PROYECTO

IMPLEMENTACIÓN, CAPACITACIÓN Y CONFIGURACIÓN DE LA MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 DE ACUERDO A LOS LINEAMIENTOS DE MINTIC PARA LA ALCALDÍA MUNICIPAL DE CHIA

FASE 2: IMPLEMENTACIÓN DEL PROTOCOLO ipV6

Dirigido a: **ALCALDÍA MUNICIPAL DE CHIA**

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co

IMPLEMENTACIÓN, CAPACITACIÓN Y CONFIGURACIÓN DE LA MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 DE ACUERDO A LOS LINEAMIENTOS DE MINTIC.

Documento	Informe Diagnóstico
Versión	1
Archivo	INFORME_DIAGNOSTICO.doc
Destinatarios	Alcaldía municipal de chia.
Elabora	Cristian Camilo Amézquita Romero Ingeniero OPS
Revisa	Jorge Alberto Rodríguez Profesional Universitario Alcaldía municipal de chia
Aprueba	Jorge Iván Ortiz Ardila Jefe Oficina Tic Alcaldía de Chia.

NOTA DE CONFIDENCIALIDAD

La metodología descrita en este documento es considerada confidencial y es propiedad exclusiva de la ALCANDÍA MUNICIPAL DE CHIA) 2022. Ninguna parte de dicha metodología podrá ser reproducida por alguna otra persona o por cualquier medio sin la previa autorización de la ALCANDÍA MUNICIPAL DE CHIA 2022.

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co

CONTENIDO

1 DESCRIPCIÓN DEL DOCUMENTO

Este documento contiene el inventario realizado a la ALCALDÍA MUNICIPAL DE CHIA frente a la compatibilidad con el protocolo IPv6 teniendo como base la información suministrada por la entidad.

Este documento incluye:

- ✓ Plan detallado de implementación
- ✓ Configuraciones y diagramas de IPv6.
- ✓ Plan de diagnóstico.
- ✓ Pruebas realizadas y resultados bajo IPv6.
- ✓ Configuraciones y diagramas de IPv6.
- ✓ Componentes tecnológicos no migrados.
- ✓ Inventario final IPv6.
- ✓ Recomendaciones y casos fallidos

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co

2 DEFINICIONES

Con el objetivo de dar mayor contexto del documento se presentan las siguientes definiciones:

SIP: es un protocolo de señalización utilizado para establecer una “sesión” entre 2 o más participantes, utilizado para telefonía IP.

IPv4: El Protocolo de Internet versión 4 en inglés, Internet Protocol versión 4 (IPv4), protocolo de interconexión de redes basados en Internet, y fue la primera versión implementada para la producción de ARPANET.

IPv6: El Protocolo de Internet versión 6, en inglés, Internet Protocol versión 6 (IPv6), es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol versión 4 (IPv4) RFC 791

DHCP: Protocolo de configuración de host dinámico, es un protocolo de red utilizado en redes IP que se encarga de asignar direccionamiento IP a dispositivos de red.

NAT: es un mecanismo utilizado por Routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.

Dual Stack: El Dual Stack o pila doble permite desplegar las dos versiones del protocolo IP de manera simultánea en toda la red, se determinará de manera automática cuando se deberá usar IPv4 y cuando se deberá usar IPv6 de esta manera habrá inter-operatividad entre todos los equipos independiente de la versión del protocolo los mismos estén usando.

3 PLAN DETALLADO IMPLEMENTACIÓN

Con el objeto de proponer a la entidad el cumplimento de adopción bajo IPv6 en su red datos se debe mencionar que la metodología propuesta y en concordancia con los lineamientos definidos por MinTic (Ministerio de Tecnologías de la Información y Comunicaciones), el mecanismo de transición recomendado para la Alcaldía Municipal De Chía, es doble pila (Dual Stack), debido a que este modelo provee las coexistencia de IPv4/IPv6 y para la desactivación controlada del protocolo IPv4.

3.1 OBJETIVO GENERAL

Elaborar un plan estratégico para la transición de IPv6 en la red de datos de Alcaldía Municipal De Chía, con el fin de preparar el proceso de adopción del nuevo protocolo IPv6.

3.2 OBJETIVOS ESPECÍFICOS

- ✓ Identificar la topología actual de red y funcionamiento dentro de la entidad.
- ✓ Proponer un plan que permita la coexistencia de los dos protocolos (IPv4/IPv6).
- ✓ Conocer el inventario actual TI, con el fin de incluir todos los elementos de red para que estos estén incluidos en el plan estratégico de migración a IPv6.
- ✓ Desarrollar las actividades que conforman cada una de las fases que hacen parte de plan estratégico para la adopción IPv6.

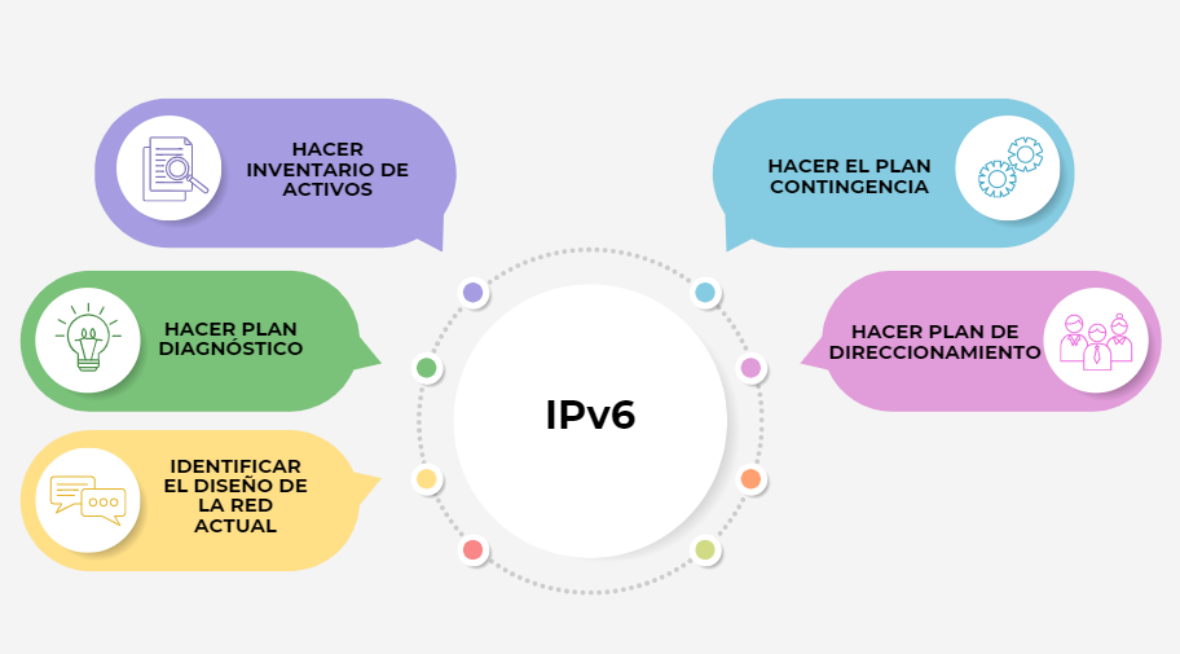
3.3 ALCANCE

El plan estratégico consiste en realizar un análisis de la plataforma tecnológica en la infraestructura de red con el fin de ir identificando todos los elementos de red que pueden introducir la funcionalidad de IPv6 en sus plataformas, también cabe resaltar que el plan está sujeto a una constante mejora a medida del avance en las diferentes etapas del desarrollo, su alcance es poder llevar a cabo una migración controlada en la medida que se vaya activando IPv6, esto con la finalidad de generar el menor riesgo posible de perdida de servicios existentes o algún comportamiento inesperado frente a su activación.

3.3 FASES DEL PLAN ESTRATÉGICO DE MIGRACIÓN

En este punto se define el desarrollo mínimo que debe contener cada una de las actividades que conforman las fases para la adopción de IPv6.

En la siguiente imagen se puede observar de acuerdo a los lineamientos del MinTic, las fases que debe contener un plan estratégico para la migración de IPv6



1. **Hacer el inventario de activos**: en esta actividad se requiere desarrollar y mantener el inventario de hardware y software, identificando claramente cuales equipos soportan el protocolo IPV6, cuales se deben actualizar y cuales no soportan el nuevo protocolo, dejando escrito el soporte al momento de adoptar hacia IPV6.
2. **Hacer el plan de diagnóstico**: Es de suma importancia documentar el plan de diagnóstico de la infraestructura de TI del protocolo IPV4 a IPV6.
3. **Identificar el diseño de la red actual**: realizar la documentación detallada de la red, en el cual se requiere identificar lo siguiente.

✓ Topología actual y su funcionamiento dentro de la Alcaldía Municipal De Cajicá y diseñar futura red sobre IPV6.

✓ Planear el proceso de transición de los siguientes servicios tecnológicos: Servicio DNS, Servicio de Asignación Dinámica de Direcciones IP (DHCP),

Directorio Activo, Servicios WEB, Servidores de Monitoreo, Validación del Servicio de Correo Electrónico,

- ✓ Validación del Servicio de la Central Telefónica, Servicio de Backups, Servicio de Comunicaciones Unificadas e Integración y servicio en la nube. Validar el estado actual de los sistemas de información, comunicación, almacenamiento y evaluar la interacción entre ellos.
- ✓ Identificar la configuración y los esquemas de seguridad de la red de comunicaciones y sistemas de información en compatibilidad con los dos protocolos.

4. **Hacer plan de direccionamiento IPV6:** Elaborar en detalle el proceso de segmentación entre los distintos dispositivos y servicios de la red, teniendo en cuenta los esquemas de enrutamiento ya sea por ejemplo en /64, /56, /48, /44, según sea el caso y la necesidad de cada red, dicho cambio nos daría una mayor facilidad y orden en la asignación de la IP a cada equipo de cómputo o dispositivo, ya que la IPV6 maneja un direccionamiento de 128 Bits contra un paquete de direccionamiento 32 bits para la IPV4, es decir pasaríamos de una notación numérica con punto decimal a una notación hexadecimal alfanumérica.

3.4 BENEFICIOS DE DESARROLLO PLAN ESTRATÉGICO

Algunos de los puntos beneficios importantes en el desarrollo de un buen plan estratégico de migración son:

- ✓ La posibilidad de tener un mayor número de equipos conectados a la red de las entidades públicas al ser implementado esta solución frente a la escasez de direcciones IPv4.
- ✓ Incrementar la movilidad de los usuarios al tener mayor número de IP para conectividad de dispositivos.

- ✓ Gran número de direcciones IP para conexiones a Internet con el mundo exterior, facilitando el crecimiento de nuevas tecnologías como el internet de las cosas, las ciudades inteligentes, redes de sensores, entre otras.
- ✓ Proteger la infraestructura tecnológica de la entidad.

Al realizar el proceso de migración se debe garantizar la compatibilidad de los dos ecosistemas sin perjudicar el funcionamiento de cualquier elemento que soporte IP o tener que incurrir en compra de renovación tecnológica que pueda dar cumplimiento al lineamiento del MinTic.

3.5 PLAN DE SENSIBILIZACIÓN

Dentro del marco de un plan estratégico para la transición de IPv6 es importante formular un plan que con lleve a todos los colaboradores de la organización a sensibilizarlos y divulgarles del porque la importancia de migrar al protocolo IPv6, es por esto por lo que en este capítulo se presente un plan a todo el personal de la Alcaldía Municipal De Chía, este incluye.

- ✓ Sensibilización funcional.
- ✓ Sensibilización técnica.
- ✓ Cronograma de sensibilización.
- ✓ Puntos importantes.

