

UNIVERSIDAD TECNOLÓGICA NACIONAL

CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

MATERIA: PROYECTO FINAL

TÍTULO DEL PROYECTO

REESTRUCTURACIÓN DE RED DE DATOS DE UNA REPARTICIÓN PÚBLICA

ALUMNO: JOSE FEDERICO VISSANI

Indice

Proyecto de instalación de red y sus servicios.....	3
1 Introducción.....	3
2 Objetivo.....	6
3 Metodología.....	8
1. Planificación.....	8
I. Segmentar la red y redefinir todas las direcciones IP, tanto de las PC como de los servidores.....	11
II. Implementar inmediatamente un servidor de archivos (NAS) para uso de las direcciones.....	12
III. Reinstalar todos los equipos PC con software libre y restricciones a los usuarios.....	13
IV. Cambiar el servicio de internet existente por uno corporativo.....	13
V. Disponer de un lugar físico para montar un datacenter.....	14
VI. Crear una sala de capacitación.....	14
2. Tendido alámbrico.....	15
3. Tendido de fibra óptica.....	19
4. Datacenter.....	22
5. Migración.....	26
6. Diseño de VLAN.....	33
7. Implementación.....	37
Conclusión.....	41
Apéndice I – Fichas Técnicas.....	43
Ficha Técnica: Caja de empalme e interconexión Ref: FTCAEMP.....	43
Ficha Técnica: Gabinete de Distribución Ref: FTGAB12U.....	44
Ficha Técnica: Switch GigaEthernet Administrable. REF: SWETH24.....	45
Ficha Técnica: Cable Óptico de 12 fibras Monomodo - Aerea Ref: FTFO12MM.....	46
Ficha Técnica: Switch GigaEthernet Administrable. REF: SWETH24.....	47
Ficha Técnica: Servidor para Virtualización Ref: FT-SRV-V.....	48
Ficha Técnica: Gabinete Rack de 40U Ref: FTRACK40U.....	50
Ficha Técnica: UPS 2KVA Ref: FTUPS2KVA.....	51
Apéndice II – Configuración de VLAN en un switch HP 1920.....	52
Bibliografía.....	56

Proyecto de instalación de red y sus servicios

1 Introducción

El avance de la tecnología basada en las redes de datos hace que surjan nuevas expectativas para el futuro próximo en el desarrollo de las comunicaciones, siendo la imaginación el único límite. La facilidad, flexibilidad y movilidad que nos brinda, han hecho que sea la mejor forma de comunicación, conectividad y transferencia de datos entre diferentes lugares.

Estas redes de datos son una herramienta fundamental en las empresas e instituciones siendo un verdadero factor de competitividad y hasta de podría decir de subsistencia, debido a que el manejo y procesamiento de la información se ha convertido en un factor esencial y muy importante en el crecimiento de estas. Los ámbitos de aplicación van desde la interconexión de los diferentes lugares (Fábricas, Almacenes, Direcciones, Delegaciones, dependencias, etc.) hasta posibilitar aplicaciones de comunicación y control interactivo con proveedores, vendedores, directores, jefes, etc.

Me recibí de Analista Universitario de Sistemas en el año 1998 y comencé a realizar la actividad profesional en el campo de las redes y servidores en pequeñas y medianas empresas en forma independiente, implementando redes para solucionar problemas de conectividad, y con ello la forma de trabajar, en ámbitos muy diferentes como industria metal-mecánica, supermercados, empresas constructoras, etc. Esta diversidad de ambientes hace que se generen necesidades y urgencias muy distintas, lo que me llevó a adquirir conocimientos y experiencias para dar solución a las problemáticas de los distintos ambientes de trabajo. Entre toda esa diversidad de ambientes que se me presentaron fue uno en particular el más extenso y el que necesitaba urgentemente una total reestructuración. Se trataba de una Repartición Pública de la Provincia de Santa Fe, con una infinidad de problemas y necesidades no cubiertas. Citar que no mencionaré el nombre de la repartición por motivos de confidencialidad, puesto que los trabajos prácticos de proyecto final son propiedad de la Universidad. Al evaluar y reconocer la envergadura de los cambios y reestructuración que se debían realizar, consideré que era muy adecuado para presentar el Proyecto Final de la Carrera de Ingeniería en Sistema de Información.

Comencé este proyecto en el año 2017 primero como pasante de la Facultad y luego como personal contratado en la Repartición Pública de referencia, donde se planteó la necesidad de un mejor funcionamiento, en realidad se me consultó si era posible que funcione la red de datos. Al relevar el estado y la forma en que estaba instalado todo, les comuniqué que la única alternativa de solución a las graves fallas de todo tipo que presentaba la misma era una total reestructuración. Esta reestructuración fue profunda y radical, modificando positivamente la forma de trabajar y de afrontar las situaciones laborales diarias, con otra dinámica y entusiasmo de parte de los empleados que hacen uso de la red. Este proyecto hizo posible mejorar los servicios brindados a la comunidad, y además incorporar nuevos servicios digitalizados, haciendo de esta forma mucho más dinámicos muchos trámites tanto internos como externos (brindados a la comunidad) de la repartición.

Esta repartición está compuesta por 10 oficinas repartidas en toda la Provincia de Santa Fe, más la administración central la cual se encuentra en Santa Fe Capital. El promedio de usuarios de cada oficina de las que están repartidas en la Provincia es de 15 usuarios, mientras que en la administración central este número asciende a 340 usuarios, repartidos en 17 direcciones, lo que da un total de unos 490 usuarios aproximadamente.

Para comenzar con la descripción de la situación en la que se encontraba la Red de Datos haré referencia al predio del edificio de la Administración Central en Santa Fe Capital debido a que es el que posee mayor cantidad de usuarios, siendo la situación similar en las distintas oficinas repartidas en la Provincia pero en menor escala. Como primera reseña de la situación hay que destacar la cantidad de fallas de conectividad que se producían en el predio, dejando a los usuarios sin servicio de red muy seguido, además con una respuesta tardía de la solución, ya que encontrar las fallas era una labor muy tediosa y complicada, debido a la falta de información sobre el tendido del cableado y a los problemas que se generaban en los dispositivos de red. Se había llegado a esta situación porque no existía control ni mantenimiento alguno sobre las instalaciones, con lo cual, los usuarios tenían la libertad de configurar los equipos, instalar cualquier cosa, navegar por internet sin ninguna restricción, etc, lo que ocasionaba la saturación de la Red de Datos; sumado a no tener ningún diagrama de cableado ni plan de mantenimiento, el servicio era muy pobre.

En relación a como estaba la parte física de la instalación, se destacaba el mal estado del cableado. Realmente llamaban la atención la falta de criterio con la que se habían realizado muchas partes de la instalación, por ejemplo había partes cableadas al exterior realizadas con cable de interior, lo que hizo que el deterioro del cableado en los sectores realizados de esta manera fuera muy acelerado, por lo que en algunos sectores era pésimo su estado. Con respecto a la parte activa de la instalación física, los dispositivos de red, el mayor problema de ellos no era el estado, sino su emplazamiento y su conexionado. Estaban ubicados en cualquier lugar, poniendo en riesgo su integridad en algunos casos, debido a humedad y exposición a condiciones inapropiadas (agua, manipulación, roedores, etc) y la interconexión entre ellos era totalmente desorganizada y caótica. Para aclarar lo mencionado anteriormente, cuando menciono “la manipulación” de los dispositivos, me refiero al hecho de que estaban al alcance de cualquier usuario, por lo que muchas veces, con o sin intención, se realizaban desconexiones, cambios de puertos, reemplazo del equipo, lo que provocaba muchísimos problemas de funcionamiento de la red. Este tipo de prácticas hizo que se perdieran los registros de los puertos de conexión de los switches, nunca se informaba ni se tenía en cuenta a switchwes con puertos que no funcionaban o estaban fuera de servicio (quemados). Había también dispositivos muy antiguos con la velocidad de trabajo muy baja para los estándares de hoy.

Algunos de los switches estaban instalados en gabinetes, pero la ubicación era inadecuada, ya que estaban expuestos a las malas condiciones mencionadas anteriormente y además estaban abiertos (sin llavar), por lo que estaban expuestos al problema de manipulación mencionado anteriormente, cualquier persona conectaba y desconectaba lo que le parecía cuando tenía problemas. La mayoría de los gabinetes montados en el predio no respetaban las normas del cableado estructurado, y en los pocos gabinetes que cumplían con algunos puntos de las normas, los paneles o patcheras estaban mal etiquetados o sin etiquetar; por motivos desconocidos se fueron reconectando los cables sin respetar la señalización y muchas de las etiquetas de las bocas de pared no estaban o eran incorrectas, por lo que resultaba muy difícil detectar la falla cuando una PC perdía conectividad. Otra situación que provocaba confusión era la de equipos de una misma oficina conectados a switches ubicados en otras oficinas, si sumamos a esta situación que el cableado de interconexión de los switches entre si era en forma de cascada, con todos los problemas que eso conlleva, los tiempos de respuesta a los problemas se multiplicaban.

Con el tiempo el parque informático fue creciendo sin ningún tipo de control, lo que contribuyó a que empeorara la situación. Como esto no fue previsto, todo el conexionado de los equipos nuevos, se realizó de forma muy desordenada y sin ningún tipo de previsión, lo que provocó una proliferación de switches pequeños de 8 puertos por todas las direcciones desparramados por todos lados, y además interconectados en forma de cascada entre si, existiendo varios de estos dispositivos por oficina. Como consecuencia el cableado era realmente una maraña, y se pasaban cables de red hasta las PC y entre los switches por cualquier lado, de cualquier forma y sin ninguna identificación. Como consecuencia de este crecimiento anárquico, cuando fallaba algo en alguna oficina era muy difícil encontrar la falla y llevaba mucho tiempo.

Toda esta falta de previsión y mantenimiento de la instalación, provocó una situación muy curiosa, llevó a que un sector del predio con dos direcciones quedara totalmente desconectado de la red de la repartición, motivo por el cual se había contratado un proveedor de internet con servicio hogareño para que tengan servicio de Internet estas direcciones aisladas. El servicio de internet en el todo el predio era provisto por una sola empresa, mediante seis modems hogareños funcionando detrás de routers sin ningún tipo de control en la navegación, por lo que estaba permitido visitar cualquier tipo de sitios, generándose descargas, streaming, juegos, etc, lo que provocaba una sobrecarga de tráfico enorme sobre los routers, que los hacían salir de servicio repetidas veces durante la jornada laboral.

Con respecto a la parte lógica el caos era total. Las direcciones IP estaban asignadas al azar, no existía ningún tipo de segmentación ni organización de las direcciones. Para dejar clara esta situación paso a describir el método para asignar IP a un equipo a conectar a la red, se probaban direcciones disponibles con ping hasta que la que alguna no respondía, entonces se asignaba esa IP al equipo. Este método de asignación fue desastroso, ya que por ejemplo, si un equipo estaba apagado y no respondía al ping se asignaba esta IP, lo que ocasionaba IP duplicadas, y la posterior salida de servicio cuando se encendía el equipo que no había respondido. Para empeorar la situación aún más, existían distintas redes dentro de la repartición. Esto se originó cuando se reestructuró la red de datos a nivel provincial y se asignaron otros segmentos de red a la repartición, pero no se reconfiguraba la red existente, sino que se configuraron varias IP en la placas de red de las PC (binding), por lo que convivían las tres redes simultáneamente conectadas con el mismo cableado.

Pasando a otra parte de este caos queda por mencionar los equipos PC, estas presentaban dos problemáticas importantes. Una era con respecto a las restricciones sobre la operación de las mismas y la otra era su sistema operativo. Haciendo referencia a que no tenían ningún tipo de restricción en la configuración e instalación de aplicaciones, permitía cambiar cualquier parámetro de configuración o instalar cualquier aplicación que el usuario sin conocimiento técnico considerara, recurriendo a alguien autodidacta que sabía “algo” de informática, estas modificaciones se hacían sin seguir una normativa por lo que cada uno hacía lo que le parecía. Con respecto al segundo de los problemas, todas las PC tenían instalado cualquier sistema operativo, ya que no se tenía ningún criterio para la instalación, en muchos casos se instalaba un sistema operativo en hardware que no reunía los requerimientos mínimos para el funcionamiento del mismo, lo que hacía funcionar en forma deficiente a una gran cantidad de equipos PC (lentitud en la respuesta, bloqueos, esperas interminables, etc).

La situación en las distintas oficinas de las diez zonas repartidas en la Provincia era similar con respecto a la infraestructura y la configuración. Estaban conectadas al datacenter provincial mediante servicio de internet hogareño, realizando VPN por software. Todo lo descrito anteriormente se repetía en las distintas oficinas de las zonas, pero los problemas no eran tan notorios debido a la menor cantidad de usuarios que estas tienen.

2 Objetivo

En plena era de la revolución de las comunicaciones parece increíble que haya lugares a los que no haya llegado todavía la comunicación digital, pero se me había presentado un lugar en estas condiciones y el objetivo principal de este emprendimiento que la red de datos quede operativa y brinde las condiciones básicas para insertarlo dentro este tipo de tecnología digital y comenzar a dejar atrás los lentos trámites realizados con soporte de papel, e implementar sistemas que permitan realizar digitalmente los procesos que esta repartición requiere para su normal funcionamiento, tanto internamente como hacia la comunidad interactuando con el público en general. Esto estaba muy claro, pero el estado en que se encontraba la infraestructura no permitía realizar esta labor.

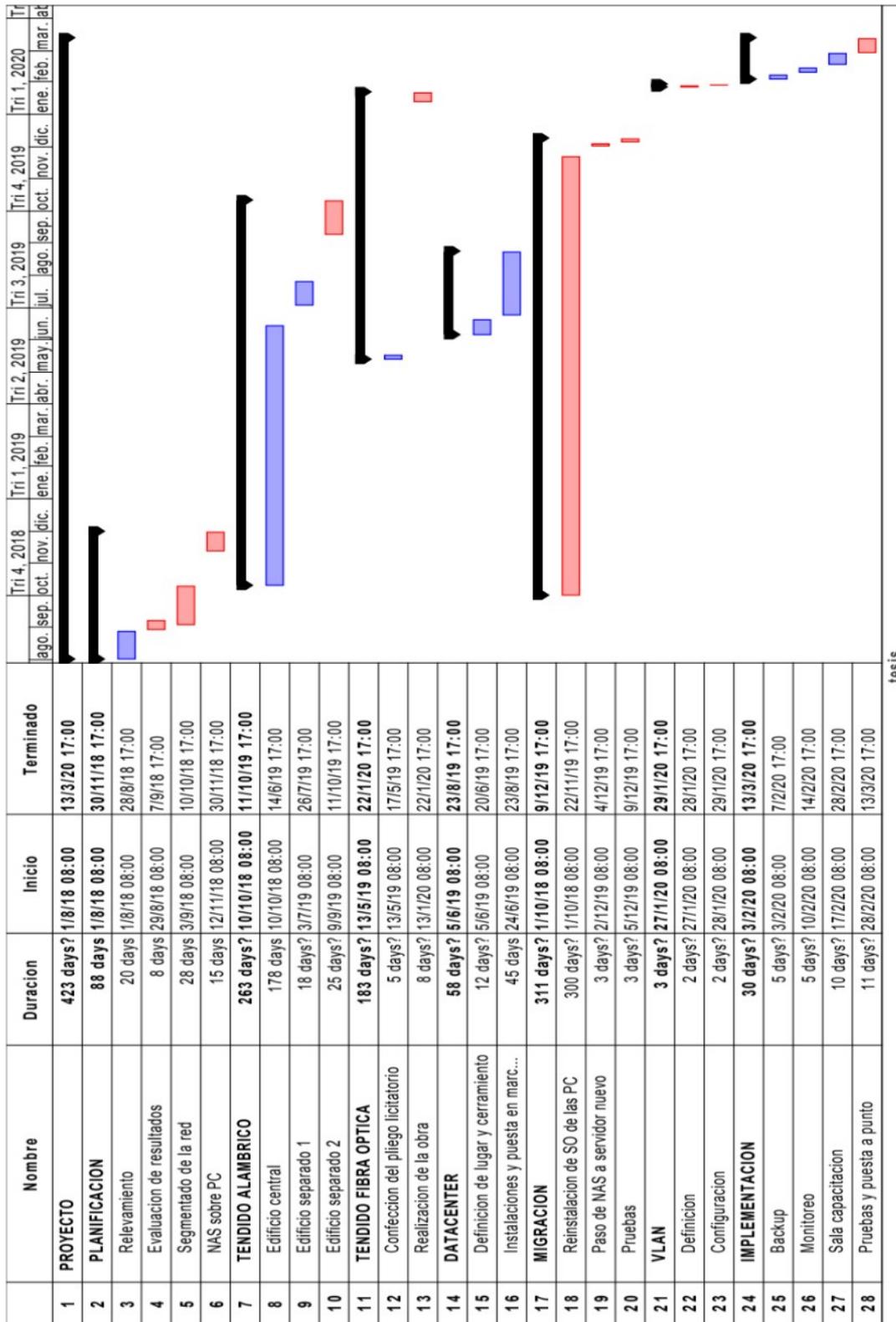
Cuando tomé contacto con la repartición pública en cuestión, me plantearon una cantidad de necesidades que me hizo ver, ya del principio, las dimensiones de este emprendimiento. Motivo por el cual, el siguiente paso fue relevar la infraestructura para definir en que situación se encontraba esta repartición. Cuando comienzo con el relevamiento di cuenta del abandono en que se encontraba y del caótico crecimiento que tuvo la red; había que empezar de cero.

Esta situación me lleva a plantear dos objetivos secundarios como paso previo para lograr el objetivo principal de este proyecto, uno es la parte de la infraestructura (puramente técnica), y el otro es revertir la mala predisposición de los usuarios al cambio, o sea a la nueva forma de trabajar a la que se tendrían que adaptar. En la reestructuración de la infraestructura, también era un objetivo lograr el cambio sin dejar fuera de servicio ninguna dirección mas de un lapso de tiempo razonable de horas, esta era una parte que debía cumplirse ya que sus complicaciones no van mas allá de las propias de una instalación; en la parte de interacción con los usuarios sería mas complicado, debido a que estaban habituados a utilizar la red de datos y los equipos PC para navegar en internet en busca de alguna información y además para recreación y uso personal (juegos, redes sociales, escuchar radios, descargas de todo tipo, etc), y a partir de este proyecto debían trabajar con esta infraestructura como soporte de sus tareas diarias, la forma en que lo logré fue con capacitación, buena atención cuando necesitaban ayuda y mostrándoles que en lugar de complicarse su trabajo, este era realizado con mayor rapidez y facilidad.

