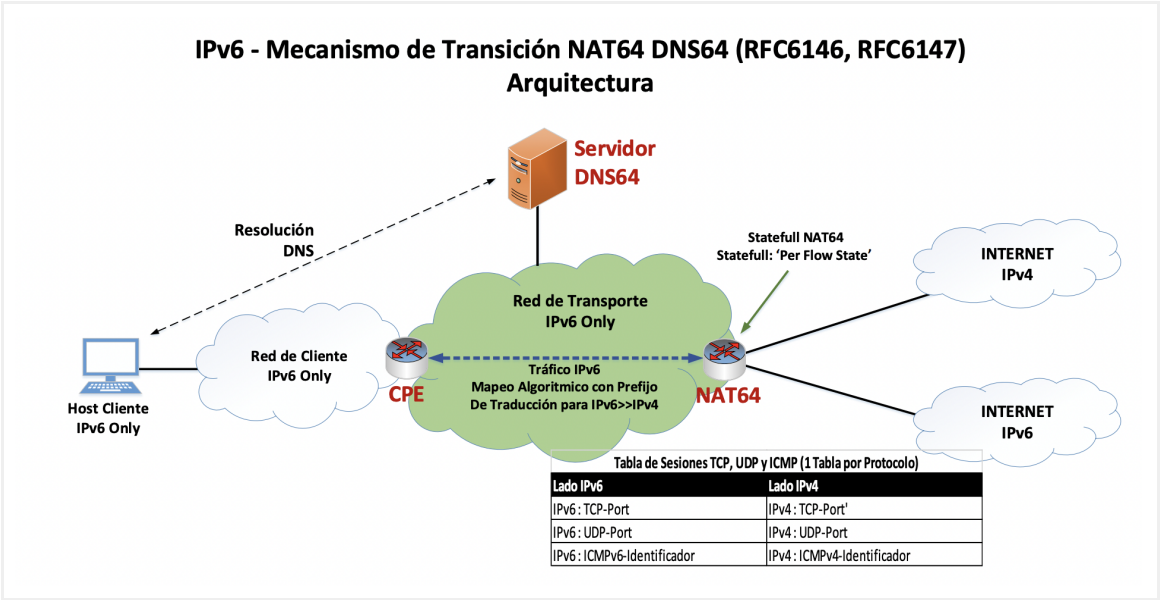


Figura 17.- Funcionamiento de NAT64 y DNS64

Fuente: https://www.lacnic.net/innovaportal/file/5495/1/nat64.pdf

Ventajas

- No requiere modificación ni aplicaciones ni protocolos adicionales en los clientes IPv6.
- No usa encapsulado.
- El tráfico IPv6 no es encapsulado ni traducido.
- Hay balanceo de cargas usando varios NAT64 y varios esquemas de prefijos de traducción.
- Permite que varios clientes IPv6 compartan el uso de direcciones públicas IPv4.

Desventajas

- No resuelve conexiones entrantes desde internet IPv4.
- Limitado solamente a TCP, UDP e ICMP.
- Falla para aplicaciones que necesiten “local binding” en IPv4, en general aquellas que requieran IPv4 en forma nativa en el cliente IPv6.

5.6.2. 464XLAT (RFC6877)[22]

Los clientes usan un traductor SIIT para convertir paquetes de IPv5 hacia IPv6.Es necesario mandar estos paquetes hacia un NAT64 para que se pueda realizar la traducción; se requiere un dispositivo intermedio conocido como CLAT o PLAT para poder realizar esta comunicación.
Si una red debe soportar aplicaciones y host con direccionamiento IPv4, la solución recomendada es 464XLAT.

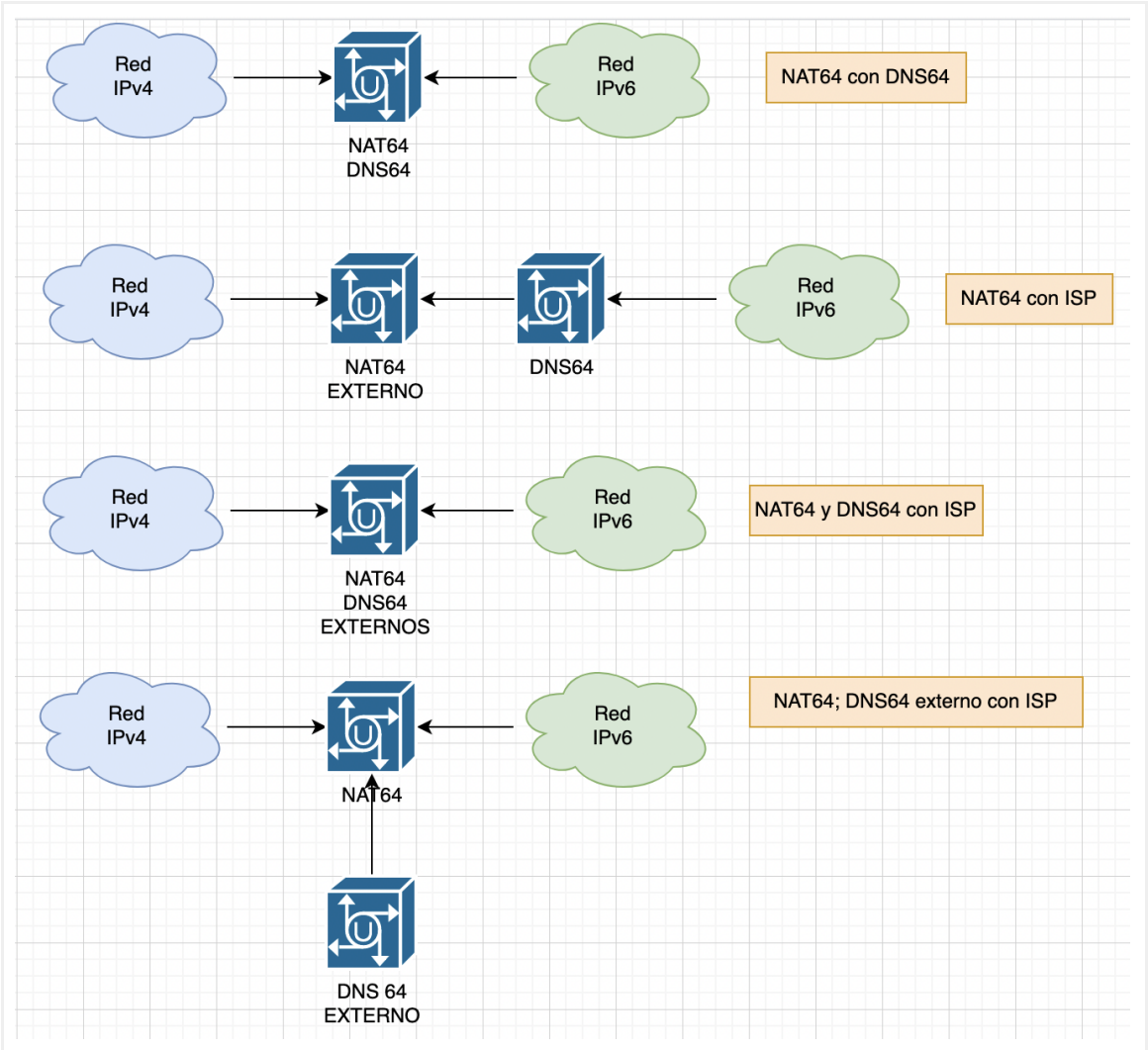


Figura 18.- Posibles escenarios para 464XLAT

fuente: Autor

5.6.3 DNS64

Servicio de Domain Name Server (DNS) modificado para generar un registro AAAA. Encargado de convertir registros A de IPv4 a registros AAAA de IPv6. Donde el FQDN no tiene registro AAAA, este servicio dinámicamente genera uno que permite al cliente usar IPv6 y traducir de la red IPv6 hacia la red IPV4 en un NAT64.

5.6.4 Prefix64 Discovery

Consultas para el WKP de FQDN ipv4 only.arpa, el cual está definido solo en redes IPv4. Si hay una respuesta AAAA proporcionada, entonces existe un DNS64 que conoce la ruta para llegar.

5.6.5 NAT64 con estado stateless (RFC 6145)

Se requiere traducir los 32 bits de direcciones IPv4 dentro de paquetes de 32 bits de direcciones IPv6. CLAT ,es decir un NAT de IPv4 a IPv6. El algoritmo utilizado es determinístico y dinámico, bidireccional, es decir, con un mapeo 1 a 1. Esta funcionalidad permite transportar IPv4 sobre una red solo IPv6, se usa solo en CPE.

5.6.6 NAT64 sin estado stateful (RFC 6146)

Es un proveedor de traducciones PLAT , es decir, un NAT de IPv6 a IPv4.El algoritmo utilizado es dinámico, no determinístico, la traducción se basa en un pool de direcciones IPv4; el estado de la conexión se basa de sesiones (creación y término). Traduce IPv6 del CLAT a IPv4 público.

Para realizarlo se requiere

- definir un prefijo de NAT64:
    - Well-Known-Prefix (WKP): Prefijo único en la red definido como 64:ff9b::/96.
    - Network-Specific-Prefix (NSP); Longitudes de prefijo posibles: 32, 40, 48, 56, 64, o 96. Pueden existir varios en la red.
- Establecer un grupo de direcciones IPv4 a usar en NAT64,
    - Se define si es determinístico o dinámico.

5.6.7 Mapping Address Translation[21]

Permite al ISP proporcionar acceso a clientes IPv4 hacia una red IPv6. Es sin estado (stateless), es decir, no mantiene ningún enlace o estado de sesión mientras realiza la traducción.

Un componente necesario en el ISP es el Stateless Border Relay (BR), el cual permitirá un ruteo es asimétrico y acepta tráfico *"anycast*". Genera un único punto de fallo.

Existen dos componentes necesarios:

- MAP CE (Customer Edge).-Envía tráfico nativo de IPv6 y traduce entre IPv4 y IPv6. Puede ser un gateway o un router que soporte MAP

- MAP BR (Border Relay) .- Localizado en la red del cliente, en el borde de internet IPv4.

5.6.7 Mapping of Address and Port- Encapsulation (MAP-E) [25]

Definido en el RFC 7597. Está basado en el encapsulamiento de IPv4 sobre IPv6 y el mapeo de direcciones y puertos IPv4 a IPv6 y viceversa. La característica de este RFC es que se tiene transparencia completa por encapsulación, dado que se encapsula el tráfico dentro del encabezado IPv6, generando una carga superior a las 40 bytes.

5.6.8 Mapping of Address and Port - Translation (MAP-T) [25]

Definido en el RFC 7599. Está basado en la traslación de direcciones y puertos IPv4 a IPv6 y viceversa. A diferencia de MAP-E, tiene alta transparencia debido a las traducciones, ya que se traducen los encabezados de IPv4 a IPv6, generando una carga superior a las 20 bytes.

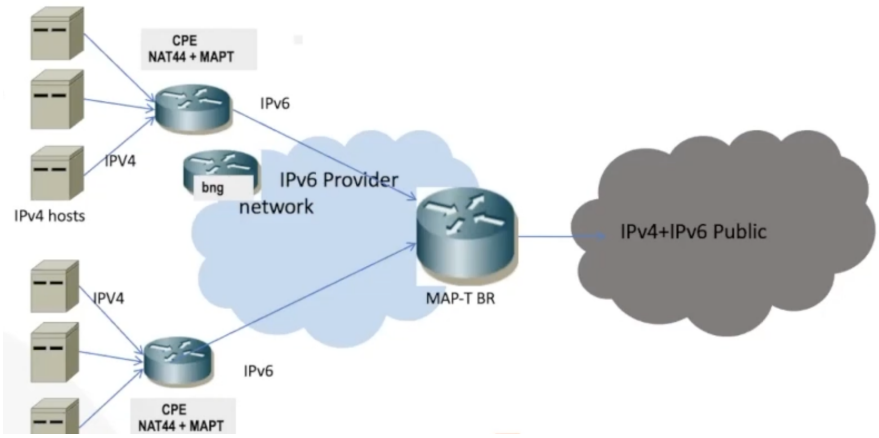


Figura 19.- Arquitectura de MAP-T

Fuente: https://www.lacnic.net/innovaportal/file/5495/1/map-e-y-map-t.pdf

5.7 IPv6-Only

Este es el término con varias acepciones, de acuerdo al contexto, pero ninguna oficialmente aceptada aún en la IETF. Se conoce cuando solo IPv6 está corriendo o está habilitado, sin IPv4 habilitado o configurado sobre algún enlace ya sea físico o virtual, o en alguna aplicación y/o servicio. Se encuentra limitado porque es necesario tener solo el soporte de IPv6 en todos sus elementos de la red y de las aplicaciones.

Para cerrar este apartado de los mecanismos de transición utilizados en la actualidad, es importante destacar que estas arquitecturas dependen de las condiciones de las topologías de red que se tengan, así como el tipo de servicio que ofrezca el ISP, sin embargo, existen implicaciones técnicas a considerar en cada una de ellas, como: es el manejo del tráfico para telefonía móvil, el soporte del uso de traductores o túneles sobre los dispositivos cores frontera, los riesgos de seguridad implícitos sobre cada solución.

El presente trabajo tiene como objetivo dar a conocer estos mecanismos de transición y permitir al lector evaluar las necesidades que tiene que cubrir para que pueda elegir o inclusive combinar dichas tecnologías.

Capítulo 6. Aspectos de seguridad con IPv6

Hablar de seguridad en redes implica conocer las diferentes amenazas que existen con el uso y despliegue de las redes IPv6, por ello se presentan en la tabla 11 algunas amenazas que explotan las características de IPv6 y cómo mitigarlas.

Tabla 11.- Algunas amenazas de seguridad en IPv6 [11]

Amenaza	Características IPv6	Mitigación
Exploración del medio	El escaneo de dispositivos no es tan factible por el gran espacio de direcciones. Las direcciones conocidas (multicast) son vulnerables.	Las extensiones de privacidad pueden hacer el reconocimiento del medio menos efectivo.
Acceso no autorizado	La seguridad de punto a punto reduce la exposición. Las cabeceras de extensión (EH) abren brechas para nuevos ataques.	El uso de las extensiones de privacidad para reducir la exposición de los dispositivos. Uso de múltiples direcciones con diferentes alcances. Administrar el uso de EH.
Manipulación de cabeceras	IPv6 puede aprovechar el tamaño y dependencia de las EH. Las EH pueden ser procesadas por todas las pilas, son usadas particularmente por los atacantes.	Las EH deben ser estrictamente usadas en el despliegue y control de servicios .
Fragmentación	el “overlap” en la fragmentación no está permitido, pero algunas pilas reensamblar paquetes “overlap”. El impacto de los fragmentos pequeños en IPv6 es muy bajo.	Uso adecuado en la implementación de las pilas para no permitir el “overlap” en la fragmentación.
Suplantación de identidad en capa 3 ó 4	El uso de túneles permite tener más oportunidades para la suplantación de identidad, no es diferente de IPv4.	Se usan las mismas técnicas de defensa para IPv4.
Ataques de resolución de direcciones e inicialización de dispositivos	DHCP tiene similares vulnerabilidades para los dos protocolos (IPv6 e IPv4). Neighbor Discovery tiene	Utilizar una solución provisional como neighbor estáticos. Hay recomendaciones para que el mensaje SEND se adopte en la pila

	vulnerabilidades similares a ARP. La autoconfiguración y la re-numeración ofrecen nuevas opciones para los ataques.	de IPv6.
Smurf (amplificación del broadcast)	No hay concepto de broadcast en IPv6 y se reduce la opción de ampliar el ataque.	Se utiliza el filtrado de tráfico multicast, ya que es solo esa opción de propagarse.
Ataques de ruteo	IPSec proporciona algunos puntos de seguridad para algunos protocolos. Es similar a IPv4.	Técnicas similares a IPv4. Donde sea posible, implementar IPSec.
Virus y gusanos	El escaneo aleatorio para propagar los gusanos es impráctico por el gran tamaño del espacio de direcciones.	Mismas técnicas que IPv4.
Ataques a los mecanismos de transición	Nuevos puertos son abiertos en IPv4 en el firewall. El túnel automático es más susceptible a ataques. La transición de IPv6 a IPv4 puede ocultar la fuente del ataque.	Control más estricto de los puertos en los firewalls, abriendo solo los necesarios. Uso de túneles estáticos donde sea posible.
IP móvil	Está embebido en IPv6. Tiene características específicas de seguridad.	Filtrar todos los encabezados de enrutamiento excepto los tipo 2 si MIPv6 es usado. MIPv6 más allá del uso de IPSec.
Sniffing	Similar a IPv4.	Similar a IPv4.
Ataques en la capa de aplicaciones	IPSec ofrece el potencial de incrementar la seguridad para rastrear a los atacantes.	similar IPv4. La seguridad en la última línea depende del servidor de defensa.
Dispositivos no autorizados	Similar a IPv4.	IPSec previene la interacción con estos dispositivos. Algunos protocolos como el 802.1x puede prevenir el bloqueo de dispositivos no autorizados desde la conexión a la red.
Ataques de Denegación de Servicios	IPSec puede proteger mientras no sea robada la llave.	Hay una gran necesidad para una autenticación escalable y operacionalmente factible y un mecanismo de intercambio de llaves.
Ataques de saturación de ancho de banda	Similar a IPv4.	Mecanismos de limitación del uso y del tipo de tráfico.

La NIST (National Institute of Standards and Technology) recomienda no asignar direccionamiento IPv6 secuencial para evitar los escaneos de red de los atacantes y preservar la ventaja de tener rangos de direcciones muy grandes.

Otras recomendaciones de seguridad hechas por CISA (CyberSecurity Infraestructure Security Agency) para redes implementadas en IPv6, no para ambientes *Dual Stack* dentro de las áreas TIC se muestran en la tabla 12. Cabe destacar que asocian las características de IPv6 con capacidades de seguridad, describiendo qué consideraciones se deben tener con la adopción de esta versión del protocolo.

Tabla 12.- Recomendaciones de CISA hacia TICs[11]

Característica de IPv6	Capacidades de Seguridad	Consideraciones de Seguridad
No se tiene experiencia de implementar y correr redes IPv6.	Conocimiento y capacitación del personal de redes.	No se entienden las diferencias de seguridad entre IPv4 e IPv6. Se requiere aprender y capacitar para un correcto despliegue de IPv6
Las diferencias entre las versiones de los protocolos requieren revisión de las políticas de seguridad	Las políticas actuales fueron creadas para IPv4, es necesario revisar las diferencias con las redes IPv6, como es la distribución del direccionamiento y opciones de la cabecera, para tener políticas más efectivas.	Revisión, actualización y publicación de políticas de seguridad.
El crecimiento del direccionamiento de red puede generar retos en la administración de los activos	Las subredes de IPv6 generan más de 2^{128} direcciones la cuales hacen que los procedimientos de administración de activos no sean factibles, como el escaneo o descubrimiento de activos por rango de direcciones de IP.	Inventario. Administración y configuración de activos. Control de Accesos. capacidades web.
Múltiples direcciones en un dispositivo puede generar problemas en la correlación de eventos en el análisis de bitácoras.	Un dispositivo puede tener múltiples direcciones IPv6, lo cual puede producir problemas de correlación, ya que un dispositivo representa distintas bitácoras con diferentes direcciones.	Centralización de bitácoras en la administración y análisis. Auditorías y cumplimiento. Automatización, respuesta y gestión de la seguridad.
El tráfico sitio a sitio puede dirigirse a través de Internet en lugar de hacerlo mediante túneles el uso de VPN	La habilidad de comunicarse entre dispositivos con dirección IPv6 en zonas de confianza (debido a la IP GUA), esto significa que hay tráfico de intercambio entre sitios que puede estar pasando sin el uso de VPN. Si la VPN se pierde, el tráfico es	Pérdida de información en servicios como web, correo. Uso de VPN. Segmentación de red. Administración de la seguridad.

	vulnerable a escuchas ilegales y ataques de inyección de paquetes.	
Direcciones temporales pueden crear desafíos en la administración de las ACLs	Las extensiones de privacidad de IPv6 mediante SLAAC permiten a un dispositivo generar periódicamente una nueva dirección IP temporal, esto genera que la lista de ACL tenga que estar actualizándose constantemente. La utilización de direcciones privadas estables, la asignación manual o vía DHCPv6 puede ayudar a mejorar la administración de las ACLs	Denegación de acceso a Internet. Control de Accesos.
Las direcciones temporales pueden generar más búsquedas frecuentes de direcciones en las bitácoras durante las auditorías.	Los ruteadores pueden almacenar grandes cantidades de direcciones en la memoria caché, cuando las extensiones de privacidad del protocolo SLAAC se utilizan para generar direcciones IP temporales. En consecuencia, la memoria caché de vecinos debe de ser consultada con frecuencia para asegurar que las direcciones IP sean almacenadas y recuperadas para un análisis forense y correlación de eventos. Esto puede provocar potenciales problemas en el registro y la precisión de los eventos.	Control del ancho de banda. Protección de una Denegación de Servicios. Auditoría y cumplimiento. Planeación y respuesta de incidentes.
El direccionamiento automático es vulnerable a ataques de denegación de servicio. (DoS)	SLAAC y NDP determinan la dirección link-local. El ataque ocurre cuando un router se satura cuando requiere la resolución de una dirección en una amplia subred IPv6. DoS se puede mitigar reduciendo el rango de las subredes y controlando la velocidad de asignación de direcciones. También se puede limitar el caché para el descubrimiento de “neighbor” mediante la asignación de un prefijo único IPv6 para cada dispositivo, sin embargo esto puede afectar la privacidad si los prefijos no se cambian periódica o aleatoriamente	Control del ancho de banda. Protección de una Denegación de Servicios. Auditoría y cumplimiento. Planeación y respuesta de incidentes.
Los anuncios del router (RAs) pueden ser falsificados y vulnerar el tráfico con una escucha activa no autorizada.	NDP utiliza los mensajes RA, los cuales pueden ser vulnerables a la falsificación. Las redes deberían ser configuradas utilizando RA Guard, que ayuda a protegerlos de estos ataques. RA Guard, recomienda un proceso de descubrimiento dinámico para los routers IPv6. Se recomienda revisar periódicamente la lista de los routers válidos. También aplica para DHCPv6 porque utiliza los	Administración de la configuración. Inventario. Auditoría y cumplimiento. Trazabilidad de la información.

	mensajes RA para la determinación del prefijo y descubrir los ruteadores por defecto.	
Dispositivos con direccionamiento manual pueden ser vulnerables a ataques de servidores DHCPv6 comprometidos.	Los servidores DHCPv6 comprometidos pueden asignar direcciones IP maliciosas. Esas direcciones vuelven vulnerables a los dispositivos a ataques como “on-path”. La red debe ser configurada para el correcto filtrado de puertos para paquetes autorizados , y registrar para luego borrar los paquetes maliciosos.	Administración de la configuración. Administración de la seguridad. Prevención de pérdida de información.
Pérdida de confianza en los archivos del servidor DHCPv6.	DHCPv6 utiliza un identificador único (DUID) para identificar a los dispositivos que puede obtener la dirección data-link, esté identificador representa una interfaz de red del cliente. Puede que el cliente utilice solo red cableada y no red inalámbrica para conectarse a la red.	Administración centralizada de bitácoras. Administración de la configuración. Auditoría y cumplimiento.

Internet Protocol Security (IPSec)

Conjunto de protocolos para asegurar la protección de las comunicaciones en Internet a través de la autenticación del emisor y proporcionando integridad opcional en la transmisión de datos.

IPSec utiliza dos cabeceras de extensión de IPv6: *Encapsulating Security Payload* (ESP) y *Authentication Heade*r (AH). La administración y negociación de las llaves secretas asociadas en este proceso están a cargo del protocolo Internet Key Exchange (IKE). IPSec ofrece la misma seguridad que en IPv4.

En IPv6 existe la posibilidad de agregar mecanismos de seguridad con SEND (SEcure Neighbor Discovery), usando IPSec y el cifrado para incrementar el nivel de seguridad en la red, sin embargo no es mandatorio, ya que el manejo de llaves para cada conexión a internet no es fácil de administrar, sin considerar los requisitos de hardware para poder tener el soporte de IPSec, por tanto su uso queda como una recomendación sobre IPv6 y no como un requerimiento absoluto en el equipo de cómputo.

DNSSEC

El servicio de DNS tiene como propósito realizar la traducción directa o de reversa de direcciones IP hacía nombre de dominios y su base de datos está estructurada en un conjunto de registros (SOA, A,NS,MX,etc.). Cada registro tiene 5 campos: clase, tipo, valor, nombre y TTL. Este servicio presenta vulnerabilidades como Man in the middle,

cambio de datos en DNS secundarios, DoS, Spoffing entre el maestro y esclavo, es por ello, que surge DNSSec como una extensión del protocolo.

Domain Name Security System Extension (DNSSEC) fortalece la autenticación utilizando una firma digital con cifrado de llave pública entre sus diferentes niveles., ya que proporciona un mecanismo para poder validar la autenticidad y la integridad de los datos contenidos en la zona DNS.

DNSSec resuelve problemas de seguridad del servicio DNS, ya que ofrece un mecanismo para delegar la confianza en ciertas llaves públicas (cadenas de confianza) y un mecanismo para autenticar la zona entre primarios y secundarios.

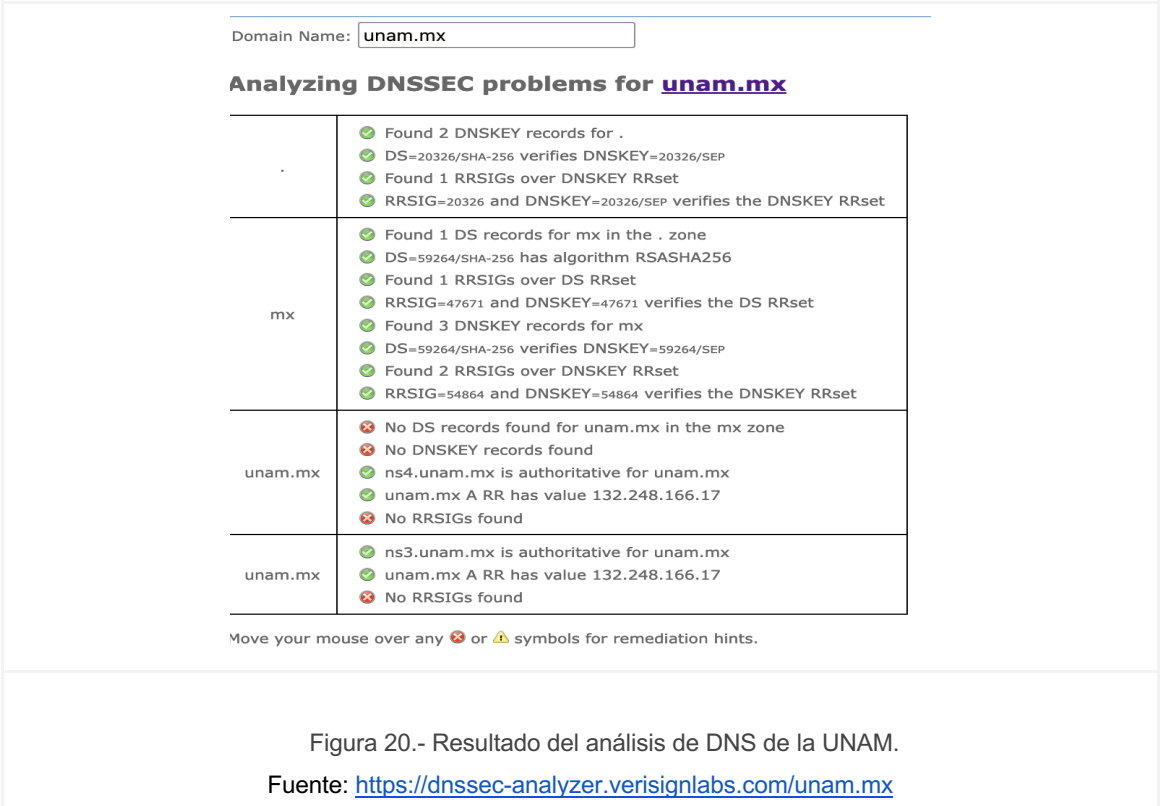


Figura 20.- Resultado del análisis de DNS de la UNAM.

Fuente: https://dnssec-analyzer.verisignlabs.com/unam.mx

DNSSec firma los registros(RRSet) que se tienen guardados y se genera otro registro (RRSIG) al igual que se genera un par de llaves (pública y privada) para cada zona (DNSKEY). En la figura 20, se muestra el registro firmado con SHA-256.

Debido a que las direcciones IPv6 no son fáciles de recordar, el servicio de DNS proporciona un mapeo básico entre dominios y direcciones, es por ello, que IPv6 y DNSSec dentro de la infraestructura de red integran muchos beneficios para el usuario final, sin embargo, no hay dependencia uno del otro para operar dentro de la red.

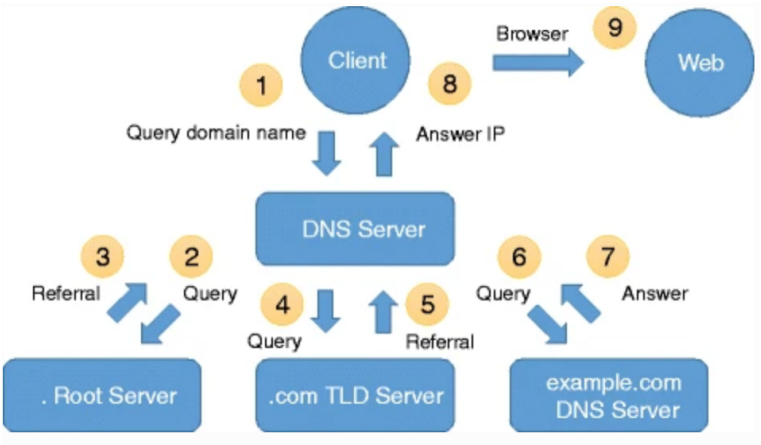


Figura 21.- Proceso de consulta a un DNS

Fuente: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-016-0675-4/figures/3

Capítulo 7. Mecanismos de capa 3

En este capítulo se ha realizado un breve resumen de todas las buenas prácticas y recomendaciones que tiene de manera pública el NIST (National Institute of Standards and Technology).

7.1 Firewall

A continuación se muestra en la tabla 13 el ejemplo de algunas reglas de filtrado que se utilizan para IPv6.

Tabla 13.- Reglas de filtrado para IPv6 [28]

Acción:	Ejemplo:
bloqueo de direcciones “bogus” en IPv4 en todos los firewalls.	127.0.0.0/8 192.0.2.0/24 198.51.100.0/24 203.0.113.0/24 240.0.0.0/4 (192.0.0.0/24)
bloqueo de direcciones “bogus” en IPv6 en todos los firewalls.	::1/128 2001:db8::/32 2001:10::/28 (2001::/23)
bloqueo de direcciones “bogus” en IPv4 en firewalls de frontera.	0.0.0.0/8 10.0.0.0/8 100.64.0.0/10 169.254.0.0/16 172.16.0.0/12 192.0.0.0/29 192.168.0.0/16 198.18.0.0/15 255.255.255.255/32
bloqueo de direcciones “bogus” en IPv6 en firewalls de frontera.	::/128 100::/64 2001::/32 2001:2::/48 fc00::/7 ::ffff:0:0/96 fe80::/10 no válido fuera de una red local excepto fe80::/64 usado para ND
Borrar opciones desconocidas de las cabeceras de extensión.	NH=43 permit NH=0 drop con IPv4 opción 131 y 137

7.2 Algoritmos de Cifrado

El manejo de ESP y AH son mecanismos de protección que permiten habilitar algoritmos de cifrado en los datos que se envían sobre IPSec. En la tabla 14 se muestra la lista de Algoritmos soportados en ESP.

Tabla 14.- Algoritmos de cifrado soportados en ESP

Algoritmo	RFC
ENCR_DES_IV64	No especificado
ENCR_DES	2405
ENCR_3DES	2451
ENCR_BLOWFISH	2451
ENCR_3IDEA	No especificado
ENCR_DES_IV32	No especificado
ENCR_NULL	2410
ENCR_AES_CBC	3602
ENCR_AES_GCM_8	4309
ENCR_AES_GCM_16	4106
ENCR_CHACHA20_POLY1305	7634

Capítulo 8. Aplicaciones con IPv6

En este apartado, se presentan sólo algunas de las muchas aplicaciones que soportan Dual Stack y que en condiciones técnicas específicas permite administrar ambos protocolos.

8.1 OpenVPN

Este es un software de código abierto que permite realizar conexión VPN utilizando IPv6 a través de túneles de conexión punto a punto. Soporta SLAAC, CGA, NAT64, IPv6 to IPv6, ILNP, shim6.

8.2 Wireguard

Este software permite realizar conexión VPN utilizando IPv6 a diferencia del anterior, está integrado con el kernel de linux, que reemplaza a TLS y a IPSec, por el manejo de llave pública y cifrado DTLS.

8.3 FoxyProxy

Es un servidor proxy que proporciona el servicio de VPN,que ofrece su código abierto para transmisión de video, geolocalización, manejo de cifrado en los canales de comunicación.

8.4 Shorewall

Un software que configura el paquete de Netfilter de las distribuciones linux para poder cubrir requerimientos de router/gateway/firewall se requiere como mínimo la versión 4.2.4 para que soporte IPv6.Separa las reglas de filtrado de IPv4 e IPv6 en cada una de las etapas de su configuración. En conjunto con Squid pueden trabajar como un proxy transparente de http/ https. No soporta balanceo entre routers.

8.5 RADVD

Es un software que nos permite activar un demonio dentro del sistema operativo linux para generar mensajes de anuncio del router (RA), que son necesarios para la autoconfiguración con estado en el protocolo IPv6. También proporciona mensajes de direcciones que darán resolución en IPv6. Proporciona información del default gateway, mientras que el servicio de DHCPv6 ofrece direcciones IP aleatorias para garantizar la protección de la privacidad en la red y envía configuraciones de la red opcionales para algunos clientes como NTP e IPXE.

8.6 Squid

Es un servidor proxy para consulta de servicios Web.Se requiere al menos la versión 3.1 para poder habilitar la versión IPv6. Puede detectar las pilas de tcp y soporta dual stack a través de dos sockets en el sistema operativo que se encargan de realizar un mapeo. La parte de dual stack. También puede administrar listas de Accesos para IPv4 e IPv6.

8.7 Kubernetes

Es un orquestador de contenedores de código abierto el cual permite automatizar y administrar aplicaciones que radican en contenedores. Se requiere al menos la versión 1.2 para poder soportar el servicio de Dual Stack para el aprovisionamiento de red en IPv6 e IPv4.

8.9 DNSMASQ

Es un software que proporciona servicios como DHCP,DNS y la autoconfiguración de los equipos para IPv6 en redes pequeñas. Su capacidad máxima según las publicaciones de estudios hechos por Red Hat, se logra tener 99.99999% de disponibilidad de estos servicios [51].

El siguiente estudio se realizó con un DNS local y se realizaron pruebas con la herramienta dnsperf, donde se alcanzan hasta 10000 peticiones hacia el DNS.

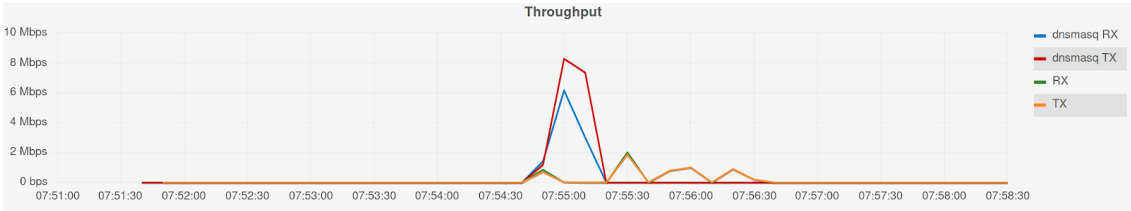


Figura 22.- Rendimiento de DNSMASQ

Fuente: https://www.redhat.com/en/blog/five-nines-dnsmasq
Autor: Ahmed Nazmy

Capítulo 9. Protocolos de Ruteo

Los protocolos de ruteo dinámico permiten la comunicación entre routers para interconectar las diferentes redes; integrando nuevas versiones para el soporte de la red IPv6, que a continuación se describen brevemente. Se agrupan por dos tipos, ya sea por exterior o interior. Para el protocolo Internal Gateway Protocol (IGP), y en base a su funcionamiento se dividen en vector distancia y en “link-state” ; dentro de vector distancia, dependiendo su comportamiento con clase tenemos el RIPng, OSPFv3, IS-IS y EIGRP. Mientras que para el External Gateway Protocol (EGP) se incluye BGP.

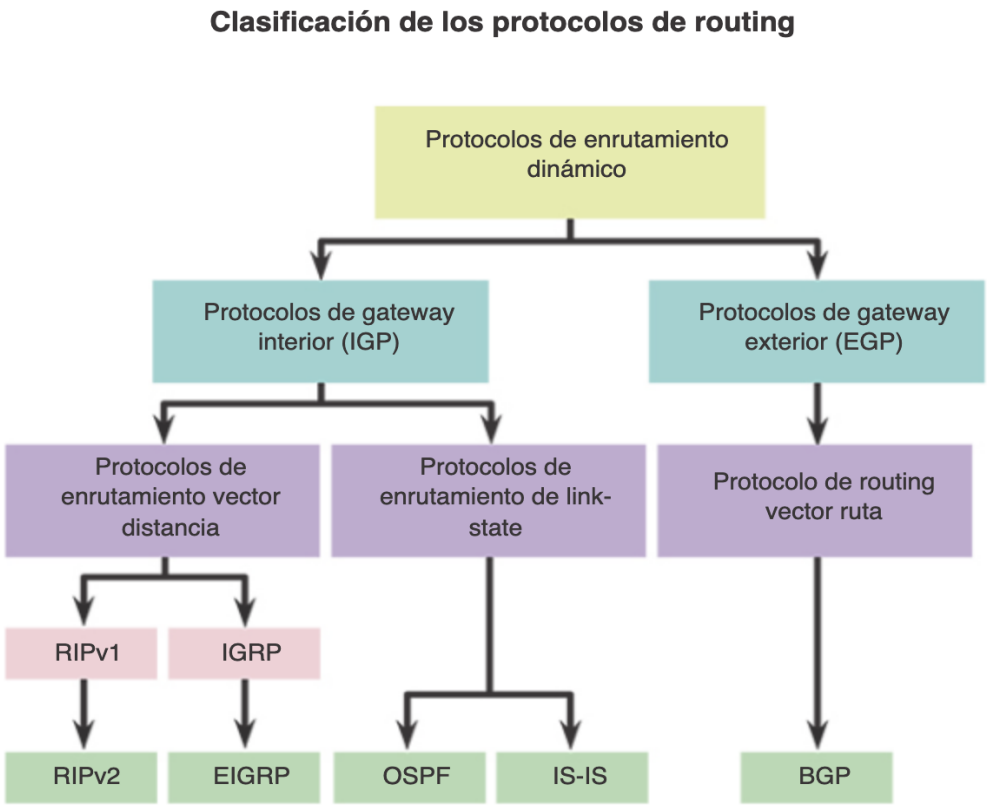


Figura 23.- Clasificación de los protocolos de Ruteo

Fuente:https://quizlet.com/379801616/semana-5-pdfs-protocolos-de-enrutamiento-dinamico-y-vlans-flash-cards/

9.1 RIPng

Este protocolo usa un algoritmo de vector de distancia y su tiempo de convergencia es bajo; es escalable hasta en 15 saltos. Los router mantienen una base de datos que contiene los valores de las distancias conocidas de toda la red. Periódicamente se envía esta información a los vecinos, los cuales actualizan las tablas, así se realiza su mecanismo de propagación en toda la red.
Implementa mecanismos como “Poison-reverse” o “split-horizon” para evitar propagar errores y evitar los bucles. Elige la ruta más corta de acuerdo con el conteo de los saltos.
Dado que en IPv6 no se usa el “broadcast”, los mensajes de RIPv6 se envían a todos los routers y se usa la dirección Multicast Link-local FF02::9.

9.2 OSPFv3

Es usado para distribuir información entre los routers de un sistema autónomo simple, es decir, cada router construye y descubre su topología de red. Está basado en la conservación en la tecnología de estado-enlace y permite que las redes sean agrupadas en lo que se llama “áreas”. Un router mantiene su base de datos donde conserva los participantes de cada área y la topología de un área se oculta para el resto de los sistemas autónomos. Estas áreas constituyen el concepto de “Stateful” que habilita la jerarquía de dos niveles de enrutamiento. OSPF incorpora el soporte para el enrutamiento de los interdominios sin clase (CIDR), cada router tiene un destino y una máscara. OSPF elige la ruta más corta de acuerdo con el ancho de banda.

9.3 IS-IS para IPv6.

Intermediate System - to - Intermediate System (IS-IS). Este enlace de estado es similar al OSPF, pero su terminología e implementación son diferentes. El estado del enlace, el prefijo/máscara del enlace y otros parámetros de conectividad local se anuncian en los paquetes de estado (LSP). Los LSP se intercambian en la capa 2, esto es hace que IS-IS sea menos vulnerable a la suplantación de identidad.

