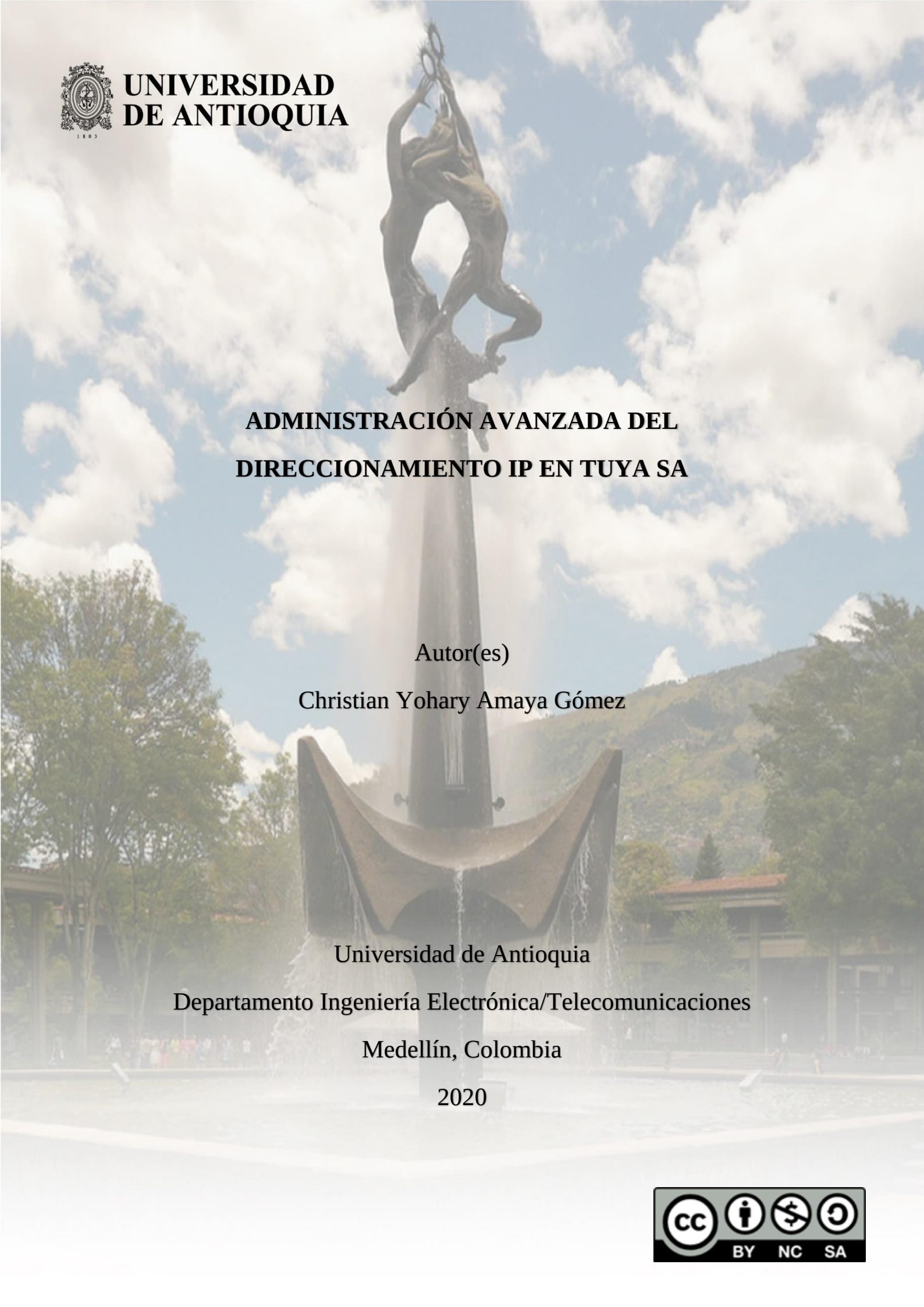


UNIVERSIDAD DE ANTIOQUIA

ADMINISTRACIÓN AVANZADA DEL DIRECCIONAMIENTO IP EN TUYA SA

Autor(es)

Christian Yohary Amaya Gómez

Universidad de Antioquia

Departamento Ingeniería Electrónica/Telecomunicaciones

Medellín, Colombia

2020

INFORME FINAL

Administración avanzada del direccionamiento IP en TUYA SA

CHRISTIAN YOHARY AMAYA GÓMEZ

ASESOR INTERNO:

ERWIN ALEXANDER LEAL

ASESOR EXTERNO:

MAURICIO RESTREPO MUÑOZ

UNIVERSIDAD DE ANTIOQUIA

DEPARTAMENTO INGENIERÍA ELECTRÓNICA/TELECOMUNICACIONES

MEDELLÍN, COLOMBIA

2020

Contenido

Capítulo 1: Resumen

La Compañía de Financiamiento TUYA S.A., posee una gran infraestructura de red, con aproximadamente 10 mil direcciones IP en uso, la cual conlleva un gran desafío con la administración y asignación del direccionamiento. Este proyecto se centró en el direccionamiento asociado a la granja de servidores, el cual posee alrededor de 600 direcciones IP. En este escenario existía un problema en la reserva, asignación y liberación de direcciones IP a los nuevos servidores que se instalaban. Esta reserva se hacía manualmente en una hoja de cálculo y luego se hacía su respectiva asignación, sin reflejar el estado actual de la red. Además, no existía un proceso de liberación de IP para dar de baja completamente un servidor, provocando que no se pudiera determinar si una dirección IP estaba libre de reglas en firewall u otro tipo de restricción para su uso. Ante la problemática planteada se optó por implementar un servidor IPAM (IP Address Management) a través de la plataforma de monitoreo de red OpManager, donde se logra obtener una actualización diaria de cuáles direcciones están disponibles o han hecho alguna modificación (sea que se apagó, se eliminó o se cambió de dispositivo). Como complemento a esta solución, se creó una nueva oferta de servicios relacionados con la gestión de direcciones IP en la plataforma Sarita (plataforma de la organización donde los usuarios reportan sus requerimientos o incidentes, para dar solución a alguna problemática). De esta manera, con la adopción del servidor IPAM y la creación de la nueva oferta de eliminación de IP en la intranet, se logró que el proceso de asignación y liberación sea ágil, y su respectivo monitoreo esté centralizado y brinde información confiable.

Capítulo 2: Introducción

TUYA S.A. es una compañía de financiamiento, que cuenta con más de 2000 empleados distribuidos geográficamente a nivel nacional. Presenta 2 sedes principales en Medellín, que en conjunto poseen más de 500 empleados, y que, debido al momento actual, en su mayoría nos conectamos vía VPN (Virtual Private Network) desde nuestras casas. El resto de personal de TUYA, está distribuido en los puntos de atención al usuario llamados CATT (Centro de Atención Tarjeta Tuya), ubicados en los almacenes Éxito, Carulla y Alkosto de todo el territorio nacional, y además otras oficinas en Bogotá y Cali.
Aquí es importante destacar que cada punto de atención CATT, se visualiza a nivel de infraestructura de red, como una pequeña intranet de la compañía que también demanda direccionamiento IP. En dichos puntos se instalan PCs, Tablets, celulares y otros periféricos que deben conectarse a servidores en nube o físicos de la organización vía SSH (Secure Shell) o escritorio remoto, lo cual permite el uso de aplicativos para el funcionamiento del negocio.

En la siguiente Ilustración 1, se ve la manera como los PCs (puede ser cualquier dispositivo de red), se conectan al enrutador de Tuya, que permite la conexión con el data center, donde están configuradas las políticas de acceso para cada dispositivo.

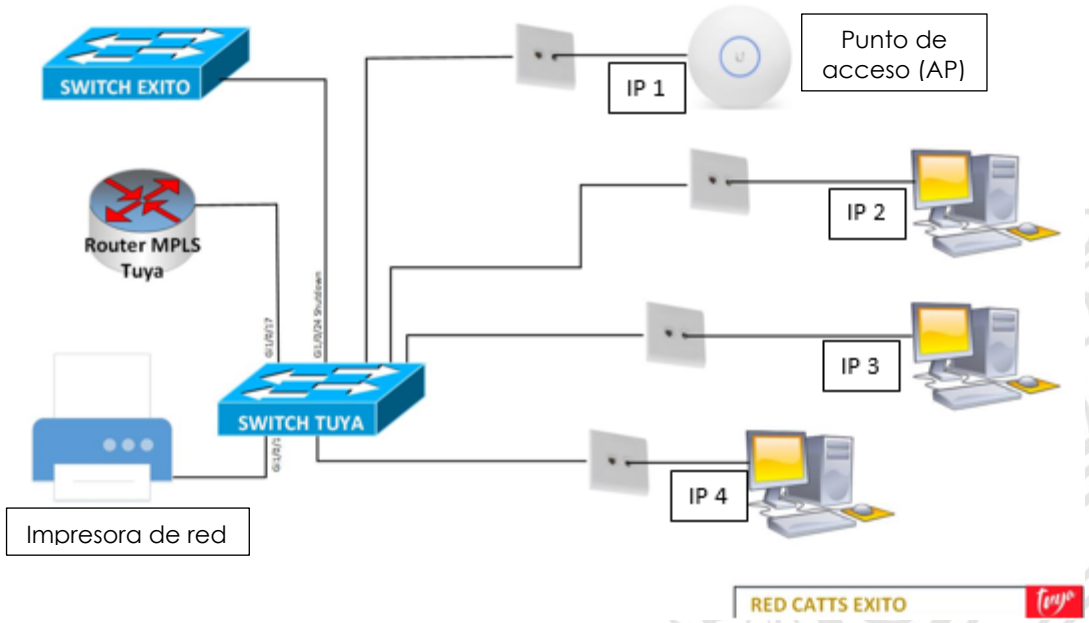


Ilustración 1. Diagrama de conexión CATT

En este contexto, el requerimiento de asignación de direcciones IPv4 (Internet Protocol versión 4) para los servidores, por solicitud de los usuarios está en constante crecimiento, logrando tener alrededor de 600 direcciones IP en uso en la granja de servidores y un total de 10 mil en la compañía. Anteriormente, el proceso de asignación de recursos IP, se hacía de forma manual, almacenando esta información en hojas de cálculo, lo cual es un procedimiento que no proveía una adecuada gestión de recursos y era susceptible a errores. Por ejemplo, cuando se daba de baja un servidor, su dirección IP se marcaba como disponible en la hoja de cálculo, pero las reglas de seguridad asociadas continuaban vigentes en el Firewall, generando errores si se usa con otro dispositivo.

Con el propósito de dar solución a la problemática planteada, se propuso a través de la práctica empresarial, instalar una solución de tipo IPAM (IP Address Management), que permite mejorar la gestión y supervisión del direccionamiento IP. En principio, la cobertura y evaluación de la solución propuesta fue solo para la granja de servidores localizada en Niquia (Bello, Ant.), pero se espera que dicha solución sea desplegada al 100% de las

direcciones IP en uso. Como complemento a la solución IPAM planteada, se realizó la creación de una nueva oferta de servicios en la plataforma Sarita (plataforma para la gestión de requerimientos o incidentes de la organización), a modo de garantizar que cuando aparezca una IP disponible realmente si lo esté. Con esta nueva oferta, se garantiza que la eliminación de políticas restrictivas para un determinado recurso IP se haya realizado exitosamente, obteniendo así una alta confiabilidad en la información suministrada por el servidor de monitoreo IPAM.

