Fundamentos de Redes de Computadoras

Diseño de la Red para Servicio de Mapas de Tráfico en Tiempo Real

Francisco Iván San Segundo Álvarez
Adrián Fernández Delgado
Daniel Garcia Salinas

16 de diciembre de 2024

Índice

Índice de figuras

Índice de tablas

Resumen

Este documento pretende servir como ejemplo para el desarrollo de una memoria técnica de un proyecto de diseño de una red de computadoras. En él se ejemplifica el contenido que debería constar en una memoria técnica de estas características, intentando ser lo más fiel posible al caso de estudio en concreto, pero sin pretender ser la mejor solución posible al problema, por lo que debería tomarse como lo que és, un ejemplo de documentación técnica. El documento contiene algunos errores de diseño, por lo que no debe tomarse como ejemplo de diseño, sino como ejemplo de documentación técnica a presentar. Este documento ha sido construido a partir de las indicaciones de [**?**].

1. Resumen Ejecutivo

Este documento presenta el diseño de la red de una empresa de seguros que busca modernizar completamente su infraestructura de red. La red renovada está destinada a optimizar la gestión de pólizas, la atención al cliente y los procesos administrativos, garantizando un acceso eficiente y seguro a los servicios necesarios.

La red cuenta con una sede central en Valladolid, desde la cuál se podrá acceder a un servidor DNS para gestionar la resolución de nombres en toda la red y, además, será el punto desde el que se sale a Internet y se conecta con el ISPy varias sedes regionales distribuidas entre algunas ciudades de Castilla y León, estas últimas contarán con diferentes VLANs para cada uno de los departamentos que se encuentren en dicha sede, además, cada sede regional dispondrá de un servidor DCHP para automatizar la asignación de direcciones IP.

La red finalizada resulta en una red central conectada a 8 redes mas que trabajarán en torno a ella, todas las redes ofrecerán servicios como acceso telematico, punto de acceso wifi

2. Objetivo del Proyecto

Este proyecto trata del diseño y despliegue de una red dedicada a dar servicios a las oficinas, tanto centrales como regionales, para así poder proveer a los empleados de herramientas de gestión de polizas, atención al cliente y de manejar procesos administrativos

3. Alcance del proyecto

Se implementará una nueva infraestructura de red que incluye una LAN en la sede central, distribuida a lo largo de varias plantas para servir a unos 100 empleados, con conexión cableada y WiFi para empleados y visitas, además de algún puesto libre que se podrá usar por invitados externos. En cada una de las ocho sedes regionales se instalará una LAN adaptada a las necesidades de unos 10 empleados por sede.En las sedes regionales podrá haber uno o varios de los siguientes departamentos:1.Ventas 2.Reclamaciones 3.Finanzas y Contabilidad 4.Publicidad 5.Legal. Todas las sedes estarán interconectadas mediante una WAN corporativa, que permitirá el tráfico seguro de datos y el acceso centralizado a recursos desde cualquier sede o ubicación remota, habilitando a todos los empleados para trabajar en movilidad mediante un acceso remoto seguro.

4. Requisitos de Diseño

En esta sección se definen los requisitos de diseño de la red, atendiendo a dos dimensiones. En primer lugar se concretarán los requisitos de la red desde la perspectiva del negocio.

4.1. Requisitos del Negocio

Los requisitos del negocio indican que la red debe ser privada, segura, escalable y soportar datos críticos como pólizas y procesos administrativos, garantizando acceso simultáneo entre la sede central y las regionales. También debe permitir conexiones remotas, soportar hasta 100 usuarios en la central y proporcionar terminales para empleados, además de incluir servicios comunes como DNS para reducir costos. Además debe ofrecer un sitio web público y acceso a servidores para gestiones de nóminas y viajes.

La relación completa de requisitos del negocio se encuentra en la Tabla 4.1.

Tabla de requisitos de negocio

Num.	**Descripción del Requisito**	**Crítico (S/N)**
1	La red soportará datos sobre las polizas de los clientes y los procesos administrativos.	S
2	Las sedes regionales podrán acceder de forma simultanea a los recursos de los servidores de la sede central.	S
3	La sede central tendrá mas compentencias que las sedes regionales, estas ultimas deberán acceder a la central para obtener determinados recursos.	S
4	Ciertos servicios de la red seran comunes en toda la infraestructura (DNS, router ISP) con el fin de ahorrar costes.	N
5	La red debera ser totalmente privada y segura, bloqueando cualquier acceso indebido por parte de cualquier usuario ajeno a la empresa.	S
6	La sede central deberá dar soporte al menos a 100 usuarios conectados simultaneamente, pudiendo llegar a miles de usuarios simultáneos, en las regionales aproximadamente a 10, pudiendo llegar a varias decenas de usuarios simultáneos.	S

Tabla 1: (Continuación)

Num.	Descripción del Requisito	Crítico (S/N)
7	La red debe de ser escalable, debido a que la empresa esta en crecimento.	S
8	Los empleados podrán acceder a un servidor web interno dedicado a la gestión de nóminas, viajes, vacaciones, etc.	S
9	La red deberá ofrecer la posibilidad de una conexión en remoto para todos sus empleados.	N
10	La red deberá ofrecer una conexión wifi para los empleados y las visitas.	N
11	La red dispondrá de terminales para que los empleados conecten sus portatiles, además, contará con espacios de sobra para visitas (empleados de otras ofincas, colaboradores etc).	S
12	La red dispondrá de una sitio web publico para clientes, donde estos podrán gestionar sus servios, consultar productos etc.	S
13	Cada sede regional contará con un servidor DHCP para automatizar la asignación de direcciones IP a los diferentes hosts de la subred.	S

4.2. Requisitos Técnicos

Establecemos ahora los requisitos técnicos para la red de la organización. Debemos destacar velocidades mínimas para comunicar los distintos equipos de la red, medidas de seguridad como VPN, filtrado de paquetes y segmentación mediante VLANs, además de garantizar resolución de nombres y asignación automática de IP para optimizar la conectividad. También se especifica que los routers y servidores deben estar centralizados para mayor control y eficiencia. Estos requisitos se recogen en la siguiente tabla: **??**.

