Trabajo Fin de Grado
Ingeniería de las Tecnologías de Telecomunicación

Integración de sedes en una red corporativa utilizando ITIL

Autor: Assumpta María Cabral Otero
Tutor: Rafael María Estepa Alonso

Dpto. Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2020

Proyecto Fin de Carrera
Ingeniería de Telecomunicación

Integración de sedes en una red corporativa utilizando ITIL

Autor:
Assumpta María Cabral Otero

Tutor:
Rafael María Estepa Alonso
Profesor titular

Dpto. de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2020

Proyecto Fin de Carrera: Integración de sedes en una red corporativa utilizando ITIL

Autor: Assumpta María Cabral Otero

Tutor: Rafael María Estepa Alonso

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2020

El Secretario del Tribunal

A mi madre

A mi familia

A mis amigos

Agradecimientos

Y llegó el ansiado final.

Tras años de esfuerzos se termina una etapa donde cada día suponía una nueva lección y un impulso a seguir adelante.

A mi mayor apoyo, la que ha estado siempre animándome a lograr lo que me propusiese, mi madre, la razón por la que he llegado tan lejos y por la que seguiré luchando siempre. Gracias por cada historia, cada risa, por todos los consejos y por el esfuerzo que ha supuesto llegar a donde estamos. Nunca sería quién soy si no fuese por ti.

A toda mi familia por creer en mí. A mi hermano, mis primos, mis tíos y abuelos, en especial a mi abuelo Alfonso, razón por la cual estudié Ingeniería, por seguir sus pasos, siempre comentando que, aunque es un camino duro, siempre merecerá la pena.

Mis amigas del colegio, por los recuerdos y reencuentros como si nunca hubiese cambiado nada, por ser un hogar al que volver siempre que uno se pierda. Mi mejor amiga, Ana, por lo vivido, por lo sufrido, porque solo tu y yo sabemos lo que es que una persona se convierta en parte de ti, el tener una confianza y un vínculo tan fuerte que el llamarte hermana no se me haga extraño.

He tenido la suerte de conocer a tantísimas personas increibles en estos años de carrera, todas ellas únicas, que me han acompañado en el día a día, enseñándome que, tras un largo día de estudio, una cerveza con amigos puede darle la vuelta a todo. Aunque todo haya cambiado, aunque estemos en distintas ciudades, paises o continentes, Sevilla siempre nos unirá.

A los profesores que les gusta su profesión, que se preocupan de que los estudiantes aprendan, no todo es aprobar, y que siguen dándolo todo para que los estudiantes un día podamos llegar a decir que lo hemos conseguido.

Mis compañeros de trabajo, que sin dudarlo son mucho más que eso, con ellos da gusto ir a la oficina sabiendo que siempre habrá una sonrisa y apoyo cada vez que sea necesario. Por enseñarme todo lo que se y por mostrarme que, con risas, buen ambiente y esfuerzo, esta nueva etapa también va a ser inolvidable.

Assumpta Cabral Otero

Sevilla, 2020

Resumen

En la actualidad, todo entorno de la Tecnología de la Información (IT) se encuentra en constante evolución, desde la sustitución de antiguas tecnologías hasta mejoras necesarias para cumplir las nuevas regulaciones, siendo imprescindible desarrollar nuevas soluciones que satisfagan las distintas demandas del negocio que vayan surgiendo.

El presente documento tiene como objetivo el despliegue y mantenimiento de la infraestructura completa de una sede, en la que se desean potenciar los servicios corporativos en la red corporativa además de su mejora en la integración con el resto de la Intranet de dicha empresa.

Durante el proyecto se desarrollará la solución más adecuada para la implementación de esta red, en donde se definirán las distintas fases por las que pasará el proyecto para llegar a la unificación con la red corporativa. Entre estas fases encontraremos la toma y análisis de los requisitos solicitados, diseño de la red y su despliegue, además de proporcionar las distintas herramientas para su posterior monitorización y soporte.

Para este trabajo nos basaremos en la metodología de ITIL (Information Technology Infrastructure Library) que ofrece un conjunto de pautas para la gestión del cambio de manera que se lleven a cabo y se les dé prioridad de manera eficiente sin que los niveles de servicio se vean afectados.

Se expondrán los distintos dispositivos utilizados, características, además de la configuración utilizada a la hora de estructurar una red funcional que cumpla los requisitos pautados con el cliente.

Abstract

Nowadays, every IT enviroment is under constant evolution, from the substitution of old technologies to needed improves in order to meet the new regulations, which remains a key channel to develope new solutions that satisfy the upcoming business demands.

The aims of the present document are the deployment and maintenance of the whole infrastructure in a Branch office, in which it's desired to enhace the corporative services in the network in addition to the improvement of the integration with the rest of the Intranet of the business under consideration.

For this task, we'll be based on the ITIL (Information Technology Infrastructure Library) methodology, which offers a set of patterns for the management of modifications, assigning a higher priority in a efficient way, and without interrupting service levels.

The devices involved, as well as their features and the configuration used when structuring a functional network that meets the agreed requirements will also be exposed.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE CÓDIGO

1 INTRODUCCIÓN Y OBJETIVOS

"*Las masas humanas más peligrosas son aquellas*
en cuyas venas ha sido inyectado el veneno
del miedo, del miedo al cambio."
Octavio Paz

Las infraestructuras de las Tecnologías de la Información (IT), especialmente en el mundo empresarial, se encuentran en constante evolución. Esta es la base de cualquier organización para la gestión y procesamiento de los datos internos y para ello, es vital el disponer de una red de calidad y que sea segura para los usuarios y servicios ofrecidos, además de tener la capacidad de adaptación ligada a la funcionalidad de la empresa.

El apostar por las redes corporativas dentro de organizaciones proporcionan herramientas a los integrantes, ofreciendo agilidad en procesos además de mejorar el flujo de información reduciendo los costes, debido al despliegue de servicios centralizados que se ofrecen. No obstante, dicha red interna debe estar actualizada y realizar distintas auditorías a esta para poder optimizar la red de manera que sea escalable.

La estrategia de las distintas de empresas de continuidad y mejora del negocio, obliga a la constante necesidad de introducción de cambios y para ello es imprescindible establecer unas pautas que garanticen su éxito con el menor impacto posible. La metodología ITIL (Information Technology Infrastructure Library) establece una serie de buenas prácticas de gestión para organizaciones relacionadas con la tecnología. Relacionado con los cambios, tanto para los proactivos como los reactivos, ofrece herramientas que faciliten la ejecución de estos para su óptima planificación y ejecución, considerando posibles alteraciones que surjan en el transcurso del mismo, con planes de contingencia acordes a estos.

1.1. Motivación y Objetivos

La empresa para la que se desarrollará el proyecto que vamos a exponer, dispone de varias sedes agrupadas según su área de producción, con una red centralizada que las unifica. Tras la incorporación de la nueva sede a la empresa, se vuelve imprescindible garantizar a los usuarios la disponibilidad y la seguridad correspondiente para el correcto acceso a los servicios corporativos.

La planta se encontraba ya parcialmente integrada, pero la gestión de esta correspondía a otra empresa subcontratada distinta al resto de sedes, además de distintos privilegios dentro de la empresa al acceso a los servicios de la organización, por lo que se planificó dicho proyecto para completar el traspaso para garantizar la gestión centralizada.

El objetivo también incluye el aumento de personal, distribuido en distintos edificios, los cuales deben tener también acceso a la red, no solo desde la oficina central, por tanto, hay que considerar el despliegue de nuevos equipos para garantizar la conexión de los usuarios, tanto por cable como por Wi-Fi a todo servicio que sea necesario para el desarrollo de la producción.

La actualización de los todos los dispositivos, sobre todo los ya desplegados, garantizando que todos se encuentran en la última versión recomendada por cada uno de los fabricantes, de esta manera evitamos

vulnerabilidades en cuanto a la seguridad de la red que ya se hayan contemplado y corregido en las nuevas versiones, y al mismo tiempo asegurar que esta sea estable para que no afecte a la disponibilidad de estos.

1.2. Plan de trabajo

Partiendo de la red que ya constituía la sede que vamos a mejorar, la metodología de trabajo consistió en analizar la que era la infraestructura desplegada, detallar los requisitos que eran necesarios para la completa integración de esta en la red corporativa y estudiar si eran viables y cómo debería ser implementado, además de los recursos que serían necesarios.

Al basarnos en la metodología ITIL, el cambio debe interrumpir la disponibilidad de los servicios y el trabajo de los usuarios lo menos posible, por lo que la planificación debe ser exhaustiva con una documentación del cambio donde se especifiquen todos los detalles habiendo considerado los posibles y previsibles inconvenientes que se pueden encontrar, con su posible solución o marcha atrás.

Definimos a continuación los pasos seguidos para alcanzar los objetivos, los cuales será agrupados en distintas fases.

1.1.1 Fase de Planificación

El primer paso en todo cambio es entender la necesidad de realizarlo, por lo que se planificaron diversas reuniones donde el cliente podría exponer el motivo y la idea que tenían en mente de cómo mejorar la sede. A través de dichas reuniones, de correos intercambiados con la información adicional y de analizar la posible forma óptima de realizarlo, se establecieron los requisitos que se deberían cumplir para un despliegue exitoso.

Una vez se tienen las pautas que se deben seguir, lo siguiente es revisar la situación actual, qué equipos componen la red, cómo están desplegados y en qué condiciones, qué resultado es el que se quiere obtener y con toda esta información se van planificando si es posible la implementación. Entre la documentación que es necesaria para poder contextualizar de la manera más precisa, se necesitaría tener acceso a mapas de red, informes y auditorías entre otros.

1.1.2 Fase de Diseño

Una vez tenemos toda la información necesaria recopilada, analizados los requisitos establecidos y la primera versión de como resultarían los cambios, se realiza una propuesta, en ITIL se denomina RFC o solicitud del cambio. Esta primera aproximación presenta una idea de cómo sería el diseño tras el cambio y debe ser evaluada y aprobada por el responsable del cambio antes de poder continuar.

Se adjuntarán mapas de red y análisis de cobertura que plasmen la manera técnica del desarrollo del proyecto y como deben ser distribuidos los equipos para una mayor eficiencia de la comunicación. Mediante diagramas de Gantt se planificarán cronológicamente todos los puntos que se deberían cubrir durante el periodo de transición y la facturación del coste que supondría la ejecución del cambio.

1.1.3 Fase de Configuración

En esta fase se especificarán los modelos de los distintos fabricantes que se utilizarán y se detallarán las configuraciones realizadas en cada uno de los equipos de manera que fuese posible cumplir con las especificaciones y el diseño aprobado.

Como se comentará más adelante, estos se mandarían a la planta del cliente una vez se hubiese probado en un laboratorio para solventar la mayor cantidad de errores antes de la fecha del despliegue.

1.1.4 Fase de Transición

La transición supone el paso de la infraestructura original a la deseada. En esta se incluiría el desplazamiento y trabajo en la oficina del cliente hasta dejar operativos todos los servicios dentro de la red corporativa, realizando las comprobaciones oportunas para garantizar la mínima intrusión en el trabajo de los usuarios.

Toda la información necesaria deberá ser recopilada, entregada y validada, de manera que los equipos queden integrados en las distintas herramientas pasa su posterior soporte. Habrá que garantizar una disponibilidad mensual de la sede superior a un 98% del tiempo, para ello es imprescindible una correcta monitorización de la infraestructura.

Tras dar el visto bueno el cliente, podremos proceder al cierre del proyecto.

1.1.5 Fase de Operación

Al contar con un contrato de soporte de los equipos y resolución de incidencias a través de un sistema de ticketing, habría que negociar la incorporación de una nueva sede. Por seguridad se deben actualizar los equipos regularmente, siempre y cuando las versiones de firmware a las que se pretenda actualizar sean estables y recomendadas por el fabricante, por lo que se planteará un calendario de actualizaciones, realizadas fuera de horario de la planta, siempre evitando interferir lo mínimo posible en el día a día de los trabajadores.

2 TOMA DE REQUISITOS Y CREACIÓN DE UNA SOLICITUD DEL CAMBIO

En este apartado se expondrán la especificación de los requisitos, detallados con el solicitante del cambio, el cual, tras numerosas reuniones y correos se consiguió llegar a una idea inicial de cuáles eran los cambios de infraestructura que querían realizar en la sede para integrarla definitivamente en la red corporativa.

Durante las reuniones se aclararon también puntos de la facturación que supondría el proyecto, estimando un precio inicial en función de la cantidad de equipos que fuesen a ser necesarios, personal que se dispondría para su ejecución, así como la planificación de plazos y distribución de pagos del proyecto.

2.1. Situación Inicial

El mapa de red de situación con la que nos encontramos era el siguiente:

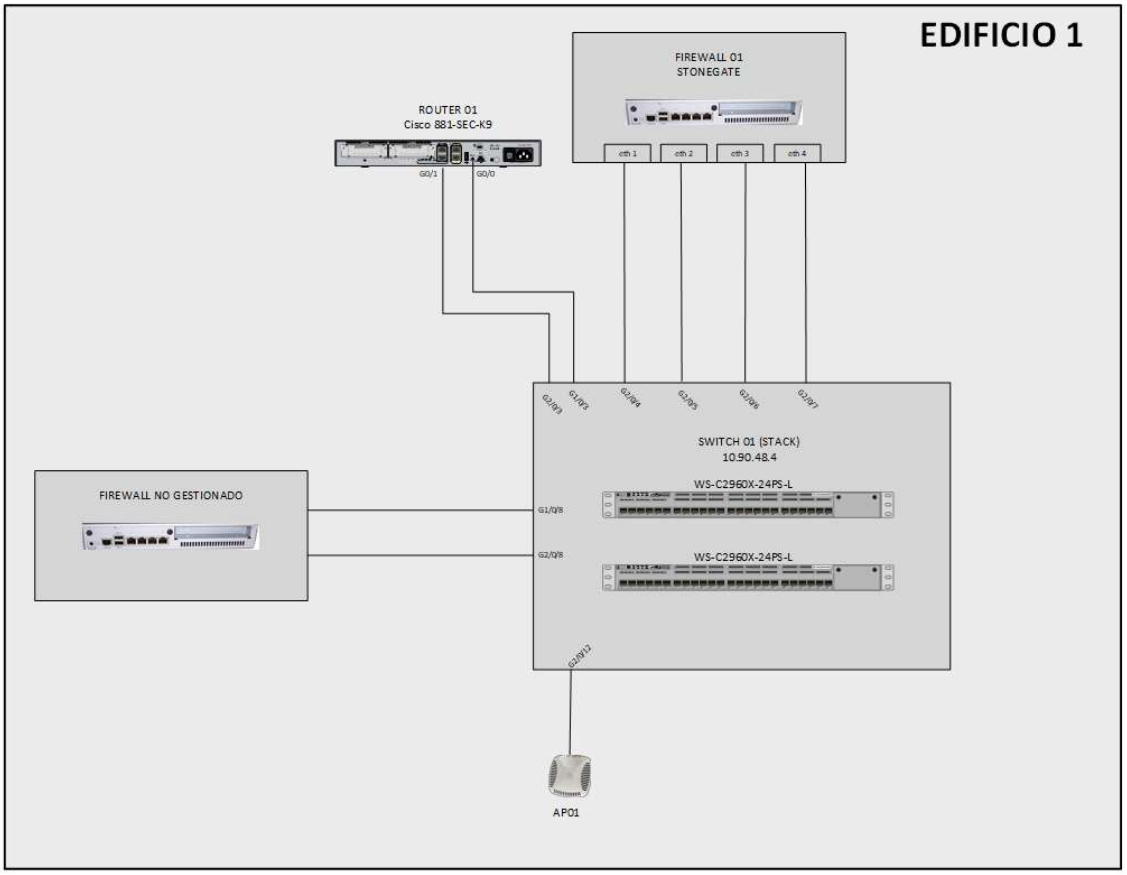


Figura 2-1. Mapa de red físico antes del cambio.

Como se puede observar la red era simple, diseñada para pocos usuarios y todos ubicados en el mismo edificio. El cliente no solo nos hizo saber que necesitaban que dicha red aumentase ya que dicha sede estaba en constante crecimiento, sino que era necesario que en distintas zonas de la planta necesitarían acceso a la red corporativa.

Se aprecia un segundo firewall, que dice "No gestionado", esto se debe a que esta sede está dividida entre dos proveedores debido a las tareas que se tienen que llevar a cabo además de las corporativas. Para las actividades relacionadas con la producción de la propia planta, se trabajaba a través de otra plataforma, por lo que teníamos que respetar dicho tráfico durante la migración y gestionar que desde la red de usuarios corporativa pudieran mantener el acceso a esta plataforma.

Como en el resto de sedes de esta empresa, la red se conecta con el resto de plantas a través del router Cisco 881-SEC-K9 utilizando un tipo de protocolo propio del fabricante, denominada DMVPN (Dynamic Multipoint Virtual Private Network).

2.2. Especificación de requisitos

Una vez analizado el punto de partida y habiendo concretado con el cliente la visión de mejora que tenía, se detallaron los requisitos para poder elaborar la propuesta de diseño de la nueva planta.

- La sede debe quedar completamente integrada en la red corporativa, garantizando los servicios que ya utilizaban como el acceso a los nuevos que serían necesarios para la productividad de nuestro cliente.
- Actualización de los equipos que componen la infraestructura de la planta a la última versión estable, recomendada por cada fabricante.
- Sustitución del firewall Stonegate 315, debido al fin de vida del equipo, por un firewall Palo Alto.
- Sustitución del router Cisco 881-SEC-K9 debido al fin de soporte por parte del fabricante, por un Cisco C1111-8P, modelo el cual ha sido desplegado también en el resto de plantas, dado que tiene las especificaciones para lo que el cliente necesita que es garantizar la comunicación entre las distintas sedes.
- Ampliación de la red, de manera que se aumente el número de puestos de usuarios en el edificio principal como en el resto de salas de producción de la planta.
- Aumento de la cobertura Wi-Fi con la inclusión de nuevos puntos de acceso.
- Es indispensable que la realización del despliegue se realice de manera que no interfiera con el trabajo habitual de los usuarios.

2.3. Análisis de los requisitos

Se mantendrá el firewall como puerta de enlace para todas las subredes, traspasando las políticas ya existentes al firewall Palo Alto, además de las políticas de la plantilla comunes a la comunicación entre sedes, la cual será sincronizada una vez esté gestionado desde la plataforma Panorama.

Para cubrir los puestos de usuario dispersados en las distintas zonas que solicitó el cliente, se concluyó que con añadir 5 nuevos switches se cubriría la demanda con suficientes puertos de más. La distribución por edificios y localización de los equipos fue determinada por el cliente. Debido a que la distancia entre edificios es superior a los 90 metros, entre estos se utilizará fibra para la interconexión y para los de la misma sala, cables de cobre. Siempre que sea posible y los equipos dispongan de suficientes puertos, se utilizarán los que puedan ofrecer mayor caudal para las conexiones troncales.

Se planteó un diseño donde la estructura estuviese mallada y haciendo uso del protocolo STP (Spanning-Tree

Protocol), de manera que hubiese más de un enlace para poder alcanzar el núcleo de la red y así no dejar aislados los edificios ante fallo en el cableado. Al recibir la información de las tiradas de fibra que había disponibles en la plantase tuvo que descartar al ya estar utilizadas, por lo que solo se podrían conectar dos equipos al central y el cuarto edificio a uno de estos.

En una de las salas se localizarían 3 switches, donde se propuso de nuevo la malla, conectados con cables de cobre, pero la idea principal que tenía el cliente era conectarlos en fila, uno tras otro, pero se argumentó que ante caída de uno de los equipos se perdería la conexión en todos los que estuviesen conectados a ellos.

Otra pauta que marcaron es la de afectar a los usuarios durante las horas de trabajo, por lo que se listarán las tareas a realizar y se categorizarán entre si impactan o no. Aquellas que puedan interferir se llevaran a cabo una vez la jornada finalice, teniendo al día siguiente especial atención a si hubiese fallos relacionados con dicho cambio.

Una vez analizados los requisitos solicitados por el cliente, se consideraron que eran asequibles por lo que se pudo seguir adelante con el proyecto, siempre abiertos a posibles modificaciones.

3.2. RFC

Una solicitud del cambio o RFC (Request for change) es el documento que formaliza la petición para cualquier modificación que no se trate de una estándar o preaprobada, que son aquellos que se realizan en el trabajo diario, no suponen corte de servicio a los usuarios y no requieren supervisión de un comité para ser aprobados. En dicho documento debe aparecer toda información requerida para su aprobación, incluyendo un plan de “rollback” del que se deberá hacer uso si este se complicase durante la implementación.

En ITIL, la solicitud del cambio es imprescindible y debe llevar ciertos puntos especificados para que tanto el solicitante como el que lo vaya a llevar a cabo, ambas partes estén de acuerdo en qué, cuándo y cómo se van a realizar las modificaciones. Se deberá especificar un flujo de proyecto, las responsabilidades asignadas a cada uno de los participantes, de manera que se puedan organizar y priorizar eficazmente las tareas.

La RFC presentada se encuentra adjunta al final del documento [Anexo A]. Debido que se trata de un proyecto real se han suprimido las partes confidenciales, como número de proyecto, nombre del cliente o personales reales involucradas entre otros.

3 TRATAMIENTO INTEGRAL DE LA SOLICITUD DE CAMBIO

3.1. Revisión y evaluación de la solicitud del cambio

3.1.1 Diseño Final

Una vez estudiados los requisitos que el cliente especificó durante las reuniones realizadas y habiendo analizado la infraestructura de la red desplegada en la sede, se hizo un diseño tanto del despliegue de equipos como de la estructura de las subredes a desplegar. El diseño final tanto de la red lógica como de la física se concluyó que fuese como se muestra en las próximas imágenes.

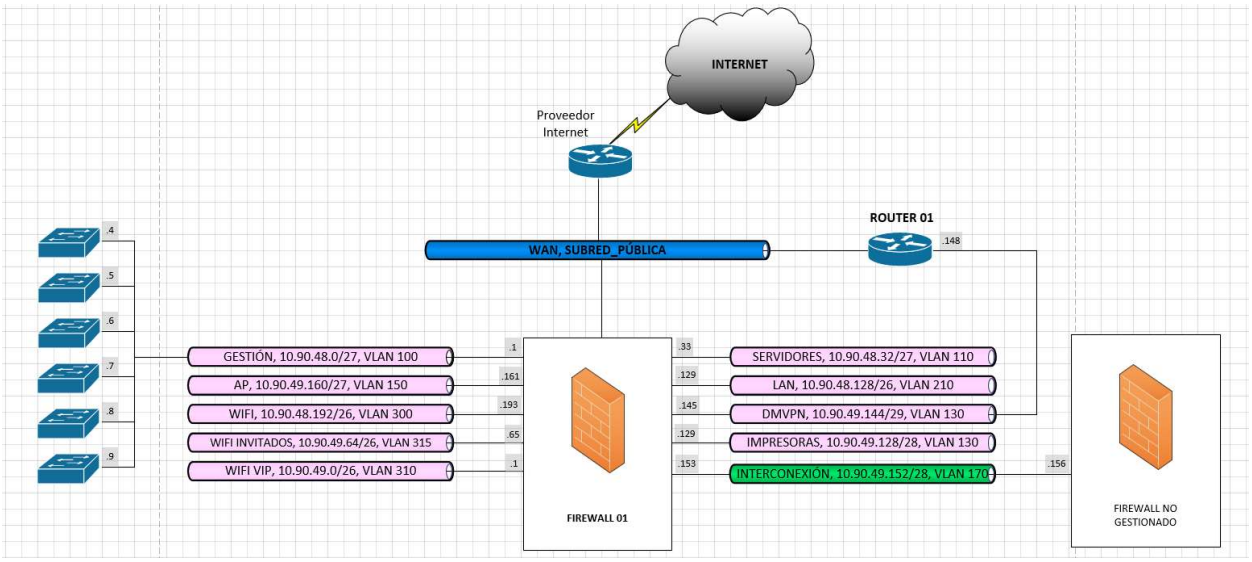


Figura 3-1. Mapa de red lógico propuesto.

