Escuela Politécnica Superior de Jaén

Grado en Ingeniería Informática

Universidad de Jaén

Escuela Politécnica Superior de Jaén

Trabajo Fin de Grado

Diseño de una red de área global para una empresa con múltiples sedes

Alumno: **Raúl Francés Moya**

Tutor: Prof. D. Joaquín Cañada Bago

Dpto: Informática

Septiembre, 2019

Universidad de Jaén
Escuela Politécnica Superior de Jaén
Departamento de Informática

Don Joaquín Cañada Bago, tutor del Proyecto Fin de Carrera titulado: **Diseño de una red de área global para una empresa con múltiples sedes**, que presenta Raúl Francés Moya, autoriza su presentación para defensa y evaluación en la Escuela Politécnica Superior de Jaén.

Jaén, Junio de 2019

El alumno: El tutor:

Raúl Francés Moya Joaquín Cañada Bago

Índice

1. INTRODUCCIÓN

En la actualidad, la mayoría de empresas están distribuidas en más de una sede situadas en distintos barrios, ciudades o incluso países pero las tecnologías actuales nos permiten lograr un trabajo conjunto, acercando virtualmente grandes distancias físicas.

Este TFG persigue el diseño de una red multimedia de área amplia para una empresa con diferentes sedes que permita la interconexión y la utilización de aplicaciones de datos y multimedia con calidad y poca latencia, sin pérdida de datos en los flujos necesarios.

Además de diseñar una red global ficticia, se ha implementado una parte básica de ésta, conectando dos sedes e implementando el control de flujos de datos, utilizando dos routers y un switch propiedad de la Escuela Politécnica Superior de Jaén.

2. ANTECEDENTES

Suponemos una empresa desarrolladora de software de unos 50 trabajadores, la mitad de los cuales trabajan en la sede central y el resto en otras sedes o son trabajadores remotos, divididos en 4 grupos de trabajo (Desarrollo, Soporte, Comerciales y Gestión) que necesita implementar una correcta red global para conectar sus sedes, a la vez que las protege de ataques remotos y proporcionando acceso a los servidores pertinentes.

Es necesario separar los grupos de trabajo entre ellos, pero permitir el acceso al servidor privado central, independientemente del grupo de trabajo o de la sede en la que se encuentre el trabajador.

Cada empleado dispondrá también de un teléfono VoIP, que si comunica con otro equipo de la misma sede, se apoya en un servidor VoIP de la sede, y con el servidor central en caso contrario.

Para interconectar las sedes se utilizaría MPLS (VPN a través del operador que hayamos contratado), pero por razones obvias no es posible utilizarlo en la implementación realizada. Para los trabajadores remotos se seguiría usando una VPN típica.

3. OBJETIVOS

- Diseñar una red de comunicación corporativa adaptada a las necesidades de la empresa, cumpliendo los requisitos de conectividad y ancho de banda de datos.
- Implementar una parte de la red. Estableceremos las VLANes, VPN y QoS en la sede central y una sede adicional, además de una DMZ.
- Medir las prestaciones de la red con herramientas como Wireshark.
- Verificar que la red puede soportar aplicaciones multimedia con streaming de video a través de VLC.

4. ESTADO DEL ARTE

4.1. LAN

Una Red de Área Local (Local Area Network) es un sistema de comunicación con el que podemos conectar una serie de equipos informáticos en una ubicación privada, generalmente de una vivienda o empresa. Lo normal en una vivienda es que todos los equipos se conecten mediante cable Ethernet o Wi-Fi a un único router, mientras que en una empresa no demasiado pequeña, lo más frecuente es que los equipos se conecten a varios switches, y estos se conecten al router.

Este tipo de redes es necesario para compartir recursos, como impresoras o un servidor privado (pe. Servidor de correo electrónico). Dentro de esta red tenemos una velocidad de transferencia muy alta, 100 Mbps ó 1 Gbps (1000 Mbps, que actualmente es lo más común), con una baja tasa de error; siempre y cuando no se excedan los 100 metros de longitud de cable. Una vez superada esa distancia se empiezan a dar problemas debido a la pérdida de energía del par trenzado. Se podría aumentar esta distancia situando switches entre medias, pero generalmente es más económico y sencillo establecer dos redes LAN diferentes y comunicarlas a través de Internet.

4.2. WAN

Las Redes de Área Amplia o Wide Area Network permiten comunicar dos o más redes LAN entre sí. Este tipo de conexión es la que permite que funcione Internet tal y como lo conocemos. La unión de redes LAN se realiza mediante un conmutador de nivel 3.

La velocidad de transferencia es mucho menor que en redes LAN, y la tasa de error bastante mayor. Esto se debe a que dependemos de la velocidad de transferencia, procesamiento y encaminamiento de todos los equipos de telecomunicaciones que se encuentran entre el equipo origen y el destino.

4.3. VLAN

Una VLAN (Virtual Local Area Network) es cada una de las separaciones lógicas de una LAN, de forma que se limitan a una parte de los equipos el acceso a uno o varios recursos. Un ejemplo simple sería evitar que los alumnos de una clase puedan configurar el router o switch al que están conectados. Cada VLAN tiene su propio identificador de red y broadcast, pero todas comparten infraestructuras.