Tabla 2: Requisitos Técnicos

Num.	Descripción del Requisito	Crítico (S/N)
1	En las sedes regionales, la red deberá soportar 150 Mbps ya que es lo adecuado para manejar el tráfico interno básico y garantizar un acceso fluido a los servicios esenciales.	S
2	En las conexiones entre las sedes regionales y la central se requerirá que la red soporte 300 Mbps debido al mayor volumen de datos compartidos, como la sincronización de bases de datos y el acceso simultáneo a los recursos de la sede central.	S
3	Dentro de la sede central, al ser donde mas afluencia de usuarios hay, el ancho de banda deberá ser de 1 Gbps para soportar la alta densidad de usuarios y la gran cantidad de acceso a los recursos.	S
4	Cada una de las sedes tendrá su propia red, pero los usuarios de estas podrán acceder a los recursos compartidos de la central.	S
5	La red deberá garantizar la resolución de nombres y la asignación automática de direcciones IP para facilitar el acceso de los usuarios y la conectividad entre sedes.	S
6	La empresa deberá disponer de un servidor accesible para los clientes, donde puedan gestionar servicios, realizar consultas y acceder a información de manera segura.	S
7	La red deberá permitir a los empleados acceder a aplicaciones y recursos internos de manera eficiente y segura desde cualquier ubicación.	S
8	Se deberá poder acceder a internet desde la red.	S
9	La red contará con un servicio de VPN para garantizar la posibilidad de acceso remoto a los trabajadores	S
10	Se definirán reglas de seguridad que defiendan la red de ataques exteriores	S
11	Se deberán implementar reglas de filtrado de paquetes para controlar y garantizar la seguridad del tráfico entrante y saliente.	S

Tabla 2: (Continuación)

Num.	**Descripción del Requisito**	**Crítico (S/N)**
12	El encaminamiento de los paquetes entre las subredes no se realizará por el mismo router encargado de filtrar paquetes y aplicar las políticas de seguridad	N
13	Los routers, punto de presencia del ISP y servidores de red estarán localizados en un centro de proceso de datos, CPD	S
14	Para cada sede existiran diferentes VLANs en función del departamento, tipo de conexión etc	S
15	Los equipos de usuarios y servidores de cada organización estarán en salas diferentes con las correspondientes tiradas de cable al CPD	S
16	Los servidores que sean utilizados por todas las sedes estarán localizados en un centro de datos en la capa core de la red.	S
17	La red tendrá un nivel de disponibilidad de 99,95 % (Tier III)	S
18	La red utilizará un protocolo de enrutamiento que sea compatible con protocolos externos.	S
19	La red utilizará conmutadores de nivel 3 MultiLayer switches, esto para garantizar una mayor escalabilidad y una mejor adaptabilidad a un gran número de protocolos.	S

4.3. Grupos de Usuarios y Almacenamiento de Datos

Los distintos usuarios que accedan a la red, se dividirán en grupos atendiendo a su equipo de trabajo (se excluirá a los clientes como usuarios ya que no será necesario estimar un valor de estos). Para los servidores, se ha de tener en cuenta los servicios que debe ofrecer la empresa, así como la disponibilidad requerida de estos.

La información sobre los principales grupos de usuarios, incluyendo su tamaño, localización y las principales aplicaciones que utilizan se recoge en la Tabla 3).

Tabla 3: Grupos de Usuarios

Grupo Usuarios	**Tamaño**	**Localización**	**Aplicaciones Utilizadas**
Equipo Ventas	60-80	Castilla y León	Aplicación web trabajadores, aplicación gestión trabajadores
Equipo análisis pólizas	20-30	Castilla y León	Aplicación web trabajadores, aplicación gestión trabajadores
Equipo Atención al cliente	30-50	Castilla y León	Aplicación web trabajadores, aplicación gestión trabajadores
Equipo legal	15-25	Castilla y León	Aplicación web trabajadores, aplicación gestión trabajadores
Finanzas	20-30	Castilla y León	Aplicación web trabajadores, aplicación gestión trabajadores
Recursos humanos	15-20	Castilla y León	Aplicación web trabajadores, aplicación gestión trabajadores

Los principales almacenes de datos (servidores) y su localización se muestran en la Tabla 4.