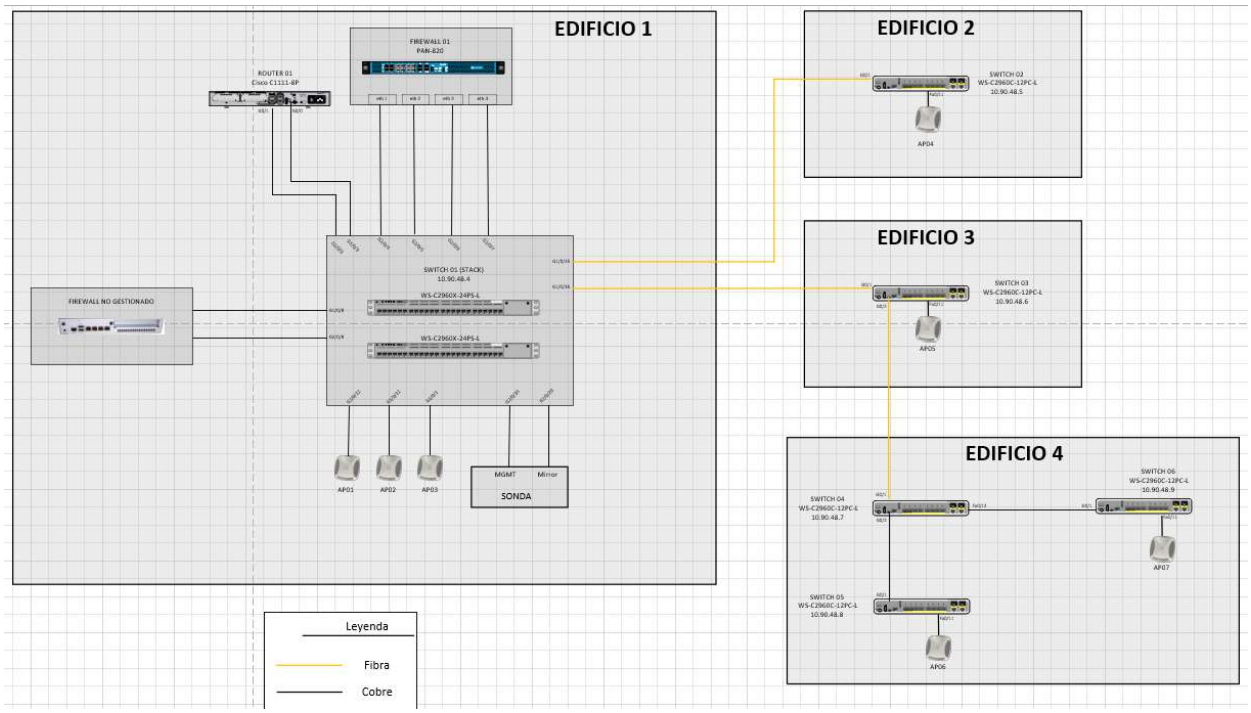


Figura 3-2. Mapa de red lógico propuesto.

La asignación del direccionamiento de las subredes y VLANs se estructuró manteniendo las que había e incluyendo nuevas para seguir la distribución estándar del resto de sedes.

Se estudió la cobertura que proporcionaba el único punto de acceso que originalmente se podía encontrar en el edificio de las oficinas centrales, por lo que era imprescindible incluir más para cubrir un espacio mayor para que todo usuario en la oficina pudiese conectarse por Wi-Fi.

El AP ya conectado podría ser reubicado con el objetivo de mejorar la calidad de la señal y para conseguir minimizar las interferencias con el resto.

- Interferencias cocanal: Se trata de interferencias causadas por los propios APs radiando en los mismos canales o canales adyacentes. En 2,4 GHz tenemos 3 canales no solapables, mientras que en 5 GHz se disponen, dependiendo de las regiones, de hasta 25 canales de 20 MHz, 12 canales de 40 MHz, 6 canales de 80 MHz o 2 canales de 160 MHz. En nuestro caso, con 3 APs no tendremos que tener en cuenta dicho problema.
- Potencia de señal (RSSI): es el nivel de señal medido en cada punto del espacio. Para obtener una tasa de transferencia adecuada es necesario tener unos niveles de señal mínimos, que depende de las necesidades de cada aplicación. Como norma general
    - > -60 dBm: Se considera niveles óptimos con el que se pueden conseguir la mayor tasa de transferencia
    - -70 dBm < RSSI < -60 dBm: Son valores correctos, se consiguen tasas de transferencia altas y la conexión es estable
    - -80 dBm < RSSI < -70 dBm: En este rango la tasa de transferencia empieza a bajar considerablemente
    - < -80 dBm: La conexión es inestable y la tasa de transferencia es baja
- Bajo SNR (Signal to Noise Relation): Es el parámetro que indica la diferencia de potencia entre la señal y el ruido, y que marca en gran medida la tasa de transferencia obtenida. Podemos considerar los siguientes valores como recomendación de referencia
    - > 40 dB: Se considera niveles óptimos con el que se pueden conseguir la mayor tasa de transferencia

- 25 - 40 dB: Son valores correctos, se consiguen tasas de transferencia altas y la conexión es estable
- 15 - 25 dB: Buena calidad todavía se consigue estabilidad de la conexión y tasas de transferencia altas
- 10 - 15 dB: En este rango nos encontramos con problemas de estabilidad y baja tasas de transferencia
- 0 - 10 dB: Conexión inestable prácticamente no es operativo

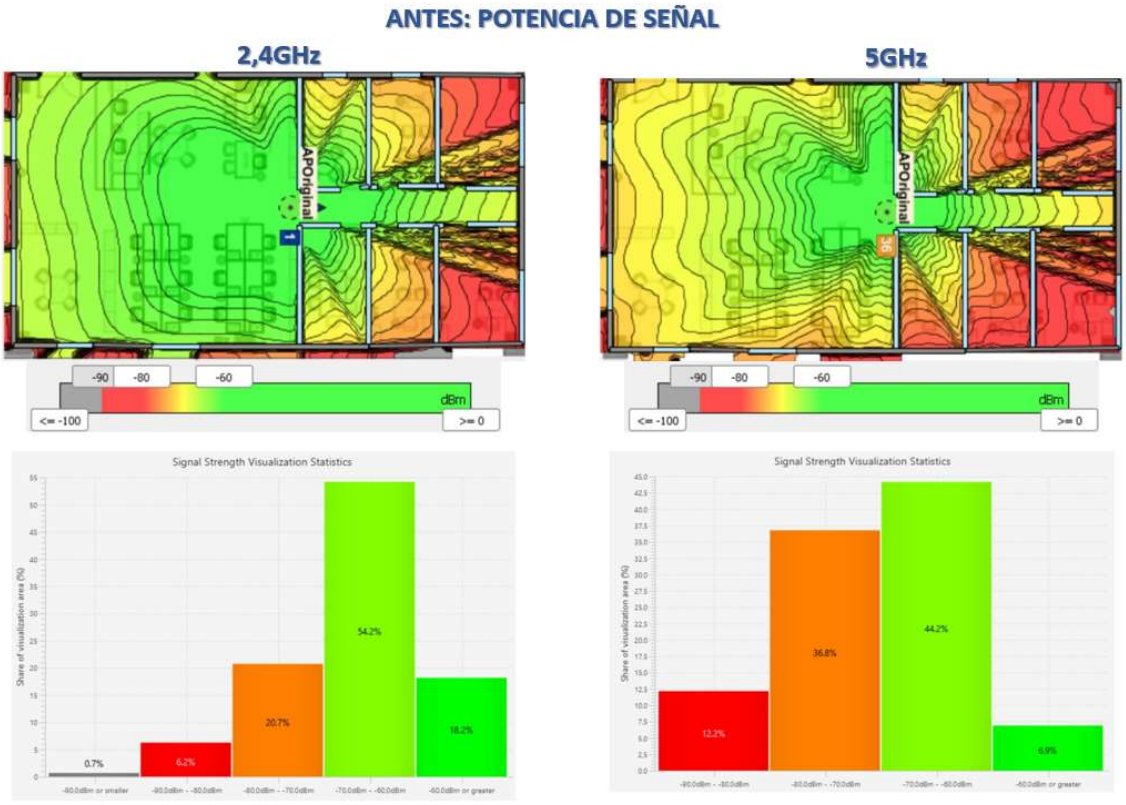


Figura 3-3. Potencia de señal recibida original.

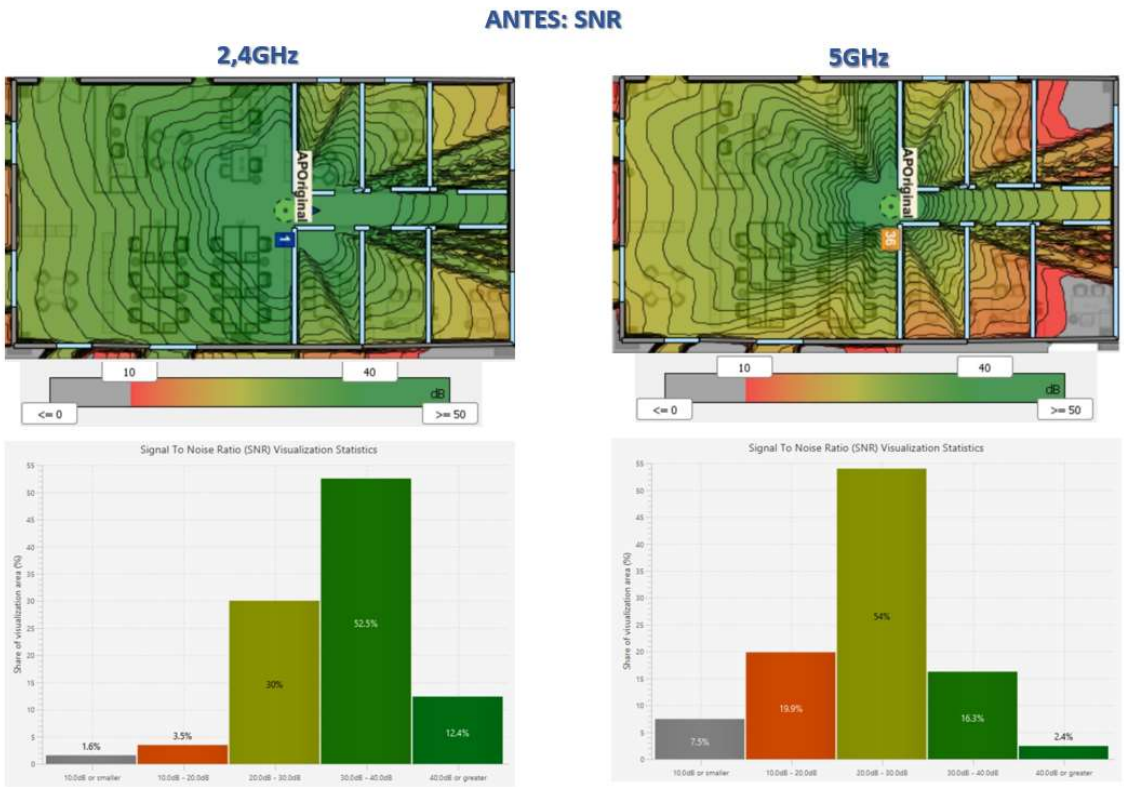


Figura 3-4. Calidad de la señal original.

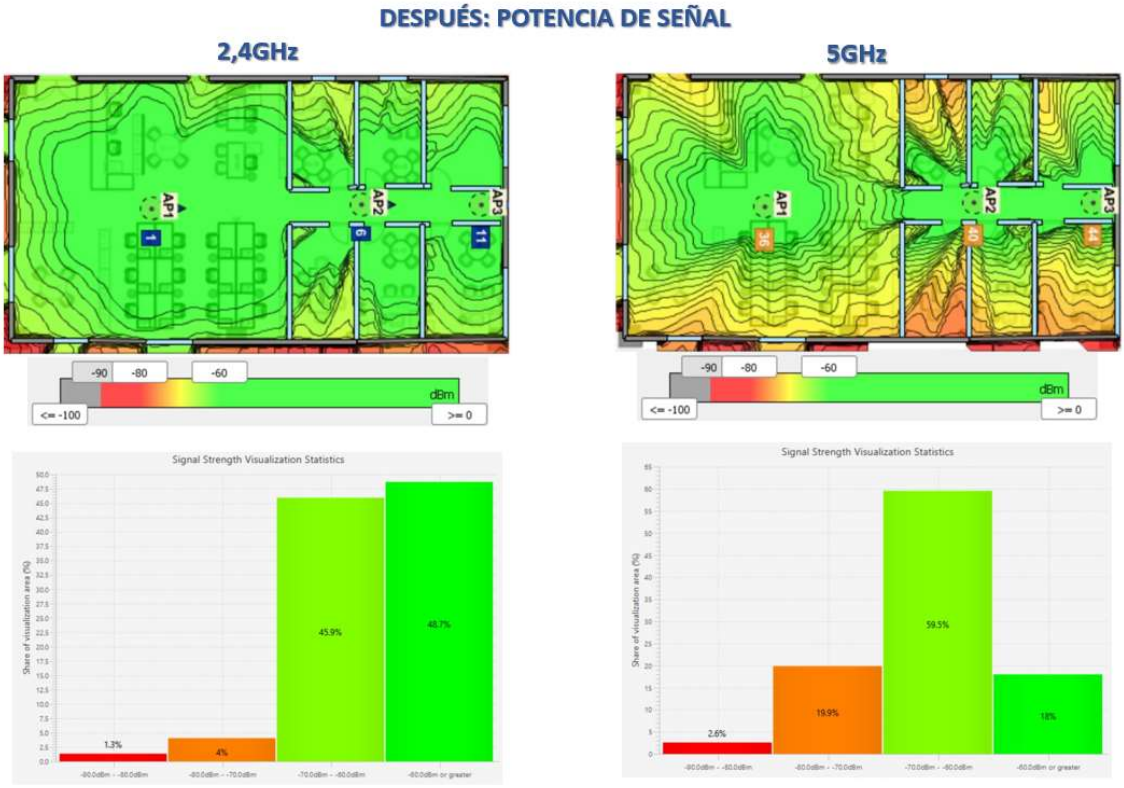


Figura 3-5. Potencia de señal recibida propuesta.

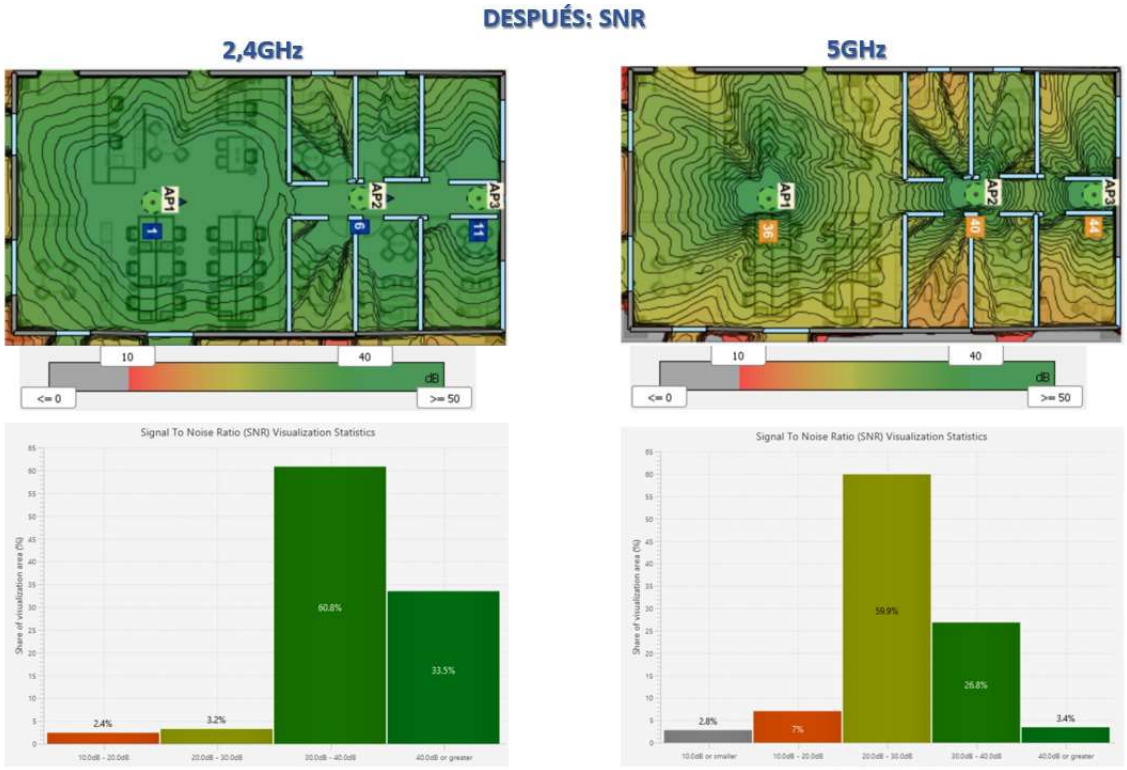


Figura 3-6. Calidad de la señal propuesta.

Como se puede ver en las imágenes anteriores obtenidas a partir del estudio hipotético de cobertura de como está y como quedará tras la intervención, se puede apreciar una mejoría en todos los aspectos. Con un solo AP observamos que, para la frecuencia de 2,4GHz podemos obtener una cobertura con una señal bastante aceptable en la mayoría de zonas de la oficina, no obtenemos los mismos resultados para los 5GHz, resultando en poca estabilidad y con alto porcentaje del espacio con una baja tasa de transferencia.

Al incluir los otros puntos de acceso y recolocar el original, poniendo especial atención en que todos estuviesen en distintos canales para ambas frecuencias, obtenemos mejorías en todos los campos, con una potencia de señal bastante óptimos en más de un 90% de la planta.

Se concluyó que era necesaria la implementación de los nuevos APs tras haber estudiado los resultados.

3.1.2 Orden de ejecución

Se establecieron los pasos a seguir, tanto previos como durante el despliegue, de manera aproximada. En el diagrama de Gantt, que podemos encontrar en la siguiente imagen, se muestra la visión global del proyecto y el tiempo que conllevaría cada una de las actividades, más un margen suficiente para solventar cualquier inconveniente que fuésemos encontrando durante el transcurso de cada una de las actividades.

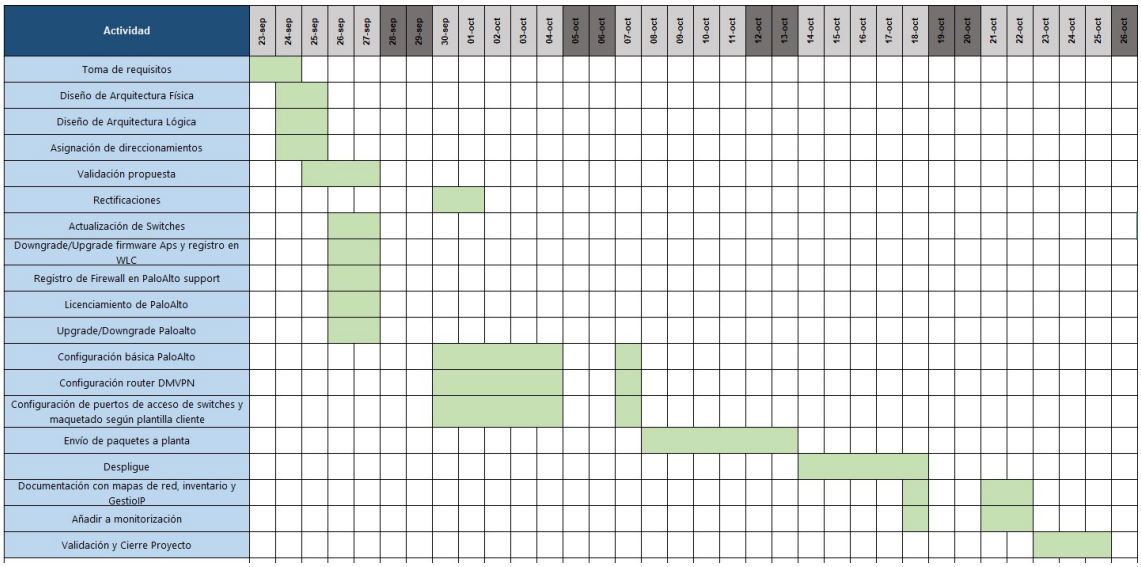


Figura 3-7. Planificación de los trabajos organizados en un diagrama de Gantt.

La actividad toma de requisitos, se realizaron a través de distintas reuniones y correos intercambiados con el cliente previos a cualquier configuración para tener una idea de las necesidades de este en cuanto al despliegue. Es imprescindible saber qué necesitaban, cómo y así poder en los poder realizar los diseños previos, los cuales hemos presentado en los apartados anteriores.

Se destinaron varios días, previos al envío de los equipos a la planta, para poder realizar todas las configuraciones que cumpliesen con los requisitos establecidos, con tiempo para realizar pruebas y montar el escenario en un laboratorio y así cerciorarnos de su correcto funcionamiento de lo que se podía testear antes de ponerlos en producción.

El despliegue en sí no podía superar los días establecidos para el acceso a la sede, por lo que habría que detallar más detenidamente el orden por actividad, además de tener en cuenta los posibles cortes a los usuarios que estaban trabajando, siendo imprescindible que estos fuesen por la tarde para que el impacto fuese mínimo. En este segundo diagrama de Gantt, se ha detallado más los pasos del despliegue para establecer las franjas horarias en las que era conveniente hacer cada uno de los trabajos.

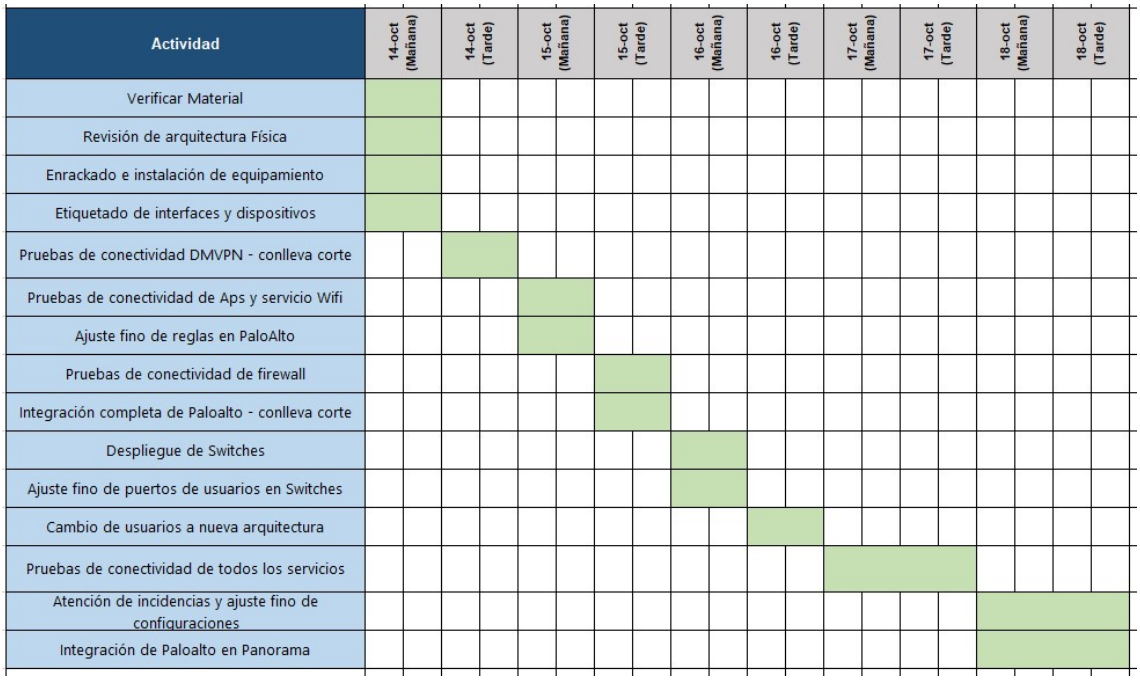


Figura 3-8. Planificación de los trabajos en la planta organizados en un diagrama de Gantt.