Capítulo 3: Objetivos

3.1. General:

Diseñar e implementar una solución que permita mejorar la gestión del direccionamiento IP para la sede Medellín de la compañía TUYA S.A.

3.2. Específicos:

1. Comprender los mecanismos y métodos que actualmente son utilizados para la gestión de la asignación de direcciones IP y monitoreo.
2. Identificar y seleccionar las soluciones, aplicativos y/o herramientas que permitan actualizar y mejorar la gestión del direccionamiento IP.
3. Implementar y automatizar la solución para la gestión del direccionamiento IP seleccionado.
4. Evaluar y verificar el adecuado funcionamiento de la solución propuesta.

Capítulo 4: Marco Teórico

Para contextualizar un poco sobre el desarrollo de la propuesta y dar a entender los conceptos involucrados, empezaremos con explicar, de qué trata una administración avanzada del direccionamiento IP.

Es importante aclarar, que, a lo largo del documento, se habla de INTERGRUPO y OLIMPIA. Estas dos empresas, son aliadas de la compañía, las cuales brindan apoyo en la administración de la infraestructura de red (Intergrupo), y brinda todo el soporte necesario. Respecto a mecanismos de seguridad, se tiene a la empresa Olimpia, que, en conjunto con el área de ciberseguridad de la compañía, hacen el despliegue de sistemas que permiten salvaguardar la integridad completa de los sistemas de información.

4.1. Dirección IP

Inicialmente, una dirección IP, es una dirección lógica de 32 bits, que tiene el propósito de identificar cualquier dispositivo conectado a una red de comunicaciones que utilice el protocolo IP. Dicha dirección es representada mediante 4 octetos en formato decimal (ver Ilustración 2)[1].

Además, es importante entender el uso de la máscara de red. Esta es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores. Su función, es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

Mediante la máscara de red, un sistema (ordenador, enrutador, etc.) podrá saber si debe enviar un paquete dentro o fuera de la subred en la que está conectado. Por ejemplo, si el enrutador tiene la dirección IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una dirección IP con formato 192.168.1.X, se envía hacia la red local, mientras que direcciones con distinto formato de dirección IP serán enviadas hacia afuera. [2]

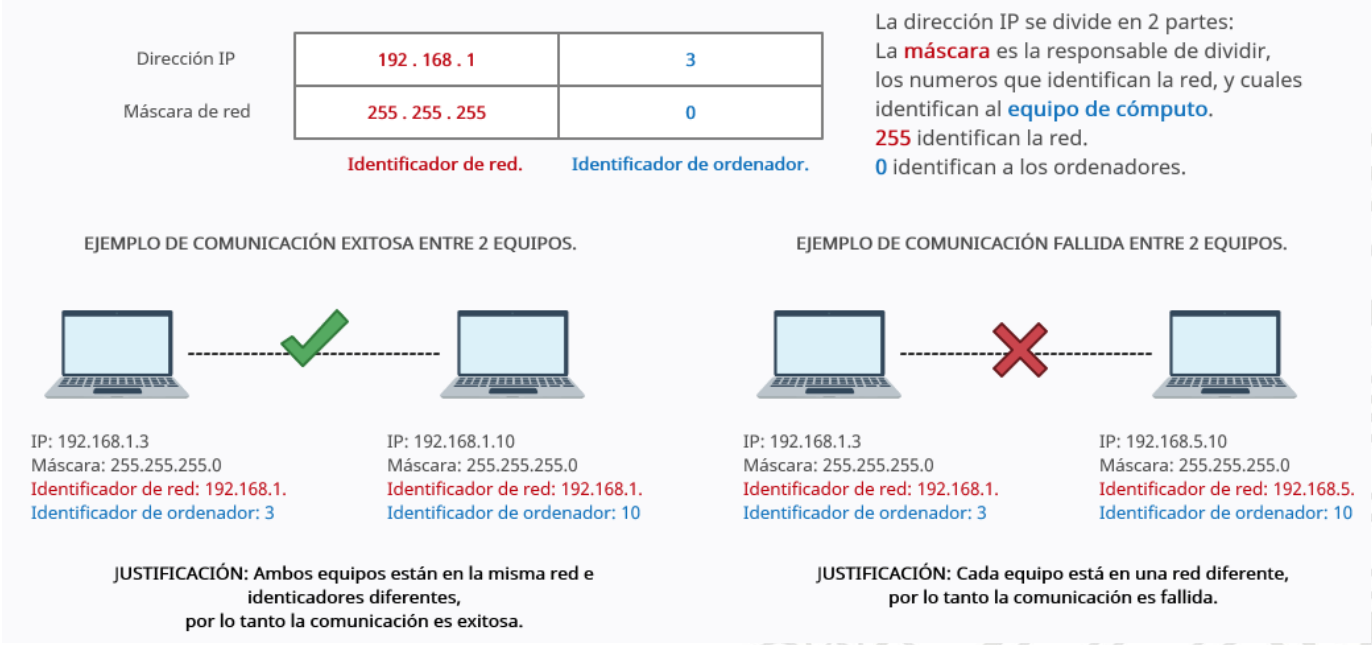


Ilustración 2. Formato dirección IP y ejemplo de comunicación.

Con lo anterior, se tiene la configuración básica que debe tener un dispositivo de red, para lograr la comunicación con otro dispositivo, en una red de telecomunicaciones.

Las direcciones IP pueden ser asignadas de manera estática, las asigna el administrador de la red; o de manera dinámica, las asigna un servidor DHCP (Dinamic Host Configuration Protocol). En este proyecto el esquema de asignación de direcciones IP para los equipos vinculados a la granja de servidores será estática, debido a políticas de red ya definidas al interior de la compañía. Una vez entendido lo anterior, se procede a pensar en una solución que brinde una adecuada gestión de los recursos IP, por lo tanto, se procede con la solución IPAM, que se detalla en la siguiente sección.

4.2. Servidor IPAM (IP Address Management)

En muchas compañías micro (<10 empleados) [3], pequeñas (de 11 a 50 empleados) [3] o medianas empresas (de 51 a 200 empleados) [3], el control y asignación de direcciones IP, es relativamente sencillo. En este tipo de escenarios, el direccionamiento IP puede ser controlado desde una hoja de cálculo, y simplemente hacer la asignación manual de direcciones IP estáticas

para servidores específicos. Sin embargo, para una empresa grande (más de 200 empleados) [3], la situación se empieza a volver tediosa y difícil de controlar, debido al gran requerimiento de asignación de direcciones IP. Un administrador de red, con la ayuda única de una hoja de cálculo, hace que la gestión del direccionamiento, sea impráctico y susceptible a errores.

Es ahí, donde se da a conocer las facultades que tiene el uso de la administración avanzada de direcciones IP (IPAM), la cual facilita la integración de herramientas ofimáticas, que permiten obtener un monitoreo centralizado y automatizado, logrando el control adecuado, sobre el uso que se les da a los recursos de red.

La gestión de direcciones de protocolo de Internet (IPAM) se refiere a un método de planificación, seguimiento y gestión de la información asociada con el espacio de direcciones de protocolo de Internet de una red. Con el software IPAM (ver Ilustración 3), los administradores pueden garantizar que el inventario de direcciones IP asignables permanezca actualizado y sea suficiente. IPAM simplifica y automatiza la administración de muchas tareas involucradas en la administración del espacio IP, incluyendo la escritura de registros DNS y la configuración de DHCP. También es común la funcionalidad adicional, como controlar las reservas en DHCP, así como otras capacidades de agregación de datos e informes. [4]

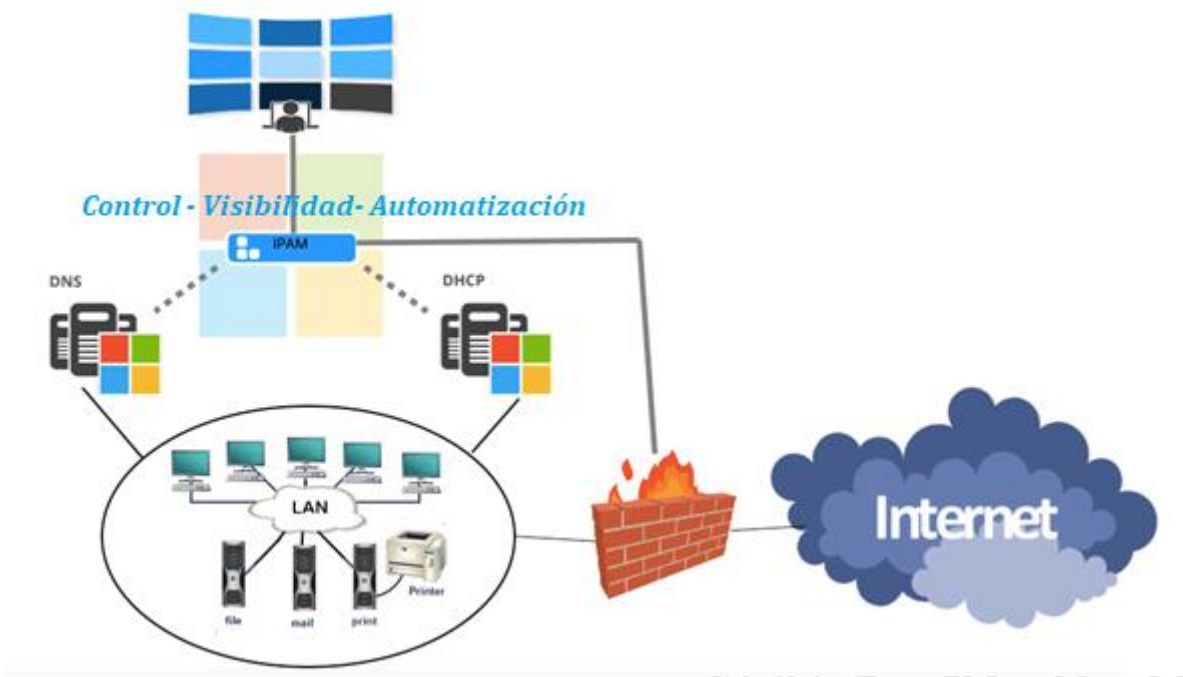


Ilustración 3. Arquitectura IPAM

Hay cinco razones principales por las que el servidor IPAM es necesario y muy útil para una organización:

- **Planificación de capacidad**: Si no puede realizar un seguimiento de su espacio de direcciones con precisión, es probable que se quede sin direcciones IP. Esto le impediría simplemente agregar nuevos suscriptores y limitaría su capacidad para hacer crecer su negocio. Cuantas más IP tenga, mayor será la administración de IP y mejor será el crecimiento de su organización.
- **Transición a IPv6**: IPAM se ha vuelto importante desde la introducción del nuevo IPv6. Un IPv6 usa una dirección de 128 bits, mientras que IPv4 sigue un esquema de direcciones de 32 bits. La complejidad agregada de IPv6 significa que, si bien un administrador pudo haber recordado una dirección IPv4, una herramienta de IPAM es necesaria para rastrear todos los recursos de IPv6. Además, una solución IPAM le permite categorizar sus recursos de red IPv4, así como el espacio de direcciones IPv6.

