VISIÓN ELECTRÓNICA

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

LA TRANSICIÓN DEL PROTOCOLO IPV4 A IPV6 EN UNA EMPRESA: REVISIÓN Y CASO

TRANSITION TO THE PROTOCOL IPV4 TO IPV6 IN A COMPANY: REVISION AND CASE

Jeisson D. Novoa[1] Luis A. Gamboa[2] Gustavo A. Higuera[3]

Abstract: Interconnection network protocols for global single addressing, whose work objectives are multiple thanks to technological advancement and the big exponential growth of the Internet, have nowadays reached exhaustion, causing its current protocol: IPV4 to consume almost the entirety of IP addresses, so it was necessary to create and implement a new addressing protocol all over the world: IPV6. And though its deployment hasn't been immediate, it is expected that the majority of companies carry it out within a two-year range. The purpose of this article is to present a guide which allows to execute the transition and provisioning of IPV6 within the companies; detailed guidelines regarding IPV4-IPV6 transition methods, forms of IP's assignation and routing protocols will be given. For this, a company's basic services have been considered, such as Dynamic Host Configuration Protocol (DHCP); Domain Name System (DNS); SYSLOG event registry; Network Time Protocol (NTP); and the MAIL service, among others.

[1]* Ing. En Telecomunicaciones. Lugar de trabajo: GrupoKonecta-ETB. Correo electrónico e-mail: jeisson.novoas.pr@etb.com.co ORCID: 0000-0001-8795-4971

[2]** Ing. En Telecomunicaciones. Lugar de trabajo: Grupokonecta-ETB. Correo electrónico e-mail: luis.gamboat.pr@etb.com.co ORCID: 0000-0002-8729-9636

[3]*** Ingeniero en Telecomunicaciones, Magister en Ciencias de la Información y las Comunicaciones. Lugar de trabajo: Docente e investigador, Fundación Universitaria San Mateo. Correo electrónico e-mail: ghiguera@sanmateo.edu.co ORCID: 0000-0001-9691-789X

Concluding from the network tests that the services function in an acceptable way, and that the methodology can be applied in any company as long as the corresponding network structure is taken into account.

Keywords: Transition, routing, services, protocols.

Resumen*:* Los protocolos de interconexión de redes para el direccionamiento IP, cuyos objetivos de trabajo son múltiples gracias al avance tecnológico y crecimiento exponencial del internet, han llevado al agotamiento de direcciones de su protocolo inmediato: IPV4, así que fue necesario la creación e implementación de un nuevo protocolo de direccionamiento global: IPV6. Aunque su despliegue no ha sido inmediato se tiene previsto que gran parte de las empresas realicen este en dos años. El presente artículo tiene como finalidad presentar una guía que permita ejecutar la transición y aprovisionamiento de IPV6 dentro de las compañías; se darán pautas detalladas de los métodos de transición IPV4-IPV6, el direccionamiento y forma de asignación de IP's y protocolos de enrutamiento. Para lo anterior se han seleccionado servicios básicos de una empresa: protocolo de configuración dinámica de host (DHCP); sistemas de nombres de dominio (DNS); el registro de eventos SYSLOG; protocolo de tiempo de red (NTP); y el servicio de correo, entre otros. Se concluye de las pruebas, que la red y los servicios funcionan aceptablemente; aplicándose la metodología en cualquier compañía siempre que se tenga en cuenta la estructura de red correspondiente.

Palabras clave: IPV4, IPV6, Transición, enrutamiento, servicios, protocolos.

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

1. INTRODUCTION

Actualmente, el atractivo e interés que genera el internet ha ido propagándose por todo el mundo ocasionando que el desarrollo adquirido por las computadoras sea notable; igualmente las redes de telecomunicaciones mejoran su estructura y sus parámetros para obtener una mejor disponibilidad, confiabilidad e integridad. En el papel todo este avance se escucha maravilloso, sin embargo, el excesivo uso de dispositivos con conexión a internet a provocado al agotamiento de direcciones IP ya que este crecimiento exponencial de la tecnología tiene implicaciones directas con la gran demanda de servicios en todo el mundo afectando la asignación de direcciones IPV4 que se tenían previstas [1], llevando al empobrecimiento de estas, las cuales ya se encuentran asignadas [2], de tal manera que el mundo necesita una innovación que permita soportar el despliegue tecnológico actual y futuro [3].

Por tal motivo se origina el protocolo IPV6 [4], el cual con la mejora en su cabecera proporciona mayor capacidad de direcciones respecto a su protocolo antecesor, Sin embargo, es importante entender que no se puede implementar IPV6 de forma inmediata [5], se debe llevar a cabo un proceso en el cual se mantenga IPV4 a la par con el que vamos a adecuar a nuestra red, esto sucede ya que no sería posible su sustitución inmediata, es decir no es posible apagar la Red, ni por un mínimo tiempo para poder ejecutar la transición [6]. Así que no se trata de una migración, sino que ambos protocolos, IPV4 e IPV6 [7], coexistirán durante algún tiempo, esto servirá directamente a algunas tecnologías que son dependientes del protocolo de direccionamiento [8], aunque la proyección que se tiene es que estas avancen a la par con el protocolo y con las necesidades que se generan mundialmente.

Se aprecian diferentes entidades y artículos que también impulsan y colaboran con la implementación de dicho protocolo, donde se resaltan en Colombia artículos realizados por el MINTIC (MINISTERIO DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES) [9] donde explican a groso modo y teóricamente como realizar el aprovisionamiento del protocolo IPV6 y cómo hacer la correspondiente transición, y otros artículos académicos efectuados tanto en Bogotá y en Pereira por las universidades de Cundinamarca [10], universidad Santo Tomás de Aquino [11] y Universidad Tecnológica de Pereira [12], respectivamente, los cuales también alimentan la información para ejecutar esos procesos.

El documento se estructura de la siguiente manera: en primer lugar se establecen los materiales y métodos donde se describen las pautas técnicas donde se explicará cómo efectuar dentro de los equipos y en la red los procedimientos adecuados, donde en primer lugar se podrá observar los materiales y métodos usados para hacer posible el desarrollo de este; seguidamente, en el apartado de la alternativa experimental propuesta se encontrará el modo de asignar el direccionamiento IPV6, así como aplicar la seguridad en capa 2 y capa 3 a la red, igualmente se identificarán los métodos de transición y el aprovisionamiento de los servicios. Todas estas pautas serán de gran ayuda para efectuar la transición del protocolo IPV4 al IPV6 [13], sin denegar los servicios que cada uno de estos ofrecen. Finalmente en las conclusiones, se exhibe, con el fin de que las empresas tengan la posibilidad de acceder a una guía la cual les permita desarrollar dicho cambio, mostrando los requerimientos básicos que pueda poseer una entidad.

2. Materiales y métodos

Para llevar a cabo la transición de una red con protocolo IPV4 a IPV6 en alguna entidad, el ingeniero de redes encargado debe generar el pre diseño, diseño, simulaciones, pruebas, antes de empezar cualquier manipulación de equipos, información o configuraciones sobre

Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

estos [14]. Si hay alguna manipulación incorrecta de esta información, se puede generar fallas sobre la red o errado funcionamiento de la misma. Inicialmente se solicita a la empresa la adquisición del segmento en IPV6 con su proveedor de servicios [15] para que, al momento de generar el pre diseño, diseño y simulaciones, sea lo más real posible. Como el énfasis es generar la transición de una red ya existente en protocolo IPV4, es importante implementar dicha red en un simulador el cual cuente con toda la información de equipos, configuraciones, seguridad de red y servicios implementados en la empresa para poder generar y manipular cambios, así como la respectiva transición con sus respectivas pruebas.

De lo anterior, en la red implementada en el desarrollo de esta investigación se simuló mediante *Packet Tracert*, software diseñado, desarrollado y aprovisionado por la empresa Cisco [16]. Este simulador es uno de los más completos puesto que cuenta con equipos CISCO, computadores, servidores entre otros; es decir, todo lo necesario para la simulación de la transición, configuraciones de equipos, procesos de seguridad y pruebas en tiempo real.

En el anterior sentido, el ingeniero encargado de la transición debe contar con la topología implementada en la empresa, el inventario de los equipos, los protocolos utilizados y servicios en dicha red en el simulador, los protocolos de enrutamiento utilizados en el desarrollo del artículo son OSPF v2 para la red IPV4, OSPF v3 para IPV6 y rutas estáticas, además de los servicios básicos como lo son DHCP, FTP, SYSLOG y DNS.

El diagrama de bloques explica la alternativa de solución propuesta, Figura 1.