En primer lugar, nada más llegar, fue imprescindible familiarizarnos con el entorno, aunque teníamos los mapas de red iniciales, es fundamental cerciorarse de que toda la información es correcta y que no falta nada, además de obtener "backups" de las configuraciones de todos los equipos en producción por si fuese necesario una marcha atrás mientras se sustituían por los nuevos. Verificar que hubiese llegado todo el material y en buenas condiciones, enracar cada uno de ellos en los armarios correspondientes y etiquetar tanto equipos como cables que fuésemos a utilizar, siempre con el objetivo de dejarlo ordenado y fácil de identificar cualquier conexión.

El primer día, por la tarde, se decidió que se comenzaría con el cambio del router, ya que la configuración del nuevo equipo era exactamente igual y el cambio solo supondría un cambio de modelo por fin de soporte del producto anterior por parte del fabricante. Una vez conectado se realizarían las pruebas pertinentes para comprobar que los túneles DMVPN estuviesen levantados correctamente y por tanto poder acceder a todos los servicios corporativos, además de la salida a Internet.

El segundo día, por la mañana se conectarían los distintos puntos de acceso que fuesen necesarios en el edificio principal, los cuales irían conectados a los switches en producción, ya que esta tarea no afectaría a los usuarios. Se realizarían estudios de cobertura de Wi-Fi para comprobar que la localización escogida para los APs es la adecuada y ofrecen un radio suficiente potencia en todos los puntos de la planta.

El firewall se mandaría configurado con las reglas que estaban en uso en el anterior además de las generales para los accesos e inclusión de la sede en la red corporativa, aun así, se revisaron las reglas una vez más antes de su puesta en producción. Una vez sustituido, se realizarían pruebas de accesos y actividades usuales de los trabajadores.

Despliegue en el tercer día de todos los switches en el resto de los edificios de la sede probando conectividad con el de core, conexión de impresoras y resto de APs.

Finalmente se pasarían todos los puestos de usuarios a la nueva arquitectura, para que quedase tiempo suficiente para que se pudiesen realizar todas las pruebas y comprobar que trabarían con normalidad sin que el cambio le afectase a la productividad. Se añadiría entonces, el Palo Alto a Panorama para su gestión centralizada, contando con que se podría realizar sin corte alguno.

Una vez validado el cambio, se pasaría a documentar todos los equipos en el inventario del cliente, mapas de red y subredes utilizadas en GestioIP, que es una herramienta donde mantiene información de todas las sedes para una mejor gestión. Se añadirían a la monitorización para poder dar por finalizado el proyecto.

3.1.3 Facturación

Con el diseño presentado y validado, se presentó el presupuesto al cliente, en el que se incluían tanto los equipos, licencias, además de lo que costaría llevar a cabo su ejecución.

En la siguiente tabla se especifican todos los productos necesarios, la cantidad y el coste individual de cada uno de estos.

Material	Descripción Material	Unidades	Precio	Importe
WS-C2960C-12PC-L	Catalyst 2960C Switch 12 FE PoE, 2 x Dual Uplink, Lan Base	5	649,41 €	3.247,05 €
CON-SNT-C296012P	SNTC-8X5XNBD Catalyst 2960C Switch 12 FE PoE, 2 x Dua	5	281,00 €	1.405,00 €
CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	5	0 €	0 €
GLC-SX-MMD=	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	6	231,65 €	1.389,90 €
AIR-AP1832I-E-K9	802.11ac Wave 2; 3x3:2SS; Int Ant; E Reg Domain	5	269,47 €	1.347,35 €
CON-SNT-AIR2IEK9	SNTC-8X5XNBD 802.11ac Wave 2; 3x3:2SS; Int Ant; E Reg Service duration in months: 60	5	83,31 €	416,55 €
AIR-AP-BRACKET-1	802.11 AP Low Profile Mounting Bracket (Default)	5	0 €	0 €
L-LIC-CTVM-1A	1 AP Adder License for the Virtual Controller (eDelivery)	5	98,54 €	492,70 €
CON-ECMU-CTVM1A	SWSS UPGRADES 1 AP Adder License for the Virtual Controller Service duration in months: 60	5	89,26 €	446,30 €
-	Instalación del equipamiento	1	1.280,00 €	1.280,00 €
-	Gestión y documentación del proyecto	1	640,00 €	640,00 €
-	Desplazamiento a la sede	1	1.550,00 €	1.550,00 €
-	Envío de equipamiento a la sede	1	352,94 €	352,94 €
TOTAL				12.567,79 €

Figura 3-9. Facturación detallada del proyecto.

Los pagos se irían realizando por porcentajes en función de los hitos alcanzados, estructurando el proyecto en tres bloques.

El primer hito constaría de las fases de diseño de la nueva sede tras haberle dado el visto bueno el cliente, compra y configuración de los equipos adquiridos, el cual constaría de un 20% de la facturación total. En este mismo hito también se incluirían las pruebas realizadas en el laboratorio.

Un segundo bloque incluiría el traslado y despliegue de la nueva infraestructura, finalizando una vez se comprobasen todos los servicios y habiendo resuelto las posibles incidencias que surgiesen, es decir, se realizaría el pago una vez la planta estuviese incorporada completamente a la red corporativa y los usuarios trabajando con total normalidad. Este hito supondría el 50% del total de la facturación del proyecto.

Por último, se cobraría el 30% restante una vez se hubiese entregado toda la documentación acordada y necesaria para la posterior gestión de esta, además de la monitorización de los equipos.

Como ya se contaba con un plan de soporte de la infraestructura de red, se acordó que, al faltar un par de meses para la finalización de este, se esperaría hasta entonces para negociar un nuevo contrato donde se incluyese el aumento de equipos y se tuviesen en cuenta el coste de los meses previos.

3.2. Planificación del cambio

3.2.1. Equipos necesarios

Para el despliegue se consideró que se debía cambiar el firewall, aumentar los puestos para usuarios finales por lo que se necesitaría más switches, para los distintos edificios en los que era necesario desplegar la red, con sus puntos de acceso, para que tuvieran conexión tanto por cable como por Wi-Fi, y sustituir el router.

Una de las principales razones por la que se decidió realizar el despliegue en esa fecha, era debido al firewall que había antes en la sede, era un Stonegate 315 al cual le llegaba la fecha de fin de soporte en unos meses, por lo que se decidió que se sustituiría por un Palo Alto 820, el cual podría ser gestionado como otras sedes desde Panorama, que es la solución que ofrece Palo Alto Networks para la gestión y visibilidad de numerosos firewalls, todos centralizados en una misma interfaz web. Los firewalls Palo Alto están considerados uno de los mejores de nueva generación (NGFW Next-Generation Firewall), los cuales son capaces de ofrecer una mejor seguridad de la red, no solo al bloquear el tráfico como los firewalls hasta ahora, sino garantizando la inspección a fondo de los paquetes que se transmiten para la pronta detección de una posible amenaza. [Anexo B.1].

El router que estaba activo era un Cisco 881-SEC-K9, el mismo que se estaba utilizando en el resto de las sedes, pero todos ellos fueron sustituidos debido al fin de servicio de estos, por lo que se decidió que ajustándose al presupuesto y por las prestaciones que tenía el modelo, estos se sustituirían por routers Cisco C1111-8P [Anexo B.2].

Una de las especificaciones que solicitó el cliente era cambiar la configuración en el switch del núcleo de la red (Cisco WS-C2960X-24PS-L) [Anexo B.3] de manera que en vez de estar configurados como dos switches independientes entre ellos, se convirtiese en un “stack”, lo que significaría que los dos switches pasarían a actuar como uno solo con el doble de puertos. Para el resto de las salas se decidió durante las reuniones que con los Cisco WS-C2960C-12PC-L [Anexo B.4] se cubría las tomas necesarias, tanto para usuarios como para APs, impresoras o servidores. Para las conexiones entre switches que se encuentran en distintos edificios fue necesario trabajar con tiradas de fibra óptica, debido a que las distancias entre salas eran superiores a los 100 metros por lo que no es recomendable utilizar cables de cobre. El modelo WS-C2960X-24PS-L tiene 4 puertos SFP (Small Form-factor Pluggable), por lo que en el core principal dispondremos de 8 de estos puertos. Por

otro lado, los switches WS-C2960C-12PC-L disponen de 2 puertos de este tipo, pero para poder conectar cables de fibra a los equipos cisco, son imprescindibles transceptores SFP, utilizando para este despliegue los módulos GLC-SX-MMD [Anexo B.6].

Para la selección de los APs que se iban a utilizar, había que tener en cuenta que dicha empresa tiene una controladora Wi-Fi (Cisco Wireless LAN Controller AIR-CTVM-K9) desde la que se gestionan todos los APs, por lo que aquellos que se escogiesen debían ser compatibles con esta y se decidió utilizar los AIR-AP1832I-E-K9 [Anexo B.5].

3.2.2. Configuración y actualización de los distintos equipos

3.2.2.1. Palo Alto 820

La primera tarea que realizar antes de comenzar con las configuraciones del firewall era la actualización. La idea principal era actualizar la última versión estable, recomendada por el fabricante, pero como debíamos integrarlo en Panorama una vez estuviese desplegado, la versión del firewall debía ser menor o igual a la que actualmente Panorama, por lo que optó que para asegurar el correcto funcionamiento que se pondría una inferior.

Para poder actualizar estos equipos, activar las licencias o poder abrir casos con el fabricante en caso de fallos del firewall, tienen que estar registrados en la plataforma de Soporte de Palo Alto, para ello, con la cuenta con la que se quiere tener asociada estos equipos hay que darlo de alta, para ello en el menú que aparece, en el apartado "Assets" y luego en "Device" creamos uno.

Nos pedirá el número de serie del equipo y así como su localización para solicitar un RMA (Return Merchandise Authorization) en caso de necesitar la sustitución del equipo.

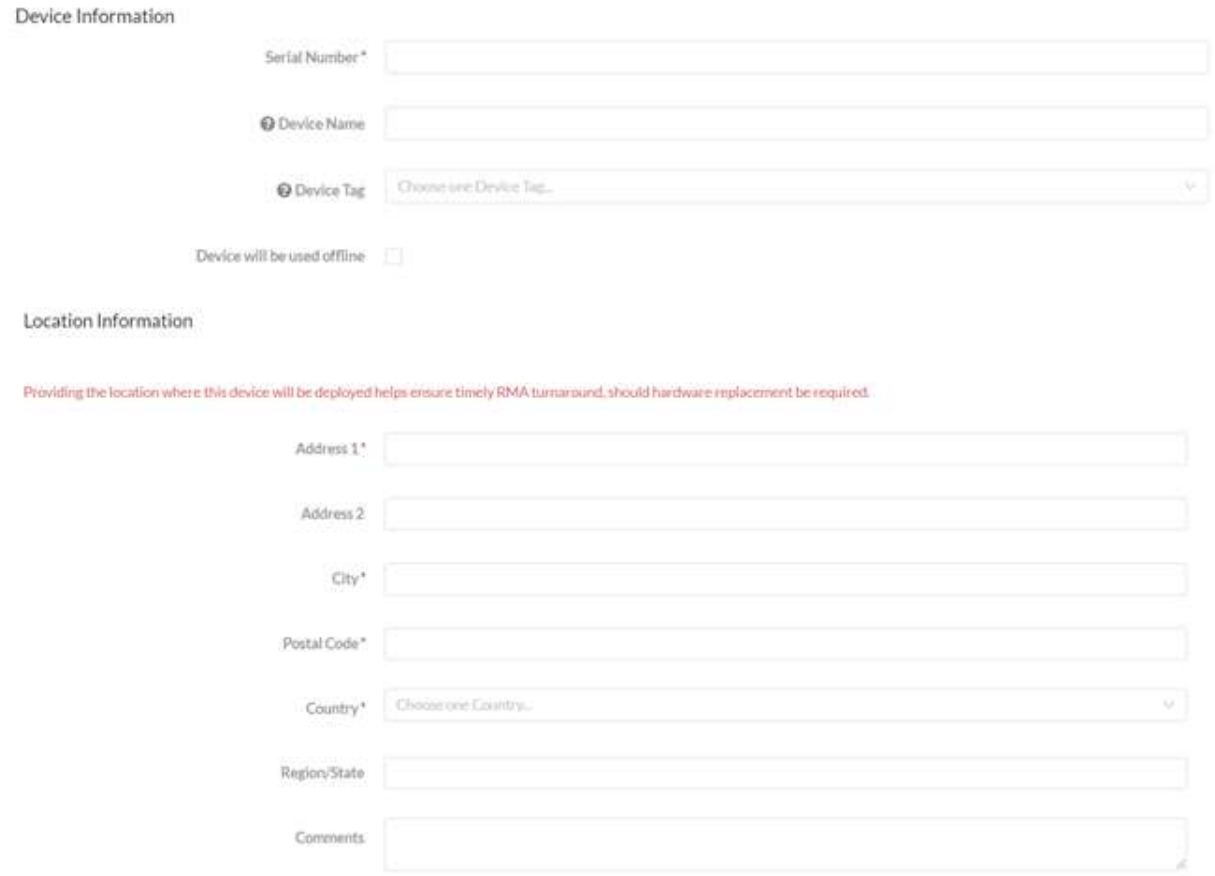


Figura 3-10. Alta de un nuevo equipo en el Soporte de Palo Alto.

Una vez creado nos aparecerá junto al resto de firewalls dados de alta, desde donde podremos descargar las licencias que luego tendremos que cargarle al Palo Alto para poder hacer uso de distintas funcionalidades como la de Prevención de amenazas o Wildfire, las cuales hablaremos más adelante.

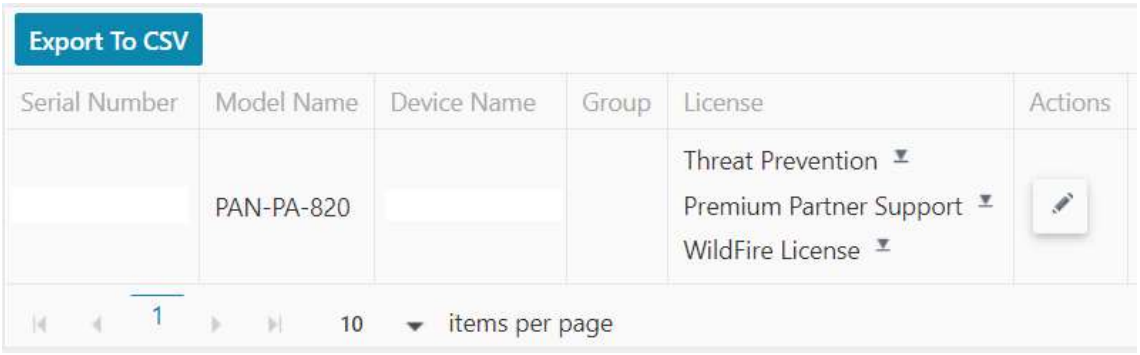


Figura 3-11. Licencias asociadas al equipo.

A la hora de acceder por primera vez a la interfaz gráfica del palo alto, debemos conectarnos con un cable al puerto de "MGT" (puerto de gestión) el cual estará configurado con la IP 192.168.1.1. Luego debemos configurar la tarjeta de red del equipo con una IP del rango 192.168.1.0/24 y como puerta de enlace la del firewall y acceder a la URL https://192.168.1.1 donde nos pedirán un usuario y contraseña, siendo por defecto admin/admin. Por supuesto, como primera recomendación cuando se tiene acceso es cambiar dicha IP y crear usuarios con los permisos que se requieran, ya sean solo lectura o superusuarios, es decir, que puedan realizar cualquier cambio en la configuración.

Figura 3-12. Ruta para creación de usuarios locales en Palo Alto.

Necesitamos tener conexión hacia Internet para poder actualizarlo, por lo que necesitaremos configurar una interfaz, con una IP pública e indicar en la configuración que para poder obtener la información de las actualizaciones disponibles se enrute el tráfico por dicha interfaz e indicar que el servidor de actualizaciones se encuentra en "updates.paloaltonetworks.com".

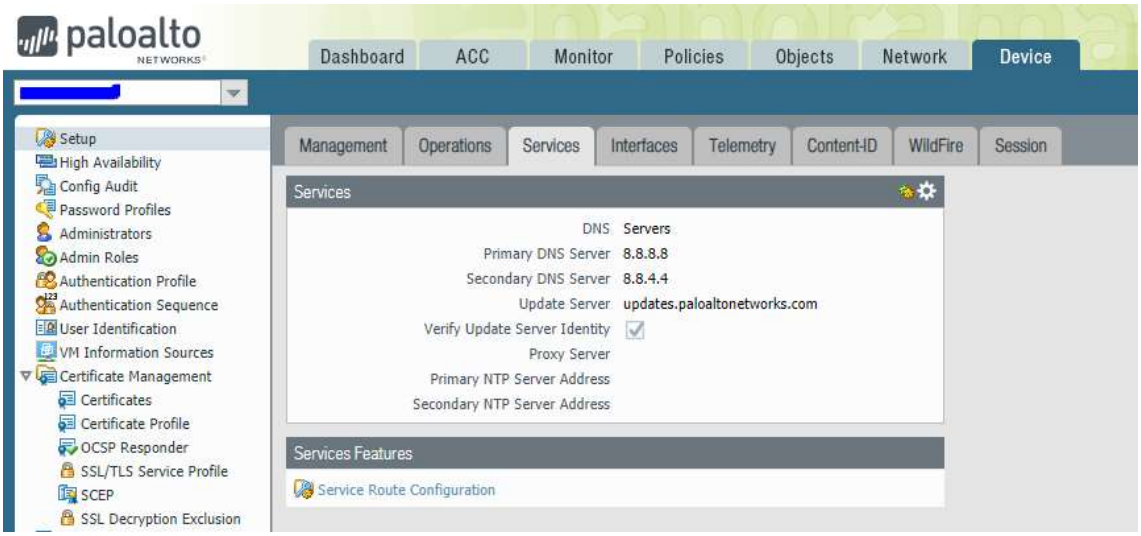


Figura 3-13. Servidor de actualizaiones de Palo Alto.

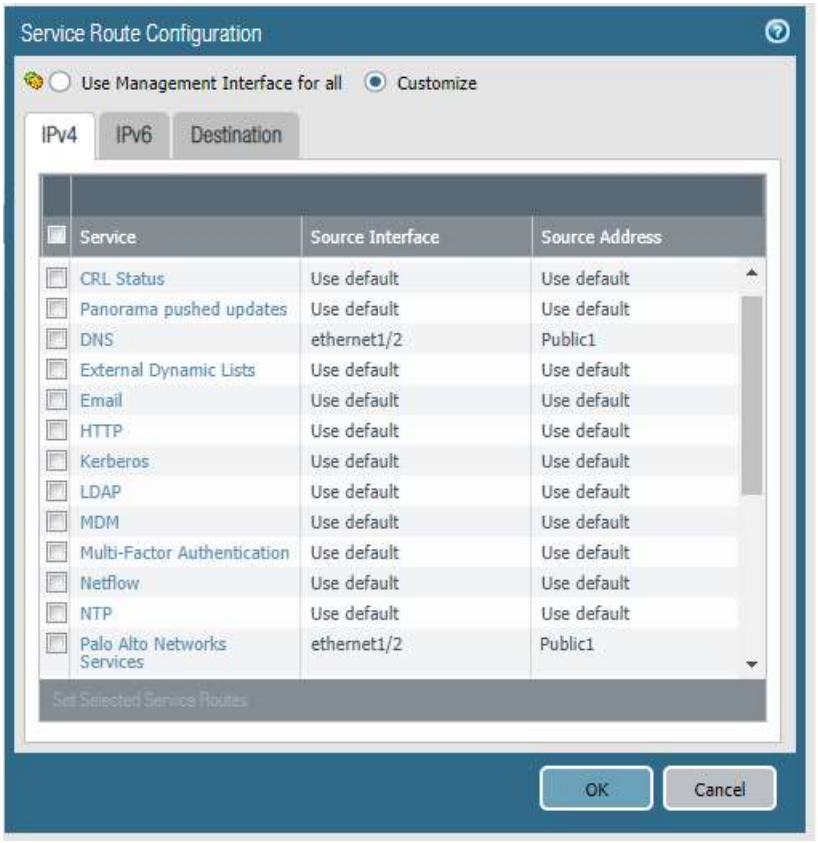


Figura 3-14. Especificación del origen del tráfico según el servicio.

Para la navegación sea correcta, debemos crear un NAT (Network Address Translation), para que al acceder a IPs públicas no se presente con el direccionamiento interno, ya que la vuelta del tráfico no sería posible. Para ello accedemos por la interfaz gráfica del firewall a la pestaña Policies > NAT y como origen seleccionamos todas aquellas zonas que necesitan tener conexión a Internet y especificamos que se traduzcan todas estas a la IP pública.

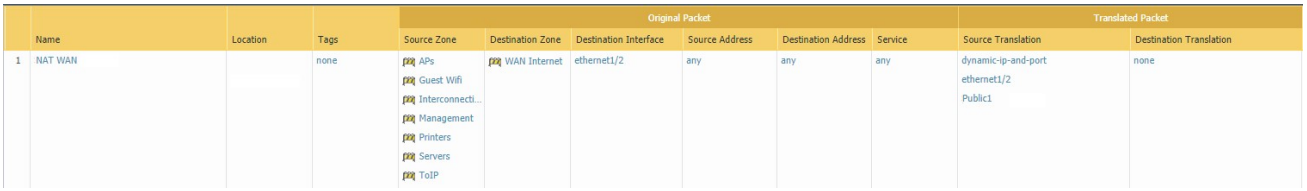


Figura 3-15. Políticas de traducción de IPs.

Una vez realizados los pasos previos, para proceder a actualizarlo a la versión que quedemos hay que dar varios "saltos", es decir, distintos reinicios para llegar al objetivo. Si queremos instalar la 8.0.7, y partimos de la 7.1.3, primero debemos descargar e instalar la última versión del tramo 7.1 que en este caso sería la 7.1.14 y tras ello reiniciar el firewall. Se repite el proceso para la versión base, 8.0.0, la cual sólo se descargará, sin necesidad de reiniciar el equipo ya que no es necesario instalarla, y continuar hasta llegar a la que necesitamos. Encontraremos dicha información en la pestaña en Device > Software.

Las licencias que nos aparecen asociadas al dispositivo, tenemos varias maneras de gestionarlas; desde un servidor que necesita de un código de autorización activado desde el portal de soporte, directamente introduciendo el código que se entrega con la compra de la licencia o descargando e importándolas una a una en el firewall.

Figura 3-16. Carga de las licencias asociadas al firewall.

Para la configuración de interfaces, debemos tener claras las subredes que son necesarias para prestar los servicios de la sede. Palo Alto ofrece la posibilidad de dividir por zonas, que permite agrupar interfaces, físicas o virtuales, clasificando de esta manera el tráfico para que sea más fácil interpretar desde donde viene y a donde se dirige. Por las especificaciones del cliente, quería que cada subred estuviese asignada a una zona distinta, para segmentar el flujo de tráfico lo máximo posible, sin embargo, la zona de "Users" contiene tres subredes, debido a que, tanto por Wi-Fi como por cable, los usuarios no deben percibir la diferencia de navegación o en la utilización de los distintos servicios propios de la planta.

Presentamos el direccionamiento que se van a utilizar en la siguiente tabla.

Tabla 3–1 Direccionamiento asociado a las distintas Zonas y Vlans.

Zona	Vlan ID	Subred
Management	100	10.90.48.0/27
APs	150	10.90.49.160/27
ToIP	200	10.90.48.64/26
Users	210, 300, 310	Usuarios - 10.90.48.128/26, Wi-Fi - 10.90.48.192/26, Wi-Fi VIP - 10.90.49.0/26
Printers	220	10.90.49.128/28
Guest Wi-Fi	315	10.90.49.64/26
Servers	110	10.90.48.32/27

Al disponer únicamente de cuatro puertos en el firewall, había que decidir como asignar las subredes y cuáles de ellas necesitarían puertos dedicados o podrían ser integrados como subinterfaces. Por demanda del cliente, se especificó que se quería mantener la distribución de puertos como estaban configurados en el firewall StoneGate.