3.5.1 SENSIBILIZACIÓN FUNCIONAL

DIRIGIDO A: Personal no técnico de la entidad.
OBJETIVO: Brindar un entendimiento general del proyecto enfocado en los aspectos culturales, funcionales y beneficios de la implementación y transición al protocolo IPv6.
DESCRIPCIÓN: Se plantea realizar sesiones grupales presenciales o virtuales, estas sesiones serán realizadas en los puestos de trabajo del personal de la entidad en grupos de entre 10 y 15 personas y en donde se tratarán los siguientes temas

TEMÁTICA:
¿Qué es el protocolo IPv6? Entender que es el protocolo IP, como es usado en el día a día y porque existe.
¿Por qué realizar la transición al protocolo IPv6? Entender cómo surgió el protocolo, las razones de su creación y por qué se debe realizar la transición.
¿Beneficios de la transición? Dar a conocer los beneficios de la transición a corto y lejano plazo.
¿Cómo la entidad está realizando la transición? Dar a conocer el alcance del proyecto, su impacto y como este beneficiara a la entidad.
METODOLOGÍA: Estos conceptos serán desarrollados en una forma amigable para los funcionarios de la entidad teniendo en cuenta que se trata de un público que no pertenece a las áreas de tecnología, buscando su motivación en el tema y un entendimiento general de los aspectos funcionales del protocolo IPv6.
Estas sesiones serán llevadas a cabo por personal de la oficina Tic de Alcaldía Municipal De Chía, se realizará un recorrido por la entidad con el fin de llegar a los puestos de trabajo del personal y realizar las sesiones con los grupos de cada área, al final de cada capacitación se diligenciarán los siguientes documentos:

- ✓ Listado de asistencia por el personal que impartió y que participó en la jornada de sensibilización y socialización.
- ✓ Encuesta de satisfacción para cada persona que participó en la jornada de sensibilización y socialización.

DURACIÓN: Se plantea que cada sesión tenga una duración aproximada de 60 minutos y 30 minutos de sesión para preguntas y respuestas. Las jornadas de sensibilización y socialización se realizarán durante una semana con el fin de llegar a todas las personas de la entidad.
SENSIBILIZACIÓN PREVIA: Se plantea en conjunto con la entidad, desarrollar píldoras informativas las cuales serán enviadas una (1) semana antes por correo electrónico a todo el personal de Alcaldía Municipal De Chía, con el fin de informarlos sobre el proyecto y la sensibilización que se va a realizar.

3.5.2 SENSIBILIZACIÓN TÉCNICA

DIRIGIDO A: Personal técnico de la entidad.
OBJETIVO: Brindar un conocimiento técnico sobre el protocolo IPv6, funcionamiento, requerimientos para la transición y configuraciones aplicadas a la infraestructura tecnológica de Alcaldía Municipal De Chía,
DESCRIPCIÓN: Se plantea realizar sesiones presenciales o virtuales de forma personalizada en la entidad con un contenido especifico dependiendo de la especialidad

del personal, esta sensibilización se plantea hacer solo para el equipo de TICs de la entidad la cual está constituida por los siguientes grupos.

GRUPO ADMINISTRADORES DE RED.

Enfocada en direccionamiento IP, rutas, configuraciones realizadas en switches y dispositivos de seguridad. Dirigida a personal administrador de la plataforma de red, y Firewall.

GRUPO ADMINISTRADORES DE SISTEMAS DE INFORMACIÓN.

Enfocada en los cambios aplicados a las bases de datos, servidores de aplicaciones y requerimientos para transición. Dirigida a personal a cargo del manejo y administración de los sistemas de información en la entidad.

GRUPO ADMINISTRADORES DE INFRAESTRUCTURA.

Enfocada en los servicios de DHCP, DNS, AD y la plataforma de virtualización en la que se encuentran la mayoría de los servidores. Dirigida al personal encargado de la infraestructura de Datacenter y los administradores de la plataforma de servidores.

TEMÁTICAS

-GRUPO INFRAESTRUCTURA DE RED.

- Generalidades del protocolo IPV6.
- Método dual-stack.
- Segmentación de red en IPv6.
- Enrutamiento, NDP, rutas.
- Configuraciones aplicadas a equipos de red. (Switches, Firewalls).

-

GRUPO SISTEMAS DE INFORMACIÓN

- Generalidades del protocolo IPV6.
- Método dual-stack.
- Requerimientos de sistemas de información para migración a IPv6.
- Configuraciones aplicadas a sistemas de información.
- Configuraciones aplicadas a bases de datos.

-**GRUPO SERVICIOS DE RED Y SERVIDORES**

- Generalidades del protocolo IPV6.
- Método dual-stack.
- DHCP y DNS en IPv6.
- Configuraciones aplicadas a servicios de red (DNS, DHCP, AD).
- Configuraciones aplicadas a plataforma de virtualización.

METODOLOGÍA:

Estos conceptos serán desarrollados en sesiones personalizadas con cada grupo de especialidad en donde se abordarán los temas de dos formas:

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co

PRESENTACIÓN.
CAPTURAS DE PANTALLA.
Por medio de capturas de pantalla se reforzará la explicación teórica explicando las configuraciones realizadas en dichos equipos.
Estas sesiones serán llevadas a cabo por personal de la oficina Tic de la Alcaldía Municipal De Chía, al final de cada capacitación se diligenciarán los siguientes documentos:

- ✓ Listado de asistencia. Por el personal que impartió y que tomo la capacitación.
- ✓ Encuesta de satisfacción. Por el personal que tomo la capacitación.
- ✓ Evaluación. Sobre los conceptos teóricos explicados durante la capacitación.

DURACIÓN:
Se plantea que se tome seis (4) horas en 2 sesiones para el grupo de Tics y de manera paralela se puedan hacer preguntas y respuestas durante estos espacios.

3.5.3 CRONOGRAMA

A continuación, se muestra el cronograma planteado para la sensibilización en la entidad:

NOMBRE DE LA TAREA	DURACIÓN	COMIENZO	FIN	HORA
SENSIBILIZACIÓN	**3 días**	Por definir	Por definir	Por definir
SENSIBILIZACIÓN FUNCIONAL	**1 días**	Por definir	Por definir	Por definir
Grupo general de la entidad - Sesión 1	5 hora	Por definir	Por definir	Por definir
SENSIBILIZACIÓN TÉCNICA	**2días**	Por definir	Por definir	Por definir
Grupo TICs - Chía	2 horas	Por definir	Por definir	Por definir
Grupo TICs - Chía	2 horas	Por definir	Por definir	Por definir

3.5.4 PUNTOS IMPORTANTES

- ✓ Las actividades de sensibilización se planean realizar entre las 8:30 a.m., de cada día y finalizar a más tardar a las 5:30 p.m.
- ✓ Se plantea realizar la sensibilización técnica finalizando cada fase del proceso dado que se requiere que la entidad este alineada a la adopción de IPv6 que viene adelantando la entidad.

3.6 PLAN DE DIRECCIONAMIENTO

Este capítulo incluye el plan de direccionamiento a borrador el cual fue presentado a LACNIC con la finalidad de obtener el recurso IP para poder desarrollar todo el proyecto

3.6.1 DEFINICIONES

PREFIJO: Numero de bits contados de izquierda a derecha de una dirección IPv6, equivalente a la porción de red de una dirección IPv4.

IID: Interface ID o identificador de interface equivalente a la porción de Host de una dirección IPv4.

RIR: Registro Regional de Internet, es una organización que supervisa la asignación y registro de recursos de internet en una región especifica.

LACNIC: Latín América and Caribeña Network Information Centre, es el registro regional de internet para la zona de Latino América y el Caribe.

NIBBLE: Digito hexadecimal (0-F) de 4 bits de una dirección IPv6.

SEGMENTO: Porción de 16 bits de una dirección IPv6 compuesta por 4 nibbles, cada uno de los segmentos debe estar delimitado por ¨:¨ los valores de cada segmento oscilan entre :0000: y: FFFF:

SLAAC: Stateless Address Autoconfiguration, Auto configuración de direcciones IPV6 sin estado.

DHCPv6: Dinamic Host Configuration Protocol, protocolo de configuración dinámica de direcciones IPv6.

3.6.2 ESTRATEGIA DE SEGMENTACIÓN

Verificando las necesidades actuales de la entidad y basándonos en la cantidad de sedes y redes actuales en IPv4, se estima que se requiere un pool de direccionamiento **IPv6 con prefijo /48**.

A continuación, se muestra una propuesta del plan de direccionamiento para el Pool /44

	16 REDES /48 ***SEDE PRINCIPAL / SEDES REMOTAS***	**16 REDES /52** ***DIVISIÓN POR ZONAS***	**16 REDES /56** ***DIVISIÓN POR DISPOSITIVOS O SUBZONAS***	**256 REDES /64** ***DISTRIBUCIÓN DE VLANS FINALES***
280X:XXXX::/48 **POOL IPV6 CHÍA**	2801:XXXX::/48 SEDE PRINCIPAL	2801:XXXX::/52 ZONA LAN	280X:XXXX::/56 REDES CABLEADAS	VLANS FINALES **VID 10:** 280X:XXXX:0:10::/64 **VID 20:** 280X:XXXX:0:20::/64 ……
			2801:XXXX:0:100::/56 REDES WIRELESS	Segmentos Finales **SSID_1:** 2801:XXXX:0:100::/64 **SSID_2:** 2801:XXXX:0:101::/64 **SSID_3:** 2801:XXXX:0:102::/64 **SSID_4**: 2801:XXXX:0:103::/64 **SSID_5:** 2801:XXXX:0:104::/64 ……
			280X:XXXX:0:200::/56 REDES SEGURIDAD	Segmentos Finales 280X:XXXX:0:200::/64 DDOS: 280X:XXXX:0:201::/64 ……
			280X:XXXX:0:300::/56 RESERVA	Segmentos Finales 280X:XXXX:0:300::/64 ……

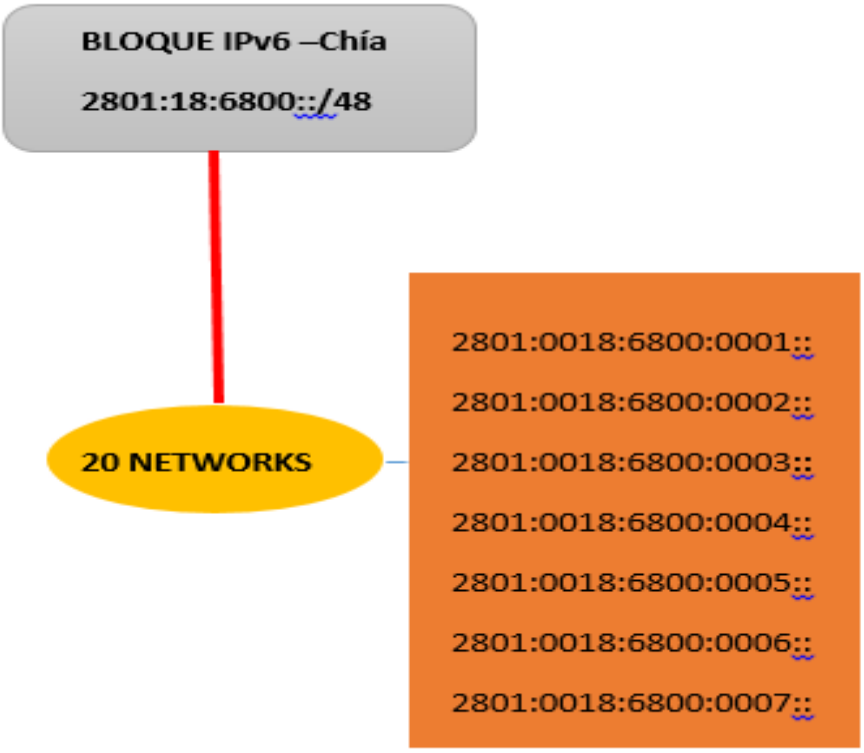
		280X:XXXX:0:1000::/52 ZONA WAN	280X:XXXX:0:1000::/56 CANALES	**Segmentos Finales** **280X:XXXX:0:1000::/64** 280X:XXXX:0:1001::/64 ……
			280X:XXXX:0:1100::/56 RESERVA	VLANS FINALES 280X:XXXX:0:1100::/64 280X:XXXX:0:1101::/64 280X:XXXX:0:1102::/64 280X:XXXX:0:1103::/64 ……
	280X:XXXX:1::/48 SEDE FUTURA A			
	280X:XXXX:2::/48 SEDE FUTURA B			
	280X:XXXX:3::/48…. SEDE FUTURA C			
	280X:XXXX:F::/48 SEDE FUTURA			

Para el desarrollo del plan de direccionamiento se tuvo en cuenta las necesidades actuales que tiene la entidad y para poder cubrirlas se realizó de la siguiente manera:

Se tomó un bloque /44 este podrá ser subdividido en 16 redes /48 asumiendo que la entidad actualmente tiene en promedio 15 sedes cubriría la necesidad actual y cada una de estas tiene su propio enlace a internet, todas las sedes, convergen a la sede principal para la salida a internet y consumo de recursos local, el ISP que les permite la salida a internet y conectividad MPLS es TIGO para toda la red de datos de Alcaldía Municipal De Chía,
En la siguiente imagen se muestra una ilustración con el bloque de direcciones entregado por Lacnic y se puede ilustrar visualmente como se desprenden cada una de las subredes.