Tabla 4: Servidores

Servidor	**Localización**	**Aplicaciones**	**Usado por Grupo Usuarios**
SVR-Web-DMZ	DMZ de la red	Aplicación Web Clientes y Trabajadores	Clientes
SVR-DNS-DMZ	DMZ de la red		Empleados y Clientes
SVR-DHCP-Central	Red interna de la sede central		
SVR-DHCP-Sede Regional	Red de cada sede regional		
SVR-Datos-Central/Web	Red campus saliente del core	Aplicación Gestión Trabajador	Empleados
SVR-DNS-Central	Red campus saliente del core		Empleados
SVR-VPN-DMZ	DMZ de la red		Empleados y Clientes
SVR-RADIUS	Capa distribución sede central		Empleados

4.4. Aplicaciones en Red

Las aplicaciones en red nos permitirán gestionar las pólizas, atender al cliente y demás trámites administrativos necesarios para la empresa.
Debemos tener en cuenta las siguientes estimaciones de ancho de banda:

- En Microsoft Teams, por usuario en una videollamada se van a necesitar unos 1,2Mbps.
- Para Salesforce, aplicación para gestionar ventas, un usuario usa una media de 150kbps de ancho de banda para esta aplicación.
- En Duck Creek, aplicación usada para gestionar las pólizas, unos 500kbps. Zendesk, para ayudar a la atención al cliente, necesita unos 500kbps para funcionar (lado a lado) luego por cada conexión con un usuario se necesitará 1Mbps.
- Adobe Acrobat Reader, para que el equipo legal pueda descargar archivos judiciales, 5Mbps por usuario.
- Oracle NetSuite para la gestión de finanzas básicas, con un ancho de banda necesario de uno 3Mbps.
- Workday para la gestión de los recursos humanos, que necesitaría unos 300 kbps por usuario activo.

Ver tabla 5.

Tabla 5: Aplicaciones en red y características del tráfico asociado

Aplicación	**Nueva (S/N)**	**Crítica (S/N)**	**Grupo Usuarios**	**Servidor**	**Ancho de Banda Estimado**
Microsoft Teams	S	S	Empleados	SVR-Datos-Central/Web	150MBps /300Mbps
Salesforce	S	S	Equipo de Ventas	SVR-Datos-Central/Web	3Mbps /10Mbps
Duck Creek	S	S	Equipo de gestión de pólizas	SVR-Datos-Central/Web	12,5Mbps /20Mbps
Zendesk	S	S	Equipo de atención al cliente	SVR-Datos-Central/Web	25Mbps/ 35Mbps
Adobe Acrobat Reader	S	S	Equipo legal	SVR-Datos-Central/Web	50Mbps /200Mbps
Oracle NetSuite	S	S	Equipo de finanzas	SVR-Datos-Central/Web	70Mbps /90Mbps
Workday	S	S	Equipo de recursos humanos	SVR-Datos-Central/Web	4,5Mbps /6Mbps

5. Diseño Lógico

En esta sección, se pueden ver los aspectos seguidos para el diseño de la red, relacionados con la topología y las directrices que se han seguido para nombrar a los dispositivos y su enumeración

5.1. Topología

En la topología de la red, se pueden observar los distintos elementos y conexiones que componen a la misma, a partir de los requisitos impuestos por el cliente. El esquema de alto nivel se corresponderá con la siguiente imagen:

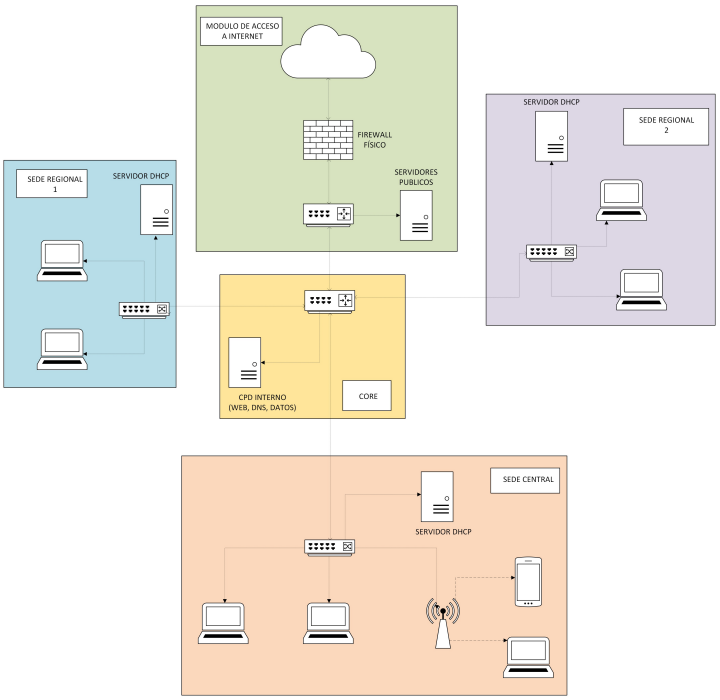

Figura 1: Diagrama del Diseño Lógico de la Red de Alto Nivel

En esta imagen se pueden observar, los distintos elementos (de forma resumida) que configuran la red, así como sus conexiones entre si. Podemos observar que para cada sede, habrá un servidor DHCP para automatizar la asignación de direcciones IP, ademas, la sede central cuenta con puntos de acceso wifi. También podemos observar que en el modulo de acceso a internet hay un firewall físico, el cual restringirá el acceso a ciertas partes de la red a fuentes externas.

Los detalles de la topología a más bajo nivel mostrados en la Figura 3 permiten observar la implementación de la red. Existirán 2 servidores in-

ternos, el primero, ubicado en el CPD, será el que usen los empleados y la directiva de la empresa para gestionar cosas como políticas de empresa, normas, vacaciones del empleado, etc. El segundo, ubicado en la DMZ, será usado mayoritariamente por los clientes para acceder a datos sobre productos y gestionar sus servicios. Este servidor web, aparte de funcionar como tal, también permitirá a los clientes conectarse desde una app móvil para así gestionar de forma más sencilla, dichos servicios. Este último servidor debe ser conocido para que los usuarios puedan acceder remotamente a estos datos.