El objetivo de este proyecto no solo alcanza a la parte de infraestructura, sino también a la parte de software; todas las PC deben correr software libre sobre su hardware, para ajustarse a la ley 12360 que establece que los poderes ejecutivo, legislativo, judicial, organismos descentralizados y empresas en que el estado posea mayoría accionaria, deberán emplear en sus sistemas y equipamientos de informática preferentemente software libre. promulgada el 15-12-2004, art.57 de la c.p.; publicada en b.o. el 20-12-2004. La excepción serían equipos cuyos usuarios debían trabajar con software propietario y no existe una opción en software libre.

Este proyecto como cualquier otro tiene una fecha de inicio y una de finalización, pero debido a cuestiones presupuestarias y de tiempos ineludibles e imprevisibles de la gestión pública, tuve que prorrogar la fecha de finalización inicial. Para la realización éramos un equipo de cinco personas, dos del área de sistemas y tres del área de mantenimiento. Estos últimos eran los encargados de hacer el trabajo del tendido de cables, instalación de bandejas y cablecanal en las oficinas. En principio la propuesta era realizarlo en un año, a partir de agosto de 2018 hasta septiembre de 2019, pero se debió extender hasta febrero de 2020.

A continuación presento el plan de trabajos, en el se incluyen los tiempos de espera propios de la gestión pública, los cuales son ineludibles, como por ejemplo el tiempo desde que se genera un expediente hasta la realización de la licitación. En estos tiempos de espera fuimos realizando otras tareas que demandaron mucho tiempo, como la migración de los sistemas operativos de los equipos PC a software libre, que no significa solo el tiempo de la instalación en si del sistema operativo, sino la configuración particular de los usuarios de las distintas direcciones que tienen diferentes necesidades operativas y su capacitación para utilizar el nuevo sistema operativo y las aplicaciones.



Plan de trabajo representado mediante diagrama de Gantt

3 Metodología

En esta sección describo las diferentes etapas mediante las cuales llevé adelante el proyecto. Estas fueron diseñadas acorde a las necesidades y posibilidades de la reestructuración realizada en la repartición, teniendo en cuenta que fue hecha en forma paralela a lo que había en funcionamiento por la obvia razón de que se debía seguir con las tareas laborales diarias de la repartición. Las diferentes etapas fueron las siguientes:

1. Planificación.
2. Tendido alámbrico.
3. Tendido de fibra óptica.
4. Datacenter.
5. Diseño de VLAN.
6. Migración.
7. Implementación.

A continuación explico como lleve adelante cada una de estas etapas.

1. Planificación

En esta primera etapa el desafío era encontrar la manera proceder para lograr el gran cambio en la infraestructura de datos y llevar adelante el proyecto en todas sus etapas posteriores, combinando mis conocimientos de gestión de proyectos con las habilidades técnicas obtenidas en instalaciones y proyectos en mis experiencias anteriores como profesional de redes. El primer paso que di fue dimensionar el proyecto para presentar a las autoridades encargadas de aprobar todo lo que se debía realizar para lograr el objetivo planteado.

Parte del proyecto son siempre las partes interesadas, las cuales pueden ser afectadas o afectar, positiva o negativamente al mismo. Por este motivo fundamental, el primer paso para dimensionar esta gran tarea fue obtener un registro de los usuarios, para lo cual diseñé una planilla electrónica con el objetivo de generar una base sobre la cual diferenciar los tipos de usuarios, sus expectativas, nivel de decisión y otros datos para la gestión. Los campos representan los datos que consideré necesarios, fueron los siguientes:

ID_USUARIO	NOMBRE	DESCRIPCION	NIVEL DE INFLUENCIA	TIPO	EXPECTATIVAS	CORREO DEL USUARIO
------------	--------	-------------	---------------------	------	--------------	--------------------

A continuación describo de que se tratan los campos considerados:

- ID_USUARIO: identificación única del usuario para un uso futuro en alguna base de datos, si fuera necesario.
- NOMBRE: nombre del usuario.
- DESCRIPCION: que funcion cumple el usuario dentro de la repartición.
- NIVEL DE INFLUENCIA: este nivel de influencia puede ser ALTO, MEDIO o BAJO, según el puesto jerárquico del usuario.
- TIPO: el tipo es POSITIVO o NEGATIVO, según la predisposición que tiene el usuario hacia el proyecto de reestructuración.
- ESPECTATIVAS: que espectaiva tiene el usuario sobre el proyecto.
- CORREO DEL USUARIO: un medio para contactar con el usuario de ser necesario.

Aclarando el porqué del campo TIPO, tuve en cuenta que una parte interesada positiva puede ver el beneficio que traerá a la repartición el proyecto y normalmente está interesada en ayudar, mientras que una parte negativa no puede ver, se siente amenazada o no desea el beneficio generado por el proyecto, por lo que puede ofrecer resistencia al cambio. Haciendo un análisis de los resultados de este relevamiento siempre trate de que las partes de tipo negativo se conviertan en neutras o en el mejor de los casos, en partes interesadas positivas. De esta manera documenté quienes eran las personas mas influyentes o con mayor competencia a la hora de tomar decisiones, ya que comunicarse de manera efectiva con estas personas jugó un papel fundamental en el éxito del proyecto. Esto no quiere decir que los usuarios con menor nivel de decisión no fueron tomados en cuenta, sino que sus opiniones y requerimientos fueron presentados a los usuarios con el grado adecuado de toma de decisiones para llevar adelante esta tarea de reestructuración.

Conjuntamente con el relevamiento de los usuarios también realicé un relevamiento mediante planilla electrónica de todas las direcciones y lugares donde existieran dispositivos de red, registrando sistema operativo por PC, estado y cantidad de PC por dirección y oficina, todos los switches repartidos por todos lados, las necesidades de los usuarios y el estado de la instalación.

ID_EQUIPO	IP	SISTEMA OPERATIVO	USUARIO	DIRECCION	OFICINA	ANTIGUEDAD
-----------	----	-------------------	---------	-----------	---------	------------

A continuación describo de que se tratan los campos considerados:

- ID_EQUIPO: una identificación única del equipo para un uso futuro en alguna base de datos, si fuera necesario.
- IP: la dirección IP del equipo en la red.
- SISTEMA OPERATIVO: sistema operativo instalado en el equipo.
- USUARIO: el usuario que trabaja en el equipo.
- DIRECCION: Dirección a la que pertenece la oficina.
- OFICINA: nombre de la oficina donde está emplazado el equipo.
- ANTIGUEDAD: el valor es ALTA, MEDIA o BAJA, y hace referencia a la antigüedad del hardware de la PC, siendo ALTA una PC con más de ocho años, BAJA un equipo con menos de tres años de antigüedad.

Después de esta labor ya tenía un mapa físico de los equipos, de los de problemas más apremiantes y principalmente de las expectativas de los usuarios. Al tener conocimiento de la forma en que estaban desarrollando sus tareas diarias los usuarios, la disposición real de dispositivos y oficinas, y las expectativas que tenían sobre el proyecto, concerté reuniones con los usuarios con el grado adecuado de toma de decisiones para enumerar los requisitos del proyecto, y así determinar las funciones, capacidades y calidad que la nueva red debía tener. Cabe destacar que los requisitos presentados por los usuarios no fueron cien por ciento técnicos debido a que algunos problemas a resolver en las metodologías laborales fueron presentados por personas ajenas al ámbito informático o del área de sistemas, por lo que como profesional presenté alternativas adecuadas a las circunstancias.

Luego de las reuniones de las cuales surgieron los requisitos del proyecto, generé un documento mediante el cual se asociaron los requisitos con cada parte interesada. De esta manera obtuve el rumbo a seguir y los objetivos a cumplir para presentar a la autoridad firmante. De esta forma quedó registrado que dirección solicitaba determinado servicio o requerimiento, por lo que quedó claro a quien se debía informar por la aprobación o denegación de los requerimientos realizados después de la evaluación por la autoridad que aprueba la realización. Como resultado de todo esto el proyecto tenía ahora una dirección a seguir y objetivos que cumplir, mientras que se puede mantener un registro de todo el trabajo que se necesita realizar, y además fue posible priorizar las tareas según su nivel de importancia.

La planilla presentada a la autoridad fue la siguiente:

ID_USUARIO	REQUISITO	PARTE_INTERESADA	STATUS
------------	-----------	------------------	--------

A modo de aclaración de los campos considerados:

- ID_USUARIO: identificación única del usuario para un uso futuro en alguna base de datos, si fuera necesario.
- REQUISITO: contenido generado por el profesional en sistemas, puramente técnico.
- PARTE INTERESADA: autor del requerimiento.
- STATUS: el STATUS es APROBADO o NO APROBADO

Una vez que todas las partes interesadas fueron informadas sobre los requisitos aprobados se generó un documento de conformidad sobre la definición del ámbito del proyecto: “La creación de una nueva red de datos que cumpla con las especificaciones técnicas enumeradas en el documento llamado requisitos de la nueva red de datos”.

A continuación enumero los ítems que establecí como la base para la nueva red de datos y fueron aprobados. Todos ellos junto con los requerimientos surgidos de los usuarios estaban incluidos en el documento llamado **Requisitos de la nueva red de datos:**

- La topología de la red debe ser en estrella, bajo ninguna circunstancia debe haber algún dispositivo en cascada.
- Un switch debe ser designado para la función de conmutador principal de la red en estrella.
- Los gabinetes a instalar deben cumplir con la norma de cableado estructurado.
- Los switches deben ser administrables.
- Debe haber un gabinete por dirección con los switches necesarios según la cantidad de PCs.
- Los puertos de los switchs deben ofrecer una velocidad de 1Gbps.
- Debe ser posible administrar los switches por líneas de comandos, ssh, telnet y http.
- Los switches deben enviar sus logs a un servidor syslog.
- Debe ser posible limitar el ancho de banda utilizado por un puerto.
- Debe ser posible bloquear el acceso a direcciones IP específicas.
- Debe ser posible monitorear los switches mediante SNMP.
- Debe mantenerse la conectividad de la red actual para permitir el normal desarrollo de la repartición mientras se implemente la nueva red de datos.

Una vez definido el ámbito comencé a comparar los requerimientos técnicos del proyecto con las especificaciones técnicas de los fabricantes de servidores y switches para definir con que dispositivos se implementaría la red. Después de analizar distintas opciones y teniendo en cuenta la existencia de switches HP instalados en la Repartición decidí elegir el switch HPE OfficeConnect 1920S 24G 2SFP para conectar dispositivos finales de las oficinas, Pcs e impresoras. Ya que se han diseñado para redes medianas, estos switches son ideales para el entorno que requieren funciones avanzadas para un control granular y donde la flexibilidad es imprescindible para facilitar la gestión y la configuración de red.

Para cumplir la función de switch principal de la topología estrella elegí el HP 5500-24G, debido a que esta serie de switches es una familia de switches Gigabit con gestión web inteligente con enlaces ascendentes de 10GbE que permiten conexiones de alto rendimiento.

Ahora tenía que definir un servidor a adquirir, debía contar con la capacidad para poder brindar los servicios propuestos y aprobados, también tener en cuenta un crecimiento a futuro de la red, o sea de los servicios y los usuarios. Debido al tipo de equipamiento y al monto de esta adquisición había que realizar la compra mediante una licitación, por lo tanto realizar el pliego, tarea para la cual me contacté con personal de otra repartición provincial relacionada con la tecnología de servidores. Este área, entre otras cosas, se encargaba de la generación de los pliegos bajo los estándares de compras de tecnología de la Provincia, por lo que tenía que hacerle llegar la necesidad y ellos realizaron el pliego que luego fue evaluado por un comité para dar el visto bueno para poder iniciar la licitación. El pliego licitatorio fue realizado para comprar un paquete que incluía un servidor, una ups y un gabinete de 40U para equipar el datacenter. Los requerimientos técnicos de los equipos con los que se realizó la licitación se muestran en las fichas técnicas con referencia **FT-SRV-V** para el servidor, **FTRACK40U** para el gabinete y **FTUPS2KVA** y se adjuntan en el apéndice I. La empresa que ganó la licitación nos proveyó de un servidor marca DELL PowerEdge R540, una UPS marca APC SRT2200RMXLA-NC y el gabinete de 40U marca Gabitel. No se incluyó al switch HP 5500 24G en el pliego debido a que la infraestructura tecnológica Provincial cuenta con un switch HP 5500 mediante el cual la repartición está vinculada a la red MAN de la Provincia, o sea es el punto de acceso de la Repartición a la MAN provincial. El enlace entre la repartición y el switch es de fibra óptica, por lo que se utilizó este switch para realizar el ruteo entre las VLAN internas de la repartición.

Además de los requerimientos técnicos determiné necesidades y/o servicios de la red que debían implementarse en el proceso de reestructuración, que enumero a continuación con un orden descendente de prioridades. Luego de enumerarlos doy una breve descripción de ellos:

- I. Segmentar la red y redefinir todas las ip, tanto de las PC como de los servidores.
- II. Implementar inmediatamente un servidor de archivos (NAS) para uso de las direcciones.
- III. Reinstalar todos los equipos PC con software libre y restricciones a los usuarios.
- IV. Cambiar el servicio de internet existente por uno corporativo.
- V. Disponer de un lugar físico para montar un datacenter.
- VI. Crear una sala de capacitación.

I. Segmentar la red y redefinir todas las direcciones IP, tanto de las PC como de los servidores.

Había que redefinir las IP de todos los equipos que integraban esta red, ya que estaban otorgadas en forma aleatoria en toda la repartición, y resultaba imposible realizar cualquier planificación. La propuesta era otorgar a cada dirección un segmento diferente para segmentar esta gran red en subredes y así mejorar el rendimiento en el futuro, para ello definí los segmentos para cada dirección. Pero en esta etapa todavía sería una red plana de todos contra todos, el objetivo en este momento era tener una mejor organización para seguir con el objetivo final. También definí un segmento para los servidores y otro para la sala de capacitación que aun no existía en esta etapa.

Este cambio de IPs traía un problema asociado con un sistema de seguimiento de expedientes alojado en los servidores del datacenter provincial. Las PC que realizaban transacciones sobre la base de datos de dicho sistema validaban el acceso por usuario y por IP, por lo que al modificar las IP de las PC los usuarios del sistema dejarían de tener acceso. A este problema lo resolví poniéndome en contacto con el administrador y proponiéndole si era posible que dejara vigentes ambas listas de IPs, las nuevas y las que se estuvo trabajando hasta el momento, y luego de una semana dé de baja la lista antigua; así de esta manera coexistirían las dos listas para permitir realizar los cambios sin dejar de poder operar sobre el sistema. Al encargado de administradores le pareció adecuado, por lo que lo hicimos de

esa manera y el cambio de las IP resulto exitoso sin tener usuarios inhabilitados a realizar transacciones en ningún momento.

II. Implementar inmediatamente un servidor de archivos (NAS) para uso de las direcciones.

El almacenamiento conectado a la red, NAS (Network Attached Storage), es un tipo de dispositivo de almacenamiento de archivos dedicado que brinda nodos de la red de area local para almacenamiento compartido de archivos a través de una conexión Ethernet. Es un dispositivo de almacenamiento conectado a la red que permite almacenar y recuperar los datos en un punto centralizado para usuarios autorizados a realizar acciones sobre el. Los dispositivos NAS por lo general no tienen un teclado o pantalla, se configuran mediante un acceso basado en un navegador mediante una interfaz web, radica en la LAN como un nodo de red independiente con su propia dirección IP. El beneficio mas importante del NAS es su capacidad de proporcionar a varios usuarios de la red acceso a los mismos archivos. Sin un NAS, se tienen a los archivos dispersos, generando los problemas ya conocidos con datos desincronizados, problemas de fiabilidad y de control de restricciones al acceso, retrasos a la hora de responder a solicitudes de servicio, la configuración y mantenimiento por separado de los diferentes equipos donde residen los archivos, por citar los inconvenientes mas relevantes.

Con un sistema NAS, los datos siempre están accesibles, lo cual facilita a los usuarios colaborar y responder a las peticiones de manera oportuna. Del punto de vista de la parte técnica se puede dar seguimiento de inmediato a situaciones problemáticas, gracias a que la información y el hardware están en un solo lugar. Por citar algunas de las ventajas de estos sistemas de almacenamiento son fáciles de operar, tienen costos más bajos de mantenimiento, las copias de seguridad son mas sencillas, entre otras muchas mas.

La propuesta de implementar el servidor de archivos en esta red, aparte de las ventajas propias de esta tecnología para ordenar el trabajo en red, fue para lograr dos objetivos, uno mejorar la forma en que estaban realizando las tareas diarias los usuarios y el otro fue para que los usuarios comiencen a ver a la red como un medio mas efectivo y simple para trabajar y no como algo mas complicado. Detallando los dos objetivos mencionados quiero aclarar que, dependiendo de la dirección, había archivos a los cuales accedían varios usuarios para obtener o volcar datos en ellos. A esta tarea la realizaban pasándose los archivos mediante algún medio externo(pendrive, disco externo, DVD, impresión, etc), por lo que resultaba realmente engorroso el trabajo, entonces al poner en producción un servidor de archivos, mediante capacitación y buen servicio comenzaría a cambiar la percepción por parte de los usuarios a esta nueva forma de trabajar.

Hay diferentes fabricantes de dispositivos NAS, como SEAGATE, WESTERN DIGITAL, etc, que comercializan un producto final constituido por un hardware y sistema operativo propio, que solo hay que configurarlo acorde a la red donde se va a conectar, generar los usuarios con sus permisos y nada mas, el dispositivo queda en funcionamiento. Pero esta solución no era la adecuada para nuestra situación, ya que la idea fue implementar un NAS provisorio, con una solución de software que permita realizar mas adelante la migración del mismo al servidor sobre el cual se iban a virtualizar los servicios de la red, hardware que estaba en proceso de adquisición en esta etapa del proyecto.

Este servidor NAS provisorio se puso en servicio con el software libre OpenMediaVault 4.1 basado en Linux Debian virtualizado sobre la plataforma de virtualización PROXMOX 5.2. OpenMediaVault 4.1(OMV) es una distribución libre de Linux lanzada en 2009 diseñado para almacenamiento conectado en red (NAS). Su desarrollo se basa en la distribución Debian del sistema operativo Linux, y está disponible a través de la v3 de la Licencia Publica General de GNU. Opté por este sistema base para el NAS, debido a que las características que presenta se ajustan muy bien a la funcionalidad que se necesita en la repartición para trabajar con este tipo de servicios de red.