A continuación, se muestran los objetos creados para las distintas interfaces. De las subredes que se mostraban en la última tabla, se escogió la primera IP de cada segmento para asignársela al firewall. Como se puede ver en la imagen, no se crea un objeto como un host, es decir, con una máscara de 32 (255.255.255.255), sino que se especifica el tamaño de la subred a la que pertenece, para que a la hora de encaminar sepa cuán grande es el rango al que pertenece dicho tráfico.

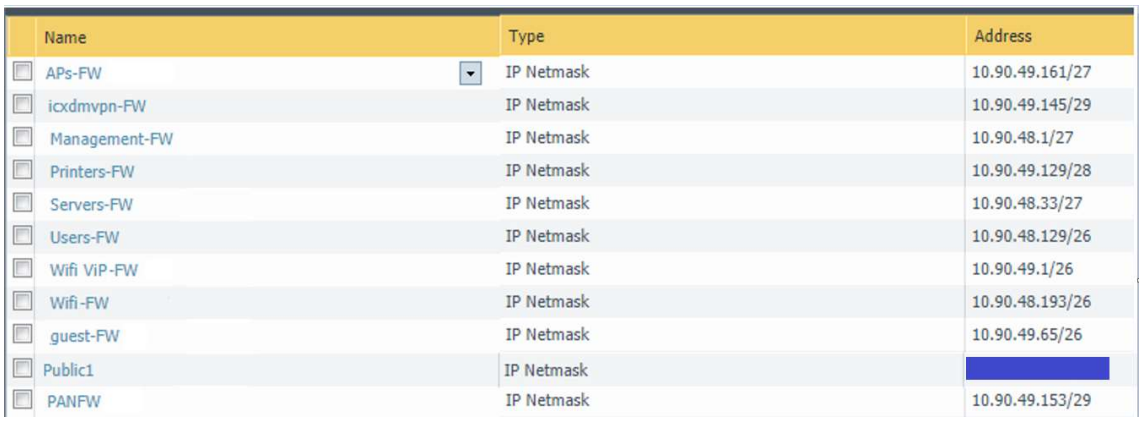
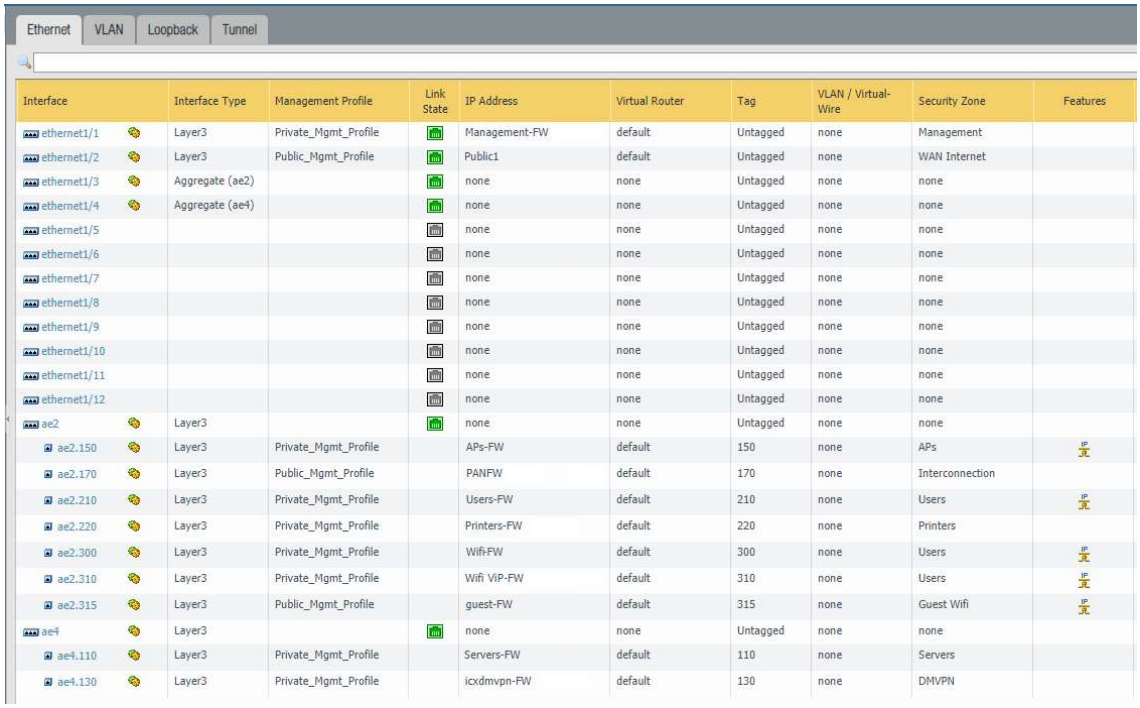


Figura 3-17. Objetos de las interfaces del Firewall.

Una vez creados los objetos, se asignan las IPs a las interfaces.



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features
ethernet1/1	Layer3	Private_Mgmt_Profile		Management-FW	default	Untagged	none	Management	
ethernet1/2	Layer3	Public_Mgmt_Profile		Public1	default	Untagged	none	WAN Internet	
ethernet1/3	Aggregate (ae2)			none	none	Untagged	none	none	
ethernet1/4	Aggregate (ae4)			none	none	Untagged	none	none	
ethernet1/5				none	none	Untagged	none	none	
ethernet1/6				none	none	Untagged	none	none	
ethernet1/7				none	none	Untagged	none	none	
ethernet1/8				none	none	Untagged	none	none	
ethernet1/9				none	none	Untagged	none	none	
ethernet1/10				none	none	Untagged	none	none	
ethernet1/11				none	none	Untagged	none	none	
ethernet1/12				none	none	Untagged	none	none	
ae2	Layer3			none	none	Untagged	none	none	
ae2.150	Layer3	Private_Mgmt_Profile		APs-FW	default	150	none	APs	
ae2.170	Layer3	Public_Mgmt_Profile		PANFW	default	170	none	Interconnection	
ae2.210	Layer3	Private_Mgmt_Profile		Users-FW	default	210	none	Users	
ae2.220	Layer3	Private_Mgmt_Profile		Printers-FW	default	220	none	Printers	
ae2.300	Layer3	Private_Mgmt_Profile		Wifi-FW	default	300	none	Users	
ae2.310	Layer3	Private_Mgmt_Profile		Wifi ViP-FW	default	310	none	Users	
ae2.315	Layer3	Public_Mgmt_Profile		guest-FW	default	315	none	Guest Wifi	
ae4	Layer3			none	none	Untagged	none	none	
ae4.110	Layer3	Private_Mgmt_Profile		Servers-FW	default	110	none	Servers	
ae4.130	Layer3	Private_Mgmt_Profile		icxdmvpn-FW	default	130	none	DMVPN	

Figura 3-18. Interfaces Ethernet del Palo Alto.

Como se puede ver, en los agregados se especifican los VLAN ID que pertenecen a cada interfaz, pero a las que tienen una interfaz dedicada no es necesario en el firewall, pero en la configuración de los puertos del switch al que se conecta, la cual veremos más adelante, se limitará.

Se le asignan distintos perfiles de gestión, como se aprecia en una de las columnas. Estos perfiles protegen el acceso al firewall especificando los protocolos permitidos además de restringir por IPs de origen luego en las políticas. Si no se habilitasen dichos protocolos en cada una de las interfaces, el firewall no respondería a ninguno, aunque estuviese aceptado dicho tráfico, por lo que para poder gestionarlo por la interfaz gráfica o bien por la CLI (Command Line Interface) habría añadir en los perfiles HTTP/HTTPS y SSH respectivamente.

En este caso, el cliente tiene un servidor el cual se encarga de llevar el DHCP de las distintas plantas, por lo que no tenemos que configurar el Palo Alto para que ofrezca IP a los distintos equipos, pero sí tenemos que activar el "DHCP relay" por cada interfaz que lo necesitemos, lo que permitirá reenviar los mensajes a dicho servidor para ofrecer el direccionamiento que se haya reservado para dicha sede. En Network > DHCP > DHCP Relay creamos una entrada por cada VLAN que se necesite especificando la IP de dicho servidor, teniendo en cuenta que debemos configurar una entrada en la tabla de enrutamiento que nos permita conectar con dicho equipo, añadiendo la ruta en Network > Virtual Routers > Static Routes.

Figura 3-19. Configuración para la retransmisión de paquetes DHCP.

A la hora de crear las políticas que determinarán la acción a tomar según el tráfico, pensamos en dos maneras; la primera sería a través de la GUI (Graphical User Interface), lo cual es poco eficaz debido al número de reglas que debían configurarse, por lo que optamos por crearlas mediante comandos. Para ello exportamos de la configuración de Stonegate los objetos y grupos creados con los equipos finales o subredes que se tenían asociadas a la sede. Los comandos necesarios para realizarlo son lo siguientes.

Código 3-1. Creación de objetos y reglas por línea de comandos en un firewall Palo Alto.

```
  // ENTRAR EN MODO PRIVILEGIADO PARA PODER REALIZAR
MODIFICACIONES:
  > configure
  #

  // CREAR OBJETOS:
  // IP:
  # set address “NOMBRE OBJETO” ip-range IP/MÁSCARA
  // FQDN:
  # set address "NOMBRE OBJETO" fqdn "DOMINIO"

  // CREAR GRUPOS:
  # set address-group "NOMBRE GRUPO" static "NOMBRE OBJETO"

  //CREAR REGLAS:
  # set rulebase security rules "NOMBRE REGLA" to ZONA_DESTINO
  # set rulebase security rules "NOMBRE REGLA" from ZONA_ORIGEN
  # set rulebase security rules "NOMBRE REGLA" source [
OBJETO/GRUPO_ORIGEN ]
  # set rulebase security rules "NOMBRE REGLA" destination [
OBJETO/GRUPO_DESTINO ]
  # set rulebase security rules "NOMBRE REGLA" application [
APLICACIÓN ]
  # set rulebase security rules "NOMBRE REGLA" service [ SERVICIO ]
  # set rulebase security rules "NOMBRE REGLA" action [ deny |
allow | drop ]
  # set rulebase security rules "NOMBRE REGLA" profile-setting
group PERFIL_DE_SEGURIDAD
  # set rulebase security rules "NOMBRE REGLA" log-setting
PERFIL_REENVÍO_LOGS
```

3.2.2.2. Cisco C1111-8P

La versión del router que viene de fábrica puede no ser la útlima versión, por lo que puede suponer muchas vulnerabilidades. Por tanto, lo primero que realizamos en estos casos es actualizarlo. Para ello debemos acceder a la página de soporte de Cisco en donde buscaremos por el tipo y modelo del equipo las IOS disponibles. No instalaremos la última versión, ya que esta puede no ser estable o tener fallos no resueltos, por lo que descargaremos la recomendada por el fabricante.

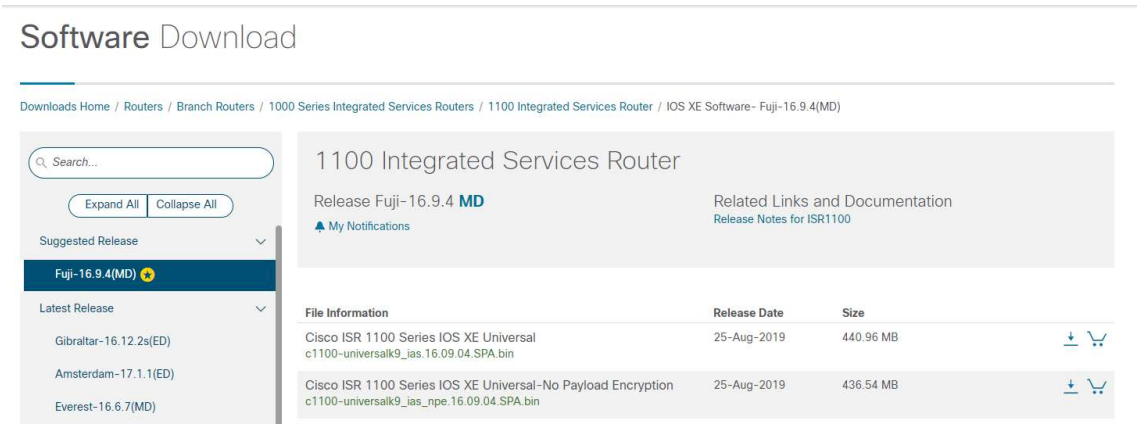


Figura 3-20. Página de Cisco para la descarga de fichero para actualización de dispositivos.

Una vez finalizada la descarga debemos cargar dicho fichero al router, siendo posible realizarlo mediante el protocolo TFTP (Trivial File Transfer Protocol), pero para ello debería estar conectado a la red y tener acceso al servidor desde donde queremos realizar el traspaso, o este modelo permite conectar un USB, por lo que para no realizar configuraciones que luego debamos revertir, optamos por esta segunda opción. Para ello debemos conectarnos al router a través del puerto "console" con el cable que se muestra en la siguiente imagen, el cual está compuesto por un cable RJ45-DB9 conectado a un RS232-USB, extremo el cual conectaremos a nuestro equipo para el acceso a la CLI. Conectamos el USB con el fichero con la versión a instalar y utilizaremos los comandos a continuación mostrados para la importación.

Figura 3-21. Cable de consola.

Figura 3-22. Router Cisco C1111-8P indicando puerto USB y consola.

Para actualizar el router, necesitamos indicarle al equipo cual es el fichero a utilizar una vez reinicie, confirmar que ha cogido el fichero necesario y reiniciar el equipo. Una vez levante, podemos ver si se ha actualizado y

comprobar que efectivamente está utilizando el fichero correcto con los siguientes comandos. Luego procedemos a borrar el fichero anterior para no ocupar innecesariamente memoria en el dispositivo.

Código 3-2. Copiar fichero en un dispositivo Cisco ubicado en un USB.

```
// PASAR DE MODO USUARIO A MODO PRIVILEGIADO:
> enable
#

// EXTRAER FICHERO DEL USB Y GUARDARLO EN LA MEMORIA FLASH:
# copy usb0:NOMBRE_FICHERO flash:NOMBRE_FICHERO_DESTINO
# show flash:

# configure terminal
(config)# boot system flash:NOMBRE_FICHERO_DESTINO
(config)# end
# show boot
# reload

# show version
# show flash:
# delete flash:NOMBRE_FICHERO_ANTIGUO
# delete /force /recursive flash:NOMBRE_DIRECTORIO_ANTIGUO
```

Una vez llegado a este punto podemos comenzar a configurar el router según las necesidades que presenta la red. Si revisamos el mapa de red que esperamos tener, observamos que necesitaremos configurar las IPs pertenecientes a cada una de las subredes (Management – 10.90.48.2/27, WAN – IP PÚBLICA y DMVPN – 10.90.49.148/29), además de las rutas estáticas que consideremos oportunas, como la salida hacía Internet.

A lo largo del proyecto se han mencionado varias veces los túneles DMVPN (Dynamic Multipoint Virtual Private Network); es un diseño propietario de Cisco, el cual supone un avance para las VPN "Hub and Spoke" donde se implementan túneles estáticos entre un equipo central y el resto de los extremos. En esta arquitectura, todo el tráfico siempre tendría que pasar por el enrutador principal que tendrá que reenviar la información de un túnel a otro, pudiendo ocasionar colisiones y retardos en el flujo de información. A pequeña escala esta configuración puede resultar útil, pero a medida que la red comienza a crecer no será la solución óptima. Dicho protocolo trata de descubrir bajo demanda y de manera dinámica los destinos de los túneles mGRE (multipoint Generic Routing Encapsulation), los cuales son aprendidos por NHRP (Next Hop Resolution Protocol) y las comunicaciones continuarán siendo seguras ya que se realizan a través de Ipsec (Internet Protocol security) que cifrará los datos transmitidos. El tráfico entre todos los equipos se realizará usando una única subred asignadas a las interfaces mGRE, que en nuestro caso será 192.168.249.0/24.

MGRE es una extensión del protocolo GRE, desarrollado por Cisco Systems, que estable una conexión donde se encapsulan los datos transmitidos entre dos puntos por un túnel. Con mGRE se consigue que la misma interfaz del túnel pueda utilizarse para establecer varias sesiones remotas simultáneamente, por lo que se simplifica significativamente la configuración.

El protocolo NHRP se define en la RFC 2333 de la organización IETF (Internet Engineering Task Force), siendo un protocolo de capa 2 utilizado para determinar el direccionamiento público del resto de Spokes. Definimos dos roles para el paso de mensajes, el servidor (NHS – Next Hop Server), que será el hub, y los clientes (NHC – Next Hop Client). En la siguiente imagen podemos ver el paso de mensajes para establecer la conexión; primero los equipos de las sedes mandan un "NHRP Registration Request" al router central, por lo que este actualiza la entrada de la tabla que asocia la IP pública de este con la interna de la interfaz del túnel mGRe. Una vez establecida la conexión con el Hub, para que un extremo conozca al otro, se intercambian "NHRP Resolution Request" los cuales reenvía el central de un Spoke a otro, permitiéndose así la comunicación directa entre ellos.

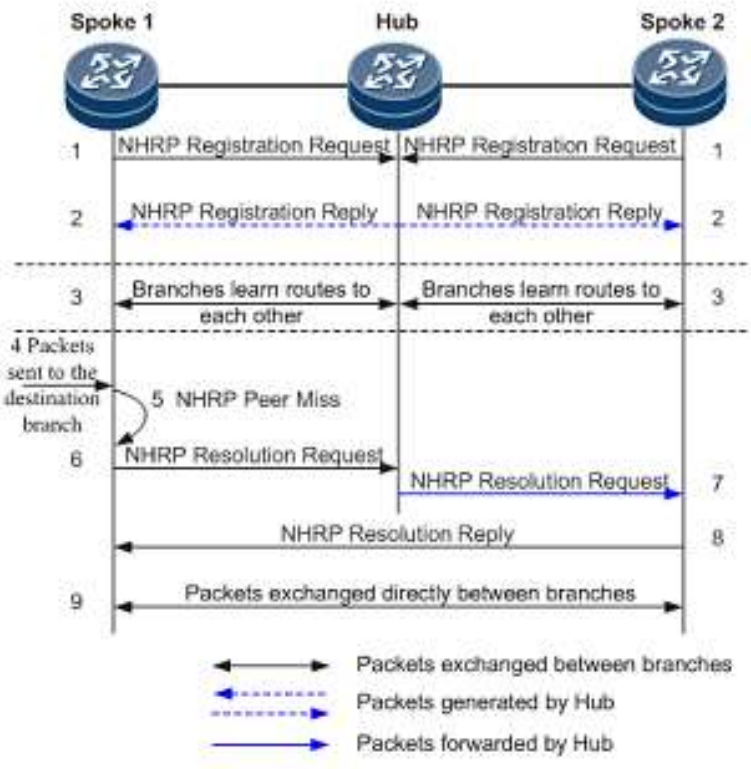


Figura 3-23. Paso de mensajes del protocolo NHRP (Next Hop Resolution Protocol).

Para poder visualizar la tabla de asociaciones en los router cisco solo tenemos que ejecutar el comando que se observa en la siguiente figura en modo privilegiado.

```
[redacted]#sh ip nhrp brief
**************************************************************************
    NOTE: Link-Local, No-socket and Incomplete entries are not displayed
**************************************************************************
Legend: Type --> S - Static, D - Dynamic
        Flags --> u - unique, r - registered, e - temporary, c - claimed
        a - authoritative, t - route
==========================================================================

Intf     NextHop Address                                    NBMA Address
         Target Network                              T/Flag
-------- ------------------------------------------ ------ ----------------
Tu100    192.168.249.2                                      [redacted]
         192.168.249.2/32                            D/r
Tu100    192.168.249.3                                      [redacted]
         192.168.249.3/32                            D/r
Tu100    192.168.249.7                                      [redacted]
         192.168.249.7/32                            D/r
Tu100    192.168.249.8                                      [redacted]
         192.168.249.8/32                            D/r
Tu100    192.168.249.9                                      [redacted]
         192.168.249.9/32                            D/r
```

Figura 3-24. Información sobre el protocolo NHRP en un dispositivo Cisco.

Hasta ahora hemos comentado los protocolos necesarios para levantar los túneles, pero para saber el direccionamiento que se encuentra detrás de cada uno de los encaminadores necesitaremos utilizar algún protocolo de routing dinámico, en nuestro caso utilizaremos EIGRP (Enhanced Interior Gateway Routing Protocol), de esta manera las sedes tendrán comunicación entre ellas. Se optó por este protocolo debido a que proporciona tiempos de convergencia considerablemente bajos, lo cual en una red como la de nuestro cliente y con el trabajo que desempeñan es imprescindible.

La configuración en los equipos necesarios para poder establecer los túneles DMVPN es la siguiente. El

esquema de red del Hub con el resto de las sedes es el que se muestra en la siguiente imagen, donde hay que recalcar que debe haber conexión entre las IPs públicas de las distintas sedes previa a la configuración del DMVPN. Las IPs asignadas dentro del rango 192.168.248.0/24 serán la asignadas a las interfaces mGRE.

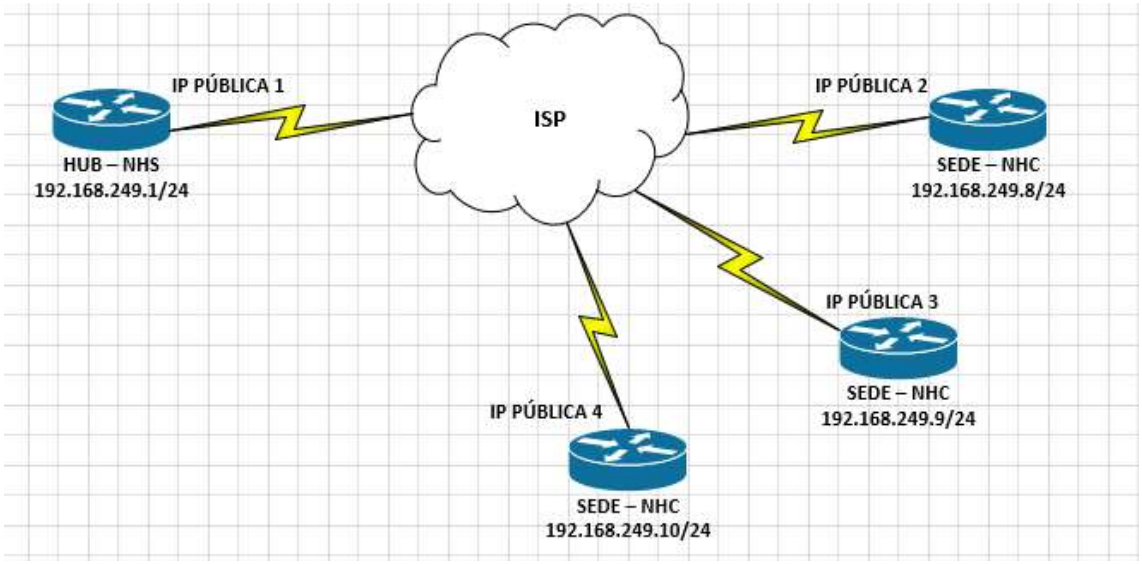


Figura 3-25. Diagrama de conexión entre el servidor y los clientes del protocolo NHRP.

Comenzaremos por detallar los comandos necesarios en el router central y después la utilizada en los extremos.

Configuraremos IPSec (será igual tanto en el Hub como en el resto de las sedes), para esto usaremos el protocolo ISAKMP (Internet Security Association and Key Management Protocol), que se encarga de la negociación entre dos equipos para establecer las pautas que se seguirán con el fin de conseguir una comunicación segura con autenticación de los extremos y encriptación de los datos transmitidos.

Código 3-3. Configuración en el extremo del Hub.

```
interface GigabitEthernet1
 description WAN
 ip address IP_PÚBLICA1 MÁSCARA

crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 2
crypto isakmp key XXXXXXXX address 0.0.0.0
crypto ipsec security-association replay window-size 1024
crypto ipsec transform-set ESP-AES128-SHA esp-aes esp-sha-hmac
 mode transport
crypto ipsec profile DMVPN_PROFILE
 set transform-set ESP-AES128-SHA
```

La configuración del túnel será la siguiente.