Además, podemos ver en el siguiente esquema, la conexión desde la frontera de la red al ISP:

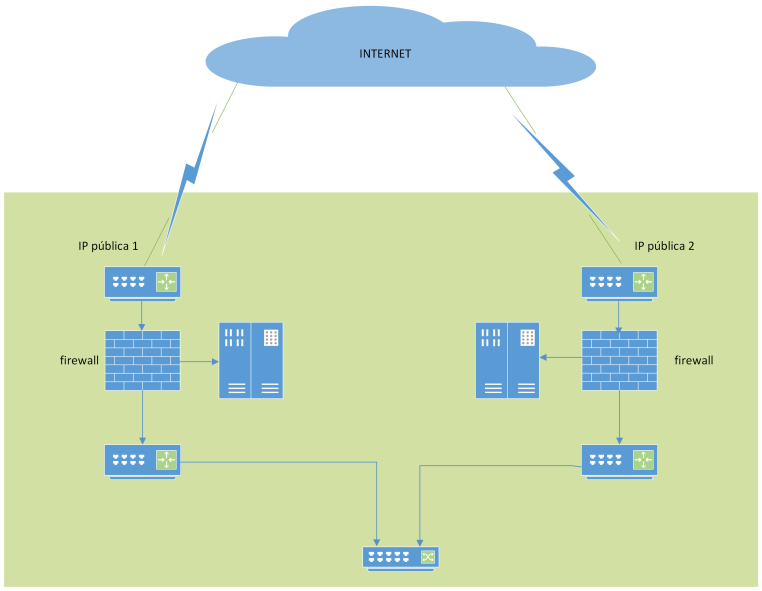

Figura 2: Esquema del modulo de acceso a internet

En más detalle, gracias al esquema de la red de bajo nivel, podemos observar las distintas zonas de las que está compuesta la red, tales como sedes regionales, la sede central e Internet

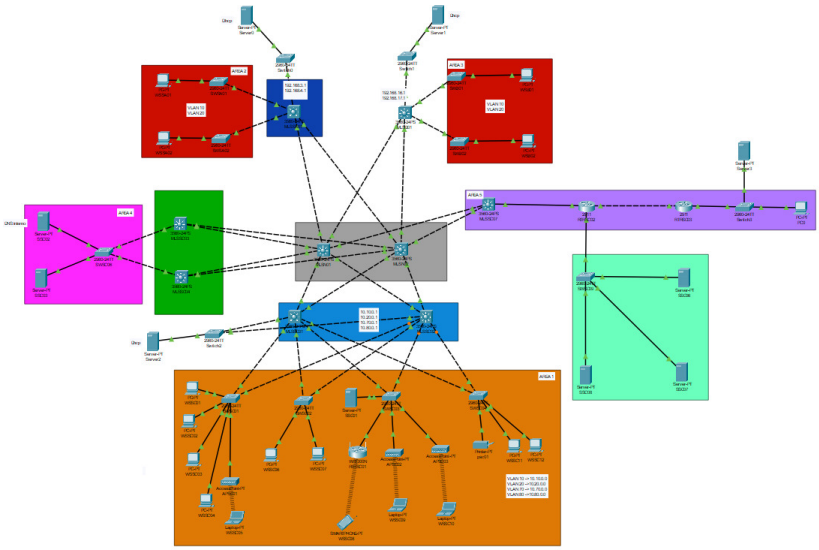

Figura 3: Diagrama del Diseño Lógico de la Red de Bajo Nivel

5.2. Nombres

Todos los dispositivos de esta red va a recibir un nombre que determinará tanto su función (ver Tabla 8) como su disposición en la red. En caso de que existan varias instancias del mismo dispositivo, por ejemplo, varias estaciones de trabajo, se numerarán con un número de dígitos suficientes para su identificación inequivoca. Por ejemplo, la tercera estación de trabajo de la sede regional de Salamanca, se denominará WSSA03.

Tabla 6: Esquema de nombres

Dispositivo	**Nombre**
Estación de trabajo	WS
Servidor	S
Router	RTR
Switch	SW
Multilayer Switch	MLS
Punto de acceso	AP
Firewall	F
Printer	P

Como los dispositivos se dividen en sedes regionales, estas tienen las

siguientes claves identificativas:

Tabla 7: Clave de los dispositivos por ciudad

Ciudad	**Clave**
Valladolid	V
Palencia	P
León	L
Burgos	B
Soria	SO
Segovia	SE
Ávila	A
Salamanca	SA
Zamora	Z

Ciertos dispositivos no se encuentran en una sede regional y se identificaran con la siguiente clave:

Tabla 8: Clave de los dispositivos que no estén en una sede regional

Ciudad	**Clave**
Núcleo	N
Sede Central	SC
Internet	I

El formato de cualquier dispositivo será del tipo: <TipoDeDispositivo><ClaveDeLaLocalización><NúmeroDeDispositivo/Función>.

- Estaciones de trabajo Sede Regional Salamanca: WSSA01 ... WSA10
- Estaciones de trabajo Sede Reginal Burgos: WSB01 ... WSB10
- Estaciones de trabajo Sede Regional Palencia: WSP01 ... WSP10
- Estaciones de trabajo Sede Central: WSSC01 ... WSSC100
- Estaciones de trabajo VPN: WSVPN01 ... WSVPN100
- Servidores: SCPDDNS, SCPDDATA, SCPDWEB, SSCDHCP, SDMZWEB, SPDHCP SSCRAD...
- Switches: SWSC01, SWB01, SWSA01...
- Routers: RTRI01, RTRVPN01
- MultilayerSwitches: MLSSC01, MLSP01...
- Puntos de acceso: APSC01, APB01, APSA01...
- Firewall: FI01
- Wireless Controler: WLCSC01

5.3. Direcciones

En la red se han definido distintas subredes. Estas se dividen en: 1 subred para la sede central, 8 subredes para las distintas sedes regionales que conformarán la empresa, 2 subredes para direccionamiento en el core, 1 subred para la gestión, otra para las conexiones remotas mediante VPN y por último, una subred para el CPD con los servidores.