Para esta tarea se armó un equipo PC con un microprocesador Intel i5, 24Gb de RAM DDR4 y tres discos rígidos de 1Tb configurados en RAID 5 por software, mediante el sistema operativo, sobre el cual se instaló la

plataforma de virtualización PROXMOX 5.2 para que luego sea posible realizar la migración al servidor nuevo, una vez adquirido y en funcionamiento. Este NAS solo brindaría servicio temporalmente hasta que esté en producción el servidor nuevo en el datacenter. El servicio de NAS fue habilitado solo a los usuarios mas apremiados con el uso de archivos debido a las limitaciones del hardware sobre el cual estaba implementado. A los demás usuarios se les dio acceso una vez que estaba en servicio el servidor nuevo en el datacenter.

III. Reinstalar todos los equipos PC con software libre y restricciones a los usuarios.

Este punto era de fundamental importancia para que tuviera éxito el gran cambio de la infraestructura ya que al realizar el relevamiento quedó en evidencia la anarquía reinante en la red. Todos los equipos PC eran irregulares en cuestión de licencias, no había un criterio de seguridad de ningún tipo, había cualquier tipo y variedad de software instalado, en algunos casos el hardware de la PC no tenía la capacidad para que el sistema operativo funcione de manera correcta, entre muchas otras irregularidades en las instalaciones de los sistemas operativos de las PC.

Los detalles de esta etapa están desarrollados en la sección 5.MIGRACIÓN, pero aquí dejo a modo de introducción un breve resumen. El sistema operativo que se instalaría en todas las PC sería Linux UBUNTU 18.04, salvo justificación por escrito avalada por el director de la dirección para utilizar software con licencia paga. El software ofimático también debía ser libre y se utilizó LibreOffice en todos los casos, Windows y Linux, porque cumplía con las necesidades de los usuarios y además es compatible con muchos formatos de archivos que utilizaban en las oficinas (planillas de cálculo y documentos de texto) y no había que realizar conversiones para mantener la compatibilidad en la gran mayoría de los casos.

Otro punto a lograr era que los usuarios no instalen cualquier aplicación que se les ocurra o creen necesaria, por lo que se generó el usuario para uso de informática con privilegios de administrador y un usuario limitado en los permisos y accesos para todos los usuarios. De esta manera cuando alguno requería instalar alguna aplicación o necesitaba cambiar alguna configuración debía informar al área de informática para que este área evalúe si ese cambio o instalación es justificado, y de ser así se realice la tarea requerida. Para poner en práctica estos cambios se habilitó el acceso por ssh a las PC para poder acceder remotamente y realizar los cambios o instalación de forma rápida y segura. Además se instaló también la aplicación NoMachine para tener un acceso remoto desde la interfaz gráfica, para indicar como realizar alguna tarea a los usuarios sobre alguna aplicación a modo de ayuda, o para configurar remotamente algunas aplicaciones que se administran desde el entorno gráfico.

IV. Cambiar el servicio de internet existente por uno corporativo.

El servicio de internet que estaba funcionando cuando realicé el relevamiento consistía en seis modems hogareños provistos por el mismo ISP, que daban servicio a toda la repartición. Este servicio hogareño funcionaba en un ámbito que estaba integrado por 60 PC aproximadamente por cada modem en promedio sin un balanceo de carga de los módems por lo que algunos tenían mucho más que ese número. Como resultado de esta distribución el servicio era bastante malo; no por un mal servicio del ISP, sino por la sobrecarga a la que estaban expuestos los modems. Como consecuencia se tenía una muy baja velocidad y los modems salían de servicio cada ciertos periodos debido a la sobrecarga. Hay que tener en cuenta que todavía los usuarios hacían uso irrestricto del servicio de internet.

Para lograr una mejora me contacté con la empresa proveedora solicitando una propuesta de distintos servicios y evaluar cual sería el más adecuado. La opción que elegí fue una conexión con fibra óptica de 100 M para reemplazar los modems, este cambio fue primero aprobado y autorizado por la autoridad firmante. Por un mes se mantuvieron ambas conexiones, la fibra óptica y los modems, para no cortar el servicio a los usuarios mientras se realizaban las modificaciones correspondientes a las PC de toda la repartición. Para llevar a cabo este cambio de servicio había configurado previamente el firewall y un servidor proxy SQUID sobre el sistema operativo Linux UBUNTU 18.04 con las reglas necesarias para comenzar a restringir la navegación web en sitios no permitidos (pornografía, redes sociales,

srteamaing, juegos, etc). A medida que se iban conectando los distintos sectores al servicio de fibra se daba de baja al modem correspondiente que brindaba servicio de internet al sector.

V. Disponer de un lugar físico para montar un datacenter.

Otro punto importante que determiné es que los servidores que fueran a implementarse deberían operar sobre un entorno de virtualización. Esta decisión se debe a dos motivos principales, el mejor aprovechamiento del hardware, el servidor DELL PowerEdge R540 y la mayor seguridad de los entornos virtuales. Con respecto al hardware, la virtualización aprovecha al máximo la capacidad de los servidores y reduce su tiempo de inactividad, permite ahorrar una gran cantidad de energía y al haber menos servidores físicos también se ahorra en mantenimiento de equipos. Desde el punto de vista de la seguridad la virtualización permite programar de una forma fácil y rápida los backups de cada una de tus máquinas virtuales de tal modo que, en caso de sufrir un ataque o un fallo importante, se pueda restaurar la máquina en un breve período de tiempo. Se tiene mejor respuesta ante interrupciones imprevistas cuando los servidores sufren problemas, bien por un fallo en su sistema operativo o por un fallo del hardware. El uso de la virtualización permite trasladar los servidores virtuales a otro servidor físico que esté en perfecto estado o tenga mas recursos para poder continuar trabajando en muy poco tiempo (Este fue el caso del NAS que se había implementado sobre un PC con microprocesador Intel i5). Otro aspecto importante que tuve en cuenta fue la posibilidad de hacer pruebas de forma segura, ya que la virtualización es una plataforma excelente y segura para realizar diferentes pruebas de configuraciones o actualizaciones de software y comprobar que este funciona correctamente para implementarlo más tarde sin miedo a que ocurra algún problema.

El entorno de virtualización debía estar basado en software libre, por lo que decidí que se utilizaría Proxmox Virtual Environment, o Proxmox VE 5.1, que es un entorno de virtualización de servidores de código abierto. Es una distribución GNU/Linux basada en Debian con una versión modificada del kernel, y permite el despliegue y la gestión de máquinas virtuales y contenedores. Incluye una consola Web, herramientas de línea de comandos, y proporciona una API para herramientas de terceros. Dos tipos de virtualización son compatibles: los contenedores basados con LXC y la virtualización con KVM. Tomé la decisión de usar Proxmox 5.1 en base a que otras reparticiones están utilizándolo con muy buenos resultados, e investigando comprobé que existe mucha información sobre esta distribución en internet y gran variedad de bibliografía en librerías o sitios online.

Ahora había que definir un lugar físico para montar un datacenter y comenzar a tramitar la adquisición del equipo hardware servidor con la capacidad para virtualizar los nuevos servicios a implementar y además los servidores que estaban funcionando dispersos por toda la repartición, que no solo estaban en lugares inapropiados, sino el hardware era muy antiguo y estaba en muy malas condiciones debido a que no se le realizaban los mantenimientos de rutina.

Además, para la ubicación de este datacenter, se debía contemplar que estaría ubicado aquí el nodo central de la red, por lo que debe converger el cableado de todas las direcciones hacia él, formando la distribución en estrella de la red de datos de la repartición.

VI. Crear una sala de capacitación.

El objetivo de este punto era de disponer de un lugar para capacitar a los usuarios en el uso de las nuevas aplicaciones y en la nueva manera de realizar su trabajo, basado, a partir de esta reestructuración, en la red de datos. Un ejemplo de ello seria el uso del servidor de archivo y LibreOffice como aplicación ofimática. El fin de esta sala no solo contempla capacitar a los usuarios para utilizar esta nueva infraestructura, sino que a futuro también sea utilizada para dar capacitaciones de cualquier tipo, realizar video conferencias, realizar cursos online y que esté disponible para cualquier usuario que requiera acceder a contenidos online. Para ello se debía comenzar a gestionar la compra de equipos y materiales para este fin.

2. Tendido alámbrico

La base de toda la red de la repartición era cableada y su estado era pésimo. Para comenzar con el cambio estructural lo primero que se renovó fue el tendido de cable de toda la red, debido a que el tendido ya existente estaba muy deteriorado en algunos casos y mal instalado en otros. A todo el tendido lo dividí en dos partes para llevar de forma mas organizada la instalación nueva, una parte es el cableado de la topología en estrella que conecta las direcciones al switch principal y la otra es el cableado interior de las oficinas.



El cableado que conectaba distintas direcciones tenía partes tendidas al exterior con un gran deterioro en algunos tramos producto de una mala elección de los materiales o ignorancia de quien lo había instalado, por ejemplo había lugares en los que estaba cableado el exterior con cable para interior. Este tendido en algunos sectores estaba tirado arriba de un techo sin ningún tipo de protección, como caños o bandejas con tapa, en otros sectores estaba instalado dentro de caños pero no se habían sellado las uniones, y como consecuencia de ello entro agua y algunas alimañas a los caños, en otros casos el cable quedo a la intemperie en esos pequeños tramos deteriorándose y provocando un mal funcionamiento.



Toda esta mala instalación hizo que la duración en buen estado y con una buena operatividad de estos tramos sea muy corta, por lo que poco tiempo después comenzaron los problemas de cortes y de lentitud en el vinculo de las direcciones que dependían de estos tramos en su conexión a la red. Otro gran problema de las conexiones de las direcciones es que muchos switches estaban conectados en cascada entre ellos, y además no existía ningún plano o croquis que indique el lugar por el cual estaba pasado el cable, por lo que en algunos casos de falla se tuvo que realizar una conexión provisoria por el complicado recorrido (inalcanzable o imposible de seguir en algunos casos de cables tendidos sobre cielorraso sellado) que realizaba el cable que conectaba los switches que tenían el problema de conexión.

En el interior de las oficinas el principal problema estaba en la organización de la conexión a los puestos de trabajo por varios motivos diferentes. Lo primero que me llamo mucho la atención era la cantidad de switches de 8 puertos desparramados por todas las direcciones, y en la mayoría de los casos estaba tirados en el piso y en cualquier lugar, incluso por lugares de paso, por lo estaban pisoteados y bastante deteriorados; además de esta situación había otros switches de las mismas características conectados en cascada para darle servicio a otros puesto de las mismas oficinas y en tres casos a otras oficinas con la misma metodología. Analizando mas en detalle me di cuenta del motivo de este problema en la mayoría de las oficinas; el cableado a los puestos era embutido, partía del gabinete con un switch hacia el cielorraso y luego bajaba a la boca de conexión.





Esto estaba bien realizado, salvo que en algunos casos no estaba señalizado a que puerto estaba cableado el puesto, pero no había suficientes bocas, entonces se empezaron a colocar switches por todos lados, a medida que se necesitaba un puesto nuevo. Para graficar la situación que se había generado, es suficiente comentar que una oficina con catorce puestos funcionando solo tenía instaladas tres bocas de red embutidas desde el gabinete con el switch. Esto no era un caso aislado sino que a todas las oficinas (sin excepción) les faltaban bocas de conexión, en mayor o menor cantidad, incluso algunas no tenían bocas de conexión y a estos casos se los proveía conectando en cascada algún puerto libre del switch de 8 puertos que estaba tirado en el piso de una oficina cercana.

Resulta imposible pensar en las comunicaciones sin la existencia de normas. El principal objetivo de cualquier norma consiste en crear especificaciones uniformes para productos que permitan garantizar la interoperabilidad entre productos de diferentes fabricantes y lograr una uniformidad en las instalaciones para evitar situaciones como la descripta.

Normas de redes y cableado

Para mejorar toda esta situación muy complicada, había que encontrar una manera que sea práctica para instalar, permita extenderse con el tiempo dado la dinámica de los puestos de trabajo y además se pueda seguir con la instalación existente operativa mientras se instalaba lo nuevo. Como primera medida debía realizarse la instalación siguiendo las normas correspondientes al cableado estructurado. Una norma contiene especificaciones acerca de los componentes de sistemas o cableados, el rendimiento de las transmisiones, la arquitectura de los sistemas y los procedimientos de medición necesarios para verificar las instalaciones de redes de cables. Se define a una norma como: *"Documento establecido por consenso y aprobado por un organismo reconocido, que suministra, para un uso común y repetido, reglas, directrices o características para las actividades o sus resultados, encaminados al logro del grado óptimo de orden en un contexto dado"*. Las redes de telefonía celular y las conexiones Ethernet e inalámbricas (WiFi), entre otros sistemas, dependen de las normas de la industria, al igual que los cables que se utilizan para su conexión.

El cableado de comunicación de datos fue realizado según las normas de cableado estructurado ANSI/TIA/EIA TSB 36 y 40 que se utilizan para las especificaciones de cables UTP de par trenzado sin blindaje, que se incluye en la norma ANSI/TIA/EIA-568-B, y la norma ANSI/TIA/EIA 606, a continuación doy una breve descripción de lo que contemplan:

- ANSI/TIA/EIA-568-B: especifica los requerimientos mínimos para el cableado de oficinas. Establece recomendaciones para la topología, la distancia máxima de los cables, los tomas y conectores de telecomunicaciones, los parámetros del medio de comunicación que determinan el rendimiento, disposiciones de sujeción y conexión para asegurar la interconexión. Esta norma define un sistema de cableado de telecomunicaciones para los edificios que deban soportar un ambiente de productos y proveedores múltiples.
- ANSI/TIA/EIA-606: esta norma define la administración de la infraestructura de telecomunicaciones en edificios. Establece la codificación de colores, etiquetado y documentación de un sistema de cableado instalado. Seguir esta norma permite una mejor administración de la red, creando un método de seguimiento en los traslados, cambios, adiciones y la detección de fallas.

Teniendo en cuenta estas especificaciones el interior de las oficinas fue replanteado para realizar la instalación mediante la utilización de bandejas portacables desde los gabinetes con los switches para distribuir el grueso del cableado hacia toda la oficina y realizar las bajadas mediante cablecanal hasta la roseta de conexión montada en su caja correspondiente. Para el cableado de las oficinas hice cumplir de forma estricta las normas que se habían planteado, por lo que no se permitió el tendido exterior de ningún cable, ni el pasaje por sobre los cileorrazos y no debían quedar cables colgando ni en el suelo.



Tendido exterior que conectaba dos direcciones, como se observa en muy mal estado.



Bandejas instaladas para reemplazar el tendido por el exterior mostrado mas arriba.

Debido a que mi objetivo principal al recablear toda la repartición era que las direcciones queden conectadas al datacenter con una topología estrella y mediante bandejas portacables por el interior del edificio, eliminando de esta manera tendidos exteriores que se deterioran, estas debían respetar sin excepción este tipo de distribución de la conexión. Cumplir con este objetivo fue complicado en algunos sectores debido a su arquitectura, pero para lograrlo hice instalar las bandejas y los accesorios necesarios para poder llegar desde las distintas direcciones con el cableado de forma organizada al datacenter y así poder tener un fácil acceso en caso de alguna falla en la comunicación o en un futuro conectar una nueva dirección con sus todas sus oficinas completas.



Detalle de cableado exterior con caño plástico totalmente deteriorado



Acceso de cableado al edificio a través de una rejilla de ventilación junto con electricidad y aire acondicionado

El tendido por exterior solo se realizó para conectar los edificios que están separados de la edificación principal donde radica el datacenter. Se conectaron las direcciones que se ubicaban en otros tres edificios separados, dos a 90 metros y el tercero a 180 metros aproximadamente. En estos casos el tendido para vincularlos con el datacenter fue exterior con fibra óptica, de esta manera se eliminó la conexión mediante cable UTP que vinculaba los dos primeros edificios y los switches intermedios para recuperar la señal debido a las distancias que limitan al cable de cobre. El mas apartado estaba desconectado del edificio principal, así que de esta manera quedo vinculado con el datacenter y por lo tanto al resto de la red. Estas tres direcciones fueron provistas de sus respectivos gabinetes completos (con patchera, organizadores, línea de tensión y switches) vinculando sus oficinas con el datacenter. En los tres casos se respetó la distribución en estrella, llegando cada uno de los switches de estas direcciones al datacenter. Este tema se trata mas detalladamente en la sección siguiente Tendido de Fibra Optica.

En el interior de las oficinas las bandejas se instalaron desde los switches y de manera de cubrir la totalidad del recinto donde funcionan bajando a los puestos de trabajo mediante cablecanal con cajas y rosetas rj45 etiquetadas con el puerto de la patchera al cual se conectaba. Después de esta etapa quedaron los puestos de trabajo conectados directamente desde el switch, por lo que se eliminaron completamente los switchs de 8 puertos desparramados por todas las direcciones y los cables tendidos por cualquier lado.



Estado de un gabinete antes y después del reacomodamiento del tendido alámbrico.

Una vez concluida esta etapa prácticamente desaparecieron las incidencias y reclamos por desconexión de los puestos, cuando algún usuario reporta problemas de conexión se le brinda atención inmediata; y si hay que generar un puesto nuevo o mover alguno existente a otro lugar se realiza en no mas de un par de horas. Los usuarios notaron inmediatamente la mejora del servicio por la gran estabilidad lograda en el mismo y la mayor velocidad de respuesta que tenían al utilizar los servicios brindados por la red.

3. Tendido de fibra óptica

Dentro del predio de la repartición existen tres edificios distanciados del edificio principal. A modo de aclarar el texto denominaré a los puntos de conexión finales de la fibra óptica como DT, DE y DL. Las distancias al datacenter son de 90 metros para los gabinetes ubicados en DT y DE y el tercero se encuentra en DL a 180 metros aproximadamente. Siendo que tienen que estar conectados a la red, tenían que llegar al datacenter por algún medio de conexionado. El edificio mas alejado excedía la distancia máxima para un cable UTP CAT5, por lo que se tenía que utilizar otro medio. Los dos restantes estaban sobre el límite de los 90 metros, si bien la norma dice que se puede extender a 100 metros con el UTP CAT5, esta distancia era lineal; las vueltas y las propias características de una instalación hacían que se exceda de estos 100 metros. Evaluando estas características técnicas y también las económicas, opté por utilizar un vínculo de fibra óptica.

Esta obra fue realizada por una empresa privada designada mediante una licitación privada. Mi función en esta etapa fue la de conformar las bases de la licitación, por lo que a continuación expongo los principales puntos, sin entrar en los detalles característicos de una licitación ya que escapa al alcance de este documento.

Alcance de los Trabajos y de las Especificaciones.