- **Gestión de Recursos**: Un sistema para organizar el espacio de direcciones IP es importante porque solo hay una cantidad limitada de recursos IP disponibles y estos cuestan dinero. Si no tiene un sistema de red IPAM para rastrear y administrar sus direcciones IP, problemas como conflictos de IP causarán serios problemas a los usuarios. Las soluciones de IPAM hacen que la administración de los recursos disponibles sea una tarea fácil.
- **Convertir los datos en información**: La solución de administración de direcciones IP tiene la capacidad de recopilar datos asociados con dispositivos, redes, servicios y luego convertirlos en una imagen clara. IPAM permite a los usuarios asociar la información de todos los objetos en una base de datos para que los administradores puedan buscar, ordenar y exportar en función de cualquier información.
- **La información necesaria**: Los administradores de red están interesados en el espacio de direcciones IP y el recurso asignado a cada dirección IP. Con IPAM, un administrador puede obtener la información relacionada con un recurso como el nombre de host, el tipo de dispositivo, la ubicación física, etc. desde su propia ubicación con tiempo libre. Las alertas se envían en los momentos necesarios y los informes con la información necesaria también se pueden generar fácilmente.

Adicionalmente, en el mercado existen diferentes soluciones para implementar servidores IPAM. Entre estas, se destacan Efficient IP[1], SolarWinds[2] y ManageEngine[3]. En este proyecto, después de mirar las diversas alternativas que hay en el mercado, se optó por trabajar con el software de monitoreo de red ManageEngine OpManager.

[1] https://www.efficientip.com/es/productos/ipam-para-microsoft/
[2] https://www.solarwinds.com/ip-address-manager
[3] https://www.manageengine.com/network-monitoring/ipam-spm-plugin.html

Para llevar a cabo dicha labor de elección, se procede con la elaboración de un documento, donde se involucra el área de Arquitectura, Seguridad y Gestión Tecnológica, permitiendo así, la consolidación de varias características que son indispensables para dar cumplimiento a las políticas internas de la compañía. Entre estos criterios están:

- Soporte 24/7 y en español.
- Precio y tiempo de licencia.
- Criterios de seguridad, contemplados en la normativa interna de TUYA.
- Funcionalidades y capacidad de crecimiento.

Como se menciona anteriormente, existen varias alternativas en el mercado, donde con la ayuda del documento consolidado, se hizo la validación correspondiente con los coordinadores de cada área involucrada. Finalmente llegan a la conclusión de elegir el software de Manage Engine OpManager. Es de tener en cuenta, que también una de las características indispensables en la elección del software, era que tuviera el complemento de IPAM, ya que no todas las herramientas de monitoreo poseen este servidor en mención.

El software de monitoreo de red ManageEngine OpManager, es una solución de monitoreo de red asequible y fácil de usar. Monitorea dispositivos de red como enrutadores, conmutadores, firewalls, balanceadores de carga, controladores LAN inalámbricos, servidores, VM (Virtual Machine), impresoras, dispositivos de almacenamiento y todo lo que tenga una IP y esté conectado a la red. ManageEngine OpManager monitorea continuamente la red y proporciona una visibilidad y un control en profundidad sobre ella. En caso de una falla, puede profundizar fácilmente en la causa raíz y eliminarla antes de que las operaciones se vean afectadas. [5]

En la siguiente Ilustración 4, se brinda solo un ejemplo general, de la información que muestra el software de monitoreo, respecto al uso de ancho de banda en la red donde se configuró, sin embargo, se pueden obtener muchas más características.

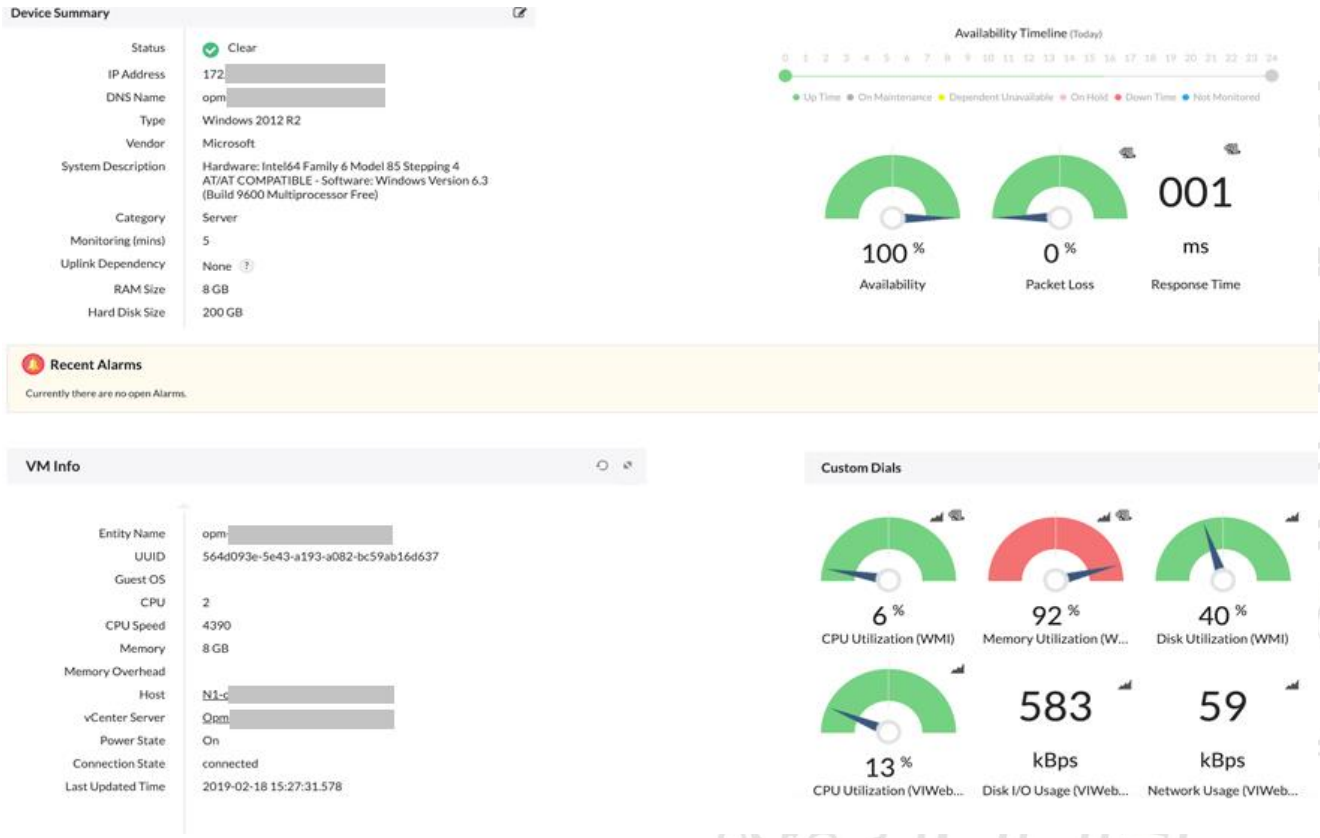


Ilustración 4. Ejemplo de rendimiento y consumo del ancho de banda.

Entre sus funciones se tiene:

- Software de gestión de infraestructura de redes y centros de datos para grandes empresas, proveedores de servicios y pymes.
- Flujos de trabajo automatizados, motores de alerta inteligentes, reglas de descubrimiento configurables y plantillas extensibles.
- Complementos para el cambio de red y la gestión de la configuración, la gestión de direcciones IP, así como la red, la aplicación, la base de datos, la virtualización y la supervisión del ancho de banda basado en NetFlow.
- La interfaz fácil de usar lo pone en funcionamiento rápidamente.

4.3. DNS (Domain Name System - sistema de nombres de dominio)

Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominio asignados a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. [6]
En su forma más básica, DNS es un directorio de nombres que coinciden con números. Los números, en este caso son direcciones IP, que las computadoras usan para comunicarse entre sí. [6]

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. [6]

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio Google es 216.58.210.163, la mayoría de la gente llega a este equipo especificando www.google.com y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable (ejemplo en Ilustración 5). [6]

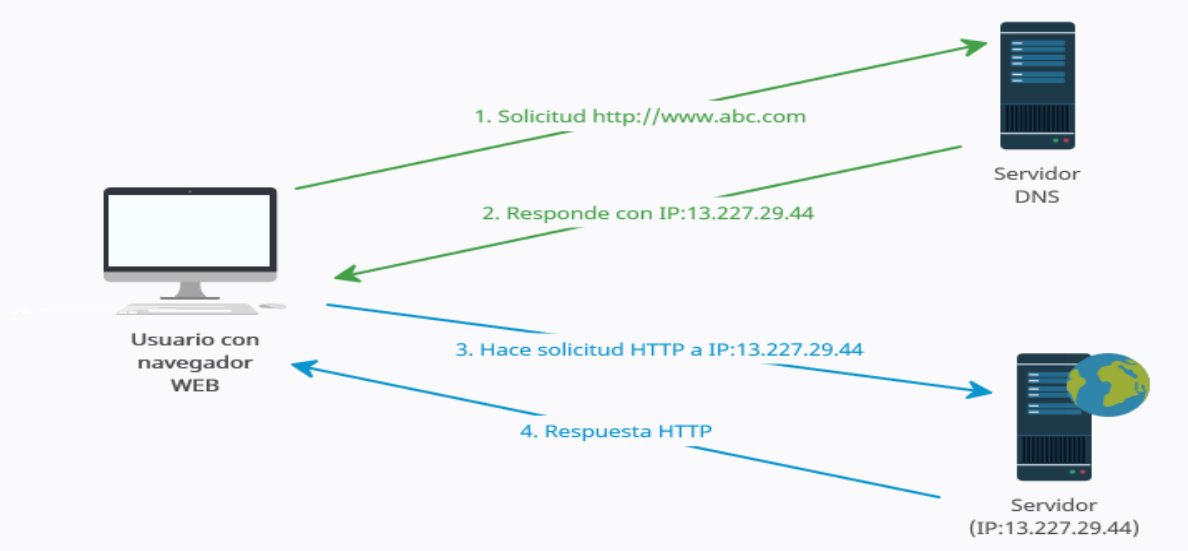


Ilustración 5. Breve ejemplo al ingresar a un sitio web un cliente.

En ese orden de ideas, el DNS, es el servicio usado por la compañía para asociar una IP, con un nombre de servidor o servicio usado. Por ejemplo, la IP 10.10.10.1 se asocia a un datáfono, que tiene el nombre de DataExito2.
De esta manera, mediante el uso de nombres en vez de direcciones IP, se logra identificar y localizar de manera más sencilla los dispositivos y servidores, aspecto clave en las labores de monitoreo ejecutadas por el servidor IPAM.