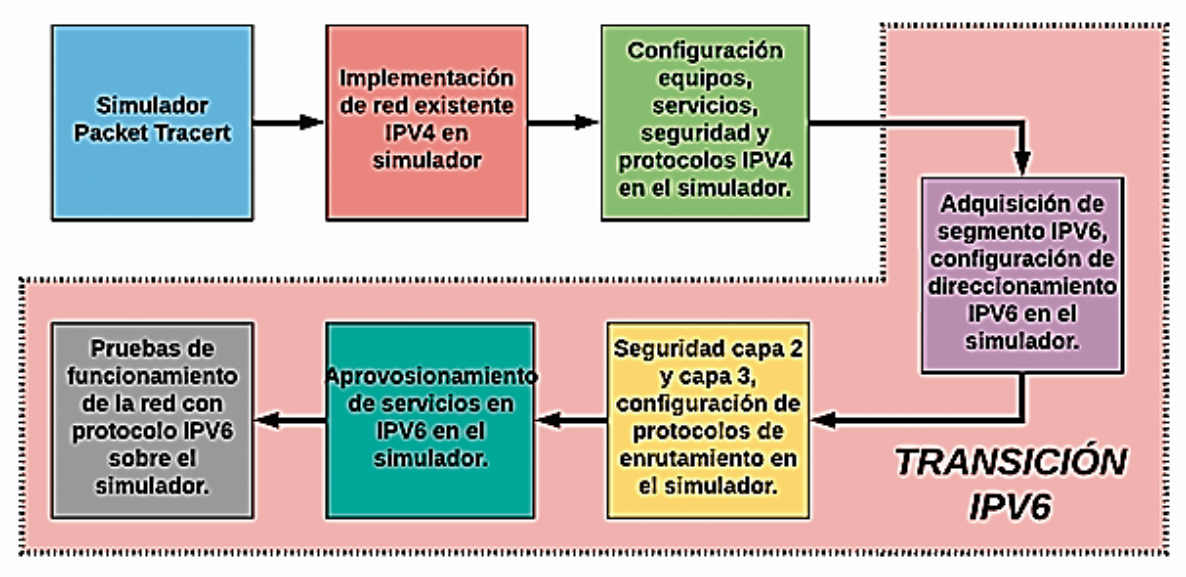

Figura 1. Diagrama de bloques alternativa de solución. **Fuente:** Propia elaboración.

2.1 Metodología

En la figura 2 se puede observar las fases en la que fue estructurada la transición de IPV4 a IPV6, teniendo en cuenta que en gran parte de la red coexistirán ambos protocolos [17].

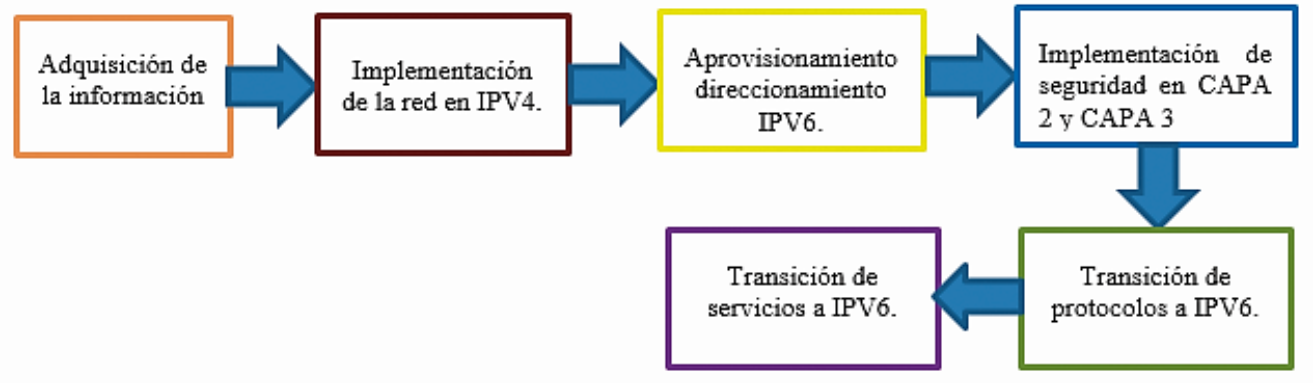

Figura 2. Diagrama de bloques metodología. **Fuente:** Propia elaboración.

2.1.1 Adquisición de la Información:

Inicialmente se efectuará la recopilación de información propuesta a nivel nacional sobre el protocolo IPV6, donde se puede apreciar que el MINTIC es una de las entidades que impulsa el cambio de protocolo. De igual manera es de importancia tener conocimiento sobre el

Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

direccionamiento en IPV6, sus reglas y su estructura; los protocolos de enrutamiento, cómo se configuran y de qué manera se utilizan, allí se puede encontrar: EIGRP, OSPF, BGP; sin embargo, se dará más énfasis al OPSF (que también se encentra en IPV4) [18], aunque teniendo en cuenta que el aprovisionamiento de este cambia con respecto al protocolo antecesor [19]; los métodos de transición en donde se pueden apreciar varios de estos como: **Dual stack, tunelización, NAT64, 464XLAT** y **MAP** [20]**,** los cuales son los más conocidos y más usados, serán enfatizados más adelante. También se ejecutó el estudio de los servicios y aplicaciones [21], aunque no se debe tener total relevancia con esto, dado que a pesar que hay varios servicios que no soportan IPV6, estos se pueden apoyar en el protocolo IPV4 teniendo en cuenta que ambos coexistirán por cierto tiempo.

Por lo anterior, también se debe tener en cuenta los equipos que permiten hacer uso del protocolo IPV6, aunque durante la implementación se hace referencia a equipos CISCO, también se nombrarán otros dispositivos que permiten IPV6:

- HUAWEI NE80E [22].
- HUAWEI NE40E [22].
- Cisco Catalyst 6500 Series Switches.
- Catalyst 4500.
- Catalyst 3750.
- Cisco ASR 1000 Series router.
- Cisco ISR G2 router.
- Router cisco 2500.

De otro lado, inicialmente se indicó que el MINTIC es uno de los mayores promotores del aprovisionamiento de IPV6 en Colombia [23]; sin embargo, hay varias entidades más, no solo en Colombia sino en américa Latina con el objetivo de asignar IPV6 de manera masiva [24]:

- ✓ Compañía de Circuitos Cerrados S.A. De argentina, el cual ya implemento IPV6.
- ✓ Consulnetworks S.A, de Colombia, quienes se encuentran implementando.
- ✓ Castro Tello Marco Iván (Conexión Global), de Ecuador, ellos ya implementaron IPV6.
- ✓ Americana Digital, de Brasil, ya implementaron el protocolo.
- ✓ CABLE COLOR, de Chile, ya aprovisionaron IPV6.
- ✓ CENIT, de Venezuela, quienes ya asignaron IPV6 en su estructura.
- ✓ COPACO S.A, de Paraguay, ellos ya efectuaron la implementación.
- ✓ IFX NETWORKS, ya aprovisionaron el servicio IPV6.
- ✓ Universidad Distrital Francisco José de Caldas

Las que se encuentran en proceso de implementación.

2.1.2 Implementación de la red en IPV4.

El artículo, en este ítem, los parámetros básicos para la configuración e implementación del protocolo IPV6 en los equipos de las organizaciones, sin embargo, depende del ingeniero en redes de cada empresa, que topología, dispositivos, métodos, protocolos y diseño le convendrá más a la compañía, es de aclarar que se debe establecer inicialmente la red IPV4 [25], aunque en esta ocasión ya se posee una estructura de red, figura 3.

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

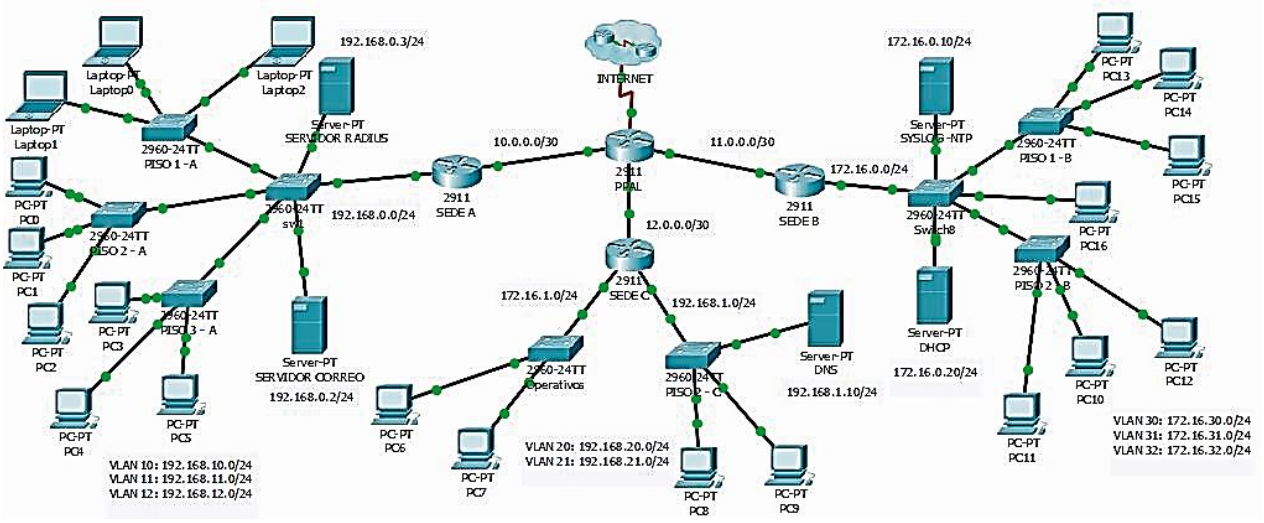

Figure 3. Topología de red en IPV4 **Fuente:** Propia elaboración.

Se observan tres sedes que estarán comunicadas con una principal y saldrá a internet bajo una IP pública con ayuda de NAT. Sin embargo, como se manifestó anteriormente, únicamente son pautas básicas de configuración, ya que muchas de las organizaciones utilizan la solución MPLS para sus redes.

En el ejemplo de empresa, se tienen tres áreas: ***ADMINISTRATIVA, OPERATIVA y TECNOLOGIA***, las cuales será conocidas como **SEDE A, SEDE B, SEDE C Y SEDE PRINCIPAL.**

Los servicios que la compañía tiene implementados con el protocolo IPV4 son los siguientes:

- DHCP (Mediante servidor).
- DNS.
- Servidor SYSLOG.
- NTP.
- CORREO ELECTRONICO.