Tabla 9: Direccionamiento de localizaciones y grupos de usuarios

Localización	**VLAN**	**Subred/más**	**Grupo Usuarios**	**Red resumen**
Valladolid				10.0.0.0/8
	10	10.10.0.0/16	Ventas VA	
	20	10.20.0.0/16	Análisis de pólizas VA	
	30	10.30.0.0/16	Atención al cliente VA	

Localización	VLAN	Subred/másc	Grupo Usuarios	Red resumen
	40	10.40.0.0/16	Equipo legal VA	
	50	10.50.0.0/16	Finanzas VA	
	60	10.60.0.0/16	Recursos humanos VA	
	70	10.70.0.0/16	Red Wifi Invitados	
	80	10.80.0.0/16	Sala de reuniones	
	90	10.90.0.0/16	Red Wifi Empleados	
Salamanca				192.168.0.0/21
	10	192.168.1.0/24	Ventas SAL	
	20	192.168.2.0/24	Análisis pólizas SAL	
	30	192.168.3.0/24	Atención al cliente SAL	
Palencia				192.168.8.0/21
	10	192.168.8.0/24	Equipo Legal PA	
	20	192.168.9.0/24	Análisis pólizas PA	
	30	192.168.10.0/24	Atención al cliente PA	
Leon				192.168.16.0/21
	10	192.168.16.0/24	Finanzas LE	
	20	192.168.17.0/24	Análisis pólizas LE	
	30	192.168.18.0/24	Atención al cliente LE	
Soria				192.168.24.0/21
	10	192.168.24.0/24	Recursos humanos SO	
	20	192.168.25.0/24	Análisis pólizas SO	
	30	192.168.26.0/24	Atención al cliente SO	
Segovia				192.168.32.0/21
	10	192.168.32.0/24	Ventas SEG	

Localización	VLAN	Subred/másc	Grupo Usuarios	Red resumen
	20	192.168.33.0/24	Análisis pólizas SEG	
	30	192.168.34.0/24	Atención al cliente SEG	
Ávila				192.168.40.0/21
	10	192.168.40.0/24	Equipo Legal AV	
	20	192.168.41.0/24	Análisis pólizas AV	
	30	192.168.42.0/24	Atención al cliente AV	
Zamora				192.168.48.0/21
	10	192.168.48.0/24	Finanzas ZA	
	20	192.168.49.0/24	Análisis pólizas ZA	
	30	192.168.50.0/24	Atención al cliente ZA	
Burgos				192.168.56.0/21
	10	192.168.56.0/24	Recursos humanos BUR	
	20	192.168.57.0/24	Análisis pólizas BUR	
	30	192.168.58.0/24	Atención al cliente BUR	

Toda la información relevante respecto al direccionamiento IP de cada subred se recoge en la Tabla 10. En ella se especifica la dirección de la subred, máscara, dirección del router por defecto y servidor DHCP para los hosts.

La gestión de las direcciones de las subredes regionales, se realizará mediante DHCP y se guiará por las siguientes reglas:

- Para la sede central se ha optado por una subred de máscara /8, ya que consideramos que esta va a ser la red más escalable, causando que se deban conectar muchos hosts.
- Para las sedes regionales, la máscara es un /21 ya que nos permite sumarizar las redes de forma más sencilla y el número de dispositivos será notablemente menor en estas sedes que en la central.
- Para las VLANes de las sedes regionales, la máscara es un /24 lo que puede llegar a producir una limitación de la escalabilidad en caso de que la empresa crezca enormemente en cada sede regional y se requieran

Tabla 10: Direccionamiento de subredes

Segmento o Subred	**Dirección IP/Máscara**	**Router por Defecto**	**Servidor DHCP**
Red Valladolid	10.0.0.0/8	10.0.0.1	192.168.255.10
Red Salamanca	192.168.0.0/21	192.168.0.1	192.168.255.2
Red Palencia	192.168.8.0/21	192.168.8.1	192.168.255.3
Red Leon	192.168.16.0/21	192.168.16.1	192.168.255.4
Red Soria	192.168.24.0/21	192.168.24.1	192.168.255.5
Red Segovia	192.168.32.0/21	192.168.32.1	192.168.255.6
Red Avila	192.168.40.0/21	192.168.40.1	192.168.255.7
Red Zamora	192.168.48.0/21	192.168.48.1	192.168.255.8
Red Burgos	192.168.56.0/21	192.168.56.1	192.168.255.9
Red de Gestión	192.168.64.0/21	192.168.64.1	Estática
Red de Conexiones Remotas	192.168.72.0/21	192.168.72.1	Estática(Servidor VPN)
Subred Core 1	192.168.1.0/30	-	Estática
Subred Core 2	192.168.2.0/30	-	Estática
CPD	192.168.250.0/24	192.168.250.1	Estática
Servidores DHCP	192.168.255.0/24	192.168.255.x (x depende del servidor DHCP)	Estática
DMZ	192.168.250.0/24	192.168.250.1	Estática
Internet1	192.168.200.0/24	-	Estática
Internet2	192.168.201.0/24	-	Estática

más departamentos en cada una de ellas al igual que en caso de que la empresa crezca enormemente en el número de sedes regionales.

Para el resto del direccionamiento hemos optado por direcciones estáticas, ya que serán equipos que no deberían necesitar cambiar de dirección.