4.4. Firewall

Un firewall o cortafuego, es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permitir o bloquear tráfico específico (ver Ilustración 6) según un conjunto definido de reglas de seguridad.
Los cortafuegos han sido la primera línea de defensa en seguridad de redes durante más de 25 años. Establecen una barrera entre las redes internas seguras y controladas en las que se puede confiar y en las redes externas no confiables, como Internet. [7]

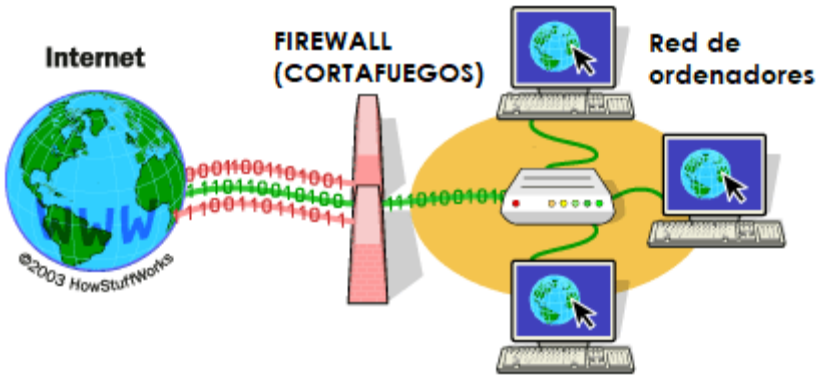


Ilustración 6. Esquema funcionamiento FIREWALL

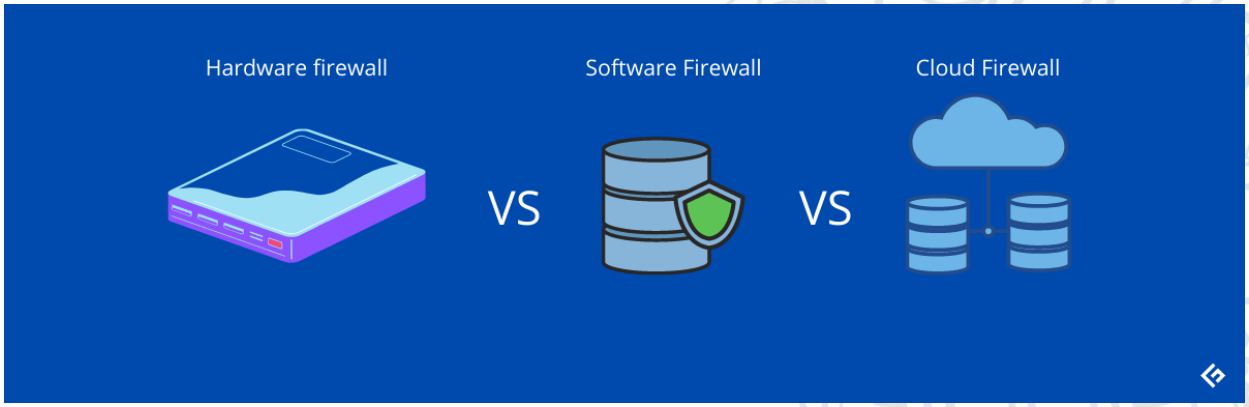
Un cortafuego puede ser hardware, software o nube (ver Tabla 1). Existen varios tipos de cortafuegos, entre los cuales están:

- **Cortafuegos proxy**: Uno de los primeros tipos de dispositivo de firewall, un firewall proxy sirve como puerta de enlace de una red a otra para una aplicación específica. Los servidores proxy pueden proporcionar funcionalidad adicional, como almacenamiento en caché de contenido y seguridad, al evitar conexiones directas desde fuera de la red. Sin embargo, esto también puede afectar las capacidades de rendimiento y las aplicaciones que pueden admitir.
- **Firewall de inspección de estado**: Ahora considerado como un cortafuego "tradicional", un cortafuego de inspección de estado permite o bloquea el tráfico según el estado, el puerto y el protocolo. Supervisa toda la actividad desde la apertura de una conexión hasta que se cierra. Las decisiones de filtrado se toman en función de las reglas definidas por el administrador y del contexto, que se refiere al uso de información de conexiones anteriores y paquetes que pertenecen a la misma conexión.
- **Firewall de gestión unificada de amenazas (UTM):** Por lo general, un dispositivo UTM combina, de una manera débilmente acoplada, las funciones de un firewall de inspección de estado con prevención de intrusiones y antivirus. También puede incluir servicios adicionales y, a

menudo, gestión de la nube. Los UTM se centran en la simplicidad y la facilidad de uso.

- **Cortafuego virtual**: Un firewall virtual generalmente se implementa como un dispositivo virtual en una nube privada (VMware ESXi, Microsoft Hyper-V, KVM) o en una nube pública (AWS, Azure, Google) para monitorear y asegurar el tráfico a través de redes físicas y virtuales. Un firewall virtual suele ser un componente clave en las redes definidas por software (SDN).

Tabla 1. Comparativa de diferentes cortafuegos. [8]



FIREWALL	¿QUE ES?	VENTAJAS	DESVENTAJAS
HARDWARE	Dispositivo físico instalado entre una red informática e Internet o en el borde de la red para monitorear paquetes de datos en tránsito es un firewall de hardware. El nombre también lo conoce del firewall perimetral, ya que protege toda su red al evaluar el tráfico entrante y saliente en el perímetro.	• Un solo firewall puede proteger su zona de red completa • La velocidad y el rendimiento permanecen intactos • Menos vulnerable a los ataques • Se integra fácilmente con otros sistemas de seguridad como equilibrio de carga, VPN, etc.	• Poco escalable.
SOFTWARE	Solución basada en software que se instala como un dispositivo virtual o en computadoras individuales en su red	• Asequible, incluso si opta por los firewalls mejor calificados • Económico para una oficina pequeña con sistemas limitados	• Utiliza más recursos, incluida la memoria y el espacio en disco, en

	para protegerlas contra vulnerabilidades. Puede controlar el comportamiento asociado con determinadas aplicaciones.	• Fácil de configurar y administrar • Puede determinar el nivel de protección durante su instalación y definir el nivel de seguridad en consecuencia para un usuario • Mejor control y flexibilidad para evaluar qué aplicaciones deben permitirse o bloquearse	comparación con los firewalls de hardware. • El rendimiento puede verse afectado según la velocidad del sistema • Necesita administración y actualización periódicas
NUBE	También se les conoce como Firewall-as-a-Service (FaaS). Forma una barrera virtual segura que rodea las plataformas, aplicaciones e infraestructura en la nube.	• Despliegue sencillo sin perder tiempo • Escalable de acuerdo con las necesidades de una organización • La mayor disponibilidad garantiza un flujo constante de servicios de seguridad, energía redundante y copias de seguridad automatizadas. • Protección de identidad porque son capaces de integrarse con controles de acceso, lo que brinda a los usuarios un mejor control sobre las herramientas de filtrado. • Mejor rendimiento, ya que puede controlar todo, desde la visibilidad, la configuración, el uso, el registro, etc. • En caso de cualquier problema, puede utilizar instantáneas y luego recuperar los estados deseados inmediatamente.	• La disponibilidad depende de la disponibilidad de la infraestructura de la nube. • Las funciones avanzadas pueden ralentizar su red. • A menudo considera casos de uso genéricos que pueden no ser eficientes para bloquear vulnerabilidades específicas de software como las de los complementos.

Ahora, es de tener en cuenta, que la compañía actualmente usa las 3 estrategias presentadas para proteger la infraestructura de red (hardware, software y nube). En los datacenter y como primera medida de protección usa tipo hardware, para los empleados en sus computadores, se tiene el de tipo software, y para los aplicativos de los usuarios (ejemplo Tuya Pay), se tiene seguridad en la nube.

Por lo tanto, el firewall es un mecanismo importante de protección contra intrusos, que desean acceder a la red de TUYA sin ser autorizados, entonces es necesario monitorear constantemente que su funcionamiento sea óptimo en todo momento.

Para el desarrollo de este proyecto, la interacción con este tipo de dispositivos (Firewall) es muy importante, ya que cada que se da un proceso de liberación de IP, se procede con la eliminación de reglas en el firewall. A través de este procedimiento se logra garantizar que las direcciones IP obtenidas, producto de la liberación, no tengan restricciones de tráfico y puedan ser asignadas a nuevos dispositivos sin presentar conflictos.

4.5. Automatización

La automatización de la TI, también denominada automatización de la infraestructura, consiste en el uso de sistemas de software para crear instrucciones y procesos repetibles a fin de reemplazar o reducir la interacción humana con los sistemas de TI. El software de automatización funciona dentro de los límites de esas instrucciones, herramientas y marcos para realizar las tareas con muy poca intervención humana. [9]

La automatización es clave para la optimización de TI y la transformación digital. Los entornos modernos y dinámicos de TI necesitan poder adaptarse más rápido que nunca, y la automatización de la TI es fundamental para que esto sea posible. [9]

De allí surge una pregunta, ¿cómo implementarlo?... En teoría, se puede aplicar cierto nivel de automatización a cualquier tarea de TI. Por lo tanto, la automatización puede incorporarse y aplicarse a cualquier elemento, desde la automatización de la red hasta la infraestructura, la implementación de la nube y los entornos operativos estándares (SOE), e incluso a la gestión de la configuración y la implementación de aplicaciones. [9]

Las aplicaciones y las funciones de automatización pueden extenderse hasta abarcar tecnologías específicas, como los contenedores; metodologías, como DevOps (acrónimo inglés de Development/Operations, Desarrollo/Operaciones); y áreas más amplias, como la nube, la seguridad, las pruebas y la supervisión o las alertas. [9]

Para nuestro caso, tenemos una automatización a nivel de tareas, ya que con la herramienta OpManager, se logra monitorear en tiempo real, los cambios que se producen al interior de la red y también, se tiene una visualización global del estado en que se encuentra una dirección IP, para así poder tomar decisiones al respecto sobre su uso.

4.6. VLAN (red de área local virtual)

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Las VLAN son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador). [10]
Una VLAN consiste en dos o más redes de computadoras (ver Ilustración 7) que se comportan como si estuviesen conectados al mismo conmutador, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local.