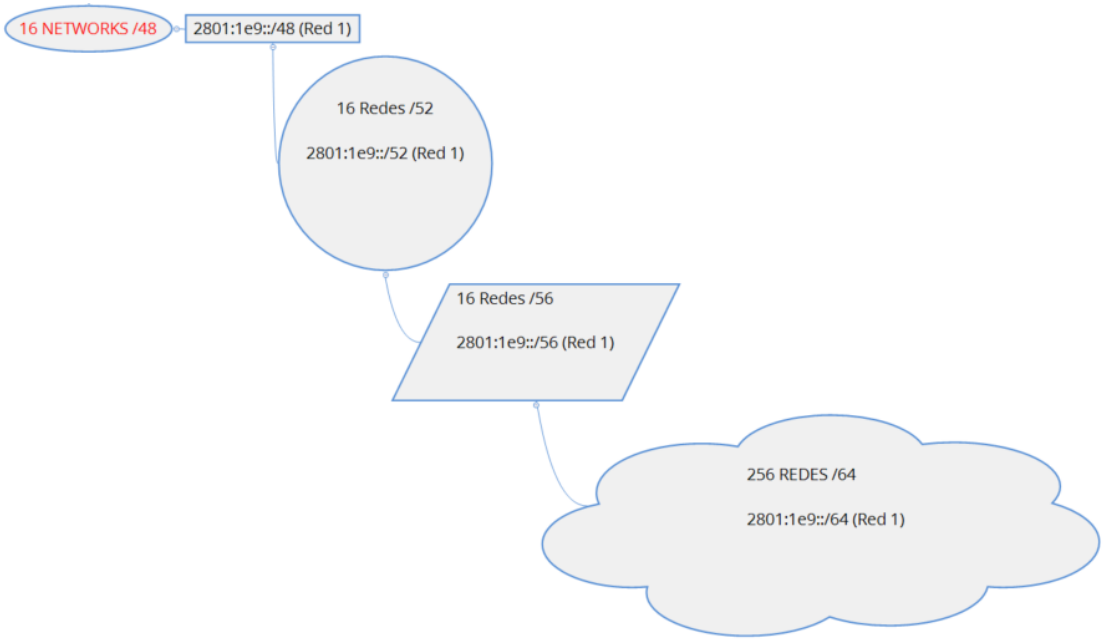
Por otra parte, se debe mencionar que cada /48 será utilizado para cada una de las sedes actuales y futuras recordando que el ISP solo puede publicar un /48 menor o igual a un bloqué 48 para la salida a internet, se debe mencionar que la administración y supervisión del recurso IP será supervisado desde la sede principal de la Alcaldía Municipal De Chía.
De acuerdo a la estrategia del plan de direccionamiento se toma una de las redes /48 y esta a su vez se puede subdividir en /52 dieciséis (16 redes), prefijo/52, en la siguiente imagen se puede dar un bosquejo de cómo quedaría.

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co



Como se observa en la imagen anterior los bloques con (/64), se dispondrán para cada zona por ejemplo zona WAN, zona LAN, zona perimetral de seguridad.
Dando continuidad se explica que ya teniendo las definiciones previas de que se puede obtener de cada red /64 dieciséis (20), redes, se sigue realizando la segmentación para las redes que conformara cada una de las zonas de manera que de cada /52 se puede dividir en 16 subredes /56, en el siguiente grafico sedara un representación de ejemplo de cómo quedaría.
Por último, se menciona que las redes finales tendrán un prefijo /64 este se obtendrá de tomar la primera dirección de red /56 obteniendo la 256 redes por cada dirección de red /56 que tome en la siguiente grafica se puede ilustrar como seria.
De acuerdo al grafico anterior de plan de direccionamiento podemos obtener de cada Subred /64 la cantidad de 18,446,744,073,709,551,616 direcciones de host utilizables obteniendo de que por la primera red 2801:0018:: /64 para nuestro ejemplo la primera dirección de host disponible y la 2801:1E9::ffff:ffff:ffff:ffff, ultima dirección de host disponible.

El siguiente bosquejo mostraría un resumen de cómo sería el plan de direccionamiento



3.7 PLAN DE DIAGNÓSTICO

Con respecto al plan de diagnóstico se deben evaluar los diferentes puntos que se mencionan a continuación con la finalidad de cumplir con los requisitos mínimos de IPv6 al tipo de activo y su funcionalidad. Estos puntos son:

- ✓ Recolección de inventario TI.
- ✓ Determinación de la compatibilidad de IPv6 del inventario obtenido.
- ✓ Los requerimientos mínimos para el cumplimento de IPv6 es decir RFCs para cada activo de información.

3.7.1 COMPATIBILIDAD -NIVELES MÍNIMOS PARA LOS ACTIVOS TI

La compatibilidad de los activos de TI se define de acuerdo con los requisitos mínimos de IPv6 frente al tipo de activo y su funcionalidad. Esto dado que un equipo servidor que tiene direcciones IP estáticas y no requiere realizar ninguna acción adicional a recibir y enviar tráfico IPv6, podría tener la configuración básica de IPv6, y funcionar adecuadamente. Sin embargo, un enrutador, el cual, si requiere recibir y reenviar paquetes, descubrir equipos y manejar otro tipo de funcionalidades, requeriría implementar un RFC como el de routing IPv6, SLAAC, u otros acordes con su función. De acuerdo con lo anterior, se presenta la siguiente tabla, la cual incluye por tipo de activo el requerimiento mínimo de RFC que debería cumplir.

TIPO DE DISPOSITIVO. INVENTARIO DE ACTIVOS DE TI	RFC MÍNIMO	FUNCIÓN DEL EQUIPO	FORMA DE VALIDAR LA COMPATIBILIDAD
Computadores de Escritorio y Portátiles Servidor de Almacenamiento Servidor Físico Servidor Virtual Impresoras	**RFC de Nodo/Host** - [RFC2460] IPv6 Protocol - [RFC 2460] Packet transmisión rules. - [RFC4861] Neighbor Discovery - [RFC4443] ICMPv6	**Nodo/Host IPv6:** Activo que implementa IPv6 y que no es un enrutador.	**Marca y Modelo** Revisión de fichas técnicas, manual de configuración o antigüedad de la Marca y Modelo de los activos de TI.

TIPO DE DISPOSITIVO. INVENTARIO DE ACTIVOS DE TI	RFC MÍNIMO	FUNCIÓN DEL EQUIPO	FORMA DE VALIDAR LA COMPATIBILIDAD
	- [RFC4291] IPv6 Addressing Architecture - [RFC4862] IPv6 Stateless Address Autoconfiguration - [RFC 4862] Duplicate Address Detection. Quoting from Section 5.4. - [RFC3484] Default Address Selection for IPv6. - [RFC3315] DHCPv6 - [RFC1034], [RFC1035], [RFC3363], [RFC3596] DNS. - [RFC4213] Dual Stack		

TIPO DE DISPOSITIVO. INVENTARIO DE ACTIVOS DE TI	RFC MÍNIMO	FUNCIÓN DEL EQUIPO	FORMA DE VALIDAR LA COMPATIBILIDAD
DVR (Digital Video Recorder) NVR (Network Video Recorder) Cámara de Video	**RFC de Nodo/Host** - - [RFC2460] IPv6 Protocol - [RFC 2460] Packet transmisión rules. - [RFC4861] Neighbor Discovery	**Nodo/Host IPv6:** Activo que implementa IPv6 y que no es un enrutador.	**Marca y Modelo** Revisión de fichas técnicas, manual de configuración o antigüedad de la Marca y Modelo de los activos de TI.

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co

TIPO DE DISPOSITIVO. INVENTARIO DE ACTIVOS DE TI	RFC MÍNIMO	FUNCIÓN DEL EQUIPO	FORMA DE VALIDAR LA COMPATIBILIDAD
UPS (Uninterruptible Power Suppy	- [RFC4443] ICMPv6 - [RFC4291] IPv6 Addressing Architecture - [RFC4862] IPv6 Stateless Address Autoconfiguration - [RFC 4862] Duplicate Address Detection. Quoting from Section 5.4. - [RFC1034], [RFC1035], [RFC3363], [RFC3596] DNS		

OTROS TIPOS DE ACTIVOS DE TI QUE APLICAN AL			
Sistemas operativos	Todos los RFC de Nodo/Host [RFC2460] IPv6 Protocol - [RFC 2460] Packet transmisión rules. - [RFC4861] Neighbor Discovery - [RFC4443] ICMPv6 - [RFC4291] IPv6 Addressing Architecture - [RFC4862] IPv6 Stateless Address Autoconfiguration - [RFC 4862] Duplicate Address Detection.	Sistema Operativo que se comporta como Nodo/Host IPv6	Validación del sistema operativo según su antigüedad. Por ejemplo, versiones de Microsoft Windows desde Windows XP tiene la funcionalidad de IPv6

	Quoting from Section 5.4. - [RFC3484] - [RFC3315] DHCPv6 - [RFC1034], [RFC1035], [RFC3363], [RFC3596] DNS. - [RFC4213] Dual Stack		
APIs	- [RFC3493] Basic Socket Interface Extensions for IPv6" [RFC5014] "IPv6 Socket API for Source Address Selection"	**Nodo/Host IPv6:** Activo que implementa IPv6 y que no es un enrutador.	Validación de Sistema Operativo, Manejo de direcciones IP, Métodos de Interacción con otros sistemas, versión del motor de base de datos, versión del servidor web, adquisición de certificados digitales y lenguaje de desarrollo.

3.7.2 GENERALIDADES DE LOS SISTEMAS DE INFORMACIÓN.

El desarrollo del plan de análisis descrito en la presente sección del documento se realiza teniendo en cuenta las siguientes variables de enfoque, con el fin de evaluar de una forma detallada la compatibilidad del inventario de aplicaciones en la implementación de IPv6:

- ✓ Sistema operativo y versión de sistema operativo.
- ✓ Lenguaje de programación y versión del lenguaje de programación.
- ✓ Motor de base de datos y versión del motor de base de datos.
- ✓ Servidor de aplicaciones, junto con su versión.
- ✓ Cadena de conexión a base de datos.
- ✓ Tipo de asignación IPv6.

Esta clasificación construida dentro del análisis busca apoyar al lector en el desarrollo del diagnóstico final para la implementación de IPv6, con el fin de identificar los sistemas o aplicaciones que requieran configuraciones o atenciones especiales en el momento de la implementación.

3.8 PLAN TÉCNICO OPERATIVO DE LA TRANSICIÓN IPV6

Para la elaboración de un plan técnico operativo con la finalidad de realizar la activación de IPv6 se deberé tener la preparación que contemple todos los aspectos técnicos operativos necesarios para realizar su despliegue., la estrategia que se comparte a continuación incluye realizar esta transición a través de capas de acuerdo a la siguiente imagen.

Para efectuar la implementación se deben realizar las siguientes actividades y en el siguiente orden especifico. Lo anterior basado en los resultados del Análisis de la

información de activos de TI recopilada. La priorización para la implementación se define de acuerdo con los siguientes parámetros:

- ✓ Prioridad a los servicios con criticidad Alta, Media y Baja.
- ✓ Orden de implementación por Capa

3.8.1 PREPARACIÓN Y REVISIÓN DE SERVICIOS DE RED.

3.8.1.1 REVISIÓN DEL SERVIDOR DNS Y SERVIDOR DHCP

Para una apropiada adopción del protocolo IPv6, es recomendable hacer una revisión sobre el servidor de DNS consistente en:

- ✓ Verificación de correspondencia de nombres con direcciones IPv4.
- ✓ Eliminación de registros DNS duplicados y obsoletos.
- ✓ Creación de objetos DNS que no estén registrados o que tengan problemas de registro DNS.

Así mismo, teniendo en cuenta que se tendrá una coexistencia entre dos protocolos, es necesario hacer la revisión del servidor de asignación automática de direcciones IPv4 (servidor DHCP), en los siguientes aspectos.

- ✓ Verificación de los registros de direcciones IPv4 duplicados.
- ✓ Verificación de registros de direcciones IPv4 obsoletos.
- ✓ Eliminación de registros no coherentes.
- ✓ Verificación de asignación correcta de los hosts en sus VLAN correspondientes.
- ✓ Revisión de las asignaciones estáticas.