9.4 BGP4+

RFC 4760 (Border Gateway Protocol). - Es un protocolo exterior usado principalmente para conectar dominios separados por routers que contienen políticas independientes (sistemas autónomos). La conexión hacia un proveedor de servicios para acceder a internet es común usar BGP. La versión 4+ es una extensión de este protocolo para soportar IPv4 e IPv6 el cual es más eficiente y flexible.

Capítulo 10. Desarrollo de la Propuesta

En este capítulo no solo se presenta una metodología para guiar al lector a comenzar a revisar qué aspectos se tienen que considerar para iniciar el proceso de adopción de IPv6, sino que se pretende ejemplificar en cada uno de los pasos, los datos, muestreo, diseño, análisis y pruebas sobre un laboratorio a fin de iniciar a incursionar en la búsqueda de una propuesta para sus respectivas redes a cargo.

Se definen perfiles para el caso dentro la red UNAM, que son diferentes a los comerciales, dado que el dimensionamiento es para un ámbito educativo, en el cual no se tienen tantos servicios como la telefonía celular, red IoT, red industrial, etc.

Se desarrolla un laboratorio y se implementa un router shorewall inmerso en ambientes físicos y virtuales para instalar, configurar y probar la conexión en IPv4 e IPv6, lo cual permitirá tener en los anexos técnicos las guías para su implementación.

A través de ese laboratorio se podrá demostrar que las sesiones concurrentes en la red pueden ser atendidas con pocos recursos en hardware y con software de código abierto.

10.1.-Metodología para la Adopción IPv6

Como parte del desarrollo de este trabajo se propone la metodología los pasos a seguir y que se describe en la **figura 24** para comenzar con la adopción dentro de cada unidad educativa de la UNAM, que contempla las mejores prácticas y los pasos que recomienda LACNIC para iniciar con este proceso, una vez que se cuenta con el apoyo de la Dirección de cada entidad.

10.1.1 Capacitación

A fin de apoyar a las áreas de TIC para una rápida adopción del protocolo, se generaron guías y manuales para administradores y usuarios finales de los diferentes sistemas operativos para su configuración y pruebas de conectividad con el direccionamiento IPv6 y el mecanismo de transición Dual Stack, que se pueden consultar en los anexo técnicos de este trabajo (Ver anexo técnico B).

10.1.2 Perfilado de red.

Existen diferentes criterios para realizar un dimensionamiento que defina el consumo de los recursos en red, algunos utilizan el ancho de banda contratado con el ISP, otros el número de usuarios concurrentes en la red, y otros más el conteo de número de componentes de red capa L3 que conforman la red corporativa. En este trabajo se proponen tres perfiles, considerando que la redUNAM, cuenta con más de 369 mil alumnos y 42 mil académicos a nivel nacional [53].

Tabla 16.- Criterios para un perfil para el tamaño de la red [44]

Tipo de red	Ancho de Banda (Mbps)	Número de usuarios	Número de Componentes
Chica	50- 100	entre 1000 y 5000	hasta 1000
Mediana	100-500	más de 5000 hasta 10,000	hasta 2000
Grande	Mayor a 500	de 10,000 hasta 20,000	más de 2000

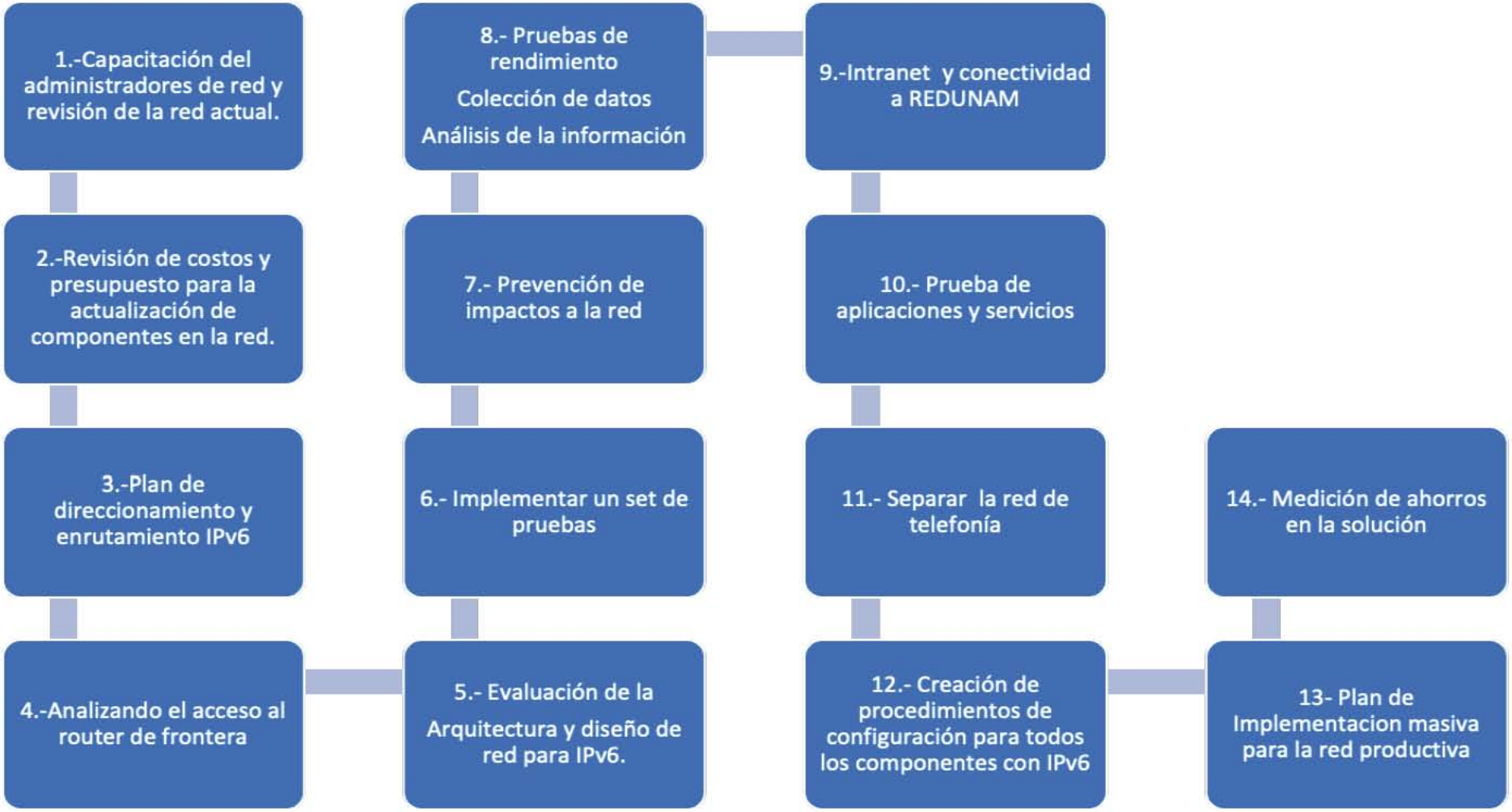


Figura 24.- Metodología propuesta para adopción de IPv6

Fuente: Autor

10.1.2 Revisión de Costos

A continuación se muestra una pequeña investigación de mercado con respecto a los costos de algunas soluciones comerciales y de código abierto que se ofrecen para un perfil mediano, cabe destacar son precios de lista del año 2022, sin impuestos y cotizados en moneda dólar. Se consideraron 3 años de soporte y garantía del equipo de hardware y el software con licenciamiento mínimo. Se trataron de unificar algunos criterios de hardware, dependiendo del fabricante se especifican los diferenciales en software. No se incluye ninguna consultoría u horas de servicios por instalación y configuración de los componentes.

Tabla 15.- Comparativa de soluciones comerciales vs código abierto

Soluciones On Premise*				
Fabricante	**PFSense+**	**VyOS**	**Cisco**	**Fortinet**
Modelo	**Netgate 1541**	**Supermicro SYS-E300-9A**	**ISR 1111X-8P**	**FORTIGATE-200F**
Cores	8	8		
Cores	Intel Xeon® 2.1 GHz	Intel® Atom® processor C3858		
Memoria	DDR4	DDR4-2400MHz		
Memoria	32 GB	hasta 64GB		
Discos	M.2 SSD	SATA 2.5		
Discos	2x256GB	512GB		480GB
Tarjeta Red	4 x 1Gbps RJ45	4 x 1Gbps RJ45	4 x 1Gbps RJ45	4 x 1Gbps RJ45
Tarjeta Red	1	1	2	1
Firewall	10K ACLs	Stateful, NAT		
IPSec VPN	AES-GCM-128 w/QAT	IPsec, VTI, VXLAN, L2TP3, OpenVPN		
L3 Forwarding	IPERF3,IMIX			
Routing		BGP,OSPF,RIPng		
Perfil	Empresa Mediana			

Soporte	3años x **$999**	$1000 x año		
Software	TAC Lite	VyOS Enterprise		
TOTAL (USD)	**$4,696.00**	**$8,000.00**	**$9,011.86**	**$9,615.87**
***Precios de lista 2022 sin IVA y cotizados en dólar**				

10.1.4.- Análisis de acceso al Router de Frontera: Caso Campus Juriquilla

Con apoyo de la Coordinación de Servicios Administrativos del campus de Juriquilla se han logrado analizar el tráfico de entrada y salida del core del campus, a fin de conocer el consumo del ancho de banda sobre el IPv4 de algunas instituciones, para poder establecer qué perfil de red se tiene y desde allí sustentar el tipo de solución que se requiere para transicionar la red actual hacia IPv6.

Población:
Actualmente, el campus cuenta con 11 instituciones universitarias. Su conexión a Internet se realiza a través de dos proveedores ISP diferentes y cuenta con una alta disponibilidad en el core de conexión de este servicio, con un ancho de banda contratado de 750 Mbps (WAN-2 secundario) y uno 750Mbps (WAN1- primario) cada enlace. Se cuenta con una población integrada por alumnos, investigadores, académicos y administrativos de 1500 usuarios.

Muestra:
Se colectó el uso del ancho de banda de los principales enlaces de red del campus Juriquilla, así como el consumo del ancho de banda del core hacía cada instituto en el periodo de 15 días.

Medida:
Se utilizan el máximo y el promedio del ancho de banda por día de entrada y salida de cada instituto y del core.

Dato:
Se monitorea la transferencia de paquetes por segundo. Para mayor detalle ver Anexo técnico G.

En la tabla 17 se establecen, a través del consumo de ancho de banda y la matrícula que se tiene en cada facultad, el tipo de red para permitirnos clasificar cada una de las entidades.

Tabla 17.- Criterios para un perfil en consumo de ancho de banda por facultad

Tipo de red	Promedio de uso del ancho de banda Entrada (Mbps)	Promedio de uso del Ancho de Banda Salida (Mbps)	Ejemplos de entidades Educativas	Total usuarios: alumnos profesores Investigadores y administrativos.
Grande	2.3	38.03	Escuela Nacional de Estudios Superiores (ENES)	461
Grande	9.36	22.06	Centro de Física Aplicada y Tecnología Avanzada (CFATA)	129
Mediana	3.29	5.9	Laboratorio de Investigación en Procesos avanzados- Instituto de Ingeniería(LIPATA)	60
Mediana	6.34	18.02	Instituto de Neurobiología (INB)	264
Chica	5.75	1.44	Instituto de Matemáticas (Tel-Mat)	54
Chica	0.026	0.03	Unidad Multidisciplinaria de Docencia e Investigación de la Facultad de Ciencias (UMDI)	68

Se colectaron varias muestras para analizar estos datos plasmados en la tabla 18, mientras que en la figura 25 y 26 se muestra el consumo máximo promedio del ancho de banda de ambas vías del campus Juriquilla, lo cual nos permite observar que, se genera más tráfico de salida que de entrada. Se consideraron los consumos máximos durante inicio de semestre para considerar los escenarios con mayor demanda en la red.

Figura 25- Gráfica de Consumo Promedio máximo de Ancho de Banda para la Vía Principal del Campus Juriquilla

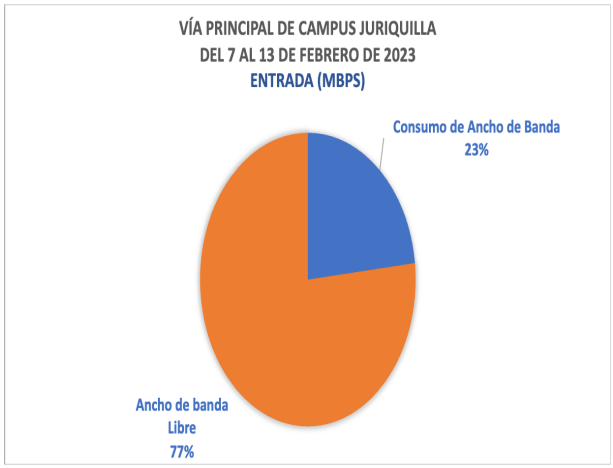
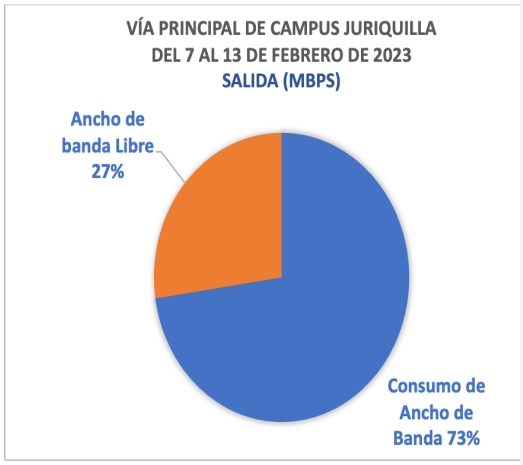
ENTRADA (Mbps)	SALIDA (Mbps)
	

Figura 26.- Gráfica de Consumo promedio máximo de Ancho de Banda para la Vía Alterna del Campus Juriquilla

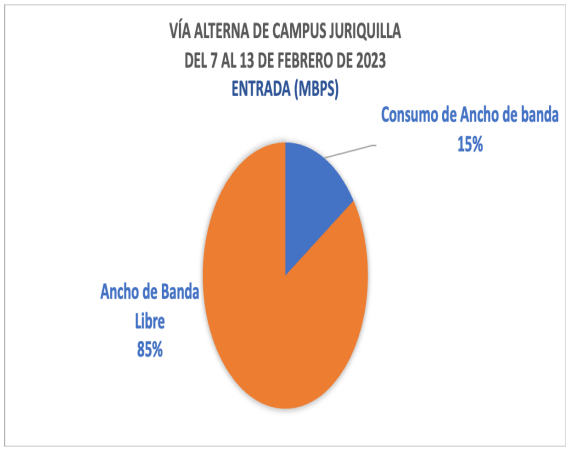
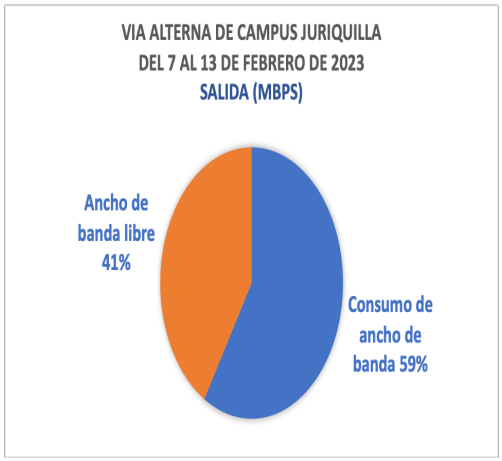
ENTRADA (Mbps)	SALIDA (Mbps)
	

Tabla 18. Consumo del ancho de banda de las vías de acceso hacia el Campus Juriquilla del 7 al 13 de Febrero del 2023

	VIA Principal Ancho de Banda				Via Alterna Ancho de Banda			
	Promedio Entrada(Mbps)	Entrada Máximos (Mbps	Salida Máximos (Mbps	Promedio Salida (Mbps)	Promedio Entrada(Mbps)	Entrada Máximos (Mbps	Salida Máximos (Mbps	Promedio Salida (Mbps)
Consumo	174	350	545	72	116	300	440	5.2
Resto	576	400	205	678	634	450	310	745
Total contratado	750	750	750	750	750	750	750	750
Porcentaje de uso	23%	47%	73%	10%	15%	40%	59%	1%

En la tabla 19, se realizó un muestreo del 7 al 13 de febrero y se clasificó el tipo de red que se tiene en cada instituto y se presenta su consumo de ancho de banda tanto para la entrada como para la salida, observando que algunos institutos como ENES y CFATA generan más tráfico de salida; caso contrario como el Tel-Mat que tiene más tráfico de entrada.

Tabla 19 . Muestreo de Consumo de ancho de Banda de Institutos en Campus Juriquilla del 7 del 13 de febrero

Muestra del 7 al 13 de Febrero			
		Ancho de Banda	
Perfil	Instituto	Entrada(Mbps)	Salida (Mbps)
Grande	ENES	2.300	38.03
Grande	CFATA	9.360	22.06
Mediano	LIPATA	3.290	5.90
Mediano	INB	6.340	18.02
Chico	Tel-Mat	5.750	1.44
Chico	UMDI	0.026	0.03
N/A	Resto de Institutos	89.344	13.850
	Resto del Total Contratado	633.590	650.670

Ahora bien, en el muestro del 21 al 26 de Febrero, en la tabla 20, se muestra otro comportamiento muy diferente al de la tabla 19 en el Instituto CFATA o el INB, y de manera general, se tienen mayor consumo en su ancho de banda.

Tabla 20 . Muestreo de Consumo de ancho de Banda de Institutos en Campus Juriquilla

del 21 del 26 de febrero

Muestra del 21 al 26 de Febrero			
		Ancho de Banda	
Perfil	Instituto	Entrada(Mbps)	Salida (Mbps)
Grande	ENES	3.520	91.78
Grande	CFATA	50.000	54.00
Mediano	LIPATA	1.370	39.78
Mediano	INB	7.050	37.85
Chico	Tel-Mat	6.710	1.40
Chico	UMDI	0.621	0.77
N/A	Resto de Institutos	104.729	95.866

Adicionalmente, se generó un comparativo relativo al porcentaje de uso del ancho de banda relativo al ancho de banda total que se tiene contratado con el ISP en las vías principales (es cual es de 750 Mbps en ambas vías).

En la tabla 21 y 22 se representa el consumo de entrada y salida a nivel campus Juriquilla para la primera muestra del 7 al 13 de febrero.

En la tabla 23 y 24 se representa el consumo de entrada y salida a nivel campus Juriquilla para segunda muestra del 21 al 26 de febrero.

Tabla 21 . Porcentaje de uso del ancho de banda relativo al contratado por Instituto

Muestra del 7 al 13 de Febrero		Porcentaje de uso del ancho de banda relativo al contratado	
Perfil	Instituto	Entrada(Mbps)	Salida (Mbps)
Grande	ENES	0.3%	5%
Grande	CFATA	1%	3%
Mediano	LIPATA	0.4%	1%
Mediano	INB	1%	2%
Chico	Tel-Mat	1%	0.2%
Chico	UMDI	0.004%	0.004%
N/A	Resto de Institutos	24%	4%

Tabla 22 . Porcentaje de uso del ancho de banda relativo al contratado por Instituto

Muestra del 21 al 26 de Febrero		Porcentaje de uso del ancho de banda relativo al contratado	
Perfil	Instituto	Entrada(Mbps)	Salida (Mbps)
Grande	ENES	0.5%	12%
Grande	CFATA	7%	7%
Mediano	LIPATA	0.2%	5%
Mediano	INB	1%	5%
Chico	Tel-Mat	1%	0.2%
Chico	UMDI	0.083%	0.103%
N/A	Resto de Institutos	14%	13%

Tabla 23 . Porcentaje de uso del ancho de banda relativo al consumo total de la muestra del 7 al 13 de Febrero del 2023

Muestra del 7 al 13 de Febrero		Porcentaje de uso del ancho de banda relativo al consumo total	
Perfil	Instituto	Entrada(Mbps)	Salida (Mbps)
Grande	ENES	0.32	5
Grande	CFATA	1.29	3
Mediano	LIPATA	0.45	1
Mediano	INB	0.87	3
Chico	Tel-Mat	0.79	0.2
Chico	UMDI	0.00	0.0
N/A	Resto de Institutos	12.28	1.9

Tabla 24 . Porcentaje de uso del ancho de banda relativo al consumo total de la muestra del 7 al 13 de Febrero del 2023

Muestra del 21 al 26 de Febrero		Porcentaje de uso del ancho de banda relativo al consumo total	
Perfil	Instituto	Entrada(Mbps)	Salida (Mbps)
Grande	ENES	2.97	9
Grande	CFATA	42.24	5
Mediano	LIPATA	1.16	4
Mediano	INB	5.96	4
Chico	Tel-Mat	5.67	0.1
Chico	UMDI	0.52	0.1
N/A	Resto de Institutos	60.19	65.2

10.1.4.1 Resultados

Los consumos de ancho de banda máximos sobre la vía principal del core en el campus Juriquilla que se detallan en el anexo H se presentaron en el horario laboral y derivado de actividades como transmisiones en vivo sobre plataformas de redes sociales de algunos curso y talleres publicados en tiempo real, lo cual generaron elevado tráfico por el servicio de streaming.

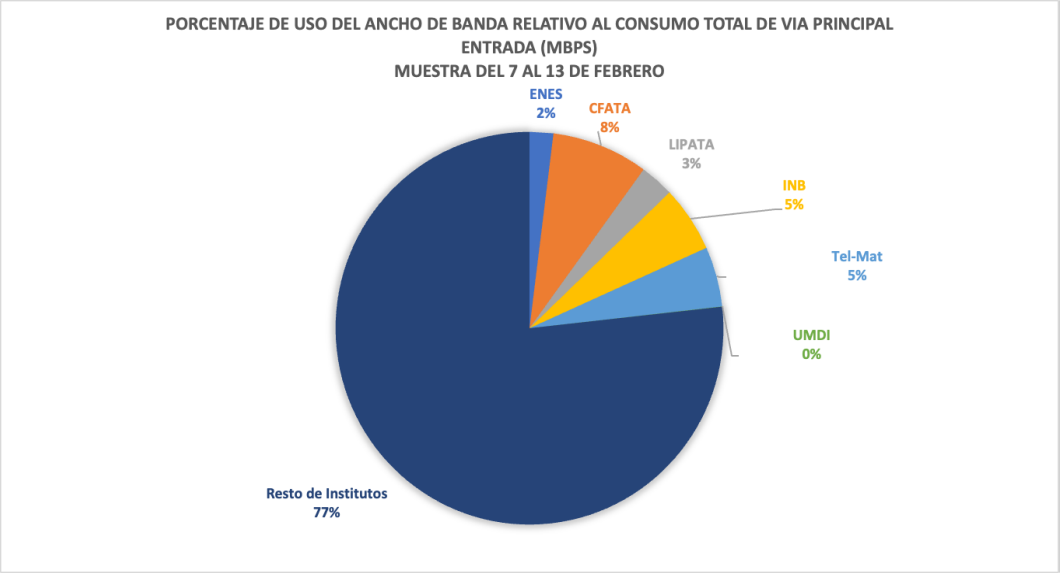
Otro de los mayores consumos de ancho de banda detectados fueron aplicaciones administrativas que explotan bases de datos y conexiones muy específicas para la comunicación con ciudad Universitaria con manejadores de base de datos como mysql y oracle (ver anexo H, Figura 50).

Adicionalmente, los consumos máximos que se mostraron en fin de semana fueron monitoreados y se detectó que es generado por el servicio de respaldo en nube ofrecido por la DGTIC hacia la ENES Juriquilla, para servicios críticos.

Considerando 6 de los 12 Institutos que conforman el campus Juriquilla, en la figura 27 se observa que CFATA, con tan solo 129 usuarios, tiene un consumo de ancho de banda de entrada del 8% del total del consumo del ancho de banda de entrada sobre la vía principal, es decir, realiza más descargas de información que los demás Institutos. En comparación con el instituto ENES con un 22% del consumo de ancho de banda de salida, es decir, genera mayor contenido hacia internet.

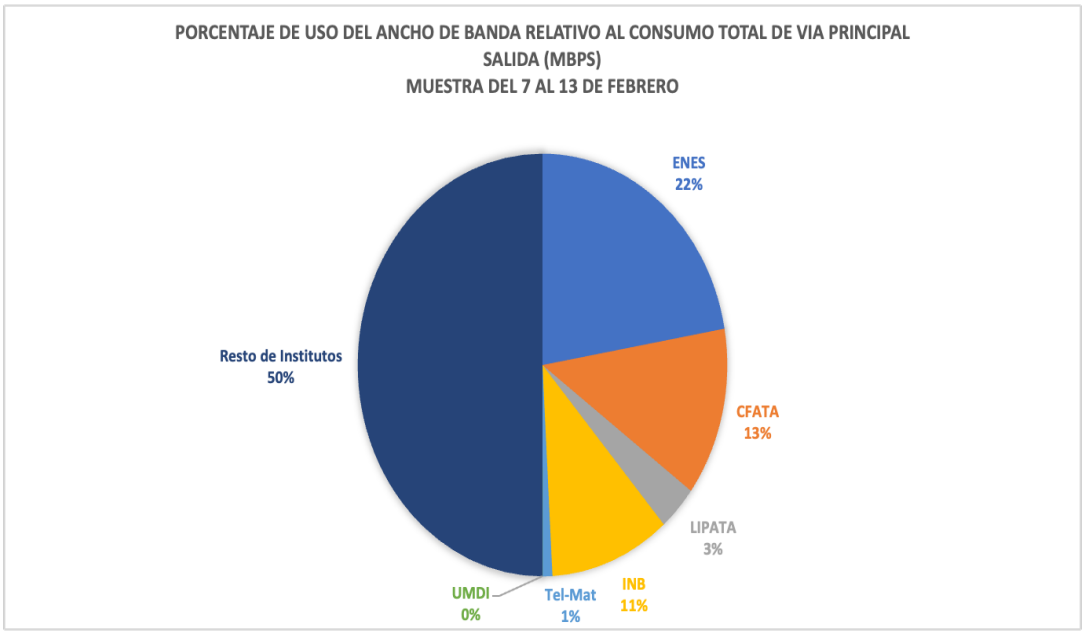
Por tanto, nos permite exponer la importancia de realizar el análisis de varios aspectos de la red como son consumos, usuarios, horarios y tipo de cargas que se presentan en dicha red, para tener un definir el correcto perfil del tamaño de la red.

Figura 27.- Consumo relativo del ancho de banda al consumo total de la entrada de la vía principal del campus Juriquilla. Muestra del 7 al 13 de febrero.



En la figura 28 se puede observar que el consumo del ancho de banda relativo al consumo total del ancho de banda de la salida en la vía principal el mayor porcentaje es para la ENES Juriquilla con el 22%, sin embargo, en la figura 29 la dinámica de consumo cambia y el mayor porcentaje es para CFATA con un 29%.

Figura 28.- . Consumo relativo del ancho de banda al consumo total de la salida de la vía principal del campus Juriquilla. Muestra del 7 al 13 de febrero.



Teniendo en cuenta el consumo total del ancho de banda en la vía principal, tanto de la entrada como de la salida, con respecto al ancho de banda total contratado con el ISP, se generó el consumo proporcional de ancho de banda de cada uno de los institutos, se muestran los resultados en la figura 29 y la figura 30.

Figura 29 . Consumo relativo del ancho de banda al consumo total de la salida de la vía principal del campus Juriquilla. Muestra del 7 al 13 de febrero.

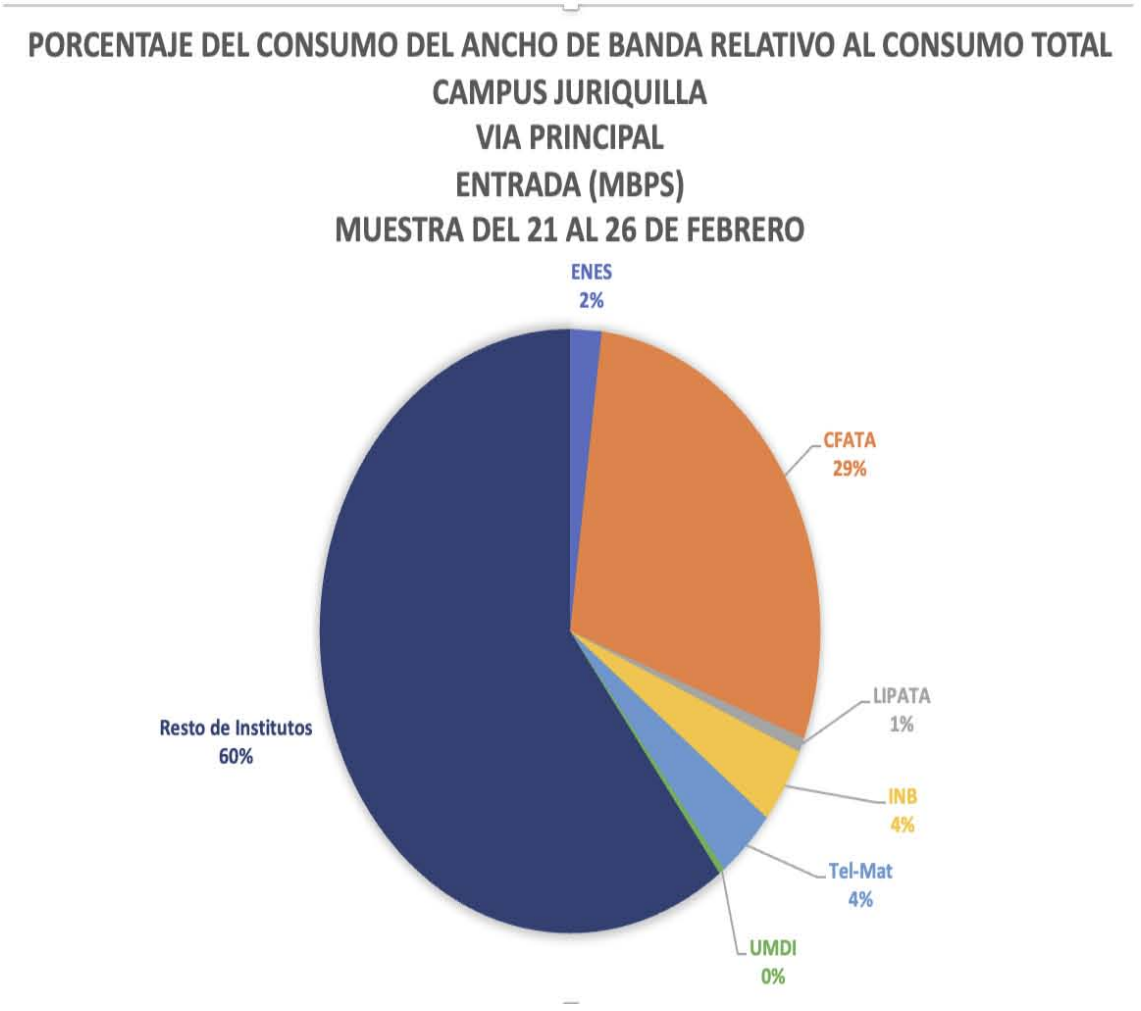
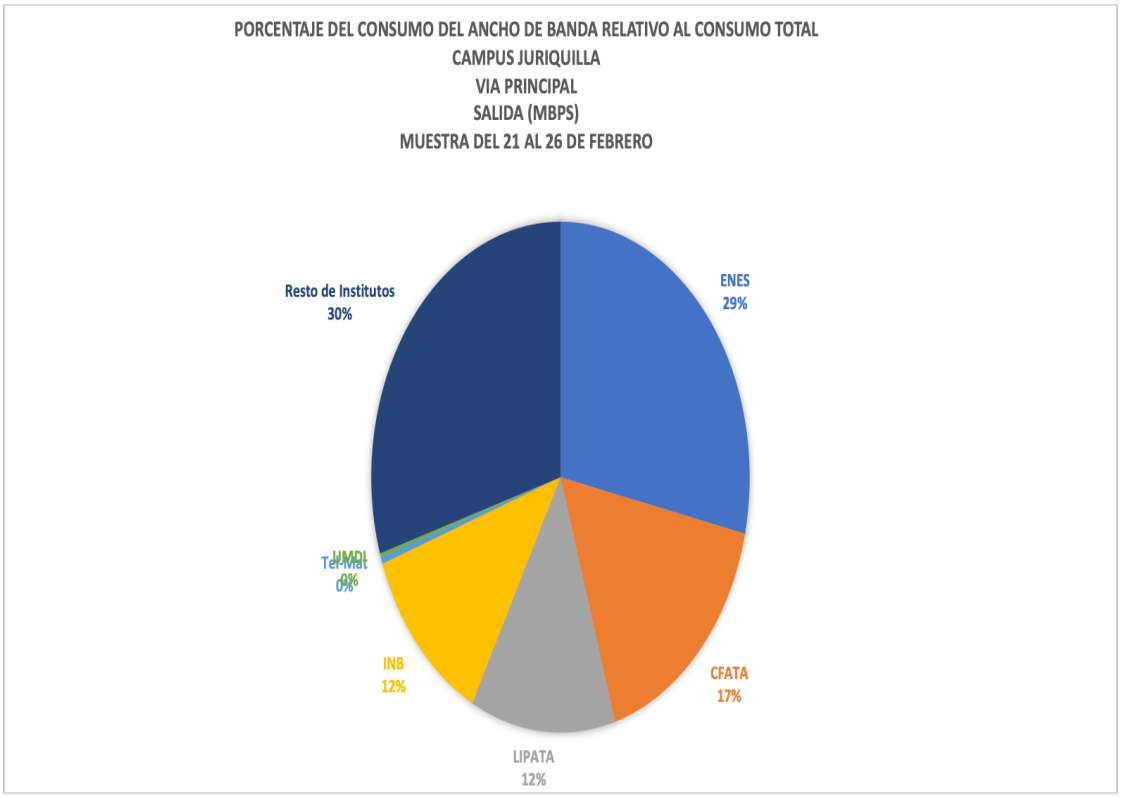


Figura 30 . Consumo relativo del ancho de banda al consumo total de la salida de la vía principal del campus Juriquilla. Muestra del 7 al 13 de febrero.



10.1.5. Evaluación de la Arquitectura y diseño de la red para IPv6

Se ha elegido el mecanismo de transición para IPv6: Dual Stack por la simplicidad y los cambios y configuraciones que se tienen que realizar se pueden hacer de manera gradual, sin realizar grandes afectaciones a la red y los servicios.

En el anexo técnico H figura 49, se muestra el diagrama general de la red del campus Juriquilla, se tomó de referencia para el análisis de las posibles peticiones de usuarios concurrentes que podría presentar un router frontera, ya que para el ICN, no fue posible obtener un monitoreo detallado dado que lo custodia la DGTIC.

El anexo H, ayudará al lector a evaluar la importancia de tener el monitoreo activo y la generación de estas estadísticas históricas para conocer el comportamiento de la red actual, porque se requiere evaluar qué condiciones gestionará sobre la red actual, qué mejoras se podrían realizar.

Otro rubro que se presenta en el apartado 10.5.1 es generalizar los servicios en las redes que puede llegar a tener una área TIC dentro de las entidades de la UNAM.

10.5.1 Servicios de redes en el área TIC

Las áreas TIC dentro de muchas dependencias de la UNAM ofrecen servicios de red. A continuación, en la tabla 25, se realiza una lista general de algunos de los más comunes de estos servicios, a fin de poder tener un contexto para los criterios de direccionamiento de red que se tendría que cubrir.

Tabla 25 .- Servicios de Red

Grupo	Servicio
1	Red para telefonía IP
2	Red para Video (vigilancia)
3	Red Interna por Edificio
4	Red administrativa TIC

Tabla 25 .- Servicios de Red

Grupo	Servicio
5	Red de Respaldos
6	Red Inalámbrica
7	Red Invitados
8	Red Servicios Públicos
9	Red Pruebas
10	Red Desarrollo
11	DMZ (Servidores)
12	Conexión backbone / Infraestructura de Red
13	Futuro Servicio (Crecimiento)
14	Futuro Servicio (Crecimiento)
15	Futuro Servicio (Crecimiento)
16	Futuro Servicio (Crecimiento)

Un ejemplo de la diversidad de estos servicios es el ICN, el cual tiene a su cargo la administración de la red de 8 edificios, independiente de su respectivo centro de datos. Por ello se describen en la tabla 26 los requerimientos de red para cada uno de ellos, así como los perfiles de los usuarios a los que atienden (Académicos, Investigadores, Administrativos, Alumnos).

El ICN necesita cubrir las necesidades de direccionamiento IPv6 para el enrutamiento para su red frontera, red de distribución y la red de acceso, este rubro se ha considerado dentro de la tabla 25 en el grupo 12.

10.1.5.2 Plan de direccionamiento teórico

Contexto:

La Universidad actualmente cuenta con 2 mil 207 edificios, 4,613 Aulas, 4,266 cubículos y 3,213 laboratorios/talleres,18 recintos históricos y 27 museos; además, de 136 bibliotecas y con 90,987 computadoras propiedad de la UNAM y 202,333 cuentas para red inalámbrica [54], sin considerar los celulares conectados a la red de la UNAM; tan solo el campus de ciudad universitaria cuenta con más de 50 edificios.

Se integran dependencias como 17 planteles de bachillerato (Preparatorias y CCHs), 6 Campus: Aragón, Acatlán, Iztacala, Cuautitlán dentro del área metropolitana, y se requiere proporcionar servicio de red a las sedes foráneas en Baja California, Chiapas, Querétaro, Michoacán, Guanajuato, Guerrero, Jalisco, Morelos, Puebla, Quintana Roo, Sinaloa, Sonora, Veracruz, Oaxaca[54]; y si agregamos todos los dispositivos móviles que acceden a la red UNAM por 369,607 alumnos, 42,535 académicos y 5430 investigadores.

También cuenta con entidades Internacionales en EUA, Canadá, España, China, Costa Rica, Francia, Inglaterra, Alemania y Suiza.

Considerando las estadísticas generales presentadas en la UNAM descritas en párrafos anteriores, se presenta en la tabla 26 la propuesta teórica para la distribución de los prefijos [52] por jerarquía y niveles a nivel Red UNAM (ver tabla 26).

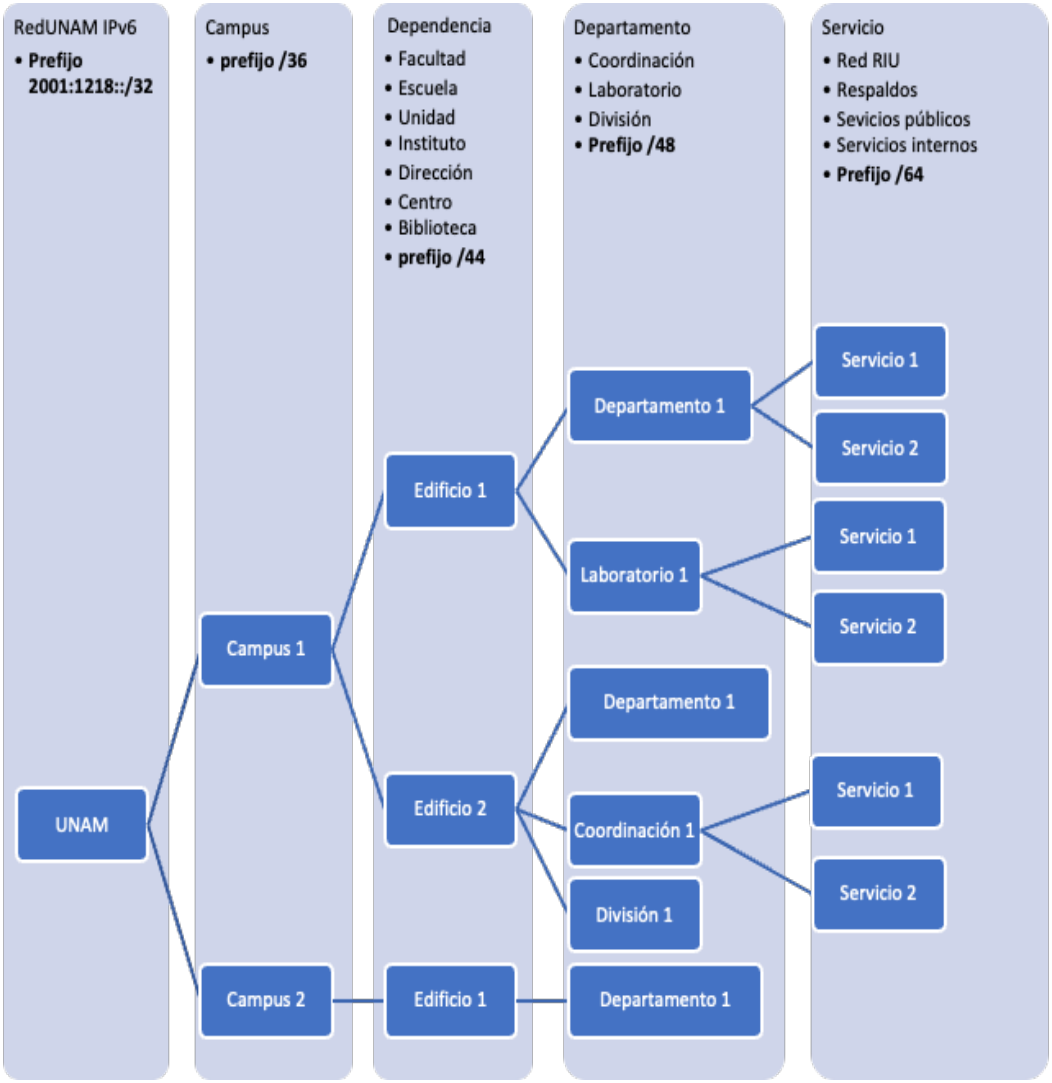
Tabla 26 .- Prefijos ***teóricos*** sugeridos

Prefijo	Tipo Red	Organización	Número de Redes	Detalle
/32	ISP	UNAM	4,294,967,296 redes de /64	Prefijo asignado por NIC-MX
/36	Grande	Campus	16 redes de /36	Prefijo asignado por DGTIC
/40	Mediana	Dependencia	16 redes de /40	
/48	Pequeña	Departamento	256 redes de /48	

/64		Servicios	1 subred (2^{64}=18,446,744,073, 709,551,616 direcciones)	
/127	N/A	ruteo	cuatro direcciones	conexión entre routers
/126	N/A	punto a punto	dos direcciones	Conexión punto a punto para equipo sin soporte de /127

Para el primer nivel de subred se asignan prefijos (/36) para los diversos campus con los que cuenta la UNAM; para el segundo nivel se asignan prefijos /40 para los edificios o dependencias que conforman cada campus; el tercer nivel se consideran prefijos /48 para los departamentos y cubículos que integran ese edificio y finalmente se divide por los tipos de servicio que se ofrecerán con un prefijo /64.