Los trabajos realizados bajo estas especificaciones incluyeron la mano de obra, dirección técnica, materiales y obras civiles necesarias, para realizar el tendido de fibra óptica mono-modo, que comprendió:

- Cableado de FO entre los edificios con su correspondiente morsetería de sujeción.
- Cordones de conexión ('patch-cord'), **conectores y todo tipo de elementos necesarios para el conexionado**. Cada gabinete estaba provisto del panel de conexión con sus accesorios, de acuerdo a lo especificado en la ficha técnica de referencia **FTCAEMP** adjunta en el apéndice I.
- Los materiales y equipamiento debían cumplir con todas las normas y recomendaciones que hayan emitido los organismos públicos y/o privados, nacionales e internacionales de competencia. Se exigió las especificaciones fijadas por la CNT y la ITU (ex CCITT).
- El gabinete a instalar en dos de las direcciones deberán ser provistos de acuerdo a lo especificado en ficha técnica adjunta referencia **FTGAB12U** adjunta en el apéndice I. A estos gabinetes se los debía proveer también de 2(dos) switches administrables de 24 puertos cada uno, de acuerdo a lo especificado en ficha técnica adjunta referencia **SWETH24** adjunta en el apéndice I.

El tendido físico consistió en la vinculación del gabinete ubicado en el datacenter, el gabinete a instalado en DT, el gabinete instalado en DE y el gabinete ubicado en DL. El recorrido irá vinculando las oficinas enumeradas, realizando el sangrado de cuatro pelos de fibra en cada una, todo de acuerdo a lo especificado en la tabla TABLA DE FUSIONADO, la que se detalla mas adelante. Todos los empalmes debían ser por fusión y no por unión mecánica.

Esta conexión se realizará mediante el tendido de un cable totalmente dieléctrico de FO mono-modo de 12 pelos de fibras. El tendido debe reservar una ganancia del 10 % distribuido en el tendido, debiendo quedar el tendido de toda la fibra óptica prolijo y seguramente instalado.

No se aprobaría el tendido de FO si se detectaba algún faltante de morsetería, preformados o si los herrajes no eran los adecuados.

Las características técnicas de la fibra óptica debían cumplir con lo especificado en ficha técnica con referencia **FTFO12MM** adjunta en el apéndice I.

Se consideró que los cables de fibra óptica se debían terminar en los extremos en un panel de interconexión ('patch panel') con capacidad de fijar y empalmar las fibras individuales mediante conectores SC. Debían disponer acopladores para conectar todos los hilos de la fibra solicitados.

No se permitió la realización de empalmes o soldaduras en ningún punto del tendido de la fibra óptica. Se debió respetar rigurosamente el radio mínimo de curvatura especificado por el fabricante de la fibra.

Se exigió garantía de 5 años para los cables, conectores y hardware de conexión (pasivo) contra defectos de material, manufactura y cualquier otro problema atribuible a una falla propia de los componentes del cableado.

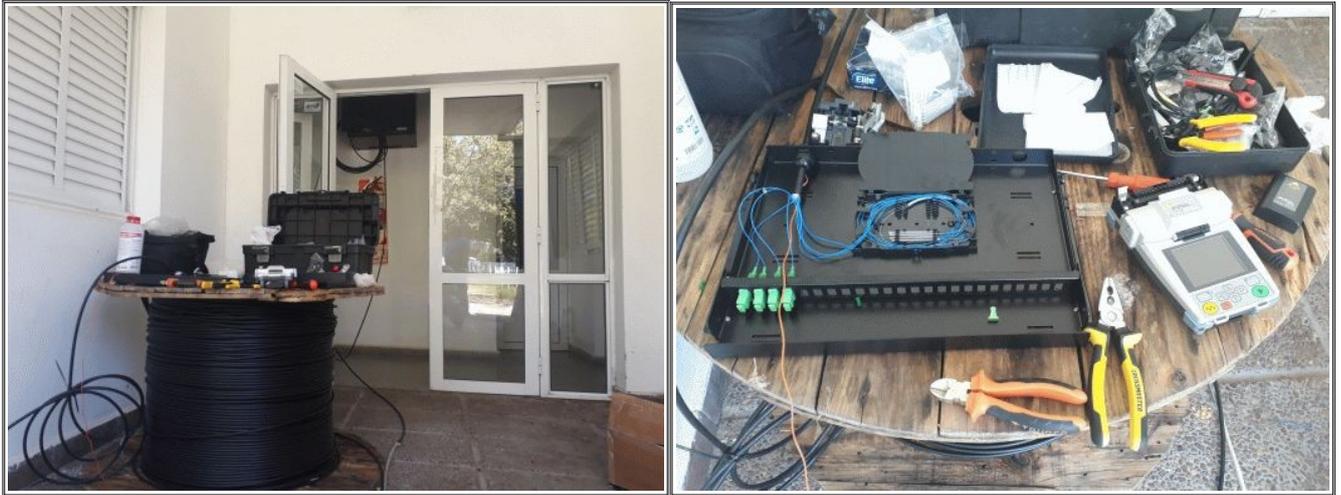
La certificación del enlace fue realizado por personal competente de la Secretaria de tecnología de la Provincia. Se midió la atenuación a 1310 y 1550 nanómetros, el testeó fue medido en ambas longitudes de onda en una dirección en cada hilo de fibra. Este fue realizada de acuerdo con el standard EIA/TIA-526-7, método 1A. La evaluación de panel a panel (backbone) se basó en los valores establecidos en la EIA/TIA-568-A anexo H, Optical Fiber Link Performance Testing.

Una vez terminado y certificado el trabajo, la empresa que realizó el tendido entregó un plano especificando detalles del tendido (trayectoria, rollos envolventes, puntos de fijación, etc.), acto por el cual se da por finalizada esta etapa.

TABLA FUSIONADO					
	Tramo 1		Tramo 2		Tramo 3
Fibra N°	Datacenter	DT		DE	DL
1	SC/pig/Fus	SC/pig/Fus			
2	SC/pig/Fus	SC/pig/Fus			
3	SC/pig/Fus	SC/pig/Fus			
4	SC/pig/Fus	SC/pig/Fus			
5	SC/pig/Fus	Fusión Tramo 1 y 2		SC/pig/Fus	
6	SC/pig/Fus	Fusión Tramo 1 y 2		SC/pig/Fus	
7	SC/pig/Fus	Fusión Tramo 1 y 2		SC/pig/Fus	
8	SC/pig/Fus	Fusión Tramo 1 y 2		SC/pig/Fus	
9	SC/pig/Fus	Fusión Tramo 1 y 2		Fusión Tramo 2 y 3	SC/pig/Fus
10	SC/pig/Fus	Fusión Tramo 1 y 2		Fusión Tramo 2 y 3	SC/pig/Fus
11	SC/pig/Fus	Fusión Tramo 1 y 2		Fusión Tramo 2 y 3	SC/pig/Fus
12	SC/pig/Fus	Fusión Tramo 1 y 2		Fusión Tramo 2 y 3	SC/pig/Fus
Total Pig SC	12	12		8	4
Total Fusión	12	12		8	4

En esta tabla se detallan los distintos puntos de fusionado y corte de la fibra óptica en la distintas direcciones.

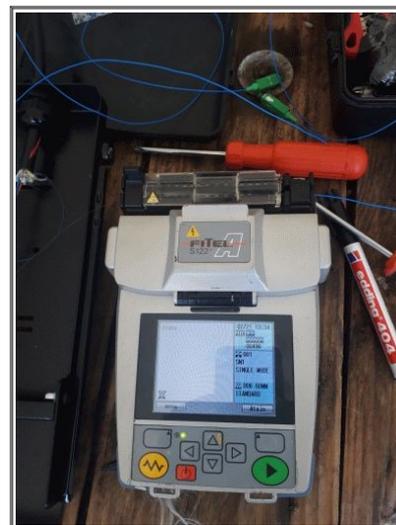
A continuación algunas imágenes de la realización del tendido de la fibra óptica:



Instalación del ODF en uno de los gabinetes.



Realización del tendido de fibra óptica



Fusionador de fibra óptica empleado en la instalación.

4.Datacenter

Al comenzar este proyecto no había un lugar donde ubicar un servidor, no había donde centralizar el nodo para migrar la topología de la red de cascada a estrella. Este motivo hizo que se comenzara a pensar donde ubicar un datacenter, y luego de definir su ubicación comenzar los tramites necesarios para adquirir todo el equipamiento y realizar las obras necesarias.

El datacenter estaría compuesto por el servidor, el switch conmutador principal de la estrella, una UPS, el transceptor del proveedor de internet, el switch de distribución de internet, el transceptor de la fibra optica de la MAN provincial y el switch de interconexión con la misma. Todos estos componentes o dispositivos debían ser rackeables para instalarlos en el gabinete de 40U.

Para determinar la ubicación física tuve en cuenta la topología en estrella, por lo que de ser posible debía ubicarse en un lugar equidistante con la mayor cantidad de direcciones posibles. Encontré tres lugares posibles, entonces comencé la gestión para determinar cual era viable para destinar al datacenter. Luego de un tiempo de idas y vueltas quedó finalmente determinado el lugar, entonces comencé con la adecuación del mismo. El lugar designado era como un apéndice de una gran oficina, mide aproximadamente 1,80 x 2,30 metros, no tenia ventanas y tenia acceso por ambos lados. Uno de los lados daba a una gran oficina y el otro a un pasillo de paso, entonces lo que primero que se realizó fue cerrar con pared la parte que daba a la oficina y se colocó una puerta en la abertura que daba al pasillo de paso.

Una vez definido y cerrado el recinto donde se instalaría, comencé a realizar la gestión para la proveer al lugar de una instalación eléctrica estabilizada y confiable, un equipo de aire acondicionado y la luminaria necesaria. Esta obra fue realizada por una empresa privada designada mediante una licitación privada. Mi función en esta etapa fue contactar con el Ingeniero Eléctrico que redactó las bases y condiciones de la licitación, por lo que a continuación expongo los principales puntos, sin entrar en los detalles característicos de la licitación ya que escapa al alcance de este documento.

Descripción de los trabajos.

La ejecución de todos los trabajos, provisión de materiales y mano de obra especializada para las instalaciones fue realizada por la empresa ganadora de la licitación. Las instalaciones realizadas cumplen, en cuanto a provisión de materiales y ejecución, con las normas y reglamentaciones fijadas por los siguientes organismos:

- Instituto Argentino de Racionalización de Materiales I.R.A.M.
- Asociación Electrotécnica Argentina.
- Cámara Argentina de Aseguradores.

Los conductores se instalaron en cañerías, cable canal y zócalo canal según la necesidad, fabricados y ensayados según norma IRAM NM 247-3. No se efectuó ningún empalme de conductores fuera de las cajas de paso o de derivación y tienen en cuenta un espacio de reserva de un 20 % de la capacidad utilizada de acuerdo a la cantidad y sección de cables a incorporar en la misma. El cableado interno en los tableros seccionales se realizó mediante conductor unipolar de sección acorde al consumo por circuito y bajo Norma IRAM NM 247-3 para fases, neutro y conductor de protección (conductor requerido en ciertas medidas de protección contra choque eléctricos y que conecta masas, elementos conductores, borne principal de tierra, toma de tierra.). Se utilizaron los colores según la norma:

- Fase: Rojo/Marrón.
- Neutro: Celeste.
- Conductor de Protección: Verde-Amarillo (bicolor).

Las canalizaciones utilizadas fueron bandejas porta cables, caños metálicos o plásticos, cablecanal o pisocanal según la necesidad. Se utilizaron para la alojar la totalidad de los cables para la instalación eléctrica exclusiva informática, además, tienen en su interior un tabique separador de los cables de electricidad respecto de los cables de datos (señales débiles). Los gabinetes utilizados como tableros, tienen indicado en la tapa o en el frente su correspondiente nombre. De igual manera, en el contrafrente del mismo, los dispositivos que lo componen tienen indicado los circuitos que controlan.

Para la toma de energía se modificó el tablero seccional general de la Repartición, colocándose un Interruptor Automático Termo-Magnético (IATM) tetrapolar, para llegar desde este hasta el tablero seccional del datacenter y al tablero seccional del aire acondicionado. En el exterior del inmueble, se colocaron jabalinas acoplables de acero-cobre según norma IRAM 2309, de 5/8” de diámetro, alcanzando un largo total de 6 [m], a la cual se conectaron las borneras de los tableros seccionales del datacenter y del aire acondicionado.

Refrigeración del recinto.

La refrigeración del lugar fue calculada por el mismo ingeniero con el cual tuve contacto para diseñar la instalación eléctrica, y había determinado que el equipo para refrigerar este lugar debía ser de 2500 frigorías como mínimo. A partir de ese momento comencé con las gestiones para proveer del equipo a este datacenter; así llegué a conseguir un equipo que se había desinstalado de una oficina que tuvieron que ampliar. Comencé la gestión para que cedan desde la dirección en la cual estaba instalado este equipo, al área de informática. Una vez concluido el trámite y cerrado el recinto del datacenter gestioné el contacto con el instalador para que realice la verificación del funcionamiento ya que era un equipo usado. Una vez verificado su perfecto funcionamiento se lo instaló y se lo puso en funcionamiento en el datacenter.

A continuación algunas imágenes de la etapa en la que estábamos armando el gabinete del datacenter:



Instalación del servidor.

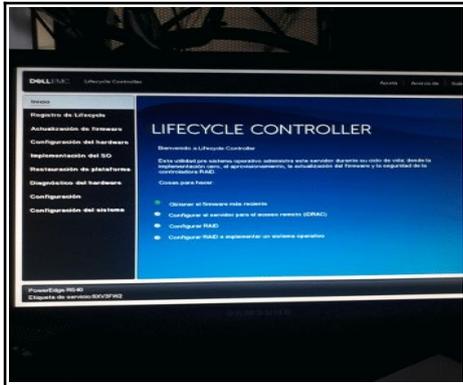
Todos los servidores Dell PowerEdge tienen integrada la iDRAC (integrated Dell Remote Access Controller) que es una controladora de acceso remoto integrada de Dell. Proporciona una funcionalidad que ayuda a implementar, actualizar, supervisar y mantener los servidores Dell PowerEdge. Está integrada en el servidor de fábrica, por lo que no requiere de un sistema operativo o un hipervisor para trabajar. Cuenta con potentes opciones de configuración y administración mediante una interfaz web y una interfaz de línea de comandos, lo que permite a los administradores realizar tareas de administración de manera remota reduciendo o eliminando la necesidad de los administradores de visitar el servidor físicamente; incluso si el servidor no está operativo. La iDRAC puede generar una alerta cuando ocurre un problema y permite la administración de servidores remota y local optimizada.

El sistema operativo que elegí para instalar sobre el servidor fue el Linux Proxmox VE, debido a que es un sistema operativo completo de administración de virtualización de servidores de código abierto. Se basa en la virtualización de KVM y la virtualización basada en contenedores y gestiona máquinas virtuales KVM, contenedores Linux (LXC), almacenamiento, redes virtualizadas y clústeres de alta disponibilidad. Las características de clase empresarial y la interfaz web intuitiva están diseñadas para aumentar el uso de sus recursos existentes y reducir el costo del hardware y administrar el tiempo. Al combinar dos tecnologías de virtualización bajo una sola plataforma, Proxmox VE ofrece la máxima flexibilidad al entorno virtual profesional. Utiliza la virtualización completa de KVM para las imágenes de Windows y Linux y los contenedores ligeros para ejecutar aplicaciones Linux libres de conflictos.

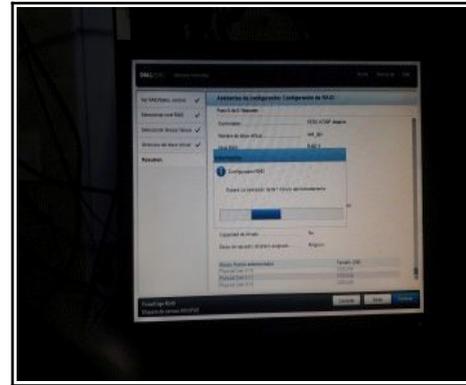
La virtualización es una tecnología de software que permite ejecutar al mismo tiempo varios sistemas operativos y aplicaciones en el mismo servidor. Está transformando el entorno de TI y cambiando radicalmente la forma en que se utiliza la tecnología. La virtualización puede mejorar la flexibilidad, la escalabilidad y la agilidad del departamento de TI a la vez que permite ahorros importantes. Las cargas de trabajo se implementan más rápido, el rendimiento y la disponibilidad mejoran, y las operaciones se automatizan, con la consiguiente simplificación de la gestión de la infraestructura de TI, que es más fácil de implementar y menos costosa de adquirir y utilizar. A continuación los principales motivos por los que opté por virtualizar:

- Reduce los costes de capital y los gastos operativos.
- Ofrece una alta disponibilidad de las aplicaciones.
- Minimiza o elimina los tiempos de inactividad.
- Aumenta la productividad, la eficiencia y la capacidad de respuesta del departamento de TI.
- Acelera y simplifica el despliegue de recursos y aplicaciones.
- Respalda la continuidad y la recuperación ante desastres.
- Permite una gestión centralizada.
- Crea un auténtico centro de datos definido por software.

Una vez terminadas las obras y las instalaciones, estaban dadas las condiciones de seguridad físicas y eléctricas, por lo que comencé con la instalación del servidor. Al encender el servidor, este realizó las verificaciones de hardware y luego se abrió la consola de configuración propia del fabricante, la iDRAC. Aquí configuré el arreglo RAID como RAID 5, le asigné una dirección IP al iDRAC e ingresé los demás parámetros de red. Luego determiné la prioridad de los dispositivos para el arranque, configurando al medio externo con el instalador del PROXMOX primero en la lista. Una vez realizado esto, al grabar los cambios me dio la opción de reiniciar, y luego del reinicio comenzó la instalación del sistema operativo. Una vez terminada la instalación estaba todo listo para comenzar la migración de lo que estaba funcionando en las PC al servidor nuevo.