3.8.1.2 PREPARACIÓN DE LOS DISPOSITIVOS DE CONEXIÓN A INTERNET

La preparación de los dispositivos requiere tener presente varias de las consideraciones expuestas hasta ese momento, estas son:

- ✓ Haber adquirido un direccionamiento IP global.
- ✓ Contemplar el mecanismo de transición seleccionado.
- ✓ Haber definido el plan de direccionamiento IPv6.

Contemplar que en este momento la mayoría de los sitios de internet en América Latina aún se comunican con direccionamiento IPv4, por lo tanto, es necesario mantener activo el protocolo IPv4.

3.8.1.3 PREPARACIÓN DE LOS DISPOSITIVOS DE SEGURIDAD FIREWALL

Para este capítulo se deberán tener en cuenta las siguientes consideraciones:

ALISTAMIENTO PREVIO

- ✓ -Realizar backup de todos los dispositivos antes de cualquier cambio en la infraestructura.
- ✓ Validar previamente logs, alarmas, consumo de memoria en los dispositivos para asegurar que los equipos estén en un estado óptimo antes de cualquier cambio.
- ✓ En lo posible tener los equipos actualizados para evitar bugs el sistema.
- ✓ Bloque de direccionamiento IPV6 asignado y publicado por el ISP.

El proceso de transición se debe llevar a cabo en el siguiente orden con el fin de generar el menor impacto en la red.

- ✓ **Activación de protocolo IPV6** en los firewalls. Se debe realizar la activación del protocolo en cada firewall con el fin de habilitar los comandos de IPV6 en las consolas.
- ✓ **Configuración de interfaces en dual stack con protocolo IPV6.** de acuerdo con el plan de direccionamiento y segmentación se deben habilitar las interfaces con su respectiva dirección IPV6.
- ✓ **Configuración de rutas.** De acuerdo con el plan de direccionamiento se deben crear las rutas en IPV6 correspondientes.
- ✓ **Pruebas de conectividad**. Realizar pruebas a otros dispositivos habilitados en IPV6 con el fin de validar que los pasos anteriores se hayan ejecutado de forma correcta, adicional, realizar pruebas de conectividad a internet, estas pruebas se realizarán desde las consolas de cada dispositivo.
- ✓ **Creación de objetos.** Se deberá duplicar los objetos que estén creados en IPV4 a IPV6 con la segmentación correspondiente al plan de direccionamiento.
- ✓ **Configuración de políticas de seguridad**. Realizar la configuración de las políticas para IPV6 (Equivalentes a las políticas existentes en IPV4) de los servicios que se vayan a migrar. Estas políticas se deben realizar en todas las zonas de seguridad.
- ✓ **Configuración de políticas de NAT**. Realizar la configuración de las políticas de NAT para los servicios que se encuentren publicados en IPV4 y que se contemplen migrar a IPV6.
- ✓ **Pruebas de conectividad desde redes externas**. Realizar pruebas desde internet de conectividad a los servicios internos que se encuentren operando.

- ✓ **Configuración de otros servicios**. De acuerdo con el plan de diagnóstico se deben habilitar en IPV6 los servicios que sean 100% compatibles con el protocolo IPV6 y que estén corriendo en el Firewall actualmente en IPV4 (Ejemplo. NTP, SNMP, DNS, VPNs etc.).
- ✓ **Pruebas de configuraciones.** Realizar pruebas de los servicios activados.
- ✓ **Backup.** Realizar backup de las configuraciones realizadas.

3.8.1.4 PREPARACIÓN DEL SERVIDOR DE DIRECCIONAMIENTO DHCP IPV6

Para la preparación del servidor de direccionamiento IPv6 (DHCP IPv6) se deben tener en cuenta las siguientes consideraciones.

- ✓ Haber definido un plan de direccionamiento IPv6 acorde con la topología de red de la entidad y necesidades de la entidad.
- ✓ Depurar previamente Políticas y configuraciones heredadas en IPv4 que no se estén usando.
- ✓ Activar las características IPv6 en el servidor que maneja DHCP.
- ✓ Asignar una dirección IPv6 estática, acorde con el plan de direccionamiento IPv6.
- ✓ Crear un entorno de pruebas para validar la correcta asignación de direcciones IPv6. Si las pruebas son satisfactorias crear los ámbitos necesarios de acuerdo con su topología y su plan de direccionamiento.
- ✓ Mantener un plan de direccionamiento que permita mantener su equivalencia de IPv4 a IPv6.

3.8.1.5 PREPARACIÓN DE ESTACIONES FINALES- USUARIOS.

Para este capítulo se deberán tener en cuenta las siguientes consideraciones:

ALISTAMIENTO PREVIO

- ✓ Tener previamente configurados todos los servicios en IPv6 que van a operar en dual Stack.
- ✓ Tener previamente ejecutado el plan piloto de pruebas.
- ✓ Validar los segmentos a asignar en IPV6 para los equipos de red antes de realizar cualquier configuración.

- ✓ Validar que la información de segmentación, inventarios y demás esté actualizada al momento de iniciar el proceso de implementación, de no ser así realizar las respectivas actualizaciones a los documentos.

El proceso de transición se debe llevar a cabo en el siguiente orden con el fin de generar el menor impacto en la red:
1. **Activación de protocolo IPV6 en los sistemas operativos**. Se debe realizar la activación del protocolo en las tarjetas de red de cada máquina, por default vienen habilitados.
2. **Configuración de IPs estáticas**. De acuerdo al plan de direccionamiento y segmentación habilitar una cantidad pequeña de estaciones por vlan con IPs estáticas en IPv6.
3. **Pruebas de funcionamiento**. Realizar validación de correcta operación con los servicios habilitados en IPv6 y con los servicios que operan en IPv4. Si hay algún problema con algún servicio se deben realizar los respectivos ajustes antes de continuar.
4. **Activación de pools de DHCP**. Habilitar los pools de DHCP en las vlans en las cuales se hayan realizado las pruebas de funcionamiento.
5. **Quitar IPs estáticas**. Remover IPs estáticas previamente configuradas en el punto 2 para que obtengan su dirección por DHCP.
6. **Pruebas de funcionamiento.** Realizar validación de correcta operación con los servicios habilitados en IPv6 y con los servicios que operan en IPv4. Si hay algún problema con algún servicio se deben realizar los respectivos ajustes.

3.8.1.5 PREPARACIÓN DE LOS SISTEMAS DE COMUNICACIÓN – SWITCHES

Para este capítulo se deberán tener en cuenta las siguientes consideraciones
ALISTAMIENTO PREVIO

- ✓ Realizar backup de todos los dispositivos antes de cualquier cambio en la infraestructura.
- ✓ Validar previamente logs, alarmas, consumo de memoria en los dispositivos para asegurar que los equipos estén en un estado óptimo antes de cualquier cambio.
- ✓ En lo posible tener los equipos actualizados para evitar bugs del sistema.
- ✓ Validar los segmentos a asignar en IPV6 para los equipos de red antes de realizar cualquier configuración.
- ✓ Validar que la información de segmentación, inventarios y demás esté actualizada al momento de iniciar el proceso de implementación, de no ser así realizar las respectivas actualizaciones a los documentos.

El proceso de transición se debe llevar a cabo en el siguiente orden con el fin de generar el menor impacto en la red.

- ✓ **Activación de protocolo IPV6 en los switches**. Se debe realizar la activación del protocolo en cada switch con el fin de habilitar los comandos de IPV6 en las consolas.
- ✓ **Configuración de interfaces en dual stack con protocolo IPV6**. de acuerdo con el plan de direccionamiento y segmentación se deben habilitar las interfaces con su respectiva dirección IPV6.
- ✓ **Configuración de rutas.** De acuerdo con el plan de direccionamiento se deben crear las rutas en IPV6 correspondientes.
- ✓ **Pruebas de enrutamiento.** Realizar pruebas a otros dispositivos habilitados en IPV6 con el fin de validar que los pasos anteriores se hayan ejecutado de forma correcta.

3.8.1.6 PREPARACIÓN– RED WIRELESS

Para este capítulo se deberán tener en cuenta las siguientes consideraciones:

ALISTAMIENTO PREVIO

- ✓ Realizar backup de todos los dispositivos antes de cualquier cambio en la infraestructura.
- ✓ Quitar los relays de DHCP de la controladora en IPV4 y activarlos en el core para guardar consistencia con los relays de IPV6 los cuales se asignarán en el core.
- ✓ Validar previamente logs, alarmas, consumo de memoria en los dispositivos para asegurar que los equipos estén en un estado óptimo antes de cualquier cambio.
- ✓ En lo posible tener los equipos actualizados para evitar bugs del sistema.
- ✓ Tener configuradas las vlans y relays correspondientes a los SSIDs inalámbricos configurados en IPV6.
- ✓ Tener configurados los Scopes correspondientes a las vlans de los SSIDs en IPV6 en los servidores Windows

El proceso de transición se debe llevar a cabo en el siguiente orden con el fin de generar el menor impacto en la red.

- ✓ **Activación de protocolo IPV6 en la Wireless Lan Controller**. Se debe realizar la activación del protocolo IPV6 en la plataforma con el fin de que se habiliten todas las funciones. (Si existe una controladora inalámbrica)

- ✓ **Configuración de interfaces en dual stack** con protocolo IPV6. de acuerdo con el plan de direccionamiento y segmentación se deben habilitar las interfaces con su respectiva dirección IPV6.
- ✓ Pruebas de respuesta de interfaces. Realizar pruebas desde dispositivos externos en IPV6 a las interfaces en IPV6 configuradas.
- ✓ **Configuración de listas de acceso**. Si existen listas de acceso en IPV4 que estén en uso y de plataforma que haga parte de la implementación, se deben configurar en IPV6.
- ✓ **Configuración de otros servicios**. De acuerdo con el plan de diagnóstico se deben habilitar en IPV6 los servicios que sean 100% compatibles con el protocolo IPV6 y que estén corriendo en la controladora actualmente en IPV6 (Ejemplo. NTP, SNMP, NETFLOW etc.).
- ✓ **Pruebas de asignación de direccionamiento** sobre SSIDs. Realizar pruebas de conexión de usuarios a las redes Wifi y validar que tomen direccionamiento IPV6.
- ✓ **Pruebas sobre SSIDs**. Probar que se tenga acceso a diferentes redes cableadas en IPV6 desde las redes inalámbricas (De acuerdo con los permisos de cada red).
- ✓ **Backup**. Realizar backup de las configuraciones realizadas.

3.8.1.7 PREPARACIÓN PARA PLATAFORMAS DE VIRTUALIZACIÓN

Para este capítulo se deberán tener en cuenta las siguientes consideraciones.

ALISTAMIENTO PREVIO

- ✓ Verificar la existencia de switches sin soporte IPV6 conectados a los servidores físicos.

El proceso de transición se debe llevar a cabo en el siguiente orden con el fin de generar el menor impacto en la red.

- ✓ Configurar interfaces LAN con dirección IPV6 en los nodos físicos del clúster.
- ✓ Verificar creación Registros DNS IPV6 para cada uno de los Servidores VMware.
- ✓ Desde cada servidor VMware realizar un ping al controlador de dominio
- ✓ Desde cada servidor VMware realizar un ping al default gateway.
- ✓ Desde cada servidor Hyper-V realizar un ping al DNS.
- ✓ Verificar creación registro DNS del equipo cliente.

3.8.1.8 PREPARACIÓN PARA SISTEMAS DE INFORMACIÓN.

Para este capítulo se deberán tener en cuenta las siguientes consideraciones.
Alistamiento Previo

- ✓ Validar que las cadenas de conexión a base de datos y apis externas estén utilizando los nombres de dominio.
- ✓ Configurar las cadenas de conexión a base de datos y apis externas con los nombres de dominio respectivos, en los casos en que estén configuradas con IPs y no con nombres de dominio.
- ✓ Verificar conectividad en IPV4 entre la infraestructura de los sistemas de información con el objetivo de corregir cualquier error que se esté presentando actualmente.
- ✓ En lo posible contar con un plan de pruebas a realizar para verificar el funcionamiento de los sistemas de información.
- ✓ Verificar las reglas de Firewall relacionadas con el sistema de información.
- ✓ Verificar el funcionamiento de los sistemas de información en IPV6.
- ✓ Elaborar un plan de implementación IPv6 para las aplicaciones de acuerdo con la criticidad dada en el inventario de activos de TI IPv6.
- ✓ Antes de poner en producción una aplicación modificada para IPv6, crear un ambiente de pruebas y cerciórese que arroja los resultados esperados.
- ✓ Crear copias de respaldo antes de cualquier modificación.