Esta división se consigue añadiendo una etiqueta o tag a cada uno de los paquetes de la capa de Enlace que envía un equipo, indicando la VLAN al que pertenece. Si un equipo transmite paquetes sin etiquetas, se le asigna la VLAN Nativa. Es posible configurar que para cada uno de los puertos RJ45 de un conmutador asigne una VLAN estáticamente. Una vez hecho eso, hay que ajustar el puerto ascendente como troncal, y aceptar todos los paquetes marcados con un tag que pertenezcan a VLANes.

4.4. VPN

El propósito de una VPN (Virtual Private Network) es unir redes LAN, VLAN o equipos a través de Internet mediante un túnel VPN. De esta forma se pueden tratar ambas redes o equipos como si fueran parte de una misma VLAN. Un trabajador que quiera acceder al servidor privado desde su casa necesita un túnel VPN a la red a la que pertenezca el servidor (o directamente al servidor).

Para conseguir esto primero debe de haber una conexión establecida entre los dos routers. Luego se deben de configurar ambos conmutadores con los mismos parámetros de:

- Rango de IPs de la red 1
- Rango de IPs de la red 2
- Contraseña (en caso de precompartirla)
- Servidor generador de claves (en caso de usar certificados)

Cuando se han establecido dichos parámetros y se compruebe que concuerdan los parámetros y las claves son compatibles o las contraseñas son iguales, se ha establecido el túnel VPN. A partir de dicho momento, todos los paquetes enviados a través del túnel encapsulan un paquete de la capa de enlace, indicando la IP local de los equipos emisor y receptor, después de las direcciones IP públicas. De esta manera, el paquete se manda por Internet sin modificar las IPs públicas, pero tampoco las privadas.

4.5. IPSec

Consiste en un conjunto de protocolos que pretende asegurar la red a niveles de autenticación, cifrado y gestión de claves. Es transparente para las aplicaciones y los usuarios y bien implementado en un cortafuegos o router protege toda la red.

A nivel de autenticación, añade (cuando sea necesario) un campo a la cabecera para confirmar que el remitente de ese mensaje es realmente quien es. Se utiliza AH (Autentication Header) como protocolo.

En cifrado se utiliza ESP (Encapsulating Security Protocol), que permite solo cifrado o cifrado y autenticación. Para cifrar, utiliza una clave privada con el fin de encriptar todo el paquete. Como es obvio, el destinatario debe de poseer nuestra

clave pública para descifrarlo. Si se le añade autenticación, después del cifrado añade un campo en la cabecera parecido al de AH.

Para gestionar las claves, proporciona herramientas para la creación de las mismas y para contactar con un servidor generador de claves, necesario para establecer una VPN con certificado. Esta función se consigue mediante el uso del protocolo IKE (Internet Key Exchange).

4.6. DMZ

El uso de una DMZ (DeMilitarized Zone) es un método para exponer un equipo o subred a Internet con algo de seguridad. Esta técnica evita que los equipos expuestos no puedan acceder al resto de la red local, por lo que aunque alguien consiguiera romper alguno de los equipos, no podría causar daños al resto de la red.

Todos los paquetes que recibe el router se reenvían a la DMZ, pasando antes por un cortafuegos. El uso ideal de esto para un servidor público es filtrar los paquetes que no vayan a los puertos 80 (HTTP) ni 443 (HTTPS), desecharlos y reenviarle los que sí pertenecen a esos puertos.

4.7. VoIP

Voice over Internet Protocol es una tecnología que permite el envío de datos de voz (tradicionalmente enviados analógicamente a través de la Red Telefónica Conmutada) por medio de Internet.

Los teléfonos fijos con esta capacidad están diseñados para conectar con un conmutador y un ordenador, pudiendo gestionar una VLAN propia y otra para el ordenador al que se conecta.

4.8. ACL

Una Lista de Control de Acceso nos permite clasificar los flujos de datos y agruparlos a nuestro gusto, permitiendo su acceso o no. Esto se hace en función de varios parámetros:

- IP Origen
- IP Destino
- Protocolo
- Puerto Origen (en caso de protocolo TCP o UDP)
- Puerto Destino (en caso de protocolo TCP o UDP)
- DSCP

Así, pues, podríamos clasificar todos los paquetes que tienen como origen y/o destino los puertos 80 y 443 como WWW, los que utilicen el protocolo RTCP como Control de VoIP, etc…

Cada una de las reglas involucradas en una lista es una Entrada (ACE). Las listas se ejecutan linealmente. Esto permite poner primero, por ejemplo, permitir los accesos SSH desde la red local y, en caso de que no sea desde esta red, denegarlo.

4.9. QoS

La calidad de servicio (Quality of Service) procura que los conmutadores de nivel 3 asignen a una serie de paquetes cierta prioridad a la hora de enviarse a otra red (generalmente a la puerta de enlace), así como un máximo de ancho de banda. Antes de nada, debemos de filtrar y categorizar el tráfico de nuestra red.

