# Transición IPV4 a IPV6

# IPV4 to IPV6 transition

DOI: 10.46932/sfjdv3n2-059

Received in: February 15th, 2022
Accepted in: March 1st, 2022

**Miguel Ángel Ruiz Jaimes**
Institución: Universidad Politécnica del Estado de Morelos
Dirección: Boulevard Cuauhnáhuac No. 566, Col. Lomas del Texcal, Jiutepec Morelos. CP. 62550
Correo electrónico: mruiz@upemor.edu.mx

**Sandra Elizabeth León Sosa**
Institución: Universidad Politécnica del Estado de Morelos
Dirección: Boulevard Cuauhnáhuac No. 566, Col. Lomas del Texcal, Jiutepec Morelos. CP. 62550
Correo electrónico: lsandra@upemor.edu.mx

**Irma Yazmín Hernández Báez**
Institución: Universidad Politécnica del Estado de Morelos
Dirección: Boulevard Cuauhnáhuac No. 566, Col. Lomas del Texcal, Jiutepec Morelos. CP. 62550
Correo electrónico: ihernandez@upemor.edu.mx

**RESUMEN**
En la actualidad se manejan redes de IPv4, sin embargo, es muy importante aclarar que las direcciones IPv4 se están agotando por lo que las empresas e instituciones que manejan IPV4 deberán actualizarse lo más pronto posible para evitar la limitación de crecimiento de la red. Es importante mencionar que surgió un nuevo protocolo IPv6 que ofrece la mejor amplitud en cantidad de direcciones ya que su longitud es de 128 bits lo que ayuda a mitigar el problema de IPv4, ofrece un sistema de direccionamiento escalable y amplio. Dentro de las grandes ventajas que tiene el protocolo IPv6 es internet sin límites y sumado a esto grandes mejoras como es la seguridad y eficiencia, de manera que al tener una dirección IP más larga y compleja será más difícil un ataque a la red, ofrece la autoconfiguración de direcciones. Se pretende saber qué tan factible y viables es realizar la conversión de la red de la institución de IPV4 a IPv6, confirmar los beneficios que ofrece la configuración IPv6 y que la red sea dé mayor escalabilidad de acuerdo a las necesidades de la Institución

**Palabras clave:** transición, actualización, eficiencia, mejoras, mayor escalabilidad.

**ABSTRACT**
Currently IPv4 networks are managed, however, it is very important to clarify that IPv4 addresses are running out, so companies and institutions that handle IPV4 should update as soon as possible to avoid the limitation of network growth. It is important to mention that a new IPv6 protocol has emerged that offers the best amplitude in the number of addresses since its length is 128 bits, which helps mitigate the problem of IPv4, offers a scalable and comprehensive addressing system. Among the great advantages that the IPv6 protocol has is internet without limits and added to these great improvements such as security and efficiency, so that having a longer and more complex IP address will make an attack on the network more difficult, it offers the address autoconfiguration. It is intended to know how feasible and feasible it is to convert the institution's network from IPV4 to IPv6, confirm the benefits offered by the IPv6 configuration and that the network be more scalable according to the needs of the Institution.

**Keywords:** transition, upgrade, efficiency, improvements, greater scalability.

**Categorías y Descriptores Temáticos**
**Seguridad informática y redes telemáticas.**

- Redes definidas por software.
- Radio Cognitiva – Computación cognitiva.
- Computación y criptografía cuántica – Modelos de gestión de seguridad.
- Edge computing.
- Redes 5G y nuevas tecnologías.

## 1 INTRODUCCIÓN

Internet se convirtió en una herramienta de trabajo sumamente importante que permite estar comunicados de manera efectiva virtualmente, es decir, sin la necesidad de recurrir de manera física, esta herramienta está presente y nos otorga grandes beneficios, actualmente se maneja IPv4 para la comunicación, sin embargo, es muy importante tener en cuenta que las direcciones IPv4 se están agotando, de manera que, en algún momento será necesario hacer el cambio a IPv6, este cambio se volverá inevitable por la expansión mundial y el agotamiento de direcciones IPv4.

Para hacer este cambio de IPv4 a IPv6 en algunos casos el gasto seria exponencial al tamaño de la institución, de manera que, se podrá recurrir a los mecanismos de transición que permitirá un ahorro y la oportunidad de trabajar con IPv6, para el presente artículo se verán los mecanismos NAT-PT y Túnel Manual.

Los mecanismos de transición permiten trabajar en conjunto IPv4 con IPv6, el esfuerzo laboral para la aplicación de estos mecanismos es contar con los conocimientos necesarios para aplicarlos, son métodos transparentes que no consumen recursos excesivos y es posible implementarlo en la mayoría de los routers.