3.8.1.9 BASE DE DATOS.

El proceso de transición se debe llevar a cabo en el siguiente orden con el fin de generar el menor impacto en la red.

- ✓ Crear una copia de seguridad de las bases de datos.
- ✓ Actualizar la tabla de Host, con las direcciones IPv6 correspondientes.
- ✓ Actualizar los Jobs, Procedimientos almacenados y toda configuración de base de datos que invoque a una aplicación, modificando acorde a la tabla de Host actualizada.

- ✓ Para las Bases de Datos, crear una copia de seguridad, realizar las configuraciones para IPv6 en un entorno de pruebas, modificando acorde a la tabla de Host actualizada.
- ✓ Validar los modelos de bases de datos con el fin de determinar si existen campos dentro de las tablas que deban modificarse, ya sea en su tamaño o en su tipo. Lo anterior para el almacenamiento de variables que tengan datos de dirección IPv6.

3.8.1.9 CONEXIONES CLIENTE/APLICACIÓN

De acuerdo con la manera en que se invoque a la aplicación, tener en cuenta.

- ✓ Para las Aplicaciones WEB, hacer el llamado a través del nombre del Host, ya que a través de la dirección IP puede generar inconvenientes. Es importante tener en cuenta que si se desea acceder a una aplicación por su dirección IPv6 se debe usar la sintaxis adecuada de la dirección entre corchetes: [ ].
- ✓ Para las Aplicaciones Cliente/Servidor, actualizar orígenes de datos, documentos conexión o cualquier otro tipo de conector que la aplicación tenga, para que esta se realice a través de nombre de Host. En caso de que los clientes compilados ya tengan direcciones IP quemadas en el código, se recomienda recompilar la aplicación con el nombre del servidor en vez de la dirección IP.
- ✓ Para las unidades mapeadas, hacer el llamado de las unidades de red compartidas invocando directamente el nombre del Host donde se encuentra el recurso.

3.8.1.10 PREPARACIÓN DE LOS SERVIDORES

Con el fin de llevar a cabo la transición de IPv6 en dicho frente, es necesario tener las siguientes consideraciones las cuales se mencionan a continuación.

- ✓ Verificar que los dispositivos de red de los servidores soportan, son compatibles y se encuentran actualizados para su operación en IPv6.
- ✓ Acorde al análisis de criticidad IPv6, es necesario establecer un plan ordenado de asignación de direcciones para estos dispositivos.

- ✓ Activar las características de IPv6 en cada uno de los sistemas operativos de los servidores.
- ✓ Asignar una dirección IPv6 estática, de acuerdo con el plan de direccionamiento.
- ✓ Verificar el correcto registro del servidor en el DNS con su correspondiente dirección en IPv6 y en el Servidor DHCP IPv6.

3.8.1.10 CONSIDERACIONES GENERALES

En este capítulo se mencionan algunas de las consideraciones que se deberán tener en cuenta para el desarrollo del plan técnico operativo para la transición de IPv6.

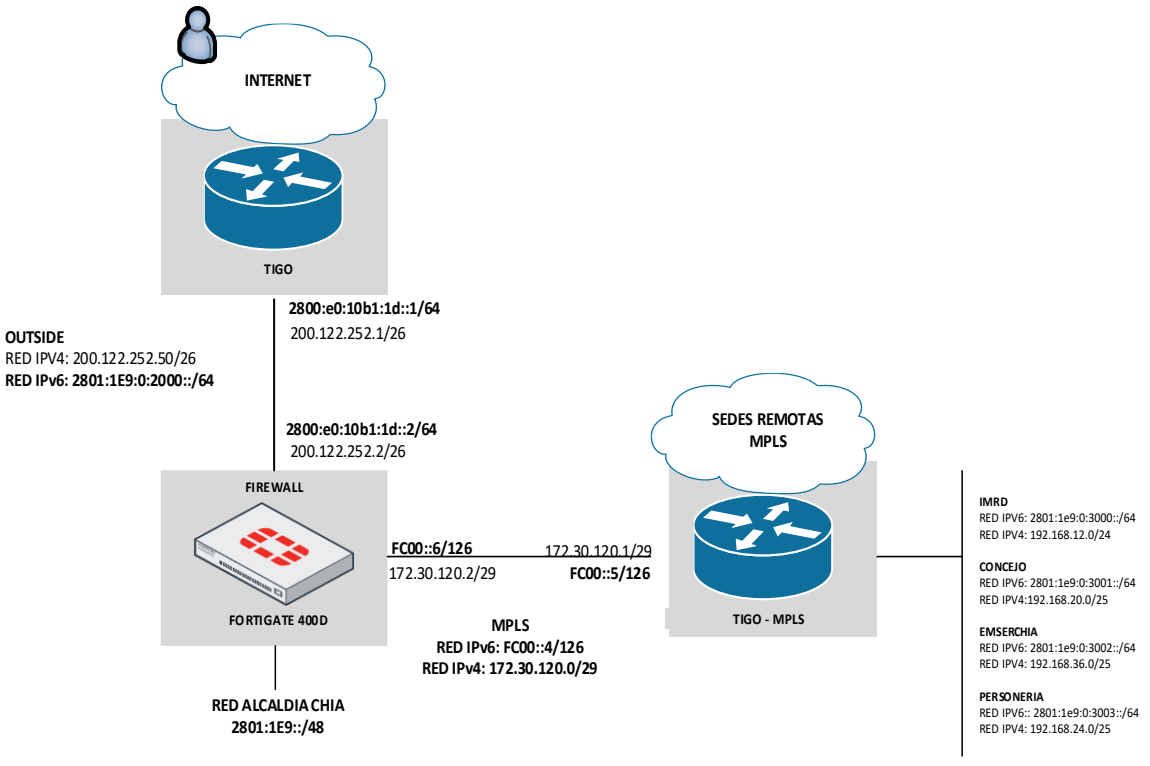
- ✓ Capacitar a todo el personal implicado en la gestión y manejo del protocolo IPv6.
- ✓ Socializar ante la organización el plan de implementación de IPv6.
- ✓ Todos los procesos de adquisición tecnología a futuro deben exigir la compatibilidad con IPv6.
- ✓ Aunque el porcentaje de compatibilidad de los equipos con IPv6 es importante, se deben tener en cuenta que todos los nuevos equipos deben adquirirse con compatibilidad en IPv6.
- ✓ Validar el plan técnico de implementación con el fin de determinar las actividades y fechas en las que deben llevarse a cabo dichas actividades de implementación.
- ✓ Dado que la entidad cuenta con infraestructura a la nube, ya sea pública o privada, se recomienda tener en cuenta los siguientes aspectos.
    1. Debe contarse con el direccionamiento de la entidad propio para poderlo entregar al proveedor.
    2. Debe seleccionarse el segmento de red IPv6 que se asignará a las direcciones IP que se migrarán a la nube con el fin de que no se traslape con el direccionamiento interno. Estas direcciones serán anunciadas por el proveedor en su nube, por lo tanto, el rango debería ser único para los servicios que son públicos.
    3. Definir junto con el proveedor de servicios el mejor esquema de direccionamiento y segmentación de acuerdo con las condiciones adquiridas de la nube privada o pública.

4. CONFIGURACIONES Y DIAGRAMAS DE IPV6

En el siguiente capitulo se presenta las configuraciones realizadas para la implementación de IPv6 con los cambios detallados de todas las configuraciones realizadas incluyendo las configuraciones realizadas sobre los canales de comunicación, también incluye los diagramas de conectividad y mapas de conexión de equipos de red, recordando que la estrategia de migración será (Dual-stack), por otra parte también contiene información de la topología lógica con su plan de direccionamiento (IPv4/IPv6).

4.1 DIAGRAMA LÓGICO

En la siguiente sección se presenta un diagrama de red lógico de cómo está la entidad actualmente. Con su plan de direccionamiento (Dual Stack)



4.2 CONFIGURACIÓN E IMPLEMENTACIÓN INFRAESTRUCTURA

Este capítulo contiene la información correspondiente a la fase de implementación e informe de resultado de las pruebas realizadas de cada uno de los activos de información que en su mayoría son servidores, también incluye la analogía del plan de direccionamiento homologado de IPv4 a IPv6.

4.2.1 DIRECCIONAMIENTO IPv6 SERVIDORES

Para la configuración de IPv6 se utilizó como segmento final la misma dirección IPv4 que tienen actualmente los servidores, unidos al rango global y la segmentación generada para cada una de las VLAN existentes en IPv4. En cuanto a la puerta de enlace, se realiza exactamente igual, segmento VLAN + dirección final de IPv4, ejemplo:
IPv4: 10.10.16.131
IPv6: 2801:18:6800:1cf::131

NOMBRE	IPv4	IPv6
		2801:1e9:0:2006:1::18
		2801:1e9:0:2006:1::15
		2801:1e9:0:2006:1::52
		2801:1e9:0:2006:1::4
		2801:1e9:0:2006:1::10
		2801:1e9:0:2006:1::12
		2801:1e9:0:2006:1::20
		2801:1e9:0:2006:1::35
		2801:1e9:0:2006:1::133

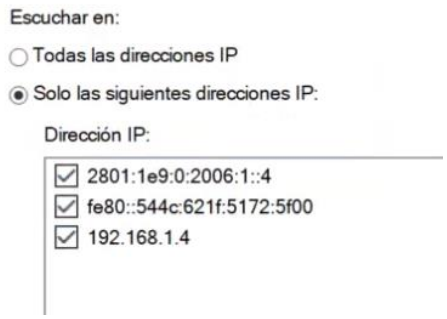
4.2.2 DIRECTORIO ACTIVO Y DNS

El directorio activo de la Alcaldía de Chia, esta sobre un solo controlador de dominio, por lo que este fue configurado en dual stack, permitiendo recibir peticiones tanto en IPv4 como en IPv6, teniendo siempre en cuenta que se preferirá el tráfico en IPv6 siempre que esté disponible.

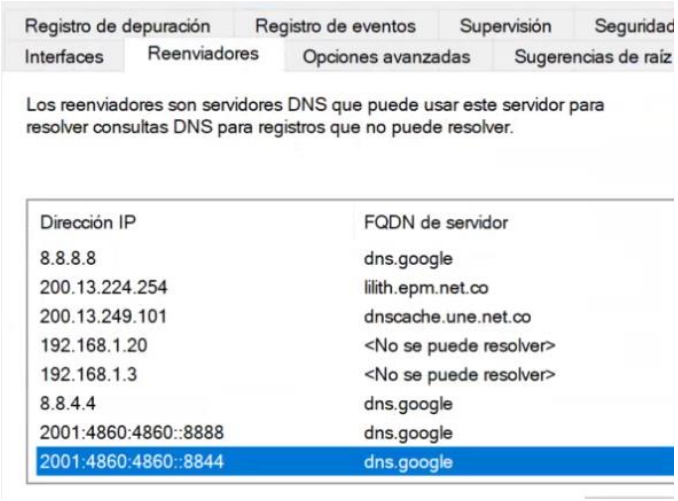
Debido a que no se cuenta con direccionamiento en sites and services ni relaciones de confianza con otros dominios, no se realizan configuraciones especiales en el directorio activo.

DNS DIRECTORIO ACTIVO

- Habilitar la escucha en el direccionamiento dual stack



- Configurar los reenviadores públicos de Google



- Registros DNS de equipos cliente con IPv6 mediante DHCP

SGDCW74137	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0346	6/12/2022 11:00:00 a. m.
SGDGHW74195	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0345	6/12/2022 11:00:00 a. m.
SGPCDCW74130	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0344	6/12/2022 11:00:00 a. m.
SGPCWIN74273	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0342	6/12/2022 11:00:00 a. m.
SIOPDEDPW72072	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:033f	6/12/2022 11:00:00 a. m.
SGDCW74132	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:033c	6/12/2022 11:00:00 a. m.
SGDCW74134	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:033b	6/12/2022 11:00:00 a. m.
SIOPDEDPW72070	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0337	6/12/2022 11:00:00 a. m.
DPOCIW72046	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0336	6/12/2022 11:00:00 a. m.
SGDCW74131	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0335	6/12/2022 11:00:00 a. m.
SGDCW74137	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0331	6/12/2022 11:00:00 a. m.
SECGENGHPC	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:032f	6/12/2022 11:00:00 a. m.
SGDCW74136	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:032d	6/12/2022 11:00:00 a. m.
SIOPW72069	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:032c	6/12/2022 11:00:00 a. m.
SIOPDCSW72074	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0321	6/12/2022 11:00:00 a. m.
SGW74143	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:031f	6/12/2022 11:00:00 a. m.
SGDCW74146	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:031d	6/12/2022 11:00:00 a. m.
SIOPW72079	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:031b	6/12/2022 11:00:00 a. m.
AUXDESPACHO-PC	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:031a	6/12/2022 11:00:00 a. m.
DCW74133	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0315	6/12/2022 11:00:00 a. m.
DGHW74032	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0314	6/12/2022 11:00:00 a. m.
UNIS	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0312	6/12/2022 11:00:00 a. m.
SIOPW74044	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0311	6/12/2022 11:00:00 a. m.
SGDCW104141	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0310	6/12/2022 12:00:00 p. m.
OCIW72044	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:030e	6/12/2022 11:00:00 a. m.
SGDGHW74045	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:030d	6/12/2022 11:00:00 a. m.
OCIW2047	Host IPv6 (AAAA)	2801:01e9:0000:2006:0002:0000:0000:0309	6/12/2022 11:00:00 a. m.