Figura 31.- Jerarquía simple de la red universitaria UNAM



Se consideran los diferentes servicios que se ofrecen y los crecimientos a futuro, la distribución geográfica y sus posibles crecimientos dentro de los campus universitarios, así como el número de usuarios y dispositivos a cubrir.

Cabe destacar que este direccionamiento **teórico** está basado en las recomendaciones de LACNIC, sin embargo, la única entidad reguladora dentro de la UNAM para determinar el direccionamiento de red es DGTIC, quien actualmente maneja otros criterios para la asignación del direccionamiento de red, ya que al ICN se le ha asignado un bloque /56, y para la conexión algunos campus se ha otorgado bloques /48.

Una vez asignado el prefijo por DGTIC, tomando en cuenta el número de edificios con el que cuenta el ICN, los servicios que requiere cubrir y asignando un rango para crecimientos futuros y/o servicios adicionales, se puede comenzar a asignar un direccionamiento IPv6 teórico. Además se consideraron los perfiles que se definieron previamente.

A continuación en la tabla 27, se muestra un ejemplo desarrollado con el prefijo de documentación IPv6 de cómo realizar la asignación de direcciones IP siguiendo las recomendaciones de NIST [11] y LACNIC [55] para realizar la creación de subredes internas.
Teniendo el prefijo asignado de la RedUNAM y cómo se manejaría las subredes para crear una jerarquía y subcategorías para poder mapear las diversas subdependencias, edificios y servicios que tiene el ICN y el campus Juriquilla.

Tabla 27 . Asignación Teórica y subredes de prefijo IPv6 para red ICN y Campus Juriquilla

	ICN	Campus Juriquilla
Prefijo asignado a RedUNAM	2001:DB8::/32	
Prefijo Asignado al Campus:	2001:DB8:8000::/36	2001:DB8::/36
Prefijo Asignado al Instituto:	2001:0db8::/40	2001:0db8:2000::/40
total de Subredes para dependencias del Instituto	16 subredes de /40	16 redes de /44
Rango inicial de Subredes para Dependencias	2001:db8:1000::/64	2001:db8:2000::/44
Rango final de Subredes para Dependencias	2001:db8:1000:ff00:/64	2001:db8:20f0::/44
total de Subredes para Edificios	256 subredes de /48	16 subredes de /48
Rango inicial de Subredes para Servicios	2001:db8:1000::/64	2001:db8:2000::/48
Rango final de Subredes para Servicios	2001:db8:1000:f0::/64	2001:db8:20ff::/48
Total de subredes por Servicio	65536 subredes de /64	256 subredes de /56
Rango inicial de Subredes	2001:db8:1000::/64	2001:db8:2000::/56
Rango final de Subredes	2001:db8:1000:ff::/64	2001:db8:20ff:ff00:/56

En la tabla 28, se presenta otro ejemplo de distribución de direccionamiento IPv6 para la subred que se tendría en primer nivel de la redUNAM con un prefijo /36.

Finalmente describe en la tabla 29 un ejemplo global donde se considera de la red Internacional, la red de interconexión de todos los campus, la red de preparatorias y CCHs, así como la red estatal (presencia en los 32 estados con diversas Instituciones y Unidades de investigación), ya considerando una reserva para el crecimiento a futuro de redUNAM.

Tabla 28 . Propuesta teórica de la asignación y subredes de prefijo IPv6 para los Campus de Red UNAM

	Campus:	Ejemplo:
1	Ciudad Universitaria	**2001:DB8:1000::/36**
2	Iztacala	2001:DB8:2000::/36
3	Acatlan	2001:DB8:3000::/36
4	Iztacala	2001:DB8:4000::/36
5	Cuautitlan	2001:DB8:5000::/36
6	Aragón	2001:DB8:6000::/36
7	Juriquilla Qro	2001:DB8:7000::/36
8	Cuernavaca, Morelos	2001:DB8:8000::/36
9	Morelia, Michoacan	2001:DB8:9000::/36
10	Red Internacional	2001:DB8:a000::/36
11	Red Preparatorias	2001:DB8:b000::/36
12	Red Estatal	2001:DB8:c000::/36
13	Reserva	2001:DB8:d000::/36
14	Reserva	2001:DB8:e000::/36
15	Reserva	2001:DB8:f000::/36
16	Reserva	2001:DB8:0000::/36

Actualmente para la red internacional, el área de DGTIC tiene diversos tamaños de bloques, algunos como en Francia de /32, EUA con /28, Colombia con bloques /48, Inglaterra con bloque /24 [4].

Tabla 29 . Ejemplo de Asignación y subredes de prefijo IPv6 para la red Internacional en la RedUNAM.

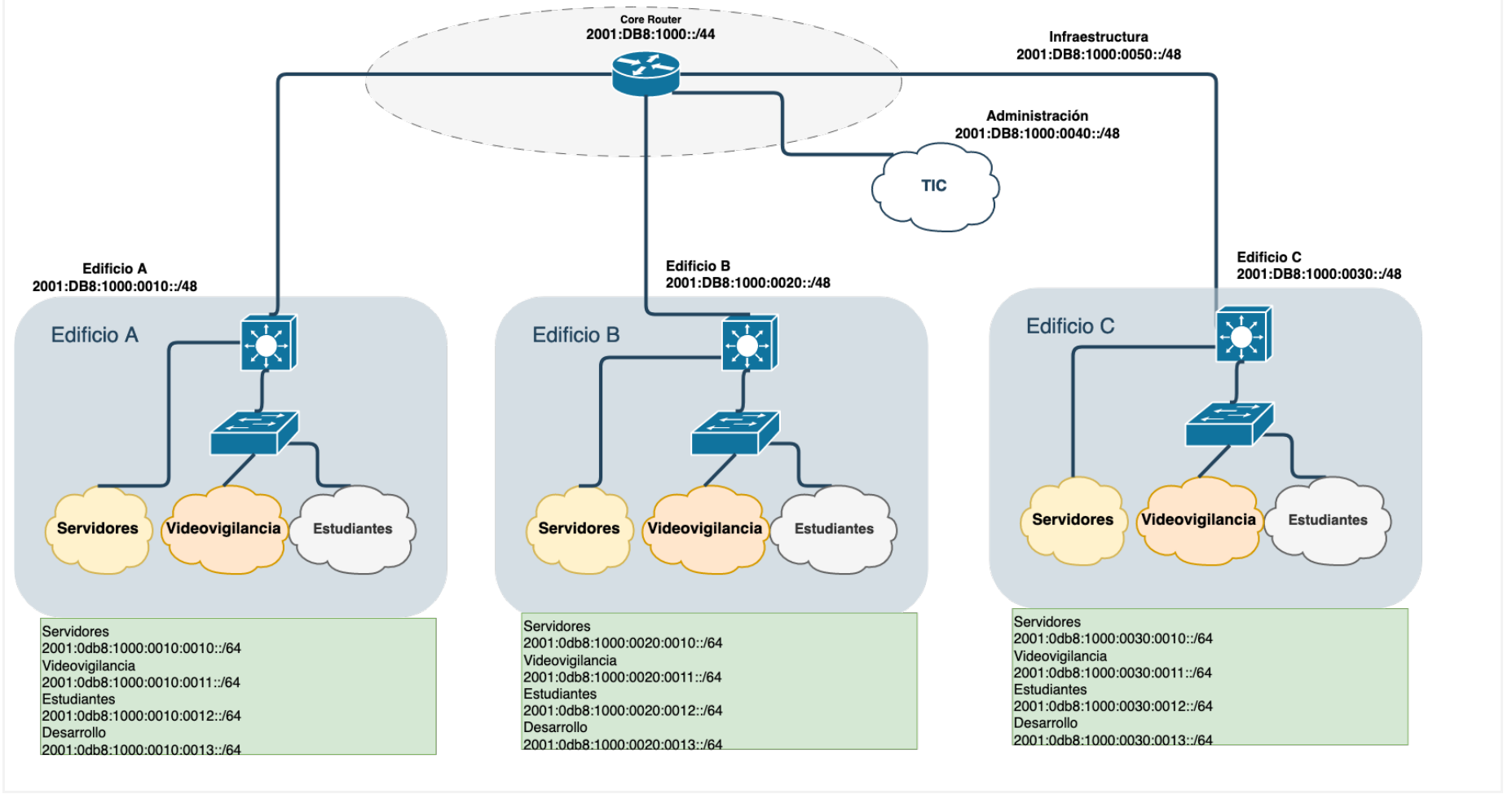
	Red Internacional	Ejemplo:
1	UNAM México	2001:DB8:a000::/40
2	UNAM San Antonio USA	2001:DB8:a100::/40
3	UNAM Canadá	2001:DB8:a200::/40
4	UNAM Chicago	2001:DB8:a300::/40
5	UNAM Los Ángeles - USA	2001:DB8:a400::/40
6	UNAM Seattle -USA	2001:DB8:a500::/40
7	UNAM China	2001:DB8:a600::/40
8	UNAM España	2001:DB8:a700::/40
9	UNAM Costa Rica	2001:DB8:a800::/40
10	UNAM Francia	2001:DB8:a900::/40
11	UNAM Reino Unido	2001:DB8:aa00::/40
12	UNAM Tucson	2001:DB8:ab00::/40
13	Reserva	2001:DB8:ac00::/40
14	Reserva	2001:DB8:ad00::/40
15	Reserva	2001:DB8:ae00::/40
16	Reserva	2001:DB8:af00::/40

Por otro lado, el ICN maneja 11 edificios actualmente y se le ha asignado un bloque /56 y para LAMOD un bloque de /48 por parte de DGTIC.

Tabla 30 . Asignación teórica y subredes de prefijo IPv6 para la red del Instituto de Ciencias Nucleares

	Prefijo Base:	16 subredes para cada Edificio	
	2001:0db8:2000:0000:0000:0000:0000:0000/56	Rango inicial de Subredes	Rango final de Subredes
1	Edificio A	2001:db8:1000:0010::/60	2001:0db8:2000:0000:0000:0000:0000:0000/60
2	Edificio B	2001:db8:1000:0020::/60	2001:0db8:2000:ff10:0000:0000:0000:0000/60
3	Edificio C	2001:db8:1000:30::/60	2001:0db8:2000:ff20:0000:0000:0000:0000/60
4	Edificio D	2001:db8:1000:40::/60	2001:0db8:2000:ff30:0000:0000:0000:0000/60
5	Edificio E	2001:db8:1000:50::/60	2001:0db8:2000:ff40:0000:0000:0000:0000/60
6	Edificio F	2001:db8:1000:60::/60	2001:0db8:2000:ff50:0000:0000:0000:0000/60
7	Edificio G	2001:db8:1000:70::/60	2001:0db8:2000:ff60:0000:0000:0000:0000/60
8	Edificio H	2001:db8:1000:80::/60	2001:0db8:2000:ff70:0000:0000:0000:0000/60
9	Edificio I	2001:db8:1000:90::/60	2001:0db8:2000:ff80:0000:0000:0000:0000/60
10	Edificio J	2001:db8:1000:a0::/60	2001:0db8:2000:ff90:0000:0000:0000:0000/60
11	Edificio K	2001:db8:1000:b0::/60	2001:0db8:2000:ffa0:0000:0000:0000:0000/60
12	crecimiento	2001:db8:1000:c0::/60	2001:0db8:2000:ffb0:0000:0000:0000:0000/60
13	crecimiento	2001:db8:1000:d0::/60	2001:0db8:2000:ffc0:0000:0000:0000:0000/60
14	crecimiento	2001:db8:1000:e0::/60	2001:0db8:2000:ffd0:0000:0000:0000:0000/60
15	crecimiento	2001:db8:1000:f0::/60	2001:0db8:2000:ffe0:0000:0000:0000:0000/60
16	Reserva	2001:db8:1000::/60	2001:0db8:2000:fff0:0000:0000:0000:0000/60

Figura 32.- Distribución **Teórica** de Direccionamiento de Red IPv6 para una Dependencia de la UNAM



En la siguiente figura se ejemplifica el alcance del ámbito de cada red, con su respectiva segmentación de red.

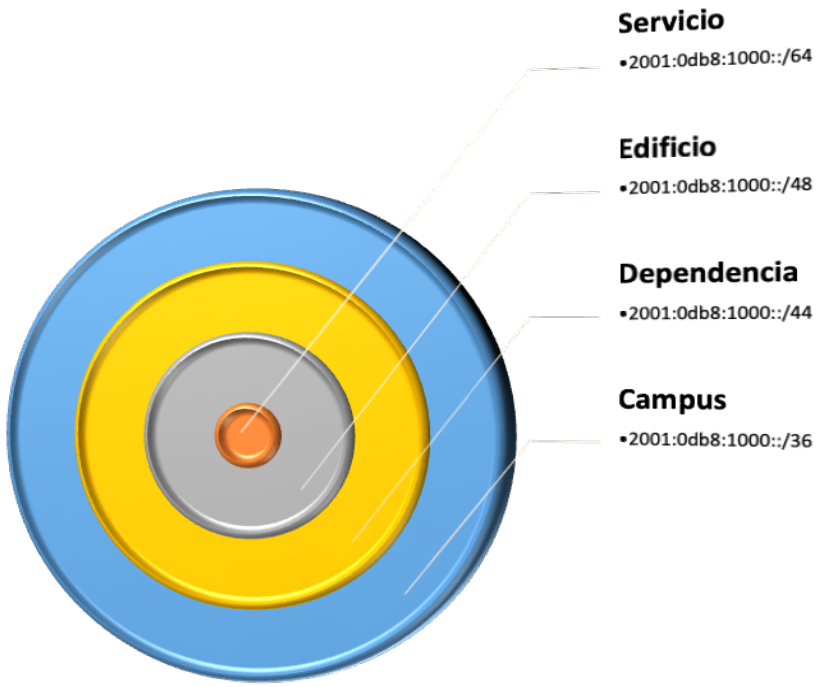


Figura 33.Rangos de subred en un campus de la red UNAM

Fuente: Autor

Tabla 31 . Ejemplo de Asignación teórica y subredes de prefijo IPv6 hasta 256 Institutos del Campus 1

Campus CU	Ejemplo:
ICN	**2001:db8:1000::/44**
Facultad Ingeniería	2001:db8:2000::/44
Facultad de Ciencias	2001:db8:3000::/44
Arquitectura	2001:db8:4000::/44
Quimica	2001:db8:5000::/44
Derecho	2001:db8:6000::/44
Filosofia y Letras	2001:db8:7000::/44
Medicina	2001:db8:8000::/44

10.1.6. Implementar una matriz de Pruebas

En la figura 34 se ha generado un diagrama de red a fin de simular la conexión entre diferentes edificios administrados por el ICN. Cada edificio tiene designado un segmento de red tanto en IPv4 como en IPv6. A partir de esta sección será la base para poder establecer una matriz de pruebas de conectividad entre dichos edificios.

10.1.6.1 Topología

Se ha generado el siguiente laboratorio de pruebas: tiene solo un puerto de red asignado al laboratorio a fin de disponer con los recursos mínimos para mostrar flexibilidad del software Shorewall montado sobre un sistema operativo Linux (Ubuntu, sin embargo, es multiplataforma). Los recursos en hardware son los que se describen en la tabla 32 y el software utilizado se describe en la tabla 34.

Tabla 32.- Recursos de hardware utilizados en laboratorio Shorewall

Recurso	Capacidad
Memoria	64Gb
Disco	1x 500GB para sistema Operativo 1x 2TB para máquinas Virtuales
Procesador	8 Cores (AMD Opteron (TM) Processor 6212)
Tarjeta de Red	Broadcom Inc. and subsidiaries NetXtreme II BCM5709 Gigabit Ethernet

Tabla 33.- Software utilizado en laboratorio Shorewall

Recurso	Software	Versión
Sistema operativo	Ubuntu	22.04.2 LTS (Jammy Jellyfish)
Hypervisor	KVM	8.0.0
DNS	DNSmasq	2.86-1.1
Firewall	Shorewall	shorewall-core: 5.2.3.4 shorewall: 5.2.3.4 shorewall6: 5.2.3.4
Monitoreo	CBM	cbm 0.3.2
Monitoreo	nmon	nmon versión 16n
	MTR	mtr 0.95

Tabla 34.- Recursos de hardware utilizados en pruebas de rendimiento: Cliente

Recurso	Capacidad
Memoria	16Gb
Disco	1x 75 GB para sistema Operativo

Procesador	8 Cores (Quad-Core AMD Opteron(tm) Processor 2350 1000 MHz
Tarjeta de Red	Broadcom Inc. and subsidiaries NetXtreme BCM5721 Gigabit Ethernet PCI Express (rev 21)

Tabla 35.- Software utilizado en pruebas de rendimiento: Cliente

Recurso	Software	Versión
Sistema operativo	Ubuntu	"20.04.6 LTS (Focal Fossa)"
HTTP	Apache/2.4.41 (Ubuntu)	2023-10-26T13:54:09
iperf	Iperf2	version 2.0.13 (21 Jan 2019)
	iperf3	iperf 3.7 (cJSON 1.5.2)

El software Shorewall se ha configurado para que ofrezca el servicio de DNAT en el segmento IPv4, sin embargo para IPv6 no es necesario tener esta configuración. El servicio de firewall, tiene la posibilidad de configurar el ruteo, túneles, integración con soluciones de contenedores, manejo de VPNs, IPSec, etc, es decir, es escalable.

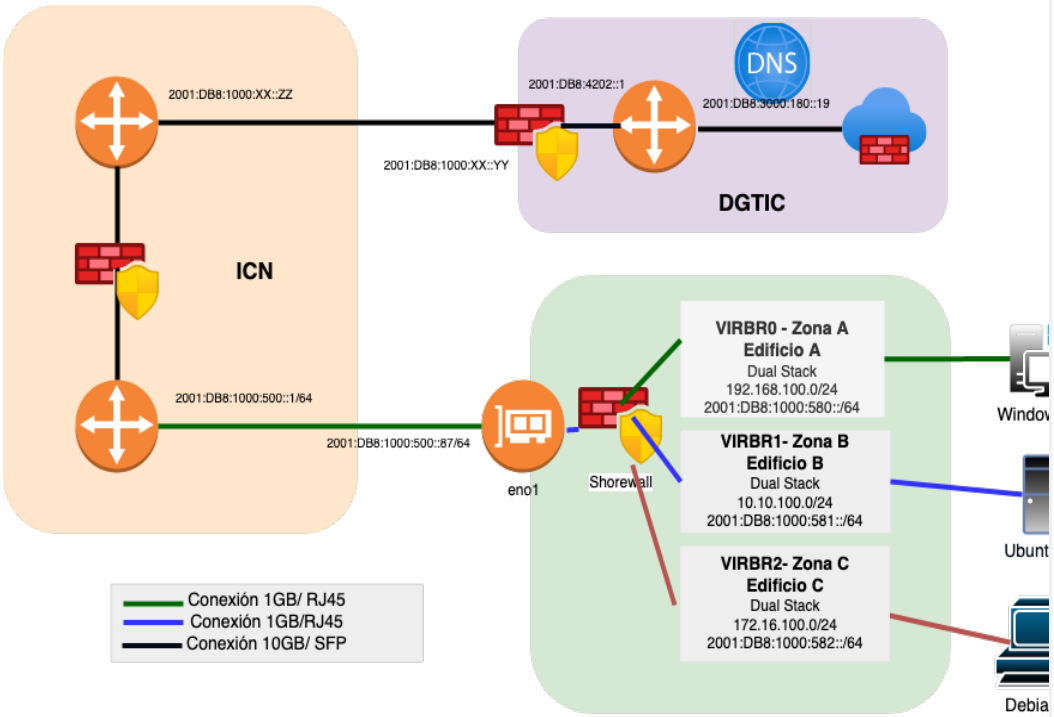


Figura 34.- Topología de Red para laboratorio de pruebas

En este laboratorio, se desactivo el método SLAAC para la asignación de dirección IP y se utilizó el método manual por asignación, se conservó el último dígito de IPv6 igual al último dígito asignado en IPv4, a fin de tener un orden para la implementación del método de Transición Dual Stack.

Por designación del departamento de telecomunicaciones, DGTIC administra los diferentes segmentos de red dentro del campus de ciudad universitaria a través de rutas estáticas conocidas y establecidas en cada entidad educativa. Por tanto, se crearon reglas de ruteo, a fin de poder controlar la comunicación entre las diferente zonas de seguridad, que representarán los dispositivos L2 de los edificios a administrar.

10.1.6.2 Configuración

Definición

Se definen tres zonas para el área de red para trabajar en el laboratorio de pruebas, a fin de simular las tres zonas que se tendría por cada edificio. Se asignan segmentos de red IPv4 e IPv6, conforme se describe en la Tabla 36.

Tabla 36.-Configuración del Laboratorio

Zona	Propósito	Descripción	Dirección IPv4	Dirección IPv6
Fw	Red	Área para el filtrado de paquetes	N/A	N/A
Net	Red Externa acceso a Internet	Representa el gateway para IPv4 y para IPv6, las direcciones son asignadas directamente al puerto de red que da salida a Internet, a través de direcciones públicas.	132.248.29.0/24	2001:DB8:1000:500::87/64
Zona A	Red Interna para servicios de Edificio A	Representa la red interna que ofrecerá todos los servicios para el edificio A del Instituto. Se generó una interfaz virtual con direccionamiento de IP privadas y servicio de dhcpv4 y dhcpv6	192.168.100.0/24	2001:DB8:1000:580::0/64
Zona B	Red Interna para servicios de Edificio B	Representa la red interna que ofrecerá todos los servicios para el edificio B del Instituto. Se generó una interfaz virtual con direccionamiento de IP privadas y servicio de dhcpv4 y dhcpv6	10.10.100.0/24	2001:DB8:1000:581::0/64
Zona C	Red Interna para servicios de Edificio C	Representa la red interna que ofrecerá todos los servicios para el edificio C del Instituto. Se generó una interfaz virtual con direccionamiento de IP privadas y servicio de DHCPv4 y DHCPv6	172.16.100.0/24	2001:DB8:1000:582::0/64
Zona D	Red Interna servicios de Edificio D	Representa la red externa para el edificio D del Instituto. Se generó una interfaz virtual con direccionamiento de IP privadas y servicio de DHCPv4 y DHCPv6	10.10.101.0/24	2001:DB8:1000:5823::0/64
Zona E	Red Interna	Representa la red externa	192.168.101.0/24	2001:DB8:1000:582::0/64

	servicios de Edificio E	que ofrecerá todos los servicios para el edificio E del Instituto. Se generó una interfaz virtual con direccionamiento de IP privadas y servicio de DHCPv4 y DHCPv6		

El firewall se configuró dentro del hipervisor KVM (ver anexo E) y dado que se está usando un bridge es necesario tener otro firewall (en este caso fue ufw) dentro de la máquina virtual para realizar el filtrado de paquetes dentro de la red local para su salida a internet, ya que solo se envian dentro del KVM. Se requiere establecer reglas básicas dentro de la configuración del firewall para asegurar que los siguientes servicios sean accesibles:

- SSH.
- HTTP/HTTPS.
- ICMP.
- Traceroute.
- Servicio de DNS.

10.1.6.3 Plan de Pruebas de conectividad

El plan de pruebas de conectividad de manera general para toda la red institucional implica definir diferentes soluciones con los mecanismos de transición descritos previamente en este documento; En la tabla 37, se describe los tipos de pruebas de conectividad y la solución propuesta la cual depende de los servicios de acceso a internet que tenga el ISP.

Tabla 37.- Plan de Pruebas en base al acceso de ISP

Prueba	Red Interna	Acceso ISP	Destino	Solución Propuesta
1	IPv4	IPv4	IPv4 Internet	NAT44
2	**IPv4 / IPv6**	**IPv6**	**IPv4 Internet**	**Dual Stack con NAT44**
3	IPv4 / IPv6 **	IPv4	IPv6 Internet	6RD

4	IPv4**	IPv6	IPv4 Internet	NAT64
** NOTA: Estas pruebas se sugieren cuando hay un ISP con IPv4/IPv6				

Ahora bien, para realizar las pruebas de conectividad dentro del laboratorio creado para este trabajo de tesis, es necesario definir diferentes niveles de comunicación de las zonas creadas.
Se propone la siguiente tabla de pruebas donde se establecen los objetivos a alcanzar dentro de la conexión de red. Se realizan a través de comandos y herramientas sencillas.

Tabla 38.- Plan de Pruebas para el laboratorio.

Prueba	Objetivo	Acceso con:	Destino	Mecanismo de prueba

1	Desde la red Interna: Conexión de IP privada IPv4	IPv4	IPv4 Internet	Conexión hacia GW interno zona A
				
				PC en zona A:
				`#ping -4 10.10.100.1`
				`#dig 132.248.10.2 10.10.100.1`
				
				PC en zona A hacia GW Externo:
				`#ping -4 132.248.248.87`
				`#dig 132.248.10.2`
				`132.248.29.254`
				
				PC en zona A hacia GW Externo:
				`#ping -4 132.248.248.254`
				`#dig 132.248.10.2 10.10.100.1`
				
				PC en zona A hacia IPv4 Internet:
				`#ping -4 google.com.mx`

2	Desde la red de servicios : Conexión de IP pública IPv4	IPv4	IPv4 Internet	Conexión de red interna hacia unam.mx
3	Desde la red de Invitados: Conexión IPv4/ IPv6	IPv6	IPv4 Internet	Conexion de red Interna IPv6 hacia unam.mx

4	Desde la red Interna: Conexión IPv6	IPv6	IPv6 Internet	Conexión Interna IPv6 hacia el laboratorio por red IPv6

10.1.6.8.- Prueba de rendimiento

Para la prueba de rendimiento para las conexiones sobre la red con IPv4 e IPv6 se cambia la arquitectura utilizada (ver figura 35), dado que se elimina el ambiente virtual y se maneja un esquema bare metal directamente. Para la medición y monitoreo del comportamiento de los componentes físicos utilizaremos dos herramientas: NMON e iperf en sus diferentes versiones para soporte de IPv4 e IPv6.

Herramienta NMON

Es una herramienta de código abierto[66] (excepto para AIX) de monitoreo para el hardware, permite visualizar estadísticas a través del sistema operativo (Linux, Unix) ya sea de modalidad interactiva o en almacenamiento histórico. Junto con otras herramientas alternas para leer esos registros en hojas de cálculos como nmon analyzer, nmon visualizer, nmon consolidator,nmonchart,etc.

Herramienta IPERF

Es una herramienta de código abierto[58] que permite tener un informe de las métricas de la capa de enlace para la red, la cual permite detectar problemas de rendimiento para los administradores de TI. Permite realizar la medición del rendimiento del ancho de banda a través de dos protocolos TCP y UDP.

Objetivo

El objetivo de la prueba es obtener el máximo número de conexiones sostenidas en la arquitectura descrita en la figura 35. Se tiene un cliente iperf que estarán haciendo peticiones a un Servidor iperf, dicho tráfico será administrado por el firewall shorewall y se podrá medir el consumo de recursos que se utiliza durante la prueba.Adicionalmente se podrá medir el tráfico entrante hacia las interfaces de conexión hacia el router.

Metodología

En la figura 35 se muestra el diseño de la red utilizada en dicha prueba con un ancho de banda de 1024 Mbps.

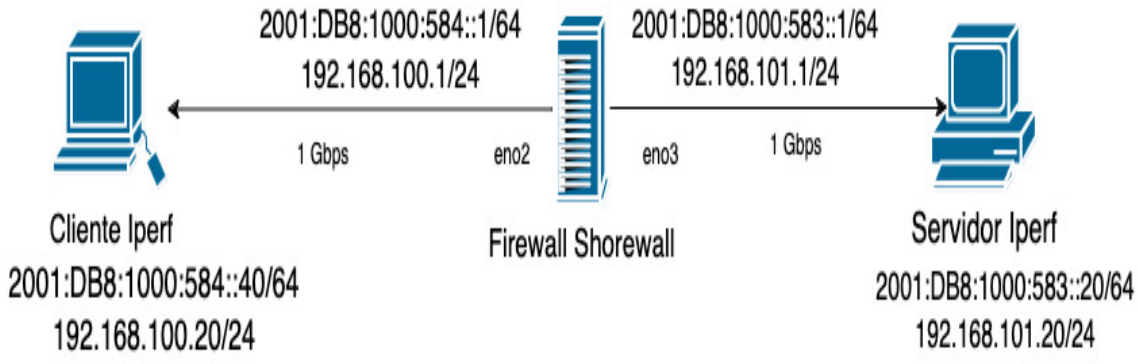


Figura 35.- Arquitectura para pruebas de rendimiento.

Fuente: autor

Para poder generar las métricas mencionadas previamente utilizarán los protocolos TCP y UDP sobre los protocolos IPv4 e IPv6 (Ver tabla 39).

10.1.6.8.1.Métricas para Rendimiento

Tabla 39.- Métricas para rendimiento

Métrica	Descripción	Importancia
Throughput (bits/sec)	Capacidad de transmitir datos exitosamente ya sea bits por segundo o paquetes por segundo de una interfaz a otra interfaz durante un periodo de tiempo.	Para IPv4 el MTU es de 1500, mientras que para IPv6 el MTU es de 9000.
Ancho de Banda(bits/sec)	Define qué tan rápido un dispositivo puede transmitir datos sobre un canal de comunicación.	Es fundamental tener el correcto ancho de banda para la calidad y la velocidad de comunicación en la red.
Latencia(ms)	Tiempo de retardo en una transmisión.	Se percibe como un tiempo de respuesta y lo deseable es que no haya tiempos de ocio en el sistema.
Jitter (ms)	Es una medida de la variación en el intervalo de tiempo de llegada de un paquete, el cual se manifiesta en la calidad de la transmisión.	Esta variación genera un retardo en los paquetes que se transmiten y los paquetes que se reciben y puede darse por una congestión en la red, o un bajo rendimiento en los dispositivos involucrados en la comunicación.

10.1.6.8.2 Matriz de pruebas para el laboratorio

Se utilizó la herramienta de código abierto iperf[58] que funciona en una modalidad cliente-servidor permite medir el máximo ancho de banda en redes tanto IPv4 como IPv6, a través de paquetes UDP y TCP. en comunicación unidireccional y bidireccional. Es necesario configurar los puertos en el firewall que se usarán en la prueba (en el ejemplo usamos 7575).

Tabla 40.- Matriz de pruebas para el laboratorio

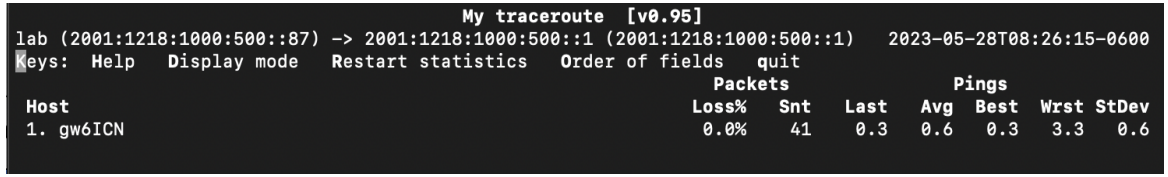
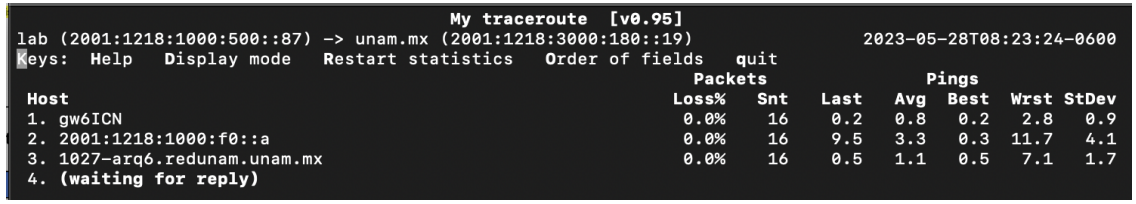
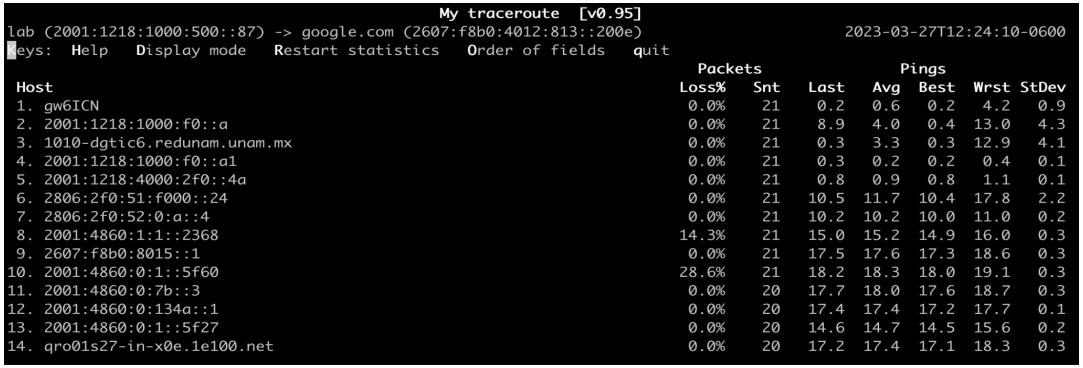
Rendimiento					Promedio del rendimiento de la velocidad del Ancho de Banda (IPv6)	Transferencia (Ipv6)	Promedio del rendimiento de la velocidad del Ancho de Banda (IPv4)	Transferencia (IPv4)
Prueba	**Objetivo**	**Servidor**	**Cliente**		**Mbits/sec**	**(MBytes)**	**Mbits/sec**	**(MBytes)**
1 Red de Acceso	Conexión unidireccional de cliente a Servidor con máximo tamaño de paquete UDP (208 kbytes) Se envían 30 paquetes en intervalos de 10 segundos con un ancho de banda de 100 Mbits por segundo del cliente hacia el servidor.	GUA Interna #iperf -s -p 7575 -V -u 2001:BD8:1000:581::1	PC1-Edificio A 2001:DB8:1000:581::3	#iperf -c 2001:DB8:1000:581::1 -p 7575 -u -t 30 -i 1 -V -b 100M	105	375	N/A	N/A
		Gateway Interno #iperf -s -p 7575 -u 10.10.100.1.e -i 1 -l 8K	PC1-Edificio A 10.10.100.3	#iperf -c 10.10.100.1 -p 75757 -t 30 -i 1 -V -u -b 100M	N/A	N/A	105	375
2 Red de	Conexión unidireccional de cliente a Servidor con máximo tamaño de paquete UDP (	Gateway Externo #iperf -s -B 132.247.20.1	PC2-Edificio C	iperf -c 132.247.20.1 -p 7575 -u -t 30 -i 1 -b 100M -F	N/A	N/A	105	375

Distribución	65536) Se envían 30 paquetes en intervalos de 10 segundos con un ancho de banda de 100 Mbits por segundo del cliente hacia el servidor.	-u -p7575 -e -l 65536	172.16.100.2	ipv6.client.udp.txt -l 65500 #iperf -c 10.10.100.3 -p75757 -f M -bidir -F Ipv4.bi.out -t 5				
		Gateway Externo #iperf -s -B 2001:BD8:1000:580::87 -u -p7575 -e -l 65536	PC2-Edificio C	#iperf -c 2001:BD8:1000:580::87 -u -p7575 -e -l 65536	105	375	N/A	N/A
3 Red de Núcleo	Conexión de cliente en zona D hacia cliente zona E, probando el enrutamiento y filtrado que ofrece shorewall para ambas zonas	Zona D #iperf -s -p 7575 -V -u 2001:BD8:1000:584::40	PC3-Edificio E	#iperf -c -p 7575 -V -u 2001:BD8:1000:584::40	105	375	N/A	N/A
		Zona D #iperf -s -p 7575 -V -u 192.168.101.20	Zona E 192.168.100.20	#iperf -s -p 7575 -V -u 10.10.101.40	N/A	N/A	105	375

Dado las condiciones controladas que se tienen en la red asignada para el Laboratorio, no se tiene mucha variación en los resultados, dado que es un ambiente controlado a fin de evitar impactos en la red productiva del ICN. Sin embargo, la matriz de pruebas ofrece al lector la posibilidad de conocer los comandos y configuraciones con la herramienta iperf para que pueda replicarla.

Otra herramienta a utilizar es MTR[59], el cual nos permite revisar la pérdida de paquetes, latencia y describe la traza de la ruta que siguen los paquetes (ICMP) en ambos protocolos, es decir, IPv4 e IPv6. En la tabla 41 podemos observar la trazabilidad de la dirección destino desde nuestro cliente y nos da un resumen del porcentaje de paquete pérdidos, cuántos paquetes se enviaron a través del comando ping.

Tabla 41.- Resultados con MTR

Dirección Origen	Dirección Destino	MTR
2001:BD8:1000:500::87	2001:BD8:1000:580::1	
2001:BD8:1000:500::87	2001:1218:3000:180::19	
2001:BD8:1000:500::87	2607:f8b0:4012:813::200e	

Dentro de las funciones que tiene iperf en su versión 2, está poder ejecutar procesos en paralelo. Por tanto se utilizó para ejecutar hasta 128 procesos simultáneamente a fin de observar la variación en la red, utilizando los protocolos UDP y TCP en conjunto con IPv4 e IPv6. Estas pruebas se realizan a nivel red de acceso, sin embargo, se pueden extender a la red de distribución o hacia el core. Lo recomendable es probar diferentes niveles, hasta cubrir la comunicación completa.

Resultados en IPv6

En la tabla 42, se presentan los resultados de UDP con IPv6 teniendo un promedio del ancho de banda de 911 Mbits por segundo. y un promedio en transferencia de 2.88 Gbytes (el bitrate utilizado durante la prueba se mantuvo fijo a 1Gb) en el servidor, mientras que en el cliente se presenta un promedio de ancho de banda de 911 Mbits por segundo y un promedio de transferencia 2.85 Gbytes.

Tabla 42.- Tabla de Resultados de rendimiento en red de distribución con IPv6 para UDP

				GW EXTERNO ZONA E	PC ZONA E		IP_Server		IP_Cliente	
Prueba	Protocolo	Protocolo	block size	IP Server	IP client	Puerto	Transfer (Gbytes)	Bitrate (Mbits/sec)	Transfer (Gbytes)	Bandwidth (Mbits/sec)
1	udp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::4(	7575	1.4	400	1.4	930
2	udp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::4(	7575	2.78	796	2.79	800
3	udp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::4(	7575	3.28	940	3.55	931
4	udp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::4(	7575	3.29	942	4.26	932
5	udp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::4(	7575	3.29	941	5.19	936
6	udp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::4(	7575	3.28	939	5.6	937

Los resultados de TCP con IPv6 se muestran en la tabla 43, en donde se tuvo un promedio del ancho de banda de 818 Mbits por segundo y un promedio en transferencia de 2.87 Gbytes (el bitrate utilizado durante la prueba se mantuvo fijo a 1Gb) en el servidor. Para el cliente se obtuvo un promedio de ancho de banda de 822.66 Mbits por segundo.

Tabla 43.- Tabla de Resultados de rendimiento en red de distribución con IPv6 para TCP

				GW EXTERNO ZONA E	PC ZONA E		IP_Server		IP_Cliente	
Prueba	Protocolo	Protocolo	block size	IP Server	IP client	Puerto	Transfer (Gbytes)	Bitrate (Mbits/sec)	Transfer (Gbytes)	Bandwidth (Mbits/sec)
1	tcp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::40	7575	1.4	400	1.4	400
2	tcp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::40	7575	2.79	800	2.79	800
3	tcp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::40	7575	3.24	927	3.25	930
4	tcp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::40	7575	3.24	928	3.25	932
5	tcp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::40	7575	3.23	926	3.26	933
6	tcp	ipv6	1428	2001:1218:1000:584::1	2001:1218:1000:584::40	7575	3.24	927	3.29	941

En la figura 36 y 37 se exhibe el total de transferencia que tuvo el cliente y el servidor durante la prueba tanto para TCP como para UDP con IPv6.