Código 3-4. Configuración en el extremo del Hub.

```
interface Tunnel100
 description Tunel DMVPN
 bandwidth 100000
 ip address 192.168.249.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication XXXXXXXXX
 ip nhrp network-id 100
 ip nhrp holdtime 300
 ip nhrp registration timeout 30
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 500
 qos pre-classify
 tunnel source GigabitEthernet1
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN_PROFILE shared
 ip virtual-reassembly

router eigrp 100
 network 192.168.249.0
 redistribute static
```

En la configuración del túnel de las sedes debemos indicar tanto la IP pública como la que se utiliza en la interfaz GRE del router central.

Código 3-5. Configuración en los equipos de las sedes.

```
interface GigabitEthernet0/1/1
 description WAN
 ip address IP_PÚBLICA2 MÁSCARA

interface Tunnel100
 description DMVPN
 bandwidth 10000
 ip address 192.168.249.8 255.255.255.0
 ip mtu 1400
 ip nhrp authentication XXXXXXXXX
 ip nhrp map 192.168.249.1 IP_PÚBLICA1
 ip nhrp map multicast IP_PÚBLICA1
 ip nhrp network-id 100
 ip nhrp holdtime 300
 ip nhrp nhs 192.168.249.1
 ip nhrp registration timeout 30
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 500
 tunnel source GigabitEthernet0/1/1
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN_PROFILE shared


router eigrp 100
 network 192.168.249.0
 redistribute static
```

De esta manera ya tendremos establecidos los túneles y a medida que necesitemos acceder a las redes privadas detrás de cada uno de los routers de las distintas sedes, se irán levantando de manera dinámica el resto.

```
[redacted]#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel100, IPv4 NHRP Details
Type:Hub, NHRP Peers:21,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 [redacted]      192.168.249.8    UP     3w0d     D
     1 [redacted]      192.168.249.9    UP     1w3d     D
```

Figura 3-26. Túneles levantados visto desde el extremo del router central.

```
[redacted]#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel100, IPv4 NHRP Details
Type:Spoke, NHRP Peers:5,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 [redacted]      192.168.249.1    UP    1d03h     S
     1 [redacted]      192.168.249.2    UP    4d13h     D
     1 [redacted]      192.168.249.9    UP 00:00:06     D
```

Figura 3-27. Túneles levantados visto desde el extremo del router satélite.

Con esto tendremos configurado el equipo cisco C1111-8P.

3.2.2.3. Cisco WS-C2960X-24PS-L

Como ya hemos comentado anteriormente, está sede ya se encontraba en producción, y este equipo es uno de los que estaban desplegados en el edificio principal, por lo que la configuración básica no fue necesaria.

Se trataban de dos switches Cisco WS-C2960X-24PS-L conectados entre sí, donde el cliente estableció como requisito que se estableciese un stack para gestionarlo como uno solo. Para ello necesitaríamos un módulo Catalyst 2960-X FlexStack Plus para cada switch y un par de cables CAB-STK-E para la conexión.

Figura 3-28. Módulo Catalyst 2960-X FlexStack Plus.

Figura 3-29. Cable CAB-STK-E.

En la configuración de cada uno de los equipos debemos establecer la prioridad que tendrán en la negociación de cuál de ellos se convertirá en el switch maestro, es decir, el que realizará las gestiones, al que se accederá y el que se encargará de guardar y periódicamente enviará al resto la última configuración del stack. La prioridad se establece numéricamente, del 1 al 15, cuanto mayor sea esta, mayor será la posibilidad del switch de convertirse en el master, para ello utilizamos los siguientes comandos.

Código 3-6. Comandos para establecer la prioridad en el stack de cada switch.

```
# configure terminal
(config)# switch NÚMERO_MIEMBRO_STACK priority PRIORIDAD
```

En la zona trasera de los equipos debemos insertar los módulos y atornillarlos, conectando el puerto etiquetado como “STACK 1” del switch que queramos considerar como maestro, al “STACK 2” del equipo esclavo y viceversa. Podemos ver como debe ser la conexión en las siguientes imágenes.

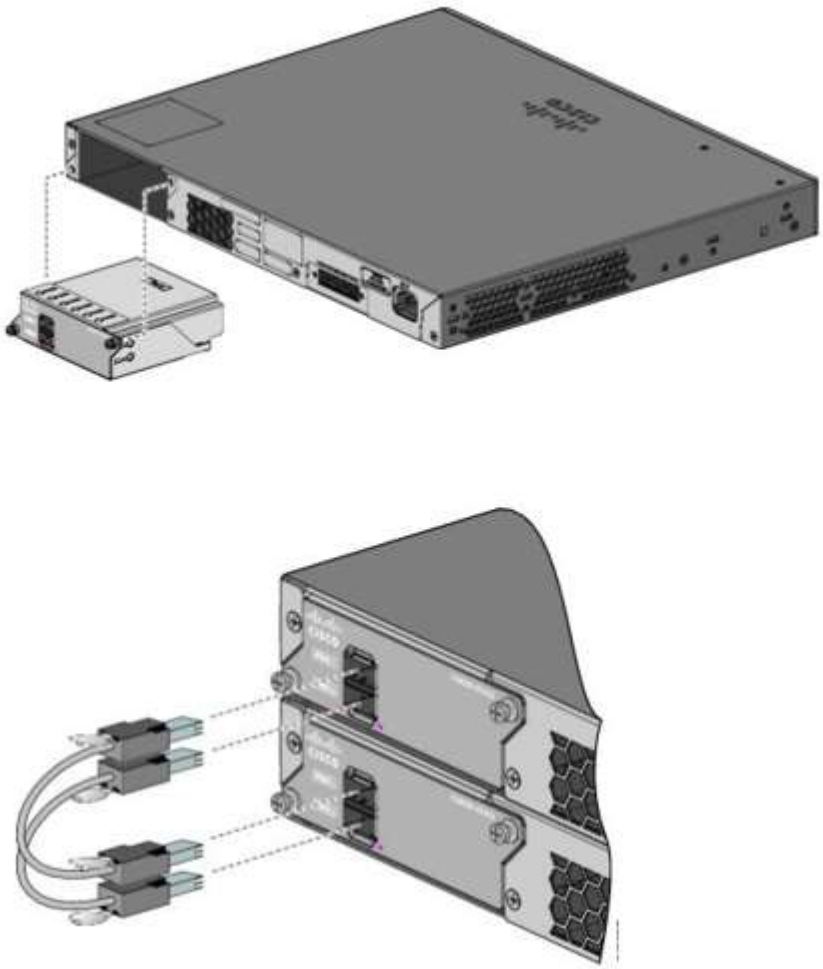


Figura 3-30. Instalación del FlexStack y conexión entre switches.

Una vez conectados, en el equipo principal debemos indicar la asociación del resto de miembros, especificando el modelo de equipo que va a formar parte del stack, en nuestro caso “ws-c2960x-24ps-l”.

Código 3-7. Comandos para asociar el resto de miembros al equipo master.

```
(config)# switch NÚMERO_MIEMBRO_STACK provision TIPO
```

Finalmente, reiniciamos los esclavos y ya tendríamos la configuración del stack completa.

```
[redacted]#show switch
Switch/Stack Mac Address : [redacted]
                                            H/W   Current
Switch#  Role    Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Master  [redacted]         15     4        Ready
 2       Member  [redacted]         1      4        Ready
```

Figura 3-31. Estado y orden del stack.

```
[redacted]#sh switch stack-ports
  Switch #    Port 1       Port 2
  --------    ------       ------
    1           Ok           Ok
    2           Ok           Ok
```

Figura 3-32. Estado de los puertos del stack.

Para conectar los switches entre sí, como hemos mencionado anteriormente, necesitamos hacer uso de los puertos SFP. Según el esquema de red que fue validado, al core se conectarían el Switch02 y el Switch03. De los seis módulos GLC-SX-MMD que se adquirieron se necesitarán dos, los cuales conectaremos al primer puerto SFP de cada uno de los equipos que forman el stack, repartiendo de esta manera las conexiones evitamos que ante fallo de alguno de ellos no se pierda conectividad con el resto de la infraestructura. Estos puertos serían el Gi1/0/25 y Gi2/0/25, los cuales configuraremos en modo "trunk" de manera que todas las vlans puedan ser transmitidas entre zonas.

Los cables que se usaron fueron de tipo LC/PC a SC/PC multimodo, conectados al puerto SFP y al panel de parcheo respectivamente, con una velocidad de 1Gbit/segundo.

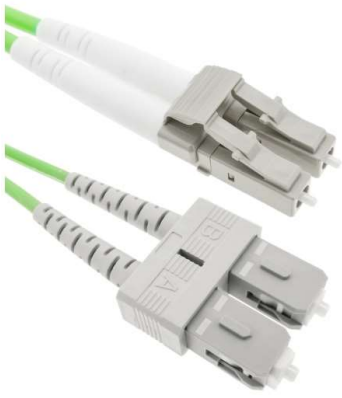


Figura 3-33. Conectores LC/PC a SC/PC de latiguillos de fibra multimodo.

```
[redacted]#sh int gi1/0/25
GigabitEthernet1/0/25 is up, line protocol is up (connected)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 1000Mb/s, link type is auto, media type is 1000BaseSX SFP
```

Figura 3-34. Información de la interfaz de fibra.

Para controlar el tipo de tráfico, el cliente solicitó que se instalase una sonda de red para el análisis y detección de ataques, utilizando el modelo "Logic Supply IMB-186". Se pensó que, habiendo puertos disponibles, lo más lógico era que se conectase esta al switch de core, ya que todo tráfico pasará por este, por lo que tuvimos que configurar un "port mirror" o también conocido como SPAN (Switched Port Analyzer). Al habilitar este método, el switch enviará copias de los paquetes cursados por la red al puerto de la sonda. Para ello necesitamos configurar dos interfaces, una para la gestión remota del equipo y el otro que será el destino donde se reenvíe todo el tráfico. Para este último, debemos utilizar los siguientes comandos.

Código 3-8. Comandos para monitorizar la información transmitida por distintos puertos.

```
(config)# monitor session NÚMERO source interface INTERFAZ
(config)# monitor session NÚMERO destination interface Gi2/0/20
```

La interfaz destino, en nuestro caso Gi2/0/20, no está configurada a ninguna interfaz.

Como se puede ver en la siguiente captura, nosotros optamos por monitorizar todos los puertos del switch, sin especificar VLANs, por eso "Ingress" está en estado "disabled".

```
          #sh monitor session 1
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Gi1/0/1-28,Gi2/0/1-18,Gi2/0/21-28
Destination Ports      : Gi2/0/20
    Encapsulation      : Native
          Ingress      : Disabled
```

Figura 3-35. Información de los puertos monitorizados en la sesión establecida.

Aparte de configurar los puertos en las distintas VLANs dependiendo de los equipos que se conecten a cada uno de ellos, podríamos dar por finalizada la configuración de este equipo.

3.2.2.4. Cisco WS-C2960C-12PC-L

Una vez tuvimos los equipos en mano, los actualizamos todos a la última versión recomendada por el fabricante, de esta manera evitábamos vulnerabilidades o defectos de las anteriores.

Tuvimos que etiquetar cada uno de los firewalls para saber que configuración tendría cada uno de ellos, además de asignarles las IPs de gestión que tendrán. Para ello, lo primero fue crear la VLAN correspondiente, asignarle a cada uno la IP especificada en el mapa de red final y especificar la puerta de enlace, la cual debe estar en la misma subred, en nuestro caso, el firewall.

Código 3-9. Comandos para la creación de Vlans.

```
(config)# vlan ID
 (config-vlan)# name NOMBRE
(config)# interface vlan ID
 (config-if)# ip address IP MÁSCARA
(config)# ip default-gateway IP-GW
```

Creamos el resto de VLANs utilizadas en la sede y configuramos todos los puertos de acuerdo al documento "Port Allocation" validado por el cliente, información la cual podemos ver en uno de los anexos [Anexo C].

Por último, de las configuraciones significativas de un switch, es el acceso remoto a este, decantándonos por el protocolo ssh ya que es más seguro que telnet porque encripta los datos de la transmisión en vez de transmitirlos en texto plano. Por supuesto, el puerto TCP 22 que es el que utiliza este protocolo, debe estar permitido en las reglas del firewall para poder acceder los equipos.

El switch debe tener asignado un "hostname" además del dominio de la sede. Debemos generar la clave RSA (Rivest–Shamir–Adleman), lo cual genera una clave pública de encriptación y una privada para desencriptar, de esta manera aseguramos la transmisión segura de datos. Estas claves se almacenarán en la memoria NVRAM (Non-volatile random access memory - memoria de acceso aleatorio no volátil), la cual es privada, no pierde la información y no se mostrará en la configuración del equipo. Debemos indicar la longitud en bits de las claves que queremos generar, el máximo es 4096, aunque se recomienda 1024 o 2048.

Código 3-10. Configuración del protocolo SSH en el dispositivo.

```
(config)# hostname NOMBRE-EQUIPO
(config)# ip domain-name DOMINIO
(config)# crypto key generate rsa modulus BITS
(config)# ip ssh versión 2
```

En la gestión de líneas VTY, que son unos puertos virtuales para el acceso remoto a la administración del equipo, debemos restringir únicamente a ssh, donde también podemos indicar el nivel de privilegio que debe tener el usuario local para poder entrar a este.

Código 3-11. Configuración del acceso al equipo según el privilegio del usuario.

```
(config)# username USUARIO privilege PRIVILEGIO (1-15) secret 0
CONTRASEÑA
(config)# service password-encryption
(config)# line vty 0 4
(config-line)# privilege level PRIVILEGIO-MÍNIMO-ACCESO
(config-line)# transport input ssh
```

Con esto podríamos dar por terminada la configuración necesaria para el despliegue de estos equipos.

3.2.2.5. Cisco AIR-AP1832I-E-K9

Para la configuración de los puntos de acceso no tuvimos que configurar mucho en el propio equipo, ya que en la oficina poseíamos un switch y un router plataformados e incluídos en la red del cliente, por lo que podíamos simular que estos estuviesen directamente conectados y poder registrarlos contra la controladora (Cisco Wireless LAN Controller - WLC).

Para esta simulación debíamos tener configurado un DHCP relay, de manera que los paquetes "DHCP Discovery", para que el AP pudiera recibir una IP, máscara o información de la propia controladora, no se quedasen en local y llegasen a la red corporativa del cliente. En la sede, como hemos visto antes, esto se realizó en el Palo Alto, donde se indicar la IP del servidor que ofrece DHCP a toda la empresa, en laboratorio utilizamos el comando "ip helper-address" para dar las pautas. En el servidor se utiliza la "Opción 43" donde se especifica la IP de la controladora, que es la manera recomendada cuando los puntos de acceso y la controladora se encuentran separadas y sobre todo para grandes organizaciones, donde no sería óptimo tener

que configurar equipo a equipo con una IP estática.

Una vez el AP recibe la información necesaria para establecer la conexión, entra entra en uso el protocolo CAPWAP (Control And Provisioning of Wireless Access Points Protocol), protocolo de capa de aplicación descrito en la RFC 5415, el cuál utiliza los puertos UDP 5246 y 5247 para la comunicación con la WLC. En la siguiente imagen podemos ver el paso de mensajes de este protocolo.

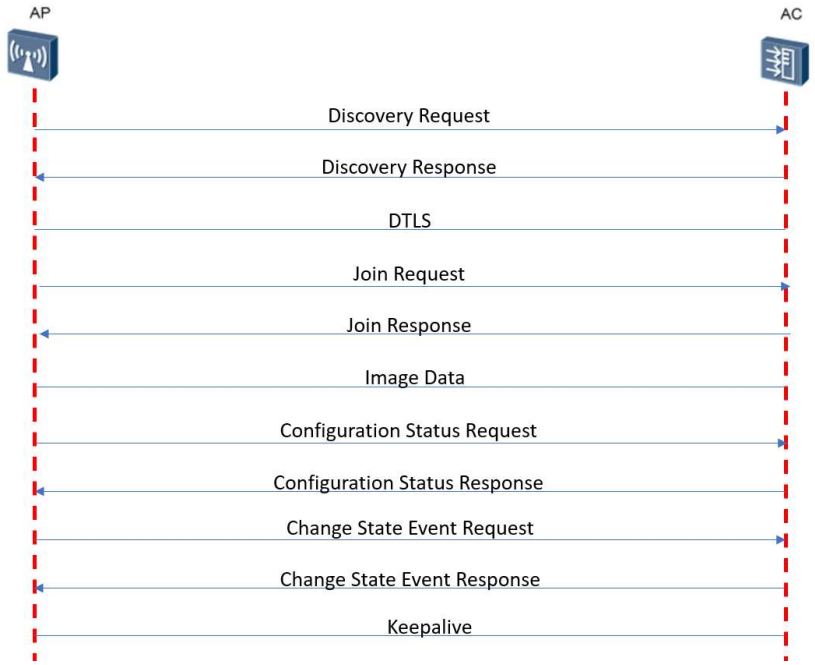


Figura 3-36. Paso de mensajes del protocolo CAPWAP.

En la fase de “Discovery”, el AP comunica con las posibles controladoras que haya en la red, y se asocia con aquella que mayor prioridad tenga, en nuestro caso, los mensajes transmitidos no serán de difusión ya que el servidor DHCP le ofreció la IP de la que debe recibir la información.

El protocolo DTLS (Datagram Transport Layer Security) se utiliza para encriptar los paquetes transmitidos entre WLC y AP, de manera que se evitan accesos indeseados o modificaciones de la información enviada.

Tras establecer el canal de control por el puerto UDP 5246 entre ambos dispositivos, se comprueba la versión del software actual del AP y si esta no es la última la controladora se encargará de enviársela, por lo que el equipo entrará en modo actualización, reiniciándose, y una vez finalizado, volverán a conectarse. Intercambiarán la información necesaria para que el punto de acceso ofrezca los servicios.

En la WLC, debemos establecer unos cuantos parámetros específicos para la configuración de los equipos que pertenecerán a una sede específica dentro de la organización. Para ello, primero crearíamos el grupo al que pertenecerán e incluirlos en este una vez registrados en la controladora. Otro punto importante, es configurar todos los equipos en modo “FlexConnect”, esto permite tener la arquitectura de red que estamos diseñando, donde no es necesaria una controladora por sede y estos equipos pueden ser gestionados desde una centralizada a través de la WAN (Wide Area Network). Otras ventajas de este modo son la conmutación del tráfico y la autenticación de los usuarios, la cual se realiza localmente sin necesidad de reenviar esta información a la WLC, por lo que permite que la red sea escalable pudiendo desplegar más sedes sin necesidad de que todos los datos tengan que pasar por la controladora.

3.3. Probar el cambio

3.3.1. Pruebas previas al despliegue

Como hemos podido ver a lo largo del apartado anterior, los equipos se mandaron a la planta con las configuraciones hechas, de manera que durante el tiempo que teníamos "in situ" fuese para la solución de los posibles problemas que nos pudiésemos encontrar, o de realizar cambios que no se hubiesen tenido en cuenta.

Una vez configurado todo, se hicieron pruebas en laboratorio, de manera que, teniendo todos los equipos conectados entre sí, no se generasen bucles o no funcionasen las comunicaciones locales. Para los puntos de acceso, los conectamos a la réplica de sede del cliente que teníamos configurada en vez de a la nueva infraestructura de red que habíamos creado, de manera que pudiésemos probar el funcionamiento de los distintos SSID corporativos.

Sin embargo, la integración del firewall en Panorama no pudo hacerse previamente ya que debía estar en producción con salida a Internet con la IP pública asignada por el proveedor. Para ello, primero tendríamos que especificar en el propio Palo Alto la información del gestor como se puede ver en la próxima imagen.

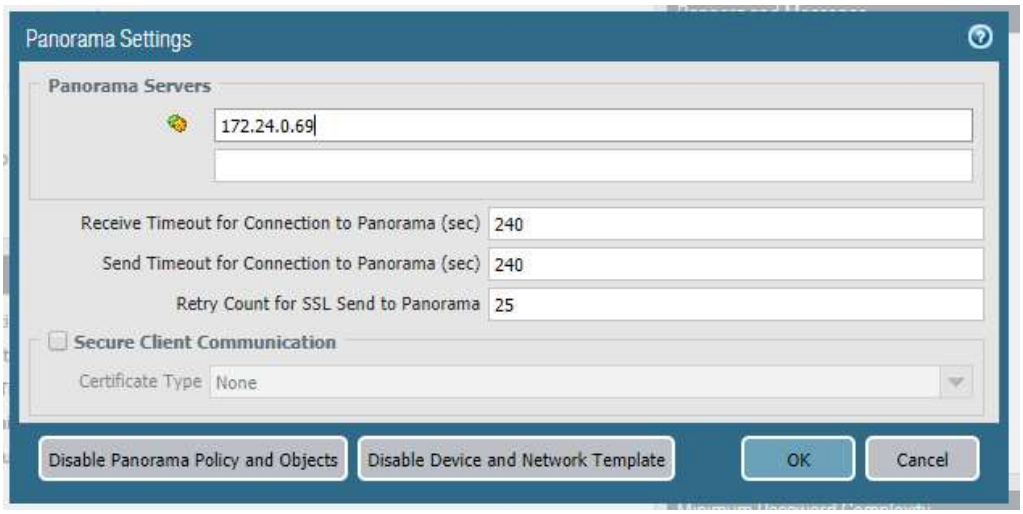


Figura 3-37. Configuración de Panorama en el firewall.

En la interfaz gráfica de Panorama agregar el nuevo firewall como equipo gestionado introduciendo el número de serie del equipo e importando luego su configuración. Desde la misma pantalla, una vez haya terminado el paso anterior, habrá que seleccionar la opción "Export or push device config bundle" de manera que Panorama pasará a ser la propietaria de las reglas locales del firewall, pudiendo gestionar estas también desde la interfaz gráfica central, junto a las compartidas con el resto de sedes.

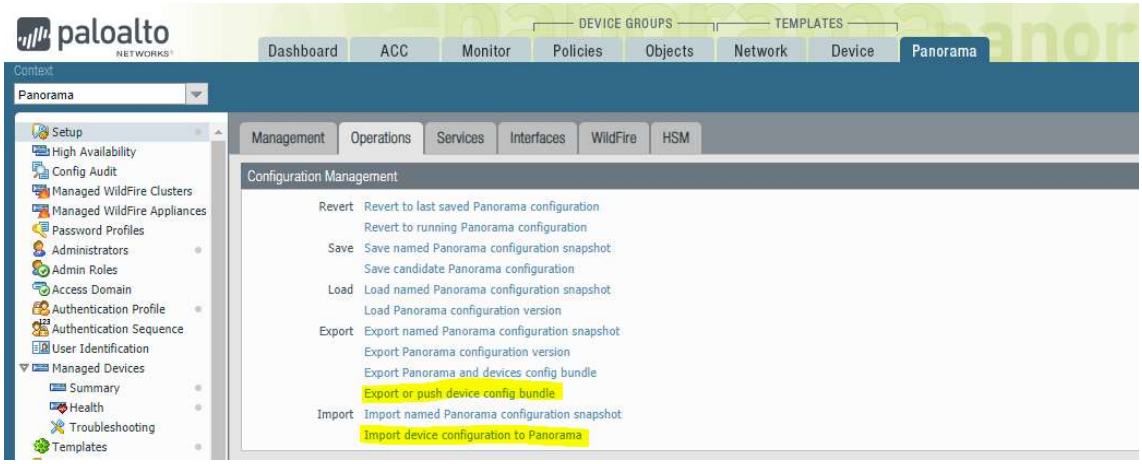


Figura 3-38. Exportar la configuración del equipo para su gestión centralizada en Panorama.

3.4. Análisis del rendimiento

Una vez implementado el cambio, rigiéndonos lo máximo posible por la planificación establecida, solventando los posibles errores que fuesen apareciendo a lo largo del despliegue, se pasaría a la prueba de todos los servicios establecidos en un "checklist" con el cliente, donde se especificaba tanto los nuevos accesos corporativos como los que tenían que mantener de la antigua arquitectura.