DNS PFSENSE

Se configuró la interfaz LAN en dual stack y se habilitó una política en IPv6 que permite escuchar peticiones DNS en dual stack.

4.2.3 SERVIDORES WINDOWS

En este capítulo se presenta la configuración realizada bajo IPv6 a cada servidor que cuanta con sistema operativo Windows en las siguientes secciones se menciona el nombre de cada servidor y su adopción a al nuevo protocolo con su

Pruebas de ping en IPv6

```
C:\Users\Administrador>ping 2801:1e9:0:2006:1::3

Haciendo ping a 2801:1e9:0:2006:1::3 con 32 bytes de datos:
Respuesta desde 2801:1e9:0:2006:1::3: tiempo<1m
Respuesta desde 2801:1e9:0:2006:1::3: tiempo<1m
Respuesta desde 2801:1e9:0:2006:1::3: tiempo<1m
Respuesta desde 2801:1e9:0:2006:1::3: tiempo<1m

Estadísticas de ping para 2801:1e9:0:2006:1::3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

4.2.3.2

En la siguiente imagen se muestra un resumen de su configuración.

Propiedad	Valor
Dirección física	00-50-56-80-7A-7C
Habilitado para DHCP	No
Dirección IPv4	192.168.1.18
Máscara de subred IPv4	255.255.252.0
Puerta de enlace predete...	192.168.1.3
Servidores DNS IPv4	192.168.1.4
	192.168.1.20
Servidor WINS IPv4	
Habilitado para NetBios a...	Sí
Dirección IPv6	2801:1e9:0:2006:1::18
	2801:1e9:0:2006:2::301
Concesión obtenida	martes, 06 de diciembre de 2022 11:5
La concesión expira	martes, 13 de diciembre de 2022 11:5
Vínculo: dirección IPv6 local	fe80::f01e:37c5:95a1:1aa2%12
Puertas de enlace predet...	fe80::724c:a5ff:fe85:3c19%12
	2801:1e9:0:2006:1::3
Servidores DNS IPv6	2801:1e9:0:2006:1::4
	2801:1e9:0:2006:1::20

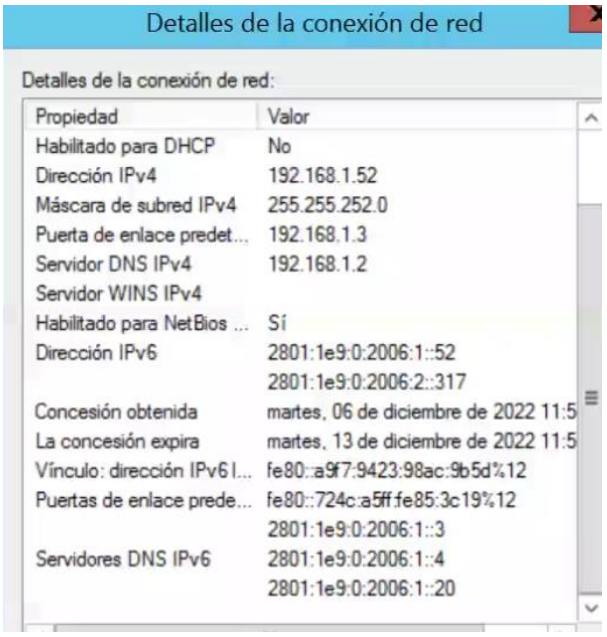
Pruebas de ping en IPv6.

4.2.3.3 xxxxxx

Servidor Oracle configurado en dual stack

Tipo	Dato
IPv4	192.168.1.52
IPv6	2801:1e9:0:2006:1::52
Gateway	2801:1e9:0:2006:1::3
DNS1	2801:1e9:0:2006:1::4
DNS2	2801:1e9:0:2006:1::20

En la siguiente imagen se muestra un resumen de su configuración.



Pruebas de ping IPv6

```
C:\Users\Administrador>ping 2801:1e9:0:2006:1::3

Haciendo ping a 2801:1e9:0:2006:1::3 con 32 bytes de datos:
Respuesta desde 2801:1e9:0:2006:1::3: tiempo=1ms
Respuesta desde 2801:1e9:0:2006:1::3: tiempo<1m
Respuesta desde 2801:1e9:0:2006:1::3: tiempo<1m
Respuesta desde 2801:1e9:0:2006:1::3: tiempo<1m

Estadísticas de ping para 2801:1e9:0:2006:1::3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

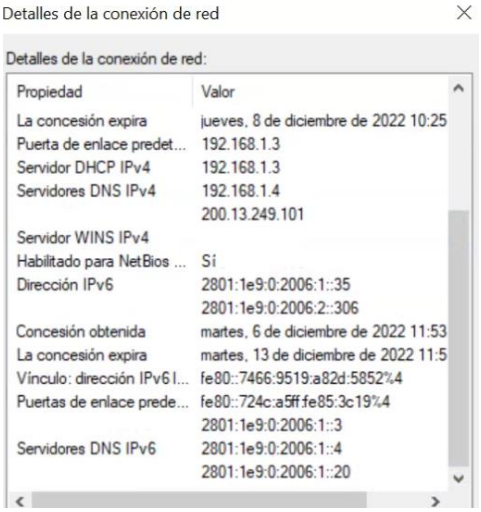
```
C:\Users\Administrador>ping 2801:1e9:0:2006:1::4

Haciendo ping a 2801:1e9:0:2006:1::4 con 32 bytes de datos:
Respuesta desde 2801:1e9:0:2006:1::4: tiempo=2ms
Respuesta desde 2801:1e9:0:2006:1::4: tiempo=1ms
Respuesta desde 2801:1e9:0:2006:1::4: tiempo<1m
Respuesta desde 2801:1e9:0:2006:1::4: tiempo=1ms

Estadísticas de ping para 2801:1e9:0:2006:1::4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 2ms, Media = 1ms
```

4.2.3.4 CORRYCOM

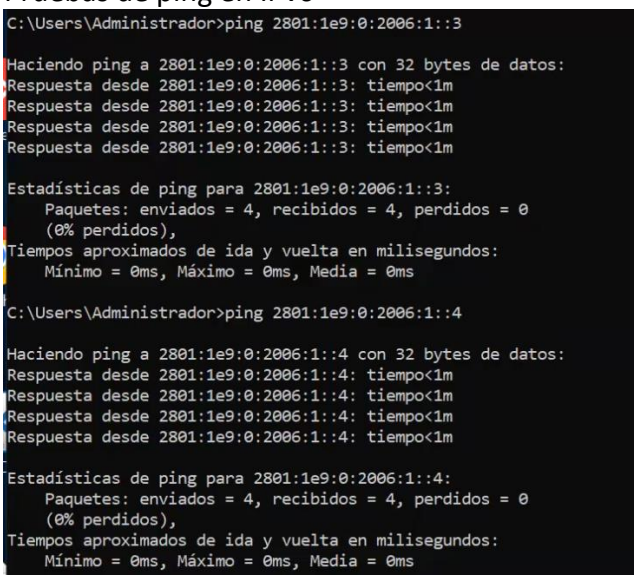
Servidor de gestor documental en dual stack

Tipo	Dato
IPv4	192.168.1.35
IPv6	2801:1e9:0:2006:1::35
Gateway	2801:1e9:0:2006:1::3
DNS1	2801:1e9:0:2006:1::4
DNS2	2801:1e9:0:2006:1::20

En la siguiente imagen se muestra un resumen de su configuración.



Pruebas de ping en IPv6



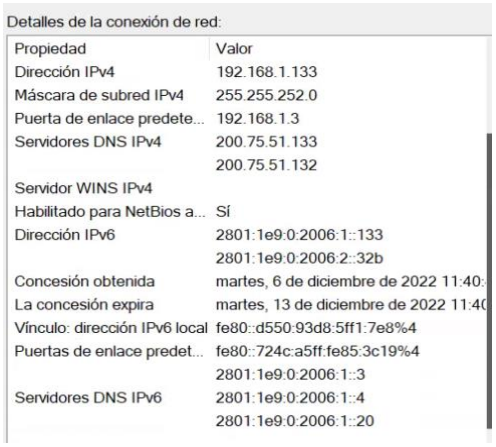
Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co

4.2.3.5 SALUD

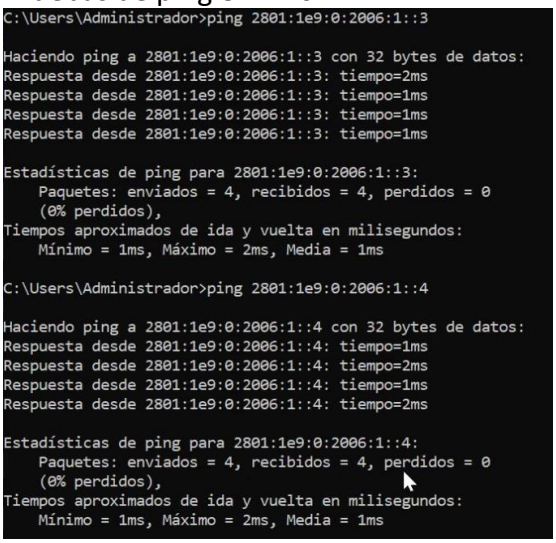
Servidor de la aplicación salud

Tipo	Dato
IPv4	192.168.1.133
IPv6	2801:1e9:0:2006:1::133
Gateway	2801:1e9:0:2006:1::3
DNS1	2801:1e9:0:2006:1::4
DNS2	2801:1e9:0:2006:1::20

En la siguiente imagen se muestra un resumen de su configuración.



Pruebas de ping en IPv6



4.2.4 SERVIDORES LINUX

En este capítulo se presenta la configuración realizada bajo IPv6 a cada servidor que cuanta con sistema operativo linux en las siguientes secciones se menciona el nombre de cada servidor y su adopción a al nuevo protocolo con su plan de direccionamiento.

4.2.4.1 ARGIS

Servidor nuevo de ArcGIS en dual stack

Tipo	Dato
IPv4	192.168.1.15
IPv6	2801:1e9:0:2006:1::15
Gateway	2801:1e9:0:2006:1::3
DNS1	2801:1e9:0:2006:1::4
DNS2	2801:1e9:0:2006:1::20

En la siguiente imagen se muestra un resumen de su configuración.

```
[root@serverarcgis apache-tomcat-9.0.19]# ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.15  netmask 255.255.248.0  broadcast 192.168.7.255
        inet6 fe80::20c:29ff:fea1:63b0  prefixlen 64  scopeid 0x20<link>
        inet6 2801:1e9:0:2006:1::15  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:a1:63:b0  txqueuelen 1000  (Ethernet)
        RX packets 3230725  bytes 224168612 (213.7 MiB)
        RX errors 0  dropped 916527  overruns 0  frame 0
        TX packets 6368  bytes 7834958 (7.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Pruebas de ping en IPv6

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co

```
[root@serverarcgis apache-tomcat-9.0.19]# ping 2801:1e9:0:2006:1::3
ping: 2801:1e9:0:2006:1::3: Address family for hostname not supported
[root@serverarcgis apache-tomcat-9.0.19]# ping6 2801:1e9:0:2006:1::3
PING 2801:1e9:0:2006:1::3(2801:1e9:0:2006:1::3) 56 data bytes
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=1 ttl=64 time=0.294 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=2 ttl=64 time=0.228 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=3 ttl=64 time=0.181 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=4 ttl=64 time=0.215 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=5 ttl=64 time=0.210 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=6 ttl=64 time=0.203 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=7 ttl=64 time=0.196 ms
^C
--- 2801:1e9:0:2006:1::3 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5999ms
```

```
[root@serverarcgis apache-tomcat-9.0.19]# ping6 2801:1e9:0:2006:1::4
PING 2801:1e9:0:2006:1::4(2801:1e9:0:2006:1::4) 56 data bytes
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=1 ttl=128 time=0.515 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=2 ttl=128 time=0.818 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=3 ttl=128 time=0.570 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=4 ttl=128 time=0.549 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=5 ttl=128 time=0.617 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=6 ttl=128 time=0.890 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=7 ttl=128 time=0.572 ms
^C
--- 2801:1e9:0:2006:1::4 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6002ms
rtt min/avg/max/mdev = 0.515/0.647/0.890/0.136 ms
```

4.2.4.2 SERVER-GLPI

Servidor GLPI en dual stack

Tipo	Dato
IPv4	192.168.1.12
IPv6	2801:1e9:0:2006:1::12
Gateway	2801:1e9:0:2006:1::3
DNS1	2801:1e9:0:2006:1::4
DNS2	2801:1e9:0:2006:1::20

En la siguiente imagen se muestra un resumen de su configuración.

