PARQUES NACIONALES NATURALES DE COLOMBIA

FASE II IMPLEMENTACIÓN IPv6 – INFORME DE CONFIGURACIÓN DE LAS PRUEBAS REALIZADAS A NIVEL DE COMUNICACIONES

Versión 2.0

NOVIEMBRE de 2020

TABLA DE CONTENIDO

1. CONTROL DE REVISIÓN

Versión	Fecha	Motivo o Comentario del Cambio	Responsable
1.0	04/02/2020	Versión Inicial	

2. INTRODUCCIÓN

2.1. ALCANCE

Este documento está enfocado a los resultados de prueba de visibilidad y alcanzabilidad del despliegue del protocolo IPv6 para Parques Nacionales Naturales de Colombia.

LACNIC tiene como función la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa para la región de América Latina.

3. PASOS PARA LAS PRUEBAS DE VISIBILIDAD Y ALCANZABILIDAD

Para las pruebas de visibilidad y alcanzabilidad se han seguido los siguientes pasos:

1. Realización de diagnóstico de la situación actual de la red de la entidad.
2. Diseño de metodología para despliegue del protocolo IPv6:

Para la implementación de IPv6, se diseñó una metodología compuesta por las siguientes fases:

- Fase preliminar.
- Fase de preparación.
- Fase de configuración y pruebas.
- Fase de post-implementación.

3. Diseño del Plan de Direccionamiento:
4. Realización de prueba piloto:

   Para realizar la prueba piloto se llevaron a cabo los siguientes pasos en el Switch Core de la entidad:

   1. Configurar de una VLAN para pruebas. Se configuró la VLAN 44 en el Switch Core.
   2. Configurar de dirección IPv6 en la VLAN 44.
   3. Habilitar el DHCP para el direccionamiento dinámico de IPv4 e IPv6.

4. Configuración de DCHPv6 PNNC

4.1. Marco Teórico:

Hay cinco tipos de mensajes ICMPv6 diferentes definidos en RFC 4861, que son:

RS : Router Solicitation (ICMPv6 tipo 133)

Cuando se habilita una interfaz, los hosts pueden enviar un RS para solicitar a los enrutadores generar anuncios de enrutador (RA) inmediatamente en lugar de en su próxima hora programada.

RA - Router Advertisement (ICMPv6 tipo 134)

Los enrutadores anuncian su presencia junto con varios parámetros de enlace e Internet, ya sea periódicamente o en respuesta a un mensaje RS. Los RA contienen prefijos que se utilizan para determinar si otra dirección comparte el mismo enlace (determinación en el enlace) y / o configuración de dirección, un valor límite de salto sugerido, etc.

NS - Neighbor Solicitation (ICMPv6 tipo 135)

Un nodo envía un mensaje de solicitud de vecino (NS) para determinar la dirección de la capa de enlace de un vecino, o para verificar que un vecino todavía es accesible a través de una dirección de la capa de enlace almacenada en caché. Los NS también se utilizan para la detección de direcciones duplicadas (DAD).

NA - Neighbor Advertisement (ICMPv6 tipo 136)

Se envía un mensaje de anuncio de vecino (NA) en respuesta a un mensaje de NS. Un nodo también puede enviar NA no solicitados para anunciar un cambio de dirección de la capa de enlace.

Redirect (ICMPv6 tipo 137)

Los enrutadores utilizan los redireccionamientos para informar a los hosts de un mejor primer salto para un destino.

Durante el proceso RA - Router Advertisement se utilizan “flags”, las cuales están presentes para especificar parámetros de configuración, en el caso de DHCPv6 se hace uso de los flags “Managed Address (M)” y “Other Stateful Configuration (O)”, Cuando está presente el “flag” M, le está indicando al host que use un protocolo de configuración para obtener una dirección “stateful”, cuando está presente el “flag” O, le está indicando al host que use un protocolo de configuración para obtener otros (Other) parámetros de configuración adicionales.

4.2. Clientes de DHCP

Definamos primero dos términos importantes a recordar respecto a la forma en que un cliente obtiene configuración IPv6 en forma automática:

- Stateless Address Autoconfiguration

Es usado para configurar además de una dirección de tipo “Link Local” otra adicional de acuerdo con un Router presente en la red, valor por omisión para Windows 7.

- Stateful Address Autoconfiguration

Es usado para configurar una dirección “No Link Local” a través del servicio DHCP Valor por omisión para Windows 8.1 y posteriores.