El protocolo de enrutamiento a usar será OSPF V2 (el cual también se establecerá para IPV6), el cual usa el algoritmo SmoothWall Dijkstra enlace-estado para calcular la ruta más idónea. OSPF presenta varias ventajas ya que ofrece una convergencia más rápida y escala a implementaciones de red mucho más grandes. Se debe tener en cuenta que el protocolo se usará con única área [26].

2.1.3 Aprovisionamiento de direccionamiento IPV6.

Para la demostración, se configurarán tres segmentos de red, dos de estos maneja IPV6-ONLY, el segundo operará con ambos protocolos y se tendrá el escenario donde el core solo estará aprovisionado IPV4.

Antes de iniciar con la respectiva configuración, es de gran utilidad identificar las redes que se manejan, ya están claros los servicios implementados, ahora se tienen que observar las tres redes. Figura 4.

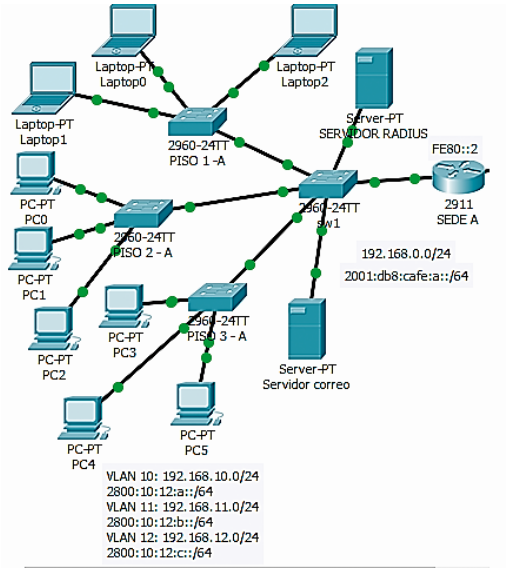

Figura 4. Topología sede A **Fuente:** Propia elaboración.

En la red de la sede A se configurará IPV4 e IPV6, en la imagen se observa el direccionamiento LAN con ambos protocolos. Figura 5.

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

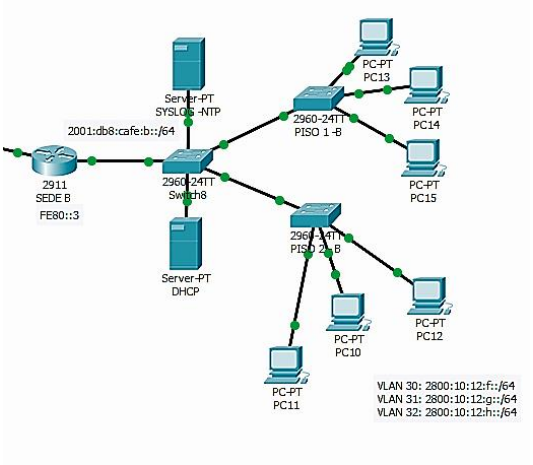

Figura 5. Topología Sede B **Fuente:** Propia elaboración.

Para la sede B se establecerá únicamente el protocolo IPV6, la comunicación con la red de la sede A se podrá efectuar con normalidad con dicho protocolo, sin embargo, si se tuviera el caso que la sede C solo se encuentre configurada con IPV4, la conexión se debería efectuar o por NAT64, 464XLAT o MAP, dependiendo de cuál de estos brinda un mayor beneficio [27], esto se explicará con mayor detenimiento en las próximas fases. Figura 6

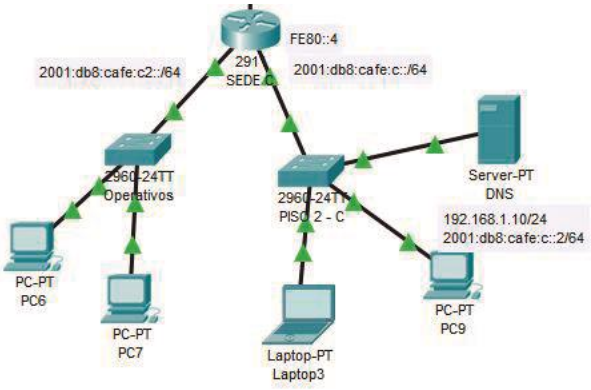

Figura 6. Topología Sede C. **Fuente:** Propia elaboración.

Por último, la empresa tiene la estructura de la sede C, la cual solamente manejará el protocolo IPV6, la comunicación con las demás sedes se puede efectuar normalmente por

IPV6, sin embargo, con este segmento y con la sede B, se demostrará la Tunelización cuando sea necesario pasará el tráfico por una red IPV4 [28].

Para la asignación de las IP's en IPV6 se efectuará de la siguiente manera: como primera recomendación, es necesario activar el protocolo IPV6 dentro del router, de la siguiente manera. (1)

$$sede\_A(config)\#ipv6\ unicast-routing\ (1)$$

Este habilita IPV6 en los router cisco, posterior se procede a configurar como en IPV4 el direccionamiento sobre las interfaces, las cuales se evidencian en la figura 7, es de aclarar que en IPV6 no existe la dirección de red como en IPV4 así que se debe configurar la dirección de Gateway en las diferentes interfaces, [29].

La forma de asignar el direccionamiento es el siguiente (2)

$$sede\_A(config-if)\#ipv6\ address\ (IP\ A\ ASIGNAR)(2)$$

Este proceso se lleva a cabo en cada uno de los router ubicado en cada sede, además se crean subinterfaces dado que se desea segmentar la red de la siguiente manera, la vlan 10 se utilizará para el personal administrativo, vlan 11 para el sector operativo y por último la vlan 12 para el sector tecnológico.

Cabe resaltar que al momento de configurar IPV6 en un router CISCO, cuando se desea configurar cada interface es necesario modificar dos direcciones IPV6: una que es la dirección LAN o WAN, que fue lo que anteriormente se indicó, y otra llamada Link Local o de enlace local [30], la cual permite que se puedan comunicar todas las redes que estén configuradas en el router y las que converjan con el router, de no ingresar esta dirección la comunicación con otras redes no será posible. Esta IP se debe colocar en todas las interfaces del router, pero en caso de olvidar colocarla, se puede hacer uso del comando

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

IPV6 Enable dentro de la configuración de la interface permitiendo que se configure de forma automática con la MAC del router, puesto que la dirección link local no se puede repetir en los router adyacentes para no generar conflicto entre redes. En IPv6, estas direcciones están reservadas con el prefijo fe80::/64 [31]. Figura 7.

```
SEDE_A#show ipv6 interface brief
GigabitEthernet0/0         [up/up]
    FE80::2
    2001:DB8:ACAD:A::
GigabitEthernet0/1         [up/up]
    FE80::2
    2001:DB8:CAFE:A::
GigabitEthernet0/1.10      [up/up]
    FE80::2
    2800:10:12:A::
GigabitEthernet0/1.11      [up/up]
    FE80::2
    2800:10:12:B::
GigabitEthernet0/1.12      [up/up]
    FE80::2
    2800:10:12:C::
GigabitEthernet0/2         [administratively down/down]
FastEthernet0/0/0          [up/down]
FastEthernet0/0/1          [up/down]
FastEthernet0/0/2          [up/down]
FastEthernet0/0/3          [up/down]
Vlan1                      [administratively down/down]
```

Figura 7. Asignación IPV6. **Fuente:** Propia elaboración.

2.1.4 Implementación de seguridad en capa 2 y capa 3.

En la estructura de una implementación o transición la parte más importante es la seguridad sobre cada equipo que pertenece a esta misma red, puesto que la seguridad de la información en una empresa o entidad es lo más valioso [32], puesto que cualquier vulnerabilidad sobre la red puede generar pérdidas de algún tipo ya sea económicos, información entre otros [33].

En tanto, para la implementación de la seguridad en nuestra red se procedió primero a proteger los equipos que permiten la comunicación con todas las sedes (router), en la seguridad de estos equipos se puede bloquear el acceso a los equipos permitiendo solo conexiones seguras como el protocolo SSH llevando esto a no permitir el acceso a usuarios sin credenciales de autenticación, este protocolo de seguridad se configura directamente en

el router además para la asignación de credenciales (usuario y contraseña) se puede ejecutar por medio de un servidor radius o credenciales locales [34], para el desarrollo del artículo se realizó mediante credenciales locales, es de aclarar que las contraseñas brindadas para este tipo de conexiones se encuentran encriptados por método RSA 1024 visualizado en la figura 8, además de se genera contraseñas de acceso al modo configuración para generar cambio sobre el equipo.

```
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
username Udistrital privilege 15 secret 5 $1$mERr$5.a6P4JqbNiMX0lusIfka/
!
```

Figura 8. Usuarios y credenciales de acceso (SSH). **Fuente:** Propia elaboración.

En capa 2 (Switch) se brindan recomendaciones adicionales de seguridad como el bloqueo administrativo de las interfaces que no se encuentran en uso como se visualiza en la figura 9, esta configuración no se ejecuta en los router puesto que se aprovisiona por defecto, de igual forma en los Switch se debe configurar protocolos de ingreso remotos a los equipos como SSH, credenciales de autenticación, otra de las indicaciones de seguridad implementada es el bloqueo de puertos por cambio de equipos (PC) almacenando la Mac de cada computador por puerto y en caso de que no sea la misma procesa a bajar el puerto evitando vulnerabilidad en la información, es de aclarar que esta configuración se debe ejecutar en cada interfaces las cuales cuenten con equipos conectados [35], Figura 10.

Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

```
SWC_2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual up                    up
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual up                    up
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
Vlan20                 unassigned      YES manual up                    up
Vlan21                 unassigned      YES manual up                    up
```

Figura 9. Interface administrativamente DOWN. **Fuente:** Propia elaboración.

```
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.63A1.9355
!
```

Figura 10. Seguridad por MAC. **Fuente:** Propia elaboración.

2.1.5 Transición de protocolos a IPV6.

En primera instancia se hará la transición del protocolo de enrutamiento, el cual es de OSPF V2 a OSPF V3 [36], se debe habilitar el protocolo de enrutamiento en el router utilizando el comando en modo configuración (3)

$$(\text{config})\#\text{ipv6 router ospf 1 } [\#](3)$$

permitiendo esto el ingreso a la estructura del protocolo OSPF [37], donde se dispone a establecer los siguientes parámetros, Interfaces pasiva las cuales el router no enviará la tabla de enrutamiento ya que por estas se propaga la red LAN evitando saturación o procesamiento elevado del router [38], el parámetro más importante es el router-ID el cual es

el identificador y cuenta con un direccionamiento en IPV4 como 1.1.1.1, nuevamente como la link local para cada router se debe contar con un identificador distinto.

En caso de contar con enrutamiento estático por defecto, para hacer el anunciamiento y propagación dentro del protocolo OSPF debemos utilizar el comando default-information, ahora en caso de contar con rutas estáticas para el anunciamiento y propagación se utiliza el comando redistribute static, estas rutas se propagan por todos los router que se encuentren en la misma área.

Para tener en cuenta, se tiene que saber que la activación del protocolo y su respectiva área se ejecuta dentro de cada una de las interfaces, esto se hace de la siguiente manera. (4) (5) Figura 11.

$$\text{config} - \text{if})\#\text{ipv6 ospf \# área \# } (4)$$

```
interface GigabitEthernet0/1.10
 description ADMINISTRATIVOS
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 172.16.0.20
 ipv6 address FE80::2 link-local
 ipv6 address 2800:10:12:A::/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1.11
 no ip address
 ipv6 address FE80::2 link-local
 ipv6 address 2800:10:12:B::/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
```

Figura 11. Configuración OSPF **Fuente:** Propia elaboración.

$$(\text{config})\#\text{show ipv6 route}(5)$$

Seguidamente, se efectuará la transición mediante métodos con el fin de que IPV6 e IPV4 coexistan dentro de la red, se de tener en cuenta que hay varios métodos de transición donde los más conocidos son:

Dual stack: el cual hace referencia a que en la red los equipos y servicios encontrados allí manejen doble pila, es decir soportan ambos protocolos [39].

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

Tunelización: es un método el cual por medio de túneles encapsula los paquetes de datos y los envía por estos, generalmente esto se realiza para dos escenarios en específico, cuando se quieren comunicar dos redes que manejan protocolo IPV6, sin embargo, el tráfico debe transportarse por una red IPV4, generalmente el Core o Backbone [40]. Figura 12

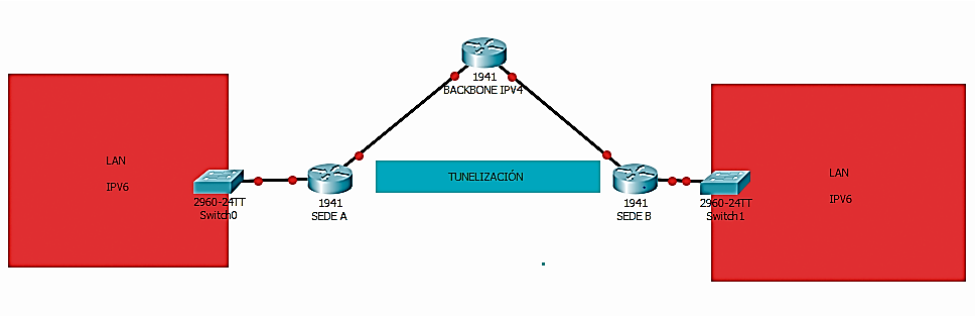

Figura 12. Tunelización. **Fuente:** Propia elaboración.

Por otro lado, el segundo escenario es cuando las redes que se pretender comunicar se encuentran aprovisionadas con IPV4, pero el Core es IPV6, aunque esto no es algo que vaya a observar muy a menudo [41].

Aunque no tan conocidos, pero con una mejor usabilidad y con mejores beneficios, también encontramos técnicas como:

NAT64: El cual consiste en usar la misma función del NAT conocido generalmente, en este caso se traducen paquetes con dirección IPV6 a direcciones IPV4 y viceversa, para esta operación se efectúa la traducción del encabezado de cada paquete. Las direcciones IPV4 son traducidas algorítmicamente desde IPV6 usando el algoritmo definido en el estándar RFC6052, y un prefijo IPV6 designado al NAT64 con estado. Para la traducción de direcciones IPV6 desde direcciones IPV4 se instalan mapeos haciendo traducción del puerto de red.

Este método es muy útil, dado que ayuda con el agotamiento de direcciones IPV4, ya que se usarían host IPV4 en las LAN de los clientes y se traduciría a IPV6 para salir a internet, dando grandes campos de aplicabilidad como el internet de las cosas [42]. Figura 13.

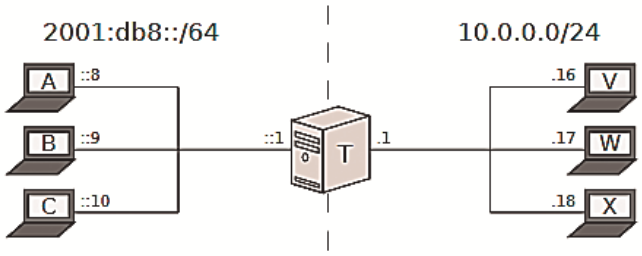

Figura 13. NAT 64 **Fuente:** [42].

Hay que aclarar que este método presenta un inconveniente; como aun esta en despliegue el protocolo, se tiene previsto que aun tarde varios años en que toda la red sea IPV6 por tal motivo, aun coexistirán varias aplicaciones que solo soportan IPV4, y este método es IPV6-ONLY, es decir, que servicios como el de SKYPE no trabajarían con NAT64, así que si se usan direcciones literales no funcionara el método, si se usan sockets APIs tampoco servirá este.

464XLAT: Como se informó anteriormente, el NAT64 presenta una falencia bastante notoria para usarse en la actualidad, es por eso que se combinó el uso del RFC6145 y el RFC6146, con el fin de proporcionar a los clientes servicios básicos en IPV4 sobre la infraestructura de IPV6. Para esto se harán uso de servidores los cuales traducirán el direccionamiento internamente antes de que los paquetes viajen a través de la red externa como se visualiza en la figura 14, [43].

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

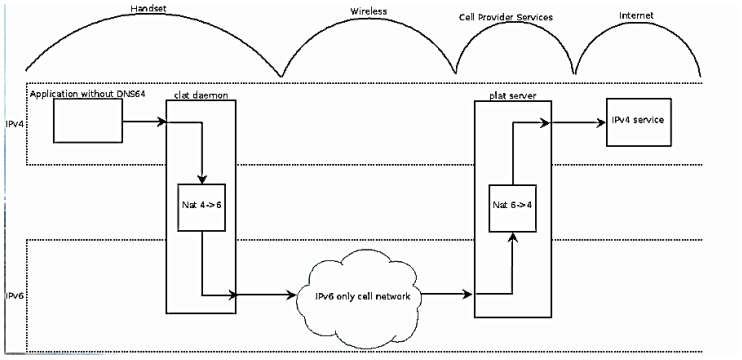

Figura 14. 464XLAT **Fuente:** [43].

Gracias a esta combinación, podremos ver las diferentes soluciones para usar en la red. Figura 15.

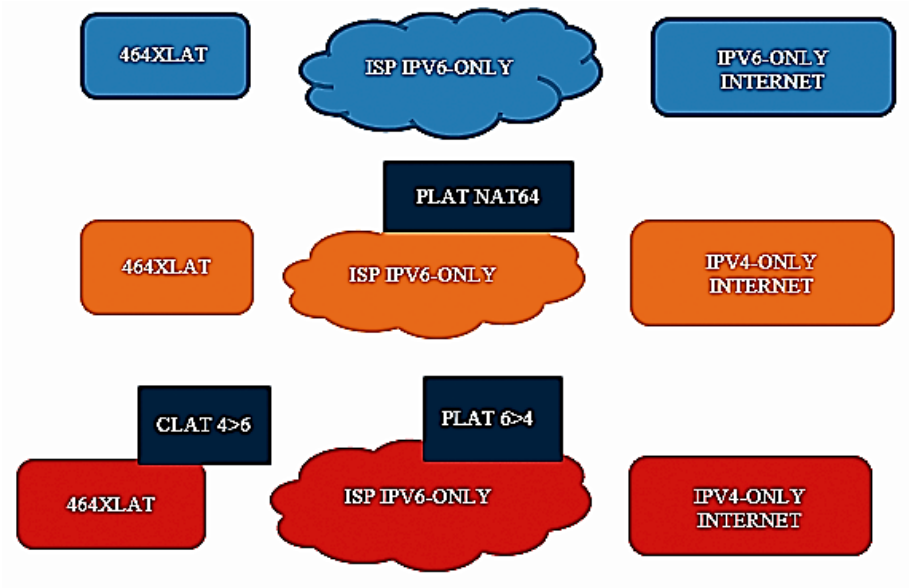

Figura 15. 464 XLAT usabilidad **Fuente:** [44].

Donde PLAT=CUSTOMER SIDE TRANSLATOR, y CLAT=PROVIDER SIDE TRANSLATOR.