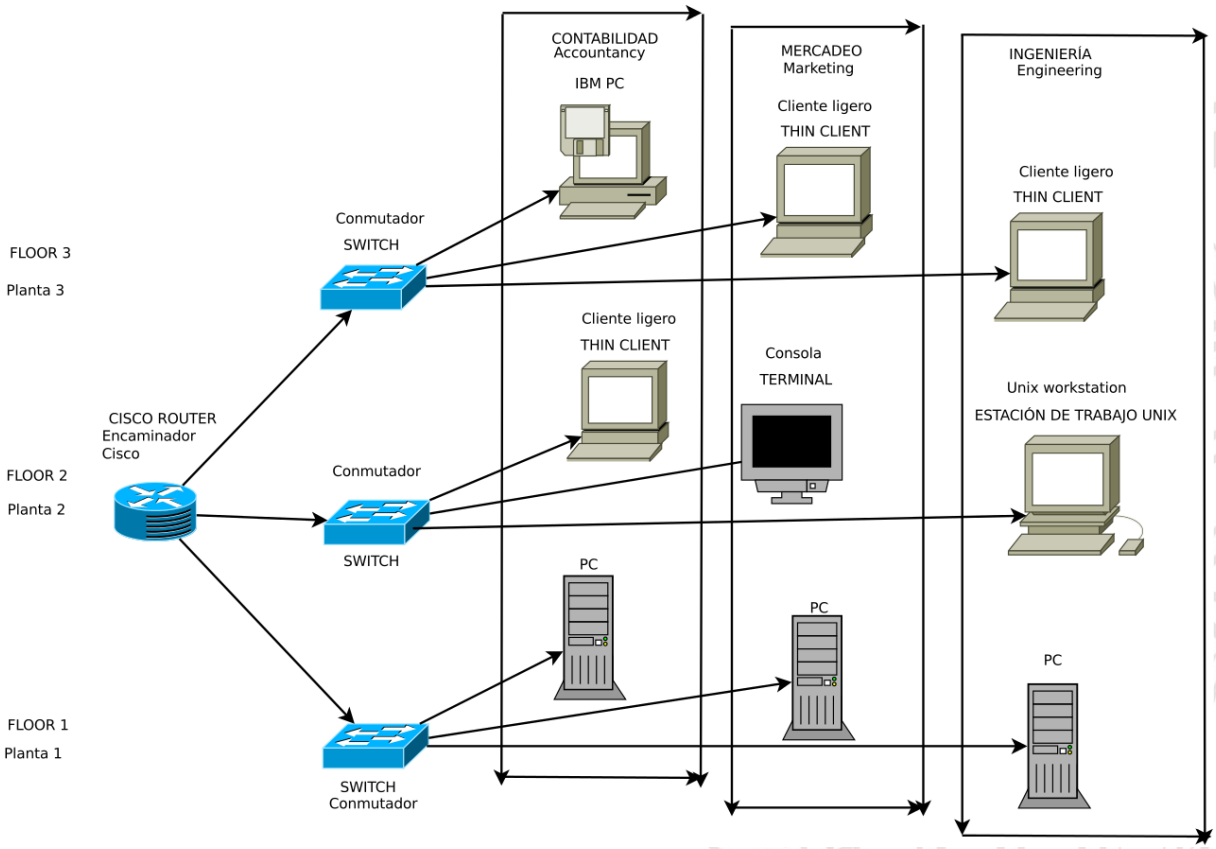


Ilustración 7. Diagrama VLAN [10]

En la compañía, se tienen separados algunos rangos de direcciones IP, con el objetivo, de no generar interferencias entre algunas áreas de trabajo y así, administrar mejor los recursos, permitiendo la adecuada continuidad del negocio y disminuir al máximo las posibles fallas de servicio. Nuestro enfoque de trabajo, es centrarnos en las VLAN: 4,50 y 327; las cuales pertenecen a la granja de servidores, que son las más usadas en la actualidad.

Capítulo 5: Desarrollo de la propuesta

En el desarrollo de este apartado, fue necesario la intervención de varias áreas de la empresa, entre las cuales se destacan las siguientes:

- Se involucró inicialmente a INTERGRUPO, empresa aliada encargada de brindar apoyo con la gestión de la asignación del direccionamiento IP.

- Posteriormente, se tuvo en cuenta al área de seguridad, división a cargo de la configuración de reglas del firewall, restricciones a usuarios, proxy, vpn, entre otras políticas de acceso a aplicativos.
- Por último, se obtuvo información del proceso de verificación y registro de actividad en la CMDB (base de datos de la gestión de configuración).

Con la información recolectada por el personal encargado, se logró obtener datos del funcionamiento de la infraestructura de red.

5.1. Esquema de asignacion de direccionamiento IP antiguo

Inicialmente, el usuario que desea o requiere la asignacion de una direccion IP, ya sea una nueva o para la solucion de algun problema, se genera un SR (Solicitud de Requerimiento), en la intranet de la compañía, de la siguiente forma: (Sarita –Ilustración 8)

Ilustración 8. Solicitud de requerimiento de IP en la plataforma SARITA

Una vez se genera un SR, la solicitud se envía a los encargados del área de Telcos de tuya, donde se revisa manualmente si la solicitud es adecuada. En el proceso de revisión, el analista de Telcos que recibe el caso, analiza cual es

el problema a solucionar, para poder escalarlo adecuadamente al área de ciberseguridad y luego miran a cuál VLAN pertenece. Esto se hace, para tener certeza de cuál ámbito se elimina la IP y obtener un histórico del uso de estos recursos. Posteriormente, se delega el caso a los colaboradores de INTERGRUPO.

Al recibir la solicitud del usuario, los campos obtenidos de la plataforma, se actualizan en una hoja de cálculo con los siguientes campos (Ver Tabla 2). Es importante resaltar que los encargados de actualizar o modificar la tabla 2 son el área de Telcos y/o INTERGRUPO.

Tabla 2. Detalle de campos hoja de calculo

Ticket	**Descripción**	**Usuario afectado**	**Tipo**	**Grupo del caso**	**Fecha creación**	**Fecha solución**	**Usuario resolutor**	**Cumple SLA solución**	**Método solución**	**Detalle del caso**
SR…	Ej: Gestión direccionamiento	Ej: sis1xxx	SR o IN	C-xxx-CO-telcos	Dd/mm/aaaa	Dd/mm/aaaa	Sis1xxx	Si/no	xxx	xxx

- Ticket: número interno se solicitud. Inicia con SR (Solicitud de Requerimiento) o IN (Incidente) y finaliza con 6 números.
- Descripción: se informa a cuál área se remite el caso.
- Usuario afectado: nombre de usuario que ha sido afectado, o que hizo la solicitud (hay un campo para especificar en caso que sea diferente). La designación es sis1xxx.
- Tipo: SR es requerimiento, IN es incidente.
- Usuario resolutor: nombre de usuario quien soluciona el SR o IN.
- Cumple SLA solución: después de que los analistas revisen el caso, se marca si se puede solucionar o no es viable.
- Método solución: manifiestan brevemente, como solucionaron el caso.
- Detalle del caso: se detalla cual es la causa de la solicitud.

Posteriormente, se hace una revisión manual de la solicitud del cliente, y luego, en otra hoja de cálculo (ver Tabla 3), se revisa cuales direcciones están disponibles para asignar, cual se debe modificar o actualizar y poder proceder con la solución del problema y la asignación de la dirección IP.

Tabla 3. Reporte asignación IP

ESTADO	Fecha de Retiro	IP	DISPOSTIVO ASIGNADO	OBSERVACIONES	FECHA ASIGNACIÓN	PERSONA SOLICITANTE	VLAN	SUBRED	MASCARA	DEFAULT GATEWAY	DESCRIPCIÓN VLAN
Activa		10.0.0.0	Router	detalle	Dd/mm/aaaa	nn	#	10.0.0.0/24	255.250.0.0	10.0.0.1	CEOH

A continuación, se brinda una breve descripción para algunos de los campos mencionados en la tabla 3.

- Estado: activa o liberada.
- IP: dirección ip para asignar al dispositivo
- Dispositivo asignado: tipo de servidor o dispositivo
- Observaciones: descripción de ruta de acceso, SR, usuario o cualquier información necesaria para usar el servidor.
- VLAN: número de vlan donde se asigna la dirección IP.
- Subred: dirección de red, que va ligada a la VLAN anterior.
- Descripción VLAN: cada vlan está asignada a un ámbito específico de la empresa.

Para el caso de una nueva asignación, se escoge alguna IP de la lista que tenga el estado de "Liberada". Posteriormente, se procede a usar herramientas de escaneo de direcciones IP, para validar si hay ping (utilidad de diagnóstico que comprueba si el dispositivo continúa activo) o alguna respuesta del DNS.

Luego, se valida con el área de seguridad, si existen reglas vigentes o antiguas en el firewall, ante una determinada IP, para así, ver si realmente está disponible la IP y se puede usar. Esta verificación es necesaria ya que, en muchas ocasiones, liberan una IP, pero dejan reglas en el firewall activas o

restricciones de algún tipo, debido a su antigua asignación en algún servidor en específico (cada dirección IP, tiene permisos diferentes).

A continuación, se presenta en la Ilustración 9, un diagrama que resume el flujo de trabajo utilizado en el proceso de asignación de IPs.

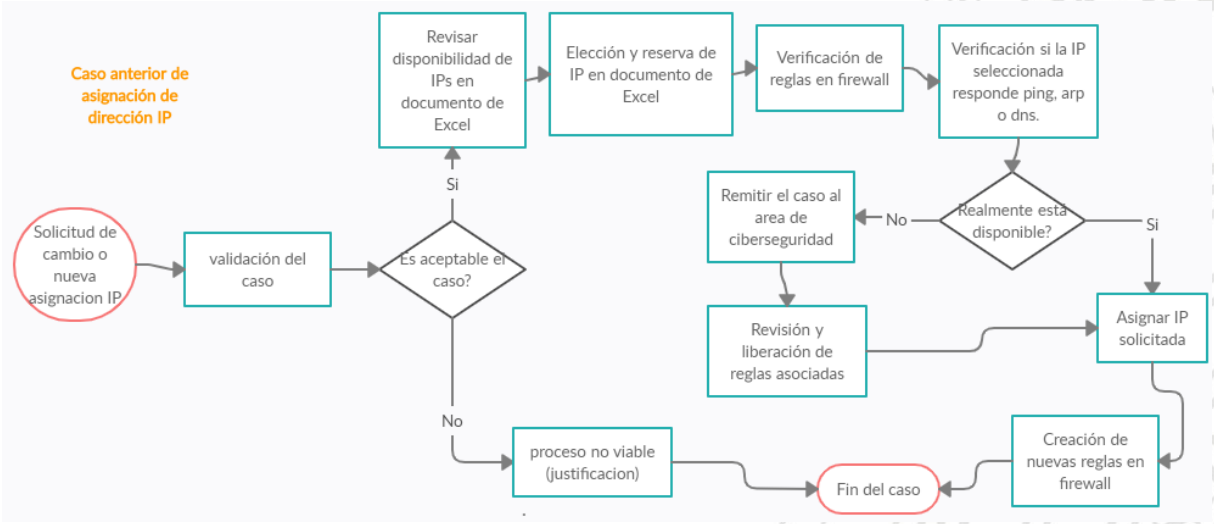


Ilustración 9. Asignación de direccionamiento IP antiguo.

5.2. Esquema de liberación para una dirección IP antiguo

Anteriormente, los procesos que se realizaban para la gestión de direcciones IP en la granja de servidores, no eran eficientes y dificultaban notablemente su gestión (ver Ilustración 10). Por ejemplo, se tenía los siguientes procesos para dar de baja un recurso IP (específicamente eliminar una IP):

- Enviar un correo a la persona a cargo de analizar y autorizar la eliminación de una IP.
- Esta persona, remite el caso al área seguridad, quienes proceden a enviar la solicitud a una empresa aliada que se encarga de eliminar políticas restrictivas asociadas.
- Finalmente, el área de Telcos o Intergrupo, quita la IP de la hoja de cálculo.