Configuración para PNNC

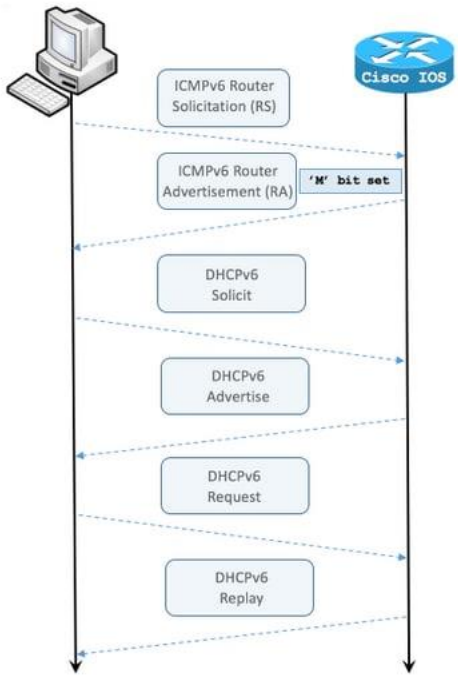
Con la información anteriormente expuesta se define que:

- los hosts con sistemas Windows obtendrán por medio de DHCPv6 la dirección IPv6 y la información de las direcciones de DNS.
- Se debe hacer uso de una configuración “Stateful” debido a que la mayoría de los clientes hace uso de versiones de Windows superiores a la versión 8.1.

DHCPv6 Stateful

Los hosts finales pueden solicitar direcciones IPv6 y parámetros adicionales con el uso de DHCPv6 Stateful. Para esto, el paquete ICMPv6 RA debe tener configurado el indicador de configuración de dirección administrada (“flag” M).

El router establece el indicador “flag” M cuando el comando **ipv6 nd managed-config-flag** está presente en el modo de configuración de la interfaz IOS de Cisco.



Paso 1. El host final envía inicialmente ICMPv6 RS.

Paso 2. El enrutador replica con ICMPv6 RA con el indicador M configurado.

Paso 3. Finalizar el envío de la solicitud DHCPv6 al host.

Paso 4. El enrutador replica la notificación DHCPv6.

Paso 5. El host final envía la solicitud DHCPv6.

Paso 6. El enrutador replica con la respuesta DHCPv6.

Si el “flag” M se establece mediante el comando **“ipv6 nd managed-config-flag”**, entonces un host adjunto puede usar la autoconfiguración con estado para obtener la otra información (DNS, NTP…) independientemente de la configuración del “flag” O "**ipv6 nd other-config-flag**", en otras palabras si el comando **“ipv6 nd managed-config-flag”** se encuentra activo, no es necesario anunciar el “Flag” O con el comando "**ipv6 nd other-config-flag**”.

Para evitar que los hosts finales tomen direcciones IPv6 temporales con el mismo prefijo asignado por el DHCPv6, se hace uso del comando **nd prefix default 1800 1800 no-autoconfig,** el cual les indica a los hosts que deben hacer uso del mismo prefijo asignado a la VLAN y la opción “no-autoconfig” desactiva la asignación de una IPv6 de manera automática**.**

La configuración final quedaría de la siguiente manera (IP’s de ejemplo):

interface Vlan102

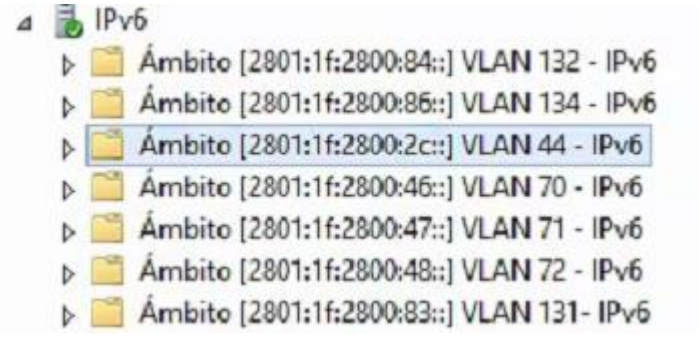
ipv6 enable	→ Se habilita IPv6.
ipv6 address 2001:0DB8:3c:102::1/64	→ Se establece la dirección IPv6.
ipv6 nd prefix default 1800 1800 no-autoconfig	→ Se le indica al host que el prefijo es el mismo de la IPv6 establecido para la VLAN, la opción no-autoconfig desactiva la asignación de una IPv6 automática.
ipv6 nd managed-config-flag	→ Se establece el indicador “flag” M, así se garantiza que el host tome solo la configuración anunciada por el DHCPv6.
ipv6 dhcp relay destination 2001:0DB8:3c:101::10	→ Se le indica al host la IPv6 donde se encuentra el servicio DHCPv6.