- Para la red de conexiones remotas hemos optado por un /24, ya que depend de el número de servidores de VPN que queramos configurar para este fin (de momento 1, pero en un futuro se puede escalar este número), pero entendemos que este número, por mucho que la empresa pase a ser una empresa mediana, no debe escalar por encima de los 254 servidores.

- Para el resto de subredes, las ips son estáticas al pertenecer estas al: Core, /30 para permitirnos identificar y sumarizar las subredes de forma más sencilla. Servidores del CPD, que necesita tener direcciones estáticas para que se los usuarios puedan acceder a los datos y al DNS de forma más eficiente. Internet, que debe ser estática para permitir la salida conocida a el exterior desde la red interna y por último, los servidores DHCP.

- Considerar que para cada subred, las 10 primeras direcciones son para: enlaces por defecto, dispositivos que necesiten direcciones estáticas para encontrarles en la subred (impresoras), etc.

Para completar la información sobre direccionamiento, en la Tabla 12 se muestran las direcciones de los servidores que tienen una dirección estática. Notar que para las sedes regionales, en la dirección estática .x, sustituir la x por el dhcp de cada sede regional (desde el .2 de la de Salamanca hasta el .9 de la de Burgos) y para el nombre del Host sustituir X por la letra/s de la sede regional. Para el servidor VPN, tener en cuenta que este sería el direccionamiento estático en caso de que solo hubiera un servidor, si hay más simplemente ir estableciendo direcciones contiguas (.2, .3 ...). Para la impresorar, notar que la "Y" en el nombre equivale a su ubicación, la "x" en la ip equivale a la vlan de donde se encuentre (los usuarios de una VLAN solo pueden acceder a dispositivos periféricos de su misma VLAN) y la "y" al nº de entre las 10 primeras direcciones que quede libre (entendemos que para una VLAN no tiene mucho sentido dar más de 9 direcciones (2-10) para periféricos que necesiten IP. En otro caso, asignar IPs y modificar el pool de direcciones del servidor DHCP).

Se habilitará el servicio de NAT en el router RTRI01 de modo que la red pueda establecer conexiones salientes y entrantes con Internet, cambiando así la dirección privada por una pública adecuada.

Tabla 11: Dispositivos con Direcciones Estáticas

Host	**Dirección IP**
SSCDHCP	192.168.255.10
SCPDDNS	192.168.250.10
SXDHCP	192.168.255.x
SDMZWEB	192.168.150.2
SDMZDNS	192.168.150.3
SDMZVPN	192.168.72.1
SCPDWEB	192.168.250.20
SCPDDATA	192.168.250.30
PSCY	10.x.0.y

Tabla 12: Direccionamiento NAT

Dirección privada	**Dirección pública**
10.0.0.0/8	202.0.0.0/8
192.168.0.0/16	202.0.0.0/8
192.168.150.2	203.0.0.10
192.168.150.3	203.0.0.11

5.4. Protocolos de la red

Para que nuestra red sea sencilla de gestionar y funcione correctamente, se han implementado una serie de protocolos para conseguirlo:

- **VTP**: para la configuración y distribución de VLANes. Este protocolo nos permite distribuir las redes gracias a un switch servidor, causando que estas se propaguen por toda la subred de forma más sencilla que teniendo que configurar cada VLAN en cada parte switch. Se debe configurar este protocolo una vez por cada subred que requiere de VLANes (central y regionales).

- **HSRP**: para la disponibilidad de las subredes. Este protocolo nos permite crear interfaces virtuales para que en caso de que uno de los multilayer switch se caiga (o uno de los enlaces), la red siga completamente funcional. Se debe configurar en todos los multilayer switches duplicados para así asegurar esa disponibilidad (sede central y regionales, CPD).

- **OSPF**: enrutamiento. Este protocolo nos permite enrutar los paquetes entre VLANes y subredes de forma sencilla. Muy útil al ser muy escalable gracias a su composición de áreas, permite conectarse con otros protocolos, lo cuál es muy útil en la salida a internet y su convergencia es muy rápida. Debemos configurar OSPF en toda la subred interna, siendo el BACKBONE (area 0) el core con los multilayer switch conectados a este y las distintas areas, equivaldrían a las distintas redes campus de la red (central, regionales, CPD) e Internet (solo una parte).

- **SNMP**:El SNMP es un protocolo estándar de la capa de aplicación diseñado para la gestión de redes. Se utiliza para supervisar, gestionar y configurar dispositivos conectados a una red, como routers, switches, servidores e impresoras. Es uno de los protocolos más comunes para la monitorización de redes debido a su simplicidad y compatibilidad .

- **SFTP**:El SFTP es un protocolo de transferencia de archivos que opera sobre el protocolo SSH (Secure Shell) para garantizar la seguridad de los datos durante su transmisión. A diferencia de FTP, que envía la información en texto plano, SFTP cifra tanto los datos como las credenciales, protegiéndolos contra intercepciones y accesos no autorizados.

5.5. Seguridad

En cuanto a la seguridad, hemos seguido la arquitectura Cisco de seguridad SAFE, la cual distribuye la red en varios módulos para asegurar su seguridad.

Además, no podemos asegurar que todos los ataques que se produzcan sobre la red se originen desde el exterior de la misma.
Algunos de los principales riesgos y políticas de seguridad que se van a implementar para protegernos del exterior son los siguientes:

- Intento de acceso desde Internet a la red. Se aplicarán filtros que impidan el acceso de paquetes no permitidos proveninentes del exterior a la red interna. Como regla general, no se aceptará ningún paquete que intente entrar sin ser parte de una conexión saliente previa. Dichos filtros se implementarán como lista de control de acceso en el firewall entre el ISP y el router periferico de la red, (ver Tabla 13).

