Plan de Implementación del Protocolo IPv6

Relación de Versiones

Versión	Fecha	Revisó	Aprobó
1	Diciembre 15 de 2023	Yorguin Gómez Ortiz	

Tabla de Contenido

1. Justificación 4

2. PLANTEAMIENTO DEL PROBLEMA 7

3. Objetivos 9

OBJETIVO GENERAL 9

OBJETIVOS ESPECÍFICOS 9

4. Fases de la transición 10

Fase I. Planeación de IPv6 10

Actividades 10

Fase iI. implementacion del protocolo IPv6 11

Actividades 11

Fase iII. pruebas de funcionalidad de IPv6 12

Actividades 12

Tiempo de ejecucion total - FaseS del proyecto 13

5. TERMINOLOGÍA 15

Plan de Implementación del Protocolo IPv6

1. JUSTIFICACIÓN

A través de los años INTERNET ha estado en constante evolución en muchos aspectos como lo son el aumento de usuarios, aumento de recursos, el uso de servicios multimediales y lo que esto conlleva en cuanto a la determinación del consumo de ancho de banda, convirtiéndose de esta manera en una red que involucra una alta interactividad entre los usuarios que la acceden. Esto también trae consecuencias que como factores inciden en la actual estructura de red de las Entidades y que deben estar preparadas para incorporar nuevas tecnologías que involucren la modernización y a su vez permitan el desarrollo de las comunidades.

Atendiendo la situación de conectividad en materia de protocolo de internet, el Gobierno Nacional ha iniciado un proceso de innovación tecnológica, en el que las entidades del país deben adoptar el proceso de transición del protocolo IPv4 hacia el nuevo protocolo IPv6 siguiendo las instrucciones descritas en la Circular 002 del 6 de Julio de 2011 del Ministerio de Tecnologías de información y las Comunicaciones, que busca promover la adopción de IPv6 en Colombia bajo la Resolución 2710 de 2017 y la Resolución 1126 de 2021.

La implementación del estándar de direcciones del Protocolo de Internet Versión seis (IPv6) permitirá que internet evolucione de cara al alto crecimiento de usuarios, así como al aumento en el número de dispositivos conectados y a la creciente demanda de servicios conectados al internet

a nivel mundial; es por ello que el IPv6 es indispensable para el desarrollo de la sociedad de la información y del conocimiento. La implementación del protocolo IPv6 evitaría un atraso tecnológico en Colombia y además generaría un crecimiento en infraestructura, en el número de usuarios conectados y en el incremento de oportunidades de negocios desde el uso del internet, entre otros; lo que permitiría a mediano plazo potenciar así el desarrollo del país de una forma constructiva e incluyente.

Cuando se habla de la nueva era con un mundo globalizado en donde cada vez es mayor el uso de aplicaciones que operan a través de la red INTERNET, nadie se pregunta cómo funciona esta red de redes simplemente se le exige como consumidores, y cada vez con mayor rigor y nivel de esta, teniendo en cuenta que los mecanismos en esta red implantados funcionen adecuadamente en todo momento. Si se considera, además que la introducción de aspectos clave como la movilidad, que es una de las funcionalidades que la informática y las telecomunicaciones han traído recientemente y le dan soporte a un gran porcentaje de la sociedad.

Lo anterior ha conllevado a que las Entidades Públicas actuales con redes IPv4 existentes, se vean en la tarea de proceder a la migración del protocolo de internet versión 4 a la versión 6, lo que implica tener que enfrentar el reto de identificar los factores que esto traiga como consecuencia y también contemplar el impacto al cambio. Por ello se determina una planificación para llevar a cabo la transición y poner en práctica las directivas protocolares de IPv6.

Este plan de Adopción del protocolo IPv6 contiene un plan técnico para que la CAS lleve a cabo la migración y reduzca, así mismo, el mayor número de impactos negativos posibles. El plan de trabajo técnico identifica recursos humanos y financieros, así como las actividades necesarias para el logro de la migración y de la respectiva adopción.

Se puede afirmar que, actualmente, los dispositivos de red y equipos de cómputo de la CAS están conectados a internet utilizando el protocolo IPv4

y que es casi imposible realizar el cambio de tecnología de manera inmediata; es por esto que se debe llevar una fase de transición en la que, se adopte al IPv6 a la infraestructura acorde a los lineamientos planteados por MINTIC.