Una vez realizada la clasificación, asignamos una prioridad, un caudal máximo y una tasa máxima de ráfaga a cada uno de los flujos. Para que se cumplan nuestras

restricciones, se pueden usar Servicios integrados (IntServ) o Servicios Diferenciados (DiffServ).

4.9.1. Servicios integrados

Este tipo de servicios opera reservando dinámicamente recursos para procesar un flujo de datos. Los routers almacenan la información sobre cada flujo.

4.9.2. Servicios diferenciados

En los servicios diferenciados, en vez de actuar sobre los flujos de datos, se marcan los paquetes individualmente y en función de la marca se les aplica un tratamiento u otro.

A cada paquete se le añade un campo de 8 bits en la cabecera, donde 6 de ellos indican la prioridad del paquete; siendo 46 (en codificación DSCP) el envío expedito o asegurado (EF) y 0 el Best Effort. El resto de tipos se indican con dos dígitos en clasificación Assured Forwarding, indicando el primero la clase (entre 1 y 4, inclusives ambos), y el segundo la prioridad dentro de ella (entre 1 y 3). Esto nos da, contando con BE y EF 14 tipos de flujo, aunque se pueden usar todos los DSCPs, saliendo del estándar.

IntServ presenta problemas de escalabilidad. Los servicios diferenciados no son tan estrictos como los integrados, pero se consideran suficiente. Estos servicios se complementan el uno al otro. Lo más común es que se utilice IntServ en los nodos de acceso y DiffServ en los enlaces troncales.

Para los conmutadores de nivel 2 existe una tecnología similar, Class of Service, que actúa sobre la capa de enlace, en vez de hacerlo sobre la de red.

4.10. Arquitectura empresa Cisco

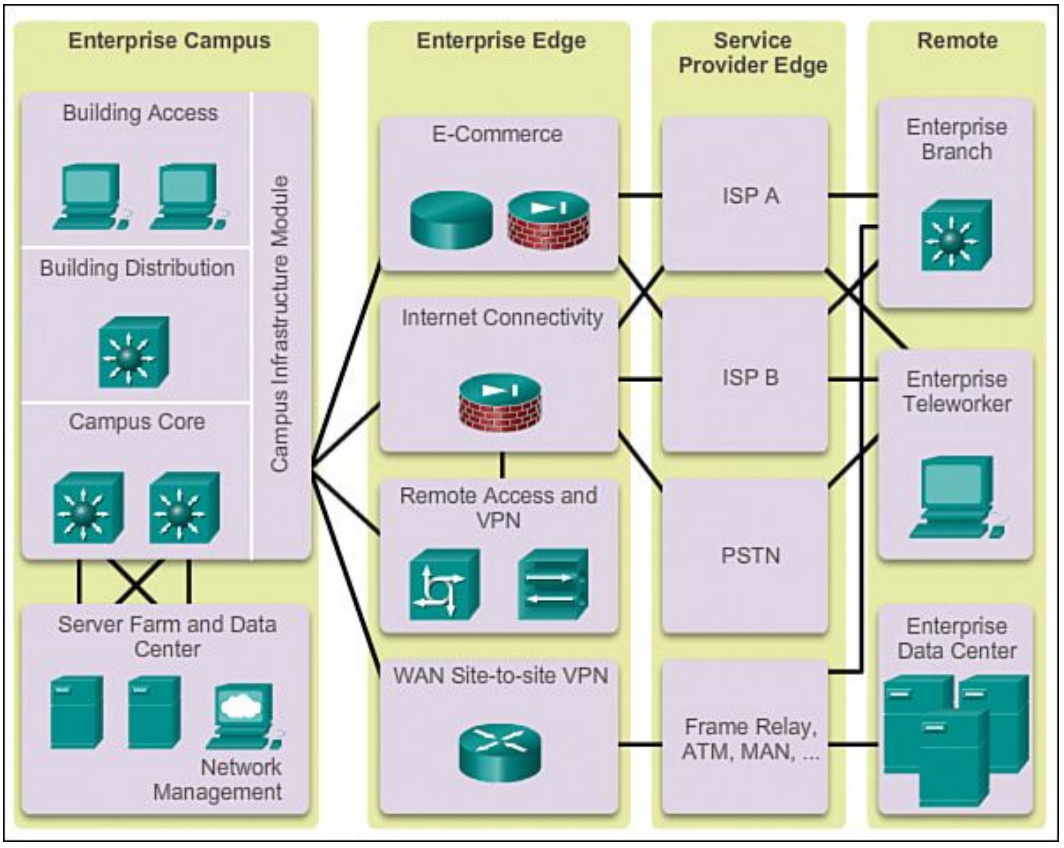


Ilustración 4.1

Como se puede apreciar en la ilustración 4.1, los estándares de Cisco separan la red global de una empresa para una mayor modularidad en cuatro capas:

- **Campus de la empresa**

  La red local del edificio o campus, separando equipos de comunicaciones en Core (acceso al exterior), Distribución (balanceo de carga) y Acceso

- **Borde de la empresa**

  En esta capa se gestiona quienes pueden salir al exterior o entrar y de qué forma. Aquí se encuentra el servidor público, el router de acceso y la gestión de VPNs

- **Borde de los proveedores de servicio**

  La parte de la red que no podemos configurar internamente, pero si las conexiones a ella. Contiene las redes de las compañías de Internet que hayamos contratado, junto con el servicio de teléfono y los mecanismos de VPN propios del proveedor.