- Cualquier intento de acceso a los servidores o dispositivos internos (exceptuando los servidores publicos de la DMZ) será denegado, y los paquetes de petición serán descartados, devolviendo un paquete "ICMP Administratively Prohibited Unreachable message".

- Para los servidores públicos se utilizarán mecanismos de seguridad de certificados de clave simétrica AES.

- Toda la información que circula por la red interna estará codificada en SHA-512, garantizando así la integridad y la confidencialidad de los datos.

- Intento de denegación de servicio del servidor web. La red dispone de mecanismos de contención de ataques DoS, se implementarán reglas en el firewall que limiten el número de conexiones simultaneas desde la misma dirección IP.En caso de que sean distribuidos, se podría llegar a limitar el número máximo de conexiones hasta que se resuelva el problema.

A continuación se enumeran algunos de los principales riesgos y politicas de seguridad que se van a implementar para protegernos de ataques realizados desde el interior de la red.

- Se implementará el protocolo 802.1X en los diferentes switches de la capa de acceso, protegiendo a la red de accesos no autorizados a los servidores internos de la red.

- Se restringirá el acceso a determinados servicios a los usuarios conectados a la red desde la subred "Wifi para invitados"

- Se establecerá un sistema de privilegios, limitando el acceso a ciertos recursos solo a los usuarios con mayores privilegios. Tener en cuenta que se seguirá el principio de establecer el menor privilegio posible.

- Para la seguridad interna física ver:

Tabla 13: Flujos de tráfico permitidos en RTP-ISP

IP origen/másc.	**IP dest/másc.**	**Tipo mensaje**	**Interfaz - sentido**	**Stateful (S/N)**
202.0.0.0/8	any	*	Gi0/0 - in	S
203.0.0.0/8	any	*	Gi0/0 - in	S
Any	203.0.0.0/8	*	Gi0/1 - in	N
Any	Any	tcp(established)	Gi0/1 - in	S
Any	Any	icmp-reply	Gi0/1 - in	S
Any	Any	icmp-unreachable	Gi0/1 - in	S
Any	Any	http(established)	Gi0/1 - in	S
Any	Any	udp-reply	Gi0/1 - in	S
Any	192.168.72.0/21	IPsec	Gi0/1 - in	N

Además de la seguridad mencionada anteriormente, los servidores de la red se van a encontrar en CPDs securizados fisicamente. Algunos de las medidas de securización son las siguientes:

- Vigilancia, autenticación multifactor (combinación de tarjetas de acceso,PINs y biometría), puertas y entradas blindadas para evitar el acceso de personas no autorizadas.
- Localización del CPD en zonas que no puedan ser afectadas en caso de la existencia de una inundación u otros fenómenos meteorológicos como la DANA.
- Localización del CPD en sótanos o plantas subterráneas para evitar explosiones de meteoritos o bombas.
- Existencia de tanques de gasóleo como fuentes de energía de respaldo en caso de fallos en el suministro eléctrico y redundancia en el suministro eléctrico con varias compañías.
- Uso de agentes extintores gaseosos de manera que mediante el aumneto de la temperatura o el consumo del oxígeno permiten que el fuego en caso de incendio no se propague.

5.6. Gestión

Para más información sobre los protocolos usados en esta sección, ver el apartado 5.4
Para la monitorizacion de la red vamos a seguir el modelo FCAPS:

- Gestión de fallos: Para detectar, aislar y resolver problemas en la red, utilizamos SNMP (Simple Network Management Protocol).
- Gestión de configuracion: Se emplea SFTP para el almacenamiento y transmisión centralizado de las configuraciones de los dispositivos
- Gestión de contabilidad: Se monitorizará a los usuarios para evitar costes excesivos ya sea de manera intencionada o no. Para este objetivo se puede usar SNMP
- Gestión de desempeño: Se monitorizará la red para medir el comportamiento de la misma y registrar cambios en las rutas. Se usará SNMP para este objetivo
- Gestión de seguridad: Se mantendrán contraseñas y claves de encriptación de manera segura y se analizarán logs y configuraciones de dispositivos para cumplir políticas de seguridad

La gestión se realizará fuera de banda, esta la llevaremos a cabo mediante un servidor de terminales. Los distintos dispositivos de red se conectarán a los puertos serie del servidor de terminales, esto permitirá a los administradores gestionar estos dispositivos de una forma remota desde una sala centralizada(NOC).

6. Diseño Físico

Esta sección se describen las características y usos recomendados de las tecnologías y los dispositivos elegidos para implementar el diseño.

Para implementar esta red se han elegido los siguientes dispositivos:

- MultiLayer Switches Cisco Catalyst 9300 Series, en el core y la sede central, específicamente el modelo C9300-24P-A, este modelo cuenta con 48 puertos Gigabit Ethernet, por lo que la red posee una escalabilidad destacable.
- En el caso de las sedes regionales, una opción más económica y suficiente sería un Cisco Catalyst 9200 Series, como el modelo C9200-24P-A, contando con 24 puertos.
- Para distribuir la red correctamente entre los diferentes departamentos utilizaremos switches Cisco SG350-28, cuenta con 28 puertos hasta los

1000 Mb/s, y soporta perfectamente VLANs y tecnologías de encapsulación 802.1Q

- Para el cableado en la capa de acceso hemos optado por cable de cobre UTP Cat 6A, este tipo de cable es ideal para conexiones a usuarios y dispositivos dentro de las oficinas, pudiendo soportar tasas de hasta 10 Gb/s en un rango de hasta 100m.
- Para la capa de distribución se usará fibra optica monomodo, esta posee altas tasas de velocidad y un gran ancho de banda.
- Para la capa de core se usará la tecnología Metro Ethernet, hemos escogido esta opción por la capacidad de la misma de combinar comportamientos WAN con LAN, se contratarán los servicios de un proveedor de comunicaciones, ellos serán los encargados de gestionar esta parte de la red y garantizar su disponibilidad.
- En la capa Core de la red se encuentra el modulo de acceso a internet, en el existe un router que actua como firewall, este tiene una interfaz conectada a la red interna, y otra conectada a los servidores publicos de la red (DMZ), además, existe un servidor DNS público para la resolución de nombres de los servidores de la red.