2. PLANTEAMIENTO DEL PROBLEMA

La evolución tecnológica y el desarrollo de nuevos dispositivos inteligentes hacen que crezcan también los problemas relacionados con la estabilidad, compatibilidad, seguridad, conectividad y acceso a direcciones IP. Debido, entre otras razones, al creciente número de usuarios y de equipos que buscan conectarse al internet.

Actualmente y desde 1981, los usuarios y equipos se pueden conectar al internet desde el Protocolo de Internet Versión 4 o IPv4. Sin embargo, la creciente demanda y la estructura con el que fue concebido el protocolo IPv4 ha requerido la utilización de la totalidad de direcciones disponibles y la cual fue agotado el pasado 19 de Agosto de 2020[1], lo que hace obligatorio realizar una migración al nuevo protocolo, es decir, al Protocolo de Internet Versión 6 (IPv6).

Migrar al protocolo IPv6 para que haya interoperabilidad y en un futuro un completo perfil de trabajo en un solo protocolo IP, requiere de unos cambios de infraestructura y demás procesos de actualización que involucran pruebas de integración y coexistencia entre el antiguo protocolo IPv4 y el nuevo IPv6 en la CAS

La migración de IPv4 a IPv6, según lo establece el MINTIC, se debe hacer de forma planeada y escalonada, con el fin de mitigar cualquier interoperabilidad entre aplicaciones que se pueda presentar durante el proceso. Ya que se tienen que utilizar ambos protocolos al mismo tiempo: IPv4 e IPv6 a través del intercambio de paquetes entre los mismos protocolos.

Se ha utilizado una asignación de direcciones mediante CIDR, así como la Traducción de direcciones de Red (NAT) que han intentado resolver este

[1] https://www.lacnic.net/4847/1/lacnic/agotamiento-de-ipv4:-lacnic-asigno-el-ultimo-bloque

problema sin obtener mucho éxito, ya que en primera instancia no todos los enrutadores de la CAS soportan CIDR, sin contar que existen aplicaciones que requieren direcciones estáticas, por lo que NAT colabora en gran medida con estos casos. Otro aspecto para destacar es la seguridad misma que ha tomado un papel muy importante en el manejo de la información académica y financiera que es enviada a través de los medios electrónicos. IPv4 no fue diseñado para que fuese un protocolo seguro y muchas de las aplicaciones creadas para solucionar este problema de seguridad solo protegen la información en las capas de comunicación más altas (Aplicación y Transporte) haciendo vulnerable la información a ataques en la capa de Red. IPv6 por su parte se presenta como una solución viable a los problemas de la red se sistemas de la anteriormente mencionados, porque incluye entre otras mejoras, direcciones de 128 bits, en lugar de las direcciones de 32 bits de IPv4, incluyendo la seguridad sobre la capa de Red.

3. OBJETIVOS

OBJETIVO GENERAL

Analizar, diseñar e implementar las actividades a realizar para la adopción del protocolo IPv6 en La CAS en modo dual stack, para la operatividad en la infraestructura y los servicios de la red, utilizando los dos protocolos, IPv4 e IPv6.

OBJETIVOS ESPECÍFICOS

- Establecer un plan de trabajo que permita Implementar el protocolo para la interoperabilidad entre IPv4-IPv6 en Dual Stack, permitiendo operar la red LAN-WAN de La CAS.

4. FASES DE LA TRANSICIÓN

Atendiendo la metodología propuesta por el MINTIC en las guías de apoyo de adopción del protocolo IPv6 para La CAS, se establecen las 3 fases con las siguientes actividades.

FASE I. PLANEACIÓN DE IPV6

La fase de planeación representa una etapa crítica e importante del proceso de transición en el que se tiene en cuenta la infraestructura general instalada y que se plasma en el plan de diagnóstico de la entidad.

Actualmente, en La CAS los dispositivos de red y terminales computacionales están conectados a internet desde el uso del protocolo IPv4. Ejecutar cualquier método como *dual stack, Tunneling, Translation* para pasar IPv6 puede proporcionar una capa adicional de opciones de conectividad; adicionalmente, las configuraciones de firewall y la administración de la lista de control de acceso cambiarían inmediatamente en IPv6 en comparación con IPv4, así que es por ello que al momento de este cambio se debe tener un plan de acción debidamente planificado.