Para la figura 38 y 39 la eficiencia máxima del 91.89 % en el cliente, usando el promedio del consumo de ancho de banda se tiene.

Figura 36. Gráfica de Transferencia para el cliente iperf en IPv6

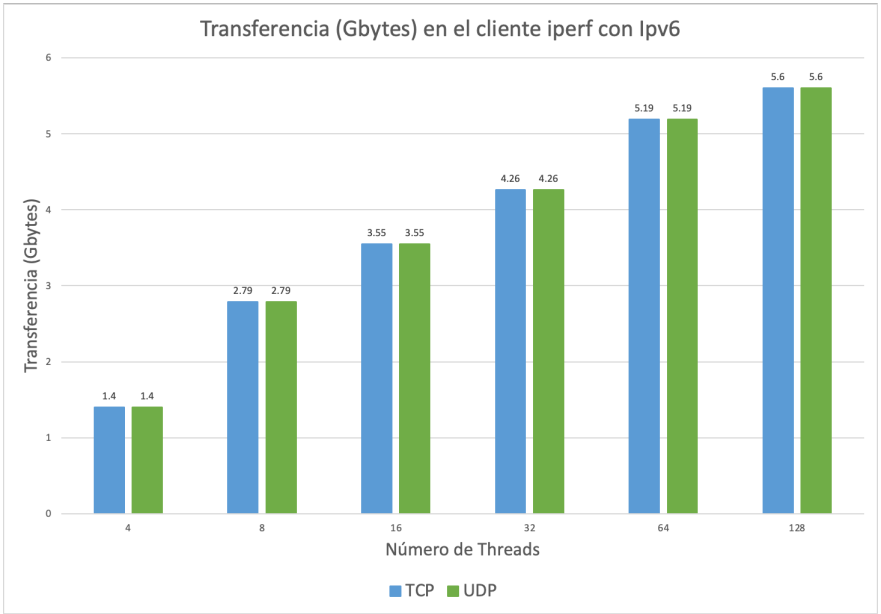


Figura 37. Gráfica Transferencia para el Servidor iperf en IPv6

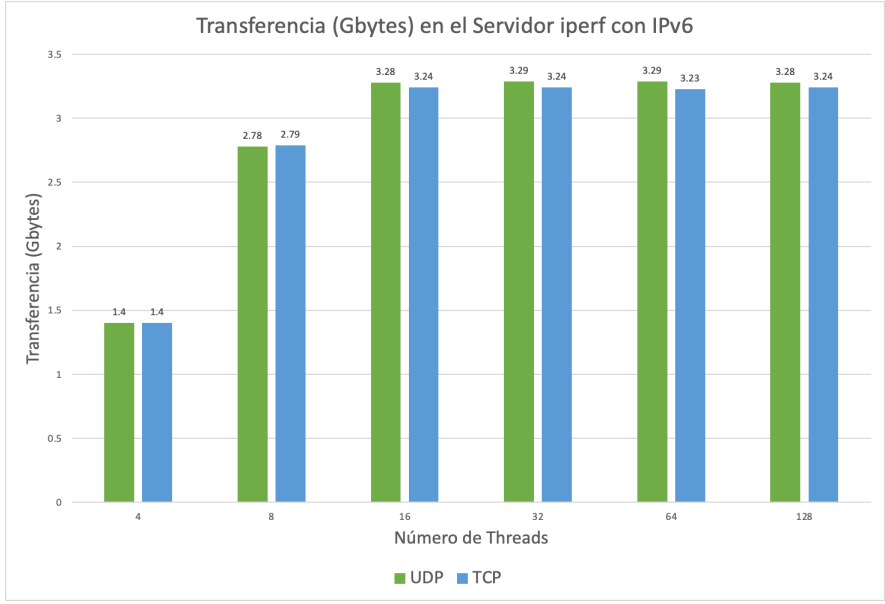


Figura 38. Gráfica de Ancho de banda para el cliente iperf en IPv6

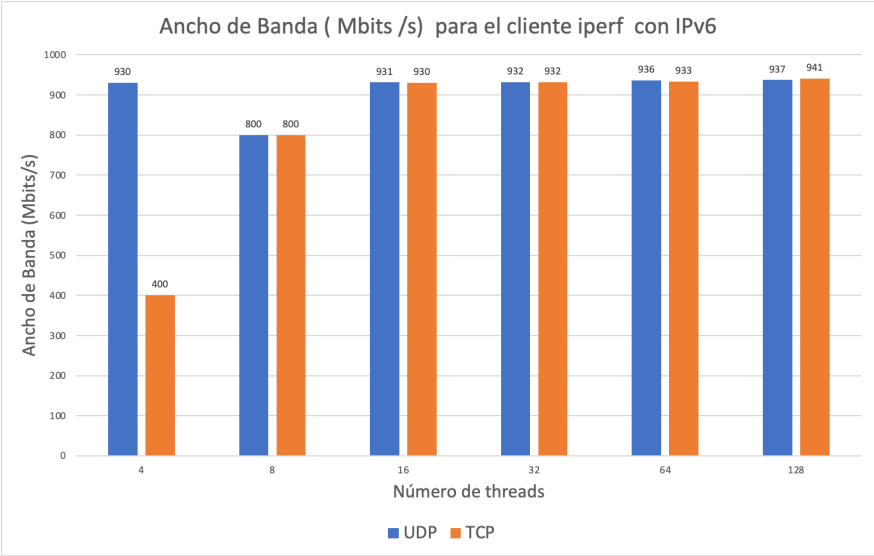
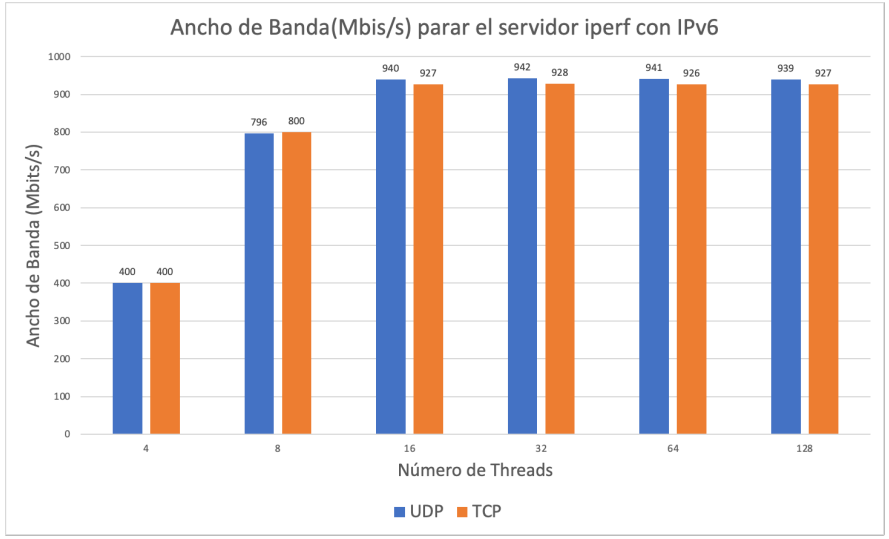


Figura 39. Gráfica de Ancho de Banda para el servidor iperf en IPv6



Resultados en IPv4

En la versión 2 de iperf con IPv4 la herramienta nos ofrece un porcentaje de consumo de CPU (desglosado por usuario, sistema, idle) tanto para el cliente como para el servidor. En la tabla 44 se presentan para UDP, teniendo un promedio del porcentaje. promedio de utilización de CPU del 57.7%, mientras que en la tabla 45 se observan para TCP y con este se obtuvo un promedio de porcentaje promedio de utilización del 18.93%, detectando que se tiene mayor consumo para UDP que para TCP.

Tabla 44.- Tabla de Consumo de recursos en red de distribución con IPv4 para UDP

				GW EXTERNO ZONA E				IP_Cliente			IP_Server		
Threads	Prueba	Protocolo	Protocolo	block size	IP Server	IP cliente	Puerto	Utilizacion CPU(%)	Utilización CPU usuario (%)	Utilización CPU Sistema (%)	Utilizacion CPU(%)	Utilización CPU usuario (%)	Utilización CPU Sistema (%)
4	1	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	24.20%	2.80%	21.40%	13.20%	1.90%	11.30%
8	2	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	37.70%	37.70%	0	20.30%	2.50%	17.80%
16	3	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	51.10%	4.50%	46.60%	20.90%	1.90%	19.00%
32	4	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	63.00%	5.30%	57.70%	24.10%	1.60%	22.50%
64	5	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	77.20%	8.50%	68.80%	24.00%	1.40%	22.60%
128	6	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	92.90%	15.70%	77.10%	25.10%	1.60%	23.50%

Tabla 45.- Tabla de Consumo de recursos en red de distribución con IPv4 para TCP

				GW EXTERNO ZONA E				IP_Cliente			IP_Server		
Threads	Prueba	Protocolo	Protocolo	block size	IP Server	IP cliente	Puerto	Utilizacion CPU(%)	Utilización CPU usuario (%)	Utilización CPU Sistema (%)		Utilización CPU usuario (%)	Utilización CPU Sistema (%)
4	1	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	5.30%	0	5.30%	13.70%	0.60%	13.10%
8	2	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	9.30%	0	9.30%	5.30%	0.20%	5.10%
16	3	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	16.10%	0.30%	15.80%	20.30%	0.70%	19.60%
32	4	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	18.80%	0.40%	18.40%	9.80%	0.40%	9.40%
64	5	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	24.90%	1.10%	23.8	9.30%	0.40%	8.90%
128	6	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	39.20%	32.40%	6.80%	68.10%	3.60%	64.50%

Visualizando los resultados en la gráfica 40, se observa que los porcentajes de consumo de CPU en el cliente son más altos para UDP que para TCP, y en mayor proporción que en el servidor. Para ambos componentes UDP con IPv4 demanda mayor recurso en CPU.

Figura 40. Porcentaje de Consumo de CPU en el cliente iperf con IPv4

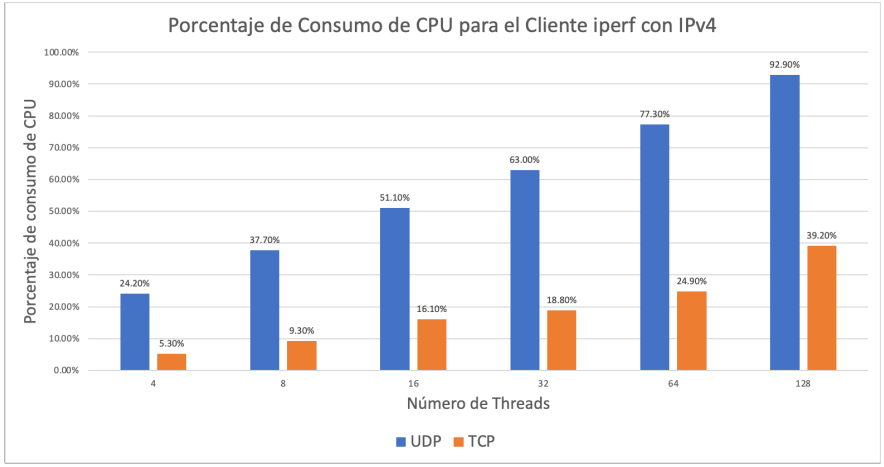
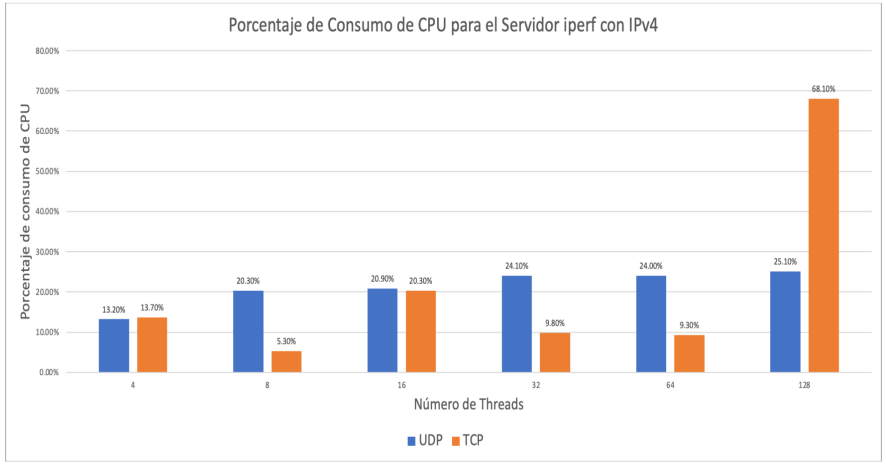


Figura 41. Porcentaje de consumo de CPU en el Servidor IPerf con IPv4



En la tabla 46, se presentan los resultados de UDP con IPv4 teniendo un promedio del ancho de banda de 824.83 Mbits por segundo y un promedio en transferencia de 2.88 Gbytes (el bitrate se mantuvo fijo durante la prueba a 1Gb) para el servidor. En el caso del cliente el promedio del ancho de banda fue de 769 Mbits por segundo y un promedio en el transfer de 3.9 Gbytes.

Tabla 46.- Tabla de resultados de rendimiento en red de distribución con IPv4 para UDP

							GW EXTERNO ZONA E			IP_Server		IP_Cliente	
Threads	Interface en Uso	Prueba	Lineas en reglas FW	Protocolo	Protocolo	block size	IP Server	IP cliente	Puerto	Transfer(Gbytes)	Bandwidth (Mbits/sec)	Transfer(Gbytes	Bandwidth (Mbits/sec)
4	1	1	90	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	1.4	400	1.4	400
8	1	2	90	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	2.79	800	2.79	800
16	1	3	90	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	3.33	953	3.58	940
32	1	4	90	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	3.34	956	4.32	941
64	2	5	90	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	3.27	936	5.17	940
128	3	6	90	udp	ipv4	1448	10.10.101.1	10.10.101.40	7575	3.16	904	6.16	936

Los resultados de TCP con IPv4 se muestran en la tabla 47, en donde se tuvo un promedio del ancho de banda de 769 Mbits por segundo y un promedio de transferencia de 2.806 Gbytes (el bitrate se mantuvo fijo a 1Gb) en el servidor; para el cliente se generó un promedio del ancho de banda de 831.3 Mbits por segundo y un promedio de transferencia de 2.903 Gbytes (manteniendo el bitrate en 1GB).

Tabla 47.- Tabla de resultados de rendimiento en red de distribución con IPv4 para TCP

							GW EXTERNO ZONA E			IP_Server		IP_Cliente	
Threads	Interface en Uso	Prueba	Lineas en reglas FW	Protocolo	Protocolo	block size	IP Server	IP cliente	Puerto	Transfer(Gbytes)	Bandwidth (Mbits/sec)	Transfer(Gbytes	Bandwidth (Mbits/sec)
4	1	1	90	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	1.4	400	1.4	400
8	2	2	90	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	2.79	800	2.79	800
16	3	3	90	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	3.28	940	3.29	943
32	4	4	90	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	3.29	941	3.31	947
64	5	5	90	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	3.29	940	3.31	949
128	6	6	90	tcp	ipv4	1448	10.10.101.1	10.10.101.40	7575	3.27	936	3.32	949

En la gráfica 42, se observa el comportamiento generado durante la prueba en el servidor con el total de transferencia con UDP y TCP sobre IPv4. A pesar de incrementar los procesos paralelos se presentan diferencias muy pequeñas en ambos protocolos. Para el caso del cliente, se exhibe en la gráfica 43, en donde la mayor transferencia se da con UDP sobre IPv4.

Figura 42.- Total de transferencia en el servidor Iperf con IPv4

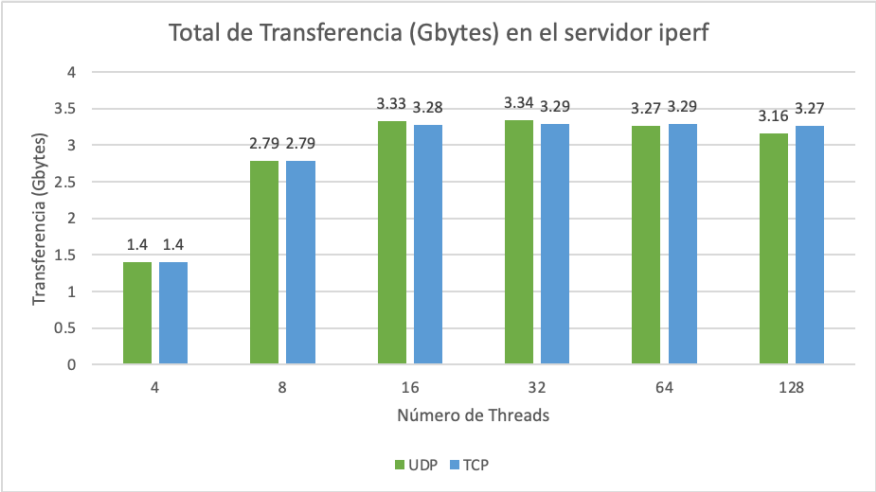
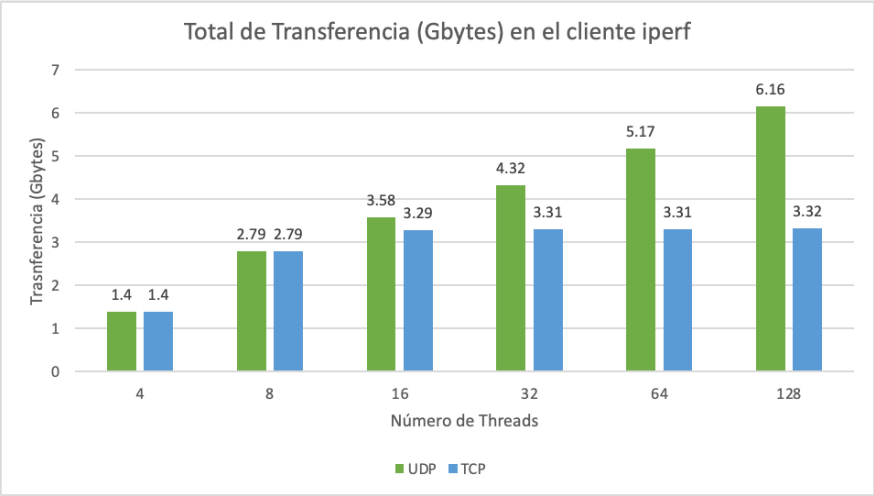


Figura 43.- Total de transferencia en el cliente iperf con IPv4



En la figura 44 se expone el comportamiento del consumo de ancho de banda con IPv4 que se generó en el cliente, comparando con los resultados que se obtuvieron en el servidor que se muestran en la figura 45, la diferencia entre el ancho de banda es muy pequeño entre UDP y TCP. teniendo una eficiencia máxima del 93%, considerando el promedio del ancho de banda se tiene un 75%.

$$\boldsymbol{eficiencia} = (\ \boldsymbol{resultado\ alcanzado}\ *\ \mathbf{100}\ )\ /\ \boldsymbol{resultado\ previsto}$$

Figura 44.- Ancho de Banda con IPv4 en el cliente Iperf

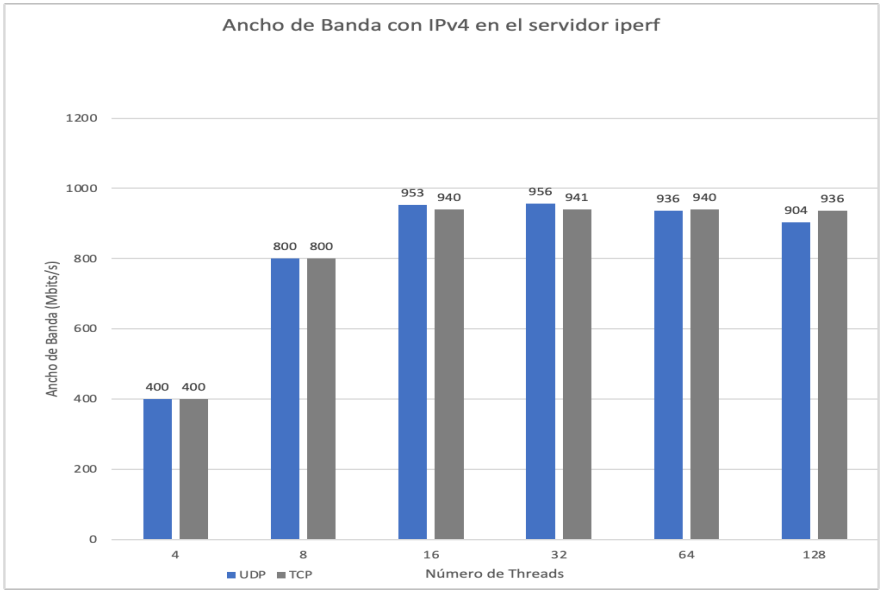
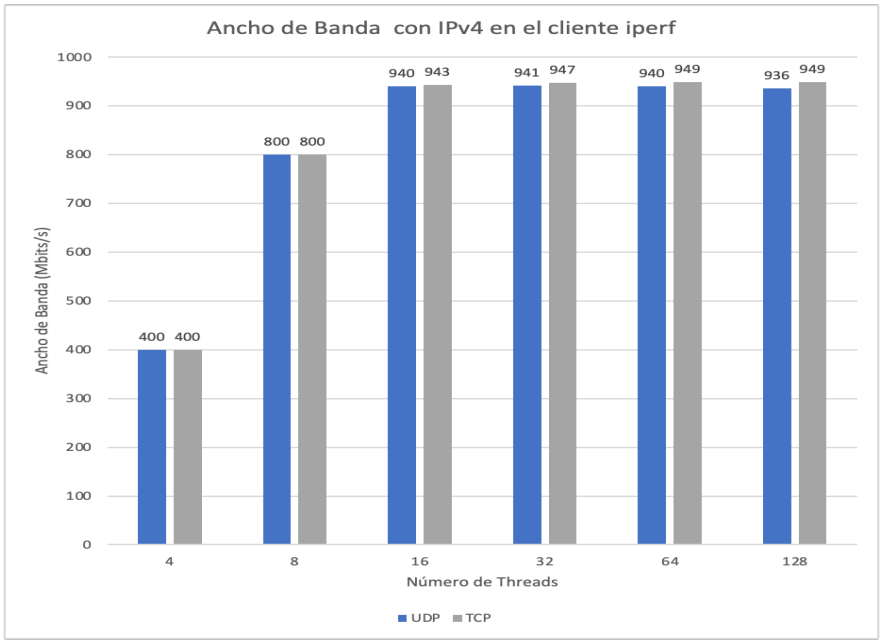


Figura 45.- Ancho de Banda con IPv4 en el servidor Iperf



Prueba utilizando protocolo HTTP para descarga de archivos a través de firewall Shorewall

Esta prueba se enfoca generar a través de un cliente el cual genera 2000 peticiones para la descarga cuasi simultánea de un archivo de 1.1Gb a través de un servidor HTTP custodiado por firewall Shorewall utilizando el protocolo IPv4 e IPv6, midiendo el consumo de los recursos en cada uno de los componentes durante la prueba. Se fijan las variables en la prueba como el ancho de banda asignado al puerto de red, el número de peticiones y el tamaño constante del archivo a descargar.

Resultados obtenidos con el protocolo HTTP

Para mayor detalle gráfico de los resultados se presentan las gráficas de consumo de recurso en Anexo Técnico en apartado L y apartado M. A continuación se presenta un resumen de los resultados obtenidos en la red con direccionamiento IPv6 e IPv4. En la tabla 48 y tabla 49 se presentan los consumos que se presentaron en cada uno de los componentes durante la prueba; mientras que la tabla.

Tabla 48.- Resultado de Consumo de recursos en IPv6

Prueba HTTP en IPv6				
Registros Máximos			Escritura y Letura	
Rol	Cores usados	Memoria Usada(Gb)	Disco (Mb/s)	Red(Mb/s)
Servidor HTTP	2.248	18	22.4 / 11	3.7 /118.4
Firewall Shorewall	0.08	5	0.02 / 0.4	122 / 122
Cliente	4.224	15	0.68 / 1.8	118 / 4

Tabla 49.- Resultado de Consumo de recursos en IPv4

Prueba HTTP en IPv4				
Rol	Cores usados	Memoria Usada(Gb)	Disco (Mb/s)	Red(Mb/s)
Servidor HTTP	2.7	13	3 / 4	3 / 118
Firewall Shorewall	1.1	19	0 / 2	123 / 123
Cliente	5.3	26	2.5 /2.5	122 / 3.4

En la tabla 50 y 51 se muestran los resultados de las peticiones que se manejaron tanto para IPv4 como IPv6

Tabla 50.- Peticiones HTTP en IPv6

Prueba HTTP en IPv6	
Tiempo Máximo de descarga	4 horas 48 min
Intentos de conexión por conexión rechazada	0
Total de descargas completas	1000
Total de peticiones solicitadas	2000
Total de peticiones atendidas	1000
Total de peticiones rechazadas	0
Total de informacion en descarga (GB)	1100

Tabla 51.- Peticiones HTTP en IPv4

Prueba HTTP en IPv4	
Tiempo Máximo de descarga	4 horas 9 min
Intentos de conexión por conexión rechazada	18 intentos por conexión rechazada
Total de descargas completas	190
Total de peticiones solicitadas	2000
Total de peticiones atendidas	1000
Total de peticiones rechazadas	810
Total de informacion en descarga (GB)	209

Resultados en comparación con datos nominales de fabricante en IPv6

Tabla 52.- Consumo de Recursos de Firewall Shorewall (Lab) durante la prueba con IPv6	
CPU Total: 32 Cores AMD Opteron 6212 Porcentaje promedio de Consumo Máximo Total de CPU: 1% Total de CPU usado: 0.08 Core	Memoria: 64GB Porcentaje promedio de Consumo Máximo Total: 2.85 GB/s Total de Memoria usada: 5 GB
Capacidad en Disco: 500 GB Velocidad Fabricante de Disco: NVMe 33 MHz 433 KB/s Velocidad promedio Máxima de Lectura en Disco: Velocidad promedio Máxima de Escritura en Disco: 402.6 KB/s	Tarjeta 4 puertos de Red RJ45: NetXtreme II BCM5709 1 GB Velocidad promedio máxima de Escritura en red: 122.45 MB/s Velocidad promedio máxima de Lectura en red : 122.48 MB/s

Tabla 53.- Consumo de Recursos de Servidor (Lab2) durante la prueba con IPv6	
CPU Total: 8 Cores AMD Opteron 2350 Porcentaje promedio de Consumo Máximo Total de CPU: 28.1% Total de CPU usado: 2.2 Cores	Memoria: 32 GB Porcentaje promedio de Consumo Máximo Total: 2.85 GB/s Total de Memoria usada:0.5GB
Capacidad en Disco: 500 GB Velocidad Fabricante de Disco: NVMe 33MHz Velocidad promedio Máxima de Lectura en Disco: 2.5 Mb/s Velocidad promedio Máxima de Escritura en Disco: : 2.5 Mb/s	Tarjeta 4 puertos de Red RJ45: NetXtreme II BCM5709 1 GB Velocidad promedio máxima de Escritura en red: 122.45 MB/s Velocidad promedio máxima de Lectura en red : 122.48 MB/s

Tabla 54. Consumo de Recursos de Cliente (Lab3) durante la prueba con IPv6	
CPU Total: 8 Cores AMD Opteron 2350 Porcentaje promedio de Consumo Máximo Total de CPU: 52.8% Total de CPU usado: 2.2 Cores	Memoria: 16GB Porcentaje promedio de Consumo Máximo Total: 11.71 GB/s Total de Memoria usada: 15 GB
Capacidad en Disco: 75 GB SATA 7 krpms Velocidad Fabricante de Disco: 7 krpms Velocidad promedio Máxima de Lectura en Disco: 0.68MB/s Velocidad promedio Máxima de Escritura en Disco: 1.8 MB/s	Tarjeta 4 puertos de Red RJ45: NetXtreme II BCM5709 1 GB Velocidad promedio máxima de Escritura en red: 118 MB/s Velocidad promedio máxima de Lectura en red : 4 MB/s

Resultados en comparación con datos nominales de fabricante en IPv4

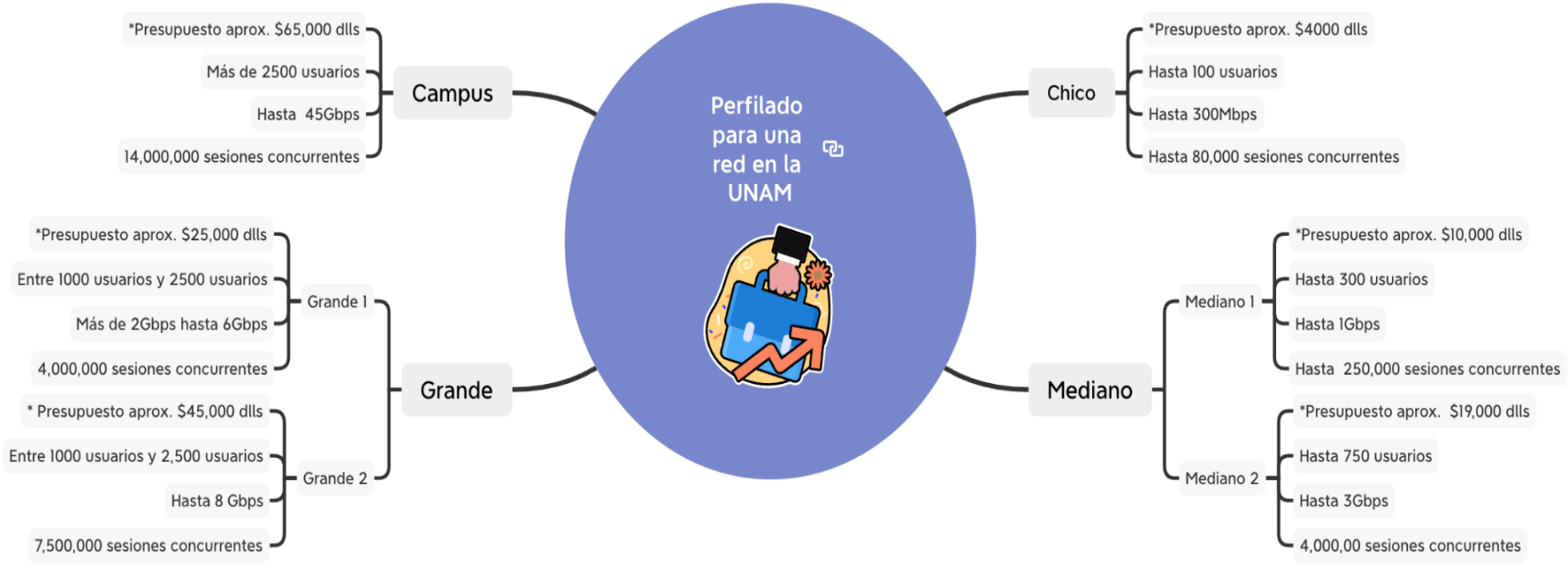
Tabla 55. Consumo de Recursos de Firewall Shorewall (Lab) durante la prueba con IPv4	
CPU Total: 32 Cores AMD Opteron 6212 Porcentaje promedio de Consumo Máximo Total de CPU: 3.5% Total de CPU usado: 1.1 Core	Memoria: 64GB Porcentaje promedio de Consumo Máximo Total: 19502 MB/s Total de Memoria usada: 19 GB
Capacidad en Disco: 500 GB Velocidad Fabricante de Disco: NVMe 33MHz 433 KB/s Velocidad promedio Máxima de Lectura en Disco: 0 MB/s Velocidad promedio Máxima de Escritura en Disco: 2 MB/s	Tarjeta 4 puertos de Red RJ45: NetXtreme II BCM5709 1 GB Velocidad promedio máxima de Escritura en red: 123 MB/s Velocidad promedio máxima de Lectura en red : 123 MB/s

Tabla 56. Consumo de Recursos de Servidor (Lab2) durante la prueba con IPv4	
CPU Total: 8 Cores AMD Opteron 2350 Porcentaje promedio de Consumo Máximo Total de CPU: 66.7% Total de CPU usado: 5.3 Cores	Memoria: 32 GB Porcentaje promedio de Consumo Máximo Total: 2.85 GB/s Total de Memoria usada: 26 GB
Capacidad en Disco: 500 GB Velocidad Fabricante de Disco: NVMe 33MHz Velocidad promedio Máxima de Lectura en Disco: 2.5 Mb/s Velocidad promedio Máxima de Escritura en Disco: 2.5 Mb/s	Tarjeta 4 puertos de Red RJ45: NetXtreme II BCM5709 1 GB Velocidad promedio máxima de Escritura en red: 122 MB/s Velocidad promedio máxima de Lectura en red : 3.4 MB/s

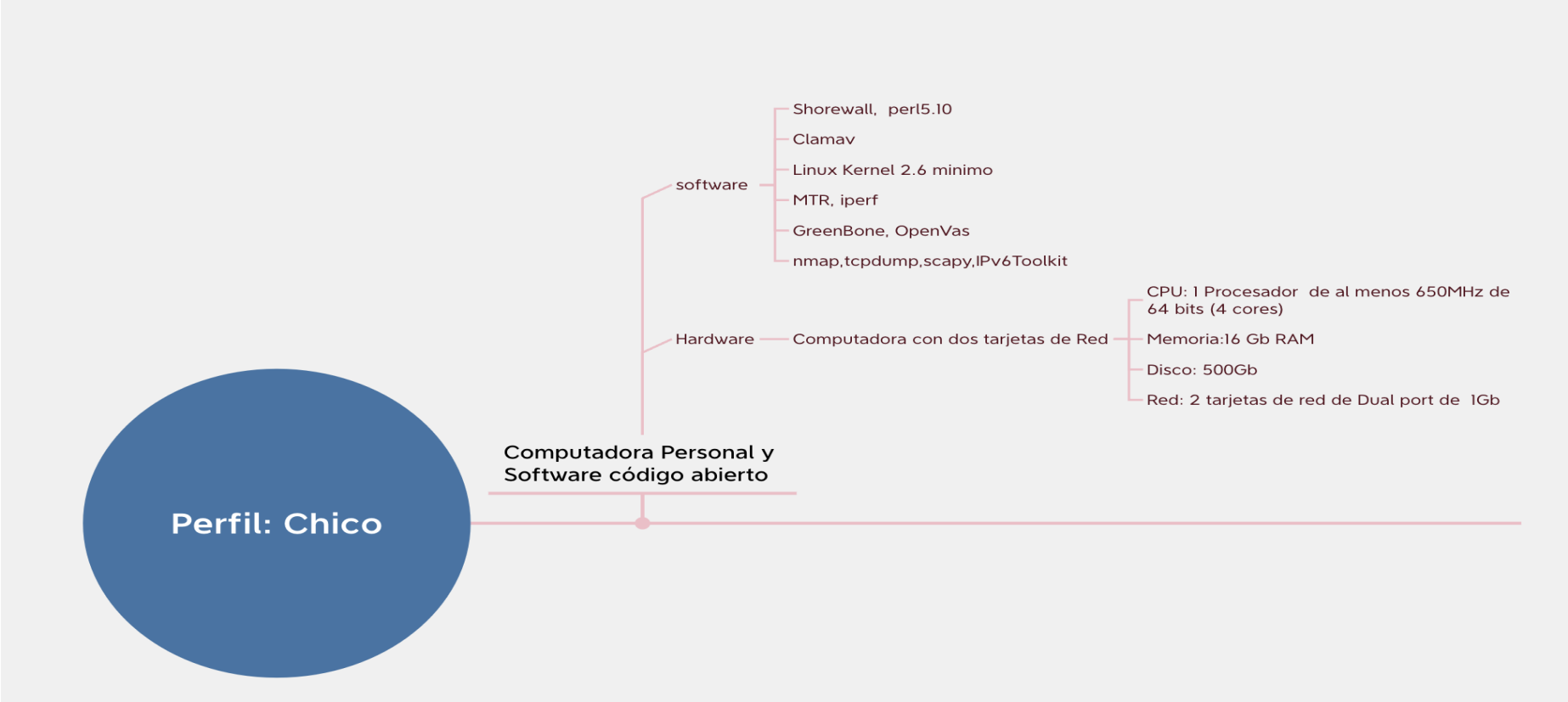
Tabla 57. Consumo de Recursos de Cliente (Lab3) durante la prueba con IPv6	
CPU Total: 8 Cores AMD Opteron 2350 Porcentaje promedio de Consumo Máximo Total de CPU: 33.5% Total de CPU usado: 2.7 Cores	Memoria: 16GB Porcentaje promedio de Consumo Máximo Total: 11.71 GB/s Total de Memoria usada: 13GB
Capacidad en Disco: 75 GB SATA 7krpms Velocidad Fabricante de Disco:7krpms Velocidad promedio Máxima de Lectura en Disco: 3 MB/s Velocidad promedio Máxima de Escritura en Disco: 118 MB/s	Tarjeta 4 puertos de Red RJ45: NetXtreme II BCM5709 1 GB Velocidad promedio máxima de Escritura en red: 122.45 MB/s Velocidad promedio máxima de Lectura en red : 122.48 MB/s

10.1.6.13.- Plan de implementación para la red UNAM

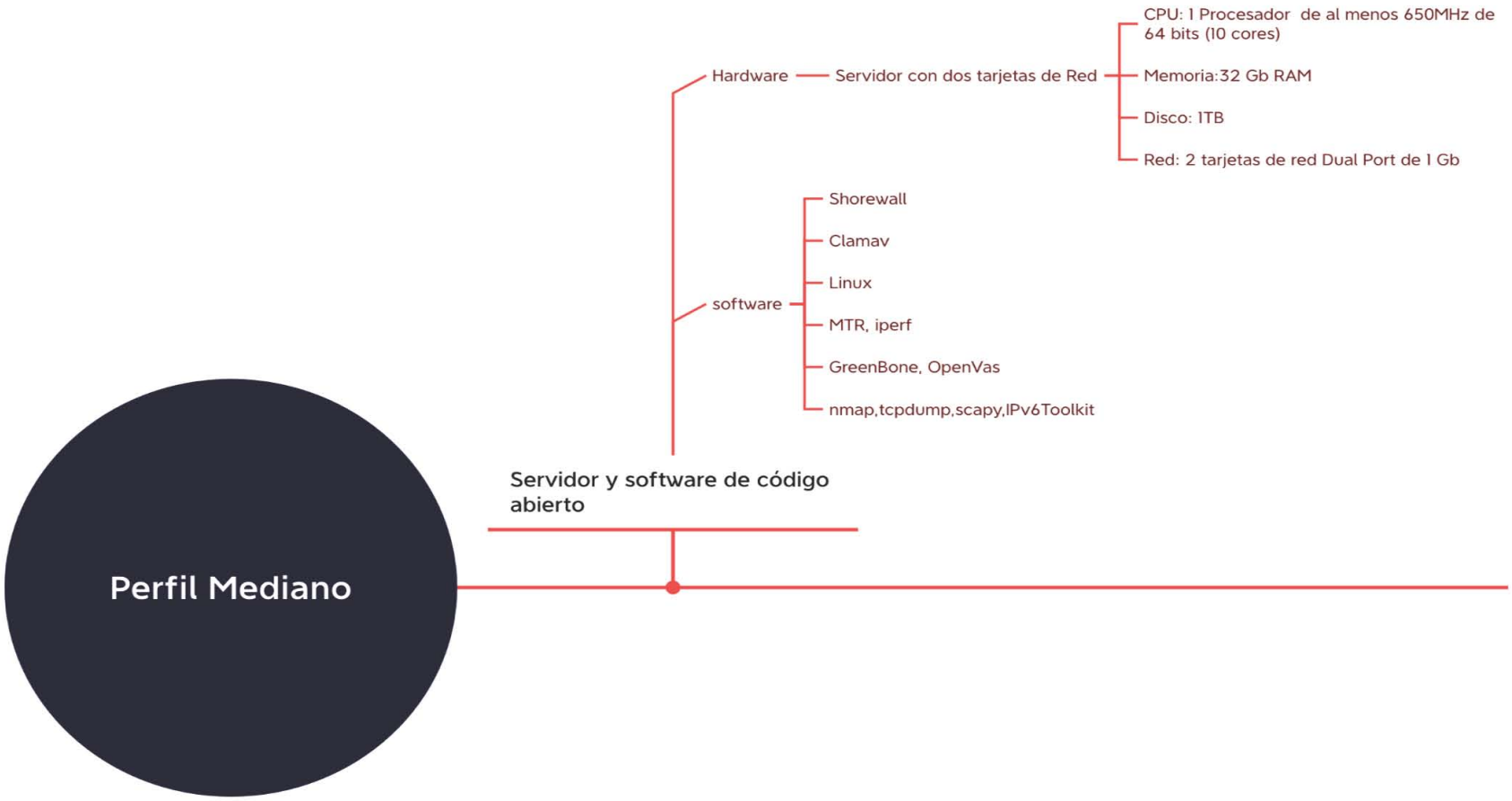
En el diagrama inferior, se muestra el perfilado que se propone para la la adopción de infraestructura que apoye a iniciar el proceso de adopción de IPv6. En cada uno de los perfiles se exponen los criterios que se pueden considerar para considerar el tipo de red que se tiene en cada institución, se incluyen rubros para el dimensionamiento como para el presupuesto que se podría requerir.