3.4.1. Comprobación de todos los servicios

Hablando con el cliente, además de tener la experiencia de gestionar la red, se especificaron los siguientes puntos de la lista, los cuáles podrían comprometer la productividad de la sede, por lo que deberían quedar todos validados.

El checklist se compone de las siguientes pautas.

- Puesto de usuarios, lo principal era comprobar la correcta configuración de todos los puertos que sería utilizados para los trabajadores de la planta y revisar las tomas desde las mesas, pasando por los paneles de parcheo hasta conectar en el switch. Nos cercioramos de que el cableado no estuviese dañado.
- DMVPN, una vez el túnel principal estuviese establecido, se probaron distintos accesos a sedes remotas con resultados exitosos, revisando que el equipo central compartiese la información para el establecimiento del resto de VPNs entre distintas oficinas.
- DHCP, hubo que comprobar que todos los usuarios recibiesen una IP de la subred destinada para ello, tanto si el acceso se realizaba por Wi-Fi como por cable, validando así la configuración de los "DHCP relay" configurados en le firewall para que alcanzasen el servidor, al ser necesario el reenvío de los mensajes de este protocolo.
- DNS, la resolución es imprescindible, tanto para la navegación que posteriormente pasaríamos a verificar, como el acceso a servidores internos a la organización por la nomenclatura definida en la empresa.
- Autenticación de usuarios contra el Directorio Activo.
- Acceso a Internet.
- Wi-Fi, se probaron todas las redes Wi-Fi desplegadas, tanto el acceso y autenticación, como el direccionamiento otorgado y la conexión con los servicios detallados anteriormente. Se probó también

que la red de invitados estuviese aislada, como indicaba uno de los requisitos.

- Realización de copias de seguridad de todos equipos desplegados, comprobando en el servidor que estas se realizaban correctamente y que se registraban las incrementales en los cambios que se iban realizando.
- Tráfico habilitado a resto de servicios utilizados en la planta.

3.4.2. Validación

Solo tras haber realizado todas las comprobaciones realizadas y viendo que los resultados fuesen satisfactorios, se podría dar por validado el cambio.

Por nuestra parte realizamos todas las pruebas detalladas en el punto anterior, acordadas con el cliente, desde los equipos de red, de manera que el groso de incidencias se resolviesen antes de que los trabajadores pudiesen percibirlas.

Se solicitó a los usuarios de la planta que revisasen todos los servicios con los que trabajaban en su día a día, solventando errores que pudiesen ir surgiendo, categorizándolos según el número de usuarios afectados, criticidad y prioridad. Fue importante determinar el orden a solventar dichos problemas, ya que un error general supone que durante el despliegue no se tomaron en cuenta ciertas pautas y por tanto debían ser solventadas y documentadas lo más rápido posible.

Tras analizar todos los comentado, validar que los usuarios trabajaban con normalidad y comprobar que el cambio había sido satisfactorio, se pudo dar por finalizado el despliegue como exitoso.

3.5. Cierre del proyecto

3.5.1. Documentación de todos los cambios realizados

Una vez desplegado, la documentación de la sede debía ser actualizada y compartida con el cliente para que este dispusiese de la información del resultado final.

El listado que se deberá modificar sería el siguiente.

- Mapa de red lógico y físico, los cuales se crearon en la fase de diseño del proyecto, añadiendo posibles cambios que surgiesen a lo largo del despliegue.
- Actualización de GestioIP con el direccionamiento utilizado, esta es una herramienta la cual recoge las distintas subredes en producción, pudiendo especificar a que equipo está asignada que IP fija, de manera que para el soporte o posterior gestión de estos.
- Archivo de Mantenimiento de equipos, Smartnets, lo cual es un servicio de Cisco que permite a las empresas que poseen dispositivos de este fabricante el acceso a soporte, actualización y reemplazo en caso de estar defectuosos sin algún coste. Este servicio es uno de los adquiridos y contemplados en la facturación.
- Añadir nuevos equipos a la herramienta de monitorización, Zabbix. La producción del cliente debe verse afectada lo mínimo posible ante caídas o fallos de los equipos de IT, por lo que se monitoricen de manera que se pueda actuar cuanto antes para restaurar el servicio.
- Inventario de equipos físicos donde se especifique modelo, números de serie y versión de firmware actual.

- Inventario WAN, donde se detalla el direccionamiento público, compañía del operador y caudal contratado, además de los datos de contacto.
- Directorio activo, donde se reservará el direccionamiento para que este pueda ofrecer por DHCP las IPs de los usuarios en la red, además de dar de alta en la red corporativa a los trabajadores con sus credenciales correspondientes.
- Actualización del archivo de contraseñas, utilizando para ello la herramienta Keepass.

3.5.2. Herramientas utilizadas para la monitorización de los equipos

Para la supervisión de la disponibilidad de los dispositivos desplegados, el cliente utiliza la herramienta de Zabbix.

Habrá que configurar en todos los dispositivos el protocolo SNMP (Simple Network Management Protocol) para que se pueda recaudar la información necesaria y establecer alertas en ante caídas.

Los comandos para en el switch como en el router son las mismas, por lo que indicaremos los comandos a utilizar una sola vez. Habrá que especificar la IP del servidor donde tenemos montada la máquina de Zabbix, que se encargará de recoger la información de los equipos, además de la comunidad propia de la empresa. Es imprescindible que haya comunicación con dicho servidor, además de permitir el tráfico por el puerto TCP 161.

Código 3-11. Configuración del protocolo SNMP en un equipo Cisco.

```
(config)# snmp-server community COMUNIDAD ro
(config)# snmp-server host IP_SERVIDOR version 2c COMUNIDAD
```

En el Palo Alto debemos acceder a la configuración del equipo y en la pestaña de “SNMP Traps” añadir un nuevo perfil, donde especificaremos la misma información del servidor. En otra pestaña debemos especificar la versión de SNMP que utilizaremos, que será la V2c.

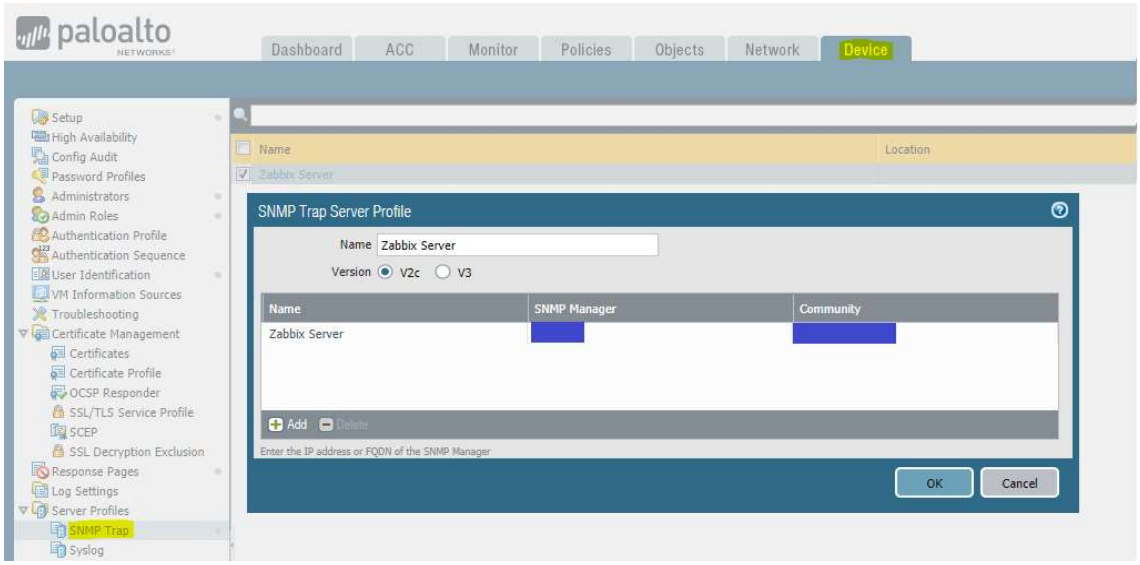


Figura 3-39. Configuración del perfil de SNMP Traps en Palo Alto.

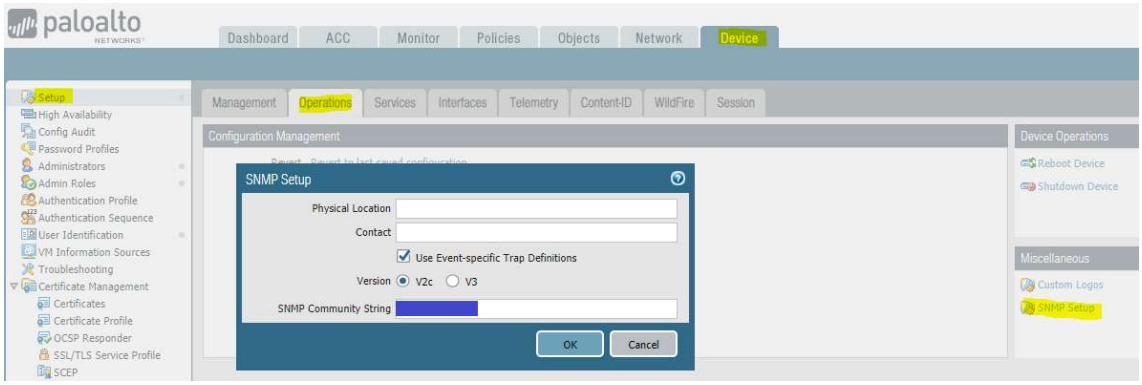


Figura 3-40. Configuración de SNMP en Palo Alto.

Con estos pasos tendríamos los dispositivos que queremos monitorizar desde Zabbix, por lo que desde la CLI de este podremos probar si efectivamente están bien realizadas las configuraciones.

Obtener información general de un equipo, con este comando podremos obtener todos los OIDs/MIBs del equipo que corresponda a la IP destino que especifiquemos.

Código 3-12. Comando snmpwalk.

```
snmpwalk -v2c -c MACRO_COMMUNITY IP_DESTINO [-On] [MIB]
```

Si buscamos un único valor de una variable específica utilizaremos el comando "snmpget".

Código 3-13. Comando snmpget.

```
snmpget -v2c -Cf -c MACRO_COMMUNITY IP_DESTINO OID.n
```

Accediendo a la interfaz gráfica, daremos de alta cada host, podremos asignarles plantillas, crear gráficas de disponibilidad o programar disparadores que conlleven una acción cuando se cumplan, como por ejemplo que envíen un correo.

Aplicaremos una plantilla, configurada previamente, describiendo cada ítem que tiene y su funcionalidad.

Los primeros que comentaremos serán utilizados para graficar la disponibilidad de los equipos.

- Icmppingloss, este objeto indica el porcentaje de pérdida de paquetes ICMP contra los hosts monitorizados
- Icmppingsec, devuelve el tiempo en segundo que tarda la respuesta del ping

Con ellos configuramos unos "triggers" o disparadores, que se tratan de condiciones que si se cumpliesen conllevarían una acción, un ejemplo sería que se activase cuando el equipo lleve más de 15 minutos sin responder y se enviase un correo para poder actuar en consecuencia y así evitar cortes prolongados en el trabajo de los usuarios. Crearemos gráficas también para tener un histórico de cada uno de los equipos, ya que como hablaremos más adelante en el plan de soporte ofrecido al cliente, debe existir una disponibilidad superior al 98% mensualmente.

Otra información que el cliente solicita saber es el caudal que pasa por cada una de las interfaces de los

dispositivos, pero al tener distintos tipos, no sería óptimo crear cada ítem individualmente, por lo que Zabbix ofrece la opción de descubrirlas automáticamente. En la siguiente imagen se muestra el "Discovery rule" creado, el cual a partir del objeto "ifDescr" es capaz de obtener todas las que existe en un equipo y crear un objeto asociado a la interfaz.

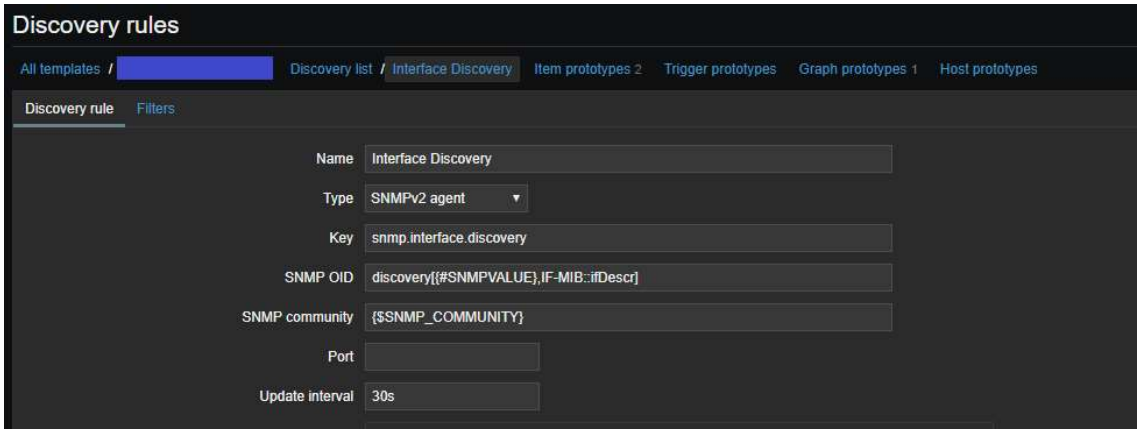


Figura 3-41. Configuración para descubrir por SNMP las interfaces en Zabbix.

Para que cree un ítem por cada interfaz de cada host, debemos indicar un prototipo de cuál es el parámetro deseado para ello, es decir, que información queremos sacar de cada uno de los puertos. En nuestro caso nos interesa el tráfico entrante y el saliente.

- ifHCInOctets[{#SNMPINDEX}], octetos entrantes en la interfaz guardada en la variable SNMPINDEX.
- ifHCOutOctets[{#SNMPINDEX}], octetos salientes de la interfaz guardada en la variable SNMPINDEX.

En la siguiente imagen podemos ver como se mostraría el tráfico cursado por una de las interfaces del firewall.

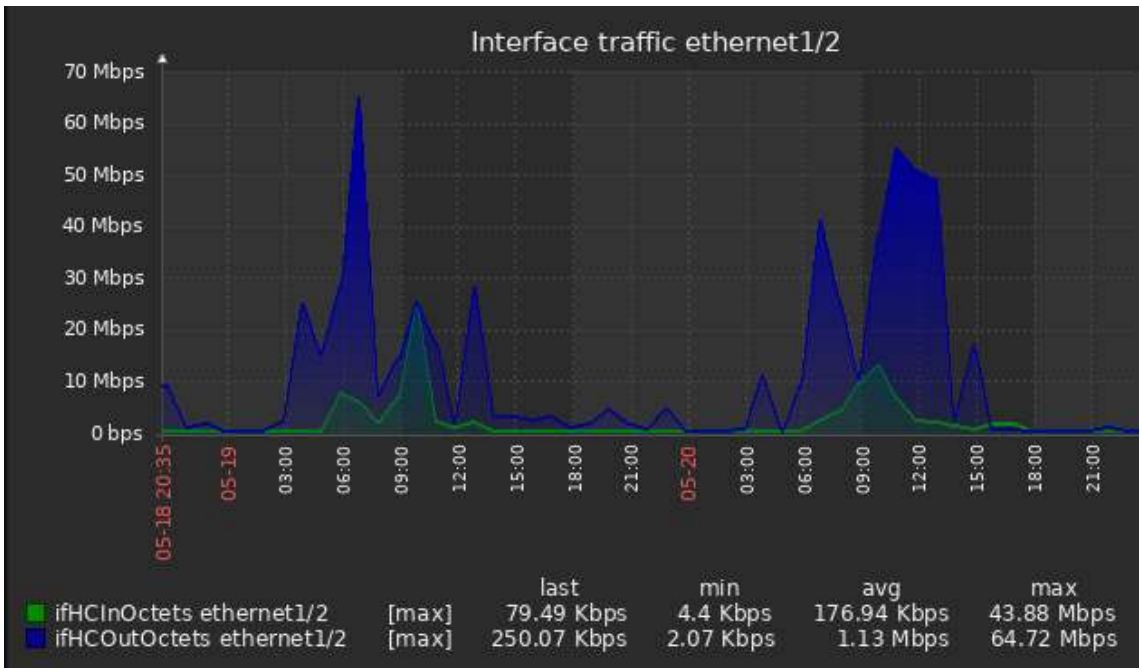


Figura 3-42. Gráfico del tráfico cursado por una interfaz del firewall.

Una vez validado, se da por terminado el proyecto del despliegue de la nueva sede en la red corporativa del cliente.

3.6. Soporte del cambio

3.6.1. Plan de Soporte para la empresa

El cliente tenía un plan de soporte, por lo que tras finalizar el proyecto, se pasaría a recepcionar y solvertar los distintos tickets que fuesen surgiendo a raíz de problemas que puedan surgir o cambios preaprobados, es decir, aquellos que no necesitan pasar por comité ya que no producirán cortes ni anomalías en el trabajo diario de los usuarios.

Los tickets se clasificarán en 6 grupos distintos, los cuales se aprecian en la siguiente tabla, teniendo cada uno un tiempo máximo para poder solucionarlos.

Tabla 3–2 Plan de soporte según prioridad del ticket creado.

Tipo	Definición	Solución (horas)	Objetivo (%)	Calendario
Incidencias Prioridad CRITICA	Pérdida de servicio global.	2	95	24x7
Incidencias Prioridad ALTA	Pérdida de servicio, CPD.	2	95	24x7
Incidencias Prioridad MEDIA	Degradación de servicio o pérdida de servicio con grupo de usuarios acotado.	4	95	8x5
Incidencias Prioridad BAJA	Resto de incidencias.	8	95	8x5
Peticiones Prioridad CRITICA	Peticiones de acciones que afectan a la seguridad o integridad de la red.	2	95	24x7
Peticiones Prioridad ALTA	Peticiones que afectan al servicio.	6	95	24x7
Peticiones Prioridad MEDIA	Peticiones de usuarios Alta / Baja, modificaciones de acceso de grupo o particulares.	12	95	8x5

3.6.2. Mantenimiento

Para evitar que los equipos se queden obsoletos, fuera de soporte o lo más importante, que pueda tener agujeros de seguridad, es imprescindible la actualización de la versión del firmware de estos.

Estas se realizarán siempre con una planificación previa, siempre teniendo en cuenta que no debe afectar al trabajo de los usuarios, por lo que se hará fuera de horario, aproximadamente cada 6 meses, siempre y cuando no haya sido detectada una vulnerabilidad muy crítica, que se actualizará el mismo día encontrado.

Si cualquier equipo se daña, tendrá que ser repuesto en el menor tiempo posible y por ello son imprescindibles guardar la configuración que tienen cada uno de ellos cada cierto tiempo.

En los switches y routers se realizarán de manera automática cada vez que se cambie la configuración de estos y se haga un “write”. Esto lo conseguimos con los siguientes comandos.

Código 3-14. Configuración para el almacenamiento de backups en un repositorio externo

```
archive
 path scp://sftp:IP_REPOSITORIO/HOSTNAME.cfg
 write-memory
 time-period 10080
```

4 CONCLUSIONES

"A veces, la persona a la que nadie imagina capaz de nada, es la que hace cosas que nadie imagina."

Alan Turing – "The Imitation Game"

4.1. Conclusiones

La finalidad de este proyecto era integrar por completo la planta del cliente en la Red Corporativa de manera que los usuarios que ya trabajaban pudiesen acceder directamente desde sus puestos, manteniendo los servicios previos a través de una interconexión realizada por medio de otro firewall no gestionado por el cliente.

Gracias a la metodología de ITIL, el orden de cada tarea estaba previamente estudiado y validado de manera que los trabajos se realizasen de manera óptima y no afectasen a los usuarios, realizando durante la jornada laboral apartados mecánicos y revisiones de las configuraciones de los equipos a desplegar, dejando los cambios que implicasen cortes para la tarde.

La estructura diseñada es fácilmente escalable, por lo que en un futuro, esta estaría preparada para poder asumir un mayor número de usuarios.

Una vez finalizado el proyecto, la mayoría de requisitos estipulados en el pliego se cumplieron por lo que se pudo considerar que el despliegue fue exitoso, ya que la red se dejó funcionando con los permisos estipulados según el perfil de cada usuario, los equipos sustituídos por los nuevos y actualizados y funcionando con un rendimiento máximo.

4.2. Líneas futuras

Uno de los púntos débiles del diseño realizado es la falta de redundancia en cuanto al cableado entre edificios. Como mejora, se recomendaría realizar una red donde los switches tuviesen enlaces redundados u otras conexiones entre dispositivos, de manera que si por cualquier motivo, algún enlace sufriese algún daño, los usuarios no sufriesen pérdidas.

Para plantas de esta envergadura y siendo el trabajo desarrollado imprescindible una buena conexión a Internet, sería importante incluir otro firewall, ya que este es la puerta de enlace para la mayoría de las comunicaciones realizadas, de manera que se configurasen en Alta disponibilidad en el modo activo-pasivo, dotando a la sede de una mayor estabilidad en cuanto a la conexión.

En cuanto a agilidad para despliegues o integraciones de otras sedes del cliente, sería bueno el afrontar el proyecto con una plantilla previamente diseñada, única para esta organización, de manera que los trabajos sean más fluidos y eliminando la posibilidad de que se repitan errores ya comentidos.

ANEXO A
PETICIÓN DEL CAMBIO

ID	DESCRIPCIÓN	
1	ID RFC	PCL19001
2	Fecha de la presentación de la solicitud	23-sep-2019
3	Propietario del cambio	NOMBRE DEL CLIENTE
4	Iniciador del cambio	NOMBRE DEL CLIENTE
5	Prioridad	Normal
6	Descripción del cambio que se solicita	
6.1	Descripción	Integración de la nueva planta en la arquitectura del Cliente
6.2	Caso de negocio	
6.2.1	Razón para implementación del cambio	Se desea que todas las plantas del cliente tengan una infraestructura centralizada y actualizada, por ello se integrará la planta en la red corporativa y se sustituirán equipos que están sin soporte por parte del fabricante, por unos que puedan proporcionar y mejorar la calidad de los servicios hasta ahora ofrecidos.
6.2.2	Costos	12.567,79 €
6.2.3	Consecuencias de no implementar el cambio	Tanto el firewall y router desplegados llegan al fin de vida de soporte por parte del fabricante, por lo que ante algún cambio o actualización para mejora de "bugs" identificados que se desease hacer no se podría. Los usuarios no tendrían un acceso normalizado a algunos servicios corporativos. Faltarían puestos de usuarios en los distintos edificios que faciliten el trabajo.
6.3	Áreas del negocio afectadas	IT, Producción
6.4	Impacto	Alto – Cortes intermitentes en todos los servicios
6.5	Servicios afectados	Wi-Fi, LAN, acceso a recursos corporativos y externos, impresión
7.	Riesgos durante la implementación del cambio	
7.1	Riesgos identificados	Fallo en las comunicaciones tanto a servicios internos como externos, además de la salida a Internet. Sin acceso a servicios de impresión.