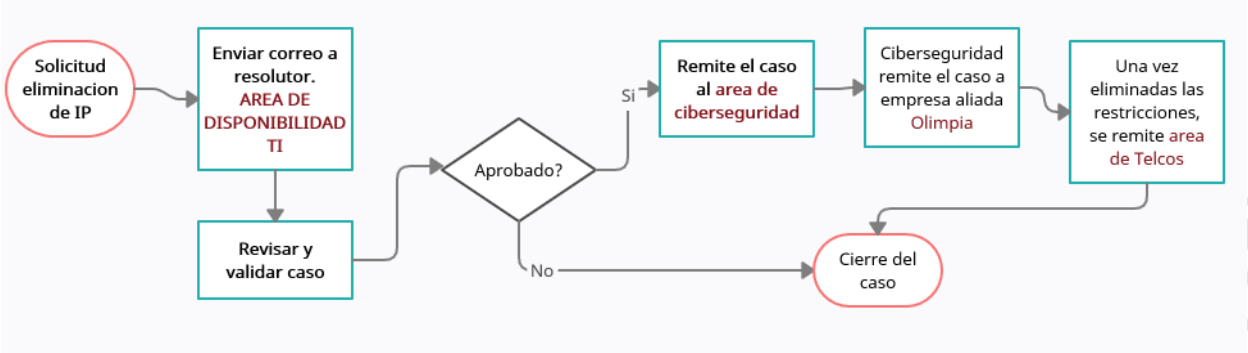


Ilustración 10. Flujo para la liberación de una dirección IP en el esquema antiguo.

Es importante resaltar que en el flujo mostrado (ver Ilustración 10), existe una falla. Antes del cierre de caso, después del área de Telcos, éste debería ser remitido al área gestión de configuración, para eliminar la dirección IP de la base de datos; y al área de nube, para eliminar los recursos asociados al dispositivo si es el caso. Vale la pena aclarar, que, al momento de asignar una IP, INTERGRUPO validaba si había reglas activas en dicho recurso. En caso de ser afirmativo, se remitía el caso al área de nube o al área de gestión de configuración, o a ambos si es requerido, para que ellos eliminaran dichas reglas asociadas.

Como se puede apreciar, el proceso existente no lograba centralizar la información, ni tener un monitoreo adecuado, provocando que las tareas de eliminación, como de cambio de IP, no se lograran en su totalidad. Además, al hacer el análisis del proceso de asignación y liberación de direcciones IP, se llega a la conclusión, que, con el área de seguridad, no es posible que el proceso de eliminación de restricciones, se pueda automatizar completamente. La razón de esto, es debido al uso de un proveedor externo que realiza tareas específicas, dificultando así, lograr la independencia y autogestión deseada.

A partir del contexto presentado en las secciones 5.1 y 5.2, este trabajo propone una estrategia para la gestión del direccionamiento IP, con el propósito de evitar reprocesos y reducir los errores.

5.3. Implementación del servidor IPAM

La implementación del servicio IPAM se logra hacer en un servidor Windows alojado en la nube de Azure, donde con la ayuda conjunta del personal de soporte de OpManager y analistas del área de ciberseguridad de TUYA, se logra hacer la instalación y configuración de los componentes necesarios para su adecuado uso.

Los requisitos mínimos de hardware pueden variar según la carga, pero a modo general, para el equipo de instalación, lo inicial es:

- Procesador - Intel Core i3 (2 core/4 thread) 2.0 Ghz 3 MB cache
- Tamaño de RAM - 2 GB
- Espacio en disco - 10 GB
- Versión del sistema - sólo equipos de 64 bit

Ahora, para entender la automatización del componente de IPAM, se muestra a continuación la manera de configurar el escaneo diario de la infraestructura de red.

Inicialmente, ingresamos a la herramienta OpManager, en el apartado settings > IP address manager > Scheduler > Add task. (Ver Ilustración 11)

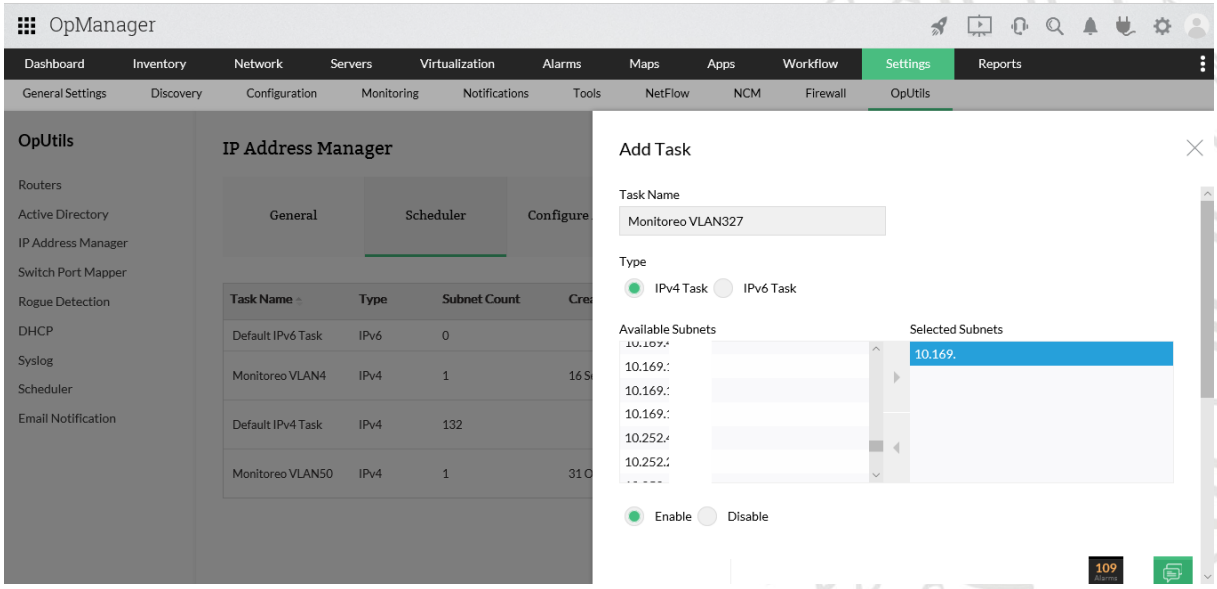


Ilustración 11. Asignación de tareas de monitoreo en VLAN.

Con la anterior ilustración, se aprecia que se debe colocar un nombre de tarea en la sección "Task Name", luego en "Type", seleccionar si es protocolo IPV4 o IPV6 el que se desea escanear, y luego, de las subredes disponibles, selecciono la dirección de red que deseo usar para monitorear diariamente; basta con colocar luego, el día o días y la hora de ejecución. Con esto, se logra la automatización del monitoreo de las tres VLAN (4,50,327) (ver Ilustración 12), que son las de la granja de servidores y por el momento solo se probará con estas, debido a que son las VLAN que más cambios en configuración están experimentando. Posteriormente, la idea, es replicar esta labor, a las demás VLAN y también a los servidores en nube.

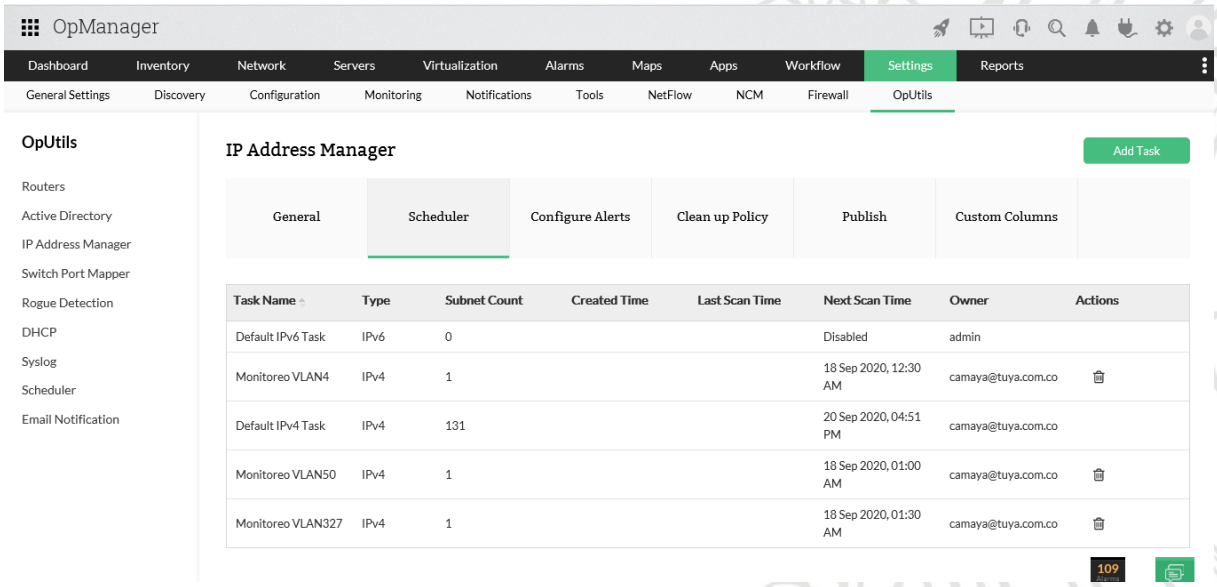


Ilustración 12. Resumen VLAN monitoreadas

5.4. Esquema de asignación de direccionamiento IP implementado.

Inicialmente, el proceso no cambia con respecto a lo expuesto en la sección 5.1. La solicitud se realiza por medio del software sarita de la intranet, donde se reporta un daño, nueva asignación o cualquier otro tipo de incidente.

Posteriormente, cuando el caso es recibido por el encargado del área de Telcos o Intergrupo, se procede a hacer la reserva en el software OpManager,

herramienta de monitoreo implementada, lo que permite asignar los siguientes campos (Ver Ilustración 13).

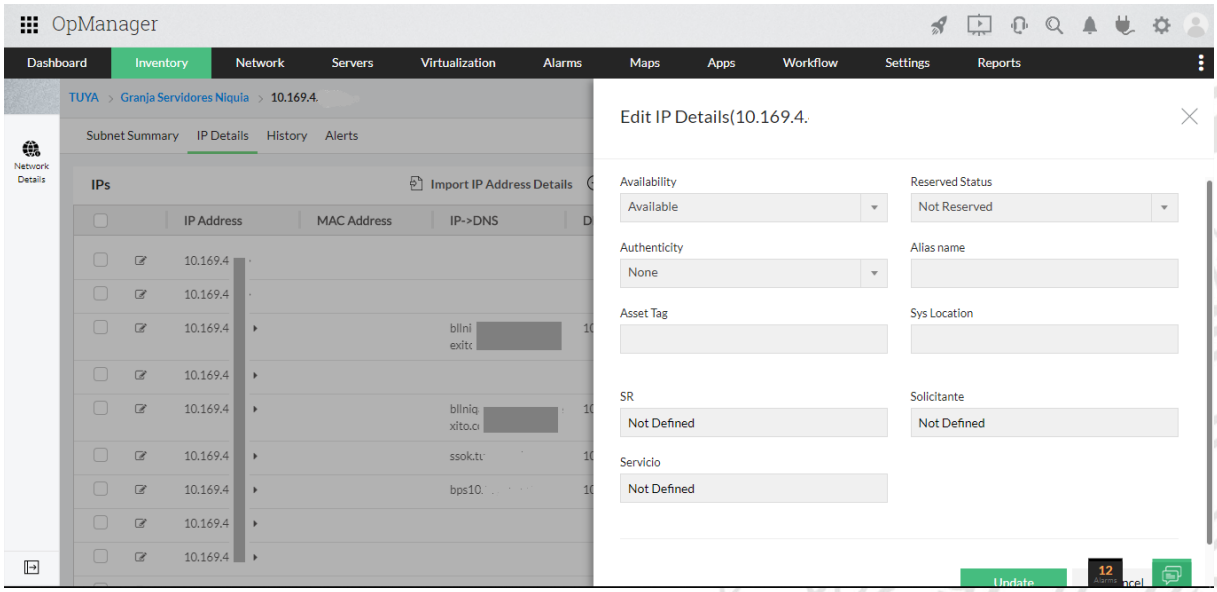


Ilustración 13. Asignación de IP a un servidor específico.