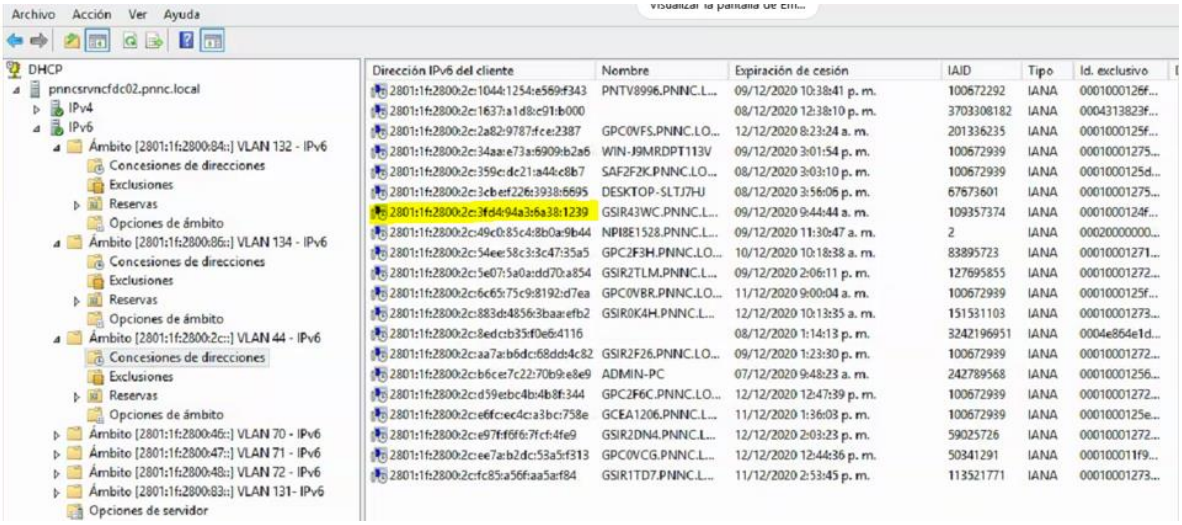
5. RESULTADOS DE LAS PRUEBAS DE VISIBILIDAD Y ALCANZABILIDAD

- Probar el dual stack. Se conectó una PC en la VLAN de prueba y se validó que se le asignó direccionamiento dinámico con IPv4 e IPv6 al mismo tiempo.
- Realizar pruebas de conectividad desde el Switch Core a la PC y viceversa.
- Realizar pruebas de conexión a Internet.
- Analizar de los resultados para identificar las brechas que se pueden presentar al momento del despliegue definitivo.

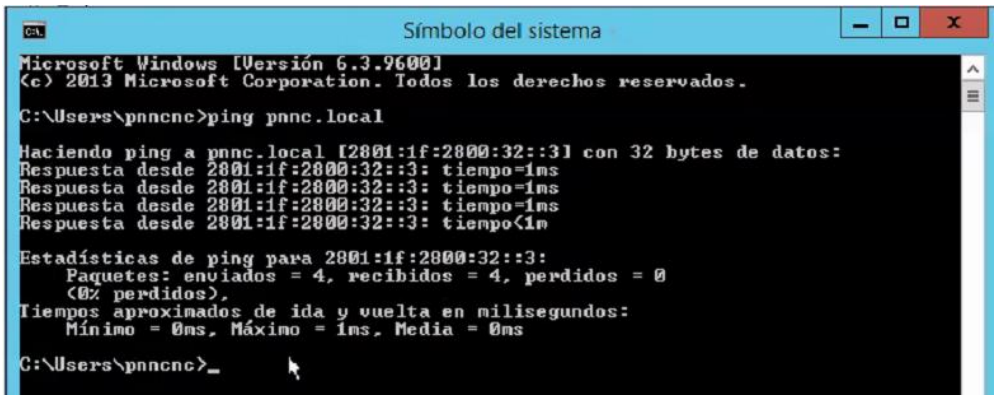
A continuación, se describen las pruebas de visibilidad y alcanzabilidad:

1) Se realizó prueba con una estación de trabajo o PC con IP 192.168.44.1 el cual se encuentra sobre la VLAN 44, este PC ha tomado direcciones IPv4 e IPv6 asignadas por el DHCPv6 del Windows Server de la entidad.