7.2	Plan de contingencia	Si el resultado no fuese satisfactorio, se volvería a conectar el firewall Stonegate 315, el cual garantiza las comunicaciones necesarias hasta el día del despliegue y se añadirían las nuevas subredes que fuesen necesarias. Se volvería a conectar el router cisco antiguo, ofreciendo a los usuarios el acceso al resto de la red corporativa. No se propone un plan de contingencia para los nuevos switches a implantar, ya que no suponen un corte en la producción actual de la planta.
8.	Calendario sugerido para la implementación	
8.1	Duración estimada	5 días
8.2	Fecha inicio	14/10/2019 9:00
8.3	Fecha fin	18/10/2019 18:00
9	Estimación de recursos	
9.1	Equipo técnico	
9.1.1	Solicitante	NOMBRE DEL CLIENTE
9.1.2	Técnico asignado	Assumpta Cabral Otero
9.1.3	Jefe de Proyecto	NOMBRE JEFE PROYECTO (EMPRESA)
9.1.4	Validado por	NOMBRE PERSONA QUE VALIDA (CLIENTE)
9.1.5	Supervisado por	NOMBRE SUPERVISOR (EMPRESA)
9.2	Equipos utilizados	
	PA-800 Series Cisco C1111-8P Cisco WS-C2960X-24PS-L Cisco WS-C2960C-12PC-L Cisco AIR-AP1832I-E-K9	
10	Tareas que realizar	
10.1	Trabajos previos	

	Actualización del Switch Diseño de Arquitectura Física Diseño de Arquitectura Lógica Asignación de direccionamientos Arranque sin errores de los switches y comprobación del funcionamiento Arranque sin errores de los Puntos de Acceso Downgrade/Upgrade firmware Aps y registro en WLC (Wireless LAN Controler) Registro de Firewall en PaloAlto support Licenciamiento de PaloAlto Upgrade Paloalto Configuración PaloAlto Configuración router Configuración de puertos de acceso de switches y maquetado según plantilla del cliente
10.2	Implementación y pruebas
	Enrackado e instalación de equipamiento Etiquetado de interfaces y dispositivos Pruebas de conectividad router DMVPN Pruebas de conectividad de APs y servicio Wi-Fi Pruebas de conectividad de firewall Integración completa de Paloalto Despliegue de Switches Cambio de usuarios a nueva arquitectura Pruebas de conectividad de todos los servicios: • DNS • DHCP • Autenticación con el directorio activo • Acceso a servicios internos y externos • Servicios no corporativos • Impresión • Internet • Wi-Fi Atención de incidencias Integración de Paloalto en Panorama

ANEXO B
FICHAS TÉCNICAS

B.1. Palo Alto 820

PA-800 SERIES

Los firewalls de nueva generación PA-800 Series de Palo Alto Networks, que incluyen PA-820 y PA-850, se diseñaron para brindar una conectividad segura a las sucursales de organizaciones y a medianas empresas.

Funciones Clave de Seguridad y Conectividad

Clasifica todas las aplicaciones, en todos los puertos, en todo momento.

- Identifica la aplicación, independientemente del puerto, la encriptación SSL/SSH o las técnicas evasivas empleadas.
- Usa la aplicación, no el puerto, como base para todas sus decisiones de políticas de habilitación segura como permitir, denegar, programar, inspeccionar y aplicar control de tráfico.
- Categoriza aplicaciones no identificadas para el control de políticas, la investigación forense de amenazas o el desarrollo de tecnología App-ID™.

Ejecuta las políticas de seguridad para cualquier usuario, en cualquier ubicación.

- Implementa políticas coherentes para usuarios locales y remotos en las plataformas de Windows®, macOS®, Linux, Android®, o Apple iOS.
- Habilita la integración sin agentes con Microsoft Active Directory® y Terminal Services, LDAP, Novell eDirectory™ y Citrix.
- Integra fácilmente sus políticas de firewall en 802.1X inalámbrico, proxies, network access control (control de acceso a la red - NAC) y cualquier otra fuente de información sobre la identidad del usuario.

Evita amenazas conocidas y desconocidas.

- Bloquea una variedad de amenazas conocidas—que incluyen exploits, malware y spyware—en todos los puertos, independientemente de las tácticas comunes de evasión empleadas.
- Limita la transferencia no autorizada de archivos y datos confidenciales y habilita de forma segura la navegación por Internet no relacionada con el trabajo.
- Identifica malware desconocido, lo analiza en función de cientos de comportamientos malintencionados y luego crea y brinda protección automáticamente.

Habilita la funcionalidad de SD-WAN.

- Adopta SD-WAN con facilidad al habilitarlo en los firewalls existentes.
- Permite que implemente SD-WAN, integrado de manera segura con nuestra seguridad líder en el sector, sin peligro.
- Ofrece una experiencia excepcional para el usuario final al minimizar la latencia, la vibración y la pérdida de paquetes.

PA-800 Series

El elemento de control de la serie PA-800 Series es PAN-OS® que clasifica todo el tráfico de forma nativa, incluso de aplicaciones, amenazas y contenido y, luego, vincula ese tráfico al usuario, independientemente de la ubicación o el tipo de dispositivo. La aplicación, el contenido y el usuario, es decir, los elementos que hacen funcionar el negocio, sirven luego como base para sus políticas de seguridad, lo que genera una postura de seguridad mejorada y una reducción en el tiempo de respuesta ante incidentes.

Tabla 1: Rendimiento y Capacidades de PA-800 Series

	PA-850	PA-820
Rendimiento de firewall (HTTP/appmix)[1]	2/2 Gbps	1.7/1.6 Gbps
Rendimiento de Threat Prevention (HTTP/appmix)[2]	1/1 Gbps	780/800 Mbps
Rendimiento de IPSec VPN[3]	1.6 Gbps	1.2 Gbps
Nuevas sesiones por segundo[4]	13 000	8300
Sesiones máximas	192 000	128 000

1. El rendimiento de firewall se mide con App-ID y registro habilitado mediante el uso de transacciones HTTP/appmix de 64 KB.

2. El rendimiento de Threat Prevention se mide con App-ID, IPS, antivirus, antispyware, WildFire, bloqueo de archivos y registro habilitado mediante el uso de transacciones HTTP/appmix de 64 KB.

3. El rendimiento de Ipsec VPN se mide con transacciones HTTP de 64 KB y registro habilitado.

4. Las nuevas sesiones por segundo se miden con cancelación de aplicación mediante el uso de transacciones HTTP de un byte.

Los firewalls de nueva generación PA-800 Series son compatible con una amplia variedad de funciones de conexión de redes que le permiten integrar con más facilidad nuestras funciones de seguridad en las redes existentes.

Tabla 2: Funciones de Red de PA-800 Series
Modos de Interfaz
L2, L3, tap, virtual wire (modo transparente)
Enrutamiento
OSPFv2/v3 con reinicio cuidadoso, BGP con reinicio cuidadoso, RIP, enrutamiento estático
Policy-based forwarding (Reenvío basado en políticas - PBF)
Point-to-Point Protocol over Ethernet (Protocolo Punto a Punto sobre Ethernet - PPPoE)
Multidifusión: PIM-SM, PIM-SSM, IGMP v1, v2 y v3
SD-WAN
Medición de la calidad de la ruta (vibración, pérdida de paquetes, latencia)
Selección de ruta inicial (PBF)
Cambio dinámico de ruta
IPv6
L2, L3, tap, virtual wire (modo transparente)
Funciones: App-ID, User-ID, Content-ID, WildFire y Descifrado de SSL
SLAAC
IPsec VPN
Intercambio de claves: clave manual, IKEv1 e IKEv2 (clave precompartida, autenticación basada en certificados)
Encriptación: 3DES, AES (128-bit, 192-bit, 256-bit)
Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512
VLANs
Etiquetas 802.1Q VLAN por dispositivo/por interfaz: 4094/4094
Interfaces agregadas (802.3ad), LACP
Network address translation (traducción de dirección de red - NAT)
Modos NAT (IPv4): IP estática, IP dinámica, dynamic IP and port (IP y puerto dinámicos - DIPP) (traducción de direcciones de puertos)
NAT64, NPTv6
Funciones adicionales NAT: reserva de IP dinámica, dynamic IP and port (IP y puerto dinámicos - DIPP) con túnel y sobresuscripción
High Availability (Alta Disponibilidad - HA)
Modos: activo/activo, activo/pasivo
Detección de fallas: monitoreo de rutas, supervisión de interfaz

Tabla 3: Especificaciones del Hardware de PA-800 Series
I/O
PA-850: (4) 10/100/1000, (8) Gigabit SFP o PA-850: (4) 10/100/1000, (4) Gigabit SFP, (4) 10 Gigabit SFP+ PA-820: (4) 10/100/1000, (8) Gigabit SFP
Gestión I/O
(1) Puerto de gestión fuera de banda de 10/100/1000 (2) high availability (alta disponibilidad - HA) de 10/100/1000 (1) Puerto de la consola RJ-45 (1) Puerto USB (1) Puerto de consola Micro USB
Capacidad de Almacenamiento
SSD de 240 GB
Alimentación
PA-850: dos fuentes de alimentación de CA de 500 W; una es redundante. PA-820: Una fuente de alimentación fija de CA de 200 W
Consumo de Energía
Máximo: PA-850: 240 W, PA-820: 120 W
Promedio: PA-850: 64 W, PA-820: 41 W
BTU/h máximo
256
Voltaje de Entrada (Frecuencia de Entrada)
100–240 VAC (de 50 Hz a 60 Hz)
Consumo de Corriente Máximo
2.0 A @ 100 VAC, 1.0 A @ 240 VAC (PA-850)
1.0 A @ 100 VAC, 0.5 A @ 240 VAC (PA-820)
Corriente Máxima de Entrada
1.0 A @ 230 VAC, 1.84 A @ 120 VAC (PA-850)
0.4 A @ 230 VAC, 0.96 A @ 120 VAC (PA-820)
Montaje en Rack (Dimensiones)
PA-850: 1U, rack estándar de 19", 1.75" alto x 14.5" prof. x 17.125" ancho. PA-820: 1U, rack estándar de 19", 1.75" alto x 14" prof. x 17.125" ancho
Peso (Dispositivo Solo/Como Se Envía)
PA-850: 13.5 lb/21.5 lb PA-820: 11 lb/18 lb
Seguridad
cCSAus, CB
EMI
Clase FCC A, Clase CE A, Clase VCCI A
Certificaciones
Vea https://www.paloaltonetworks.com/company/certifications.html
Entorno
Temperatura Operativa: 32 °F a 104 °F, 0 °C a 40 °C Temperatura no operativa: -4 °F a 158 °F, -20 °C a 70 °C
Flujo de Aire
De adelante hacia atrás

Para conocer más sobre las funciones y capacidades asociadas de PA-800 Series, visite www.paloaltonetworks.com/products.

3000 Tannery Way
Santa Clara, CA 95054
Linea principal: +1-408-753-4000
Ventas: +1-866-320-4788
Soporte técnico: +1-866-898-9087
www.paloaltonetworks.com

B.2. Cisco C1111-8P

Cisco® 1000 Series Integrated Services Routers (ISRs) with Cisco IOS® XE Software combine Internet access, comprehensive security, and wireless services (LTE Advanced 3.0 wireless WAN and 802.11ac wireless LAN) in a single, high-performance device. The routers are easy to deploy and manage, with separate data and control plane capabilities.

The Cisco 1000 Series ISRs are well suited for deployment as Customer Premises Equipment (CPE) in enterprise branch offices, in service provider managed environments as well as smaller form factor and M2M use cases.

Note: Not all 1000 series SKU variants are available in every region with different technologies (check on CCW pricelist for your region).

Figure 1.
Cisco 1000 Product Family Series

Figure 2.
Cisco 1100-8P ISR with LTE advanced, back and front view

Figure 3.
Cisco 1120 and 1160 with LTE pluggable and 802.11ac Wi-Fi options

Primary features and benefits

Table 1. Business benefits

Business need	Features/description
Lightweight, compact size with low power consumption	• Can be deployed in many different environments where space, heat dissipation, and low power consumption are critical factors (including Cisco Pluggable smaller form factor technology).
High performance to run concurrent services	• High performance allows customers to take advantage of broadband network speeds while running secure, concurrent data, voice, video, and wireless services. C1160 models will have better overall performance.
High availability and business continuity	• Redundant WAN connections for failover protection and load balancing. • Dynamic failover protocols such as Virtual Router Redundancy Protocol (VRRP; RFC 2338), Hot Standby Router Protocol (HSRP), and Multigroup HSRP (MHSRP).
Consistent, high application performance levels	• The router can run multiple services simultaneously with minimal performance degradation.
Risk mitigation with multilevel security	• Network perimeter security with integrated application inspection firewall. • Data privacy through high-speed IP Security (IPsec) Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) encryption. • High-performance VPNs: DMVPN, FlexVPN, GETVPN. • Encrypted Traffic Analytics (ETA) to identify malware communications in encrypted traffic using passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility. • Cisco Umbrella™ is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. • Security hardware acceleration. • Trustworthy systems with Field-Programmable Gate Array (FPGA) and hardware anchor.
Unified control of wired and wireless networks from a common console for streamlined operations	• Simplifies and centralizes configuration and management of wireless and wireline devices. Supports WLAN services without requiring a wireless LAN controller. • Supports Mobility Express for WLAN-enabled routers.
Remote configuration and management to keep local IT staff lean	• Supports separate console and USB ports. Can be configured to work with optional USB token. • Supports TR-069.
Performance • Throughput • Service reliability	• ISR 1000 can provide encrypted traffic performance greater than 350 Mbps. • A distributed multicore architecture with the dedicated control plane and service plane. • Remote installation of application-aware services that run identically to their counterparts in dedicated appliances (Future roadmap).
Lower WAN expenditures	• Cisco Software-Defined WAN (SD-WAN) support for optimized WAN connection. • Smaller form factor and Cisco Pluggable technology provide additional protection investment and flexibility.
Pay as you grow: IPsec performance upgrade model	• Router IPsec capacity can be increased with a remote performance-on-demand license upgrade (no hardware upgrade) for exceptional savings and CapEx budget management.
IT consolidation, space savings, and improved Total Cost of Ownership (TCO)	• Single converged branch platform integrates routing, switching, security, and performance management capabilities.
Business continuity and increased resiliency	• The entire 1000 Series supports Power over Ethernet (PoE) and PoE+ power to endpoints (Not available on C1101 and C1109 smaller form factor series).

Table 2. Support for Software-Defined WAN on ISR 1000

Cisco SD-WAN offers an entirely new way to manage and operate your WAN infrastructure. Cisco SDWAN is a cloud delivered architecture that offers secure, flexible and rich services with the following key benefits:

B.3. Cisco WS-C2960X-24PS-L

Product Overview

Cisco® Catalyst® 2960-X and 2960-XR Series Switches are fixed-configuration, stackable Gigabit Ethernet switches that provide enterprise-class access for campus and branch applications (Figure 1). They operate on Cisco IOS® Software and support simple device management as well as network management. The Cisco Catalyst 2960-X and 2960-XR Series provide easy device onboarding, configuration, monitoring, and troubleshooting. These fully managed switches can provide advanced Layer 2 and Layer 3 features as well as optional Power over Ethernet Plus (PoE+) power. Designed for operational simplicity to lower total cost of ownership, they enable scalable, secure, and energy-efficient business operations with intelligent services. The switches deliver enhanced application visibility, network reliability, and network resiliency.

Figure 1.
Cisco Catalyst 2960-X Series Switches

Product Highlights

Cisco Catalyst 2960-X and 2960-XR Series Switches feature:

- 24 or 48 Gigabit Ethernet ports with line-rate forwarding performance
- 4 fixed 1 Gigabit Ethernet Small Form-Factor Pluggable (SFP) uplinks or 2 fixed 10 Gigabit Ethernet SFP+ uplinks
- PoE+ support with a power budget of up to 740W and Perpetual PoE
- Cisco IOS LAN Base[2] or LAN Lite[2] and Cisco IOS IP Lite[2]
- Device management with web UI, over-the-air access via Bluetooth, Command-Line Interface (CLI), Simple Network Management Protocol (SNMP), and RJ-45 or USB console access
- Network management with Cisco Prime®, Cisco Network Plug and Play, and Cisco DNA Center
- Stacking with FlexStack-Plus and FlexStack-Extended
- Layer 3 features with routed access (Open Shortest Path First [OSPF]), static routing, and Routing Information Protocol (RIP)
- Visibility with Domain Name System as an Authoritative Source (DNS-AS) and Full (Flexible) NetFlow
- Security with 802.1X, Serial Port Analyzer (SPAN) and Bridge Protocol Data Unit (BPDU) Guard
- Reliability with higher Mean Time Between Failures (MTBF) and Enhanced Limited Lifetime Warranty (E-LLW)
- Resiliency with optional dual field-replaceable power supplies[2]

Power Supply

An external redundant power supply option is supported on the Cisco Catalyst 2960-X Series Switches. These switches come with one fixed power supply and an option for an external redundant power supply (Cisco Redundant Power System [RPS] 2300).

Dual redundant power supplies are supported on the Cisco Catalyst 2960-XR Series Switches. These switches ship with one power supply by default. The second power supply can be purchased at the time of ordering the switch or as a spare. These power supplies have built-in fans to provide cooling (Figure 2).

Figure 2.
Cisco Catalyst 2960-XR Series power supply

Table 1 shows the different power supplies available in the 2960-XR Series switches and the available PoE power. Table 2 lists the PoE and PoE+ power capacity for the Cisco Catalyst 2960-X and 2960-XR Series. Table 3 gives the available PoE and switch power for the 2960-XR Series with different power supply combinations.

Table 1. Cisco Catalyst 2960-XR Series default power supply configurations

Product ID	Default power supply	Available PoE power
WS-C2960XR-24TS-I WS-C2960XR-48TS-I WS-C2960XR-24TD-I WS-C2960XR-48TD-I	PWR-C2-250WAC	–
WS-C2960XR-24PD-I WS-C2960XR-48LPD-I WS-C2960XR-24PS-I WS-C2960XR-48LPS-I	PWR-C2-640WAC	370W
WS-C2960XR-48FPD-I WS-C2960XR-48FPS-I	PWR-C2-1025WAC	740W

Table 2. Cisco Catalyst 2960-X and 2960-XR Series PoE and PoE+ power capacity

Model	Maximum number of PoE+ (IEEE 802.3at) ports*	Maximum number of PoE (IEEE 802.3af) ports*	Available PoE power (single PS source)
Cisco Catalyst 2960X-48FPD-L	24 ports up to 30W	48 ports up to 15.4W	740W
Cisco Catalyst 2960X-48LPD-L	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960X-24PD-L	12 ports up to 30W	24 ports up to 15.4W	370W

B.4. Cisco WS-C2960C-12PC-L

Data Sheet

Cisco Catalyst 2960-C and 3560-C Series Compact Switches

Cisco® Catalyst® compact switches (Figure 1) easily extend an intelligent, fully managed Cisco Catalyst wired switching infrastructure, including end-to-end IP and Borderless Network services, with a single Ethernet cable or fiber from the wiring closet. These attractive, small form-factor Gigabit and Fast Ethernet switches are ideal for connecting multiple devices on the retail sales floor and in classrooms, hotels, and factories and for extending wireless LAN networks: wherever space is at a premium and multiple cable runs could be challenging.

Cisco Catalyst 2960-C and 3560-C Series Compact Switches highlights:

- Extend a highly secure, intelligent, managed Cisco Catalyst infrastructure with a single Ethernet cable or fiber from the wiring closet
- Support for advanced security and services, including voice, video, and Cisco Borderless Network services, to remote endpoints
- Power over Ethernet (PoE) pass-through enables the compact switch to draw power from the wiring closet and pass it to end devices (selected models)
- Attractive, small form factor and fanless operation fit in confined spaces where multiple cable runs could be challenging
- Easy to deploy, manage and extend the network loop free
- Enhanced limited lifetime hardware warranty

Figure 1. Cisco Catalyst Compact Switches

Cisco Catalyst 2960-C Series Compact Switches Cisco Catalyst 3560-C Series Compact Switches

Switch Configurations

Table 1 compares switch models.

Table 1. Available Cisco Catalyst Compact Switch models

Model	Ethernet Ports	PoE Output Ports	Available PoE Power	Uplinks	MACsec
2960C-8TC-L	8 x 10/100 Fast Ethernet	N/A		2 x 1G copper or 2 x 1G SFP	N/A
2960C-8TC-S	8 x 10/100 Fast Ethernet	N/A		2 x 1G copper or 2 x 1G SFP	N/A
2960CPD-8TT-L	8 x 10/100 Fast Ethernet	N/A		2 x 1G (PoE+ input)	N/A
2960C-8PC-L	8 x 10/100 Fast Ethernet	8 PoE	124W	2 x 1G copper or 2 x 1G SFP	N/A
2960CPD-8PT-L	8 x 10/100 Fast Ethernet	8 PoE	Up to 30.8W[1]	2 x 1G (PoE+ input)	N/A
2960C-12PC-L	12 x 10/100 Fast Ethernet	12 PoE	124W	2 x 1G copper or 2 x 1G SFP	N/A
2960CG-8TC-L	8 x 10/100/1000 Gigabit Ethernet	N/A		2 x 1G copper or 2 x 1G SFP	N/A
3560C-8PC-S	8 x 10/100 Fast Ethernet	8 PoE+	124W	2 x 1G copper or 2 x 1G SFP	N/A
3560C-12PC-S	12 x 10/100 Fast Ethernet	12 PoE+	124W	2 x 1G copper or 2 x 1G SFP	N/A
3560CG-8TC-S	8 x 10/100/1000 Gigabit Ethernet	N/A		2 x 1G copper or 2 x 1G SFP	Yes
3560CG-8PC-S	8 x 10/100/1000 Gigabit Ethernet	8 PoE+	124W	2 x 1G copper or 2 x 1G SFP	Yes
3560CPD-8PT-S	8 x 10/100/1000 Gigabit Ethernet	8 PoE	Up to 23.8W[2]	2 x 1G (PoE+ input)	Yes

Cisco Catalyst 2960-C and 3560-C Series Software

Cisco Catalyst 2960-C Series compact switches ship with the LAN Base version of Cisco IOS® Software, as available on other Cisco Catalyst 2960 Series Switches. Similarly, Cisco Catalyst 3560-C compact switches ship with the IP Base version of Cisco IOS Software, as with other 3560 Series switches. Neither series of compact switches can be upgraded.

Cisco Catalyst 2960-C switches deliver advanced Layer 2 switching with intelligent Layer 2 through 4 services for the network edge, such as voice, video, and wireless LAN services. The IP Base feature set on Cisco Catalyst 3560-C switches adds baseline enterprise services, including support for routed access, Cisco TrustSec®, media access control security (MACsec), and other Cisco Borderless Network services.

The LAN Base feature set offers enhanced intelligent services that include comprehensive Layer 2 features. The IP Base feature set provides baseline enterprise services in addition to all LAN Base features. IP Base also includes the support for routed access, MACsec, and Open Shortest Path First (OSPF).

B.5. Cisco AIR-AP1832I-E-K9

AIR-AP1832I-E-K9 Datasheet

Get a Quote

Router-Switch.com
Leading Network Hardware Supplier

Overview

AIR-AP1832I-E-K9 is one of the Cisco Aironet 1830 Series Access Points. Cisco 1830 AP series is ideal for small and medium-sized networks. This series supports the latest Wi-Fi standard, the 802.11ac Wave 2 standard. The 1830 Series extends support to a new generation of Wi-Fi clients, such as smartphones, tablets, and high-performance laptops that have integrated 802.11ac Wave 1 or Wave 2 support. The model AIR-AP1832I-E-K9 provides E Regulatory Domain and internal antennas.

Quick Specs

Table 1 shows the quick specs of AIR-AP1832I-E-K9.

Part Number	AIR-AP1832I-E-K9
Description	802.11ac Wave 2 AP, 3x3:2, Internal Antenna, E Regulatory Domain
Features	- 3x3 MIMO with two spatial streams, single-user or multiuser MIMO - MRC - 802.11ac beamforming (transmit beamforming) - 20-, 40-, and 80-MHz channels - PHY data rates up to 867 Mbps (80 MHz in 5 GHz) - Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) - 802.11 DFS - CSD support
Regulatory Domain	E (E regulatory domain): - 2.412 to 2.472 GHz; 13 channels - 5.180 to 5.320 GHz; 8 channels - 500 to 5.700 GHz; 8 channels
Integrated antenna	- 2.4 GHz, gain 3 dBi, internal omni, horizontal beamwidth 360° - 5 GHz, gain 5 dBi, internal omni, horizontal beamwidth 360°
Interfaces	- 1 x 10/100/1000BASE-T autosensing (RJ-45), Power over Ethernet (PoE) - Management console port (RJ-45) - USB 2.0 (enabled via future software)
Dimensions (W x L x H)	8.3 x 8.3 x 2 in. (210.8 x 210.8 x 50.8 mm)
Weight	3.12 lb (1.41 kg)

Product Details

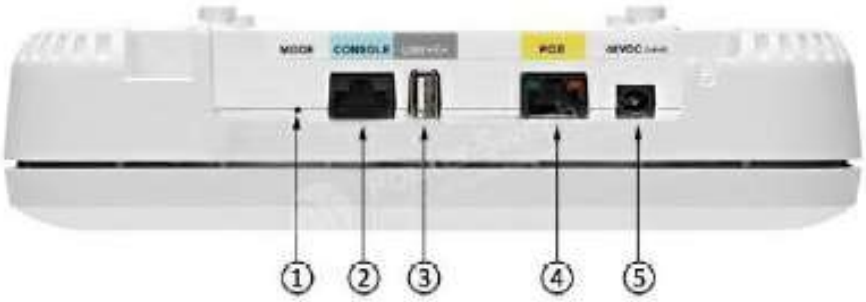
Figure 1 shows the AIR-AP1832I LED Indicator Position.