- **Remota**

  El resto de la empresa que está fuera del campus, como otras sedes, trabajadores remotos o el centro de datos

4.11. Operadores

4.11.1. Movistar

Nos ofrece servicios VoIP y VPN sin ningún tipo de problema.

Ofrecían Frame Relay a través de Uno de Telefónica Data por 6.050€ de cuota de conexión y hasta 4.719€ de cuota mensual por 2 Mbps.

Con Frame Relay a través de BT Ignite cobraban 1.815€ de cuota de conexión y 0€ cuota mensual.

Aunque son servicios casi obsoletos y precios antiguos, nos ayudan a hacernos una idea de lo que podría costar MPLS.

4.11.2. Vodafone

VoIP sin ningún tipo de complicación. Hay que llamar al soporte técnico para que habiliten VPN, pero opera correctamente tras hacerlo.

4.11.3. Orange

VoIP funciona perfectamente. Configurar VPN es bastante complejo y seguramente requiera un router distinto al que nos ofrecen por defecto al contratar sus servicios.

Todos ellos ofrecen MPLS, pero no ofrecen ningún dato sobre ello sin proporcionar los datos de una empresa real, ni precios, ni velocidades.

5. MATERIALES Y MÉTODOS

5.1. Materiales

5.1.1. Router Cisco RV320

Este conmutador es muy completo: Nos permite configurar QoS, VLANes, VPNs, Cortafuegos, DMZ, etc… Además está preparado para tener dos conexiones WAN, algo muy útil si queremos tener un servidor público siempre activo, independientemente de las caídas o subidas de latencia que se deban a nuestro proveedor de Internet, o simplemente queremos tener las conexiones de VoIP o VPN por otro operador.

Posee tan solo cuatro puertos LAN y puede implementar un máximo de 7 VLANes, pero funciona a 1000 mbps. Si queremos utilizar una DMZ tenemos que cambiar la configuración de la WAN2 a DMZ, lo que nos hace

tomar la decisión de si queremos dos salidas a Internet o una zona desmilitarizada.

5.1.2. Switch Cisco SG300-10

Un equipo que también funciona a 1000 mbps, con 10 puertos LAN configurable de forma sencilla, soportando hasta 4.000 VLANes. Un gran rendimiento, con el único inconveniente de que tarda en torno a unos 10 minutos en iniciarse y unos 20 en reiniciarse a la configuración por defecto, aunque una vez configurado correctamente no supone ningún problema.

Permite una configuración muy personalizable de las ACLs y CoS, ajustándose a cualquier necesidad de la empresa de la que forme parte.