MAP: Esta es una solución basada en técnicas de traducción sin estado existentes especificadas en algunos estándares como los son: RFC6052, RFC6144 y RFC6145 [45].

Esta técnica posee dos variantes, la primera es encapsulación MAP (MAP-E), la cual usa IPv6 para encapsular y desencapsular el tráfico IPv4. La segunda traducción MAP (MAP-T) que usa NAT64 para traducir IPv4 a IPv6 y viceversa [45].

Más específicamente la técnica MAP-T da la posibilidad de una transición completa, posee características como:

- Conserva la capacidad de los hosts finales IPv4 de comunicarse a través del dominio IPv6 con otros hosts IPv4, al mismo tiempo que permite la asignación de direcciones IPv4 individuales y el uso compartido de direcciones [45].
- Permite la comunicación entre hosts finales solo IPv4, así como cualquier host final habilitado para IPv6, a servidores nativos solo IPv6 en el dominio que están usando una dirección IPv6 mapeada IPv4 [45].
- No requiere el funcionamiento de una red de superposición IPv4 con estado, ni la introducción de un dispositivo de red no nativo IPv6 o la funcionalidad del servidor [45].
- Permite el uso de operaciones de red nativa de IPv6, incluida la capacidad de clasificar el tráfico IP, así como realizar políticas de optimización de enrutamiento de tráfico IP, como la optimización de enrutamiento, basada en políticas similares para destinos de Internet IPv4 fuera del dominio [45].

Cabe aclarar, que en este artículo se podrá observar los dos métodos inicialmente nombrados, ya que son los más conocidos y se puede trabajar en el simulador, el dual stack se puede apreciar en la sede A ya que maneja ambas pilas así como se puede apreciar en la figura 16.

Seguidamente es de gran importancia tener claridad la configuración de la tunelización para los casos en que el trafico IPV6 tenga que transportarse por redes IPV4.

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

Para la demostración, se hará uso de las sedes C y B las cuales manejan IPV6-ONLY, sin embargo, la principal se encuentra distribuida con direccionamiento IPV4, por lo tanto, es necesario ingresar a los router, para activar los túneles, estos realizan la función de simular un enlace entre ambas puntas, donde se encapsularán los paquetes desde el origen y se desencapsula en el destino, esto con el fin de no pasar el tráfico por la red IPV4 figura 16.

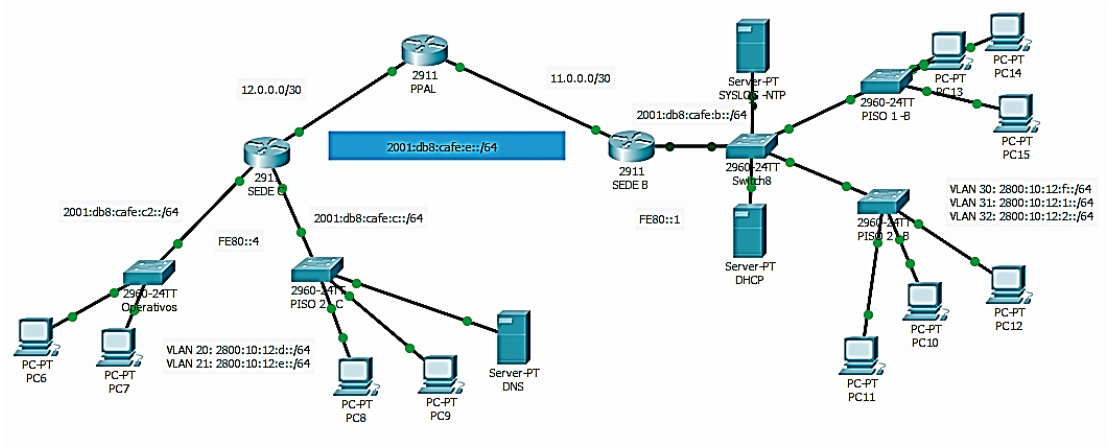

Figura 16. Red sede B y C Tunelización. **Fuente:** Propia elaboración.

Al ingresar al router, se entra al modo configuración y seguidamente se creará una interfaz lógica conocida como TUNNEL, la cual llevará direccionamiento IPV6. (6)

$$\text{config)\#interface tunnel 1 [\#](6)}$$

Esta se maneja como una interfaz física normal, ahora se activa el protocolo IPV6 (7)

$$\text{config} - \text{if)\#ipv6 enable (7)}$$

Se agrega la IP resaltada en azul en la figura 16 la cual es 2001:db8:cafe:e::/64, seguidamente se le asigna la dirección LINK-LOCAL establecida para este router [46], la cual es la FE80::1, es de aclarar que sobre esta interfaz también es obligatorio adicionar el enrutamiento OSPF para que se pueda establecer la comunicación con las demás sedes, esto se efectúa como anteriormente se indicó.

Se aprovisionarán los parámetros adecuados para que el túnel funcione correctamente, inicialmente se colocara el origen del túnel, en este caso es la interfaz por donde físicamente pasaría el tráfico hacia la otra sede. (8)

$$-\text{if)\#tunnel source gigabitEthernet } 0/0 \text{ [\#] } (8)$$

Y ahora se modifica el destino, el cual que es La IP a. donde llegarían los paquetes encapsulados, el cual sería la IP WAN del router de la sede C (9)

$$-\text{if)\#tunnel destination } 12.0.0.2 \text{ [\#] } (9)$$

Es de tener en cuenta que por defecto los túneles se establecen en TUNNEL GRE, sin embargo, el modo del túnel debe soportar IPV6, por ende se utiliza el comando (10).

$$-\text{if)\#tunnel mode IPV6ip } (10)$$

Este procedimiento ha de efectuarse igualmente en el router de la sede C. donde los parámetros que cambiarían son el destino y el origen (11) (12)

$$-\text{if)\#tunnel source gigabitEthernet } 0/0 \ (11)$$

$$-\text{if)\#tunnel destination } 11.0.0.2 \ (12)$$

Con esto se concluye la transición de protocolos.

2.1.6 Transición de servicios a IPV6:

Para la configuración de los servicios (DHCP, DNS, SYSLOG, NTP y CORREO) se realizara por medio de servidores, los cuales se encuentran instalados en las diferentes sedes para evidenciar que la red converge con protocolo IPV6, es de aclarar que todos los servidores deben contar con una dirección IPV6 configurada de forma estática puesto que ninguno de estos pueden contar con direccionamiento dinámico a causa de que los equipos de las diferentes sedes deben solicitar los servicios a estos y en caso de contar con direccionamiento dinámico esto impedirá que conozcan la ubicación de cada servidor. Figura 17.

Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

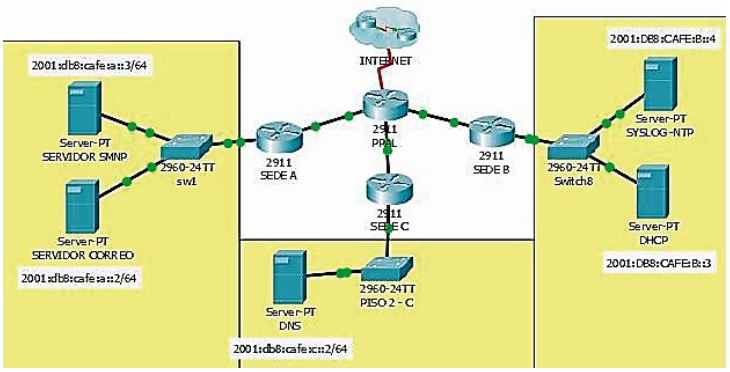

Figura 17. Topología de servidores **Fuente:** Propia elaboración

En primer lugar se establecerá el servicio DHCP encargado de brindar direccionamiento dinámico para los equipos que se encuentren en la red, a continuación se relaciona la interface de configuración del servidor pero antes de establecer esta configuración se debe contar con los segmentos de red IPV6, IP servidor DNS, prefijo, y mascara de cada red [26]. Figura 18.

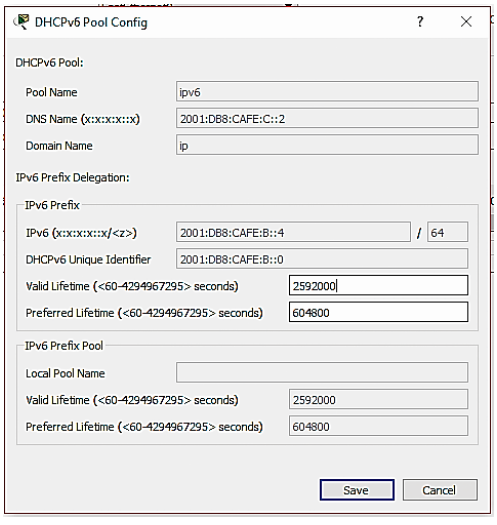

Figura 18. Configuración servidores DHCP **Fuente:** Propia elaboración

Seguidamente, para la configuración del servidor DNS el cual permite traducir un direccionamiento IPV6 a un nombre de dominio o viceversa (registros tipo A, CNAME, TXT,

PTR, entre otros), cuando un servidor DNS se encuentra dentro de una red LAN es porque la empresa u organización cuenta con Intranet la cual será accedida solo por los usuarios conectados en esta y no es publicada en internet, en la actualidad los servidores DNS son brindados por un tercero o un ISP, estos permitirán conexión a internet a los equipos conectados en la red de la compañía. En la figura 19 se muestra el nombre de dominio (www.udistrital.edu) el cual se configuro en el servidor DNS con la IPV6 (2001:DB8:CAFE:C::2) [26].