En el presente artículo se hablará de la implementación de los mecanismos de transición que permitirán la comunicación de IPv4 con IPv6 en una universidad, sin necesidad de generar un gran gasto de recursos económicos, para implementar el mecanismo de transición se requiere tener el conocimiento en estos y router que sea compatible con el mecanismo, es importante mencionar que la mayoría de estos son compatibles.

## 2 OBJETIVOS

### General:

Desarrollar la traducción de la red IPv4 a IPv6 mediante el simulador Packet Tracer que proporcione una red eficiente que mejore el tráfico de datos.

**Específicos:**

- Analizar la red actual y su distribución para simularlo en Packet Tracer.
- Traducir la red IPv4 a IPv6.
- Realizar pruebas de flujo para verificar el correcto diseño.
- Reportar los resultados obtenidos en el proyecto para comparación de IPv4 e IPv6.

## 3 METODOLOGÍA Y PROCESOS DE DESARROLLO.

La metodología Top-Down Network Design se enfoca primero en la capa 7 de las capas del modelo OSI llamada aplicación, de manera que de primera instancia se determinará que aplicaciones se ejecutarán y como se compararán esas aplicaciones en una res, se deben analizar las metas técnicas y de negocio, es sumamente importante definir quiénes ocuparán la red y la ubicación de los usuarios. (Saavedra, 2017)

Contiene un diseño estructurado, se desarrolla un modelo lógico antes que un modelo físico. (Pérez, s.f.)

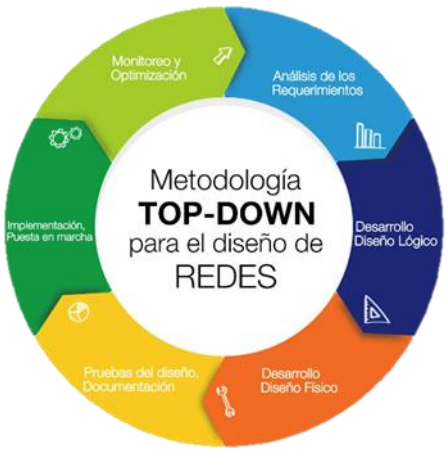
Maneja diferentes tipos de diseño de red

- Nuevo diseño
- Re-ingeniería de un diseño existente
- Diseño de expansión de la red

Las fases de la metodología son:

1. Análisis de requisitos
2. Desarrollo de diseño lógico
3. Desarrollo de diseño físico
4. Pruebas Optimización y documentación de la red
5. Implementación
6. Monitoreo y optimizar la red

En la Figura 1. se ilustra la metodología Top-Down Network Design

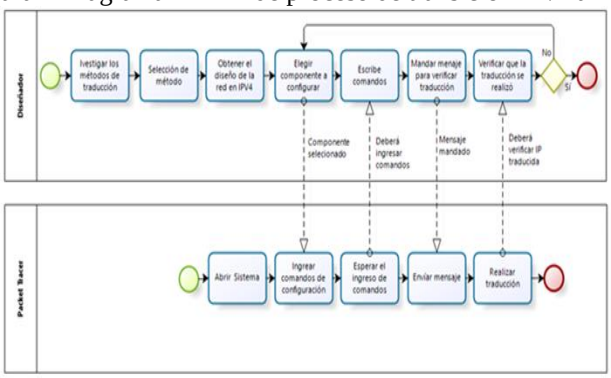


En la figura 2 se muestra el proceso que se lleva a cabo para la transición de una red IPV4 a IPV6, en este proceso se cuenta con dos actores, el diseñador y el sistema Packet Tracer.

Para el diseño se utiliza el diagrama BPMN [5] y [6]Como primer paso se debe investigar los métodos de transición de IPv4 a IPv6 para posteriormente evaluar cuál es el mejor método para la transición y se procede a seleccionar el método, en este punto debemos contar con el diseño de la red en IPv4, el diseñador procederá a interactuar con el sistema Packet Tracer en donde se seleccionara el componente en donde se realizará la configuración correspondiente al método seleccionado para realizar la transición, se ingresaran los comandos en el sistema Packet Tracer, al finalizar la configuración se enviará un paquete para verificar que la transición esté funcionando de manera correcta, de no ser así, se procederá a realizar nuevamente la configuración y verificar la transición con el envío de un paquete, si la transición se realizó el proceso da por finalizado correctamente.