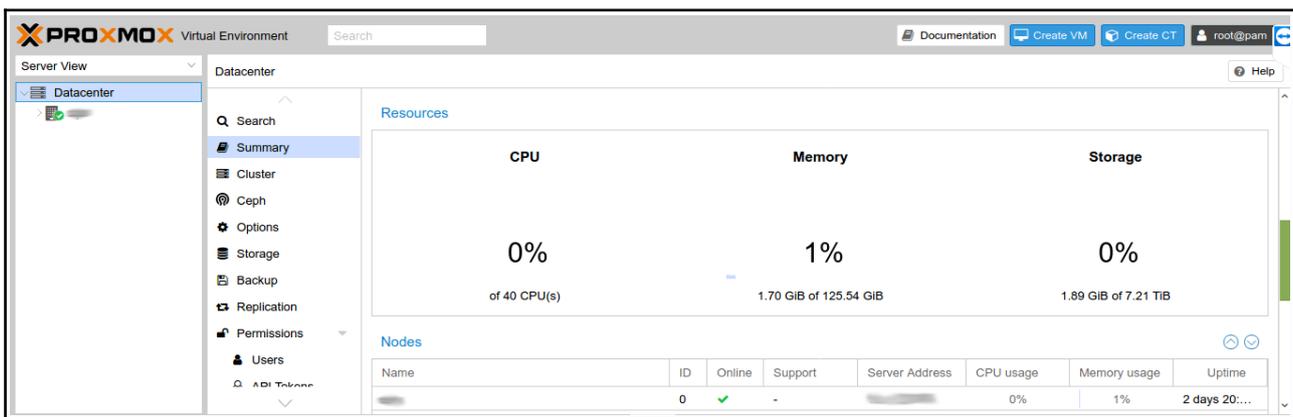
Interface iDRAC del equipo DELL PowerEdge R540



Creación del RAID 5 desde la interface del iDRAC



Reiniciando el servidor después de la configuración inicial



Interface del PROXMOX recién instalado, donde se observan los recursos del servidor

5.Migración

La migración consistió en dos partes independientes una de otra. Una de ellas estuvo relacionada con los equipos PC de toda la repartición, y la otra con el nuevo servidor, al cual se migraron los servicios que estaban implementados sobre PCs de escritorio funcionando como servidores con las limitaciones propias que un equipo de escritorio presenta con respecto a sus recursos, sobre todo microprocesador y memoria.

Las PC de toda la repartición.

Esta parte fue una de las primeras etapas con las que comenzamos, ya que había que migrar todas los equipos PC de la repartición, cerca de 400, y se extendió casi hasta la finalización del proyecto. La migración de las PCs consistió en reemplazar los sistemas operativos de todas las PC, debido a que como se mencionó anteriormente en el punto 3 de los requerimientos técnicos donde determiné necesidades y/o servicios de la red que debían implementarse en el proceso de reestructuración. La irregularidad de los equipos era total, ya sea desde el punto de vista del sistema operativo como de las aplicaciones; no existía un criterio de seguridad, no había restricción alguna sobre el acceso a la configuración, no existía ningún backup, no se tenía un sistema operativo de referencia, ya que había una gran variedad de versiones de ellos instalados (Windows XP, Windows XP ue, Windows 7, Windows 7 SP1, Windows 8, Windows 8.1, Windows 10, una PC con Linux LUBUNTU 14.04 y muchas de las versiones referenciadas estaban personalizadas). Los equipos con sistemas Windows en cualquiera de las versiones mencionadas, eran aproximadamente el 99%, por lo que había que migrar prácticamente todas las PC para estar en regla con la ley provincial 12360 de software libre.

El sistema operativo que decidí instalar fue el Linux UBUNTU 18.04, ya que es un sistema operativo de código abierto y libre, está basado en Debian y tiene versiones para escritorio y servidores. Está orientado al usuario promedio, muy enfocado en la facilidad de uso y en mejorar la experiencia del usuario. Se compone de una gran variedad de software preinstalado, normalmente distribuido bajo una licencia libre o de código abierto. Las estadísticas web indican que la cuota de mercado de Ubuntu dentro de las distribuciones Linux es aproximadamente del 52%, por lo que la comunidad de ayuda y desarrollo es enorme.

Una vez establecido el sistema operativo con el cual funcionarían las PCs, el paso siguiente fue definir como se configurarían. Para ello generé un listado con los diferentes pasos y acciones a seguir para instalar los equipos, de manera que se siga un estandar para instalar y configurar las PC. En la instalación del sistema operativo, se creaba el usuario “informatica” con privilegios administrativos o de “root” y se asignaba el nombre del host con el formato RRRR-DDDXXX (siendo R nombre de la repartición, D nombre de la dirección y X el numero de la PC). Como aclaración UBUNTU no incluye el usuario root. En su lugar, se da acceso administrativo a usuarios individuales, que pueden utilizar la aplicación “sudo” para realizar tareas administrativas. La primera cuenta de usuario que se crea en el sistema durante la instalación tendrá privilegios administrativos o de “root”, por lo tanto tiene acceso a “sudo”. Cuando se ejecuta una aplicación que requiere privilegios de administrador, sudo le pedirá que escriba su contraseña de usuario y no las puede realizar cualquier usuario no autorizado. Una vez terminada la instalación del sistema operativo, se la asigna la IP correspondiente a la PC, se la configura para utilizar el proxy, los repositorios provinciales y se instalan las actualizaciones del sistema operativo y de las aplicaciones. Luego se le instaló:

- El cliente OCS para el sistema de inventario.-
- La aplicación NoMachine para acceso remoto al entorno gráfico.-
- El servicio ssh para acceder remotamente por consola.-
- Se creaba el usuario estandar sin privilegios de acceso utilizando como nombre de usuario el nombre real del usuario que opera en la PC y se deshabilita el usuario “invitado”.-

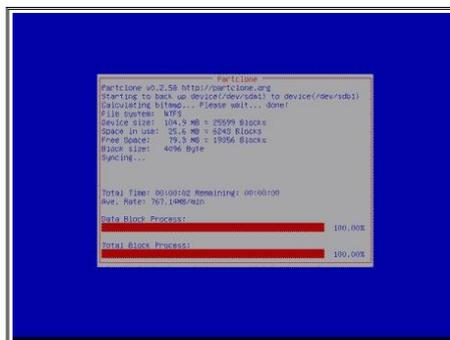
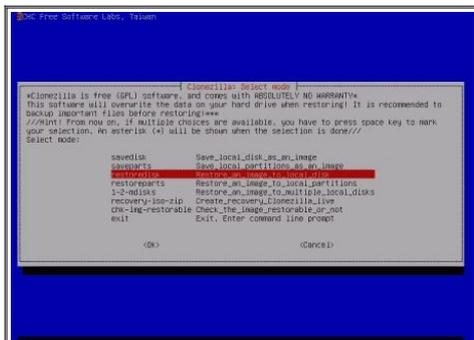
Al usuario estandar se le configuraban algunos detalles para facilitarle su labor diaria. Teniendo en cuenta que estaba habituado a un Windows personalizado en la mayoría de los casos, la cambiamos el entorno gráfico original de UBUNTU 18.04 por una llamado UBUNTU MATE, con el cual se logró una mejor adaptación por parte de ellos. Sobre este se le creaban acceso directos al navegador web y las aplicaciones ofimáticas, sobre el escritorio y la barra de tareas. Además configurábamos al sistema para que abriera el navegador en la página de cursos que ofrecía la administración provincial y así resolvimos un reclamo, que nos comunicaron los directivos era de larga data, el que se refería a que no se enteraban del dictado de los cursos.

De esta manera se instalaron todas las PC de la repartición pero había algunos casos particulares:

1. Se estaba utilizando una aplicación muy antigua con la que se llevaba el registro y liquidación de viáticos, el movimiento interno de expedientes y los registros de los empleados, esta última era de uso exclusivo de la dirección de RRHH. Esta tarea no estaba centralizada por lo que cada dirección que la utilizaba lo hacia sobre una PC local con una base de datos independiente por cada dirección. Esta corría sobre DOS, y no funcionaba sobre sistemas operativos superiores o mas modernos a Windows XP, si bien ya no se utilizaban se las debía conservar para mantener el registro de las antiguas operaciones.
2. Dos equipos PCs de la dirección de RRHH utilizaban una aplicación propietaria instalada por una empresa a la cual no se le había renovado el contrato de mantenimiento. Esta aplicación administraba los datos de los relojes biométricos para el registro de las entradas y salidas de los empleados para generar las planillas de asistencia y corría sobre Windows XP. Increíblemente no existían manuales ni instaladores, ni copia de seguridad de esta aplicación, pero debía seguir funcionando mientras se realizaba el traspaso a una nueva aplicación para control de personal centralizada en el datacenter provincial.

Para resolver estas dos cuestiones se utilizaron diversas herramientas de software, como CLONEZILLA y VIRTUALBOX. Para conocer mejor las herramientas doy a continuación un breve resumen de ellas:

- **CLONEZILLA:** Clonezilla es un software libre de clonación de discos enteros o particiones permitiendo disponer de un backup o copia de seguridad del sistema o datos antes de que se vean afectados por un fallo físico del hardware de almacenamiento o por cualquier otro problema relacionado con algun software como por ejemplo un virus o un ransomware. De esta manera permite clonar máquinas individuales, y así guardar la clonación o imagen de dicho equipo en un fichero de imagen como una copia exacta de datos. Tiene la opción para elegir guardar esta imagen localmente (en tu disco duro o pendrive) o en un servidor mediante conexión SSH, un servidor Samba o NFS de archivos, entre otras opciones mas. Por supuesto, cuando sea necesario tiene las opciones de restaurar estos puntos de backup.



Imágenes de pantalla de Clonezilla realizando un proceso de restauración de una imagen.

- **VIRTUALBOX: Oracle VM VirtualBox**, conocido generalmente como VirtualBox es un software de virtualización para arquitecturas x86/amd64. Por medio de esta aplicación es posible instalar sistemas operativos adicionales conocidos como “sistemas invitados”, en una PC, a cuyo sistema operativo se lo denomina sistema operativo “anfitrión”, cada uno con su propio ambiente. Entre los sistemas operativos soportados para la PC anfitrión se encuentran GNU/LINUX, Mac OS X, OS/2 Warp, Windows en todas sus versiones actuales y Solaris/OpenSolaris, y dentro de ellos es posible virtualizar los sistemas operativos FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris, MS-DOS y muchos otros. En cuanto a la emulación de hardware, los discos duros de los sistemas invitados son almacenados en los sistemas anfitriones como archivos individuales en un contenedor llamado *Virtual Disk Image*, incompatible con los demás softwares de virtualización. Otra de las funciones que presenta es la de montar imagenes ISO como unidades virtuales ópticas de CD o DVD.



Imágenes de la herramienta VirtualBox.

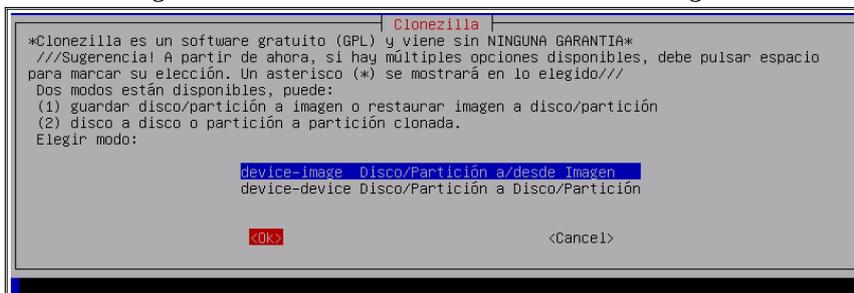
Para solucionar la primera de las cuestiones recurrimos a la herramienta VirtualBox instalada sobre el Linux UBUNTU 18.04, con la cual generamos una máquina virtual para instalarle FreeDOS. A esta máquina virtual se la configuró con 32Mb de memoria RAM, disco rígido de 500Mb y se la arrancó con el archivo .iso descargado desde <http://www.freedos.org/download/>. FreeDOS nos da la posibilidad de que tenga acceso a internet, pero en nuestro caso lo dejamos deshabilitado, ya que el objetivo solo es correr estas aplicaciones antiguas. Luego realizamos la copia de los archivos de esta aplicación antigua y le dejamos en el escritorio del usuario un instructivo con los pasos a seguir para llegar a la aplicación y ejecutarla en caso que la necesite. Estos pasos se realizaron en todas las PC donde era necesaria la aplicación.

El segundo de los casos fue mas complicado pero llegamos a una solución que fue satisfactoria y muy bien aceptada por los usuarios. La idea fue de instalar el sistema operativo Linux UBUNTU 18.04 sobre un disco rígido nuevo como cualquier otra PC de la repartición, una vez terminada la instalación del sistema operativo generé una imagen del disco rígido con el que estaba funcionando la PC que contenía la aplicación problemática, y luego arrancar con esa imagen una máquina virtual generada en un VirtualBox instalado sobre el Linux UBUNTU anfitrión. Parece muy simple pero tuvo sus complicaciones que las resolvimos oportunamente investigando y probando distintas maneras de lograrlo.

Una vez instalado el Linux UBUNTU 18.04 sobre un disco rígido nuevo, el primer paso fue iniciar una PC desde un cd booteable con clonzilla para generar la imagen del disco físico, este se ejecuta en modo texto así que seleccioné las distintas opciones iniciales como idioma, mapa del teclado moviéndonos con las teclas de cursor y a continuación seleccioné el modo en que usé Clonezilla entre las dos posibilidades:

- device-image Disco/Partición a/desde Imagen: guarda un disco duro o una partición de un disco duro en una imagen (archivo) o bien restaura una imagen desde un archivo a un disco duro físico.
- device-device Disco/Partición a Disco/Partición: realiza la imagen de disco duro físico a disco duro físico.

En este caso, para hacer una imagen del disco a un archivo selecciono "device-image Disco/Partición a/desde Imagen":



Opciones de como trabajar con imagen o disco en Clonzilla

Luego seleccioné que modalidad se utilizará para guardar la imagen que se generará del disco duro:

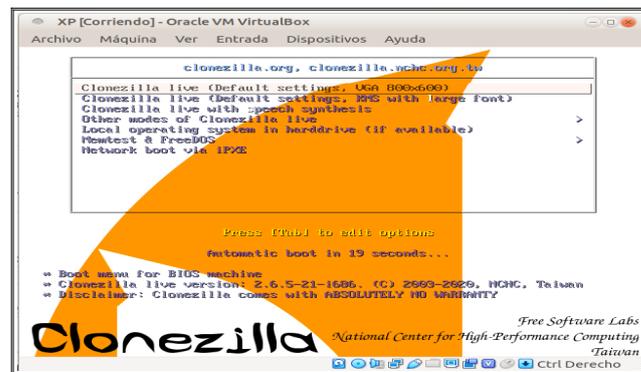
- local_dev
- ssh_server
- samba_server
- nfs_server

Entre las distintas posibilidades selecciono "local_dev", con la cual usará un dispositivo local como destino de la imagen del disco duro, en este caso particular utilicé un disco externo USB 3.0 Western Digital Elements de 1Tb de capacidad. Se selecciona el dispositivo de destino donde se guardará la imagen y después elegimos la carpeta. En este punto Clonezilla nos muestra todos los discos y todas las particiones del equipo, con el espacio total, el usado y el libre. Ahora aparece la opción de salvar el disco completo "savedisk" o una particion "saveparts", elijo "savedisk" y a continuación nos sugiere el nombre para la carpeta donde Clonezilla incluirá todos los ficheros de la imagen, con el formato "aaaa-mm-dd-01-img"(a para año, m para mes y d para día). Acción siguiente se selecciona el disco del que se realizará la imagen y como último paso elijo entre las tres opciones que nos presenta Clonezilla sobre como se comportará al finalizar la clonación, estas son "poweroff" (apagar el equipo), reboot (reiniciar el equipo) o "user choice" (decide el usuario), elegí que se espere la elección del usuario.

En este punto ya tenía la imagen del disco que contenía instalada la aplicación del problema, por lo que ahora había que hacer que bootee en la maquina virtual sobre VirtualBox. Continuando con la solución sobre este tema, instalé VirtualBox 6.0 sobre el Linux UBUNTU 18.04 y generé un maquina virtual para correr Windows XP 32bits, pero sobre ella no instalaría el Windows XP directamente, sino que restauraría la imagen generada con Clonezilla. Para ello hice arrancar la maquina virtual con el iso de Clonezilla 32bits, indicándole desde donde debía obtener esta iso para arrancar como se ve en la imagen:



Opción para que la maquina virtual arranque desde una imagen iso.



Maquina Virtual arrancando con Clonezilla.

Ahora se presentan las opciones básicas de Clonezilla para elegir idioma, tipo de teclado, etc, una vez seleccionadas elegimos trabajar con discos/imágenes o disco/disco, elegí la primera opción, luego seleccioné de donde obtendría la imagen:

- local_dev
- ssh_server
- samba_server
- nfs_server

Entre las distintas posibilidades seleccioné “local_dev”, ya que la imagen estaba almacenada en el disco externo USB 3.0 Western Digital Elements de 1Tb de capacidad. Seleccioné la carpeta donde reside la imagen, ahora pide la confirmación para proceder. Continuo y comienza a volcar la imagen sobre el disco de la máquina virtual y una vez terminado retiro la imagen iso del lector óptico virtual y la máquina arranco con el sistema que estaba funcionando sobre la PC.

Hasta ahora parecía que todo iba bien, pero cuando intentamos arrancar la segunda máquina virtual con la metodología utilizada, clonar con Clonezilla y restaurar en la maquina virtual, no arrancaba el sistema operativo huésped. Entonces investigando otras técnicas para lograrlo nos llevó a tener que realizarlo de otra forma. Para ello no utilizamos la herramienta Clonezilla, en lugar de ello utilizamos el comando “dd” de linux. Este comando “dd” (data duplicator) se usa para copiar y convertir datos. Es una utilidad muy poderosa que trabaja a bajo nivel con la cual se pueden realizar copias de seguridad, copiar particiones o discos completos, al que le indicamos donde está montado el disco particion o dispositivo del cual queremos relizar la imagen y la ruta del archivo donde guardar la imagen generada. En este caso lo utilizaría para generar una imagen iso del disco en cuestión, y luego convertiría esa imagen con formato iso a formato vdi, con el cual trabaja VirtualBox y arranque el sistema operativo huésped.

Con esta nueva técnica, entonces en una PC conecté el disco del cual se debía realizar la imagen y lancé el comando dd de la forma:

```
dd if=/dev/sdb of=imagenHD.iso
```

Sintaxis del comando:

- “if=” Ruta donde esta montada la unidad o partición de la que queremos hacer la imagen.
- “of=” Ruta donde vamos a grabar nuestro fichero de imagen ISO.

Cuando creamos una nueva máquina virtual en VirtualBox, el archivo de imagen asociado es VDI (.vdi). Una herramienta disponible con VirtualBox posibilita la conversión de una imagen ISO a VDI lo cual es un proceso de tomar la imagen .iso generada con el comando “dd” para luego convertirla en una imagen de disco virtual .vdi. Para realizar esta tarea ejecuté el siguiente comando desde la consola:

```
VBoxManage convertfromraw imagenHD.iso HD_Virtual_XP.vdi
```

terminado el proceso después de unos minutos, había que crear la máquina virtual desde VirtualBox, pero en lugar de crearla con disco nuevo había que indicarle que utilice un disco virtual existente, como se ve en la imagen:



Elección de un disco virtual existente al crear la maquina virtual en VirtualBox.

una vez terminado el proceso se inicio la maquina y arranco el sistema huésped. Con este proceso terminado ya estaban funcionando virtualizadas sobre VirtualBox las dos PC físicas de RRHH.

Migrando los servidores.