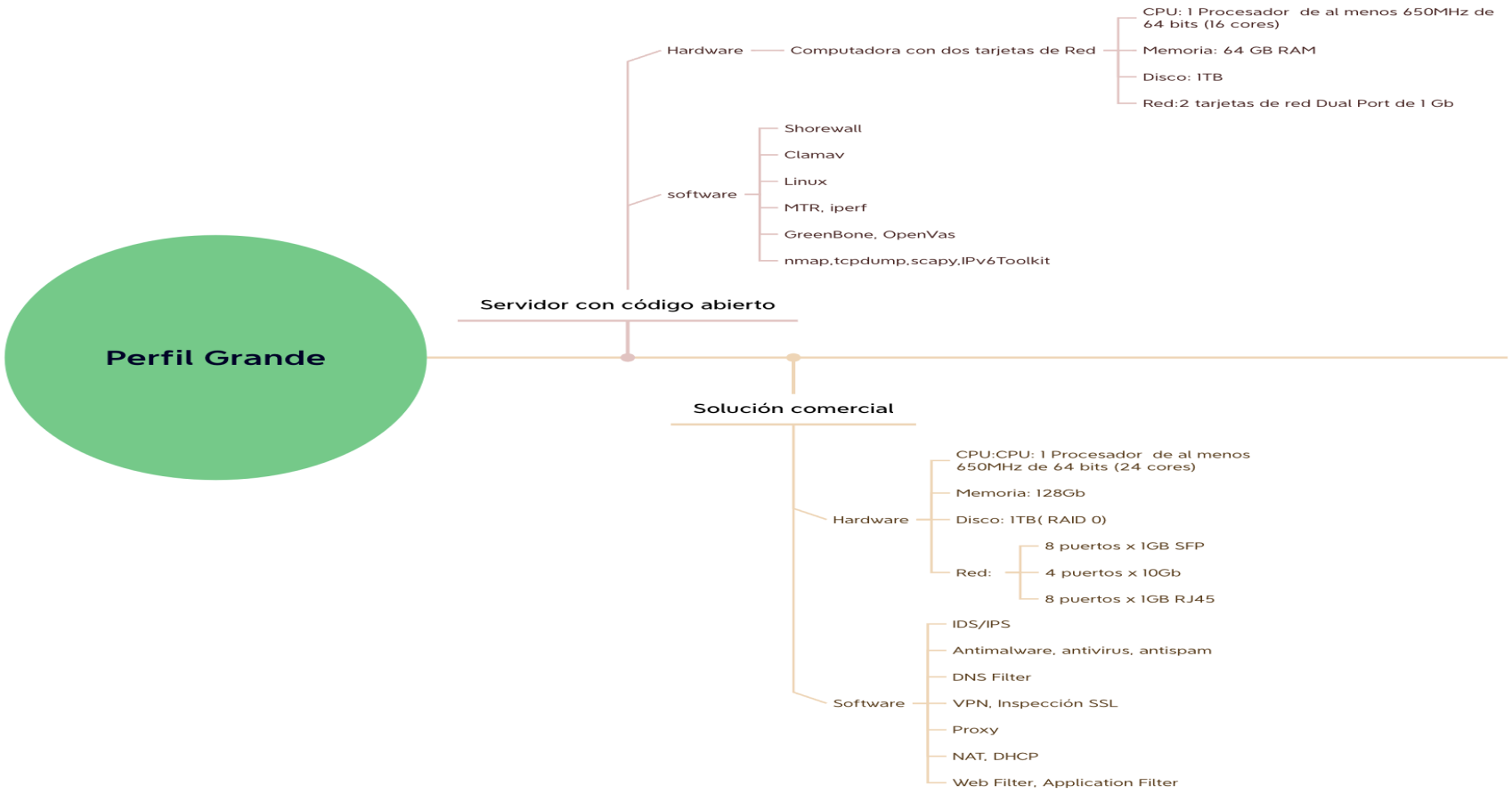
En base a la investigación de mercado que se realizó, se presenta una propuesta en hardware y software de código abierto basado en el contexto dentro de la red de la UNAM. En el siguiente diagrama se describe una solución económica para un tipo de red con perfil chico.



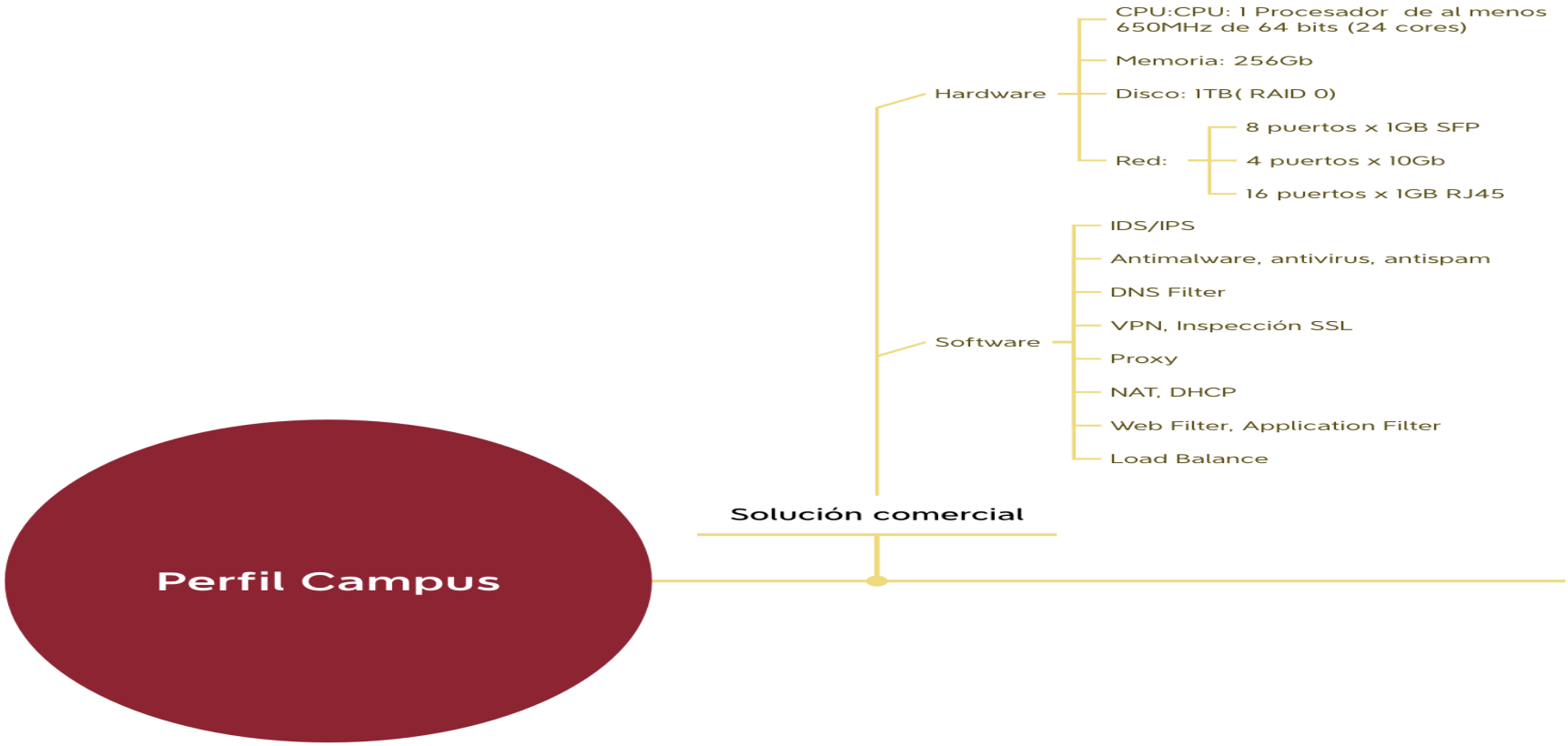
Para el tipo de red con perfil mediano, se puede seguir manteniendo una solución económica basada en código abierto, robusteciendo el hardware a diferencia del perfil chico.



Ahora bien, para el tipo de red con perfil grande, se vuelve más importante el análisis del tráfico de la red, aunado al presupuesto que se desee invertir para una solución a largo plazo, permite explorar soluciones comerciales y poder compararlas con las soluciones de código abierto.



Finalmente para una de la red más grande que se tiene en la UNAM: el campus, no se considera una solución con código abierto, dada la criticidad del servicio de red que se tiene y la afectación que pudiese tenerse a para la comunidad universitaria, ya que la conexión es directa a los ISP, allí es necesario tener un trabajo colaborativo con los proveedores para explorar las soluciones que ofrece el mercado.



Rendimiento comercial

Dado que el perfil campus necesita explorar las soluciones comerciales, es importante validar que dichos componentes están certificados para IPv6. En el anexo A, se podrá encontrar una referencia que ha trabajado el área de especializada que tiene DGTIC, la cual es una guía técnica que permitirá evaluar las soluciones comerciales.

Adicionalmente, se presentan algunos documentos técnicos relacionados con el tipo de pruebas de rendimiento a los que se someten los componentes de red:

RFC 3511.- Proporciona metodologías para la evaluación de desempeño del rendimiento de los firewall. Cubre 4 áreas: reenvío, conexión, latencia y filtrado. Se describe el número de pruebas, sin embargo, hoy queda obsoleto [60].

RFC 2544.- Define el set de pruebas que los vendedores pueden usar para medir y reportar el rendimiento de los dispositivos de red para conexiones punto a punto. No para un servicio que involucre diferentes redes [62].

RFC 2647.- Permite realizar las mediciones del rendimiento para el firewall a través de número de conexiones establecidas, concurrentes, así como su tiempo de degradación, Otras mediciones son el filtrado de paquetes, translación de direcciones de red, tráfico rechazado, número de reglas [63].

RFC 9411.- Define términos y metodologías para los dispositivos de seguridad para redes de nueva generación (NGFWs) y sistemas de prevención de Intrusos de nueva generación (NGIPSs), a diferencia del RFC 3511 se aumenta la complejidad de las pruebas en la capa 7 [61].

RFC 1242.- Establece definiciones y terminología para el rendimiento entre la interconexiones de los dispositivos de red sobre IPv4.

RFC 9004.-Junto con el RFC 1242 soporta mejora las técnicas de evaluación tratando de evitar las ambigüedades en rendimiento de las pruebas, medidas y evaluaciones. Midiendo la capacidad de procesamiento de encabezados a través pequeños paquetes de red, así como el procesamiento de los bits [64].

RFC 5180.- Similar al RFC 1242 sin embargo, se desarrolla para IPv6 dejando fuera los mecanismos de transición. Procedimiento para el manejo y administración del tamaño y enrutamiento de paquetes [65].

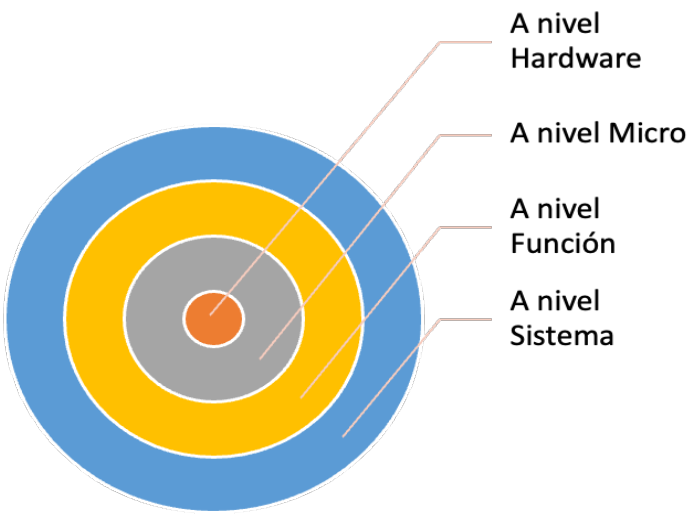


Figura 46.- Granularidad de las Capas para el rendimiento

Para tener en referencia con la conexiones concurrentes, se presenta una medida del número promedio de sesiones concurrentes que se tiene por un usuario experto y con intenso uso de internet, el promedio es de 500 conexiones sobre una unica dirección IPv4. En la tabla 59 se muestra la distribución de las posibles conexiones simultáneas por aplicación y por protocolo TCP o UDP que puede generar este tipo de usuario. En el caso de un usuario casero, no se manejan tantas sesiones, pero considerando el numero de dispositivos en casa, aunado al numero de consultas por aplicación, el lector puede estimar sus conexiones.

Application	Concurrent Sessions	TCP	UDP
Facebook	17	11	6
YouTube	22	18	4
FB Video	13	11	2
Netflix	30	27	3
Chrome	94	89	5
Instagram	17	16	1
Google Play	8	7	1
WhatsApp	3	2	1
FB Messenger	20	15	5
SnapChat	29	19	10

Figure 2. Average Concurrent Sessions Used for Popular Applications

Tabla 58.- Número de sesiones por usuario por aplicaciones sobre IPv4

Fuente:https://www.a10networks.com/wp-content/uploads/A10-EB-Making-Cents-of-IPv4.pdf?mkt_tok=NDE3LUdVQi05OTUAAAGL6lc-8zdSnJE5QQObWL8WDBK16cZmDBPI8xOmzvaiQaZa05VYz34yi0_RyNHAdccpZA7IpT1-DfMuzI8NYq2lWU7Z4qaYgzac-xZBsaz95mzYCQ

Figura 47.- Criterios para evaluar una red para la adopción de IPv6

Capítulo 11. Análisis y Resultados

El uso de la herramienta iperf permitió obtener el porcentaje de consumo de CPU sobre IPv4 y no para IPv6, a pesar de usar ambas versiones (iperf2 e iperf3), pero nos permitió conocer el ancho de banda que se puede tener en la conexión de red. Sin embargo, es importante aclarar que es una red aislada y controlada a fin de no tener afectaciones en la red productiva del Instituto de Nucleares.

Para el análisis del consumo de recursos en los componentes involucrados, se recurrió a utilizar otra herramienta de monitoreo como lo es NMON (ver resultados gráficos en anexo I, J, K, L y M), el cual cubre esta parte independientemente del protocolo que se use. Los resultados obtenidos con esta herramienta me permitió constatar el bajo consumo de los recursos en el servidor con shorewall.

El monitoreo del consumo de los recursos en cada componente durante la prueba de HTTP, me permite tener una referencia para poder establecer los límites en la creación de cada perfil de esta propuesta para la solución del router dependiendo el tamaño de de la red.

El firewall shorewall no presenta altos consumos de recursos (CPU, memoria, disco) y se detecta que el componente que presenta saturación es el puerto de red, la escalabilidad requerida en esta solución es a través del crecimiento en la conexión de la red. Dicho crecimiento se puede integrar con un LACP a nivel sistema operativo.

Tanto la tasa de transferencia como el ancho de banda obtenidos en IPv4 e IPv6 se observa que no presentan una gran diferencia que genere una distinción entre dichos protocolos. Sin embargo, revisando el número de peticiones HTTP (ver tabla 50 y 51) atendidas en IPv6 en comparación con IPv4, se observa que se tiene mayor eficacia, dado que no se tiene conexiones con rechazo ó retransmisión como se presenta en IPv4.

Otra observación es que no se alcanzaron a atender todas las peticiones solicitadas, porque no se realizó ninguna modificación en las pilas de TCP ni UDP, ni tampoco se hicieron modificaciones en la configuración del servicio HTTP y ninguna mejora al sistema operativo para incrementar el desempeño de la prueba, con el fin de tener un ambiente default que cualquier técnico TIC puede desplegar.

Con respecto al porcentaje de consumo de CPU obtenido con iperf para IPv4, se observa que el consumo es mayor en el cliente (cuenta con menos recursos que el servidor y tecnología anterior que el servidor), el cual se incrementa conforme el número de hilos del sistema operativo aumenta, sin llegar a consumir el 100% del recurso.

En la prueba de rendimiento con uso del protocolo HTTP, otro factor a considerar es que se tiene que el máximo tiempo de respuesta de servicio HTTP está limitado a la velocidad de lectura que tiene en el disco para poder atender las peticiones simultáneas, a pesar de no saturar o estresar ninguno de los componentes (no se realizó la escritura de los archivos a descargar en el cliente), se logró tener un tráfico representativo y registrar las operaciones de lectura y escritura en la red del servidor, lo cual ayudó a demostrar que el firewall shorewall no rebasó los 122 Mb/s de lectura en la red, que es menos del 12% de su capacidad nominal (1Gb/s).

El laboratorio utilizado para las pruebas de conectividad, se utilizó la herramienta gratuita iperf (código abierto) que puede saturar hasta redes de 10Gbps, pero un análisis a mayor profundidad para la red con mayores capacidades en el ancho de banda, es necesario considerar el uso de herramientas comerciales, como son los generadores de tráfico, como solarwind o packet sender.

Capítulo 12. Conclusiones

El desarrollo de este trabajo, me permitió saber que existen soluciones económicas en el mercado que resuelven las pequeñas necesidades para comenzar a adoptar IPv6, desmitificando la idea de que la transición y adopción de dicho protocolo es complejo, costoso y a largo plazo. Pero la transición y convivencia de ambas versiones IPv4 e IPv6 es un proceso continuo que requiere cada vez más tener redes unificadas y convergentes.

Se puede tener un buen desempeño de router de frontera con soluciones de código abierto, a fin de tener pequeños costos que permitan manejar un mecanismo de transición como lo es Dual Stack.

El propósito de la Universidad es generar el capital humano con el conocimiento técnico a fin de desarrollar y adaptar nuevas tecnologías en el área de comunicaciones que estarán integrándose al mercado laboral, que ya está adoptando estas soluciones, mientras que en el ámbito educativo y el desarrollo de la investigación, es vital proveer ambientes con IPv6 para que las nuevas generaciones puedan crear nuevas investigaciones, por ejemplo: IoT, Bitcoin sobre IPv6.

La experiencia que ofrece el poder implementar la metodología de la adopción de IPv6 permite al técnico de TIC integrar varios aspectos como el económico y la alineación de las necesidades de las instituciones dentro del proyecto, y no solo de obtener el conocimiento de la tecnología para solucionar los retos que se enfrentan para mejorar el servicio de la red.

Dada la interconexión que existe en la globalización de la comunicación a través de la interacción de soluciones de nubes privadas, híbridas y públicas, se vuelve primordial establecer esquemas de seguridad que permitan la convivencia entre IPv4 e IPv6, así como la creciente necesidad de soportar la conectividad para ambos protocolos para la integración de sistema híbridos.

El llevar a cabo la metodología propuesta permitió realizar la comparación y la evaluación de soluciones alternativas a las comerciales para la considerar una alternativa a la sustitución de tecnología obsoleta en el área de comunicaciones, a fin de reducir los costos al adoptar este protocolo.

Capítulo 13. Mejoras

- El presente trabajo permite tener un primer acercamiento a los técnicos de las diversas áreas TIC al proceso de integración y adopción de IPv6 en las redes de las instituciones de la UNAM. Sin embargo, se debe trabajar en conjunto con el proveedor ISP y el área de DGTIC a fin de tener una solución integral.
- Es importante establecer grupos de trabajo multidisciplinarios con experiencia a fin de conocer aspectos importantes en la dinámica y uso de las redes locales para poder ofrecer soluciones afines.
- Para la actualización de registros AAAA y AA en el DNS, es necesario desarrollar scripts que permitan actualizar ágilmente las tablas de resolución, esto ya no se logró desarrollar en este trabajo.
- Es necesario ampliar, afinar y robustecer las pruebas de rendimiento. Cabe destacar que no se realizó una puesta a punto del sistema operativo, al servicio de HTTP, ni un ajuste en la pila de TCP y UDP para mejorar los resultados de rendimiento en el número de peticiones atendidas. Es necesario tener herramientas más robustas para el análisis a profundidad del desempeño de la red.
- El desarrollo de algunas pruebas en el laboratorio permite virtualizar algunos ambientes en cualquier PC, pero es recomendable que el administrador TIC cuente con dispositivos de interconexión de red de prueba para poder manejar otros escenarios y tener resultados concretos.
- El diseño del direccionamiento de IP fue **teórico** conforme a las recomendaciones de LACNIC, sin embargo, en la práctica, se recomienda tener un acercamiento con la DGTIC y conservar el direccionamiento IPV6 lo más sencillo posible en la distribución de la red para manejar como prefijo mínimo /64, dado que en la UNAM, las áreas TIC son pequeñas y no cuentan con mucho personal.
- Es importante considerar iniciar con las actualizaciones y cambios en el DNS posteriormente, activar protocolo IPv6 a fin de no tener afectaciones en los servicios a migrar.

Anexo Técnico

Anexo A.Recomendaciones para Licitaciones

http://www.ipv6.unam.mx/documentos/Recomendaciones_Licitaciones-Compras-equipos-para-IPv6-UNAM-v7.pdf

Anexo B. Guías de Configuración IPv6

https://drive.google.com/drive/folders/17DMCSDbT6uqT6qUd1xTETAQc38tLmjMA?usp=share_link

https://drive.google.com/drive/folders/18n_6gS8dy6C2E9tdK6juKe_6FSTWpHA7?usp=share_link

https://drive.google.com/drive/folders/13WJ0apCWRhBWhw3nNnfB7_NashJyJrlR?usp=share_link

https://drive.google.com/drive/folders/13vHLdj3t6XZO-CVgFwGq8v9T_vddCrsj?usp=share_link

Anexo C. Instalación de paquete ndp Ubuntu

```
#sudo apt install libndp0 libndp-dev
#sudo apt install libndp-dbg
#sudo apt install ndp-tools
#sudo ndptool monitor
 Type: RA
  Hop limit: 64
  Managed address configuration: no
  Other configuration: no
  Default router preference: medium
  Router lifetime: 1800s
  Reachable time: unspecified
  Retransmit time: unspecified
  Source linkaddr: cc:4e:24:48:d4:00
  Prefix: 2001:1218:1000:500::/64, valid_time: 2592000s, preferred_time: 604800s, on_link:
yes, autonomous_addr_conf: yes, router_addr: no
  MTU: 1500
NDP payload len 32, from addr: 2001:1218:1000:500::1, iface: br0
  Type: NS
NDP payload len 32, from addr: fe80::ce4e:24ff:fe48:d400, iface: br0
  Type: NA
NDP payload len 32, from addr: fe80::ce4e:24ff:fe48:d400, iface: br0
  Type: NS
NDP payload len 32, from addr: fe80::ce4e:24ff:fe48:d400, iface: br0
  Type: NA
NDP payload len 32, from addr: 2001:1218:1000:500::1, iface: br0
```

Anexo D. Instalación y Configuración de Shorewall

1.- Instalar el paquete de sshguard

```
ticadmin@lab:/etc/shorewall$ sudo apt install sshguard
```

2.-Instalar el paquete de shorewall

```
ticadmin@lab:/etc/shorewall$ sudo apt install shorewall
```

3.- Configuración de parámetros del firewall con /etc/shorewall/shorewall.conf

4.- Configurando reglas IPv4

```
ticadmin@lab:/etc/shorewall$ cat blrules
#ACTION         SOURCE                  DEST                    PROTO   DPORT
DROP            net                     all                     udp     1023:1033,1434,5948,23773
DROP            all                     net                     udp     1023:1033
DROP            net                     all                     tcp
        57,1433,1434,2401,2745,3127,3306,3410,4899,5554,5948,6101,8081,9898,23773
DROP            net:221.192.199.48      all
DROP            net:61.158.162.9        all
DROP            net:81.21.54.100        all                     tcp     25
DROP            net:84.108.168.139      all
DROP            net:200.55.14.18        all
DROP     net:127.0.0.0/8          all             tcp
DROP     net:192.0.2.0/24    all                 tcp
DROP     net:198.51.100.0/24    all               tcp
DROP     net:203.0.113.0/24    all                tcp
ticadmin@lab:/etc/shorewall$ cat interfaces
#ZONE    INTERFACE    BROADCAST    OPTIONS
net     eno1    -
zonaA     virbr0    -
zonaB     virbr1    -
zonaC     virbr2    -
ticadmin@lab:/etc/shorewall$ cat policy
#SOURCE    DEST          POLICY          LOGLEVEL    RATE    CONNLIMIT
zonaA    net     ACCEPT
zonaB    net     ACCEPT
zonaC    net     ACCEPT
net    all       DROP    $LOG_LEVEL
# The FOLLOWING POLICY MUST BE LAST
all    all       REJECT          $LOG_LEVEL
ticadmin@lab:/etc/shorewall$ cat rules
#Action    #source    #dest    #proto    #dport
#
#Direcciones bogus
DROP    net    fw:27.0.0.0/8    tcp
DROP    net    fw:192.0.2.0/24    tcp
DROP    net    fw:198.51.100.0/24    tcp
DROP    net    fw:203.0.113.0/24    tcp
DROP    net    fw:240.0.0.0/4    tcp
DROP    net    fw:192.0.0.0/24    tcp
DROP    net    fw:0.0.0.0/8    tcp
DROP    net    fw:10.0.0.0/8    tcp
DROP    net    fw:100.64.0.0/10    tcp
DROP    net    fw:169.254.0.0/16    tcp
DROP    net    fw:172.16.0.0/12     tcp
```

```
DROP    net    fw:192.0.0.0/29    tcp
DROP    net    fw:192.168.0.0/16     tcp
DROP    net    fw:198.18.0.0/15    tcp
DROP    net    fw:255.255.255.255/32    tcp
#Previniendo ping en externo
Ping(DROP)      net     fw
#Paquetes inválidos
Invalid(DROP)   net     fw      tcp
#Previniendo ping en externo
Ping(DROP)      net     fw
#####
#Servicio SSH
#####
ACCEPT    zonaA    net    tcp    22
ACCEPT    zonaB    net    tcp    22
ACCEPT    zonaC    net    tcp    22
ACCEPT    net    zonaA    tcp    22
ACCEPT    net    zonaB    tcp    22
ACCEPT    net    zonaC    tcp    22
ACCEPT    net    all    tcp    22
#####
#ICMP
#####
ACCEPT    all    fw    icmp    8    -    -    10/sec:5
ACCEPT    fw    net    icmp    8    -    -    10/sec:5
ACCEPT    zonaA    net    icmp    8    -    -    10/sec:10
ACCEPT    zonaB    net    icmp    8    -    -    10/sec:10
ACCEPT    zonaC    net    icmp    8    -    -    10/sec:10
#####
##Servicio WEB
####
ACCEPT    all    fw    tcp    80,443
ACCEPT    zonaA    net    tcp    80,443
ACCEPT    zonaB    net    tcp    80,443
ACCEPT    zonaC    net    tcp    80,443
#####
#Protocolo IPv6
ACCEPT    all    all    icmp    fragmentation-needed
ACCEPT    all    all    icmp    time-exceeded
ticadmin@lab:/etc/shorewall$ cat snat
#ACTION    SOURCE    DEST
MASQUERADE    192.168.100.0/24    virbr0
MASQUERADE    10.10.100.0/24      virbr1
MASQUERADE    172.16.100.0/24     virbr2
#
MASQUERADE    132.248.29.87/24    eno1
MASQUERADE    192.168.100.0/24    virbr0
MASQUERADE    10.10.100.0/24    virbr1
MASQUERADE    172.16.100.0/24    virbr2
MASQUERADE    eno1    virbr0
MASQUERADE    eno1    virbr1
MASQUERADE    eno1    virbr2
#
# Rules generated from masq file /etc/shorewall/masq by Shorewall 5.2.3.4 - Thu Feb 16 12:57:45 CST
2023
#
MASQUERADE    132.248.29.0/24    eno1
SNAT(132.248.29.87)    192.168.100.0/24    eno1    tcp    smtp
ticadmin@lab:/etc/shorewall$ cat zones
#ZONE    TYPE    OPTIONS          IN_OPTIONS    OUT_OPTIONS
#Red local interna
zonaA    ipv4
zonaB    ipv4
zonaC    ipv4
```

```
#Red externa
net    ipv4
#Firewall
fw    firewall
```

5.- Generando reglas IPv6

```
ticadmin@lab:/etc/shorewall6$ cat blrules
#Action      source                  dest    proto    dport
#borrar paquetes Teredo desde la red externa
DROP        net:[2001::/32]         all
DROP        net                     all                     udp     1023:1033,1434,5948,23773
DROP        all                     net                     udp     1023:1033
DROP        net                     all                     tcp
    57,1433,1434,2401,2745,3127,3306,3410,4899,5554,5948,6101,8081,9898,23773
#Bloqueo de direcciones bogus
DROP         net:[::1/128]    all    tcp
DROP         net:[100::/64]    all   tcp
DROPnet:[2001::/32]    all  tcp
DROPnet:[fc00::/7]    all   tcp
DROPnet:[fe80::/10]    all  tcp
DROPnet:[::ffff:0:0/96]    all      tcp
DROPnet:[2001:2::/48]    all        tcp
DROPnet:[2001::/23]    all  tcp
DROPnet:[2001:db8::/32]    all      tcp
DROPnet:[2001:10::/28]    all       tcp
DROPnet:[::/128]    all    tcp
ticadmin@lab:/etc/shorewall6$ cat interfaces
#Zona    #interface    #opciones
net    eno1
zonaA    virbr0
zonaB    virbr1
zonaC    virbr2
ticadmin@lab:/etc/shorewall6$ sudo cat policy
net     all    DROP
fw    net    ACCEPT
zonaA    all    REJECT
zonaB    all    REJECT
zonaC    all    REJECT
all    all    REJECT    info
ticadmin@lab:/etc/shorewall6$ cat rules
#Acción     #origen     #destino    #proto    #destino    #origen     #rate
#paquetes inválidos
Invalid(DROP)    net    fw    tcp
?SECTION NEW

#Bloqueo de direcciones bogus
#DROP    net         fw:[::1/128]    tcp
#DROP    net    fw:[100::/64]    tcp
#DROP    net    fw:[2001::/32]    tcp
#DROP    net    fw:[fc00::/7]    tcp
#DROP    net    fw:[fe80::/10]    tcp
#DROP    net    fw:[::ffff:0:0/96]    tcp
#DROP    net    fw:[2001:2::/48]    tcp
#DROP    net    fw:[2001::/23]    tcp
#DROP    net    fw:[2001:db8::/32]    tcp
#DROP    net    fw:[2001:10::/28]    tcp
#DROP    net    fw:[::/128]    tcp

#Nombre de Servidores
#? SET VHOSTS "[2001:1218:1000:501::]/64,[fe80::]/10"
```

```
#Servicios de IPv6
ACCEPT    all    all    ipv6-icmp    time-exceeded
#ACCEPT    all    all    ipv6-icmp    echo-request    -    -    3/sec:10    Trcrt(ACCEPT)    all
all
#####
#Servicio SSH
#####
SSH/ACCEPT    net    fw    tcp
SSH/ACCEPT    fw    net    tcp
SSH/ACCEPT    zonaC    net    tcp
SSH/ACCEPT    net    zonaA    tcp
SSH/ACCEPT    net    zonaB    tcp
SSH/ACCEPT    net    zonaC    tcp
SSH/ACCEPT    net    all    tcp
#####
#ICMP
#####
ACCEPT    all    fw    ipv6-icmp    8    -    -    10/sec:5
ACCEPT    fw    net    ipv6-icmp    8    -    -    10/sec:5
ACCEPT    zonaA    net    ipv6-icmp    8    -    -    10/sec:10
ACCEPT    zonaB    net    ipv6-icmp    8    -    -    10/sec:10
ACCEPT    zonaC    net    ipv6-icmp    8    -    -    10/sec:10
#####
##Servicio WEB, Puerto 80
####
Web/ACCEPT    all    fw    tcp
Web/ACCEPT    zonaA    net    tcp
Web/ACCEPT    zonaB    net    tcp
Web/ACCEPT    zonaC    net    tcp
#Servicio DNS
DNS/ACCEPT    fw    net    tcp
```

6.- Creación de Zonas

```
ticadmin@lab:/etc/shorewall6$ sudo cat zones
#ZONE    TYPE    OPTIONS          IN OPTIONS      OUT OPTIONS
fw    firewall
net    ipv6
zonaA    ipv6
zonaB    ipv6
zonaC    ipv6
```

Anexo E. Instalación y configuración de Software de monitoreo IPv6

1.- Descargar software de página

```
curl -w  https://usgv6-deploymon.antd.nist.gov/govmon.html
```

2.- Descomprimir archivo

```
# wget https://usgv6-deploymon.antd.nist.gov/monitor-1.1.tar.gz
```

3.- copiar carpeta en /var/www/

```
#tar -xvfz monitor-1.1.tar.gz
#cp monitor /var/www/
```

4.- Cambiar permisos a la carpeta para publicación en apache2

```
#chown -R www-data:www-data /var/www/monitor
```

5.- Activar de módulo Perl en Apache2

```
# wget https://usgv6-deploymon.antd.nist.gov/monitor-1.1.tar.gz
#a2enmod cgi
```

6. Instalación de paquetes PERL.

```
#root@monitor:/var/www/monitor/src# ls -la
-rw-r--r-- 1 www-data www-data 259004 ene 13 10:37 [01;31mNet-DNS-1.32.tar.gz
-rw-r--r-- 1 www-data www-data  46818 ene 13 10:37 [01;31mNet-DNS-SEC-1.19.tar.gz
root@monitor: /var/www/monitor/src> tar -xvfz Net-DNS-1.32.tar.gz ; cd Net-DNS-1.32
root@monitor:/var/www/monitor/src/Net-DNS-1.32# perl Makefile.pl
Activating Non Fatal Online Tests...
Activating IPv6 Tests...
Warning!
========
Online tests depend on conditions beyond the control of Net::DNS. The tests
check for the expected results when both Net::DNS and the outside world are
functioning properly. In case of failure it is often undecidable if the error
lies within Net::DNS or elsewhere.
Generating a Unix-style Makefile
Writing Makefile for Net::DNS
Writing MYMETA.yml and MYMETA.json

root@monitor:/var/www/monitor/src/Net-DNS-1.32# make
Skip blib/lib/Net/DNS/Parameters.pm (unchanged)
Skip blib/lib/Net/DNS/RR/TXT.pm (unchanged)
Skip blib/lib/Net/DNS/RR/SIG.pm (unchanged)
Skip blib/lib/Net/DNS/Resolver/os390.pm (unchanged)
Skip blib/lib/Net/DNS/RR/ZONEMD.pm (unchanged)
```

```
            Manifying 38 pod documents
            Manifying 38 pod documents
            Manifying 9 pod documents
    root@monitor:/var/www/monitor/src/Net-DNS-1.32# make test
            PERL_DL_NONLAZY=1 HARNESS_OPTIONS=c "/usr/bin/perl" "-MExtUtils::Command::MM" "-
            MTest::Harness" "-e" "undef *Test::Harness::Switches; test_harness(0, 'blib/lib',
            'blib/arch')" t/*.t
            t/00-install.t .............
            t/00-install.t ............. 1/212
            t/00-install.t ............. ok
            t/00-load.t ................ #
            # These tests were run using:
            #   Net::DNS                  1.32
            #   Digest::BubbleBabble      0.02
            #   Digest::HMAC              1.04
            #   Digest::MD5               2.58
            #   Digest::SHA               6.02
            #   Encode                    3.08
            #   File::Spec                3.80
            #   IO::File                  1.46
            #   IO::Select                1.46
            #   IO::Socket::IP            0.41
            #   MIME::Base64              3.16
            #   PerlIO                    1.11
            #   Scalar::Util              1.55
            #   Time::Local               1.30

            t/00-load.t ................ 1/32
            t/00-load.t ................ ok
            t/00-pod.t ..................
            t/00-pod.t .................. 1/91
            t/99-cleanup.t ............. 1/1 # Cleaning
            t/99-cleanup.t ............. ok
            [32mAll tests successful.
            [0mFiles=104, Tests=3429, 144 wallclock secs ( 1.09 usr  0.44 sys + 20.22 cusr
            3.60 csys = 25.35 CPU)
            Result: PASS
    root@monitor:/var/www/monitor/src/Net-DNS-1.32# make install
            Magnifying 38 pod documents
            Magnifying 38 pod documents
            Magnifying 9 pod documents
            Installing /usr/local/share/perl/5.34.0/Net/DNS.pm
            Installing /usr/local/share/perl/5.34.0/Net/DNS/Text.pl
            Appending installation info to /usr/local/lib/x86_64-linux-
            gnu/perl/5.34.0/perllocal.pod
root@monitor:/var/www/monitor/src/Net-DNS-SEC-1.19# perl  Makefile.PL
root@monitor:/var/www/monitor/src/Net-DNS-SEC-1.19# make
root@monitor:/var/www/monitor/src/Net-DNS-SEC-1.19# make test
root@monitor:/var/www/monitor/src/Net-DNS-SEC-1.19# make install
```

7- Instalando comandos adicionales en sistema operativo

```
root@monitor:~# apt install expects
root@monitor:~# apt install coreutils
```

8.- Validando archivos de página web

```
root@monitor:/var/www/monitor# ls -la
        -rw-r--r-- 1 www-data www-data   110 ene 13 10:37 a1record
        -rw-r--r-- 1 www-data www-data   130 ene 13 10:37 a4record
        -rw-r--r-- 1 www-data www-data   275 ene 13 10:37 authsrvs
        -rw-r--r-- 1 www-data www-data     9 ene 13 10:37 date
        -rw-r--r-- 1 www-data www-data   463 ene 13 10:37 domains
        -rwxr-xr-x 1 www-data www-data  7895 ene 13 10:37 generate
        -rw-r--r-- 1 www-data www-data    39 ene 13 10:37 mailsrvs
        -rwx------ 1 www-data www-data 33831 ene 13 10:37 mmonitor
        -rw-r--r-- 1 www-data www-data  2535 ene 13 10:37 README
        drwx------ 5 www-data www-data  4096 ene 13 10:37 results
        drwx------ 4 www-data www-data  4096 ene 13 10:37 src
        -rw-r--r-- 1 www-data www-data     0 ene 13 10:37 whois
        -rw-r--r-- 1 www-data www-data   172 ene 13 10:37 wwwsrvs
```

8.- Editando archivo de domains para colectar sitios a monitorear

```
root@monitor:/var/www/monitor# vim domains
        mx.unam.nucleares,1,https://www.nucleares.unam.mx,Interna
        mx.unam,1,https://www.unam.mx,Interna
        mx.unam.ipv6,1,https://www.ipv6.unam.mx,Interna
        mx.unam.ingenieria,1,https://www.ingenieria.unam.mx,Interna
        mx.unam.iimas,1,https://www.iimas.unam.mx,Interna
        com.google,1,htps://www.google.com,Externa
        com.cloudflare,1,https://www.cloudflare.com,Externa
        com.ipv6forum.,1,https://www.ipv6forum.com,IPv6 Forum
        edu.berkeley.,1,https://www.berkeley.edu,University of California Berkeley
        gov.nist.,1,https://www.nist.gov,National Institute of Standards and Technology
        net.ripe.,1,https://www.ripe.net,RIPE NCC
        org.ietf.,1,https://www.ietf.org,Internet Engineering Task Force
```

9.- Creando script para ejecutar herramienta de monitoreo y recolectar información

```
root@monitor:/var/www/monitor# mkdir cgi-bin
10.- Copiar archivo generate hacia directorio cgi-bin
root@monitor:/var/www/monitor# cp generate cgi-bin/generate.cgi
root@monitor:/var/www/monitor# sudo vim ejecuta.sh
        PAT=/var/www/monitor
        $PAT/monitor $PAT/domains &
        /usr/bin/cp $PAT/date /usr/lib/cgi-bin/date
        /usr/bin/cp $PAT/date $PAT/cgi-bin/date
        /usr/bin/cp -r $PAT/results /usr/lib/cgi-bin/
        /usr/bin/cp -r $PAT/results $PAT/cgi-bin/
        /usr/bin/chown -R www-data:www-data $PAT
```

11.- Configurar sitio apache para publicación

```
root@monitor:/etc/apache2/sites-available# vim 000-default.conf
        <VirtualHost *:80>
                <Directory /var/www/monitor>
                Options Indexes FollowSymLinks
                AllowOverride None
                Require all granted
                </Directory>
                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
                ScriptAlias "/cgi-bin/" "/var/www/monitor/cgi-bin/"
```