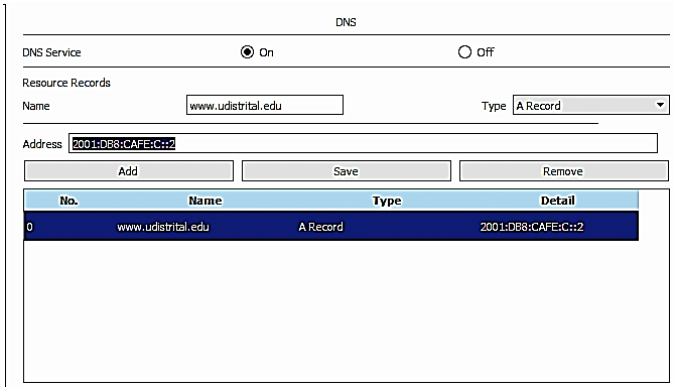

Figura 19. Configuración servidor DNS **Fuente:** Propia elaboración

Dando continuidad a la configuración de los servidores solicitados, para ejecutar la configuración del servidor de correo se procedió a establecer el dominio *udistrital.edu*, sobre este dominio se crearan todas las cuentas de correo que se utilizan sin importar la sede en la que se encuentre la persona, para la creación de un nuevo usuario bajo el dominio antes indicado se debe asociar un usuario y asignar una clave que permita autentica su identidad, en la figura 20 se puede visualizar el dominio con los usuarios creados (Administrativo, estudiante) [26].

Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

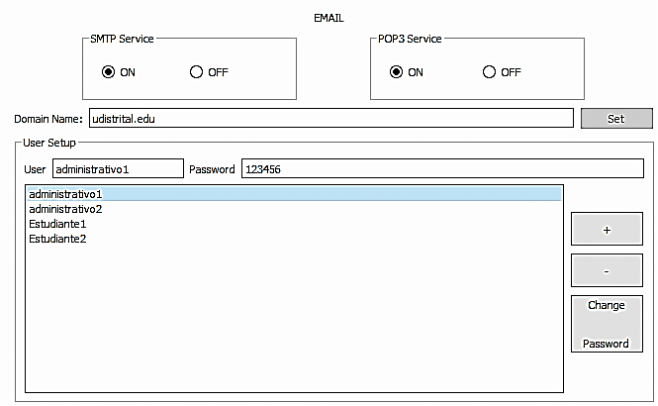

Figura 20. Configuración servidor de correo **Fuente:** Propia elaboración

Por último, y no menos importante, se configuraron los servicios NTP y SYSLOG, los cuales se puede aprovisionar en el mismo servidor; para el servicio NTP es de recordar que es el encargado de brindar y propagar la fecha y hora sobre la red, replicando estos parámetros en todos los equipos (computadores, router, servidores y switch), además este servicio permite el funcionamiento del servicio syslog, el cual permite almacenar registro de todas las actividades realizadas en los diferentes router ubicados en sus diferentes sedes, el almacenamiento de esta información se efectúa mediante el registro en el servidor syslog visualizando fecha y hora del suceso o actividad realizada en los equipos, para mayor entendimiento se expone el siguiente ejemplo: si en el router de la sede A se desconecta una interfaz o se apaga el equipo este cambió sobre el equipo será almacenado en el servidor [26].

3 Resultados

3.1 Resultados aprovisionamiento direccionamiento IPV6.

Con el comando ***show ipv6 interface brief*** se podrá apreciar el direccionamiento asignado a los router de las 3 sedes. Figura (21).

```
SEDE_C#show ipv6 interface brief
GigabitEthernet0/0          [up/up]
GigabitEthernet0/1          [up/up]
    FE80::4
    2001:DB8:CAFE:C2::
GigabitEthernet0/2          [up/up]
    FE80::4
    2001:DB8:CAFE:C::
GigabitEthernet0/2.20       [up/up]
    FE80::4
    2800:10:12:D::
GigabitEthernet0/2.21       [up/up]
    FE80::4
    2800:10:12:E::
FastEthernet0/0/0           [up/down]
FastEthernet0/0/1           [up/down]
FastEthernet0/0/2           [up/down]
FastEthernet0/0/3           [up/down]
Tunnel1                     [up/up]
    FE80::202:16FF:FE26:940A
    2001:DB8:CAFE:E::
Vlan1                       [administratively down/down]
```

Figura 21. Direccionamiento SEDE C **Fuente:** Propia elaboración

3.2 Resultados implementación de seguridad en capa 2 y capa 3

El aprovisionamiento de la seguridad como se explicaba en la parte 2.1.4, se configuro de tal forma que para los nuevos equipos (PC) que ingresen a la red se deban autorizar por el ingeniero de redes de cada empresa ya que los puertos en los equipos de capa 2 se encuentran administrativamente deshabilitados impidiendo subir el puerto como se muestra en la figura 22, además en caso de contar con un cambio de equipos sin previa autorización del administrador de la red genera un bloqueo del puerto impidiendo la conexión PC17, en la figura 22 se evidencian el puerto del PC8 operativo pero en la figura 23 cuando se genera el cambio de este computador por un equipo nuevo el bloqueo es de forma automática.

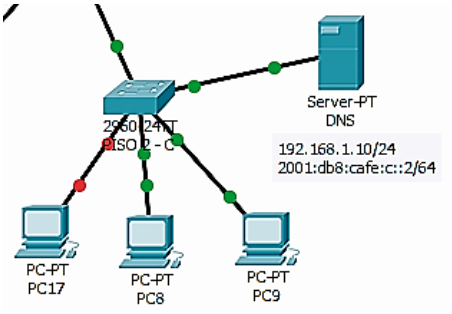

Figura 22. Acceso de equipo a la red - seguridad **Fuente:** Propia elaboración

Preparación de Artículos revista VISIÓN ELECTRÓNICA: algo más que un estado sólido
Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

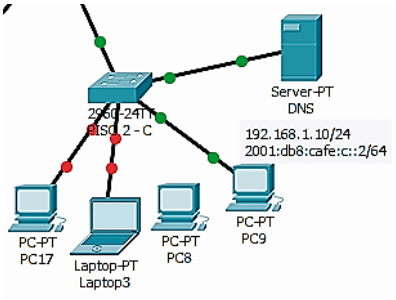

Figura 23. Cambio de PC bloqueo por MAC - seguridad **Fuente:** Propia elaboración

Otra de las configuraciones ejecutadas sobre los equipos de capa 2 y capa 3 para protegerlos de posibles ataques o vulnerabilidades es el acceso retomo por protocolo SSH [47], solo los equipos que pertenecen a la red pueden acceder a este, en la figura 24 se visualiza el acceso al router principal desde un PC ubicado en la sede A, es de recordar que el acceso a estos equipos es mediante credenciales anteriormente configuradas, en caso de que las credenciales sean incorrectas el acceso será negado, el acceso también se niega utilizando otro protocolo diferente a SSH [48].

Figura 24. Acceso SSH router principal **Fuente:** Propia elaboración

3.3 Transición de protocolos a IPV6.

En primera instancia se verificará la tabla de enrutamiento de las sedes implicadas, en donde se observará la conectividad entre las 3 sedes mediante IPV6 gracias al protocolo OSPF con el comando ***show ipv6 route***.

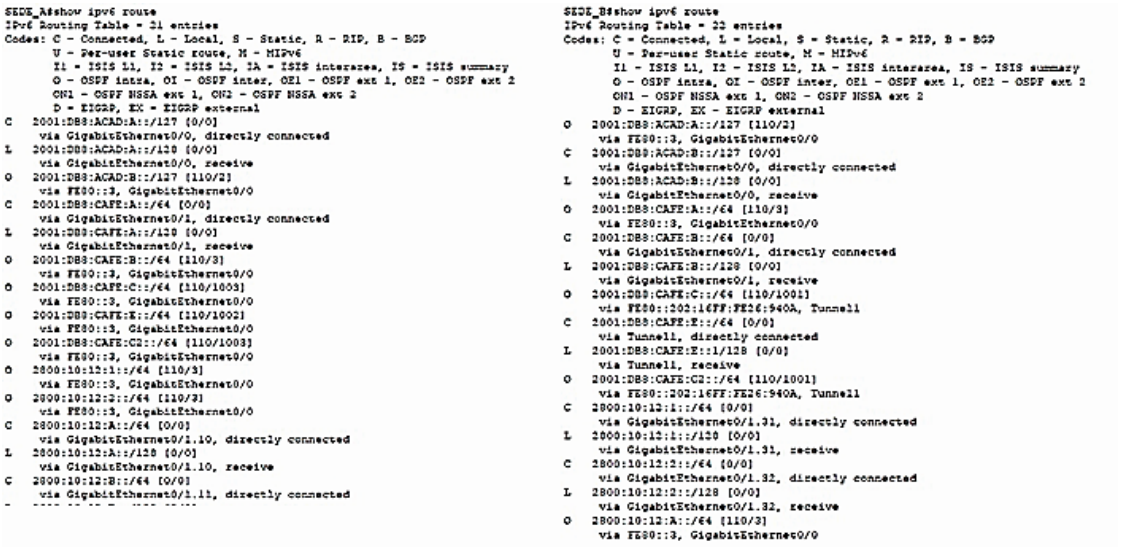

Figura 25. TABLA DE ENRUTAMIENTO SEDE A Y B **Fuente:** Propia elaboración

También se puede evidenciar mediante un PING, la conectividad entre sedes.