6. DISEÑO DE LA RED

6.1. Esquema de red

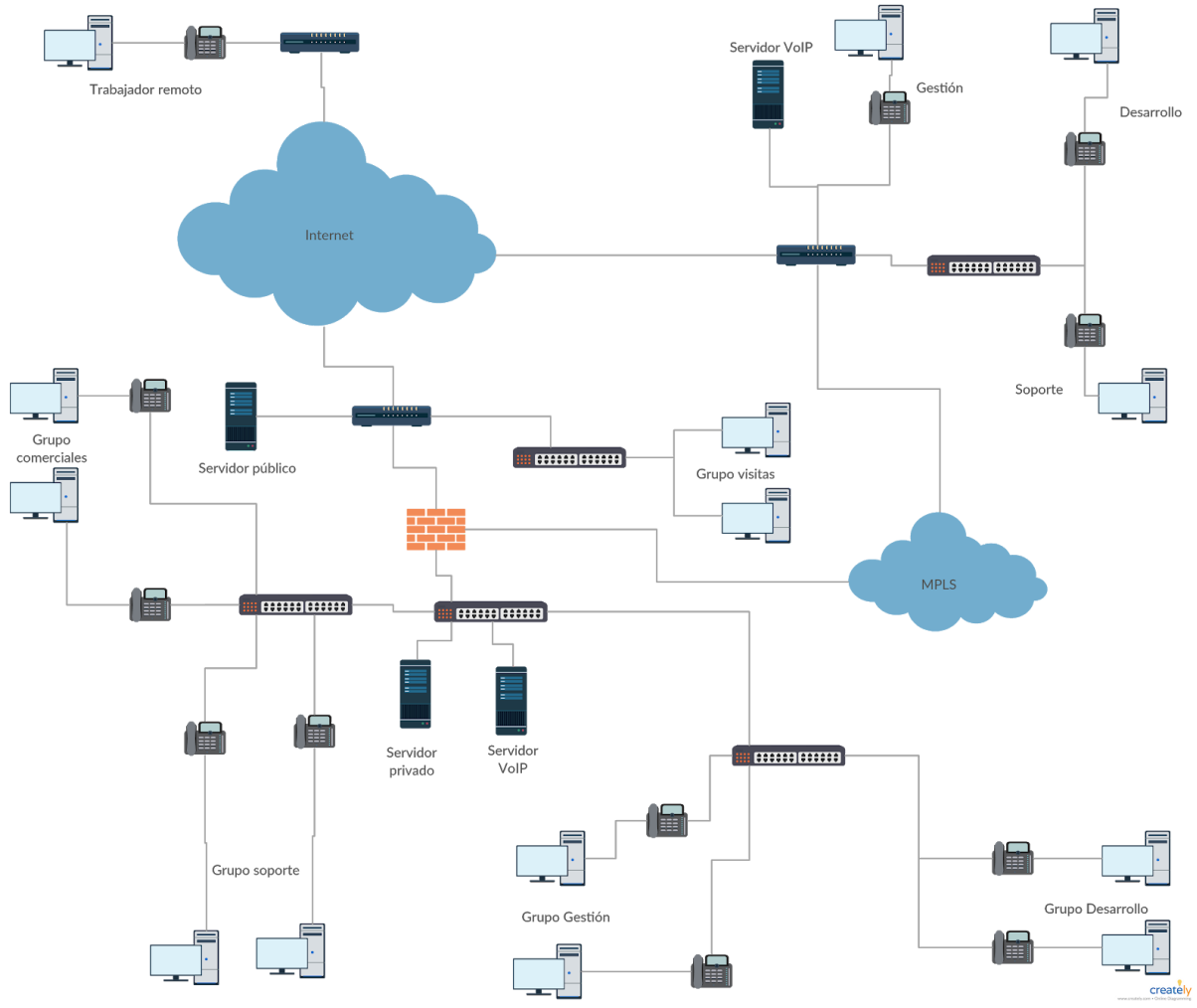


Ilustración 2.1

Con este diseño de red contemplamos la sede central (parte inferior), una sede más sencilla y pequeña (parte derecha) y el caso de un trabajador remoto (parte superior izquierda).

La sede central se compone de una parte pública, con un servidor (DMZ) y provee con acceso a Internet a los clientes o visitas; y de una parte privada, a la que

se accede a través de un cortafuegos. Éste permite solo el acceso desde una VPN directa a él o MPLS.

Dentro de la parte privada, tenemos dos servidores: uno de VoIP y otro con los datos sensibles de la empresa.

La sede menor tiene su propio servidor VoIP (para llamadas internas) y conectan con la sede central mediante MPLS directamente al cortafuegos.

En el caso del trabajador remoto, para conectarse a la sede central necesita establecer un túnel VPN a través de Internet.

El diseño de las VLANes sería el siguiente:

ID	Nombre	Equipos
2	Desarrollo	Grupo de Desarrollo
3	Comerciales	Grupo de Comerciales
4	Soporte	Grupo de Soporte
5	Servidor privado	Servidor privado
6	DMZ	Servidor público
25	Visitas	Grupo de Visitas
99	Gestión	Grupo de Gestión
100	VoIP	Teléfonos VoIP y servidores VoIP

Tabla 6.1

El grupo de Gestión serían los únicos capaces de configurar los conmutadores.

6.2. Calidad de Servicio

Supongamos que la transferencia máxima es de 100 Mbps. Aunque en la actualidad los anchos de banda superan con creces esta fibra, los equipos de

comunicaciones y cables Ethernet de 1.000 Mbps (Categoría 5 o más) son más caros y, para este caso, innecesarios.

Se preven como máximo simultáneamente unas 10 videollamadas con un ancho de banda estimado de 768 kbps cada una, 15 conferencias VoIP de 64 Kbps, 3 conexiones SSH de unos 2 Mbps y 6 accesos a base de datos de 1,5 Mbps.

La clasificación de datos sería la siguiente:

Clase	**Protocolo**	**Puerto origen**	**Puerto destino**	**IP origen**	**IP destino**
Video	TCP	- (cualquiera)	8080	-	-
		8080	-	-	-
VoIP	RTP	-	-	-	-
Control VoiP	RTCP	-	-	-	-
SSH	TCP	-	22	-	-
		22	-	-	-
BBDD	TCP	-	-	-	192.168.7.101
		-	-	192.168.7.101	-
WWW	TCP	-	80/443	-	-
		80/443	-	-	-
Resto	-	-	-	-	-

Tabla 6.2

Tanto el router Cisco SV320 como el switch Cisco SG300-10 funcionan con 4 colas físicas, por lo que ajustaremos la QoS a esto, siendo la 4º la más prioritaria.

La siguiente tabla indica la Calidad de Servicio:

Clase	Prioridad (DSCP)	Cola física	Ancho de banda (kbps)	Ráfaga (B)	Exceso
Video	46 (EF)	4	10240 (10mbps)	3000	Descartar
VoiP	38 (AF43)	4	1024 (1mbps)	3000	Descartar
Control VoIP	36 (AF42)	4	256 (0,25mbps)	3000	Pasar a BE
SSH	30 (AF33)	3	7168 (7mbps)	3000	Pasar a BE
BBDD	28 (AF32)	3	10240 (10mbps)	3000	Pasar a BE
WWW	22 (AF23)	2	15360 (15mbps)	3000	Pasar a BE
Otro	0 (BE)	1	Ninguno	Ninguno	Descartar

Tabla 6.3

Esta limitación de ancho de banda suma un total 43,5 mbps, dejándonos casi un 60% en BE, con lo que dejamos suficiente ancho de banda para el resto de datos. Los anchos de banda indicados en la Tabla 6.3 son mayores que la cantidad exacta necesaria esperada, por si se produjera un aumento por cualquier causa.