Actividades

Las siguientes son las actividades a desarrollar durante esta fase:

Actividades Generales	Tiempo en Semanas de la actividad
Construcción del plan de Diagnóstico	2
Inventario de TI (Hardware, Software)	1.5

Análisis de la nueva topología de la infraestructura actual y su funcionamiento	3
Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos	3
Planeación de la transición de los servicios tecnológicos de la Entidad. Plan de direccionamiento de IPv6 y plan de contingencia de IPv6	3
Validación de estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes.	1.5
Identificación de esquemas de seguridad de la información y las comunicaciones	1.5

FASE II. IMPLEMENTACION DEL PROTOCOLO IPV6

Durante esta fase, se describen las diferentes actividades que se desarrollarán en La CAS y definidas en la fase anterior, para poner en funcionamiento el protocolo IPv6 en la infraestructura instalada.

Actividades

Actividades Generales	Tiempo en Semanas de la actividad
Habilitación direccionamiento IPv6 (plan de numeración) para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico de la Primera Fase.	4
Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.	4

Actividades Generales	Tiempo en Semanas de la actividad
Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP.	4
Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.	5
Coordinación con el (los) proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.	5

FASE III. PRUEBAS DE FUNCIONALIDAD DE IPV6

Durante esta fase, se realiza la verificación de funcionamiento de la totalidad de la infraestructura instalada y en servicio de La CAS, garantizando su normal utilización y coexistencia con el protocolo IPv4, donde aplique. En esta fase se realizaran los ajustes necesarios a la configuración y su respectiva documentación.

Actividades

Actividades Generales	Tiempo en Semanas de la actividad
Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad.	4
Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.	4
Afinamiento de las configuraciones de hardware, software y servicios de la Entidad	4

TIEMPO DE EJECUCION TOTAL - FASES DEL PROYECTO

De acuerdo al plan detallado y descrito anteriormente, el resumen de tiempo por fases, para la adopción del protocolo IPv6 en La CAS es el siguiente:

Producto	Fase	Productos para entregar	Tiempo Entrega (Semanas)
Proceso de Implementación del protocolo de IPv6	Diagnóstico Situación Actual	Plan de trabajo para la adopción de IPv6 Inventario de TI, informe de infraestructura de comunicaciones, recomendaciones de adquisición elementos Hardware/Software, plan de diagnóstico, plan de direccionamiento IP, plan de excepciones, informe de preparación, plan de contingencias de IPv6. Documento implementación de seguridad de IPv6 en congruencia con la política de seguridad de las Entidades, plan de contingencias de IPv6 y plan de capacitación en IPv6.	16
	Desarrollo del Plan de Implementación	Informe plan detallado implementación de IPv6.	26

		Documento configuraciones del nuevo protocolo sobre las plataformas de hardware, software y servicios intervenidos durante esta fase. Informe de aplicación de políticas de seguridad de IPv6. Informe de resultados de las pruebas realizadas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento.	
	Pruebas de Funcionalidad de IPv6	Documento con cambios detallados de las configuraciones realizadas, según análisis de funcionalidad de la fase II. Acta(s) de cumplimiento a satisfacción de funcionamiento de los servicios y aplicaciones intervenidos durante la fase II. Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.	12

5. TERMINOLOGÍA

DHCPv6 (Dynamic Host Configuration Protocol): Protocolo de Configuración Dinámica de Hosts para IPv6 con característica cliente-servidor y definido por la RFC 3315 de la IEFT, que proporciona una configuración administrada de dispositivos sobre redes IPv6.

IP: Protocolo Internet.

Dirección IP: Representación numérica que identifica una interfaz en particular de manera exclusiva en una red de datos.

Direccionamiento IPv6: Es una etiqueta numérica del paquete usada para identificar una interfaz de red que provee una conexión entre nodos de una red sobre IPv6, esto facilita el enrutamiento de los paquetes entre distintos hosts.

Protocolo IPv4: Es la cuarta versión del Protocolo de Internet, es un protocolo de interconexión de redes. Utiliza direcciones de 32 bits que limitan el espacio de direcciones a 42.934.967.296 direcciones.

Protocolo IPv6: es la nueva versión del Protocolo de Internet (Internet Protocol -IP) en el cual se sustenta la operación de Internet. Las especificaciones técnicas básicas de IPv6 se desarrollaron en la década de los 90s con el IETF (Internet Engineering Task Force). Destinado a sustituir al Protocolo Internet Versión 4. IPv6 amplía el número máximo de direcciones de Internet al manejar un tamaño de dirección IP de 128 bits a diferencia de su antecesor IPv4 que maneja un tamaño de dirección IP de 32 bits.