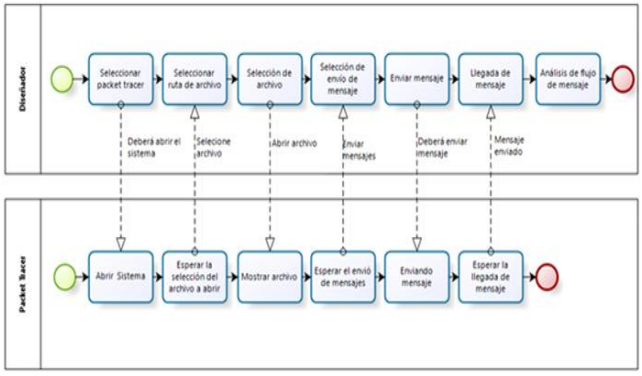
Este proceso cuenta con un nodo de decisión el cual deberá cumplir para poder finalizar el proceso exitosamente, de lo contrario se regresará al paso de elegir el componente en donde se realizará la configuración nuevamente hasta que el nodo de decisión concluya en sí cumple.

Figura 2 Diagrama BPMN de proceso de transición IPv4 a IPv6




Se realizará la verificación de flujo como se muestra en la figura 3, con la finalidad de realizar un análisis de los mecanismos de transición.

Figura 3 Diagrama BPMN de verificación de flujo



## 4 RESULTADOS

La implementación del mecanismo de transición consistió en simular la red de una institución en Packet Tracer en donde se realizaron todas las configuraciones necesarias y así tener comunicación de una red IPv4 a una red IPv6.

La configuración inicial de un router es muy importante debido a que es donde nombramos el router, colocamos las contraseñas de acceso y el mensaje donde prohibimos el acceso a personal no autorizado por cuestiones de seguridad, se configuran los accesos remotos y se encriptan contraseñas, a continuación, se detallan las configuraciones básicas del router.

Ya configurados se procede a la configuración de las VLAN's, asignación de puertos y seguridad, se configura DHCP, protocolo de enrutamiento RIP versión 2, se aplica la configuración de IPv4, en el router frontera se configura el protocolo de enrutamiento IPV6.

Para configurar el túnel es importante saber cuáles son los dos routers en donde se aplicará, en este caso, se aplicará en el router ISP y router Central.

Se configura la interface de origen e IP de destino, se habilitan las interfaces con IPv6, se configura el enrutamiento IPv6 y las interfaces con las IPv6, esta configuración es en ambos router como se muestra en la figura 4.

Figura 4 Configuración de túnel

```
interface Tunnel0
 no ip address
 ipv6 address 3000::1/112
 ipv6 rip redv6 enable
 tunnel source Serial1/2
 tunnel destination 172.16.10.26
 tunnel mode ipv6ip
```

Para realizar la configuración de NAT-PT se llevará a cabo en el router central, que es donde se realizará la traducción de IPV4 a IPv6 y de IPv6 a IPv4. Se da de alta la interface IPv6. Se habilita NAT en los seriales que corresponden a los routers de cada extremo. Ver figura 5

Figura 5 Habilitar NAT

```
Central(config)#int s1/0
Central(config-if)#ipv6 nat
Central(config-if)#exit
Central(config)#
Central(config)#int s1/1
Central(config-if)#ipv6 nat
Central(config-if)#exit
```

Se aplican los comandos de traducción de IPv4 a IPv6 y viceversa, figura. Ver figura 6

Figura 6 Comandos de traducción

```
Central(config)#ipv6 nat v6v4 source 14::4 172.16.10.100
Central(config)#ipv6 nat v4v6 source 172.16.10.26 1144::1
Central(config)#ipv6 nat prefix 1144::/96
```

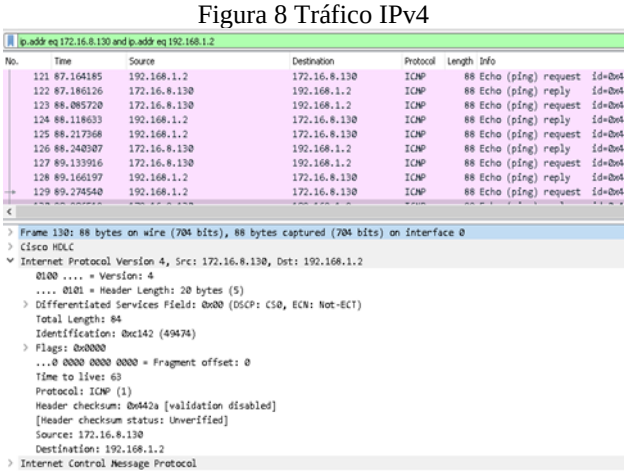
Se aplican el protocolo de enrutamiento, se habilita NAT-PT, se específica la métrica que en este caso es 2 por que se manejarán los router directamente conectados, se verifica la traducción y se realiza un debug figura 7.