7. IMPLEMENTACIÓN

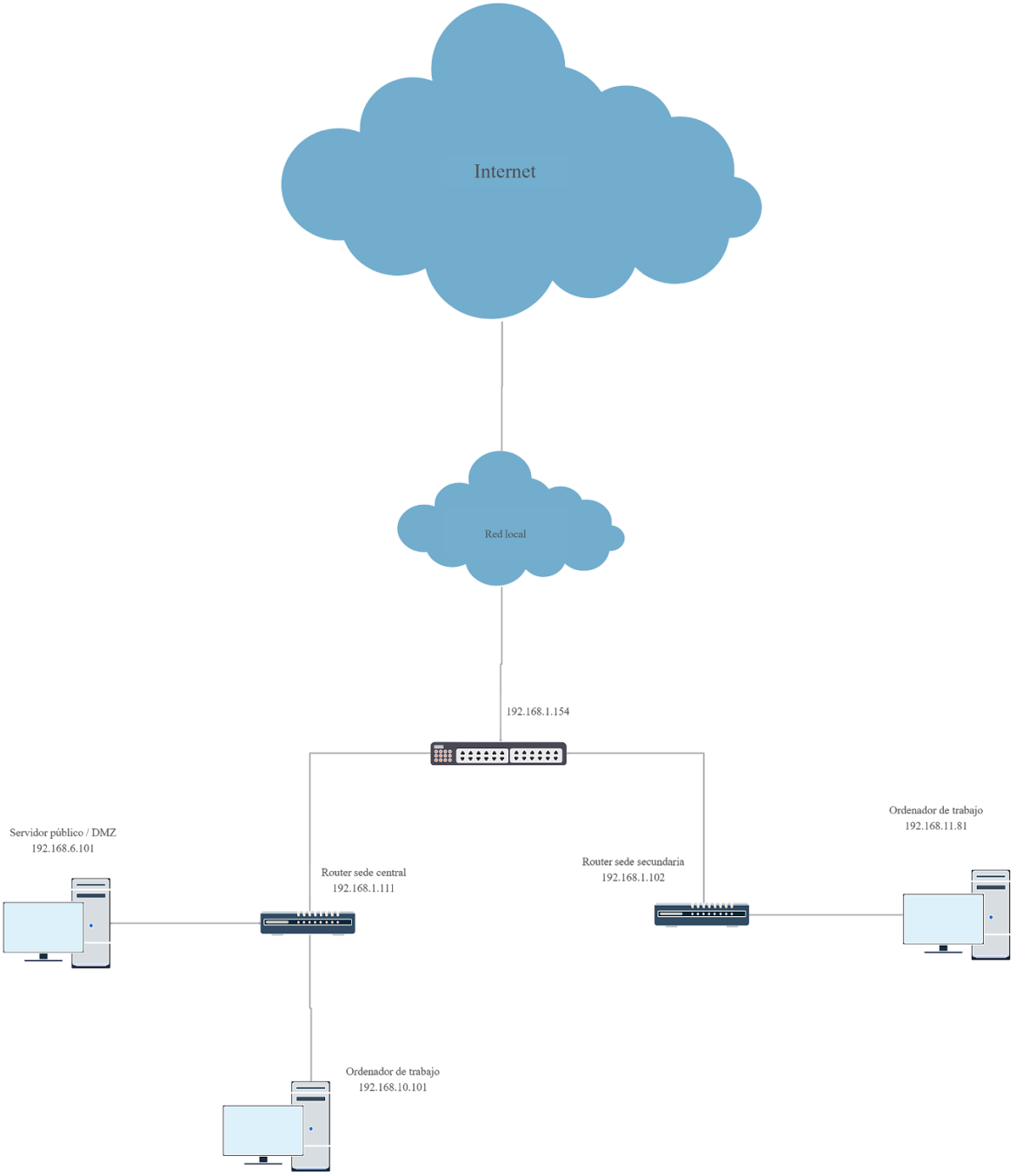


Ilustración 7.1

Como se puede apreciar en la Ilustración 7.1, con una única entrada a la red de mi casa conectamos el switch para poder separar las dos sedes. En la sede central tenemos el servidor público / DMZ que debería de ser accesible desde cualquier

parte de la red de la casa sin ningún tipo de configuración y un ordenador de un grupo de trabajo cualquiera, con el que debe de poder acceder el ordenador de la sede secundaria a través de una VPN.

El primer problema al que nos enfrentamos es que solo tenía a mi disposición dos ordenadores para esta implementación. Uno de ellos representa al conectado a la sede secundaria, mientras que el otro tenía que rotar entre los dos equipos de la sede central, en función de lo que se quisiera comprobar.