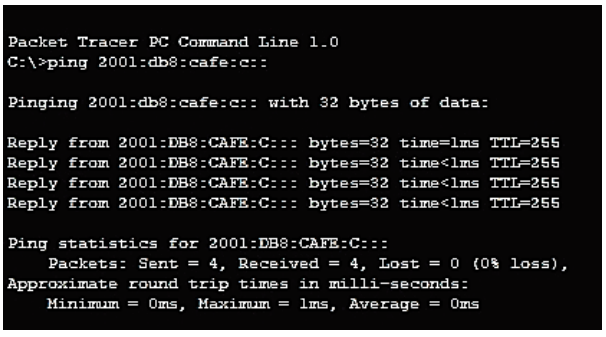

Figura 26. PING SEDE A – SEDE C **Fuente:** Propia elaboración

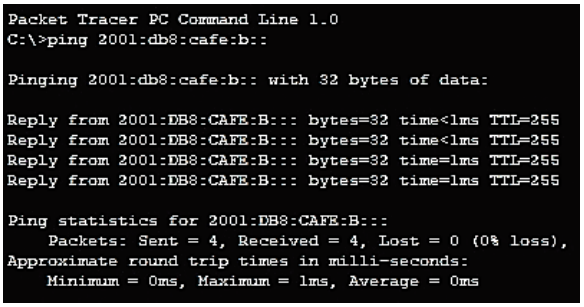

Figura 27. PING SEDE A – SEDE B **Fuente:** Propia elaboración

Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

Con respecto a la transición, el resultado obtenido se puede observar con una prueba de PING entre dos computadores [49], una de la sede B y otra de la sede C.

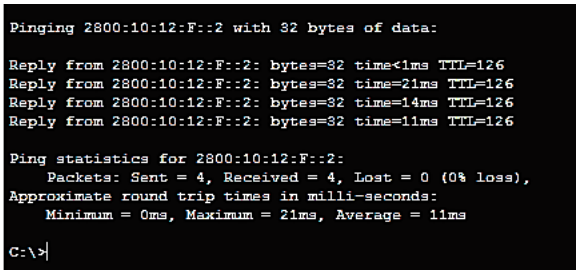

Figura 28. PING SEDE B – SEDE C **Fuente:** Propia elaboración

Igualmente, para identificar un mayor detalle de la trazabilidad del paquete se hará el uso del tracert entre estas dos computadoras [50].

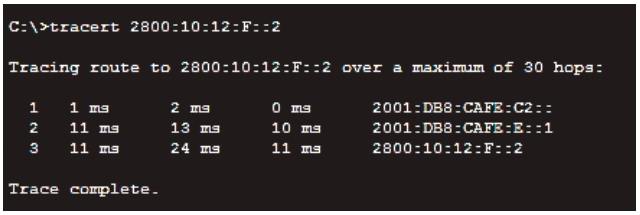

Figura 29. TRACERT SEDE B – SEDE C **Fuente:** Propia elaboración

Se aprecia cómo los paquetes pasan por el túnel y no se desvían por las interfaces físicas.

4. Conclusiones

- ✓ Con este protocolo varias empresas y compañías podrán hacer uso de nuevas aplicaciones y funciones, las cuales poseerán un diseño y software más robusto, donde se podrán conectar una gran cantidad de equipos, resaltando que se poseerá una mayor disponibilidad, integridad y confidencialidad que el protocolo antecesor.
- ✓ Aunque la transición a IPV6 en términos de enrutamiento y direccionamiento es relativamente rápida, se debe tener en cuenta que para la migración se encuentre al

100% tardara algunos años, dado que algunas aplicaciones y servidores solo permiten IPV4 por lo tanto los administradores tienen que adaptar a que estas soporten el nuevo protocolo haciendo uso de los parámetros recomendados por IPV6.

- ✓ Con la transición de los servicios básicos a IPV6 por medio de servidores se observa que la migración hacia esta nueva tecnología se ha desarrollado a tal punto que al momento de implementarlos y configurarlos se comportan de forma estable tanto para el equipo como para la red, para cumplir las necesidades se han desarrollado nuevas versiones exclusivas para el correcto funcionamiento de IPV6 tanto en los servicios como en protocolos.
- ✓ La escalabilidad de redes es uno de los beneficios más importantes y notorios dentro de la implementación del protocolo IPV6, esto puede ser de gran utilidad en las compañías, ya que generalmente los ISP brindan un pool de IP con mascara /64 (2^64), lo que proporciona una cantidad inmensa de direcciones asignables ayudando a los ingenieros de redes a realizar cambios significativos sin tener repercusiones negativas sobre sus servicios o direccionamiento de dispositivos.

Reconocimientos

Al grupo de investigación ROMA por la colaboración y asesoría técnica del artículo; igualmente a la contribución del desarrollo y estructura del mismo al grupo SciBas; ambos adscritos ante el centro de investigaciones y desarrollo científico (CIDC) de la Universidad Distrital Francisco José de Caldas.

5. Referencias

[1] J. Velasco, "La transición de IPv4 a IPv6, lo que necesitas saber", Hipertextual, 2018. [Online]. Available: https://hipertextual.com/archivo/2011/02/transicion-ipv4-a-ipv6-lo-que-necesitas-saber/. [Accessed: 07- Sep- 2018].

[2] Grupo de Investigación de Teleinformática UNAL Colombia, "Agotadas direcciones de Internet en el mundo", Mintic.gov.co, 2018. [Online]. Available:

Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

https://www.mintic.gov.co/portal/604/articles-6115_archivo_pdf.pdf. [Accessed: 27- Sep- 2018].

[3] Lacnic, "Políticas sobre el agotamiento del espacio de direcciones IPv4", Lacnic.net, 2018. [Online]. Available: http://www.lacnic.net/web/lacnic/manual-11. [Accessed: 27- Sep- 2018].

[4] Wikipedia, "IPv6", Es.wikipedia.org, 2018. [Online]. Available: https://es.wikipedia.org/wiki/IPv6. [Accessed: 27- Sep- 2018].

[5] E. Rojas, "Diez consejos para implementar IPv6 de forma segura", MuyComputerPRO, 2018. [Online]. Available: https://www.muycomputerpro.com/2012/07/03/consejos-implementar-ipv6-segura. [Accessed: 28- Sep- 2018].

[6] E. Camargo, "PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED IPV4 A IPV6 EN LA UNIVERSIDAD INDUSTRIAL DE SANTANDER EDWIN ROLANDO CAMARGO ACEVEDO - PDF", Docplayer.es, 2018. [Online]. Available: https://docplayer.es/10068407-Plan-de-transicion-del-protocolo-de-red-ipv4-a-ipv6-en-la-universidad-industrial-de-santander-edwin-rolando-camargo-acevedo.html. [Accessed: 27- Sep- 2018].

[7] C. IPv4/IPv6, "Coexistencia IPv4/IPv6", Ipv4to6.blogspot.com, 2018. [Online]. Available: http://ipv4to6.blogspot.com/p/coexistencia-ipv4ipv6.html. [Accessed: 28- Sep- 2018].

[8] IPV6, "IPv6 para Usuarios - IPv6", Ipv6.es, 2018. [Online]. Available: http://www.ipv6.es/es-ES/transicion/usuarios/Paginas/IPv6_usuarios.aspx. [Accessed: 08- Sep- 2018].

[9] Mintic, "Guía de transición de IPV4 a IPV6 para Colombia", Mintic.gov.co, 2018. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf. [Accessed: 13- Sep- 2018].

[10] D. Fonseca Castro, "PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED IPv4 A IPv6 BASADO EN LAS RECOMENDACIONES REALIZADAS POR EL MIN TIC COLOMBIA.", Fusagasuga-cundinamarca.gov.co, 2018. [Online]. Available: http://www.fusagasuga-cundinamarca.gov.co/Transparencia/MODELO%20INTEGRADO%20DE%20PLANEACION%20Y%20GESTION/Plan%20de%20Transicion%20del%20Protocolo.pdf. [Accessed: 08- Sep- 2018].

[11] E. Segura, "METODOLOGIA PARA HACER UNA TRANSICION EN UNA RED IPV4 A IPV6", Repository.usta.edu.co, 2018. [Online]. Available: https://repository.usta.edu.co/bitstream/handle/11634/9245/SeguraEdwin2017.pdf?sequence=1. [Accessed: 28- Sep- 2018].

[12] J. Moreno, "TRANSICIÓN DE PROTOCOLOS IPV4 A IPV6, PARA UNA EMPRESA DEL ESTADO, CON APLICACIÓN EN UNA CIUDAD INTERMEDIA", Repositorio.utp.edu.co, 2018. [Online]. Available: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/7787/00462M843.pdf?sequence=1. [Accessed: 28- Sep- 2018].

[13] Wikipedia, "IPv4", Es.wikipedia.org, 2018. [Online]. Available: https://es.wikipedia.org/wiki/IPv4. [Accessed: 27- Sep- 2018].

[14] Oracle, "Capítulo 4 Planificación de una red IPv6 (tareas) (Guía de administración del sistema: servicios IP)", Docs.oracle.com, 2018. [Online]. Available: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-1/index.html. [Accessed: 27- Sep- 2018].

[15] Oracle, "Descripción general de las direcciones IPv6 (Guía de administración del sistema: servicios IP)", Docs.oracle.com, 2018. [Online]. Available: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/index.html. [Accessed: 27- Sep- 2018].

[16] Cisco, "Download The Packet Tracer Simulator Tool & Find Courses | Networking Academy", Netacad.com, 2018. [Online]. Available: https://www.netacad.com/es/courses/packet-tracer. [Accessed: 28- Sep- 2018].