7. Pruebas del Diseño

En esta sección se indicarán los resultados de las pruebas realizadas para validar el diseño propuesto. Se describirán los objetivos de las pruebas, el test realizado y el resultado obtenido. Se deberán comprobar especialmente la conectividad entres las distintas delegaciones, los enlaces MetroEthernet, el acceso a internet, el acceso al CPD y el acceso a los servidores de la DMZ tanto desde el exterior como el interior. Proponemos también las pruebas para casos en los que las reglas de acceso impidan el paso de los paquetes. (Tabla 14).

Tabla 14: Pruebas

Objetivo del Test	**Prueba Realizada**	**Resultado**
Comunicación entre sede Central y Regionales	PING entre WSSC06 y WSB01	Positivo
Comunicación entre 2 sedes regionales	PING entre WSSA02 y WSB02	Positivo
Acceso desde Internet al servidor web y DNS de la DMZ	HTTP entre PCInternet y SDMZWEB	Positivo
Acceso desde la red interna al sevidor web y DNS del CPD	HTTP entre WSSC11 y SDMZWEB	Positivo
Acceso desde la red interna al sevidor web y DNS del de la DMZ	HTTP entre WSSA02 y SCPDWEB	Positivo
Acceso a internet desde la sede central	PING entre WSSC09 y PCInternet	Positivo
Acceso a internet desde una sede regional	PING entre WSB02 y PCInternet	Positivo
Acceso desde la red externa al sevidor web y DNS del CPD	HTTP entre PCInternet y SDMZWEB	Negativo

A. Apéndices

A.1. Configuración

A.1.1. Configuración del MLSSC01

A modo de ejemplo, en la subsección siguiente se muestra un fragmento correspondiente a la configuración de las VLANes y HSRP del multilayer switch MLSSC01.

```
interface Vlan10
 mac-address 00e0.a3e6.6e01
 ip address 10.10.0.3 255.255.0.0
 ip helper-address 192.168.255.4
 ip helper-address 192.168.255.10
 standby 10 ip 10.10.0.1
 standby 10 preempt
!
interface Vlan20
 mac-address 00e0.a3e6.6e02
 ip address 10.20.0.3 255.255.0.0
 ip helper-address 192.168.255.4
 ip helper-address 192.168.255.10
 standby 20 ip 10.20.0.1
 standby 20 priority 105
 standby 20 preempt
!
interface Vlan70
 mac-address 00e0.a3e6.6e03
 ip address 10.70.0.3 255.255.0.0
 ip helper-address 192.168.255.4
 ip helper-address 192.168.255.10
 standby 70 ip 10.70.0.1
 standby 70 priority 105
 standby 70 preempt
!
interface Vlan80
 mac-address 00e0.a3e6.6e04
 ip address 10.80.0.3 255.255.0.0
 ip helper-address 192.168.255.4
 ip helper-address 192.168.255.10
 standby 80 ip 10.80.0.1
```

Figura 4: Diagrama del Diseño Lógico de la Red de Bajo Nivel

A.1.2. Configuración de MLSN01

En esta subsección se muestra un fragmento de la configuración de OSPF pudiéndose ver en la imagen las direcciones de los ABRs del núcleo del multilayer switch MLSN01.

```
router ospf 1
 log-adjacency-changes
 network 192.168.1.4 0.0.0.3 area 0
 network 192.168.1.16 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.3 area 0
 network 192.168.1.8 0.0.0.3 area 0
 network 192.168.1.24 0.0.0.3 area 0
 network 192.168.1.12 0.0.0.3 area 0
 network 192.168.1.20 0.0.0.3 area 0
```

Figura 5: Diagrama del Diseño Lógico de la Red de Bajo Nivel

A.2. Bug detectado en la confuración del protocolo OSPF

Al realizar un ping desde un equipo de cualquiera de las sedes de la red al PC que se encuentra en internet "PCInternet", el paquete realiza un trayecto anómalo al llegar al MLSSC07, cuando OSPF se propaga a MLSSC07 transmite 3 rutas para llegar al PC, todas ellas con la misma métrica, el paquete entonces realiza los 3 trayectos posibles hata que en el tercero llega al host. En el siguiente enlace se puede observar un foro de Cisco en el que se

plantea un problema parecido con rutas por defecto en OSPF, algunas de las respuestas afirman que se puede tratar de un bug de Packet Tracer debido a la manera en la que este configura OSPF. Algunas soluciones planteadas sugieren el uso de comandos que no están disponibles como: "ip ospf cost 20000"
Link al foro de Cisco

A.3. Reparto del trabajo

Todos los miembros del grupo han participado en igual medida en la realización de esta tarea. Al entregar este documento con nuestros nombres, todos manifestamos estar de acuerdo con que se nos gradúe con la misma nota.

Referencias

- Transparencias de la Asignatura
- Prácticas de la Asignatura
- Catálogo Cisco