El segundo es que los routers solo soportan 7 VLANes, lo que impide implementar todos los grupos de trabajo, por lo que solo se han indicado un par de ellos

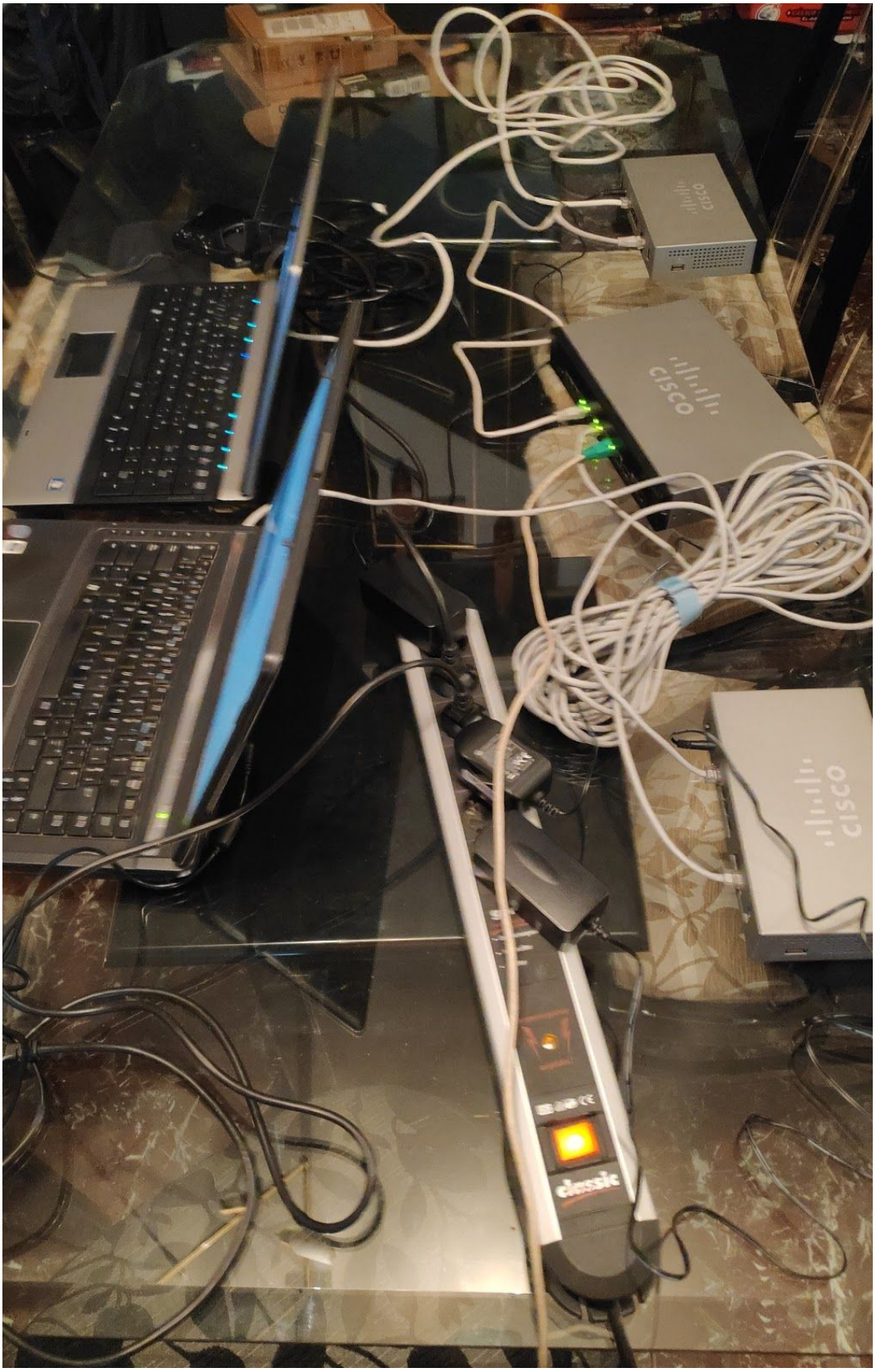


Ilustración 7.2

En la Ilustración 7.2 se puede apreciar la instalación física de la parte de la red implementada. El ordenador de la parte superior es el que pertenece a la sede central y tiene un servidor Apache2 encendido para comprobar la conexión. El portátil inferior es el que pertenece a la sede secundaria que hará de cliente.

De arriba hacia abajo se encuentran en la parte derecha de la imagen el router de la sede central, el switch que conecta los conmutadores de nivel 3, y el router de la sede secundaria, conectados como se indica en la Ilustración 7.1

7.1. Switch

La implementación de este equipo es un poco caótica, ya que incorpora parte de QoS y VLANes que pertenecería a cualquiera de las sedes, no a la unión de ellas y, a la vez, debe de interconectar ambas redes. Por lo tanto se implementa todo lo posible, pero no se hace uso de la VLANes dada su posición en la red.