[17] Baquia, "Manual para la transición de IPv4 a IPv6 - BAQUIA", BAQUIA, 2018. [Online]. Available: https://www.baquia.com/emprendedores/2011-03-21-manual-para-la-transicion-de-ipv4-a-ipv6. [Accessed: 28- Sep- 2018].

[18] L. Melo, "PROPUESTA DE DISEÑO PARA LA TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 4 (IPV4) AL PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) EN LA EMPRESA MARKET MIX S.A.S", Repository.usta.edu.co, 2018. [Online]. Available: https://repository.usta.edu.co/bitstream/handle/11634/282/PROPUESTA%20DE%20DISE%C3%91O%20PARA%20LA%20TRANSICI%C3%93N%20DE%20IPV4%20A%20IPV6.pdf?sequence=1&isAllowed=y. [Accessed: 27- Sep- 2018].

[19] D. Landy Rivera, "Propuesta de un plan de implementación para la migracion a IPv6 en la red de la Universidad Politécnica Salesiana sede Cuenca", Dspace.ups.edu.ec, 2018. [Online]. Available: https://dspace.ups.edu.ec/bitstream/123456789/5332/1/UPS-CT002767.pdf. [Accessed: 08- Sep- 2018].

[20] Lacnic, "Portal IPv6 - LACNIC", Portalipv6.lacnic.net, 2018. [Online]. Available: http://portalipv6.lacnic.net/mecanismos-de-transicion/. [Accessed: 08- Sep- 2018].

[21] D. Ramirez, J. Pantoja and J. Beltran, "DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA AGENCIA COLOMBIANA PARA LA REINTEGRACIÓN-ACR CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACIÓN DE IPV6", Repository.ucatolica.edu.co, 2018. [Online]. Available: https://repository.ucatolica.edu.co/bitstream/10983/2803/1/IPV6.pdf. [Accessed: 27- Sep- 2018].

[22] Huawei, "Basic IPv6 Configuration - HUAWEI NetEngine80E and 40E Router Configuration Guide - IP Services (V600R001C00_03) - Huawei", Support.huawei.com, 2018. [Online]. Available: http://support.huawei.com/enterprise/en/doc/EDOC0100412581?section=j00c. [Accessed: 07- Sep- 2018].

[23] Lacnic, "Portal IPv6 - LACNIC", Portalipv6.lacnic.net, 2018. [Online]. Available: http://portalipv6.lacnic.net/quienes-implementan/. [Accessed: 08- Sep- 2018].

Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

[24] Mintic, "Promoción de la adopción del Ipv6 en Colombia", Mintic.gov.co, 2018. [Online]. Available: https://www.mintic.gov.co/portal/604/articles-5932_documento.pdf. [Accessed: 27- Sep- 2018].

[25] Oracle, "Capítulo 5 Configuración de servicios de red TCP/IP y direcciones IPv4 (tareas) (Guía de administración del sistema: servicios IP)", Docs.oracle.com, 2018. [Online]. Available: https://docs.oracle.com/cd/E19957-01/820-2981/ipconfig-1/index.html. [Accessed: 27- Sep- 2018].

[26] P. Support, E. Products and C. Guides, "Catalyst 3750 Software Configuration Guide, Release 12.2(55) SE - Configuring IPv6 Routing [Cisco Catalyst 3750 Series Switches]", Cisco, 2018. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swipv6.html#23760. [Accessed: 08- Sep- 2018].

[27] M. Masataka, K. Masanobu and B. Cameron, "RFC 6877 - 464XLAT: Combination of Stateful and Stateless Translation", Tools.ietf.org, 2018. [Online]. Available: https://tools.ietf.org/html/rfc6877. [Accessed: 07- Sep- 2018].

[28] Oracle, "Descripción general sobre los túneles de IPv6 (Guía de administración del sistema: servicios IP)", Docs.oracle.com, 2018. [Online]. Available: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-160/index.html. [Accessed: 27- Sep- 2018].

[29] IPV4to6, "Comparativas en el routing", Ipv4to6.blogspot.com, 2018. [Online]. Available: http://ipv4to6.blogspot.com/p/comparativas-en-el-routing.html. [Accessed: 28- Sep- 2018].

[30] Oracle, "Configuración automática de direcciones IPv6 (Guía de administración del sistema: servicios IP)", Docs.oracle.com, 2018. [Online]. Available: https://docs.oracle.com/cd/E19957-01/820-2981/chapter1-42/index.html. [Accessed: 27- Sep- 2018].

[31] Oracle, "Capítulo 11 IPv6 en profundidad (referencia) (Guía de administración del sistema: servicios IP)", Docs.oracle.com, 2018. [Online]. Available: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-ref-76/index.html. [Accessed: 28- Sep- 2018].

[32] Mintic, "Modelo de Seguridad y Privacidad de la Información", Mintic.gov.co, 2018. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf. [Accessed: 28- Sep- 2018].

[33] Mintic, "Modelo de Seguridad - Fortalecimiento TI", Mintic.gov.co, 2018. [Online]. Available: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html. [Accessed: 08- Sep- 2018].

[34] H. Arias, "ESTRATEGIA DE MIGRACIÓN DE IPv4 A IPv6 PARA LAS PYMES EN COLOMBIA", Repositorio.ucp.edu.co, 2018. [Online]. Available: http://repositorio.ucp.edu.co:8080/jspui/bitstream/10785/958/1/CDMIST45.pdf. [Accessed: 28- Sep- 2018].

[35] S. Ramirez and M. Cervantes, "Router con soporte IPv6 - RAU", Rau.edu.uy, 2018. [Online]. Available: https://www.rau.edu.uy/ipv6/router.htm. [Accessed: 08- Sep- 2018].

[36] G. Cicileo, R. Gagliano and C. Olvera, "Ipv6 para todos", Ipv6tf.org, 2018. [Online]. Available: http://www.ipv6tf.org/pdf/ipv6paratodos.pdf. [Accessed: 28- Sep- 2018].

[37] IPV4to6, "Configuración de OSPF3", Ipv4to6.blogspot.com, 2018. [Online]. Available: http://ipv4to6.blogspot.com/p/configuracion-de-ospf3.html. [Accessed: 28- Sep- 2018].

[38] Lacnic, "No hay más direcciones IPv4 en America Latina y Caribe", Lacnic.net, 2018. [Online]. Available: http://www.lacnic.net/web/anuncios/2014-no-hay-mas-direcciones-ipv4-en-lac. [Accessed: 27- Sep- 2018].

[39] Cisco, "Dual Stack Network", Cisco.com, 2018. [Online]. Available: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/IPV6at_a_glance_c45-625859.pdf. [Accessed: 07- Sep- 2018].

[40] IPV6, "Transición IPv4 --> IPv6", Redesdecomputadores.umh.es, 2018. [Online]. Available: http://redesdecomputadores.umh.es/ipv6/Transici%C3%B3n.html#. [Accessed: 07- Sep- 2018].

[41] Google, "Transición de IPv4 a IPv6 - Redes locales y globales", Sites.google.com, 2018. [Online]. Available: https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/6-transicion-de-ipv4-a-ipv6. [Accessed: 07- Sep- 2018].

[42] Lacnic, "Implementando SIIT / NAT64 usando Jool", Lacnic.net, 2018. [Online]. Available: http://www.lacnic.net/innovaportal/file/2467/1/jool.20180222.pdf. [Accessed: 07- Sep- 2018].

[43] J. Martinez, "464XLAT", Www3.lacnic.net, 2018. [Online]. Available: http://www3.lacnic.net/eventos/lacnic23/miercoles/jordi-palet-consulintel.pdf. [Accessed: 08- Sep- 2018].

[44] J. Martinez, "Using 464XLAT in residential networks", Ripe74.ripe.net, 2018. [Online]. Available: https://ripe74.ripe.net/presentations/151-ripe-74-ipv6-464xlat-residential-v2.pdf. [Accessed: 08- Sep- 2018].

[45] Cisco, "Carrier-Grade IPv6: Mapping Address and Port-Translation Technical Brief", Cisco.com, 2018. [Online]. Available: https://www.cisco.com/c/en/us/solutions/service-provider/carrier-grade-ipv6-solution/solution_overview_c11-726499.pdf. [Accessed: 08- Sep- 2018].

[46] L. Jaquez, "Subnetting IPV6", Ccnaaldia.blogspot.com, 2018. [Online]. Available: http://ccnaaldia.blogspot.com/2015/03/subnetting-ipv6.html. [Accessed: 28- Sep- 2018].

[47] E. Morales, "MIGRACIÓN DEL PROTOCOLO IPv4 A IPv6 EN UNA RED, LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO", Biblioteca.usac.edu.gt, 2018. [Online]. Available: http://biblioteca.usac.edu.gt/tesis/08/08_0246_EO.pdf. [Accessed: 28- Sep- 2018].

[48] Mintic, "Guía de aseguramiento del Protocolo IPv6", Mintic.gov.co, 2018. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf. [Accessed: 08- Sep- 2018].

Fecha de envío: 22/10/2018
Fecha de recepción: 22/10/2018
Fecha de aceptación: 07/11/2018

[49] G. Díaz, "Redes de Computadoras Introducción", Webdelprofesor.ula.ve, 2018. [Online]. Available: http://webdelprofesor.ula.ve/ingenieria/gilberto/redes/02_introduccion.pdf. [Accessed: 27- Sep- 2018].

[50] Oracle, "Capítulo 8 Administración de redes TCP/IP (tareas) (Guía de administración del sistema: servicios IP)", Docs.oracle.com, 2018. [Online]. Available: https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-admintasks-1/index.html. [Accessed: 27- Sep- 2018].