Mecanismos de transición a IPv6: Los protocolos IPv4 e IPv6 no son compatibles y para la migración a IPv6 debe mantenerse la coexistencia de ambos protocolos por un tiempo determinado en lo que se logra la total migración a IPv6. La clave para una migración exitosa consiste en poder

utilizar ambos protocolos en la red hasta que todos los servicios sean migrados a IPv6. La mayoría de los nodos de Internet van a necesitar utilizar ambos protocolos por mucho tiempo, lo que requiere la definición e implementación de mecanismos de transición a IPv6. Esos mecanismos de transición pueden agruparse en tres grandes categorías: (Doble Pila, Traductores, Tunneling).

A pesar de las ventajas que ofrecen cada uno de estos mecanismos, la esencia principal de todos ellos es el mecanismo de Doble Pila.

De acuerdo a las recomendaciones de MinTIC (Ministerio de Tecnologías de la Información y las Comunicaciones) y organismos internacionales como LACNIC el mecanismo que garantiza con eficiencia la coexistencia de ambos protocolos (IPv4 e IPv6) es el de Doble Pila. Este será por tanto el mecanismo que se considerará para la implementación del Protocolo Internet Versión 6 (IPv6) al interior de la institución.

Topología de red: Es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (ejemplo: computadores, impresoras, servidores, switches, enrutadores, etc.) se interconectan entre si sobre un medio de comunicación.

a). Topología física: Se refiere al diseño actual del medio de transmisión de la red.

b). Topología lógica: Se refiere a la trayectoria lógica de una señal a su paso por los nodos de la red.

Políticas de seguridad: Son aquellas reglas y procedimientos definidos por una organización con el propósito de preservar la confidencialidad, la integridad y la disponibilidad de los sistemas y la información.

Políticas de enrutamiento: El enrutamiento basado en políticas proporciona una herramienta para reenviar y enrutar paquetes de datos basados en las políticas definidas por los administradores de red. En efecto, es una manera de que la política invalide las decisiones del protocolo de enrutamiento. El

enrutamiento basado en políticas incluye un mecanismo para aplicar selectivamente políticas basadas en la lista de acceso, el tamaño de los paquetes u otros criterios. Las medidas que se toman pueden incluir el enrutamiento de paquetes en rutas definidas por el usuario, el establecimiento de la precedencia, el tipo de bits de servicio, etc.

Infraestructura tecnológica: Conjunto de elementos de hardware y software sobre el que se asientan los servicios de una organización.

Segmentos de red: Resultado de dividir una red de datos con el propósito de aumentar el número de nodos conectados a ella.

Prefijos IPv6: Representan un rango o bloque de direcciones IP consecutivas. Que deberán solicitarse formalmente ante organismos autorizados para su asignación en cuyo caso la organización será propietaria indefinidamente de tal bloque de direcciones o podrá recibirse de un Proveedor de Servicios de Internet con la diferencia de que tal direccionamiento no pertenecerá a la organización.

LACNIC: Organización internacional no gubernamental con sede en Uruguay cuya función es la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa para la región de América Latina y el Caribe.

Proveedor de Servicios Internet: Empresas que proporcionan servicios de conexión a Internet y temas relacionados.

Sistemas de Información: Conjunto de mecanismos ordenados que tienen como fin la administración de datos e información para su procesamiento y entrega.

Sistemas de comunicación: Conjunto de dispositivos interconectados para el transporte y entrega de información.

Pruebas de funcionalidad: Proceso mediante el cual se valida la funcionalidad de un sistema.

Protocolo de pruebas: Programa sistemático de verificación e inspección diseñado y ejecutado para el control de calidad de la tecnología y operación de un equipo, proceso o servicio. Así como condiciones de seguridad y fiabilidad.

Redes Privadas Virtuales – VPN: (Virtual Private Network): Es una tecnología de acceso que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

IPsec (IP Security): Protocolo de seguridad definido por el estándar IETF desde 1999 y basado inicialmente en los RFC 2401 y 2412, pero en la tercera generación de documentos nacieron los RFC 4301 y 4309, que le dieron la abreviatura IPsec como hoy en día se conoce; ofrece integración a nivel de red, brindando seguridad de IP a los protocolos de capas superiores, actúa como un componente embebido dentro de IPv6 que suministra control de acceso, autenticación de origen de datos, confidencialidad, integridad es un esquema no orientado a la conexión, con independencia en los algoritmos de cifrado y negociación de compresión IP.