La otra parte de la migración consistía en dejar funcionando virtualizados todos los servicios en el servidor nuevo. Para llevarlo a cabo se presentaban dos situaciones totalmente diferentes, por un lado los servidores físicos y por otro los que estaban funcionando ya virtualizados. Ambas situaciones compartían la característica de estar corriendo sobre hardware PC. Pero estas dos situaciones requirieron distintas soluciones para llevarlos al entorno virtual sobre el servidor nuevo.

Servidores virtualizados.

Comenzando con lo que fue mas simple primero voy a describir los pasos que seguí para pasar los servidores que estaban virtualizados sobre el hardware PC i5. Básicamente el proceso fue apagar la máquina virtual, realizar el backup de la misma desde el PC i5, y luego restaurar este backup desde el servidor DELL. Los backups que estaban programados se realizaban sobre una carpeta NFS con un proceso configurado sobre el mismo PROXMOX, como mantuve este procedimiento de resguardo de las máquinas virtuales, monté esta carpeta NFS sobre el nuevo servidor DELL y se restauró desde este mismo recurso NFS. Paso siguiente se “encendió” la maquina virtual restaurada y se continuó brindando el servicio correspondiente. A este proceso lo consideré crítico debido a que estaba funcionando el servicio de NAS en el entorno virtual, entonces para evitar el corte del servicio en la jornada laboral durante el proceso de restauración, que duró cuatro horas aproximadamente, se realizó fuera del horario de trabajo. Terminado este proceso se continuó brindando los servicios desde el servidor DELL PowerEdge R540.

Servidores físicos.

Ahora quedaba migrar los servidores físicos que estaban funcionando y brindando servicios. Los pasos que seguí para realizarlo fueron:

1. Generar una imagen del disco rígido del servidor físico con la herramienta Clonezilla.
2. Copiar la imagen sobre un servidor NFS.
3. Crear una maquina virtual con las características del hardware físico a virtualizar (tamaño de disco, cantidad de memoria, núcleos del microprocesador).
4. Arrancar la máquina virtual con Clonezilla para leer la imagen desde el servidor NFS.
5. Clonar la imagen del disco físico sobre la maquina virtual creada.

Una vez realizados estos pasos, se arrancaban las maquinas virtuales desde el administrador del PROXMOX y quedaron funcionando brindando los servicios desde el entorno virtual. Una vez funcionando estas máquinas virtuales realicé una evaluación de la performance del servidor utilizando el monitor de recursos de las maquinas virtuales suministrado con el sistema de virtualización PROXMOX, y en alguno casos le asigné mas recursos, memoria y procesador.

En este punto todos los servidores estaban virtualizados y los servicios se brindaban desde el nuevo servidor DELL PowerEdge R540, por lo quedó concluida la etapa de migración.

6. Diseño de VLAN

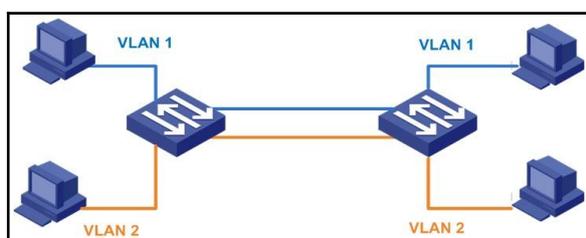
Introducción. Que es una VLAN.

Una LAN está compuesta por diversos dispositivos, como switches, impresoras, equipos y servidores, conectados entre sí en toda la extensión de los edificios de la repartición. Cuando un usuario de la LAN emite una solicitud o dato, todos los usuarios y dispositivos de la red lo reciben. A medida que aumenta el número de usuarios y dispositivos que pueden transmitir en un segmento de red, aumentan las posibilidades de que dos de ellos transmitan a la vez. Esta transmisión simultánea ocasiona una interferencia entre las señales de ambos que se conoce como colisión. Cuando se produce una colisión el paquete debe retransmitirse, por lo que conforme aumenta el número de colisiones disminuye el rendimiento de la red. Todo el espacio físico donde se producen las colisiones, y como consecuencia de ellas las retransmisiones, se conoce como dominio de colisión. La buena práctica en redes consiste en mantener los dominios de colisión pequeños, es decir, con la menor cantidad de dispositivos posible, ya que cuantos menos nodos compartan un espacio físico menor será la probabilidad de que transmitan a la vez y surja una colisión.

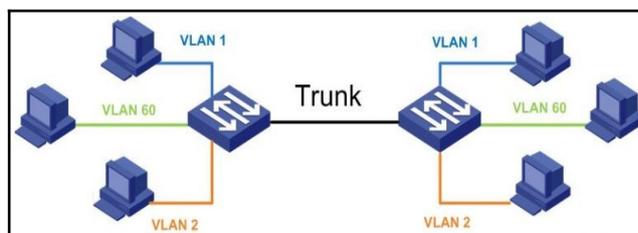
El rendimiento de la red es un factor crítico en la productividad de cualquier organización para realizar sus transmisiones en la forma adecuada. Las VLAN contribuyen a mejorar el rendimiento de la red dividiendo los grandes dominios de colisión en dominios más pequeños. De esta forma con dominios de colisión más pequeños se limita el número de dispositivos que participan en los broadcasts y permiten que los dispositivos se separen en agrupaciones funcionales (o VLANs), como por ejemplo una VLAN para servicios de base de datos para un departamento contable y otra VLAN para transferencia de datos a alta velocidad para un departamento de ingeniería. La división de las redes planas en múltiples grupos lógicos de trabajo (dominios de colisión) reduce el tráfico innecesario en la red y potencia el rendimiento. Una VLAN permite crear grupos de dispositivos conectados a la red de manera lógica que actúan como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN. A la VLAN se le puede asignar un nombre simbólico para describir la función principal de los usuarios de la misma y así se puede segmentar de manera lógica a las redes basadas en direcciones, funciones o departamentos según la necesidad. En resumen una VLAN es una subred IP separada de manera lógica.

Configuración de la VLAN.

Teniendo en cuenta las ventajas de este tipo de tecnología VLAN realicé un breve análisis de la situación y no dudé en implementarla en esta red. La implementación fue con VLAN basada en puerto. Esto quiere decir que se configura cada puerto del switch con una VLAN particular, cada uno de estos puertos se denominan “puerto de acceso”, esto significa que si dos dispositivos estén conectados físicamente a dos puertos del mismo switch pueden no comunicarse si pertenecen a diferentes VLANs. Además de los puertos de acceso, se necesita un puerto configurado en modo trunk, que permite conectar varias VLAN con otro switch a través de un único link o cable, ya que si no existiesen los puertos de trunk, necesitaríamos un cable para enviar el tráfico de cada una de las VLAN que tengamos hacia otro switch.



Implementacion de VLAN sin un puerto trunk.



Implementacion de VLAN con un puerto trunk.

Utilicé los primeros puertos del switch para conectar equipos a las VLAN y el último puerto, el 24 o 48 según el switch, para configurarlo como trunk para su interconexión.

Después de haber evaluado la situación y ubicación de las distintas direcciones, y teniendo en cuenta la cantidad de equipos funcionando en cada una de ellas, determiné que la cantidad adecuada sería de 4 VLANs, sectorizando así los edificios de la repartición asignando cada edificio a una VLAN diferente. Las direcciones están compuestas por varias oficinas o divisiones, y estas divisiones de cada dirección están ubicadas algunas en el mismo edificio y otras en edificios diferentes, por lo que pude configurar la pertenencia de cada dirección a cada VLAN sin problemas.

Para comenzar con esta etapa se configuraron los switches HPE OfficeConnect 1920S, que estaban con la configuración de fábrica. Comencé realizando la configuración inicial, que fue cambiar la contraseña del usuario *admin*, luego se le cambió el nombre del host y se le asignó una dirección IP, y también se configuró al switch para mantener automáticamente la fecha y hora con el servidor NTP de la provincia. También disponíamos de modelos más antiguos de switches HP 1920, a estos se les realizó la configuración inicial por consola, y luego se les actualizó el firmware a la última versión disponible.

El primero en configurarse fue el switch donde convergen todos los demás y mediante el cual se conecta la repartición a la RPD (Red Provincial de Datos), el nombre de host de este switch fue SWBORDE. El formato del nombre de host de los demás conectados a él fue SWDDD, siendo DDD la dirección en la cual estaba ubicado, y los restantes que conectaban las oficinas SWDDDOOO, donde SW hace referencia a que se trata de un switch, DDD a la dirección que pertenece y OOO a la oficina donde está ubicado. También configuré los switches para centralizar los archivos de registro en el servidor de syslog, que es una máquina virtual en el servidor PROXMOX. Generé dos usuarios con diferentes niveles de acceso a los switches, uno llamado informatica-admin con nivel de acceso management, no tiene ningún tipo de restricción, y otro llamado informatica-visor con nivel de acceso monitor, tienen acceso completo pero de solo lectura y permite el comando ping para pruebas de conectividad. Terminada la creación de los usuarios y los asocié al grupo que corresponde, se habilitó el acceso remoto ssh y acceso web, y en este punto comencé con la configuración de la VLAN propiamente dicha en los switch de las oficinas.

Entrando más en detalle de la configuración y a modo de describir los pasos llevados a cabo para configurar los switches, primero se definieron la VLAN y los ID fueron:

10 – VLAN10 (ADMINISTRACION)

20 – VLAN20

30 – VLAN30

40 – VLAN40

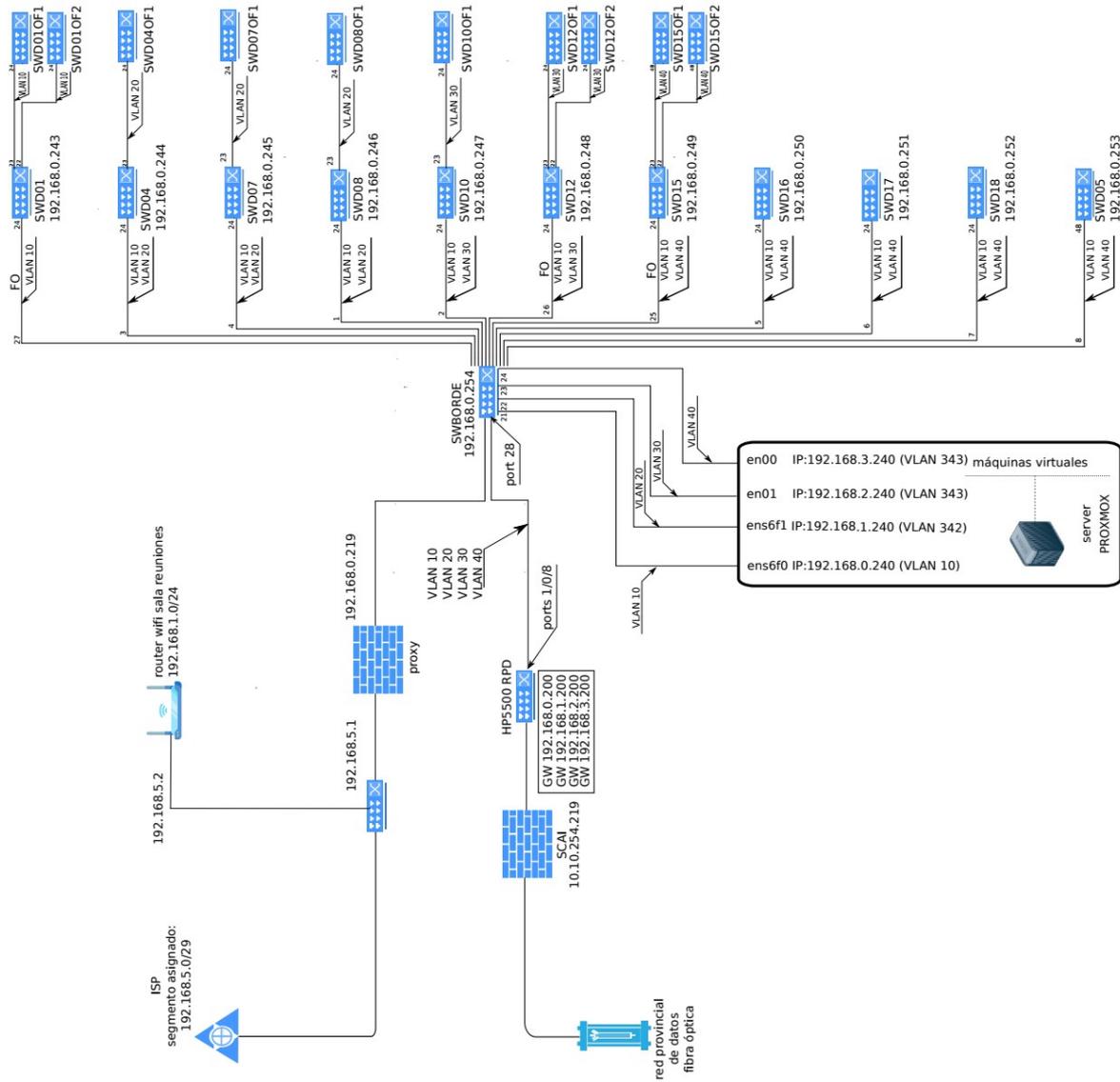
La VLAN10 se configuró en todos los switches para hacer posible poder llegar a todos ellos y poder administrarlos. Se adquirieron switches nuevos HP 1920, pero contábamos con algunos switches HP 1920 más viejos, lo que significaba que la forma de configurarlos era diferente, aunque el fin y el resultado final fuera el mismo. En estos switches más antiguos los puertos fueron configurados con tipo de enlace *“access”*, y los últimos puertos de cada switch, el 24 o el 48 según el caso, con tipo de enlace *“trunk”* para generar el enlace con el switch de borde. Con los switches nuevos fue diferente el procedimiento de configuración, ya que cambia la interface y el software. Los pasos de la configuración de estos switches se muestra con más detalle en el apéndice II.

Para habilitar el enrutamiento de las diferentes VLANs se recurrió a un switch de la red provincial que gestiona diferentes VLANs de varias reparticiones de la Provincia de Santa Fe. Esta operación se realizó de esta manera al no adquirirse el switch HP 5500 solicitado originalmente en la propuesta de reestructuración. El motivo por el cual no se incluyó en el pliego licitatorio fue porque ya estaba disponible en la infraestructura de la red provincial un switch HP 5500 con disponibilidad, capacidad de enrutamiento y manejo de paquetes acorde al tamaño de la red. Al pertenecer este dispositivo a la red provincial de datos no tenía acceso a la administración del mismo para realizar la configuración,

por lo que se pasaron los requerimientos de las VLAN al administrador de la red Provincial para que realizara la configuración necesaria del dispositivo.

Como todas la VLAN debían tener acceso a los servidores, la forma mas conveniente de implementarlo era que el servidor contara con una placa de red física para cada VLAN, y así evitar el cuello de botella que se generaría en el gateway para enrutar todas las peticiones que se dirigían al servidor. Una vez terminada esta configuración se cambiaron las máscaras de subred en las PC pertenecientes a cada VLAN y así quedó concluida esta etapa.

DIAGRAMA DE RED REPARTICION



7. Implementación

En esta etapa del proyecto ya contábamos con la infraestructura, por lo que existían los medios para que todo comience a funcionar. Esto significa no solo que los usuarios harían uso de las instalaciones y sus servicios, sino que también debían funcionar los sistemas de registro para detectar posibles fallas durante el funcionamiento o prácticas no permitidas, el sistema de copias de seguridad y el sistema de monitoreo de la red.

A continuación y entrando mas en detalle de cada sistema, realizo una descripción y explicación de ellos y la forma de como se implementaron.

Sistema de registro.

Una de las partes para proteger y dar robustez al sistema, es tener información de lo que sucede en el mismo, siendo la utilización de registros la forma mas práctica de lograrlo. Con los registros se puede diagnosticar problemas, determinar el estado del sistema y considerar que aplicaciones es necesario evaluar. Con la utilización de registros también se pueden detectar intrusos y el uso de aplicaciones o practicas prohibidas si se maneja de la forma correcta. Un mensaje de registro puede contener cualquier información, junto con la fecha y la hora del envío, por lo que es útil recolectar, registrar y analizar, por ejemplo:

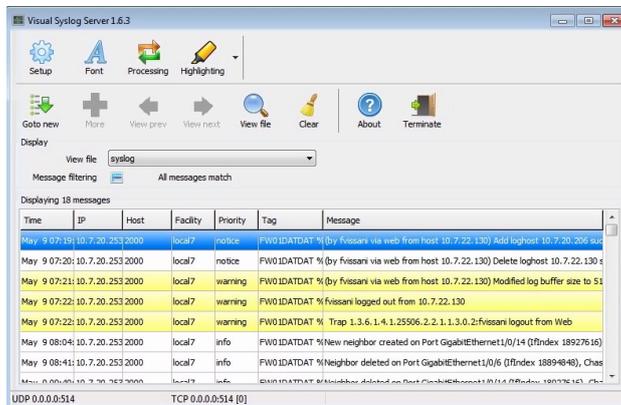
- Un intento de acceso con contraseña equivocada.
- Un acceso *correcto* al sistema.
- Anomalías: variaciones en el funcionamiento normal del sistema.
- Alertas cuando ocurre alguna condición especial.
- Información sobre las actividades de un sistema operativo.
- Errores de hardware o software.

También es posible registrar el funcionamiento normal de los programas; por ejemplo, guardar cada acceso que se hace a un servidor, aunque esto suele estar separado del resto de alertas.

Al tener que implementar esta tarea decidí llevarla a cabo con el protocolo syslog debido a que es muy sencillo, consiste en un ordenador ejecutando el servidor de syslog donde el cliente envía un pequeño mensaje de texto para el registro. Los mensajes de syslog se suelen enviar vía UDP por el puerto 514 en formato de texto plano. Para implementar este protocolo utilicé Visual Syslog Server, que permite usar TCP en vez de UDP, mejorando la seguridad. La sencillez de syslog ha hecho que muchos dispositivos lo implementen, tanto para enviar como para recibir mensajes, haciendo posible integrar mensajes de varios tipos de sistemas en un solo repositorio central. Configuré una rotación del archivo de una semana, lo que significa que se mantienen los registros por una semana. El mensaje enviado se compone de tres campos:

- Prioridad: es un número de 8 bits que indica tanto el *recurso* (tipo de aparato que ha generado el mensaje) como la *severidad* (importancia del mensaje), números de 5 y 3 bits respectivamente. Los códigos de recurso y severidad los decide libremente la aplicación, pero se suele seguir una convención para que clientes y servidores se entiendan.
- Cabecera: indica tanto el *tiempo* como el *nombre* del ordenador que emite el mensaje. Esto se escribe en codificación ASCII (7 bits), por tanto es texto legible. El primer campo, *tiempo*, se escribe en formato Mmm dd hh:mm:ss, donde *Mmm* son las iniciales del nombre del mes en inglés, *dd*, es el día del mes, y el resto es la hora. No se indica el año. Justo después viene el *nombre* de ordenador (hostname), o la IP si no se conoce el nombre. No puede contener espacios, ya que este campo acaba cuando se encuentra el siguiente espacio.
- Texto: Lo que queda de paquete *syslog* al llenar la *prioridad* y la *cabecera* es el propio texto del mensaje. Éste incluirá información sobre el proceso que ha generado el aviso, normalmente al principio (en los primeros 32 caracteres) y acabado por un carácter no alfanumérico (como un espacio, ":" o "/"). Después, viene el contenido real del mensaje, sin ningún carácter especial para marcar el final.