A continuación, se presenta una breve descripción de los campos a diligenciar en la anterior Ilustración 13.

- Availability: El modo en el cual va a estar la dirección IP seleccionada. Los modos son los siguientes: disponible, en uso o en transición.
- Reserved status: En este caso solo está el modo "reservada estáticamente", ya que no se usa DHCP.
- Authenticity: es el tipo de usuario que hará uso del servidor, ya sea un usuario invitado, externo o de la compañía.
- Alias name: nombre asignado para identificar a un usuario.
- Los campos SR, Solicitante y Servicio, son campos personalizados, necesarios para la compañía.

Luego de llenar los anteriores datos, se procede a dar clic en update.

Nota: Todas las direcciones IP que aparecen en la lista, fueron escaneadas previamente, para revisar su estado, ya sea disponible o en uso.

Posteriormente, cuando la IP estática se asigna al dispositivo requerido, el caso se cierra (llamado SR000000) en sarita (software de servicio al cliente), disponible en la intranet. Para complementar, la asignación de la dirección IP se realizará físicamente en el datacenter, si es un dispositivo físico; o de manera

remota, si la asignación se hace para un recurso en la nube. En dicha labor, está involucrada la empresa INTERGRUPO o algún analista del área de Telcos. En la Ilustración 14, se muestra el flujo de trabajo obtenido para la asignación del direccionamiento IP a partir de las modificaciones realizadas.

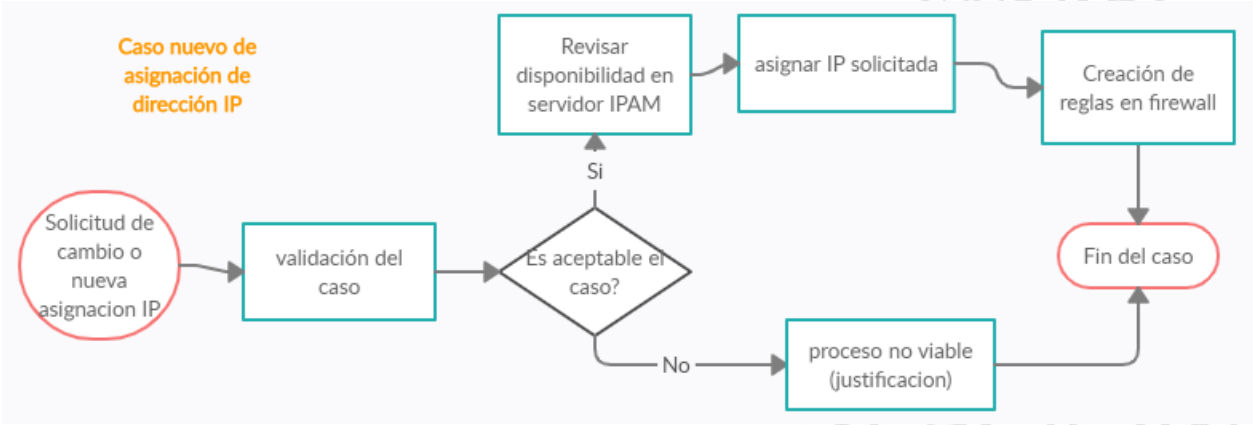


Ilustración 14. Asignación de direccionamiento nuevo.

Adicionalmente, para lograr que la herramienta en mención, logre mostrar la información adecuadamente, se hizo la implementación de una nueva oferta de servicio en la intranet para el proceso de liberación - baja de un servidor IP.

5.5. Complemento "liberación de IP, plataforma SARITA".

Teniendo presente lo anterior, no existía una categoría disponible en la mesa de ayuda de Sarita, que permitiera generar la solicitud adecuada de liberación de IP, ya que todo se hacía por correo. En muchas ocasiones no se lograba dar a conocer el proceso que se llevaba a cabo a todas las áreas involucradas, haciendo que muchos procesos no se concluyeran en su totalidad y hacía que el monitoreo no arrojara datos completamente actualizados, haciendo de esta, una mala gestión del direccionamiento IP.

Para dar solución completa a lo propuesto en los objetivos, se realizó la gestión de crear una nueva oferta o categoría, llamada "Baja-liberación Servidor", como se ve en la siguiente Ilustración 15:

Ilustración 15. Oferta de liberación IP o baja de servidor.

En la anterior Ilustración 15, se aprecia los campos que necesita llenar el usuario que desee dar de baja un servidor.

- En la sección justificación, se explica la necesidad o razón que sustenta el por qué se desea liberar una dirección IP en específico, y posteriormente el área de disponibilidad de TI, aprueba o rechaza dicha justificación.
- En la parte de nombre del servidor, se especifica el nombre que se le ha dado al servidor en mención. Cada analista tiene conocimiento del nombre asignado a un determinado servidor, y cada nombre se asocia con su respectiva IP, donde entra en acción el servidor DNS.
- En la sección "IP del servidor", basta solo con colocar la dirección IP y ya con ese dato, al verificar en la base de datos, se conoce a cuál VLAN pertenece.

Con los anteriores datos, se logra obtener todo lo necesario para poder dar de baja el recurso IP. Es importante aclarar, que, dentro de la oferta, se generan flujos de trabajo, donde la información llega a todas las áreas encargadas (ver Ilustración 16), lo cual, permite eliminar la IP en la base de datos, firewall, nube y en el dispositivo.

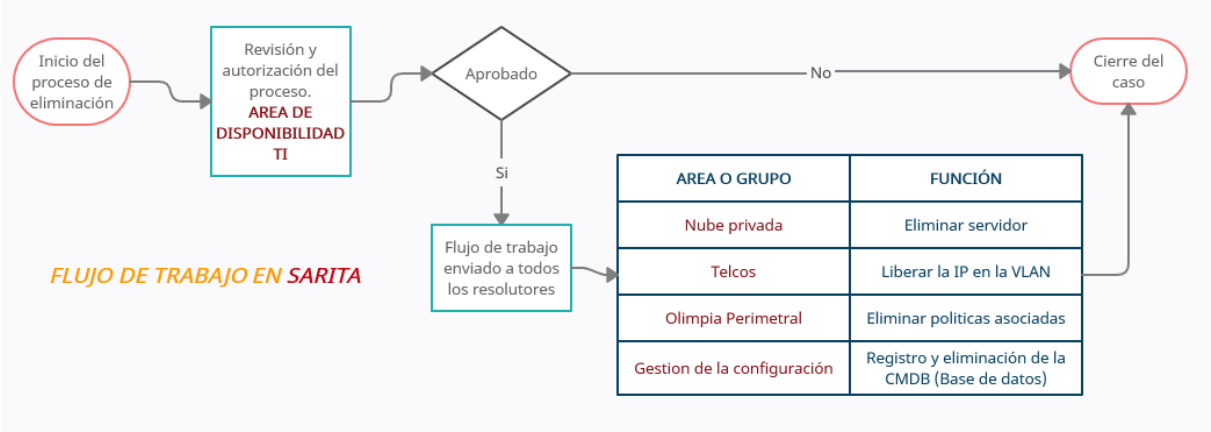


Ilustración 16. Flujo proceso de eliminación IP.

Además, el usuario tiene la opción de liberar una IP de manera temporal o definitiva, ya sea para cambiar de dispositivo o para poder hacer pruebas, haciendo que la administración y monitoreo del direccionamiento sea de manera centralizada, que las áreas involucradas tengan pleno conocimiento de los procesos que se llevan a cabo y evitar así errores de funcionamiento.

Capítulo 6: Resultados y análisis

6.1. Verificación del funcionamiento del servidor IPAM

Una vez en funcionamiento el servidor IPAM, se procede a revisar en la utilidad "IP Usage Summary", donde se revela claramente cuantas direcciones IP están en uso o cuales disponibles a modo general, como se ve en la siguiente imagen (Ilustración 17). Por ejemplo, en el apartado de la sección NAME, donde se muestra el nombre de la VLAN, se puede ver que el pool de direcciones es de 254 IPs en total, con 65 disponibles, 187 en uso y 2 en transición, este último, debido a que no se ha liberado completamente o se deshabilitó temporalmente.

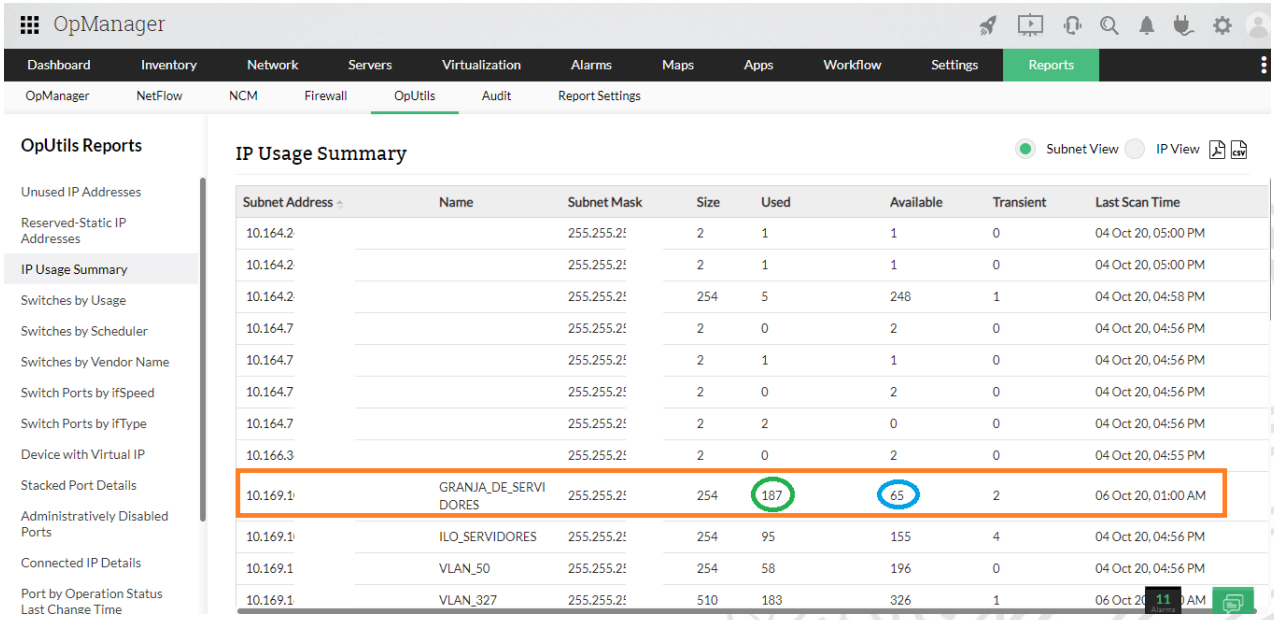


Ilustración 17. Resumen de uso de las direcciones IP.