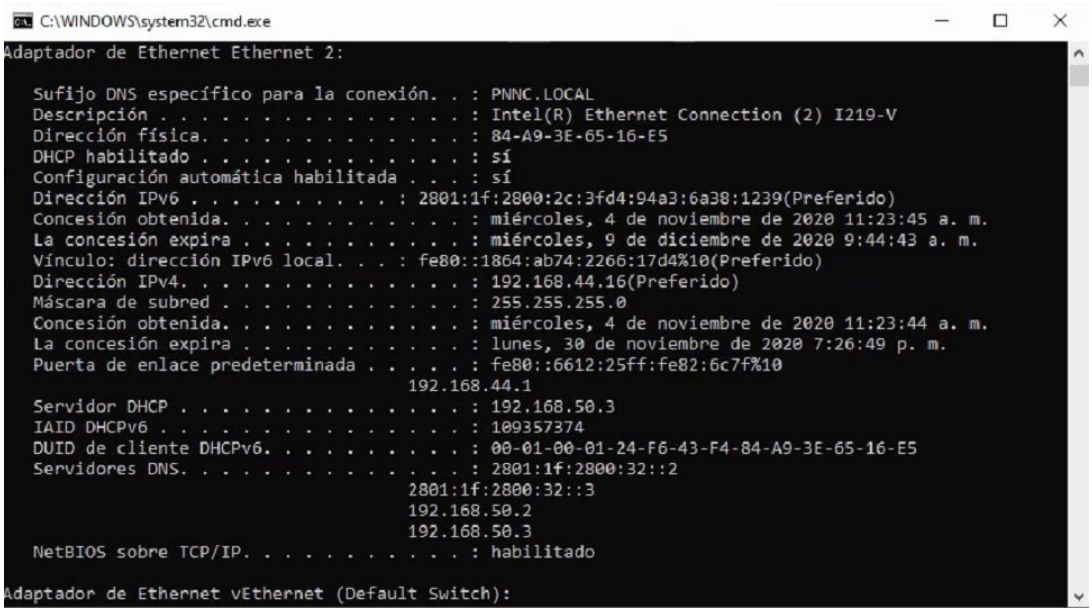




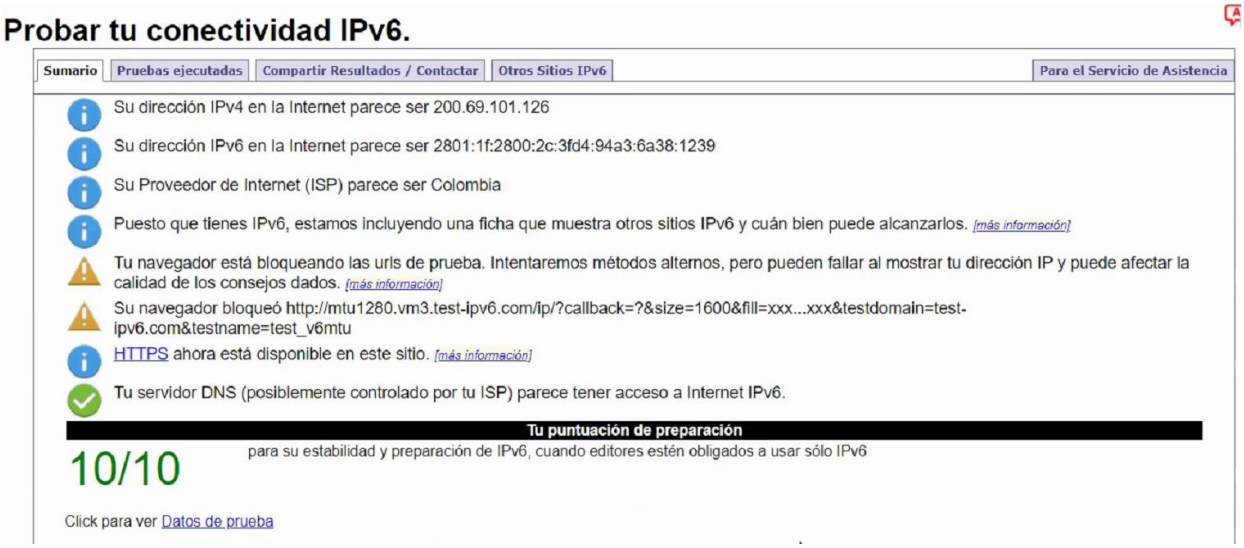
2) Se logró realizar PING desde la estación de trabajo hacia el dominio PNNC, esto permite determinar que el servicio de DNS está funcionando de manera correcta.



3) En la estación de trabajo utilizada, se pudo observar esta información con el comando ipconfig o ipconfig /all



4) La estación de trabajo puede alcanzar internet y navegar haciendo uso del protocolo IPv6 e IPv4



6. CONCLUSIONES

El informe de resultados de pruebas de visibilidad y alcanzabilidad del prefijo IPv6 mostró los pasos que se han llevado a cabo para la planificación del despliegue del protocolo IPv6 en Parques Nacionales Naturales de Colombia. Asimismo, se muestra el resultado de las pruebas de la configuración del protocolo IPv6 en dual stack o doble pila.

Como se ha mencionado en los informes anteriores, despliegue de IPv6 debe realizarse en forma paulatina y planificada. En las VLANs que se encuentran ya creadas, sólo se debe activar el direccionamiento IPv6 tal cual cómo se realizó con la VLAN de prueba.