Entre todos no han de sumar más de 1024 bytes, pero no hay longitud mínima.



Captura de Visual syslog

Backup

Una copia de seguridad o *backup* en inglés es una copia de los datos originales que se realiza con el fin de disponer de los mismo en caso de su pérdida. Esta pérdida puede suceder ante distintos eventos o usos, como una catástrofe informática natural; un ciberataque; archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus u otras causas.

El proceso de copia de seguridad se complementa con otro conocido como *restauración* de los datos, que es la acción de leer desde el medio donde se guarda el backup y grabar en la ubicación original u otra alternativa los datos requeridos. La organización del espacio de almacenamiento y la administración del proceso de efectuar la copia de seguridad son tareas complicadas. Después de evaluar varias alternativas, me decidí por **Bacula**, que es una colección de herramientas capaz de cubrir las necesidades de respaldo de equipos en una red, corre sobre Linux, permite la administración mediante una interface web y el código fuente se publica bajo la Licencia 3 de la Licencia Pública General de Affero GNU. Está basado en una arquitectura Cliente-Servidor que resulta eficaz para realizar las tareas dada la amplia gama de funciones y características que posee.

Lo primero que hay que entender de este programa es su diversificación: está dividido en varias partes que se interrelacionan entre ellas. Estas partes pueden estar instaladas en diferentes máquinas o en la misma, dando la opción de guardar los backups en una máquina diferente a la que los gestiona. Existen 3 partes principales: el Director, el Storage y el File. El File es la máquina cliente (la que necesita que se le hagan copias), el Storage es la máquina que guarda dichas copias y el Director es la máquina que administra todo el proceso. También se pueden configurar, por supuesto varias máquinas cliente (File), varias Storage lo que permite separar las copias en varios destinos y se pueden tener varios Director, aunque en este caso se configuró uno solo. Otra característica a mencionar es que el funcionamiento de Bacula se basa en un catálogo, esto quiere decir una base de datos que podemos elegir entre MySQL, SQLite y PostgreSQL, donde quedan registrados todos los eventos, volúmenes, clientes, etc. En este caso elegí PostgreSQL debido a que ya se están realizando algunas actividades con esta base de datos en la repartición. Bacula admite reutilización/reciclado de los volúmenes, esto quiere decir que permite decidir cuantas copias mantener almacenadas. Por ejemplo si se quiere tener solo un Full Backup mensual, pero se realiza uno cada semana, se puede configurar Bacula para que sobrescriba el Volumen que anteriormente contenía esa copia, y así se evita llenar el disco innecesariamente, y se evita la tarea de tener que borrar los datos viejos a mano. Bacula nos permite 3 niveles diferentes de copias de seguridad Full, Diferencial e Incremental. El Full backup es la copia clásica, se copian todos los datos independientemente de si fueron o no modificados. El Diferencial sólo copia los archivos que hayan cambiado o se generaron nuevos desde el último Full. Y con las copias Incremental pasa lo mismo pero un nivel por debajo, sólo

compara los cambios desde el último Diferencial, o desde el último Full si éste es más reciente. Esto es muy cómodo si se quiere mantener un equilibrio entre optimización de recursos y utilidad de los mismos. Con esto podemos conseguir archivos de diferentes fechas sin necesidad de ocupar mucho espacio. Es muy útil cuando surgen problemas generados por un error del usuario y se necesita el backup específico de un día.

Ahora que esta definido con que se realizan las copias de seguridad, paso a detallar que es lo que se copia. Siendo lo mas dinámico el NAS, fue lo primero que configuré. Antes de configurar el servidor Bacula, tenia programada una copia full del NAS desde el PROXMOX que se realizaba todos los viernes y sincronizaba todos los dias a ultima hora todos los datos de las carpetas compartidas del NAS con otra PC ubicada en la oficina de informática. En este periodo pude hacer una una evaluación de la dinámica de trabajo de los usuarios en la repartición y verifiqué que se daban problemas debidos a errores de los usuarios, por lo que necesitaban recuperar los archivos diarios. Por ello configuré todo el sistema de backup para realizar una copia Full de las carpetas todo los viernes a las 21:00hs, manteniendo dos copias, y una copia incremental todos los días manteniendo también dos copias de las mismas.

Al Director lo instale sobre una máquina virtual en el datacenter, y al storage sobre una PC física ubicada en el otro extremo del predio, a aproximadamente 200m del datacenter. Además los datos del storage se copian los días lunes sobre dos discos externos que se van alternando y se guardan en una caja de seguridad.

Sala de capacitación

A la sala de capacitación la consideré como una parte vital dentro de la repartición para mejorar las habilidades y conocimientos del personal. Este espacio tenía que contar con todo lo necesario para realizar cursos, seminarios, talleres, charlas o videoconferencias que se dicten en ella y pueda aprovecharse de la mejor forma. Para el buen uso de esta sala, es importante contar con una buena organización que comienza con el correcto equipamiento del mobiliario como sillas y mesas, sistemas de audio, micrófono, iluminación, red de datos, etc.

Para conformar esta sala se acondicionó un lugar que se utilizaba como archivo y depósito de materiales en desuso. Una vez confirmado que este lugar se utilizaría como sala de capacitación se comenzaron a realizar los trabajos de reacondicionamiento del lugar. Lo primero fue el reemplazo de una pared por un panel vidriado, luego se realizaron trabajos de pintura, cableado de electricidad y datos por personal electricista de la repartición. Se colocaron los muebles en su lugar y se instalaron las cuatro PC all in one y un proyector que se adquirieron para este fin.



Vista de la sala de capacitación

Conclusión

Finalmente, el objetivo de este proyecto está cumplido, detallado en este documento se describieron los fabulosos cambios realizados a la red LAN de las oficinas centrales, abarcando tanto la parte física y lógica de la red. Pero estos cambios no solo llegaron al cableado de la red, a su configuración y a los servicios anexados, sino también a quienes la utilizaban, o sea a los usuarios que diariamente utilizan los servicios que esta brinda. Esto es realmente muy gratificante debido a que al realizarse la parte técnica de la forma correcta y aplicando criterios y conceptos adquiridos en la carrera académica y luego reafirmados con la practica laboral, se llega a mejorar la forma de trabajar de muchas personas, que al comenzar este proyecto veían los cambios que se avecinaban de una forma nada amigable, hasta amenazantes en algunos casos, y al terminarlo están sumamente agradecidos por la forma en que cambio su labor diaria.

La forma en que se logró que esta repartición pública, que estaba funcionando de manera deficiente desde el punto de vista técnico, (una red de datos anárquica desde el punto de vista lógico, usuarios reacios a insertarse a la tecnología de la comunicación digital y sin ningún servicio digital), se inserte en la realidad tecnológica y logre funcionar con una red de datos trabajando correctamente y brindando soluciones a problemas muy difíciles de solucionar sin recurrir a la tecnología digital, fue mediante la aplicación de distintos pasos que fueron realizándose de manera sincronizada y organizada. Estos se realizaron de manera que la red nunca dejó de funcionar para aplicar los cambios, los que consistieron, a grandes rasgos, en el recableado de la red, la reorganización de los gabinetes de las oficinas, se creó un datacenter, se virtualizaron los servidores, se vincularon con fibra óptica los diferentes edificios separados dentro del predio de la repartición, se regularizaron todos sistemas operativos de los equipos PC, se habilitaron todos los servicios necesarios para el correcto desvolvimiento de la repartición, y además se capacitó a los usuarios, logrando el resultado mas buscado, que es que los usuarios trabajen con buena predisposición utilizando la red de datos como una herramienta con la que cuentan para lograr mejores resultados.

La ejecución de este proyecto permitió modernizar a una repartición pública muy atrasada en términos de tecnología de la información; que pasó de realizar todos los trámites y movimientos en papel, a brindar a la sociedad y a todos los empleados de la misma un servicio digital. Como punto importante, destaco que siempre consideré a los usuarios como parte del proyecto, ya que son los que interactúan con la red constantemente, y considero que si no hubiese logrado esta interacción el proyecto hubiese resultado a mi parecer un fracaso. Desde el punto de vista de la comunidad se reemplazaron varios servicios presenciales por servicios que se realizan mediante la web, y los que siguen realizándose en forma presencial se resuelven en menor tiempo. Los empleados de la repartición también se vieron beneficiados , lo que significó no solo una mejor predisposición de estos hacia la nueva forma de trabajo, sino que además comenzaron a generar inquietudes y/o propuestas sobre como solucionar algunos problemas de funcionamiento de su labor diaria, los que se fueron solucionando gracias a contar con una red que siempre de respuesta.

Particularmente, la experiencia lograda con este proyecto fue muy reconfortante, tanto de la parte técnica como de la relación con pares y distintas personas relacionadas con el mismo.

APENDICES

Apéndice I – Fichas Técnicas.

Ficha Técnica: Caja de empalme e interconexión

Ref: FTCAEMP

CARACTERÍSTICAS TÉCNICAS
•Marca
•Modelo
•Caja de empalme e interconexión para fibras ópticas, cerrado, con guías deslizantes (o pivotante) para montaje en gabinete de 19” normalizado.
•Deberá permitir la entrada y fijación de los cables de fibra óptica exteriores.
•Deberá disponer de un Panel frontal con la capacidad necesaria para alojar 24 acopladores SC .
•Deberá disponer de guías, cassettes organizadores de cables, sujeciones y accesorios necesarios para organizar correctamente todas las fibras y empalmes en su interior, manteniendo en todo momento el radio de curvatura mínimo admisible.
•Deberá permitir además la fácil extracción del panel (sistema de guías deslizantes o pivotantes) sin dañar ni forzar el cable de entrada para la supervisión visual o realización de futuros empalmes.
•Deberá proveer los pigtails necesarios para realizar la conectorización de todos los pelos de fibra solicitados en cada rack.
•La garantía será de 5 años para los conectores y hardware de conexión (pasivo), contra defectos del material y manufactura.

Ficha Técnica: Gabinete de Distribución

Ref: FTGAB12U

REQUERIMIENTOS

4

·Se debe especificar claramente la marca y modelo.
•Será cerrado, contará con una puerta frontal de vidrio transparente ahumado u otro material semejante y tendrá una cerradura de seguridad para que sólo personal autorizado tenga acceso.
•En su interior contendrán racks metálicos normalizados de 19” de tipo profesional, estructura principal de chapa de acero de 1,5 mm de espesor mínimo y profundidad de al menos 450 mm.
•La terminación superficial de las partes metálicas será esmalte horneado texturado. El modelo del gabinete a utilizar por la contratista deberá contar con la aprobación del comitente en forma previa a su instalación.
•Tendrá al menos una capacidad de 12 unidades y 450 mm de profundidad.
•Dos paneles de interconexión (‘patch panel’) para cableado UTP con 24 receptáculos . Los conectores serán modulares de 8 posiciones (RJ-45). Tanto el panel como los conectores de datos deberán estar garantizados para funcionamiento en Categoría 6. Los pares provenientes de los puestos de trabajo terminarán en regletas terminales con conexiones sin soldadura (IDC).
•Dos organizadores de cables horizontales metálicos
• 4 tomacorrientes de 220 Vca.
La garantía será de 5 años para los conectores y hardware de conexión (pasivo), contra defectos del material y manufactura, como así también su instalación.

Ficha Técnica: Switch GigaEthernet Administrable.

REF: SWETH24

CARACTERÍSTICAS TÉCNICAS

•. Especificar Marca y modelo
•. Compatibilidad con Protocolos: ETHERNET Standard IEEE 802.3 CSMA/CD IEEE 802.3u ISO 8802-3 IEEE 802.3i - 10Base-T IEEE 802.3ab IEEE 802.3z
•. Capacidad de al menos 24 puertos 10/100/1000Mbps 'autosensing' según normas 802.3i, 802.3u y 802.3z (10BaseT, 100 BaseTx y 1000BaseTx) y 2 bahías SFP para módulos SFP.
•. Manejo de al menos 8000 direcciones MAC
•. Todos los puertos deberán soportar operación en half o full duplex con autonegociación
•. Información de configuración almacenable en memoria no volátil
•. Control tráfico broadcast y multicast
•. Soporte de Vlans según Norma 802.1Q
•. Soporte de Priorización de tráfico según Norma 802.1P
•. Soporte de "full-wire-speed forwarding" sobre todos los puertos
•. Soporte Spanning-Tree (IEEE-802.1d)
•. capacidad de conmutación/encaminamiento de al menos 50 Gbps
•. Administración: Soporte SNMP MIB 2 Administración remota mediante Web
•. Montable en rack de 19". Deberá incluir todo el 'kit' de montaje. Su profundidad no deberá exceder los 300 mm.
•. Características eléctricas: 220 Vca +/- 10 % 50 Hz +/- 3 %
•. Manuales de administración y configuración del mismo
•. Características ambientales: Temperatura de operación: 0 - 40 grados C Humedad relativa: 0 - 80 % no condensado
•. Garantía: 36 meses o la que indique el fabricante (se tomará en cuenta la que sea mayor)

Ficha Técnica: Cable Óptico de 12 fibras Monomodo - Aerea Ref: FTFO12MM

CARACTERISTICAS TECNICAS

• Marca : Furukawa o similar calidad
• Código de fabricante o modelo
• 12 Fibras Monomodo G.752D
• Apta para tendido exterior (outdoor) y usos en tendidos aéreos
• Autosoportada para vanos de hasta 80 metros
• Totalmente dieléctrico
• Elemento de material dieléctrico ubicado en el centro del núcleo para prevenir los esfuerzos de contracción del cable.
• Estructura general del cable con características de tubo holgado (Losse Tube) con protección contra la penetración de la humedad mediante gel.
• Elemento de tracción tipo aramida
• Cubierta externa de Polietileno de media densidad resistente a la luz solar e intemperie.
• Diámetro nominal núcleo 9 um y 125 um de corona
• Parámetros de performance según Norma ITU-T G.652D Longitud onda (nm) Atenuación máxima (dB/km) 1310 < 0.35 1550 < 0.20
• El cable deberá tener impreso en la cubierta externa del cable los datos del fabricante características de la FO y metraje.
• Garantía: 10 años

Nota 1: Las características y requisitos de las fibras ópticas que no estén expresadas en esta ficha técnica deberán ajustarse a la Norma ITU-T G.652D

Ficha Técnica: Switch GigEthernet Administrable.

REF: SWETH24

CARACTERÍSTICAS TÉCNICAS

•. Especificar Marca y modelo
•. Compatibilidad con Protocolos: ETHERNET Standard IEEE 802.3 CSMA/CD IEEE 802.3u ISO 8802-3 IEEE 802.3i - 10Base-T IEEE 802.3ab IEEE 802.3z
•. Capacidad de al menos 24 puertos 10/100/1000Mbps 'autosensing' según normas 802.3i, 802.3u y 802.3z (10BaseT, 100 BaseTx y 1000BaseTx) y 2 bahías SFP para módulos SFP.
•. Manejo de al menos 8000 direcciones MAC
•. Todos los puertos deberán soportar operación en half o full duplex con autonegociación
•. Información de configuración almacenable en memoria no volátil
•. Control tráfico broadcast y multicast
•. Soporte de Vlans según Norma 802.1Q
•. Soporte de Priorización de tráfico según Norma 802.1P
•. Soporte de “full-wire-speed forwarding” sobre todos los puertos
•. Soporte Spanning-Tree (IEEE-802.1d)
•. capacidad de conmutación/encaminamiento de al menos 50 Gbps
•. Administración: Soporte SNMP MIB 2 Administración remota mediante Web
•. Montable en rack de 19”. Deberá incluir todo el ‘kit’ de montaje. Su profundidad no deberá exceder los 300 mm.
•. Características eléctricas: 220 Vca +/- 10 % 50 Hz +/- 3 %
•. Manuales de administración y configuración del mismo
•. Características ambientales: Temperatura de operación: 0 - 40 grados C Humedad relativa: 0 - 80 % no condensado
•. Garantía: 36 meses o la que indique el fabricante (se tomará en cuenta la que sea mayor)

Ficha Técnica: Servidor para Virtualizacion Ref: FT-SRV-V

CARACTERISTICAS TECNICAS

Marca y Modelo	a) Se deberá especificar la Marca y el Modelo del equipamiento ofrecido.
Procesador	a) 2(dos) procesadores Intel Xeon Silver de 2.2 GHz y 10 núcleos como mínimo.
Memoria	a) 128 Gb de RAM DDR4 2400MHz ECC.
Dispositivo de almacenamiento	a) 3 (tres) discos de tecnología NL-SAS de 7.2 Krpm, hot plug, de 4Tb como mínimo. El equipo deberá permitir adicionar en el futuro al menos 2 (dos) discos de similares características a los solicitados. b) Controladora de manejo de arreglos de discos, que soporte configuraciones de RAID 0,1,5. Soporte de protocolo SAS y cache de 1Gb como mínimo.
Puertos	a) 4 (cuatro) puertos USB 2.0 b) 1 puerto para salida de video analógica VGA.
Interfaz de red	a) 4 (cuatro) adaptadores de LAN ethernet, distribuidos como mínimo en dos placas físicas independientes. b) Deberán ser recomendadas por el fabricante del equipo como componente del modelo ofertado (condición que se verificara con los folletos originales del mismo) y cumplir con las siguientes características: <ul style="list-style-type: none"> • Velocidad 10/100/1000 Mbps con interfaz RJ45. • Compatibilidad con protocolos ethernet standard. • Device driver asociados para el entorno operativo del equipo. • Operación Half y Full Duplex. • Software de diagnostico que permita verificar el funcionamiento y configuración de la placa. c) Se admitirá la entrega de adaptadores de red que no formen parte original del modelo de equipo, siempre que cumplan adicionalmente con la capacidad de procesamiento de paquetes en paralelo.
Kit adaptador de raqueo	a) El equipo debera ser raqueable. Debera proveerse el kit de raqueo correspondiente para la instalacion del equipo en un gabinete standard de 19”.
Fuente de energía y ventiladores	a) El eqiopo debera contar con fuente de alimentacion y ventiladores redundantes hot-swap.
Compatibilidad de sistemas	a) El equipo debe soportar en su totalidad los ambientes operativos MS-WINDOWS 2016 Standard Edition, LINUX SUSE ENTERPRISE 11.X, Vmware ESX/ESXi v 6.x.
Controladores de dispositivos y manuales	a) En caso que fuera necesario se deberán proveer los controladores necesarios para los sistemas operativos mencionados. b) Se deberá proveer el software de configuración en caso que fuera necesario. c) Se deberá proveer toda la documentación de los equipos (guía de usuario, manuales técnicos, etc) necesaria para la utilización mas eficiente y máximo aprovechamiento de los mismos. d) Los controladores y manuales se podrán ofrecer en medio óptico

	mediante descarga de Internet. En este último caso, la descarga deben mantenerse disponible al menos durante el período de garantía.
Garantía y servicio de post venta	a) El equipamiento deberá contar con garantía y servicio de posventa por al menos 36 meses, provisto por el fabricante, en todos sus componentes, a partir de la Fecha de Aceptación Definitiva brindada por la Provincia. b) El equipo deberá ser comercializado por el proveedor en el rubro de servidores.