Figura 7 Traducción realizada

```
*Nov 25 04:51:29.279: IPv6 NAT: IPv6->IPv4:
                      src (14::4 -> 172.16.10.100)
                      dst (1144::1 -> 172.16.10.26)
```

Se realiza un análisis por medio del software Wireshark para ver el funcionamiento de la red IPv4 de la Universidad y así ver que es lo más conveniente para la institución, se muestra el flujo de la red. Figura 8.

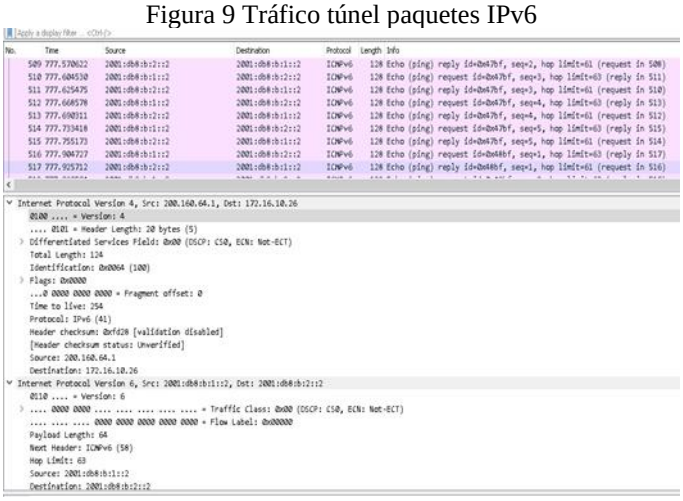
Figura 8 Tráfico IPv4




Ya configurado el túnel y verificado que está funcionando de manera correcta se procede a realizar las pruebas de tráfico pertinentes para realizar un análisis de este.

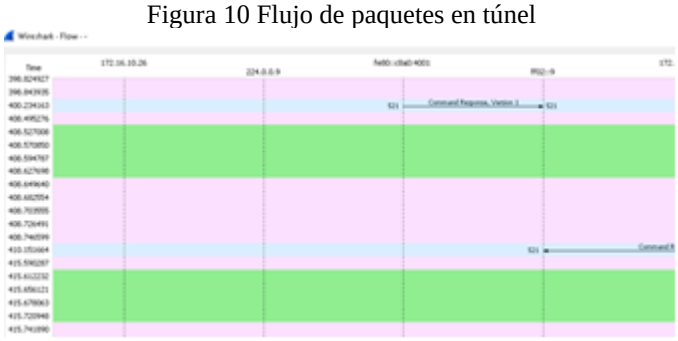
Se utiliza el software Wireshark se verifica el tráfico de la red y el funcionamiento del túnel, se envía un paquete de una red externa IPv6 al Host de la VLAN Idiomas que maneja IPv6, podemos observar que llegan sin ningún problema, figura 9. Se puede observar que su origen y destino es IPv6, pero se transportan por medio de una red IPv4.

Figura 9 Tráfico túnel paquetes IPv6



Por medio del software Wireshark podemos visualizar el flujo de tráfico, como es que se lleva a cabo durante el envío de paquetes, como se puede visualizar el flujo es bueno y los paquetes llegan a su destino sin problema alguno. Figura 10.

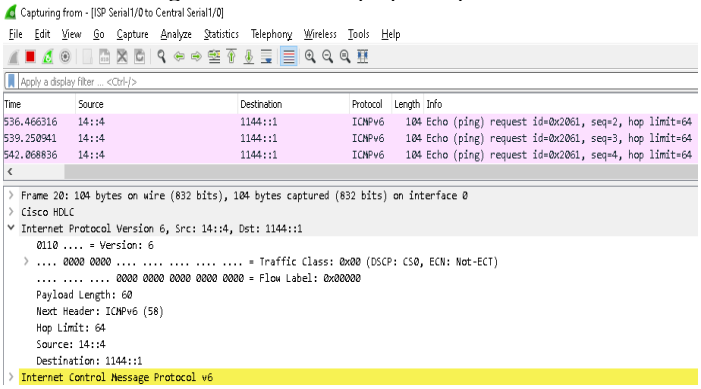
Figura 10 Flujo de paquetes en túnel



Ya que se configuro el mecanismo de traducción NAT-PT, se realizan las pruebas de envío de paquete y flujo.