```
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.12  netmask 255.255.248.0  broadcast 192.168.7.255
        inet6 fe80::20c:29ff:fe35:b487  prefixlen 64  scopeid 0x20<link>
        inet6 2801:1e9:0:2006:1::12  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:35:b4:87  txqueuelen 1000  (Ethernet)
        RX packets 69826207  bytes 5257467699 (4.8 GiB)
        RX errors 0  dropped 9  overruns 0  frame 0
        TX packets 33877  bytes 2787651 (2.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Pruebas de ping en IPv6

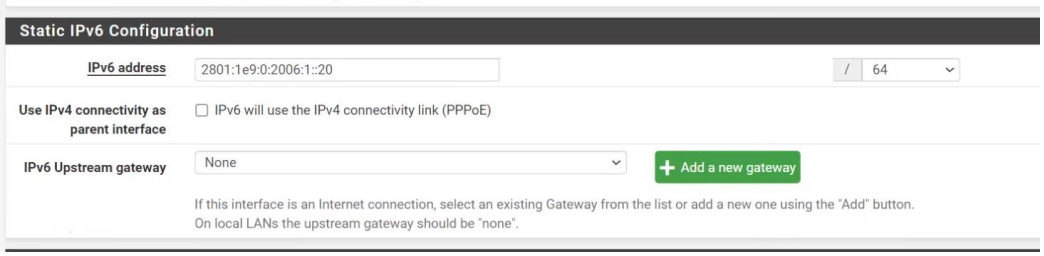
```
[root@serverglpi ~]# ping6 2801:1e9:0:2006:1::3
PING 2801:1e9:0:2006:1::3(2801:1e9:0:2006:1::3) 56 data bytes
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=1 ttl=64 time=0.358 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=2 ttl=64 time=0.224 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=3 ttl=64 time=0.215 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=4 ttl=64 time=0.243 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=5 ttl=64 time=0.231 ms
64 bytes from 2801:1e9:0:2006:1::3: icmp_seq=6 ttl=64 time=0.191 ms
^C
--- 2801:1e9:0:2006:1::3 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5000ms
```

```
[root@serverglpi ~]# ping6 2801:1e9:0:2006:1::4
PING 2801:1e9:0:2006:1::4(2801:1e9:0:2006:1::4) 56 data bytes
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=1 ttl=128 time=1.46 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=2 ttl=128 time=0.578 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=3 ttl=128 time=0.772 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=4 ttl=128 time=0.749 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=5 ttl=128 time=0.557 ms
64 bytes from 2801:1e9:0:2006:1::4: icmp_seq=6 ttl=128 time=0.774 ms
^C
--- 2801:1e9:0:2006:1::4 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5001ms
```


Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co

4.2.4.3 HASS

Configuración dual stack del servidor Hass en la interfaz LAN para los servicios de DNS



Monitoreo del acceso en IPv6 al Gateway

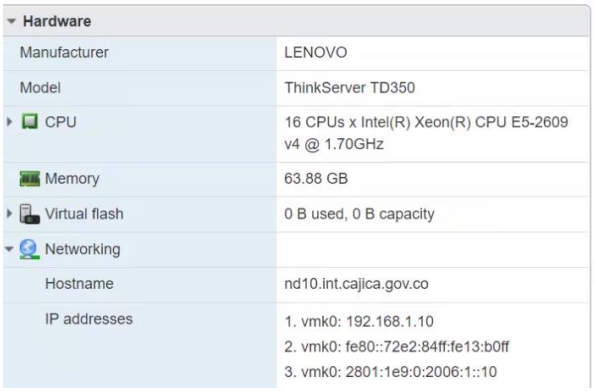
Gateways

Name	Gateway	Monitor	RTT	RTTsd	Loss	Status	Description
GWWAN (default)	190.71.132.161	190.71.132.161	0.24ms	0.029ms	0.0%	Online	GWWAN
GWLAN	192.168.1.3	192.168.1.3	0.075ms	0.014ms	0.0%	Online	GWLAN
GWLANIPV6 (default)	2801:1e9:0:2006:1::3	2801:1e9:0:2006:1::3	0.077ms	0.014ms	0.0%	Online	GWLANIPV6

4.2.5 HIPERVISOR

En este capitulo se presenta el aprovisionamiento la solución de VMware y su asignación en IPv6.

Servidor Hipervisor VMware en dual stack



Hardware

Manufacturer	LENOVO
Model	ThinkServer TD350
CPU	16 CPUs x Intel(R) Xeon(R) CPU E5-2609 v4 @ 1.70GHz
Memory	63.88 GB
Virtual flash	0 B used, 0 B capacity
Networking	
Hostname	nd10.int.cajica.gov.co
IP addresses	1. vmk0: 192.168.1.10 2. vmk0: fe80::72e2:84ff:fe13:b0ff 3. vmk0: 2801:1e9:0:2006:1::10

4.3 SEGMENTACIÓN IPV4 & IPV6

A continuación, se muestra la tabla de segmentación en IPv6 para la entidad en la cual se destaca:

- ✓ Direccionamiento IPv4 actual.
- ✓ Direccionamiento IPv6 propuesto

En la siguiente tabla se detalla el plan direccionamiento (IPv4 & IPv6), para toda la entidad

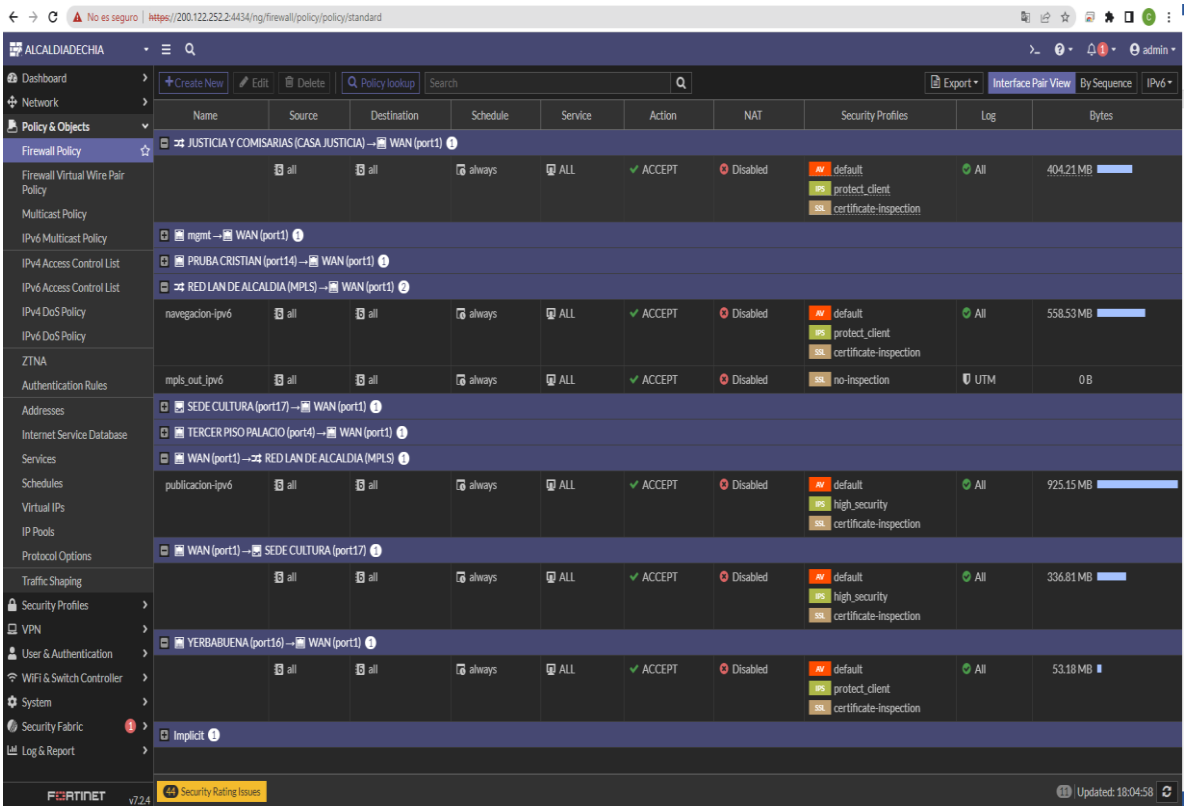
ZONA	NAME	IPV4	IPv6	UBICACIÓN
WAN	WAN TIGO	200.122.252.2/26	2801:1e9:0:2000::1/64	FIREWALL
LAN	LA-MPLS (Port13)	172.16.16.01/24	2801:1e9:0:2001::/64 - FC00::6/126 (fw)	FIREWALL
LAN	PALACIO	10.10.16.2	2801:1e9:0:2002::/64	FIREWALL
LAN	EUCACION	10.10.8.1./23	2801:1e9:0:2003::/64	FIREWALL
LAN	JUSTICIA	10.10.13.1/24	2801:1e9:0:2004::/64	FIREWALL
LAN	CALAHORRA	10.10.15.1/24	2801:1e9:0:2005::/64	FIREWALL
LAN	CULTURA	10.10.12.1/24	2801:1e9:0:2006::/64	FIREWALL
DIRECCIONAMIENTO SEDES REMOTAS				
SEDES			IPV4	IPV6
YERBABUENA			172.16.16.1/24	2801:1e9:0:3004::/64

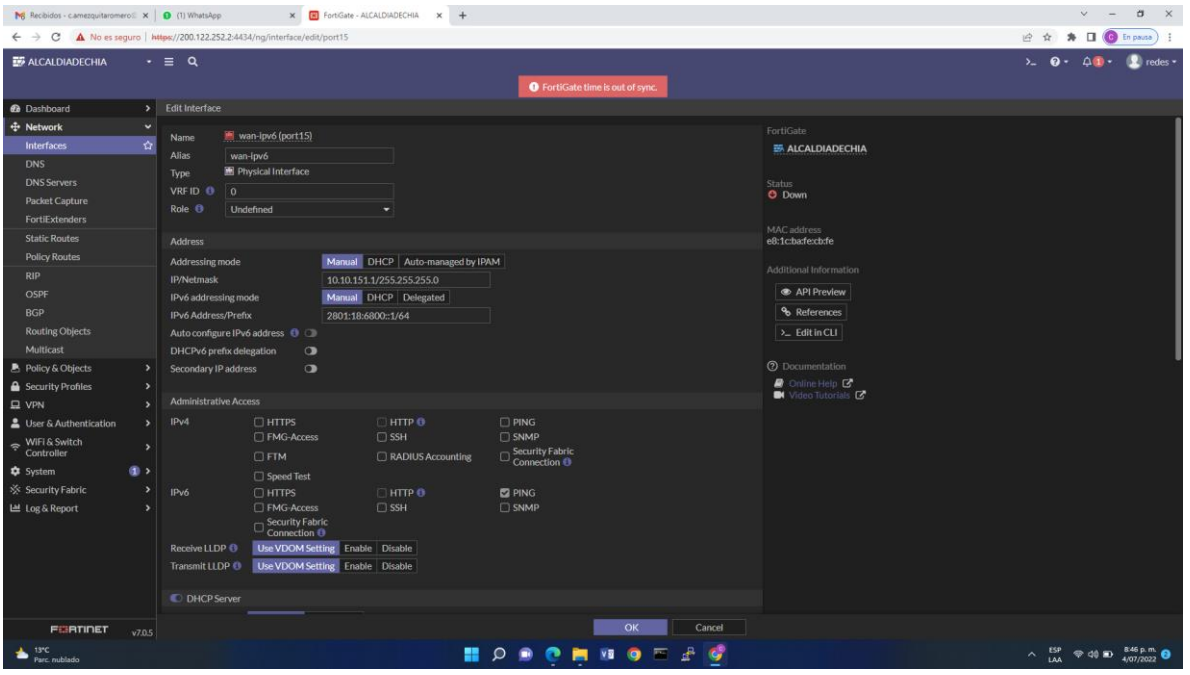
De acuerdo con la estrategia propuesta para el desarrollo de la segmentación encontramos que algunas redes en IPv4 se pueden obtener varias subredes de manera que no se podría establecer su homologada en IPv6.