Ficha Técnica: Gabinete Rack de 40U

Ref: FTRACK40U

CARACTERISTICAS TECNICAS

<p>Marca y Modelo</p>	<p>a) Se deberá especificar la Marca y el Modelo del equipamiento ofrecido.</p>
<p>Características generales</p>	<p>a) Será cerrado, contará con puerta delantera y trasera de metal microperforado (o material semejante), panel superior e inferior y ambos paneles laterales. Las puertas y los paneles laterales deberán contar con dispositivos para fácil apertura de las puertas, con cerradura y llaves, para que sólo personal autorizado pueda abrirlas o removerlas. b) Tendrá una capacidad al menos 40 unidades de rack de altura, y 42 como máximo. Deberá ser apto para servidores, equipamiento de comunicaciones y dispositivos de almacenamiento. Deberán estar indicadas las medidas de unidad de rack en todos los niveles verticales. c) En su interior contendrán racks metálicos normalizados de 19" con orificios cuadrados de 318"x3/8", estructura principal de chapa de acero de 1,5 mm de espesor mínimo y profundidad útil de al menos 750 mm. d) Deberá contener rieles horizontales necesarios para permitir la regulación en profundidad de los rieles verticales. e) La distancia entre los rieles traseros y la puerta trasera deberá ser la suficiente para permitir la instalación de patcheras de cobre y fibra óptica, anillas ordenadoras horizontales y verticales y unidades de distribución de energía (PDU) con la puerta cerrada. f) El acabado será en pintura color negro mate y aislante, tanto el gabinete principal como para los estantes solicitados en el item 3. g) Deberá contar con tornillos de nivelación, y soportar al menos 550 Kg.</p>
<p>Accesorios</p>	<p>a) Deberá contar con 2 anillas organizadoras de cable verticales y 2 anillas ordenadoras de cable horizontales de 1U (unidad). b) Deberá contar con un estante extraíble porta teclado con sujeción frontal y posterior, regulable en profundidad. c) Deberá contar con 1 estante ventilado de al menos 750 mm de profundidad, con sujeción frontal y posterior. d) Deberá contar con 2 unidades de distribución de energía (PDU) totalizando: al menos 20 tomas IRAM 2071 de 10A distribuidos en forma equitativa entre los canales y con llave térmica correspondiente. e) Se deberán incluir al menos 90 conjuntos tornillo-tuerca para los bastidores de 19".</p>
<p>Servicio de postventa</p>	<p>a) El equipamiento deberá contar con garantía y servicio de posventa por servicio de al menos 12 meses, provisto por el fabricante, en todos sus componentes, a partir de la Fecha de Aceptación Definitiva brindada por la Provincia.</p>

Ficha Técnica: UPS 2KVA

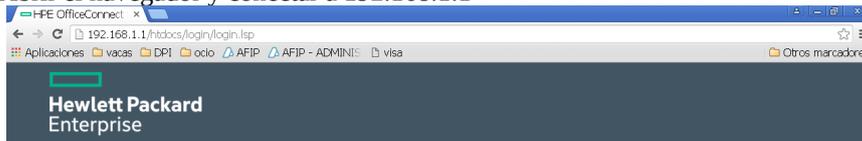
Ref: FTUPS2KVA

CARACTERISTICAS TECNICAS

• Especificar Marca y modelo
• Tipo de Operación ON LINE- doble conversión
• Potencia nominal 2 [kVA]
• Configuración Rackeable.
ENTRADA
• Voltaje 220 [Vi — Fase + Néutro + Tierra
• Rango 180 [VI a 280 [VI línea-neutro
• Frecuencia 50 [Hz] +1- 3 [Hz]
SALIDA
• Voltaje 220 [V] +1- 10%
• Frecuencia 50 [Hz] +/- 1[Hz]
• Factor de potencia 0.7 (mínimo)
• Forma de onda Sinusoidal o cuasi sinusoidal (simulada)
BATERIA
• Tipo Libre mantenimiento de electrolito absorbido con capacidad acorde a la autonomía solicitada.
• Autonomía 5 [minutos] al 80% de la carga
MONITORIZACION
• Display LED Para indicación rápida de estados de la UPS, operación con línea externa, operación con batería.
INTERFACE
• Puerto de comunicación RS232 con software de monitoreo y control compatible con SO Windows y Linux que permita apagado y encendido programable de los sistemas conectados. Slot SNMP.
CONEXIONADO DE SALIDA DE INVERSOR
• a) En caso de tomas de corriente, cantidad mínima 4 (cuatro) bajo Norma RAM 2071, en su defecto bajo Norma IEC 320 C13 (u otra), se proveerá la siguiente configuración: Un (1) cable doble aislación normalizado 3 x 1 mm2 de sección mínima por 1,5 mts. de longitud minima, con clavija IEC 320 C14 (u otra) en un extremo y en el otro una (1) base de tomas múltiples de mínimo cuatro (4) módulos bajo norma RAM 2071-
• b) En caso de borneras proveer misma configuración sin provisión de clavija.-
PROTECCIONES MINIMAS
• Detección de baja tensión: 180 [V]
• Detección de alta tensión: 240 [V]
• Estabilizador y filtro de línea incorporado
• Sobrecargas
• Transitorios y sobretensiones de la línea de entrada
CONDICIONES AMBIENTALES
• Temperatura 0°C — 40°C
• Humedad máx. 90%
GARANTIA
• 12 meses

Apéndice II – Configuración de VLAN en un switch HP 1920.

- 1) Configurar una PC con una dirección de red 192.168.1.222 mask 255.255.255.0
- 2) Conectar la PC al port 1 del switch HP 1920
- 3) Abrir el navegador y conectar a 192.168.1.1



HPE OfficeConnect Switch
1920S 24G 2SFP
JL381A

Username
Password

Log In

[Support](#)

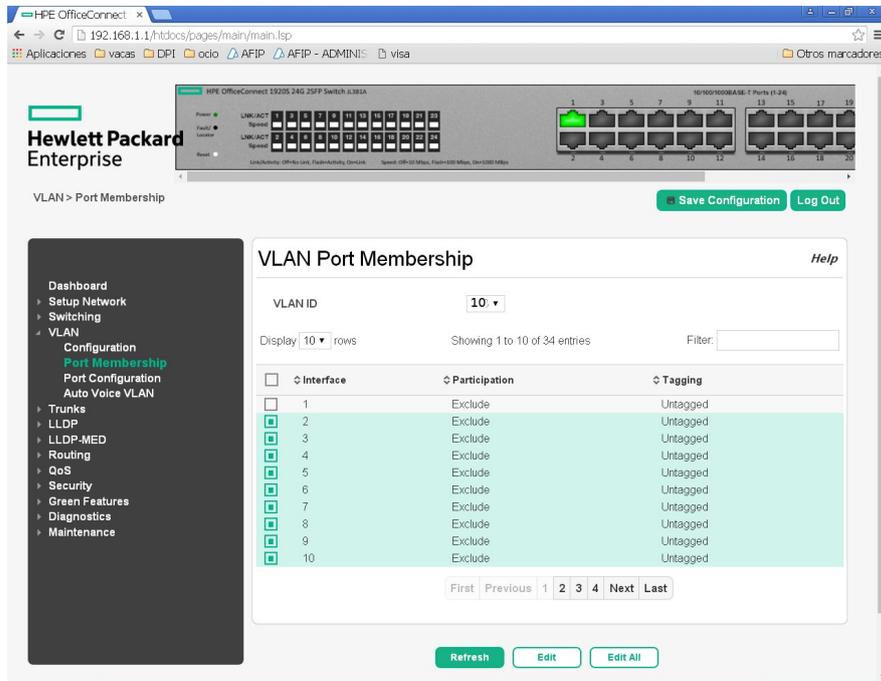
Copyright © 2010-2017 Hewlett Packard Enterprise
Development LP.

- 4) Ingresar con User y password
- 5) Ir a VLAN --->Configuration

Interface	Participation	Tagging
1	Exclude	Untagged
2	Exclude	Untagged
3	Exclude	Untagged
4	Exclude	Untagged
5	Exclude	Untagged
6	Exclude	Untagged
7	Exclude	Untagged
8	Exclude	Untagged
9	Exclude	Untagged
10	Exclude	Untagged

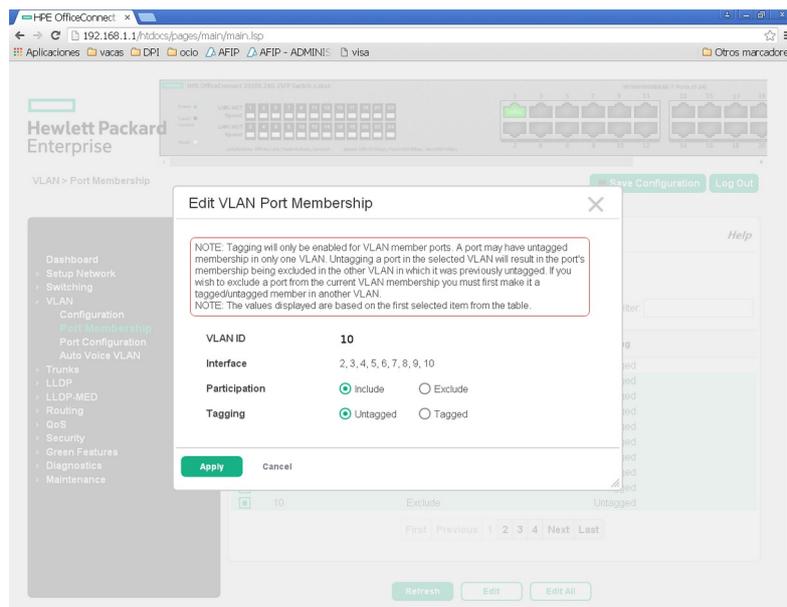
- 6) Presionar el botón ADD y en la siguiente ventana ingresar VLAN 10 y presionar APPLY

7) Ir a VLAN ---> Port Membership y en VLAN ID seleccionar 10

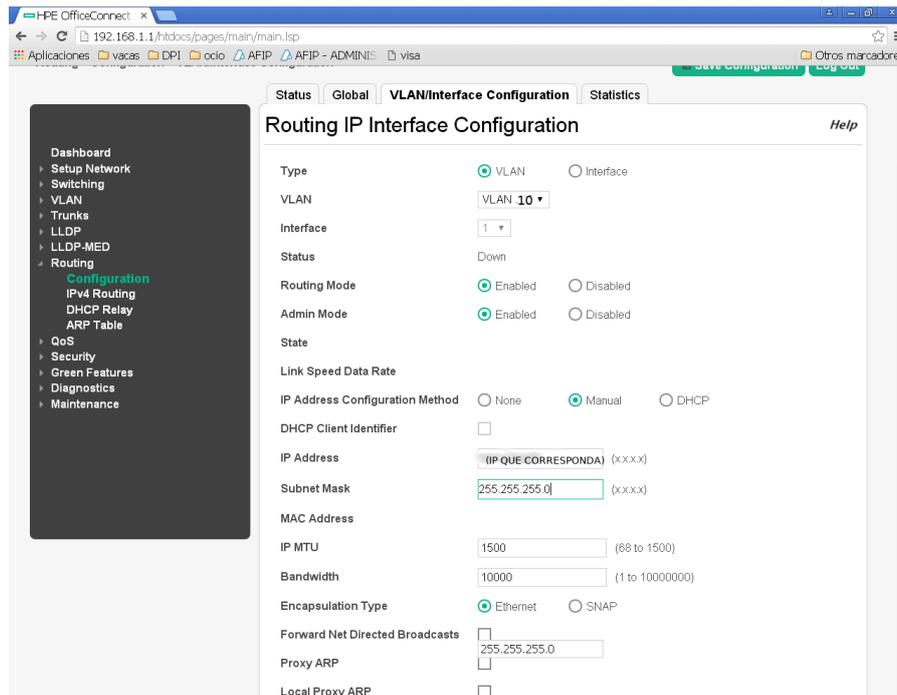


8) Marcar todos los puertos menos el 1 (del 2 al 10) y presionar EDIT

9) En la siguiente pantalla seleccionar todos los puertos como INCLUDE y UNTAGG y presionar APPLY



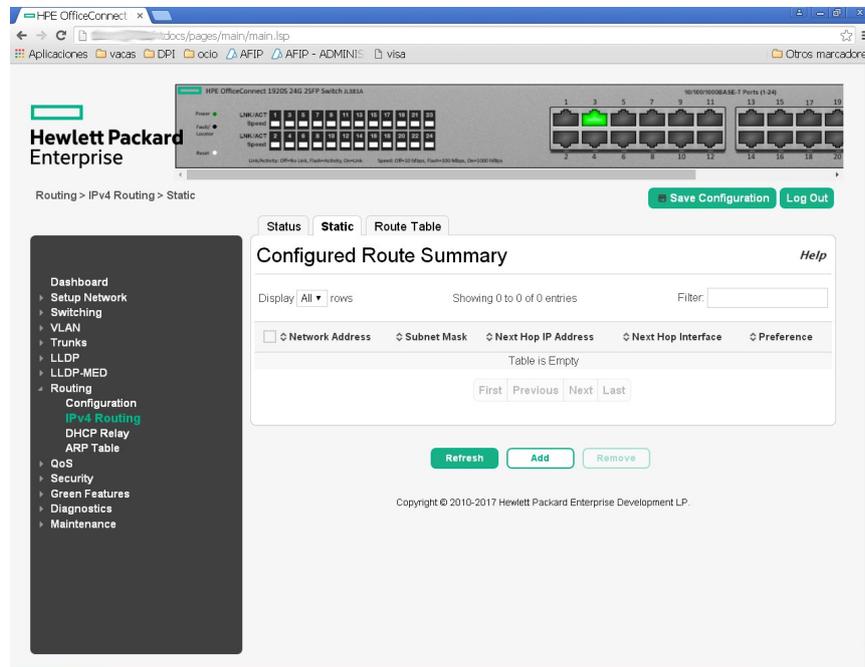
- 10) Ir a las páginas 2 y 3 para seguir seleccionando los puertos hasta el 26 y configurarlos para la VLAN 10 como INCLUDE y UNTAGG
- 11) Ir a Routing ---> Configuration ---> solapa VLAN/Interface Configuration
- 12) Seleccionar VLAN 10 y configurar como indica la siguiente figura



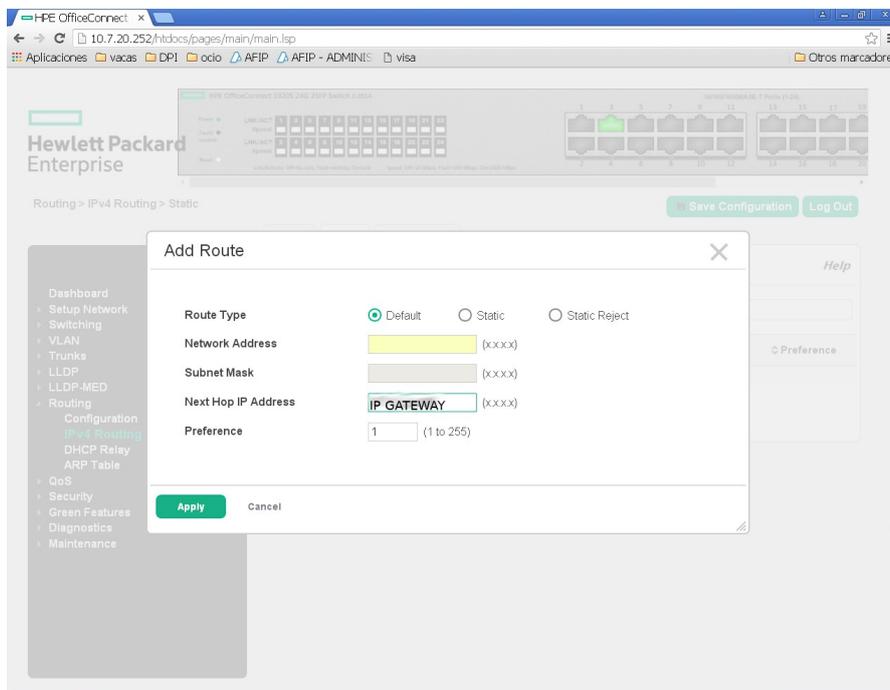
Routing mode enable
Admin mode enable
Ip Address configuration manual
IP Address (LA IP QUE CORRESPONDA)
Subnet mask (LA QUE CORRESPONDA)
Ir al pie de página y presionar APPLY

- 13) Cambiar la configuración de la placa de red IP: (LA IP QUE CORRESPONDA) MASK (LA QUE CORRESPONDA)
- 14) Cambiar el cable de red al puerto 2
- 15) Con el navegador conectarse al switch apuntando ahora a (LA IP CONFIGURADA)
- 16) Ir a VLAN --->Configuration, seleccionar VLAN 10, marcar el port1 y definirlo como INCLUDE y UNTAGG

17) Ir a Routing \leftarrow IPv4 Routing y presionar ADD



19) Configurar la ruta default al gateway correspondiente y presionar APPLY



20) En la parte superior de la pantalla (debajo de la imagen del switch) presionar el botón Save Configuration

Bibliografía

[Cableado estructurado - De Wikipedia la enciclopedia libre](#)
[OpenMediaVault -De Wikipedia, la enciclopedia libre](#)
[OpenMediaVault - The open network attached storage solution](#)
[Proxmox complete open-source platform for enterprise virtualization.](#)
[Conceptos basicos de puesta a tierra](#)
[Serie de conmutadores HPE OfficeConnect 1920S](#)
[Conmutadores HPE OfficeConnect de la serie 1950](#)
[Micropyme - Virtualizacion de servidores](#)
<https://sites.google.com/site/isaacivantorresgonzalezvlan/hp.com>