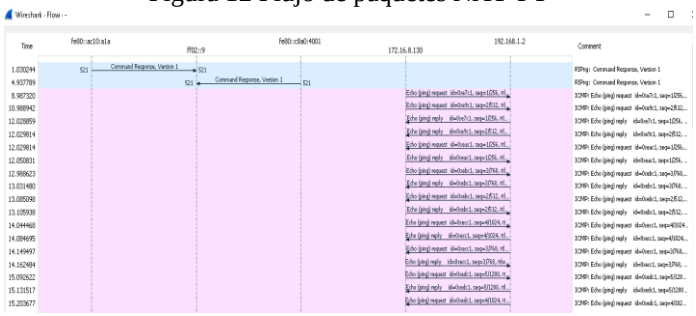
Se utiliza el software Wireshark se verifica el tráfico de la red y el funcionamiento de NAT-PT, se envía un paquete de una red IPv6 al Host de la VLAN Idiomas que maneja IPv6. Figura 11. Se puede visualizar el origen y el destino por medio del protocolo IPv6.

Figura 11 Envío de paquetes por NAT




Por medio del software Wireshark podemos visualizar el flujo de tráfico, como es que se lleva a cabo durante el envío de paquetes. Figura 12.

Figura 12 Flujo de paquetes NAT-PT



Como resultado del proyecto se obtiene el reporte del análisis realizado, con ventajas y desventajas de los mecanismos utilizados. En base a la implementación de la red de la Universidad en IPv4 y la implementación de los mecanismos de Túnel manual y NAT-PT, se realizaron las pruebas necesarias para ver el funcionamiento de envío de paquetes y flujo de estos y así concluir con el análisis de las ventajas y desventajas de cada mecanismo, tabla 1

Tabla 1 Análisis de mecanismos de transición

| Mecanismo | Ventajas | Desventajas |
|---|---|---|
| **Túnel Manual** | ✓ Fácil de implementar.<br>✓ Multiplataforma.<br>✓ Económico.<br>✓ Permite la comunicación de redes IPv6 a redes IPv4 con host IPv6.<br>✓ El flujo de los paquetes es bueno como se observó en las pruebas de flujo de tráfico Imagen 48. | ✓ Incrementa el tamaño del encabezado.<br>✓ No es escalable.<br>✓ Es manual |
| **NAT-PT** | ✓ No es necesario ningún cambio en los nodos.<br>✓ Permite la comunicación de redes de IPv6 a rede de IPv4. | ✓ La respuesta el flujo es lento.<br>✓ Compleja al configurarse.<br>✓ No existe seguridad en la información.<br>✓ Obsoleto |

## 5 CONCLUSIONES

La implementación del proyecto se realizó en el simulador Packet Tracer y el emulador GNS3, en ambas aplicaciones quedo funcional, queda pendiente implementarlo en la institución de nivel superior. Al aplicar un modelo jerárquico este ayudo a que la red sea más escalable y se tenga una mejor administración de la misma.

Se desarrolló la metodología que ayudará a llevar a cabo la implementación de la transición de manera efectiva y sin errores. En un futuro se espera que esta misma se mejore para que sea aún más eficiente y poder implementar este proyecto en otras instituciones de educación superior.

## REFERENCIAS

[1] Saavedra, J. C. (18 de junio de 2017). Metodología Top-Down para el Diseño de Redes. Obtenido de http://juancarlossaavedra.me/2017/06/infografia-metodologia-top-down-para-el-diseno-de-redes/#:~:text=La%20respuesta%20larga%3A%20Resolver%20un,y%20deben%20integrarse%20entre%20s%C3%AD.CISCO. (02 de 05 de 2005).

[2] Implementando Túneles. Obtenido de Cisco.com: https://www.cisco.com/c/en/us/td/docs/ios/12_4/interface/configuration/guide/inb_tun.html#wp1080719

[3] CISCO. (2005). NAT-PT. Obtenido de Cisco.com: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/113275-nat-ptv6.html?dtid=osscdc000283

[4] Obis Joan, A. (2014). Diseño de una red Corporativa. TFC-Integració de xarxes telemàtiques

[5] Matturro, G., & Guzmán Barrio. (2007). Introducción a la configuración de los routers CISCO. Obtenido de https://www.ort.edu.uy/fi/pdf/configuracionroutersciscomatturro.pdf

[6] Freund, J., Rücker, B., & Hitpass, B. (2014). BPMN 2.0 Manual de Referencia y Guía Práctica. Chile: Camunda.

[7] Caballero, A. (marzo de 13 de 2019). Escanear Todos los Puertos de un Host utilizando Nmap. Obtenido de Reydes.com: http://www.reydes.com/d/?q=Escanear_Todos_los_Puertos_de_un_Host_utilizando_Nmap

.