4.4 PLATAFORMA DE SEGURIDAD

En el siguiente capítulo se muestra un resumen de las configuraciones realizadas a la plataforma de seguridad marca FortiGate la cual es la capa central de la red de datos de la entidad y converge la mayoría de los activos de información.

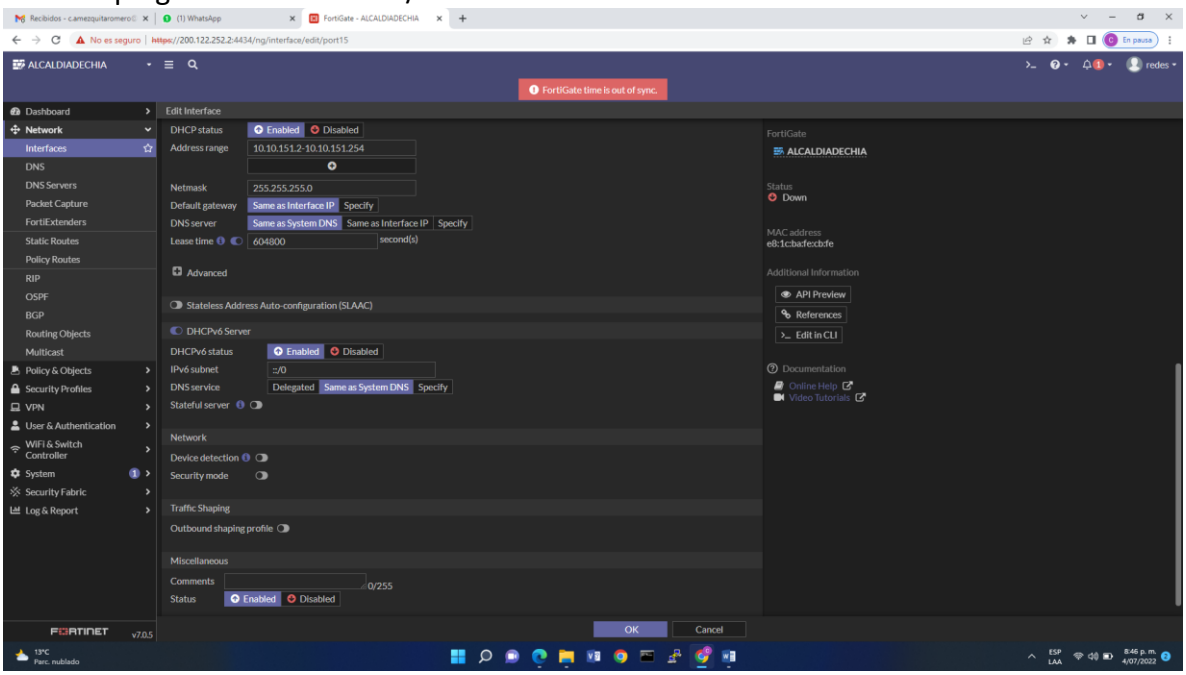
Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co



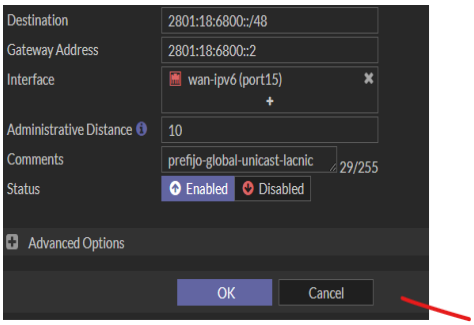


2801:18:6800::1/64
Gateway 2801:18:6800::2
2800:E0:10B1:1D::1

execute ping6 2801:18:6800::1/64



Static Route
Destination:
2801:18:6800::/48
Gateway address
2801:18:6800::2
Administrative distance
10
Comments
prefijo-global-unicast-lacnic



Local BGP Options
Local AS 271828
Router ID:
Neighbors:
IP: 2800:E0:10B1:1D::1

Remote AS: 13489

Neighbor Groups
Name
Remote AS
No results

Neighbor Ranges
Prefix
Neighbor Group
Maximum Neighbor Number
No results

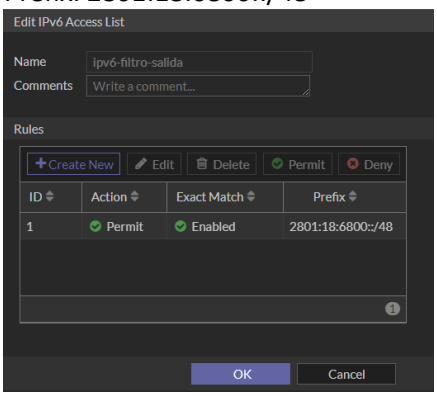
Networks
IP/Netmask
IPv6 Networks
IP/Netmask: 2801:18:6800::/48
IPv4 Redistribute
Connected
RIP
OSPF
Static
ISIS
IPv6 Redistribute
Connected
RIP
OSPF
Static on
Filter:bgp-filtro-salida
ISIS

Dampening

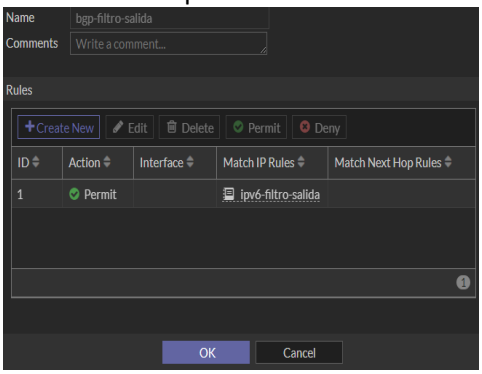
Graceful Restart
Restart timer:120
Stale path timer:360
Update delay:120
Advanced Options
Best Path Selection

Routing Objects:
IPv6 Access Lists 1
ipv6-filtro-salida1 1
Name: ipv6-filtro-salida
Comments: Write a comment...
Rules

ID:1
Action: Permit
Exact Match: Enabled
Prefix: 2801:18:6800::/48

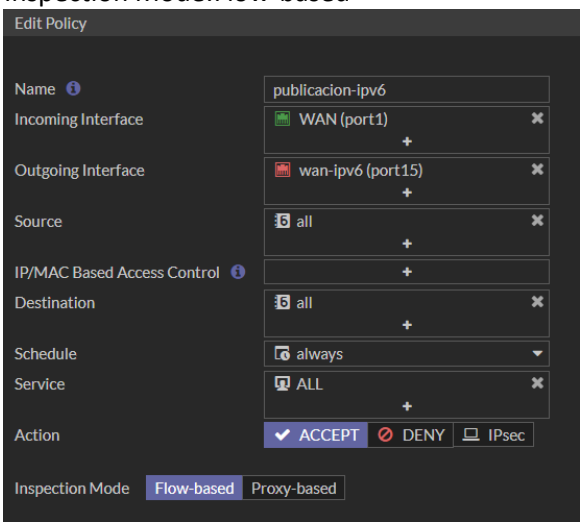


Route Maps 1
bgp-filtro-salida
Name: bgp-filtro-salida
Comments: Write a comment...
Rules
ID:1
Action: Permit
Interface:
Match IP Rules: ipv6-filtro-salida
Match Next Hop Rules



Politicas:
Name: publicacion-ipv6
Incoming Interface: WAN (port1)
Outgoing Interface: wan-ipv6 (port15)
Source:6all
IP/MAC Based Access Control
Destination: 6all

Schedule:always
Service:ALL
Action:ACCEPT
Inspection Mode:Flow-based



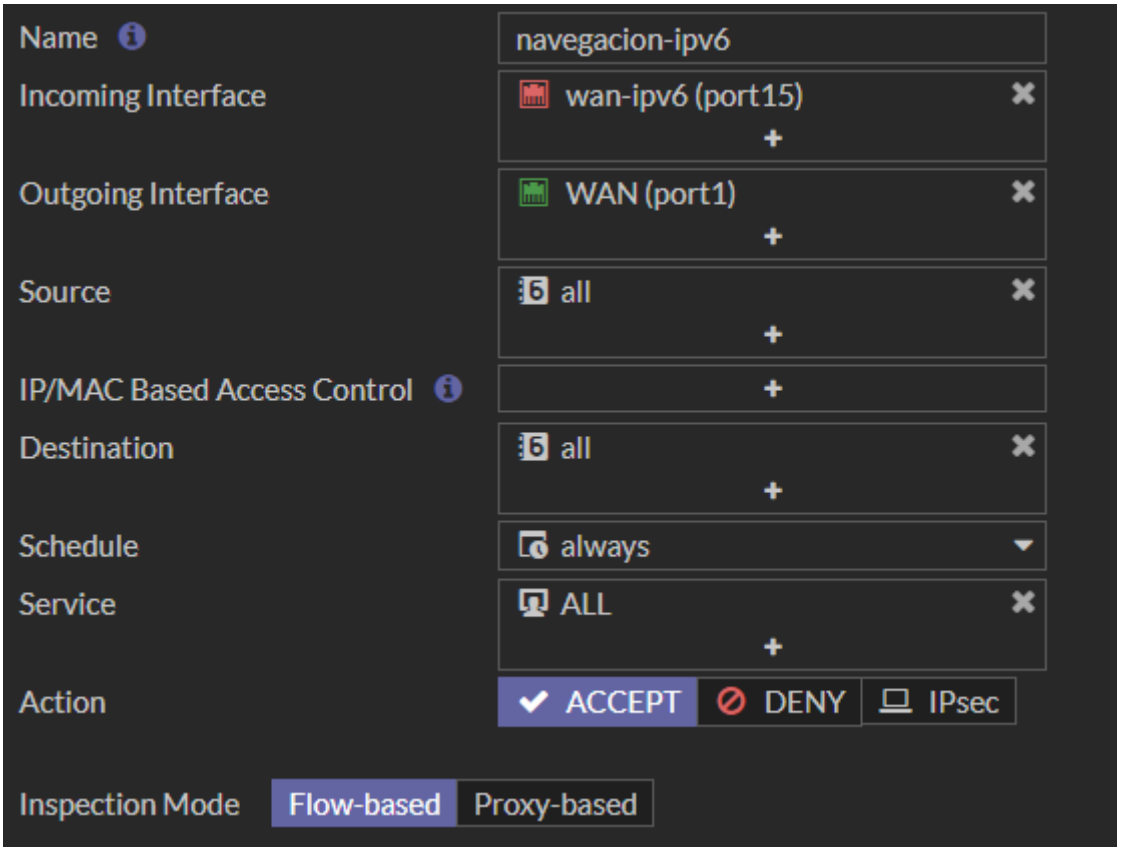
Firewall / Network Options
NAT:no

Protocol Options:default
Security Profiles:
AntiVirus:default
Web Filter:
DNS Filter:
Application Control:
IPS:high_security
File Filter
SSL Inspection:certificate-inspection

Logging Options
Log Allowed Traffic: All sessiones
Comments
Enable this policy

Navegacion-ipv6
Incoming Interface: wan-ipv6 (port15)

Outgoing Interface: WAN (port1)
Source:6all
IP/MAC Based Access Control:
Destination: 6all
Schedule:always
Service:ALL
Action:ACCEPT



Inspection Mode:Flow-based

Firewall / Network Options
NAT:no
Protocol Options:default

Security Profiles:
AntiVirus:default
Web Filter:
DNS Filter:
Application Control:
IPS:protect_client
File Filter
SSL Inspection:certificate-inspection

Logging Options
Log Allowed Traffic: All sessiones
Comments
Enable this policy

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinartic@chia.gov.co
www.chia-cundinamarca.gov.co