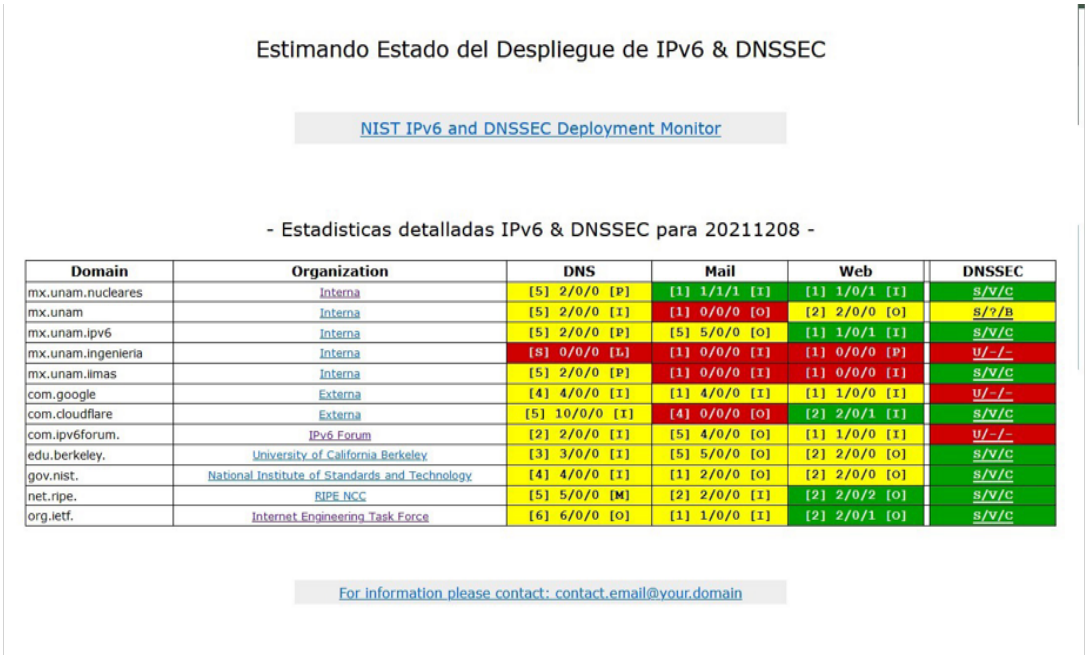
```
                <Directory "/var/www/monitor/cgi-bin">
                                AllowOverride None
                                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                                AddHandler .py .cgi .pl
                                Require all granted
                </Directory>
        </VirtualHost>
```

12.- Consultar página

```
# curl -w  http://localhost/cgi-bin/generate.cgi
```

13.- Instalar cron para automatización del monitoreo diario.

```
0 0 * * * /usr/bin/sudo -i -u root /usr/bin/bash -x /var/www/monitor/ejecuta.sh &
root@monitor:/var/www/monitor# sudo crontab -e
```



Estimando Estado del Despliegue de IPv6 & DNSSEC

NIST IPv6 and DNSSEC Deployment Monitor

- Estadisticas detalladas IPv6 & DNSSEC para 20211208 -

Domain	Organization	DNS	Mail	Web	DNSSEC
mx.unam.nucleares	Interna	[5] 2/0/0 [P]	[1] 1/1/1 [I]	[1] 1/0/1 [I]	S/V/C
mx.unam	Interna	[5] 2/0/0 [I]	[1] 0/0/0 [O]	[2] 2/0/0 [O]	S/?/B
mx.unam.ipv6	Interna	[5] 2/0/0 [P]	[5] 5/0/0 [O]	[1] 1/0/1 [I]	S/V/C
mx.unam.ingenieria	Interna	[8] 0/0/0 [L]	[1] 0/0/0 [I]	[1] 0/0/0 [P]	U/-/-
mx.unam.iimas	Interna	[5] 2/0/0 [P]	[1] 0/0/0 [I]	[1] 0/0/0 [I]	S/V/C
com.google	Externa	[4] 4/0/0 [I]	[1] 4/0/0 [I]	[1] 1/0/0 [I]	U/-/-
com.cloudflare	Externa	[5] 10/0/0 [I]	[4] 0/0/0 [O]	[2] 2/0/1 [I]	S/V/C
com.ipv6forum.	IPv6 Forum	[2] 2/0/0 [I]	[5] 4/0/0 [O]	[1] 1/0/0 [I]	U/-/-
edu.berkeley.	University of California Berkeley	[3] 3/0/0 [I]	[5] 5/0/0 [O]	[2] 2/0/0 [O]	S/V/C
gov.nist.	National Institute of Standards and Technology	[4] 4/0/0 [I]	[1] 2/0/0 [O]	[2] 2/0/0 [O]	S/V/C
net.ripe.	RIPE NCC	[5] 5/0/0 [M]	[2] 2/0/0 [I]	[2] 2/0/2 [O]	S/V/C
org.ietf.	Internet Engineering Task Force	[6] 6/0/0 [O]	[1] 1/0/0 [I]	[2] 2/0/1 [O]	S/V/C

For information please contact: contact.email@your.domain

Figura 48.- Monitoreo para dominio UNAM.MX con herramienta govmon

Anexo F. Instalación y configuración de RADVD

1.- Instalar paquete en ubuntu

```
        root@monitor:/home#apt install radvd radvdump
```

2.- Configurar servicio.Se agrega el prefijo asignado al laboratorio y se usará el servicio DNS de Google.

```
#sudo vim /etc/radvd.conf
                interface br0
                {
                        AdvSendAdvert on;
                        AdvManagedFlag off;
                        AdvOtherConfigFlag off;
                        AdvDefaultPreference high;
                        prefix 2001:db8::/32 {
                                AdvOnLink on;
                                AdvAutonomous on;
                                AdvRouterAddr on;
                                AdvValidLifetime infinity;
                        };
                        RDNSS 2001:4860:4860::6464 2001:4860:4860::64 {
                        };
                        {       AdvRouteLifetime infinity;
                        };
                };
```

3.- Activar servicio

```
#systemctl start radvd
#systemctl enable radvd
```

4.-Validar el envío de paquetes de router

```
[sudo] password for ticadmin:
# radvd configuration generated by radvdump 2.18
# based on Router Advertisement from fe80::ce4e:24ff:fe48:d400
# received by interface br0
#
interface br0#ticadmin@lab:~$ sudo radvdump

{
        AdvSendAdvert on;
        # Note: {Min,Max}RtrAdvInterval cannot be obtained with radvdump
        Adv Managed Flag off;
        AdvOtherConfigFlag off;
        Adv Reachable Time 0;
        AdvRetransTimer 0;
        AdvCurHopLimit 64;
        AdvDefaultLifetime 1800;
        AdvHomeAgentFlag off;
        AdvDefaultPreference medium;
        AdvSourceLLAddress on;
        AdvLinkMTU 1500;
```

```
        prefix 2001:4860:4860::8844/64
        {
                AdvValidLifetime 2592000;
                AdvPreferredLifetime 604800;
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr off;
        }; # End of prefix definition

}; # End of interface definition
```

Anexo G. Instalación y configuración de Bind9

1.- Instalar paquete en ubuntu

```
        ticadmin@lab:/home#apt install bind9 bind9-docs bind9-tools
```

2.- Configurar servicio de DNS

```
        ticadmin@lab:/etc/bind$ vim /etc/bind/named.conf.options

        ticadmin@lab:/etc/bind$ cat named.conf.options
        acl labv4 { 192.168.100.0/24; 172.16.100.0/24; 10.10.100.0/24; };
        acl labv6 { 2001:1218:1000:580::/64; 2001:1218:1000:581::/64; 2001:1218:1000:582::/64; };
        acl bogusnetsv4 { 0.0.0.0/8;  192.0.2.0/24; 224.0.0.0/3; 10.0.0.0/8; 172.16.0.0/12;
192.168.0.0/16; };
        acl bogusnetsv6 { ::1/128; 2001:db8::/32; 2001:10::/28; 2001::/23; };


        options {
            directory "/var/cache/bind";
            //directory "/etc/namedb";
            allow-query { labv4; labv6; };
            blackhole { bogusnetsv4; bogusnetsv6; };
            recursion no;
            forwarders {
                 8.8.8.8;
                 8.8.4.4;
                 1.1.1.1;
            };
        };
        zone "0.0.127.in-addr.arpa" {
            type primary;
            file "localhost.rev";
            notify no;
        };
        acl bogusnets {
                0.0.0.0/8;  192.0.2.0/24; 224.0.0.0/3;
                10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16;
        };
```

2.- probar el servicio de DNS

```
        ticadmin@lab:/etc/bind$ nslookup lab
        Server:          127.0.0.53
        Address:    127.0.0.53#53

        Name:    lab.nucleares.unam.mx
        Address: 132.248.28.87

        ticadmin@lab:/etc/bind$ nslookup 2001:1218:1000:500::1
        1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.0.0.1.8.1.2.1.1.0.0.2.ip6.arpa    name = gw6ICN.

        ticadmin@lab:/etc/bind$ dig lab

        ; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> lab
        ;; global options: +cmd
```

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22514
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;lab.                    IN    A