Note: (1) LED indicator position

Table 2 shows the AP LED indicators' descriptions.

Message Type	LED State	Message Meaning
Association status	Chirping Green	Normal operating condition, but no wireless client associated
	Green	Normal operating condition, at least one wireless client association
Boot loader status	Green	Executing boot loader
Boot loader error	Red	Boot loader signing verification failure
Access point regulatory domain priming status	Blinking Amber	AP priming to a new regulatory domain by Neighbor Discovery Protocol (NDP), in progress
	Cycling Red, Green and off	AP waiting to be primed
	Chirping Red	AP primed to a wrong regulatory domain
Operating status	Blinking amber	Software upgrade in progress
	Cycling through green, red, and amber	Discovery/join process in progress
	Rapidly cycling through red, green, amber, and off.	Access point location command invoked from controller web interface.
Access point operating system errors	Cycling through red, green, amber, and off	General warning; insufficient inline power

Figure 2 shows AIR-AP1832I Ports and Connections.



Note:

(1)	Mode button	(4)	PoE-In port (Ethernet Uplink port)
(2)	RJ-45 console port	(5)	48 V DC input power port
(3)	USB 2.0 port		

Compare to Similar Items

Table 3 shows the comparison between two AP.

Part Number	AIR-AP1832I-E-K9	AIR-AP1832I-E-K9C
Description	802.11ac Wave 2 AP, 3x3:2	802.11ac Wave 2 AP, 3x3:2 ★ Model number ending in C is, by default, factory-shipped with a Cisco Mobility Express software image.

B.6. Cisco GLC-SX-MMD

Cost-effective Small Form-factor Pluggable (SFP) transceivers for Gigabit Ethernet applications

Product overview

The industry-standard Cisco® Small Form-Factor Pluggable (SFP) Gigabit Interface Converter (Figure 1) links your switches and routers to the network. The hot-swappable input/output device plugs into a Gigabit Ethernet port or slot. Optical and copper models can be used on a wide variety of Cisco products and intermixed in combinations of 1000BASE-T, 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-EX, 1000BASE-ZX, or 1000BASE-BX10-D/U on a port-by-port basis.

Figure 1.
Cisco Optical Gigabit Ethernet SFP

Figure 2.
Cisco 1000BASE-T Copper SFP

Figure 3.
Cisco 2-Channel 1000BASE-BX Optical SFP

Features and benefits

- Hot swappable to maximize uptime and simplify serviceability
- Flexibility of media and interface choice on a port-by-port basis, so you can "pay as you populate"
- Robust design for enhanced reliability
- Supports Digital Optical Monitoring (DOM) capability

1000BASE-T SFP for copper networks

The 1000BASE-T SFP operates on standard Category 5 unshielded twisted-pair copper cabling of link lengths up to 100 m (328 ft). Cisco 1000BASE-T SFP modules support 10/100/1000 auto negotiation and Auto MDI/MDIX.

1000BASE-SX SFP for multimode fiber only

The 1000BASE-SX SFP, compatible with the IEEE 802.3z 1000BASE-SX standard, operates on legacy 50 µm multimode fiber links up to 550 m and on 62.5 µm Fiber Distributed Data Interface (FDDI)-grade multimode fibers up to 220 m. It can support up to 1km over laser-optimized 50 µm multimode fiber cable.

1000BASE-LX/LH SFP for both multimode and single-mode fibers

The 1000BASE-LX/LH SFP, compatible with the IEEE 802.3z 1000BASE-LX standard, operates on standard single-mode fiber-optic link spans of up to 10 km and up to 550 m on any multimode fibers. When used over legacy multimode fiber type, the transmitter should be coupled through a mode conditioning patch cable. For details on this implementation, refer to http://www.cisco.com/en/US/prod/collateral/modules/ps5455/product_bulletin_c25-530836.html.

1000BASE-EX SFP for long-reach single-mode fibers

The 1000BASE-EX SFP operates on standard single-mode fiber-optic link spans of up to 40 km in length. A 5-dB inline optical attenuator should be inserted between the fiber-optic cable and the receiving port on the SFP at each end of the link for back-to-back connectivity.

1000BASE-ZX SFP for long-reach single-mode fibers

The 1000BASE-ZX SFP operates on standard single-mode fiber-optic link spans of up to approximately 70 km in length. The SFP provides an optical link budget of 21 dB, but the precise link span length depends on multiple factors such as fiber quality, number of splices, and connectors.

When shorter distances of Single-Mode Fiber (SMF) are used, it might be necessary to insert an inline optical attenuator in the link to avoid overloading the receiver. A 10-dB inline optical attenuator should be inserted between the fiber-optic cable plant and the receiving port on the SFP at each end of the link whenever the fiber-optic cable span loss is less than 8 dB.

1000BASE-BX10-D and 1000BASE-BX10-U SFP for single-fiber bidirectional applications

The 1000BASE-BX-D and 1000BASE-BX-U SFPs, compatible with the IEEE 802.3ah 1000BASE-BX10-D and 1000BASE-BX10-U standards, operate on a single strand of standard SMF.

A 1000BASE-BX10-D device is always connected to a 1000BASE-BX10-U device with a single strand of standard SMF with an operating transmission range up to 10 km. The communication over a single strand of fiber is achieved by separating the transmission wavelength of the two devices as depicted in Figure 2: 1000BASE-BX10-D transmits a 1490-nm channel and receives a 1310-nm signal, whereas 1000BASE-BX10-U transmits at a 1310-nm wavelength and receives a 1490-nm signal. As shown, the presence of a Wavelength-Division Multiplexing (WDM) splitter integrated into the SFP to split the 1310-nm and 1490-nm light paths.

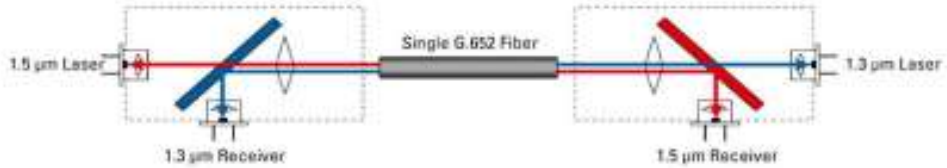


Figure 4.
Bidirectional transmission of a single strand of SMF

ANEXO C
DISTRIBUCIÓN DE PUERTOS

C.1. Switch 1

IP Address	10.90.48.4			
Model	WS-C2960X-24PS-L			
	Port Type	Port	VLAN	Descripción
	GigabitEthernet	Gi1/0/1	150,300,310,315	AP
	GigabitEthernet	Gi1/0/2	T	ROUTER INTERNET
	GigabitEthernet	Gi1/0/3	T	ROUTER DMVPN
	GigabitEthernet	Gi1/0/4	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi1/0/5	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi1/0/6	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi1/0/7	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi1/0/8	T	FW SECUNDARIO
	GigabitEthernet	Gi1/0/9	110	SERVIDOR
	GigabitEthernet	Gi1/0/10	110	SERVIDOR
	GigabitEthernet	Gi1/0/11	110	SERVIDOR
	GigabitEthernet	Gi1/0/12	150,300,310,315	AP
	GigabitEthernet	Gi1/0/13	220	IMPRESORA
	GigabitEthernet	Gi1/0/14	220	IMPRESORA
	GigabitEthernet	Gi1/0/15	210	PUERTO USUARIO
	GigabitEthernet	Gi1/0/16	210	PUERTO USUARIO
	GigabitEthernet	Gi1/0/17	210	PUERTO USUARIO
	GigabitEthernet	Gi1/0/18	210	PUERTO USUARIO
	GigabitEthernet	Gi1/0/19	210	PUERTO USUARIO
	GigabitEthernet	Gi1/0/20	210	PUERTO USUARIO
	GigabitEthernet	Gi1/0/21	210	PUERTO USUARIO
	GigabitEthernet	Gi1/0/22	210	PUERTO USUARIO
	GigabitEthernet	Gi1/0/23	210	PUERTO USUARIO
	GigabitEthernet	Gi1/0/24	210	PUERTO USUARIO
	GigabitEthernet	Gi1/0/25	T	SWITCH
	GigabitEthernet	Gi1/0/26	T	SWITCH
	GigabitEthernet	Gi1/0/27	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi1/0/28	D	PUERTO DESHABILITADO

Figura C-1. Distribución de puertos en el switch 1, stack principal.

IP Address	10.90.48.4			
Model	WS-C2960X-24PS-L			
	Port Type	Port	VLAN	Descripción
	GigabitEthernet	Gi2/0/1	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi2/0/2	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi2/0/3	T	ROUTER DMVPN
	GigabitEthernet	Gi2/0/4		PALO ALTO
	GigabitEthernet	Gi2/0/5		PALO ALTO
	GigabitEthernet	Gi2/0/6		PALO ALTO
	GigabitEthernet	Gi2/0/7		PALO ALTO
	GigabitEthernet	Gi2/0/8	170	FW SECUNDARIO
	GigabitEthernet	Gi2/0/9	110	SERVIDOR
	GigabitEthernet	Gi2/0/10	110	SERVIDOR
	GigabitEthernet	Gi2/0/11	110	SERVIDOR
	GigabitEthernet	Gi2/0/12	150,300,310,315	AP
	GigabitEthernet	Gi2/0/13	220	IMPRESORA
	GigabitEthernet	Gi2/0/14	210	PUERTO USUARIO
	GigabitEthernet	Gi2/0/15	210	PUERTO USUARIO
	GigabitEthernet	Gi2/0/16	210	PUERTO USUARIO
	GigabitEthernet	Gi2/0/17	210	PUERTO USUARIO
	GigabitEthernet	Gi2/0/18	210	PUERTO USUARIO
	GigabitEthernet	Gi2/0/19	100	SONDA
	GigabitEthernet	Gi2/0/20	MIRROR	SONDA
	GigabitEthernet	Gi2/0/21	210	PUERTO USUARIO
	GigabitEthernet	Gi2/0/22	210	PUERTO USUARIO
	GigabitEthernet	Gi2/0/23	210	PUERTO USUARIO
	GigabitEthernet	Gi2/0/24	210	PUERTO USUARIO
	GigabitEthernet	Gi2/0/25	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi2/0/26	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi2/0/27	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi2/0/28	D	PUERTO DESHABILITADO

Figura C-2. Distribución de puertos en el switch 1, stack secundario.

C.2. Switch 2

IP Address	10.90.48.5			
Model	WS-C2960C-12PC-L			
	Port Type	Port	VLAN	MAC
	FastEthernet	Fa0/1	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/2	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/3	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/4	210	PUERTO USUARIO
	FastEthernet	Fa0/5	210	PUERTO USUARIO
	FastEthernet	Fa0/6	210	PUERTO USUARIO
	FastEthernet	Fa0/7	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/8	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/9	220	IMPRESORA
	FastEthernet	Fa0/10	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/11	150,300,310,315	AP
	FastEthernet	Fa0/12	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi0/1	T	SWITCH
	GigabitEthernet	Gi0/2	D	PUERTO DESHABILITADO

Figura C-3. Distribución de puertos en el switch 2.

C.3. Switch 3

IP Address	10.90.48.3			
Model	WS-C2960C-12PC-L			
	Port Type	Port	VLAN	MAC
	FastEthernet	Fa0/1	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/2	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/3	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/4	210	PUERTO USUARIO
	FastEthernet	Fa0/5	210	PUERTO USUARIO
	FastEthernet	Fa0/6	210	PUERTO USUARIO
	FastEthernet	Fa0/7	210	PUERTO USUARIO
	FastEthernet	Fa0/8	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/9	220	IMPRESORA
	FastEthernet	Fa0/10	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/11	150,300,310,315	AP
	FastEthernet	Fa0/12	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi0/1	T	SWITCH
	GigabitEthernet	Gi0/2	T	SWITCH

Figura C-4. Distribución de puertos en el switch 3.

C.4. Switch 4

IP Address	10.90.48.7			
Model	WS-C2960C-12PC-L			
	Port Type	Port	VLAN	MAC
	FastEthernet	Fa0/1	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/2	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/3	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/4	210	PUERTO USUARIO
	FastEthernet	Fa0/5	210	PUERTO USUARIO
	FastEthernet	Fa0/6	210	PUERTO USUARIO
	FastEthernet	Fa0/7	210	PUERTO USUARIO
	FastEthernet	Fa0/8	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/9	220	IMPRESORA
	FastEthernet	Fa0/10	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/11	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/12	T	SWITCH
	GigabitEthernet	Gi0/1	T	SWITCH
	GigabitEthernet	Gi0/2	T	SWITCH

Figura C-5. Distribución de puertos en el switch 4.

C.5. Switch 5

IP Address	10.90.48.8			
Model	WS-C2960C-12PC-L			
	Port Type	Port	VLAN	MAC
	FastEthernet	Fa0/1	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/2	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/3	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/4	210	PUERTO USUARIO
	FastEthernet	Fa0/5	210	PUERTO USUARIO
	FastEthernet	Fa0/6	210	PUERTO USUARIO
	FastEthernet	Fa0/7	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/8	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/9	220	IMPRESORA
	FastEthernet	Fa0/10	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/11	150,300,310,315	AP
	FastEthernet	Fa0/12	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi0/1	T	SWITCH
	GigabitEthernet	Gi0/2	D	PUERTO DESHABILITADO

Figura C-6. Distribución de puertos en el switch 5.

C.6. Switch 6

IP Address	10.90.48.9			
Model	WS-C2960C-12PC-L			
	Port Type	Port	VLAN	MAC
	FastEthernet	Fa0/1	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/2	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/3	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/4	210	PUERTO USUARIO
	FastEthernet	Fa0/5	210	PUERTO USUARIO
	FastEthernet	Fa0/6	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/7	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/8	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/9	220	IMPRESORA
	FastEthernet	Fa0/10	D	PUERTO DESHABILITADO
	FastEthernet	Fa0/11	150,300,310,315	AP
	FastEthernet	Fa0/12	D	PUERTO DESHABILITADO
	GigabitEthernet	Gi0/1	T	SWITCH
	GigabitEthernet	Gi0/2	D	PUERTO DESHABILITADO

Figura C-7. Distribución de puertos en el switch 6.

REFERENCIAS

[1] *MDAP. 2020. Gestión De Servicios ITIL.* https://uv-mdap.com/programa-desarrollado/bloque-vi-itil-v3/gestion-de-servicios-itil

[2] *Informática para tu negocio. 2020. Aprendiendo Acerca De La Gestión Del Cambio ITIL.* https://www.informaticaparatunegocio.com/blog/aprendiendo-acerca-la-gestion-del-cambio-itil

[3] *Blog.hixsa.com. 2020. ITIL Change Management Process, Paso A Paso (Segunda Parte).* https://blog.hixsa.com/posts/itil-change-management-process-paso-a-paso-parte2

[4] *HEFLO ES. 2020. Gestión De Cambios ITIL: Utilice Las Mejores Prácticas.* https://www.heflo.com/es/blog/itil/gestion-cambios-itil

[5] *prezi.com. 2020. ITIL - Gestion De Cambios Paso A Paso.* https://prezi.com/ig1yhistqwan/itil-gestion-de-cambios-paso-a-paso

[6] *Pérez, E., 2020. Por Qué Existen Los Distintos Canales Wifi Y Cómo Podemos Configurarlos Para Evitar Interferencias. Xataka.com.* https://www.xataka.com/servicios/que-existen-distintos-canales-wifi-como-podemos-configurarlos-para-evitar-interferencias

[7] *FM, Y., 2020. Wifi 2.4Ghz Y 5Ghz: Cuáles Son Las Diferencias Y Cuál Elegir. Xataka.com.* https://www.xataka.com/basics/wifi-2-4g-y-5g-cuales-son-las-diferencias-y-cual-elegir

[8] *González, M., 2020. Qué Son Los Canales Wi-Fi Y Cómo Escoger El Mejor Para Nuestra Red. Xatakamovil.com* https://www.xatakamovil.com/conectividad/que-son-los-canales-wi-fi-y-como-escoger-el-mejor-para-nuestra-red

[9] *Raya, A., 2020. Cómo Configurar La Red Wifi 5G Para Sacarle Todo El Partido A Tu Conexión. Blog de Lenovo.* https://www.bloglenovo.es/configurar-red-wifi-5g

[10] *Maneldeantonio.com. 2020. Wi-Fi: Entendiendo Los Db, Dbm Y RSSI – Maneldeantonio.Com.* http://maneldeantonio.com/dbs-dbm-rssi

[11] *NetSpot. 2020. ¿Qué Es La Relación Señal/Ruido Y Por Qué Es Necesario Medirla* https://www.netspotapp.com/es/signal-to-noise-ratio.html

[12] *Knowledgebase.paloaltonetworks.com. 2020. How To Add A Locally Managed Firewall To Panorama Management.* https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CloRCAS

[13] *Knowledgebase.paloaltonetworks.com. 2020. How To Configure Snmpv2 On The Palo Alto Networks Firewall.* https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClHaCAK

[14] *Community.cisco.com. 2020. Conociendo Dynamic Multipoint VPN (DMVPN).* https://community.cisco.com/t5/blogs-routing-y-switching/conociendo-dynamic-multipoint-vpn-dmvpn/ba-p/3101118

[15] *Community.cisco.com. 2020. Introducción A DMVPN - Dynamic Multipoint VPN Fase 1 Y Fase 2.* https://community.cisco.com/t5/blogs-routing-y-switching/introducci%C3%B3n-a-dmvpn-dynamic-multipoint-vpn-fase-1-y-fase-2/ba-p/3103707

[16] *Support.huawei.com. 2020. Understanding DSVPN - ME60 V800R011C00 Feature Description - VPN 01 - Huawei.* https://support.huawei.com/enterprise/en/doc/EDOC1100092814/cd9b2a05/understanding-dsvpn

[17] *Tools.ietf.org. 2020. RFC 2333 - NHRP Protocol Applicability Statement.* https://tools.ietf.org/html/rfc2333

[18] *CISCO, D., 2020. DMVPN (Dynamic Multipoint VPN) - CISCO. Ccnp-jncis-en-espanol.blogspot.com.* http://ccnp-jncis-en-espanol.blogspot.com/2015/12/dmvpn-dynamic-multipoint-vpn.html

[19] *Support, P., Firewalls, C. and Guides, C., 2020. Cisco Security Appliance Command Line Configuration Guide, Version 7.2 - Configuring Ipsec And ISAKMP [Cisco ASA 5500-X Series Firewalls] - Cisco.* https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/ike.html

[20] *Support, P., Switches, C. and Guides, C., 2020. Catalyst 2960-X Switch Stack Manager Configuration Guide, Cisco IOS Release 15.0(2)EX - Managing Switch Stacks [Cisco Catalyst 2960-X Series Switches] - Cisco.* https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/stack_manager/configuration_guide/b_stck_152ex_2960-x_cg/b_stck_152ex_2960-x_cg_chapter_010.html

[21] *Promax.es. 2020. Tipos De Conectores De Fibra Óptica: Guía Sencilla.* https://www.promax.es/esp/noticias/578/tipos-de-conectores-de-fibra-optica-guia-sencilla

[22] *Virtualremote.net. 2020. SSH Config And Crypto Key Generate RSA Command – Virtual Remote Networking.* http://virtualremote.net/networking-solutions/ssh-config-and-crypto-key-generate-rsa-command

[23] *Zabbix.com. 2020. 1 Supported Trigger Functions [Zabbix Documentation 3.4].* https://www.zabbix.com/documentation/3.4/manual/appendix/triggers/functions

[24] *Comunidad Huawei Enterprise. 2020. Proceso De Establecimiento De Un Túnel CAPWAP - Comunidad Huawei Enterprise.* https://forum.huawei.com/enterprise/es/proceso-de-establecimiento-de-un-t%C3%BAnel-capwap/thread/562121-100239

[25] *Cisco.com. 2020.* https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/trabajo_sin_fronteras/pdfs/cisco_unified_access_technology_overview_wp.pdf

[26] *Support, P., inalámbrica, R., Controllers, C. and Configuración, N., 2020. Entienda Flexconnect En El Regulador De La Tecnología Inalámbrica Del Catalizador 9800* https://www.cisco.com/c/es_mx/support/docs/wireless/catalyst-9800-series-wireless-controllers/213945-understand-flexconnect-on-9800-wireless.html

[27] *Bizagi.com. 2020.* http://www.bizagi.com/processcentral/Documents/42ab0200-0df5-4cae-8954-dd0d40a6cc0d/docs/Gesti%C3%B3n%20de%20Cambios.pdf

GLOSARIO

AP: Access Point (Punto de Acceso)

CAPWAP: Control and Provisioning for Wireless Access Point (Control y Aprovisionamiento de punto de acceso inalámbrico)

CLI: Command-line (Interfaz de Línea de Comandos)

CPD: Data Center (Centro de Procesamiento de Datos)

DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Equipos)

DMVPN: Dynamic Multipoint Virtual Private Network (Red Privada Virtual Multipunto Dinámica)

DNS: Domain Name System (Sistema de Nombres de Dominio)

DTLS: Datagram Transport Layer Security

EIGRP: Enhanced Interior Gateway Routing Protocol (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado)

GUI: Graphical User Interface (Interfaz Gráfica de Usuario)

HTTP: Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto)

HTTPS: Hypertext Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)

IETF: Internet Engineering Task Force

IP: Internet Protocol (Protocolo de Internet)

IPSec: Internet Protocol security

ISAKMP: Internet Security Association and Key Management Protocol

IT: Information Technology (Tecnología de Información)

ITIL: Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnologías de Información)

LAN: Local Area Network (Red de Área Local)

mGRE: Multipoint Generic Routing Encapsulation

MIB: Management Information Base (Bases de información de gestión)

NAT: Network Address Translation (Traducción de Direcciones de Red)

NGFW: Next Generation Firewalls (Cortafuegos de Última Generación)

NHC: Next Hop Client

NHRP: Next Hop Resolution Protocol (Potocolo de Resolución del Siguiente Salto)

NHS: Next Hop Server

NVRAM: Non-Volatile Random Access Memory (Memoria de Acceso Aleatorio No Volátil)

OID: Object Identifier (Identificador de Objeto)

RFC: Request For Change (Solicitud de Cambio)

RMA: Return Merchandise Authorization (Autorización de Retorno de Mercancía)

RSA: Rivest-Shamir-Adleman

RSSI: Received Signal Strength Indicator (Indicador de Fuerza de la Señal Recibida)

SFP: Small Form-Factor Pluggable Transceiver

SNMP: Simple Network Management Protocol (Protocolo Simple de Administración de Red)

SNR: Signal to noise (Relación señal/ruido)

SPAN: Switched Port Analyzer (Analizador de Puertos del Switch)

SSH: Secure SHell

SSID: Service Set Identifier

STP: Spanning Tree Protocol

TCP: Transmission Control Protocol (Protocolo de Control de Transmisión)

TFTP: Trivial File Transfer Protocol (Protocolo de Transferencia de Archivos Trivial)

UDP: User Datagram Protocol (Protocolo de Datagramas de Usuario)

VLAN: Virtual Local Area Network (Red de Área Local Virtual)

VPN: Virtual Private Network (Red Privada Virtual)

WLAN: Wireless LAN (Red de Área Local Inalámbrica)

WLC: Wireless LAN Controler