Ahora, se aprecia en mayor detalle (ver Ilustración 18), cuáles son las direcciones IP disponibles para usar (por seguridad se cubren datos sensibles).

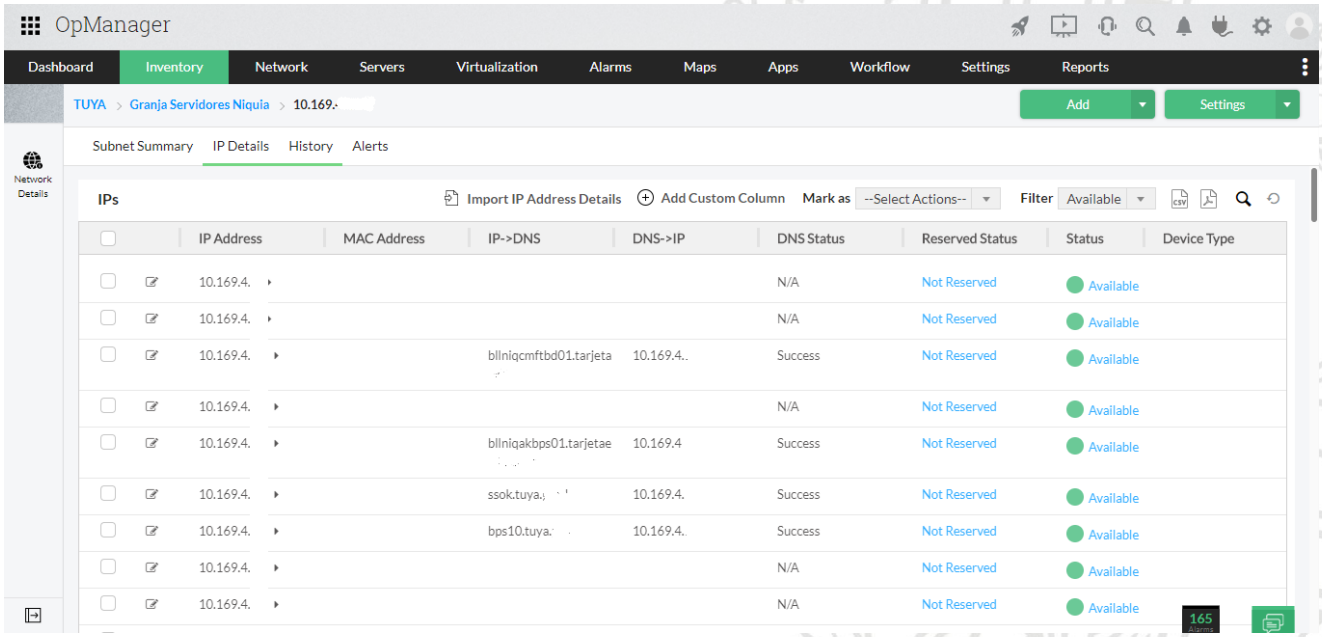


Ilustración 18. Direcciones IP disponibles.

De igual forma sucede con las direcciones IP que están en uso (ver Ilustración 19), al hacer un adecuado filtro, fácil de usar con esta herramienta, se logra ver cuales direcciones no se pueden usar.

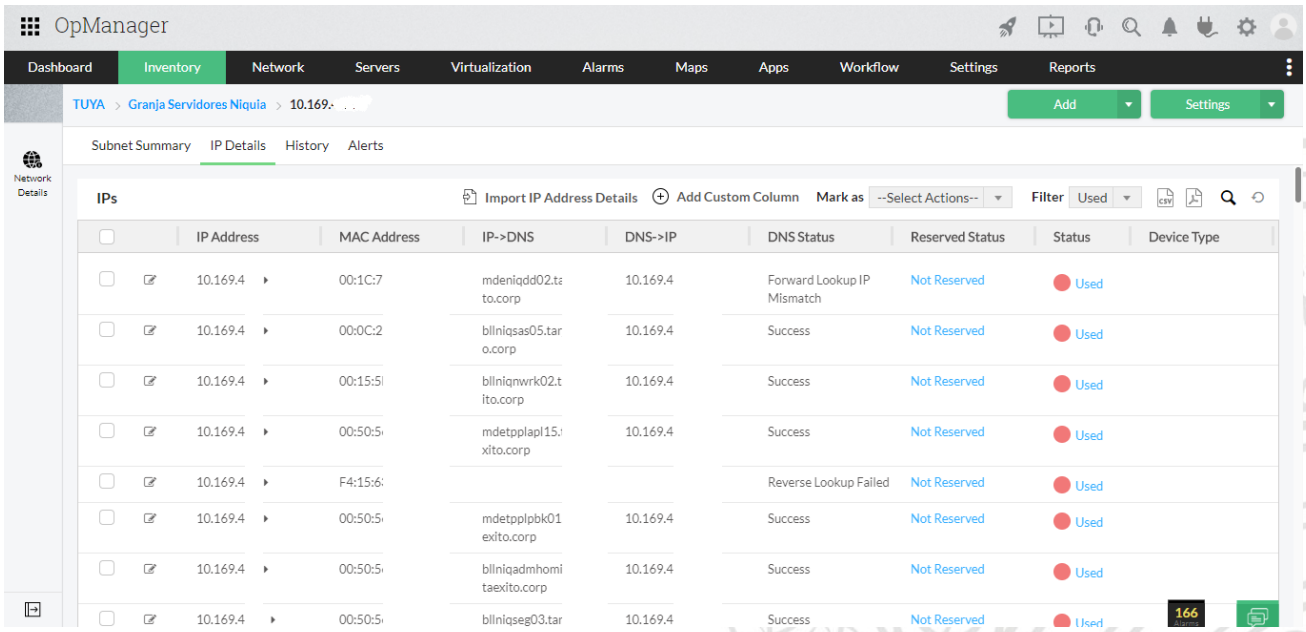


Ilustración 19. Direcciones IP en uso.

6.2. Comparativa de los procesos de asignación de direccionamiento.

Si observamos la Ilustración 9 y la Ilustración 14, las cuales hacen referencia al proceso que se realizaba antes para la asignación de una dirección IP, versus como está actualmente el proceso; claramente, se puede apreciar la mejora alcanzada en la reducción de los procesos que se requerían.

Antes el proceso involucraba aproximadamente 6 actividades a revisar, mientas que ahora solo se requieren 3 pasos para asignar el recurso IP a un servidor.

Es importante destacar que, gracias al proceso de automatización, ya no es necesario usar la hoja de cálculo para mirar disponibilidad, ni para hacer la reserva. Todo el proceso se hace de manera centralizada desde el software OpManager, gracias al servidor IPAM, donde se monitorea de manera automática, diariamente, cuales direcciones están disponibles o en uso.

De igual manera ya no es necesario realizar los procesos de verificación de IP asociados con tareas como IPScan, verificación de conectividad vía ping, arp, o resolución de nombres vía DNS; para luego proceder con su respectiva solución o escalación al área de ciberseguridad.

Ahora con el método actual (ver Ilustración 18), solo es necesario ir al apartado que dice "Filter" en el dashboard de la plataforma de monitoreo, y seleccionar la opción "Available", donde despliega el listado de direcciones IP que están disponibles para usar. Además, si el analista desea hacer una revisión adicional, se puede nuevamente verificar en una dirección IP, si existe una respuesta vía ping, dns o arp, en la misma herramienta, sin necesidad de usar otro aplicativo adicional.

En conjunto, todas estas nuevas características implican una mejora en el tiempo de asignación o solución de un incidente, por parte de los equipos de TI.

Capítulo 7: Conclusiones

1) Mediante la evaluación de características y requisitos básicos que la compañía exige y apoyándonos en el documento previamente elaborado, se eligió el software de monitoreo que mejor se ajustó a los requerimientos de la empresa, logrando una adecuada relación costo-beneficio.
2) Al mejorar el proceso de dar de baja los servidores, por ende, mejora el reporte de disponibilidad de direcciones IP que brinda el servidor IPAM. El trabajo en conjunto entre el servidor IPAM y la nueva oferta de liberación de IP, es el método adecuado para obtener información actualizada y confiable, sobre el uso de los recursos de red. Con esto se logró, que en la asignación de direcciones IP, se tenga certeza que no hay problemas de incompatibilidad con otros servicios usados anteriormente por una IP especifica.
3) Se mejoró sustancialmente el trámite de asignación y liberación de las direcciones IP, logrando entregas y soluciones mucho más eficientes, con menor probabilidad de errores y obteniendo un mejor monitoreo de la red.

4) Debido a que cada recurso IP que se asigna a un servidor, tiene diferentes restricciones y permisos, no es posible automatizar reglas en el firewall para asignar genéricamente.

Capítulo 8: Trabajo futuro.

- Se logró automatizar la mayor parte del proceso, sin embargo, por políticas de seguridad y otras dependencias de la empresa, las cuales están involucradas en el proceso tanto de asignación de direcciones IP, como de auditoría y control, no fue posible lograr una automatización al 100% en el proceso.
- Con el análisis y estudio de las herramientas usadas, se pretende escalar la solución IPAM a la nube, mejorar el monitoreo de las VPN, todo lo que comprende la seguridad activa y pasiva de la compañía, y, además, hacer un descubrimiento y monitoreo completo de las 10 mil direcciones IP que posee la compañía.

Capítulo 9: Referencias Bibliográficas (Cibergrafía)

1] RFC 791 - Internet Protocol. (2020). Retrieved 11 August 2020, from https://tools.ietf.org/html/rfc791

2] Máscara de red. (2021). Retrieved 18 January 2021, from https://es.wikipedia.org/wiki/M%C3%A1scara_de_red

3] *Duran, J. (2021). Pequeña y mediana empresa. Retrieved 18 January 2021, from https://es.wikipedia.org/wiki/Peque%C3%B1a_y_mediana_empresa*

4] México, M., 2020. *Oputils Características ¿Qué Es IPAM? | Manageengine México*. [online] Manageengine.com.mx. Available at: <https://manageengine.com.mx/oputils/caracteristicas/que-es-ipam> [Accessed 13 October 2020].

5] ManageEngine, c., 2020. *Network Monitoring Software | Network Monitoring Solutions – Manageengine Opmanager*. [online] Manageengine.com. Available at: <https://www.manageengine.com/network-monitoring/> [Accessed 13 October 2020].

6] Es.wikipedia.org. 2020. *Sistema De Nombres De Dominio*. [online] Available at: <https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio> [Accessed 13 October 2020].

7] Services, P., 2020. *What Is A Firewall?*. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html> [Accessed 13 October 2020].

8] Pathak, A. (2020). Diferencia entre hardware, software y firewalls en la nube. Retrieved 6 November 2020, from https://geekflare.com/es/hardware-vs-software-cloud-firewall/

9] Automatizacion REDHAT. 2020. *¿Qué Es La Automatización?*. [online] Available at: <https://www.redhat.com/es/topics/automation/whats-it-automation> [Accessed 13 October 2020].

10] Corletti Estrada, A. (2021). VLAN. Retrieved 14 January 2021, from https://es.wikipedia.org/wiki/VLAN