;; ANSWER SECTION:
lab.             0    IN    A    127.0.1.1

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 26 11:28:06 CST 2023
;; MSG SIZE  rcvd: 48
```

Anexo H Estadísticas de Campus Juriquilla

A continuación en la figura 49 se presenta el diagrama de la red del campus Juriquilla, que nos permitirá conocer la red core, de distribución y de enlace donde se tiene el monitoreo del tráfico de red desde el ISP hacia cada uno de los institutos que se les da el servicio.

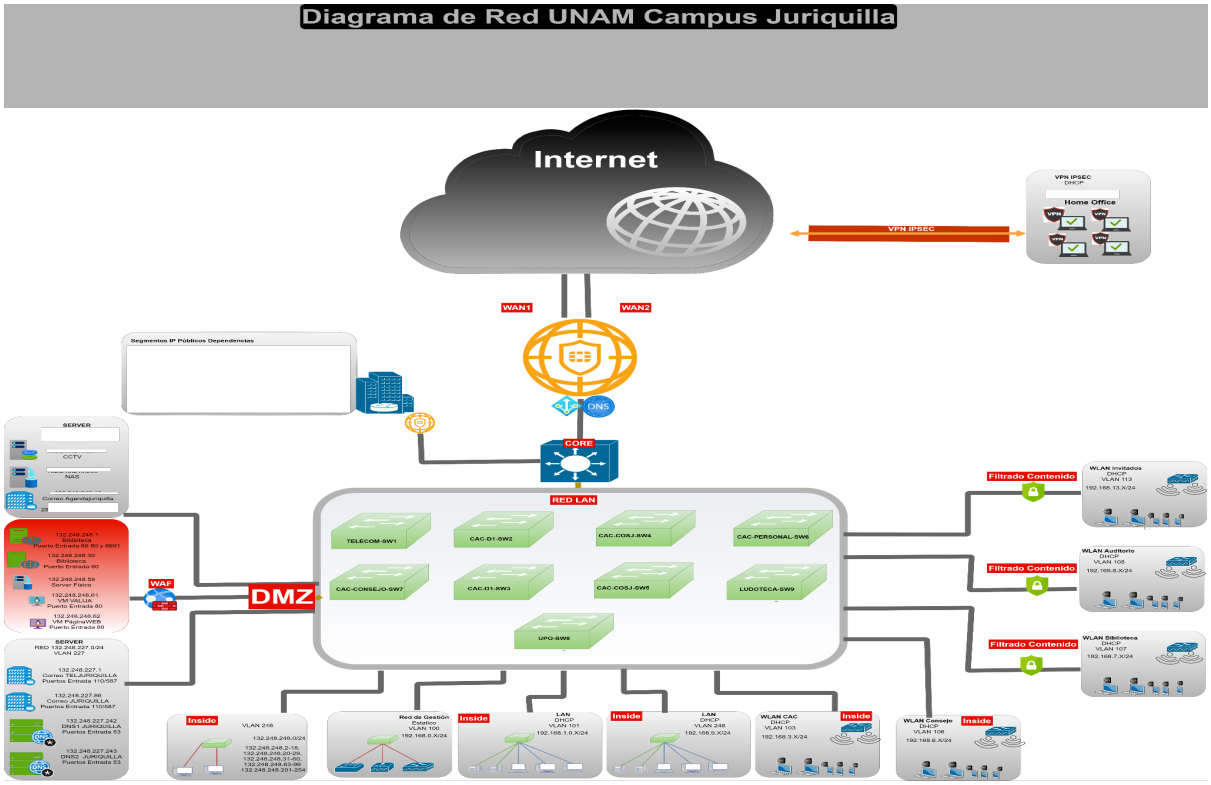


Figura 49.- Diagrama de red UNAM Campus Juriquilla.

En la figura 50 se muestra una clasificación del tipo de tráfico generado por las aplicaciones más usadas en el campus Juriquilla. Como se puede observar hay un gran flujo de servicio SSH y Mysql derivado de las consultas de sistemas internos hacia ciudad Universitaria para la contabilidad,proveeduría, Pappit, SIP, SIC,Conacyt, etc.). Posteriormente le siguen los servicios de Google, Youtube, Facebook, Apple, Zoom, ya que se continúan utilizando servicios de Nube de estas compañías después de la pandemia; en redes sociales se publican las conferencias, talleres y eventos culturales del día.

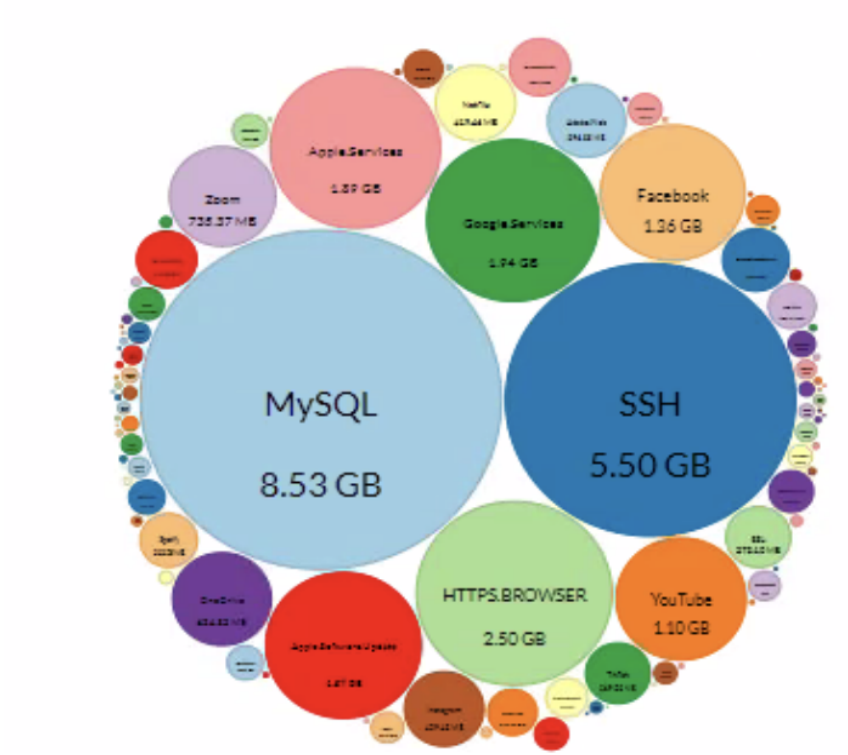


Figura 50.- Clasificación de tipo de aplicaciones del tráfico de salida en la red del campus Juriquilla sobre una vía del Core.

Muestreo del promedio del consumo de la semana del 7 al 13 de Febrero del 2023.

Conexión principal del Core

Como se puede observar en la figura 51 existen horarios en donde el consumo del ancho de banda aumenta considerablemente y coincide con el horario de la vida académica. Sin embargo, el flujo es constante inclusive fines de semana, ya que se generan respaldos que se transmiten al servicio ofrecido por DGTIC en nube.

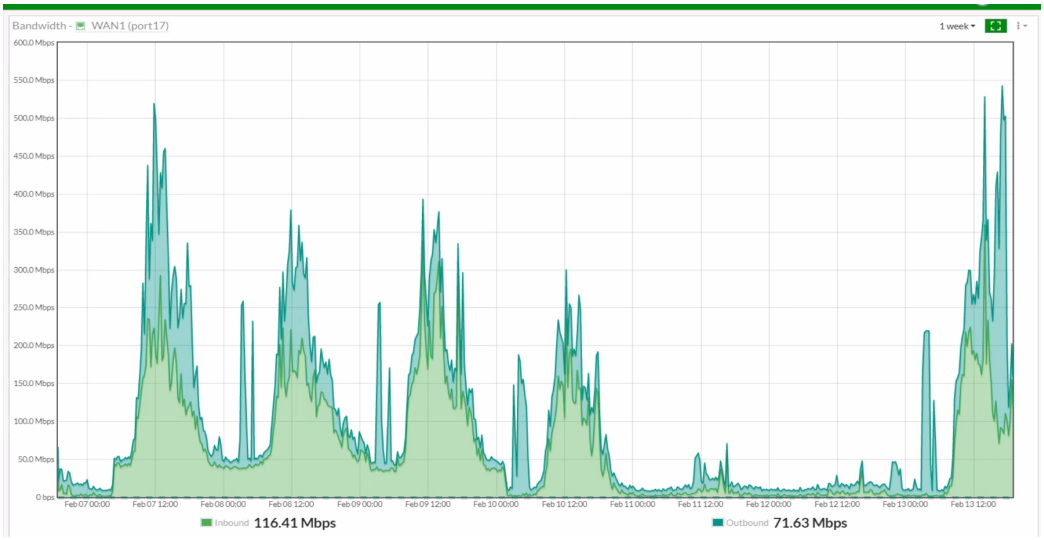


Figura 51.- Consumo del ancho de banda (entrada/salida) de la vía principal (WAN1) del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo del ancho de banda de la semana del 7 al 13 de Febrero del 2023.

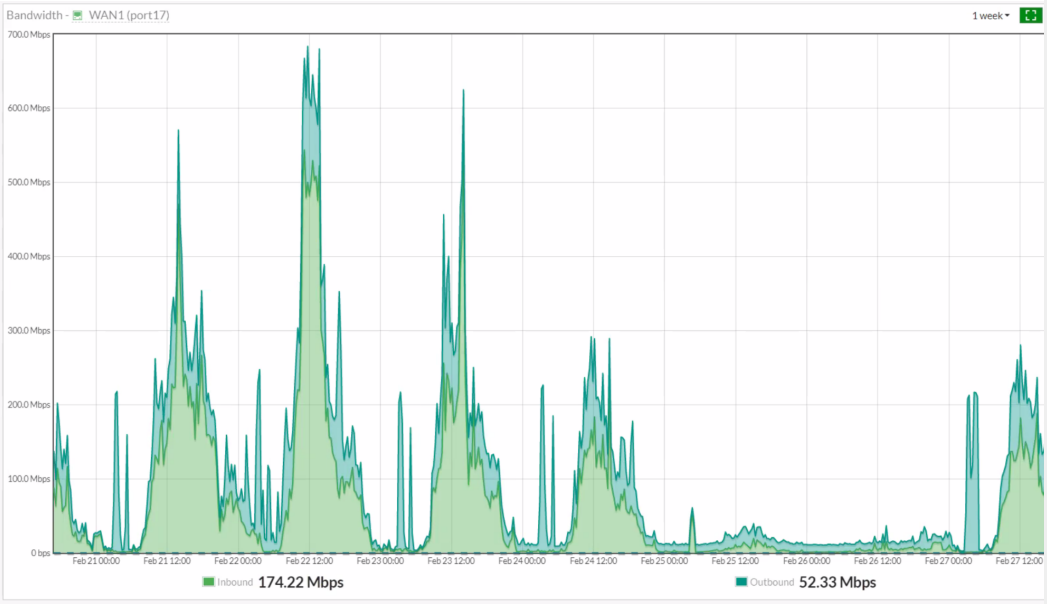


Figura 52.- Consumo del ancho de banda (entrada/salida) de la vía principal (WAN1) del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo del ancho de banda de la semana del 21 al 26 de Febrero del 2023.

Volumen datos en el Core

En la figura 53, se muestra el porcentaje promedio del volumen de datos recibidos y enviados en los dos puertos del core con los ISPs del campus Juriquilla. Se observa que se tiene un 96% se envía por el puerto 17 representando casi 38 TB de recepción contra 26 TB de envío y se recibe un 47%, mientras que en el puerto 16, se envía solo un 4% y se recibe un 53%, que representa 1 TB de envío contra 42 TB de recepción.

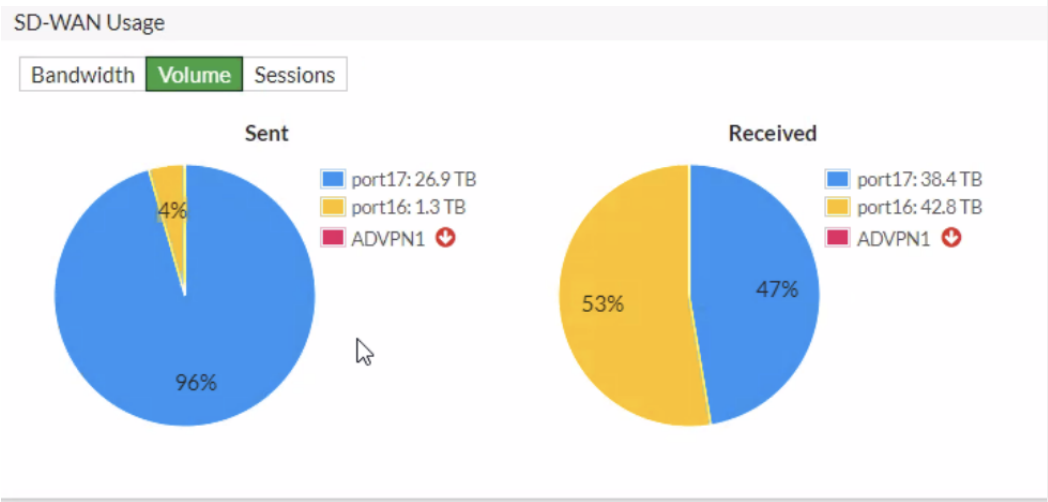


Figura 53.- Porcentaje de la distribución del volumen de datos recibidos y enviados en los puertos de conexión al Core con el ISP del Campus Juriquilla.

Aplicaciones del Core

En esta figura 54 se puede observar la distribución de las diferentes aplicaciones y el horario que generan el consumo del ancho de banda, así como el número de sesiones que se tiene en cada una de ellas.
Aplicaciones como correo gmail, outlook, zoom,youtube,facebook,buscadores de red, mysql es que mayor consumo tiene en cuanto a sesiones y ancho de banda.

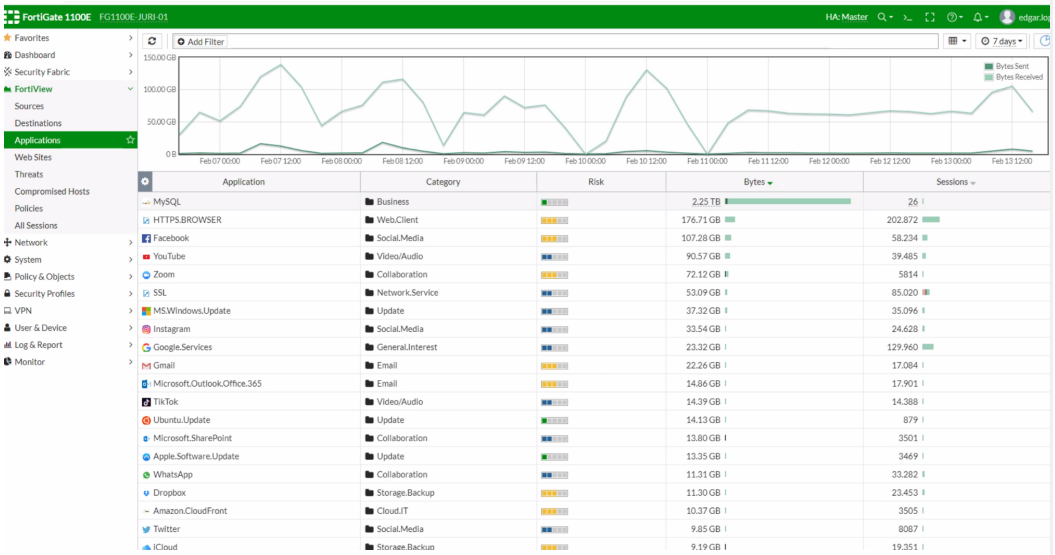


Figura 54.- Consumo de ancho de banda por tipo Aplicaciones y número de sesiones en el Core de campus Juriquilla.

Muestreo de la semana del 7 al 13 de Febrero del 2023.

Conexión alterna del Core

En la figura 55, se presenta un muestreo del 7 al 13 de febrero 2023, sobre el puerto 16 del comportamiento ancho de banda durante el horario laboral en el campus, no deja de ser continuo, teniendo un pico máximo de hasta 450Mbps.

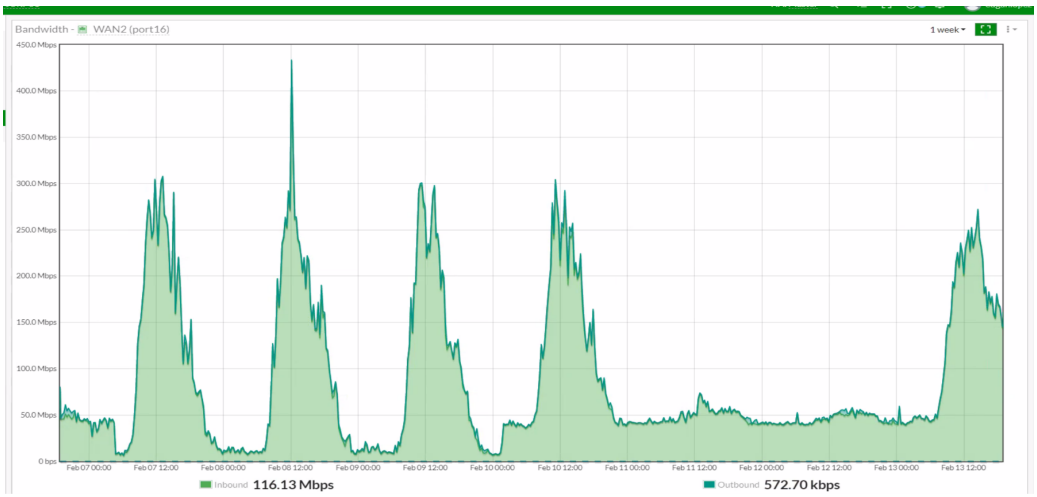


Figura 55.- Consumo del ancho de banda (entrada/salida) de la vía alterna del Core (WAN2) del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo del ancho de banda de la semana del 7 al 13 de Febrero del 2023.

En la figura 56, se presenta un muestreo del 21 al 27 de febrero 2023, sobre el puerto 16 del comportamiento ancho de banda durante el horario laboral en el campus, no deja de ser continuo, teniendo un pico máximo de hasta 700 Mbps.

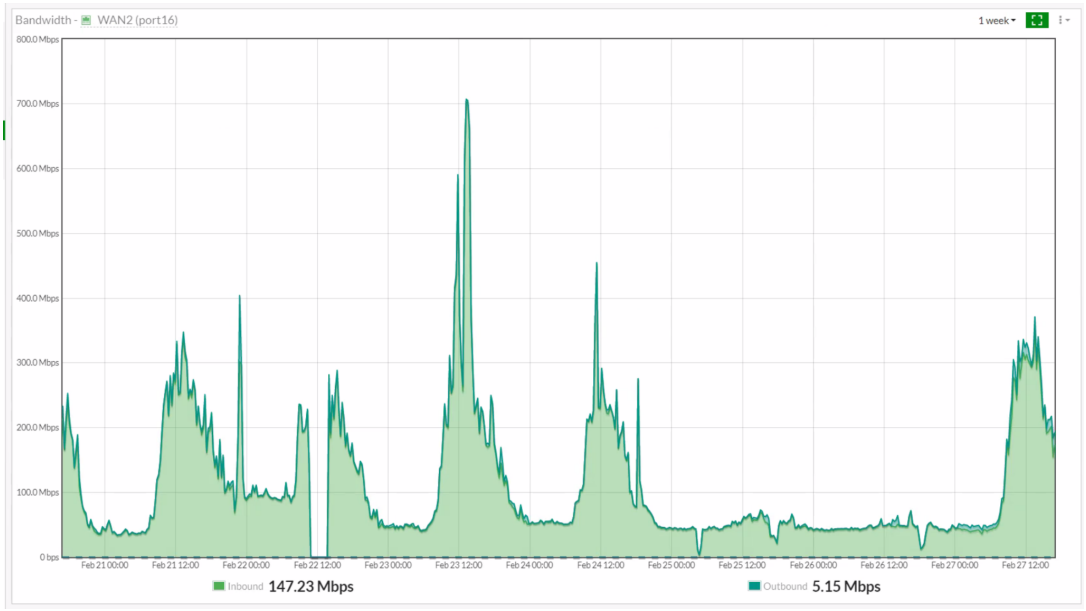


Figura 56 .- Consumo del ancho de banda (entrada/salida) de la vía alterna del Core (WAN2) del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo del ancho de banda de la semana del 21 al 26 de Febrero del 2023.

Centro de Física Aplicada y Tecnología Avanzada (CFATA)

El centro de Física Aplicada y Tecnología Avanzada (CFATA), está clasificado con un perfil grande, en la figura 57 se muestra el consumo del enlace principal que tiene el instituto del 7 al 13 de febrero, el cual muestra un pico de envio hasta de 180 Mbps, el cual se reduce hasta 120 Mbps de envío en la figura 58 que tiene el muestreo del 21 al 23 de Febrero

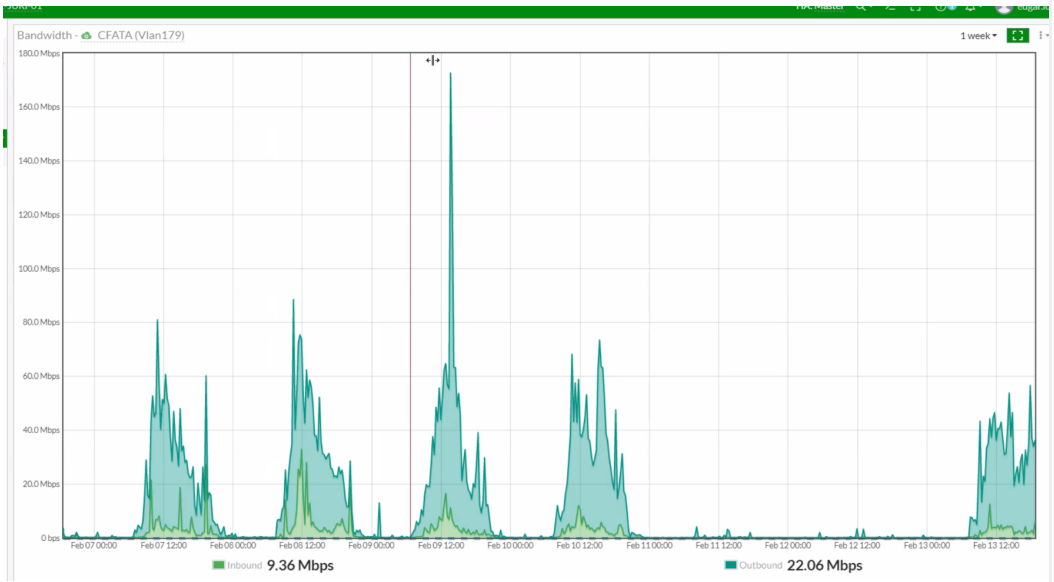


Figura 57.- Consumo del ancho de banda (entrada/salida) de CFATA del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo de la semana del 7 al 13 de Febrero del 2023.

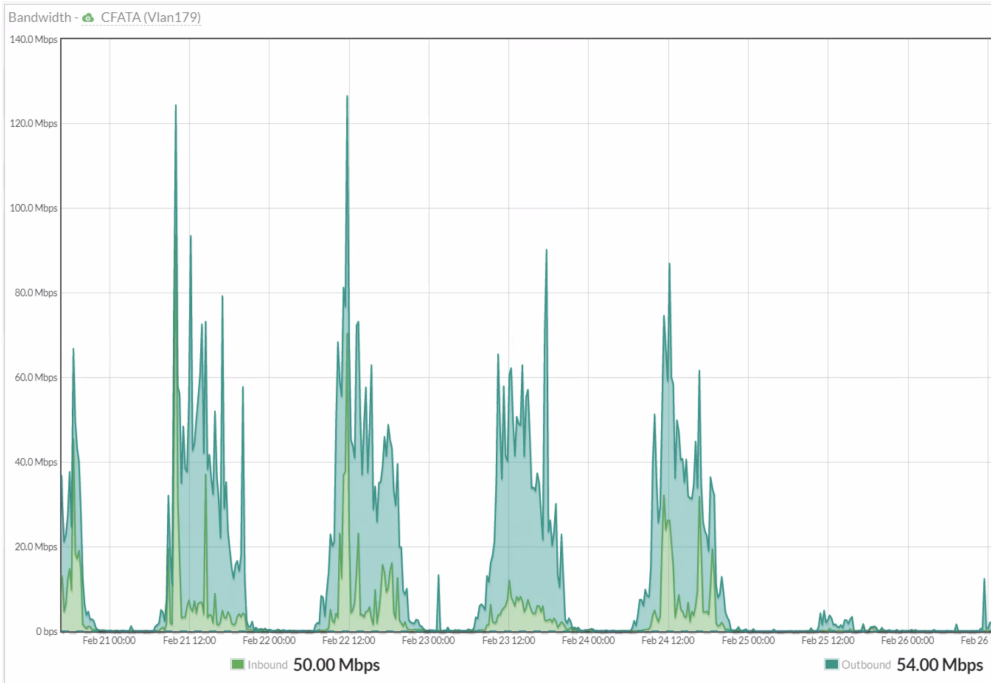


Figura 58.- Consumo del ancho de banda (entrada/salida) de CFATA del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo de la semana del 21 al 26 de Febrero del 2023.

Laboratorio de Investigación en Procesos Avanzados de Tratamiento de Aguas (LIPATA)

Para el laboratorio LIPATA se asignó perfil mediano, ya que sus picos máximos de envío oscilan entre 80 y 65 Mbps, como se muestra en la figura 59 y 60.

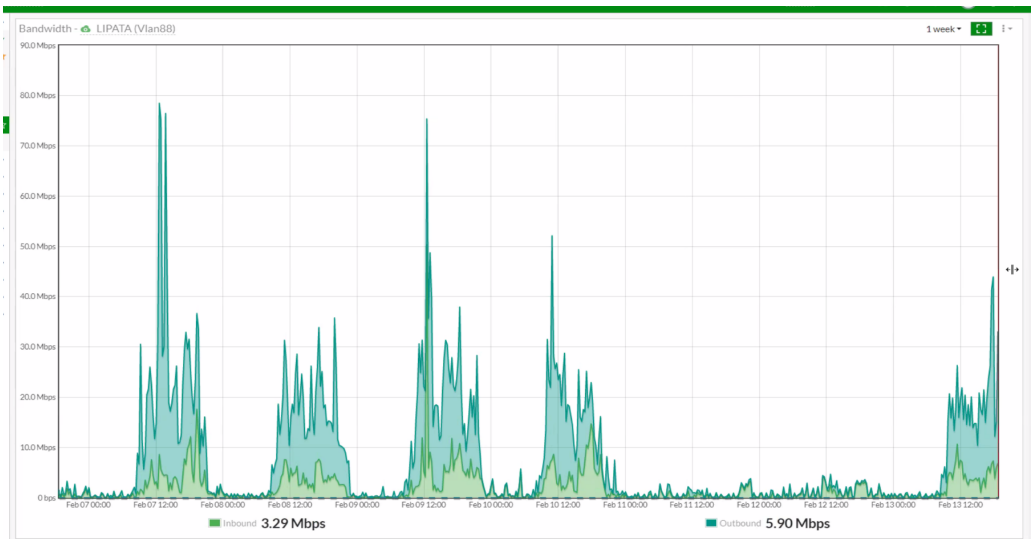


Figura 59.- Consumo del ancho de banda (entrada/salida) de LIPATA del campus Juriquilla.

Muestreo del promedio del consumo de la semana del 7 al 13 de Febrero del 2023.

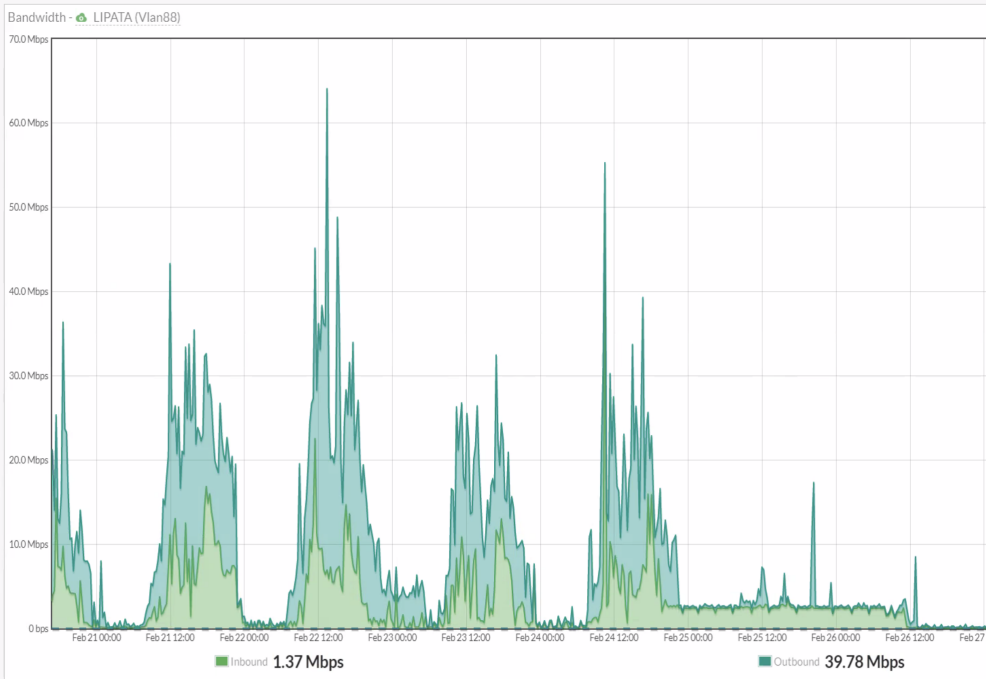


Figura 60.- Consumo del ancho de banda (entrada/salida) de LIPATA del campus Juriquilla.

Muestreo del promedio del consumo de la semana del 7 al 13 de Febrero del 2023.

Escuela Nacional de Estudios Superiores Juriquilla (ENESJ)

La ENES Juriquilla se clasificó como perfil grande, es un caso interesante, ya que del 7 al 13 de febrero se comenzaba el inicio de semestre y se observa que tiene un consumo muy pequeño pero un pico máximo de casi 120 Mbps en horario nocturno.

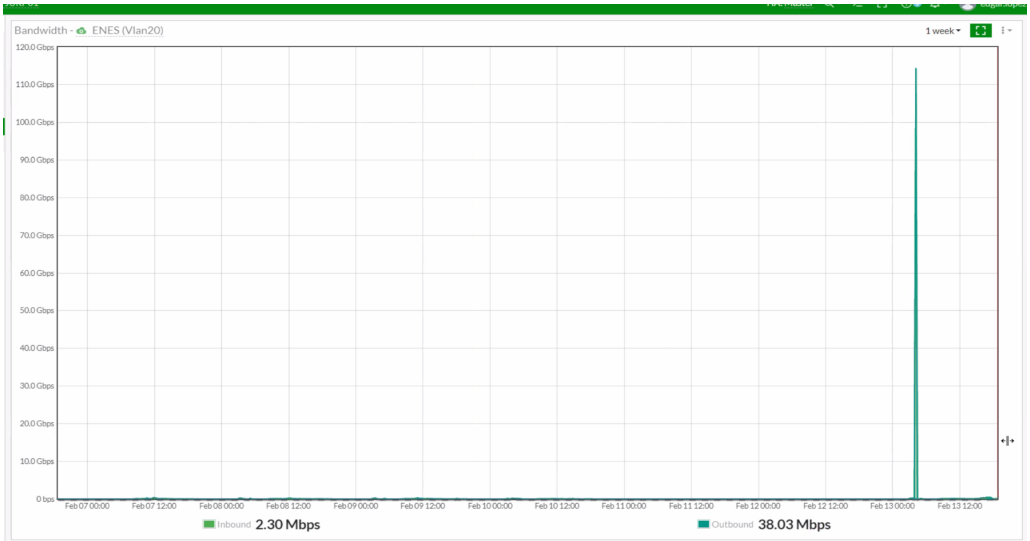


Figura 61- Consumo del ancho de banda (entrada/salida) de ENES del campus Juriquilla.

Muestreo del promedio del consumo de la semana del 7 al 13 de Febrero del 2023.

Este comportamiento cambia radicalmente en el muestreo del 21 al 23 de febrero, donde la comunidad estudiantil está más activa, y en la figura 62, se puede observar un pico máximo de hasta 800 Mbps, nuevamente en horario nocturno. Se detectó que hay un esquema de respaldo en nube que demanda este consumo.

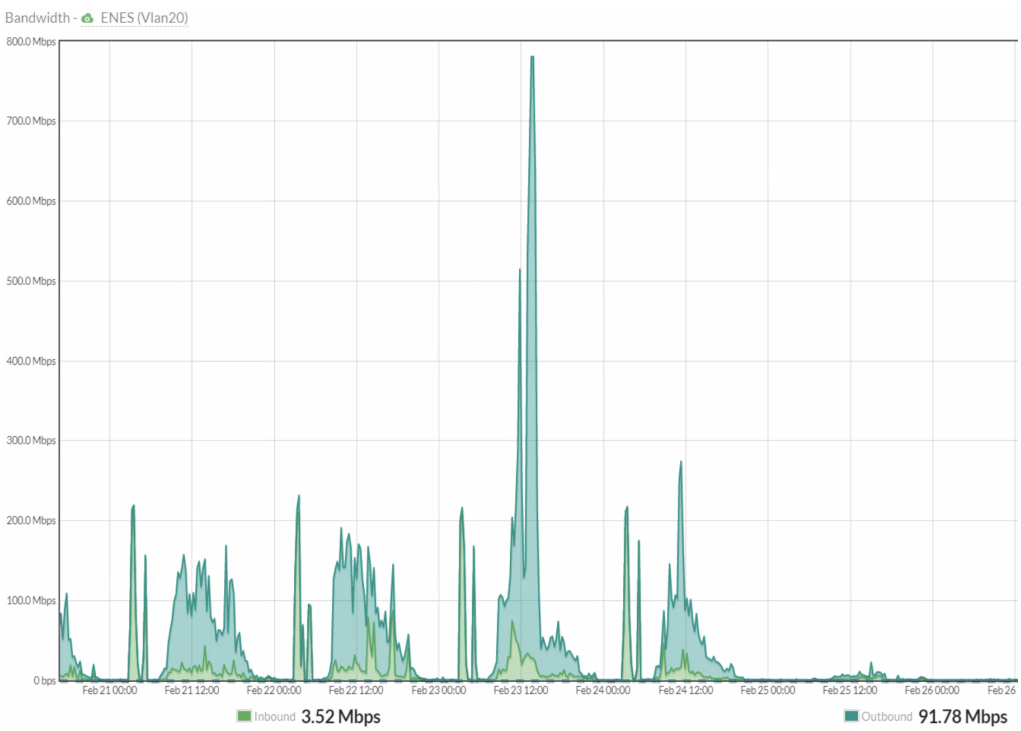


Figura 62.- Consumo del ancho de banda (entrada/salida) de ENES del campus Juriquilla.

Muestreo del promedio del consumo de la semana del 21 al 26 de Febrero del 2023.

Instituto de Matemáticas

El instituto de matemáticas recibió una clasificación de perfil chico, el cual se puede corroborar en la figura 63 y 64 , que su pico máximo no llega a los 80 Mbps

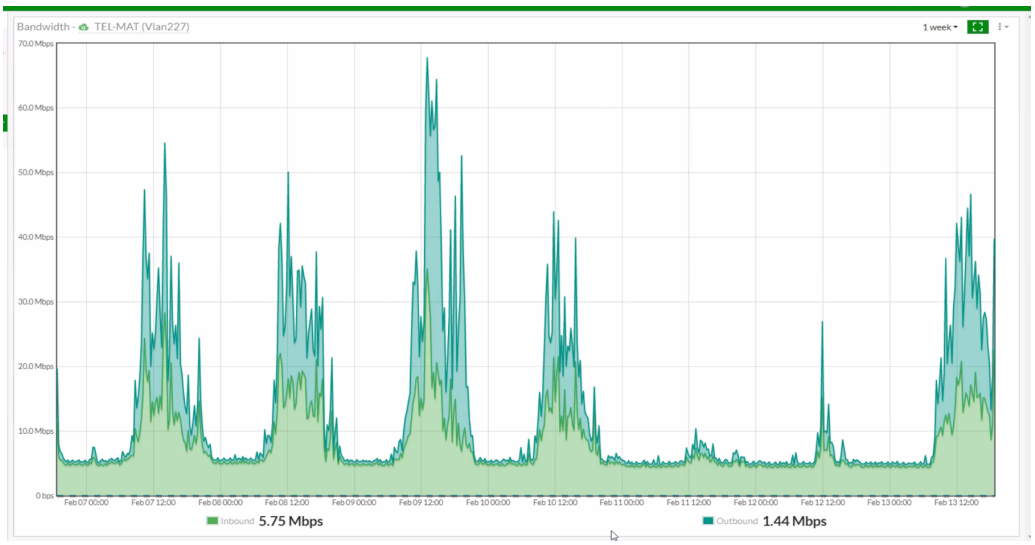


Figura 63.- Consumo del ancho de banda (entrada/salida) de Instituto de Matemáticas del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo de la semana del 7 al 13 de Febrero del 2023.

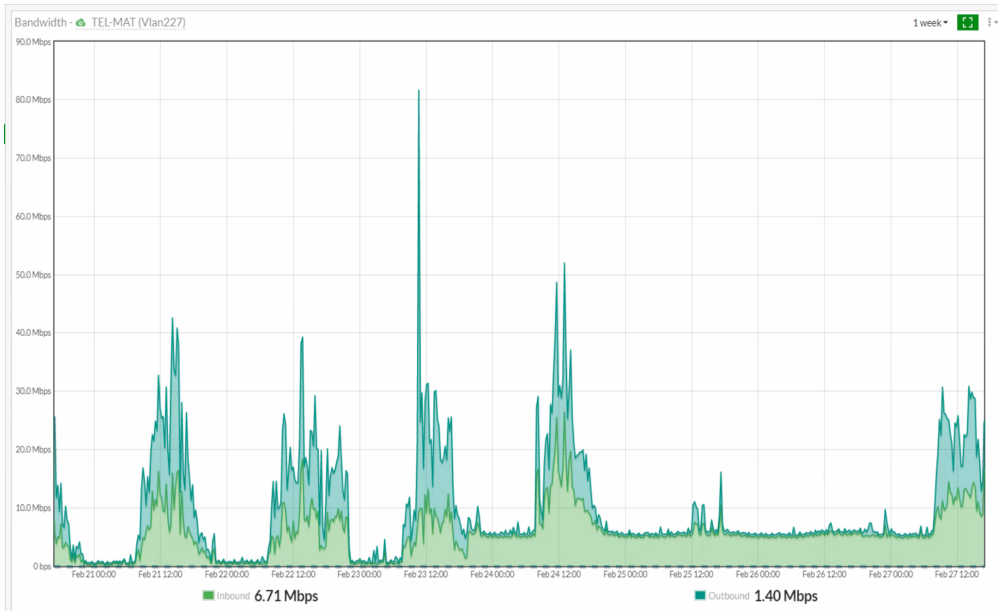


Figura 64.- Consumo del ancho de banda (entrada/salida) de Instituto de Matemáticas del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo de la semana del 21 al 26 de Febrero del 2023.

Instituto de Neurobiología (INB)

El INB es uno de los institutos con perfil mediano, en el muestreo del 7 al 13 de febrero 2023, tiene un pico máximo de ancho de banda de envió de más de 400Mbps.

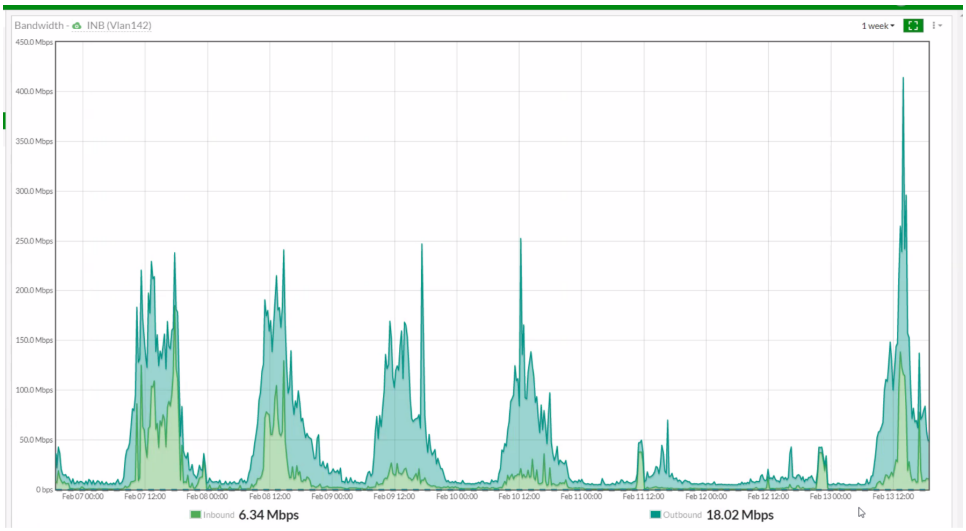


Figura 65.- Consumo del ancho de banda (entrada/salida) de Instituto de Biología del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo de la semana del 7 al 13 de Febrero del 2023.

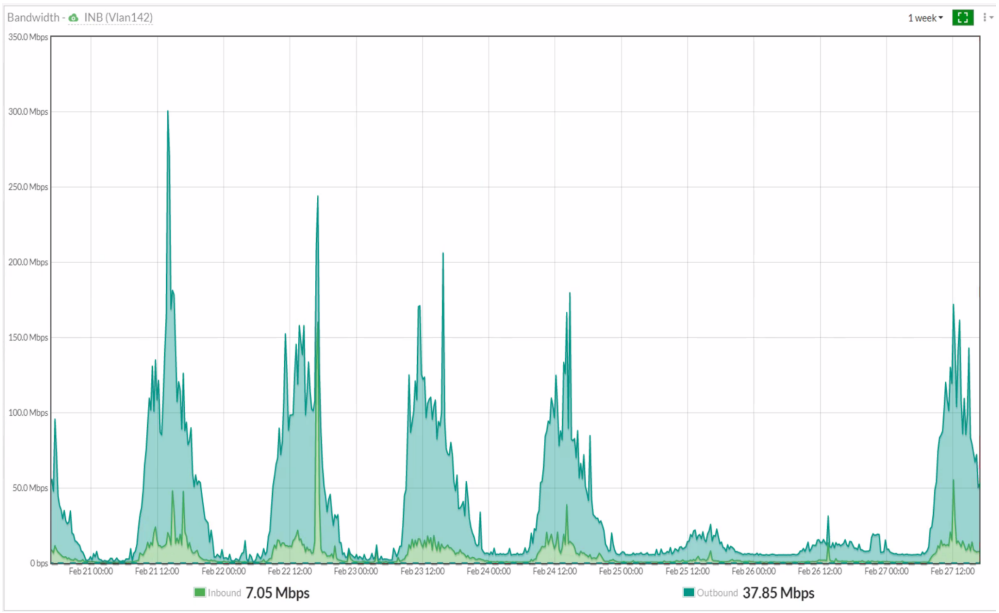


Figura 66- Consumo del ancho de banda (entrada/salida) de Instituto de UMDI del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo de la semana del 21 al 26 de Febrero del 2023.

Unidad Multidisciplinaria de Docencia e Investigación de la Facultad de Ciencias (UMDI)

La UMDI, tiene una clasificación de perfil chico dado que el pico máximo es de 140 Mbps en el consumo de ancho de banda de envió que se presenta en la figura 68.

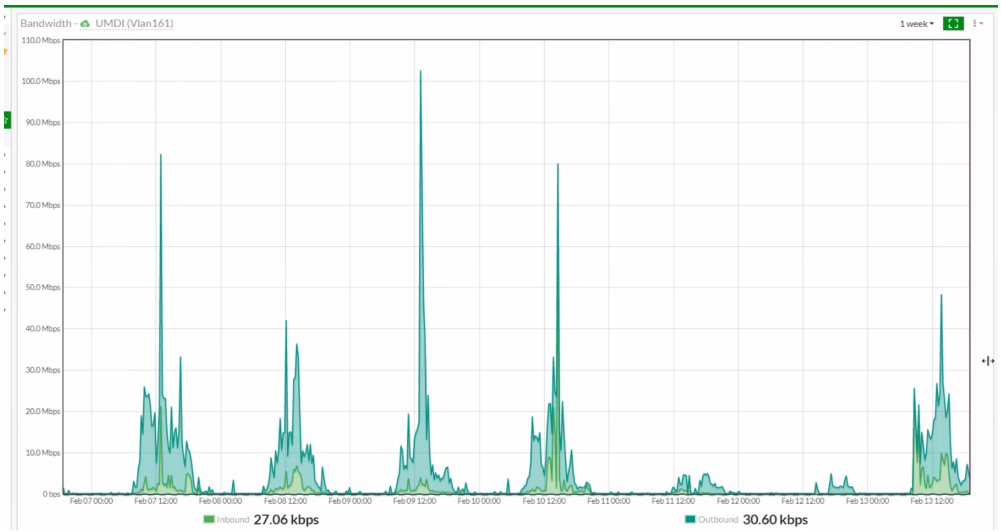


Figura 67.- Consumo del ancho de banda (entrada/salida) de Instituto de UMDI del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo de la semana del 7 al 13 de Febrero del 2023.

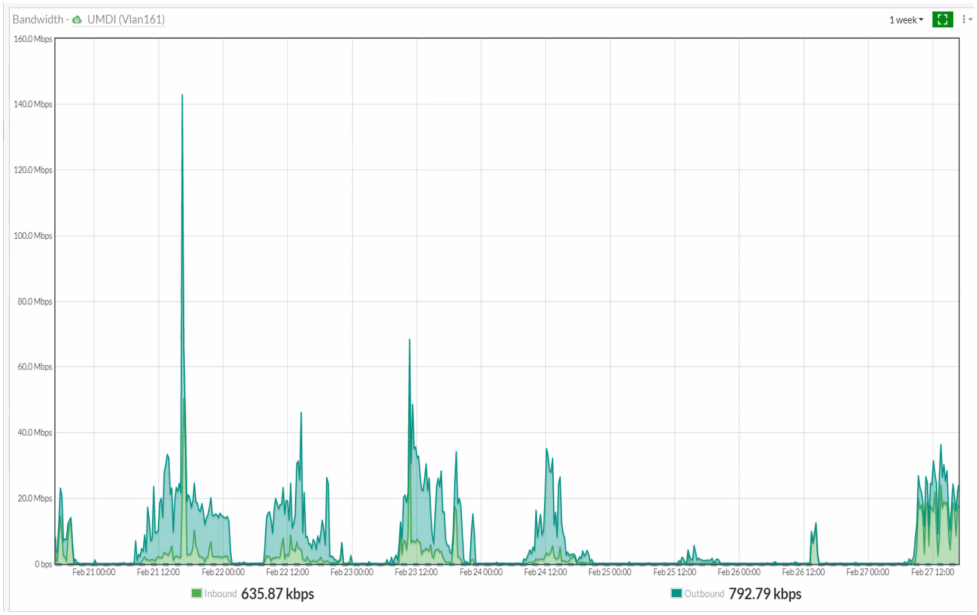


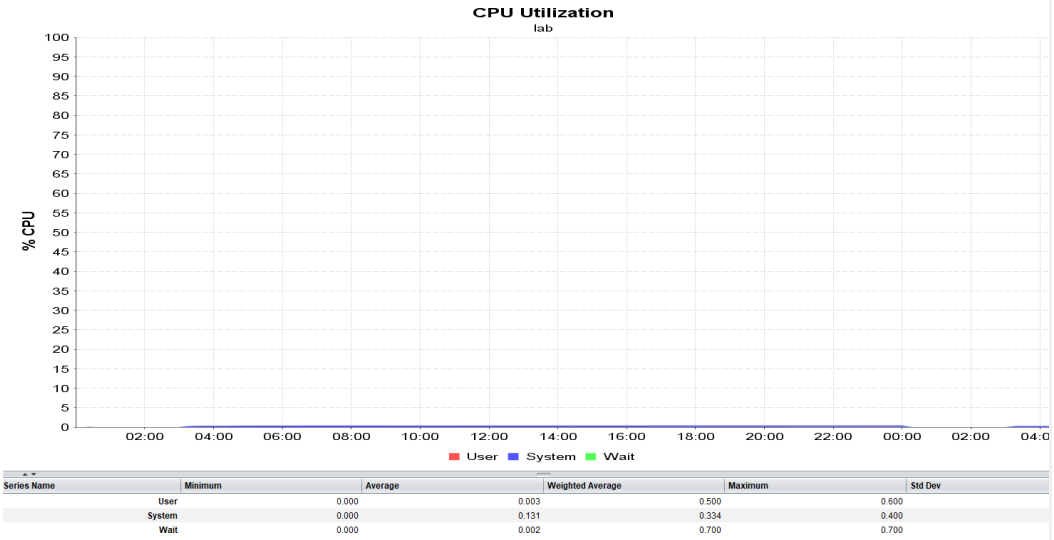
Figura 68.- Consumo del ancho de banda (entrada/salida) de Instituto de Matemáticas del campus Juriquilla.

Muestreo del promedio del promedio diario del consumo de la semana del 21 al 26 de Febrero del 2023.

Anexo I .-Recursos utilizados por Firewall Shorewall (LAB) en HTTP en IPv6

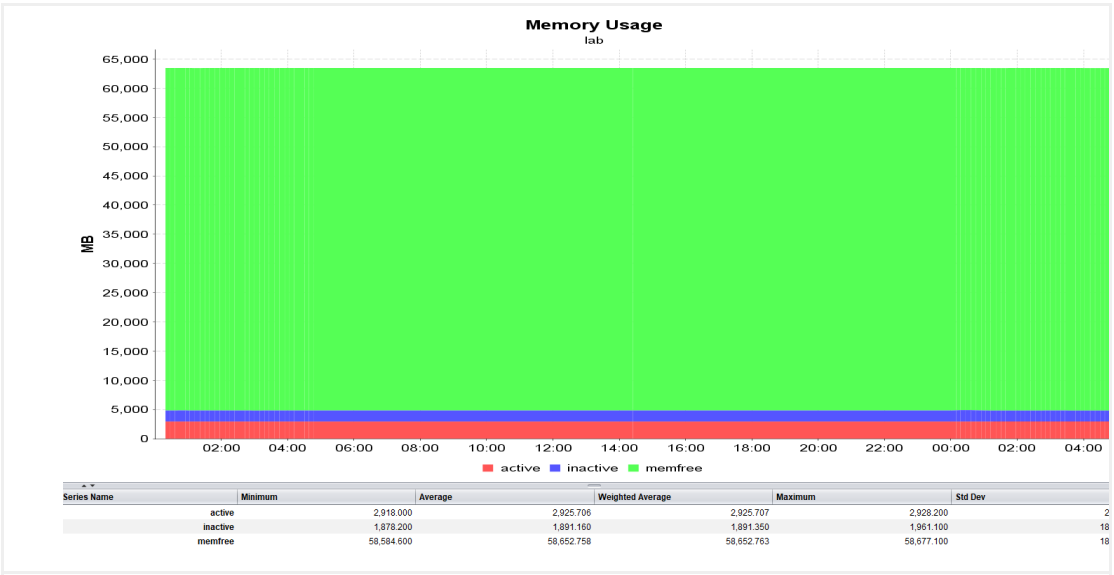
A continuación, se muestran los resultados que se obtuvieron de la herramienta de monitoreo de nmon, los cuales se tuvieron que procesar con la herramienta de NMON visualizer, a fin de consolidar los registros.

En la figura 69 se presenta el porcentaje de la utilización del CPU que se tuvo durante la prueba de peticiones de la herramienta iperf sobre la red de IPv6. Se observa en la gráfica que se presentan el consumo máximo clasificado por sistema, usuario y ocioso.



Series Name	Minimum	Average	Weighted Average	Maximum	Std Dev
User	0.000	0.003	0.500	0.600	
System	0.000	0.131	0.334	0.400	
Wait	0.000	0.002	0.700	0.700	

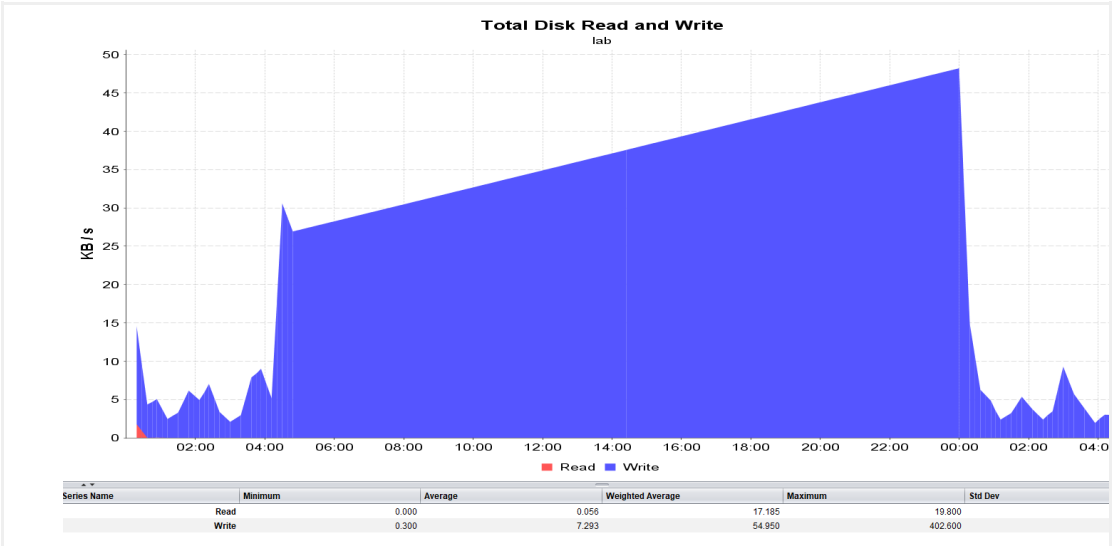
Figura 69.- Porcentaje de utilización de CPU del Firewall Shorewall durante la prueba HTTP en IPv6.



Series Name	Minimum	Average	Weighted Average	Maximum	Std Dev
active	2,918.000	2,925.706	2,925.707	2,928.200	2
inactive	1,878.200	1,891.160	1,891.350	1,961.100	18
memfree	58,584.600	58,652.758	58,652.763	58,677.100	18

Figura 70.- Uso de memoria (MB) del Firewall Shorewall durante la prueba HTTP en IPv6.

Para el recurso de memoria en el firewall shorewall, el cual se puede observar en la figura 70, se tiene un máximo de 64GB y no se consume ni 3GB durante toda la prueba. En el comportamiento que se tiene en el disco en lectura y escritura no llega ni a los 50 kB/s.



Series Name	Minimum	Average	Weighted Average	Maximum	Std Dev
Read	0.000	0.056	17.185	19.800	
Write	0.300	7.293	54.950	402.600	

Figura 71.- Total de Lectura /Escritura en disco (Kb/s) del Firewall Shorewall durante la prueba HTTP en IPv6.

El recurso que nos interesa resaltar en el firewall shorewall es la saturación en el puerto de red, la herramienta registra la lectura y escritura en el puerto de red, alcanzó un máximo de 125 MB/s, que en conjunto no alcanzó ni los 250Mb/s, al aplicar las reglas de ruteo y filtrado que se establecieron para conectividad de zona D con zona E. Cabe resaltar que se mantuvo fijo el bitrate de 100Mbps.

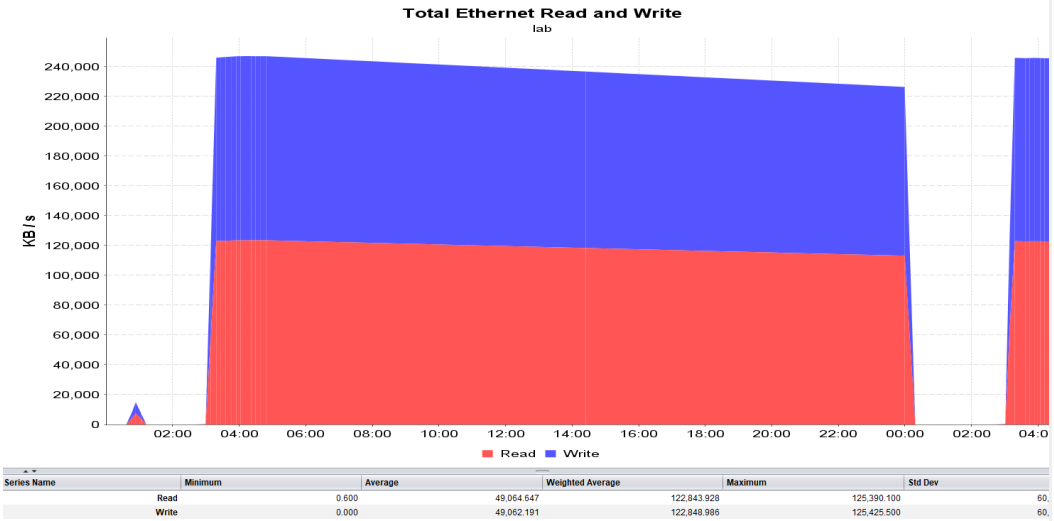
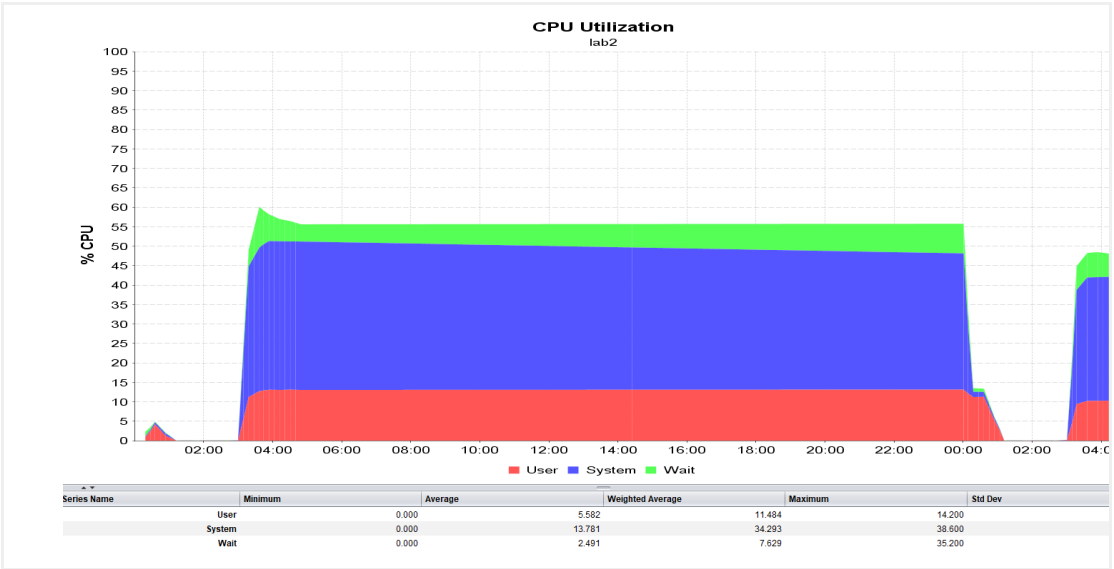


Figura 72.- Total de Lectura y Escritura en red (Kb/s) del Firewall Shorewall durante la prueba HTTP en IPv6.

Anexo J.- Recursos utilizados por Cliente (LAB2) en las pruebas HTTP con IPv6

Otro componente es el cliente que genera las peticiones hacia el servidor HTTP; en la figura 73, se presenta el porcentaje de utilización de CPU, donde se presenta un consumo máximo de hasta de un 38% de consumo por el sistema.



Series Name	Minimum	Average	Weighted Average	Maximum	Std Dev
User	0.000	5.582	11.484	14.200	
System	0.000	13.781	34.293	38.600	
Wait	0.000	2.491	7.629	35.200	

Figura 73.- Porcentaje de utilización de CPU del cliente durante la prueba HTTP en IPv6.

En la figura 74, se presenta el consumo de memoria del cliente que generó las peticiones, se tuvo un consumo máximo 10GB hecho por el sistema.

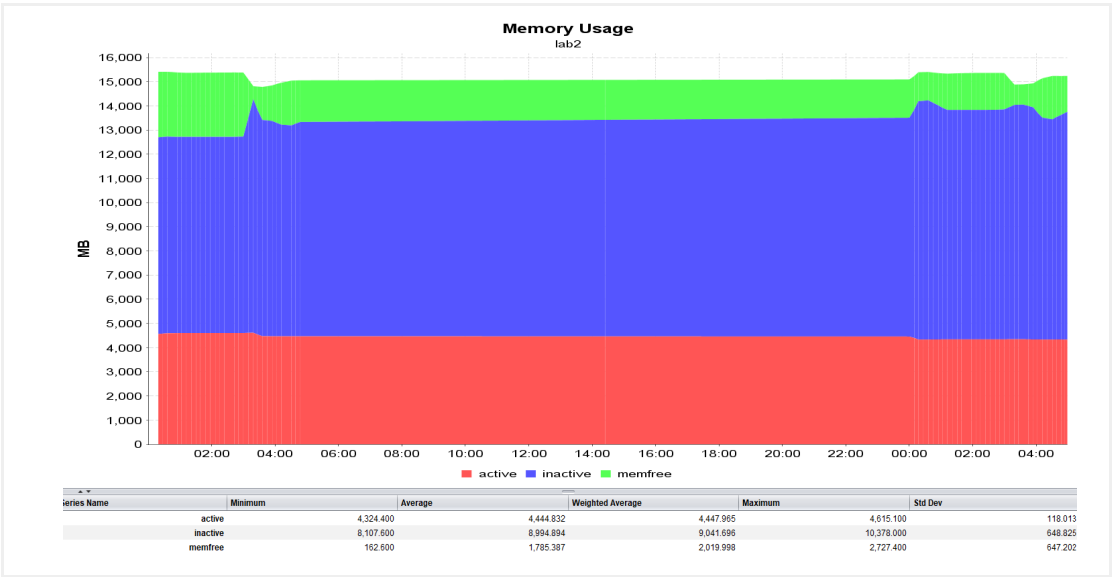


Figura 74.- Uso de memoria (MB) del cliente durante la prueba HTTP en IPv6.

Durante la prueba, se generaron bitácoras de los comportamientos de las peticiones de descargas en el servidor HTTP y por tanto se presentó escritura y lectura en el disco, se pueden observar este comportamiento en la figura 75, generando un máximo de 750 KB/s de lectura y escritura.

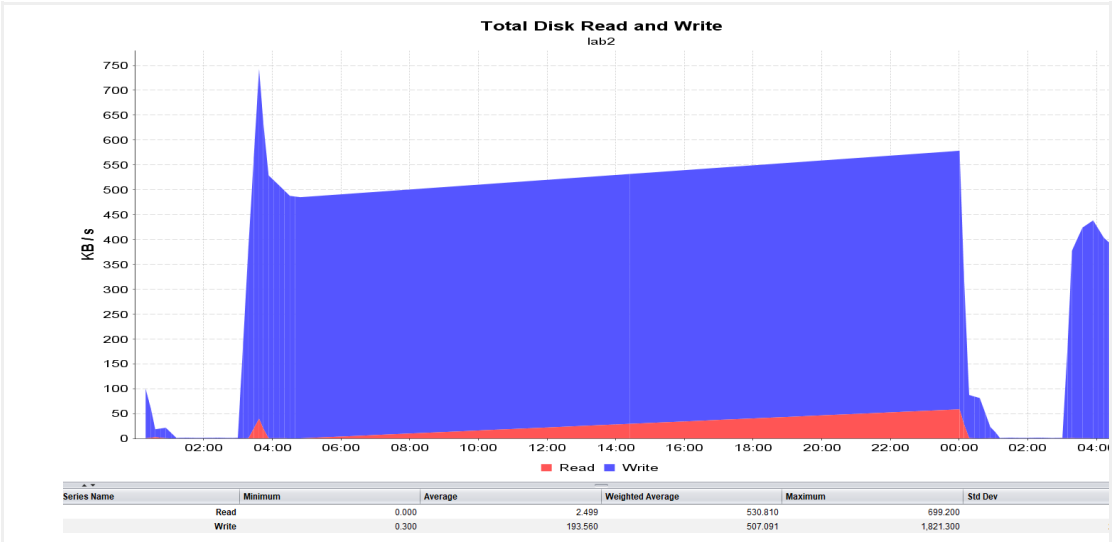
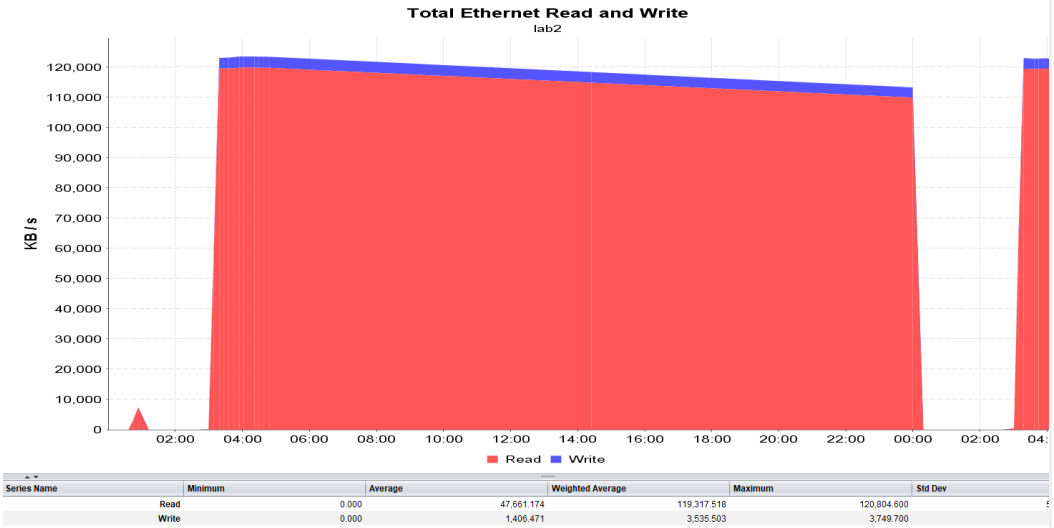


Figura 75.- Total de lectura y escritura en disco (Kb/s) del cliente durante la prueba HTTP en IPv6.

El comportamiento del recurso de la red, se presenta en la figura 76, donde por ser el proveedor de servicio HTTP tiene mayor lectura alcanzó un máximo 120 MB/s.

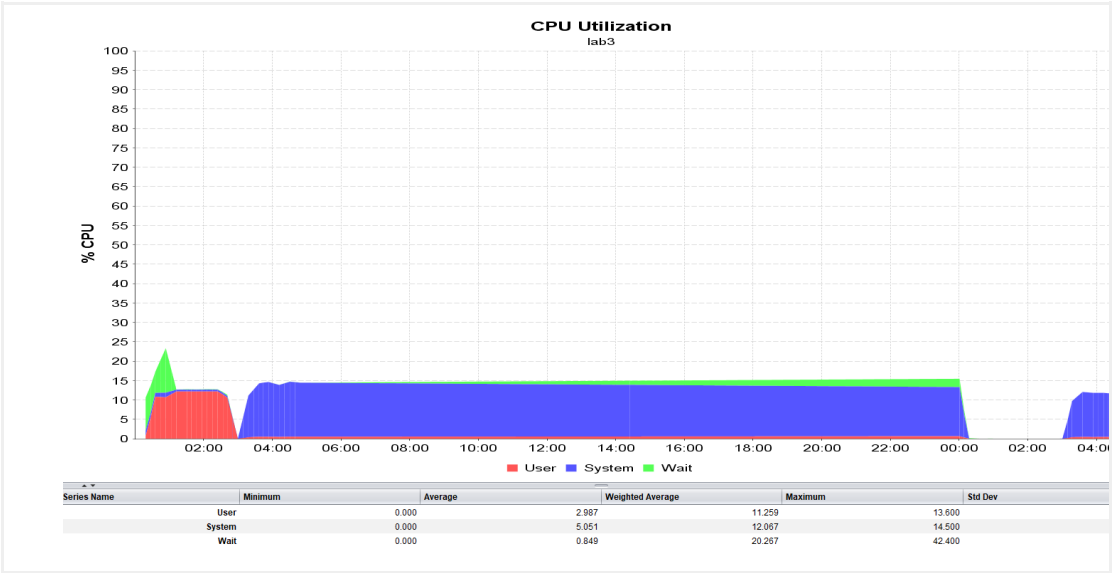


Series Name	Minimum	Average	Weighted Average	Maximum	Std Dev
Read	0.000	47,661.174	119,317.518	120,804.600	
Write	0.000	1,406.471	3,535.503	3,749.700	

Figura 76.- Total de Lectura y escritura en red (kb/s) del cliente durante la prueba HTTP en IPv6.

Anexo K.- Recursos utilizados por Servidor HTTP en IPv6

El proveedor del servicio HTTP configurado con IPv6, logró conseguir hasta un 14% de utilización de CPU



Series Name	Minimum	Average	Weighted Average	Maximum	Std Dev
User	0.000	2.987	11.259	13.600	
System	0.000	5.051	12.067	14.500	
Wait	0.000	0.849	20.267	42.400	

Figura 77.- Porcentaje de utilización de CPU del Servidor durante la prueba HTTP en IPv6.

La memoria llega a tener máximo de 11 Gbs, dejando solo 900Mb como recurso libre.

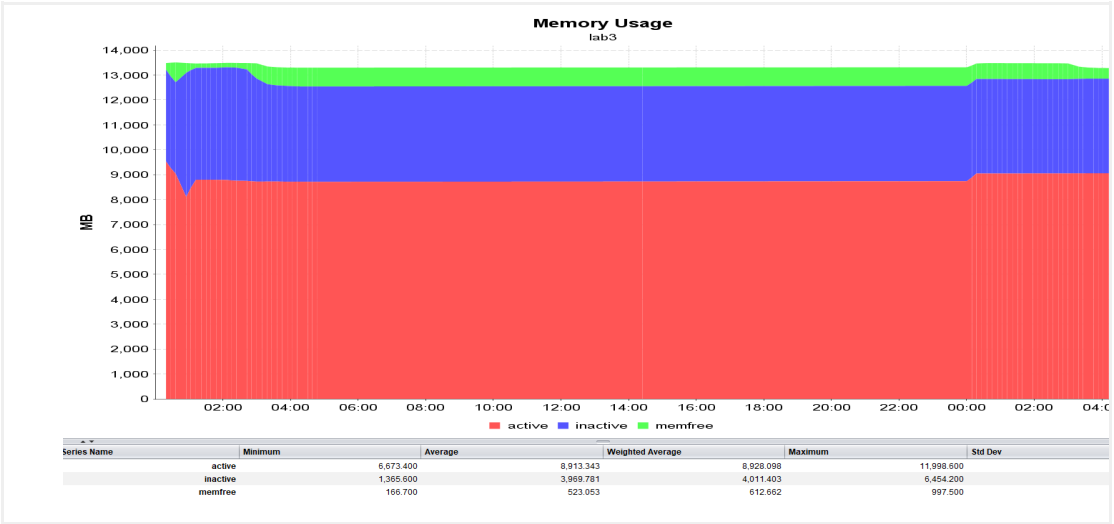


Figura 78.- Uso de memoria (MB) del Servidor durante la prueba HTTP en IPv6.

El disco en el servidor HTTP con IPv6 tuvo actividad previa a la prueba registrada antes de las 2:00 como se muestra en la figura 79, posteriormente, no se genera actividad significativa en el disco,salvo por las bitácoras de apache que se generaron.

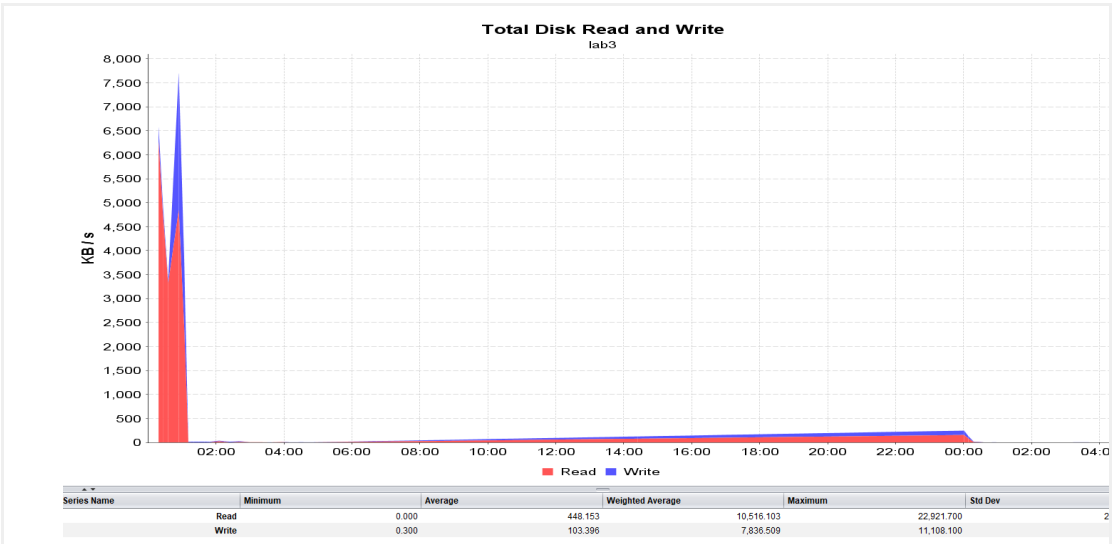


Figura 79.- Total de lectura y escritura sobre disco (Kb/s) del Servidor durante la prueba HTTP en IPv6.

En contraste con el recurso de la red con IPv6 en el servidor, se genera más escritura por el envió de la información alcanzando un máximo de 121 Mb/s, se puede observar en la figura 80.

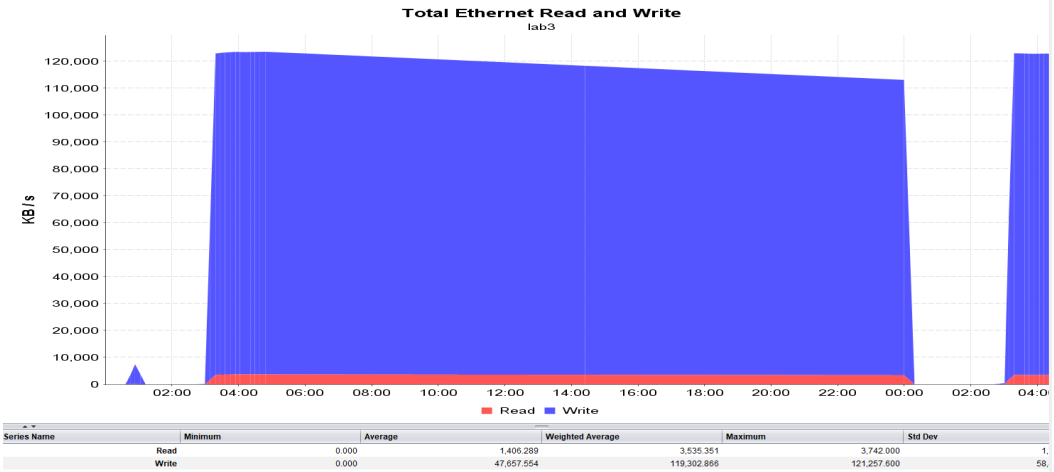
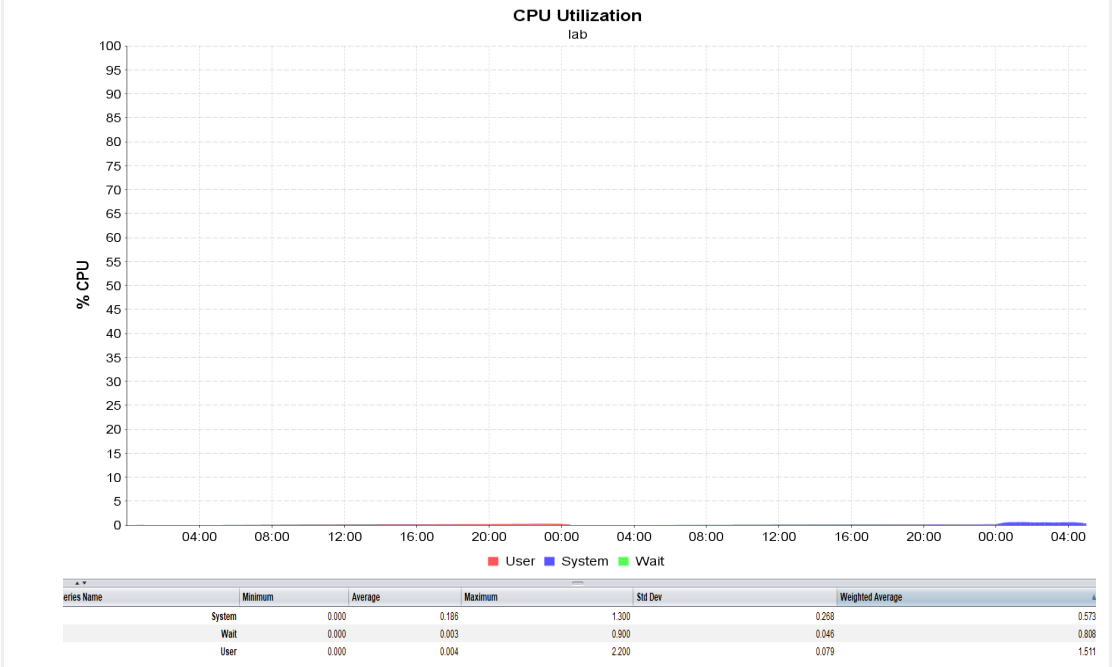


Figura 80.- Total de Lectura y Escritura en red (Kb/s) del Servidor durante la prueba HTTP en IPv6.

Anexo L.- Recursos utilizados por Firewall (LAB) en Prueba HTTP en IPv4

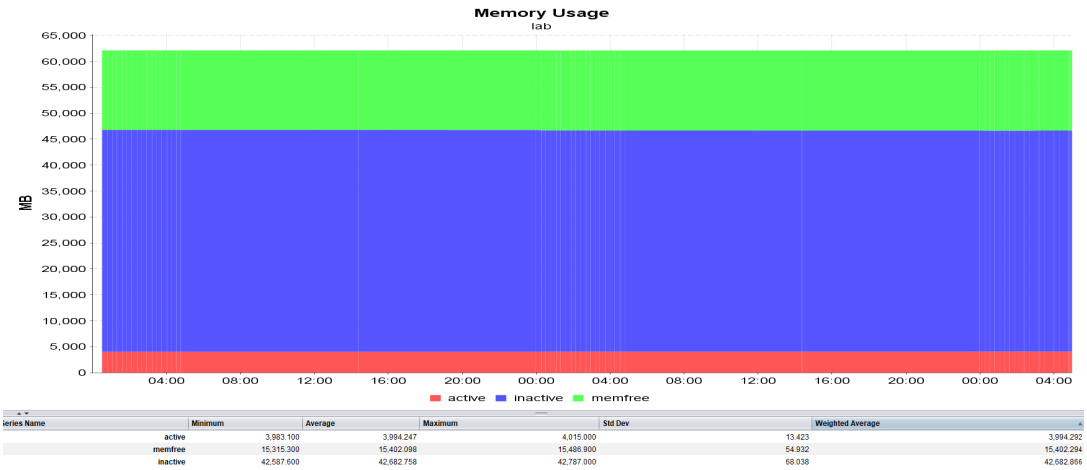
En la figura 81, se presenta el porcentaje de utilización del CPU en el firewall shorewall que se utilizó durante la prueba de peticiones HTTP, en donde se presentan un máximo de 1.3% por el sistema y un 2.2% por el usuario.



eries Name	Minimum	Average	Maximum	Std Dev	Weighted Average
System	0.000	0.186	1.300	0.268	0.573
Wait	0.000	0.003	0.900	0.046	0.808
User	0.000	0.004	2.200	0.079	1.511

Figura 81.- Porcentaje de utilización de CPU del Firewall Shorewall durante la prueba HTTP en IPv4.

Con respecto al consumo de memoria el servidor en IPv4 se presenta la figura 82, se tiene un comportamiento constante previo y durante la ejecución de la prueba, logrando un máximo de hasta 4GB de un total de 64GB disponibles.



eries Name	Minimum	Average	Maximum	Std Dev	Weighted Average
active	3,983.100	3,994.247	4,015.000	13.423	3,994.292
memfree	15,315.300	15,402.098	15,486.900	54.932	15,402.294
inactive	42,587.600	42,682.758	42,787.000	68.038	42,682.866

Figura 82.- Uso de memoria (MB) del Firewall Shorewall durante la prueba HTTP en IPv4.

La actividad del disco en el servidor servidor shorewall presenta mayor escritura que lectura, como se presenta en la gráfica 83, alcanzando un máximo de 1.9 MB/s.

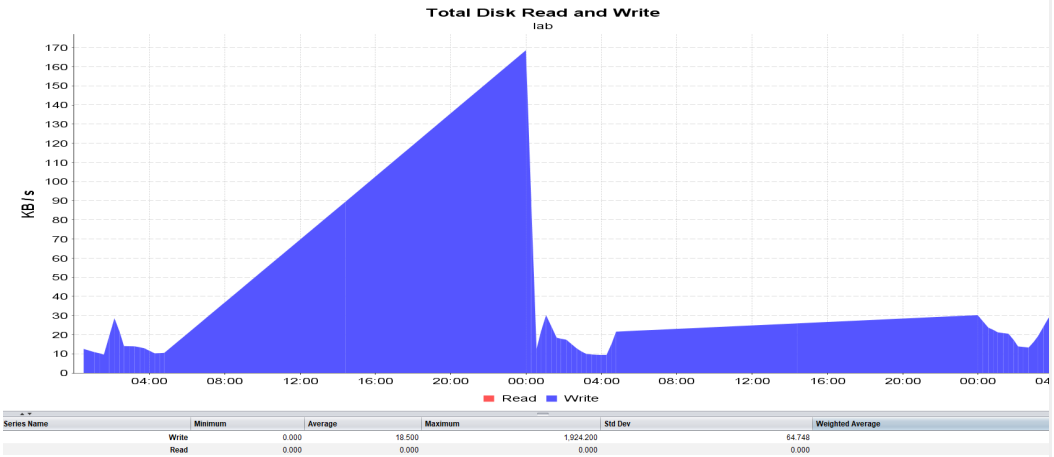


Figura 83.- Total de lectura y escritura en disco (kb/s) del Firewall Shorewall durante la prueba HTTP en IPv4.

En la red se despliega un consumo de hasta 125 Mb/s tanto en lectura como escritura, resultado esperado por el filtrado y redireccionamiento del tráfico de red.

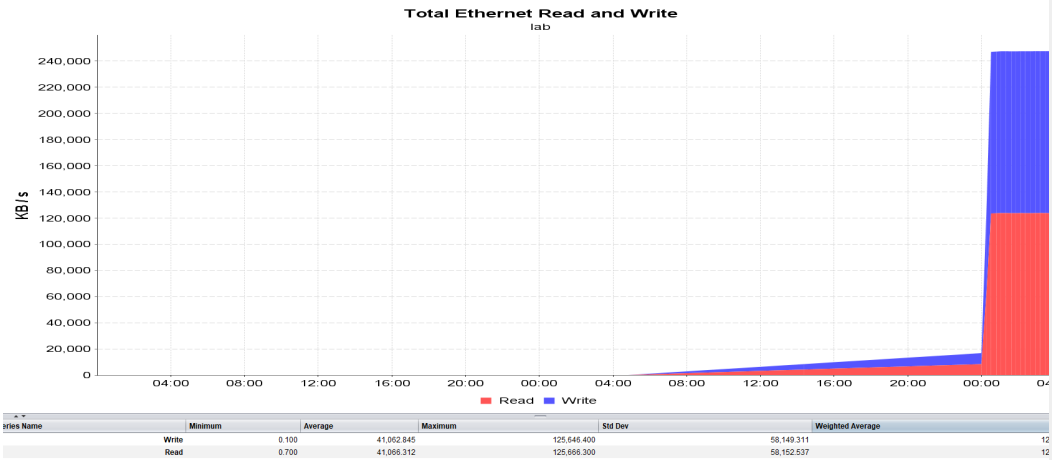


Figura 84.- Total de lectura y escritura en red (kb/s) del Firewall Shorewall durante la prueba HTTP en IPv4.

Anexo M.- Recursos utilizados por Servidor HTTP con IPv4

El servidor HTTP con IPv4, tiene un porcentaje de utilización con un máximo en sistema del 15% y a nivel usuario un 18%.

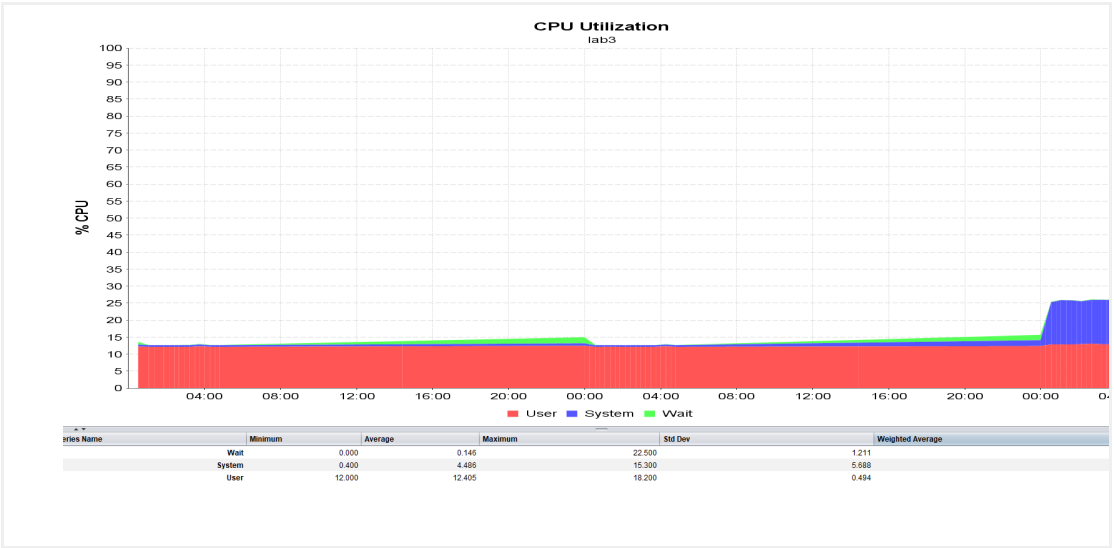


Figura 85.- Porcentaje de utilización de CPU del servidor HTTP durante la prueba con IPv4.

El uso de la memoria presenta un máximo de consumo hasta por 9GB(ver figura 86).

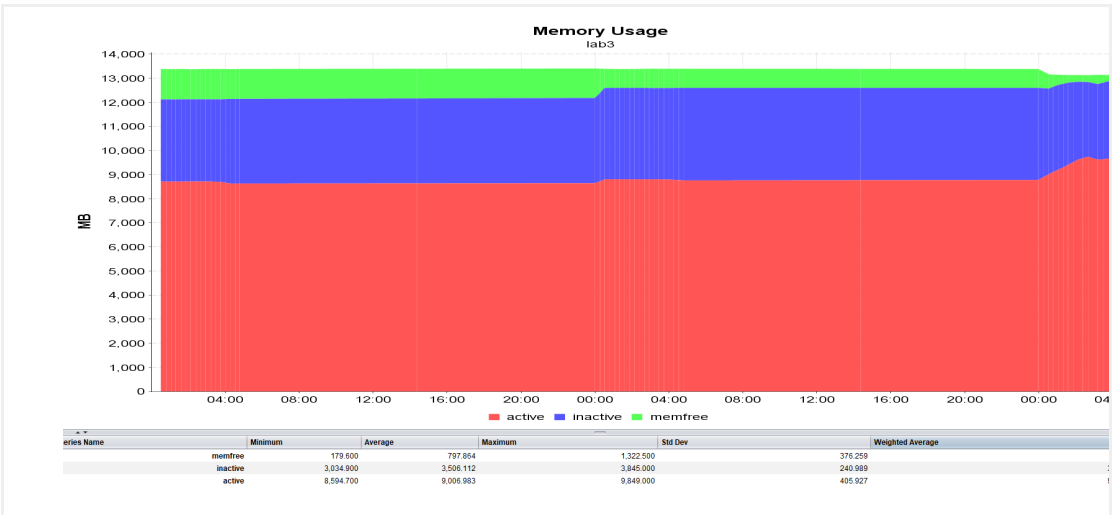


Figura 86.- Uso de memoria (MB) del Servidor durante la prueba HTTP en IPv4.

El total de lectura y escritura en el disco del servidor HTTP se generan con un máximo de 3Mb/s respectivamente.

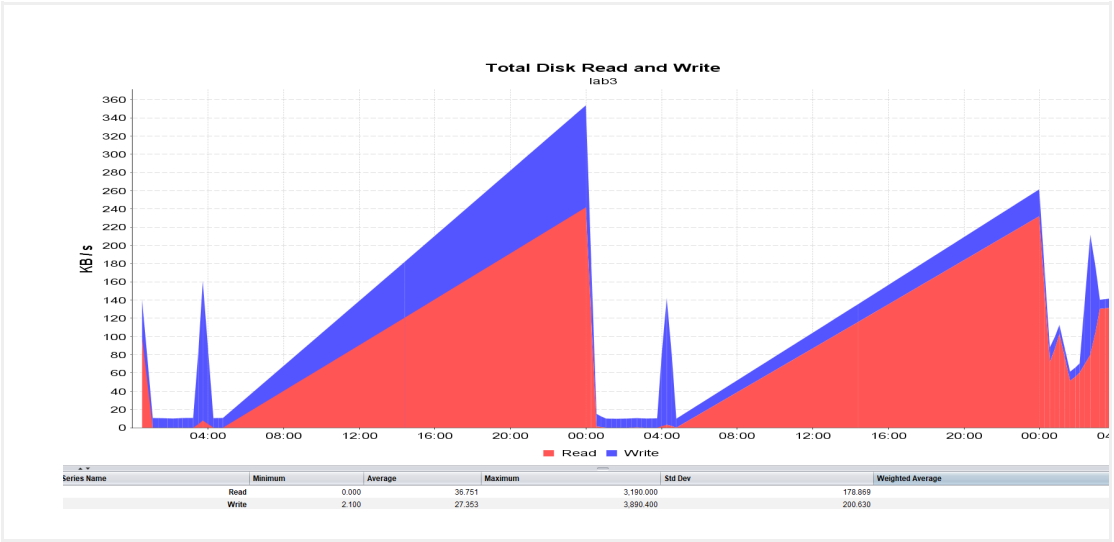


Figura 87.- Total de Lectura y Escritura en Disco (Kb/s) del Servidor durante la prueba HTTP en IPv4.

El registro del total del consumo de lectura y escritura en la red del servidor HTTP en conjunto es inferior a los 124 MB/s, sin embargo, predomina la escritura con un máximo de 121 MB/s.

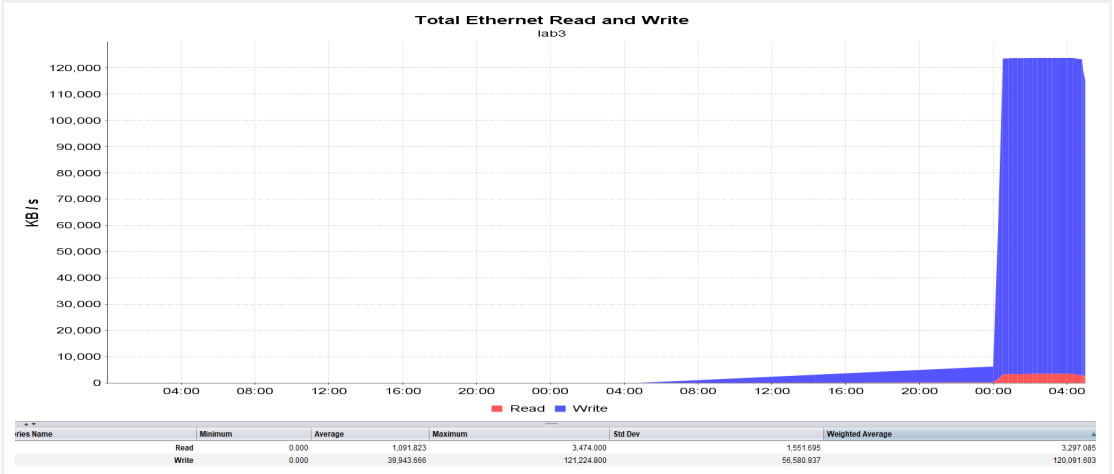


Figura 88- Total de Lectura y Escritura de red (Kb/s) del Servidor durante la prueba HTTP en IPv4.

Anexo N.- Recursos utilizados por cliente en prueba HTTP en IPv4

La utilización del CPU del cliente es baja a pesar de ser quien genera las descargas hacia el servidor (ver figura 89) alcanzando un máximo de 39% por el sistema y un 27.5% por el usuario.

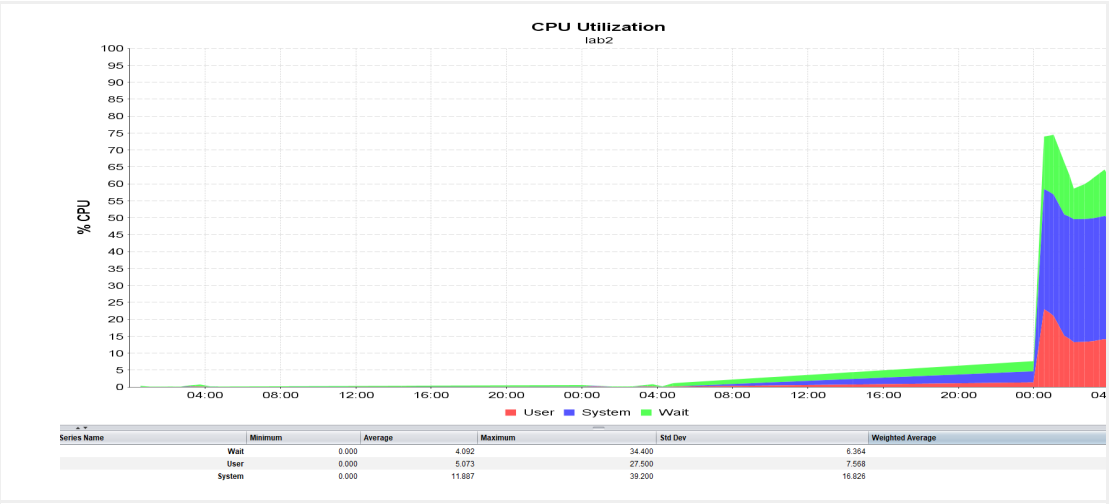


Figura 89.- Porcentaje de utilización de CPU del Cliente durante la prueba HTTP en IPv4

El uso de la memoria en el cliente alcanza un máximo de 1GB durante la ejecución de la prueba (ver figura 90).

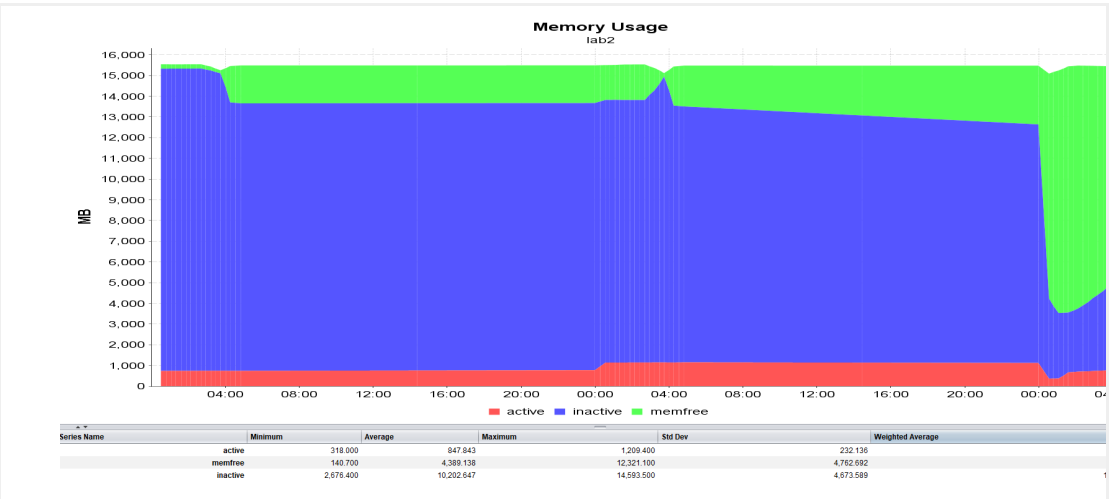


Figura 90.- Uso de memoria (MB) del cliente durante la prueba HTTP en IPv4.

Dado que durante la ejecución de la prueba se guarda registro de la duración de las peticiones de descarga, por ello, se genera lectura y escritura en el disco, se presenta el comportamiento del recurso en la figura 91, obteniendo un máximo en escritura de 1Mb/s y un máximo en lectura del 100 Kb/s.

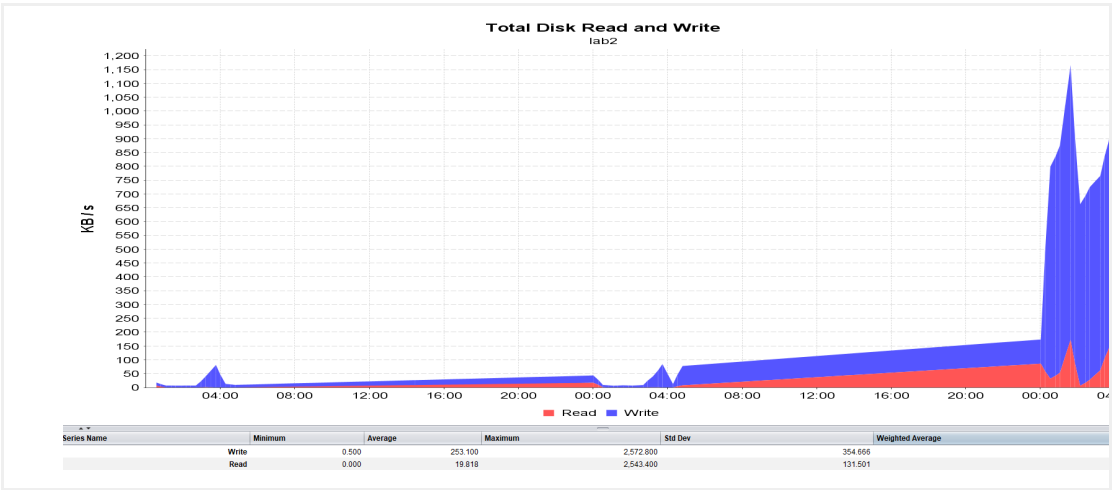


Figura 91.- Escritura y Lectura de Disco (Kb/s) del Cliente durante la prueba HTTP en IPv4.

En la red se tuvo un máximo de 110 Mb/s para lectura y en escritura un máximo de 3 Kb/s (ver figura 92).

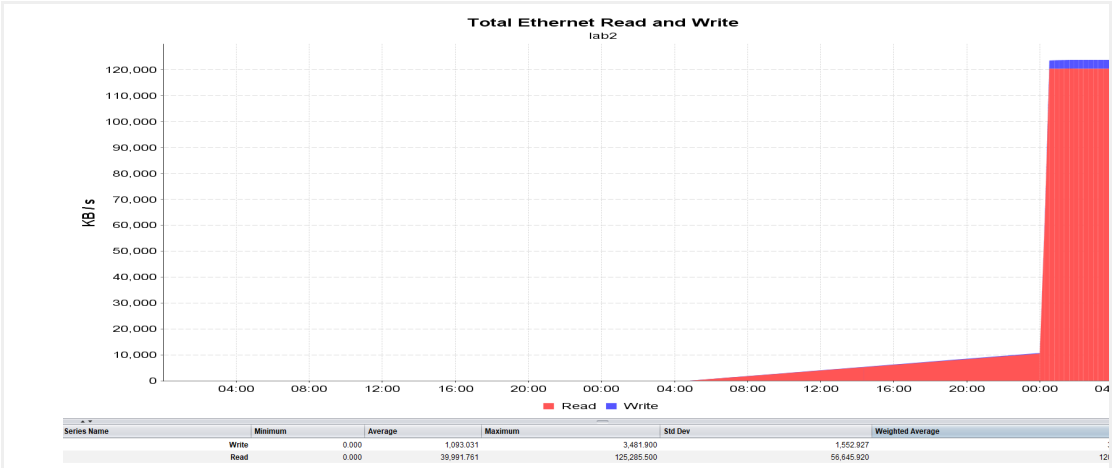


Figura 92.- escritura y Lectura de red (Kb/s) durante la prueba HTTP en IPv4.

Acrónimos

1. SIIT-DC.-Stateless IP/ICMP Translation for IPv6 Data Centers Environments
2. BR.-Border Relay
3. ECMP.- Equal-cost multi-path routing
4. EAM.- Explicit Address Mapping
5. CPE.-Customer Premises Equipment
6. DNS .- Domain Name Server
7. ISP- Internet Service Provider
8. NAT.- Network Address Translation-Protocol
9. PLAT.- Provider Side Translator
10. CLAT.- Customer Side Translator
11. WKP.- Well-Known-Prefix
12. NSP.- Network-Specific-Prefix
13. CLAT.- Customer-side transLATor
14. PLAT.-Provider-side transLATor
15. FQDN.-Fully Qualified Domain Name
16. GLBP.-Gateway Load Balancing Protocol
17. VRRP.-Virtual Router Redundancy Protocol
18. HSRP.-Hot Standby Router Protocol
19. OSPF.- Open Shortest Path First
20. EIGRP.-Enhanced Interior Gateway Routing Protocol
21. IS-IS.-Intermediate System-to-Intermediate System
22. RIPv6.-Routing Information Protocol version 6
23. BGP.-Border Gateway Protocol
24. CIDR.-Classless Inter-Domain Routing
25. ULA.- Unique Local Addressing
26. GUI.- Global Unicast Addressing
27. SIP.- Session Initialization Protocol
28. IMS.- IP Multimedia Subsystem
29. GUA.- Global unicast addresses
30. DP!.- Deep packet Inspection

Bibliografía

[1] Michael Dooley; Timothy Rooney, *IPv6 Deployment and Management*. 2013. Accessed: Jan. 09, 2023. [Online]. Available: http://pbidi.unam.mx:8080/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=cat02025a&AN=lib.MX001002173723&lang=es&site=eds-live

[2] G. Cicileo *et al.*, "IPv6 for All A Guide for IPv6 Usage and Application in Different Environments," 2009. Accessed: Jan. 09, 2023. [Online]. Available: https://www.ipv6forum.com/dl/books/ipv6forall.pdf

[3] "1.4. La solución: IPv6 - IPv6." https://sites.google.com/site/tknikaipv6/1-ipv6-basico/1-4-la-solucion-ipv6 (accessed Jan. 02, 2023).

[4] I. Azael and F. Alcántara, "Elaboró: Ing. Azael Fernández Alcántara TUTORIAL DE IPv6," 2010, Accessed: Jan. 09, 2023. [Online]. Available: http://www.ipv6.unam.mx/documentos/Tutorial-IPv6-UNAM.pdf

[5] "Dual stack o pila doble." https://www.lacnic.net/3091/1/lacnic/dual-stack-o-pila-doble (accessed Jan. 09, 2023).

[6] NIC México and Tecnológico de Monterrey, "Jool SIIT & NAT64," 2022.

[7] "Dual Stack Descripción General." Accessed: Jan. 02, 2023. [Online]. Available: https://www.lacnic.net/innovaportal/file/5495/1/dual-stack.pdf ß

[8] "Traducción." https://www.lacnic.net/3093/1/lacnic/traduccion (accessed Jan. 09, 2023).

[9] "SIIT-DC (Stateless IP/ICMP Translation for IPv6 Data Centers Environments)".

[10] Panelists: Azael Fernandez Alcantara, CUDI and CLARA, Oscar A. Robles-Garay, ULACNIC,Hector Eduardo Velarde Diaz, Federal Government of Mexico, "Sessions 2022 - Digital Around the World.IPv6 Deployment in Latin America, current status and key uses cases" Sessions 2022 - Digital Around the World (accessed Jan. 09, 2023).

[11] "Security for IPv6 Enabled Enterprises | NIST." Accessed: Jan. 09, 2023. [Online]. Available: https://www.nist.gov/news-events/events/2019/06/security-ipv6-enabled-enterprises

[12] S. Frankel and D. Green, "Internet Protocol Version 6 (IPv6)," *IEEE Secur Priv*, vol. 6, no. 3, pp. 83–86, May 2008, doi: 10.1109/MSP.2008.65.

[13] "NIST IPv6 Deployment Monitor and Test System | NIST." Accessed: Jan. 09, 2023. [Online]. Available: https://www.nist.gov/services-resources/software/nist-ipv6-deployment-monitor-and-test-system

[14] Jan Zöuz,traductores: Traductores: Azael Fernández Alcántara, Ernesto Pérez Estévez, Paul Bernal, (2022), "BCOP-Requerimientos-IPv6_Equipos-Red-LACNOG_2022", Accessed: Jan. 02, 2023. [Online]. Available: LACNOG BCOP 20160127-01 Requerimientos de IPv6 para equipos de TIC

[15] D. S. Punithavathani and K. Sankaranarayanan, "IPv4/IPv6 transition mechanisms," 2009. [Online]. Available: http://www.eurojournals.com/ejsr.htm

[16] Javier Prieto and S. y A. D.-C. A.-I. P. (Chiclana de la F. C. en C. F. U. S. Profesor Redes, "Cuando implante IPv6... ¿Se acabaron los problemas de seguridad?", Accessed: Jan. 09, 2023. [Online]. Available: www.jprietove.com

[17] Thomas Narten et al., "Políticas de Administración de Recursos de Internet en el Área de Latinoamérica y el Caribe."

[18] Ciprian. Popoviciu, Eric. Levy-Abegnoli, and Patrick. Grossetete, "Deploying IPv6 networks," p. 672, 2006.

[19] Shannon. McFarland, "IPv6 for enterprise networks," p. 372, 2011.

[20] Alejandro Acosta, "webinar-english-sep-2019-transition-mechasism LACNIC," Sep. 17, 2019. www.lacnic.net%2Finnovaportal%2Ffile%2F4012%2F1%2Fwebinar-english-sep-2019-transition-mechasism.pdf (accessed Jan. 09, 2023).

[21] "Transition a IPv6 con Mapping Address Translation (organizado junto a CISCO)." https://www.lacnic.net/3469/1/lacnic/ (accessed Jan. 09, 2023).

[22] "Lw4o6." Accessed: Jan. 02, 2023. [Online]. Available: https://www.lacnic.net/innovaportal/file/5495/1/el-mecanismo-de-transicion-lw4o6.pdf

[23] Coordinación de Estrategia Digital Nacional and Presidencia de la República Mexicana, "Guía para la Transición al Protocolo de Internet versión 6 (IPv6) en la Administración Pública Federal que emite la CEDNI", Accessed: Jan. 09, 2023. [Online]. Available: https://www.gob.mx/cedn/documentos/guia-para-la-transicion-al-protocolo-de-internet-version-6-ipv6-en-la-administracion-publica-federal-que-emite-la-cedn

[24] Edward. Horley, Practical IPv6 for Windows Administrators [electronic resource] / by Edward Horley., 1st ed. 2014. Berkeley, CA: Apress, 2014. doi: 10.1007/978-1-4302-6371-5.
[25] "MAP-Mapping of Address and Port." Accessed: Jan. 02, 2023. [Online]. Available: https://www.lacnic.net/innovaportal/file/5522/1/map-e-and-map-t-en.pdf
[26] "CISA RELEASES FINALIZED IPV6 GUIDANCE ON TIC 3.0," pp. 1–10, Jan. 2022.
[27] "IPv6: Security - HPCpublic." https://www.hpc.mil/program-areas/networking-overview/2013-10-03-17-24-38/ipv6-knowledge-base-security (accessed Jan. 02, 2023).
[28] "Firewall Configuration Guide for IPv6 – HPC public." https://www.hpc.mil/program-areas/networking-overview/2013-10-03-17-24-38/ipv6-knowledge-base-security/firewall-configuration-guide-for-ipv6 (accessed Jan. 02, 2023).
[29] A. Inc, "Apple Platform Security," 2022.
[30] "RFC 4862 - IPv6 Stateless Address Autoconfiguration." https://datatracker.ietf.org/doc/html/rfc4862 (accessed Jan. 02, 2023).
[31] "IPv6 – OpenVPN Community." https://community.openvpn.net/openvpn/wiki/IPv6 (accessed Jan. 02, 2023).
[32] J. A. Donenfeld, "WireGuard: Next Generation Kernel Network Tunnel," 2017, Accessed: Jan. 02, 2023. [Online]. Available: www.wireguard.com
[33] "IPv6 in Squid | Squid Web Cache wiki." https://wiki.squid-cache.org/Features/IPv6 (accessed Jan. 02, 2023).
[34] "DHCPv6 » CCNA desde Cero." https://ccnadesdecero.es/dhcpv6 / (accessed Jan. 02, 2023).
[35] "Network Manager - openSUSE Wiki." https://en.opensuse.org/NetworkManager (accessed Jan. 02, 2023).
[36] "Network Manager - Debian Wiki." https://wiki.debian.org/NetworkManager (accessed Jan. 02, 2023).
[37] "IPv6 - Internet Society." https://www.internetsociety.org/issues/ipv6/ (accessed Jan. 02, 2023).
[38] "Shorewall IPv6 Support." https://shorewall.org/IPv6Support.html#idm50 (accessed Jan. 02, 2023).
[39] "Cisco Collaboration Sizing Guide - Collaboration Sizing Guide for CSR 14 [Cisco Unified Communications Manager (CallManager)] - Cisco." https://www.cisco.com/c/en/us/td/docs/solutions/PA/size/SRND_sizing14/sizing14.html#15799 (accessed Jan. 02, 2023).
[40] "Cisco Collaboration Sizing Guide A Cisco Preferred Architecture (PA) design reference guide," 1981, Accessed: Jan. 02, 2023. [Online]. Available: www.cisco.com/go/offices.
[41] "Fortinet Products Comparison Tool." https://www.fortinet.com/products/product-compare (accessed Jan. 09, 2023).
[42] "RF Optimization and Deployment Models - ASE." https://ase.arubanetworks.com/solutions/id/75 (accessed Jan. 09, 2023).
[43] F. Siddika, M. A. Hossen and S. Saha, "Transition from IPv4 to IPv6 in Bangladesh: The competent and enhanced way to follow," 2017 International Conference on Networking, Systems and Security (NSysS), 2017, pp. 174-179, doi: 10.1109/NSysS.2017.7885821.
[44] A. K. Al-Ani, M. Anbar, A. Al-Ani and D. R. Ibrahim, "Match-Prevention Technique Against Denial-of-Service Attack on Address Resolution and Duplicate Address Detection Processes in IPv6 Link-Local Network," in IEEE Access, vol. 8, pp. 27122-27138, 2020, doi: 10.1109/ACCESS.2020.2970787.
[45] K. Nikolina, "Overview of the progress of IPv6 adoption in Croatia," 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), 2022, pp. 405-408, doi: 10.23919/MIPRO55190.2022.9803479.
[46] P. -K. Chen, C. -W. Lu and Q. Wu, "IPv6 Rapid Deployment in Taiwan Academic Network (TANet)," 2012 14th International Conference on Advanced Communication Technology (ICACT), 2012, pp. 694-**697.**
[47] Michael Dooley; Timothy Rooney, "IEEE Press Series in Network Management," in IPv6 Deployment and Management , IEEE, 2013, pp.i-i, doi: 10.1002/9781118590447.scard.
[48] Delgado RM. Without IPv6, there is no digital transformation for healthcare. Technology and Health Care. 2022;30(2):505-508. doi:10.3233/THC-213571.
[49] Liu, N, Xia, J, Cai, Z, Yang, T, Hou, B, Wang, Z, Sun, X, Zhang, X, Xia, Z & Bertino, E 2022, 'A Survey on IPv6 Security Threats and Defense Mechanisms', X Sun, X Zhang, Z Xia & E Bertino (eds), vol. pt.I, viewed 7 December 2022, <https://search-ebscohost-com.pbidi.unam.mx:2443/login.aspx?direct=true&db=inh&AN=22205731&site=ehost-live&scope=site >.
[50] G. Song et al., "DET: Enabling Efficient Probing of IPv6 Active Addresses," in IEEE/ACM Transactions on Networking, vol. 30, no. 4, pp. 1629-1643, Aug. 2022, doi: 10.1109/TNET.2022.3145040.
[51] DNSMASQ

[52] PREPARING AN IPV6 ADDRESS PLAN MANUAL, Version 2, 18 September 2013, surfNet. https://www.ipv6forum.com/dl/presentations/IPv6-addressing-plan-howto.pdf
[53] Portal de Estadísticas Universitarias, https://www.estadistica.unam.mx/series_inst/index.php
[54] ¿Sabías que la UNAM cuenta con más de 2 millones de m2 de área construida? | Fundación UNAM, https://www.fundacionunam.org.mx/auriazul/sabias-que-la-unam-cuenta-con-2-millones-843-mil-602-m2-de-area-construida/
[55] Sheila Frankel, Richard Graveman, John Pearce, Mark Rooks, Journal Article, Guidelines for the Secure Deployment of IPv6 Recommendations of the National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-119.pdf
[56] https://www.lacnic.net/innovaportal/file/5492/1/ejemplos-de-planes-de-direccionamiento.pdf
[57] A. Fernández (UNAM),T. Gallegos (INAO),(NOC-CUDI),Políticas de ruteo IPv6 en la RedCUDI, https://cudi.edu.mx/rfc/rfcmx/rfcmx7.pdf, ßOctubre-2012.
[58] Webpage, iperf---the-tcp,-udp-and-sctp-network-bandwidth-measurement-tool, https://iperf.fr/
[59] Webpage, GitHub - traviscross/mtr: Official repository for mtr, a network diagnostic tool, https://github.com/traviscross/mtr,
[60] B. Hickman, April 2003, GVNW, web page, Consulting Inc, https://www.rfc-editor.org/rfc/rfc3511.html
[61] B. Balarajah, C. Rossenhoevel, NetSecOPEN, web_page, RFC 9411 - Benchmarking Methodology for Network Security Device Performance, https://datatracker.ietf.org/doc/html/rfc9411, rfc-9411---benchmarking-methodology-for-network-security-device-performance
[62] S. Bradner, J. McQuaid, March 1999,https://www.ietf.org/rfc/rfc2544.txt ,Benchmarking Methodology for Network Interconnect Devices
[63] D. Newman, August 1999, Benchmarking Terminology for Firewall Performance, https://www.rfc-editor.org/rfc/rfc2647 ,Data Communications
[64] A. Morton, AT&T Labs, May 2021,https://www.rfc-editor.org/rfc/rfc9004 ,SSN:2070-1721
[65] C. Popoviciu, A. Hamza, G. Van de Velde, Cisco Systems, D. Dugatkin FastSoft Inc. May 2008 https://www.rfc-editor.org/rfc/pdfrfc/rfc5180.txt.pdf
[66] https://nmon.sourceforge.io/pmwiki.php
[67] https://www.lacnic.net/agotamiento