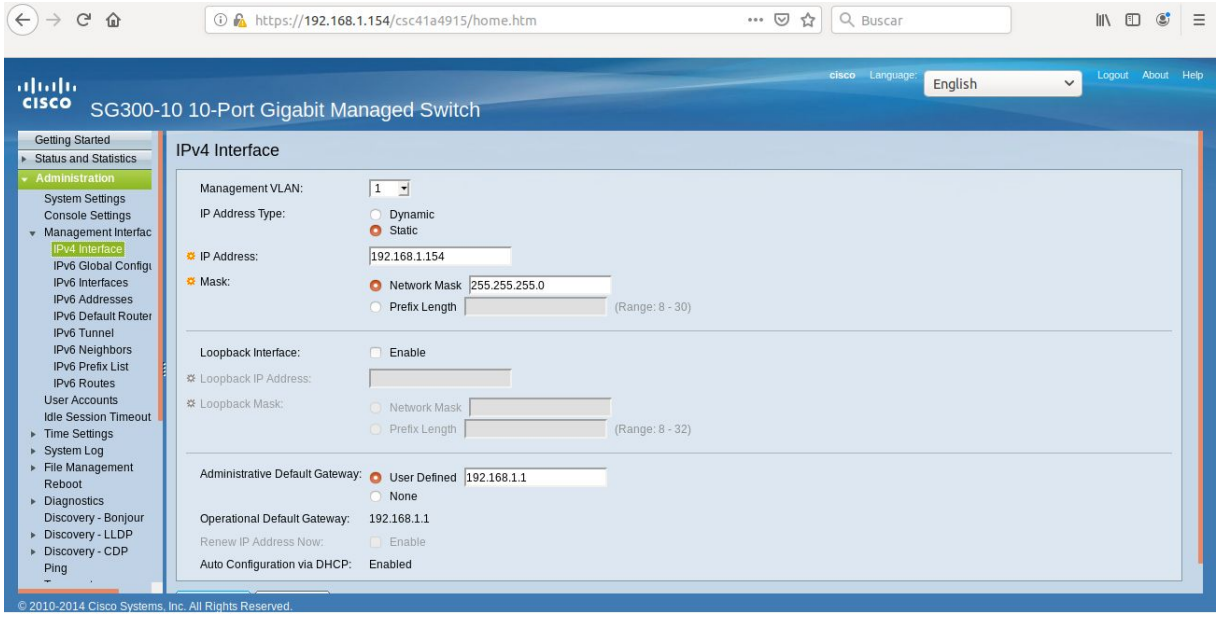


Ilustración 7.3

En este equipo lo primero que hay que configurar, antes de conectarlo ascendentemente a algún router, es fijar la dirección IP, pues al conectarlo obtiene

una dirección a través de DHCP y luego cuesta encontrar la dirección en concreto para seguir configurándose.

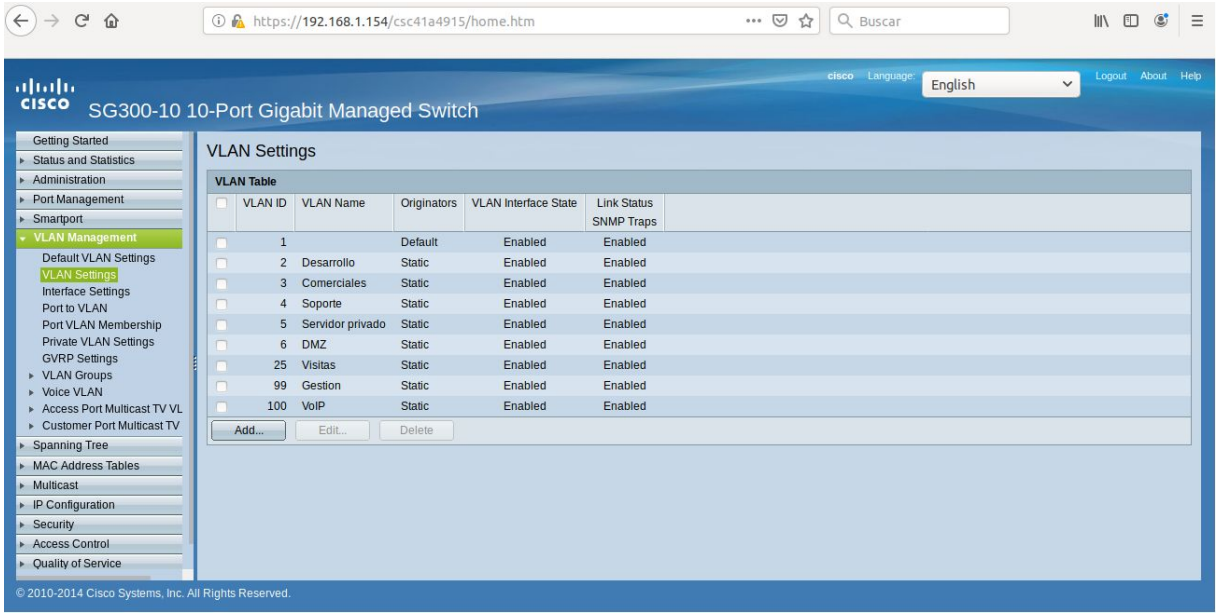


Ilustración 7.4

Continuamos añadiendo las VLANes. Utilizamos los IDs 25 para visitas y 100 para VoIP ya que por defecto los routers de Cisco utilizados hacen uso de esos IDs para dichos grupos. El 99 para la de gestión es un estándar.

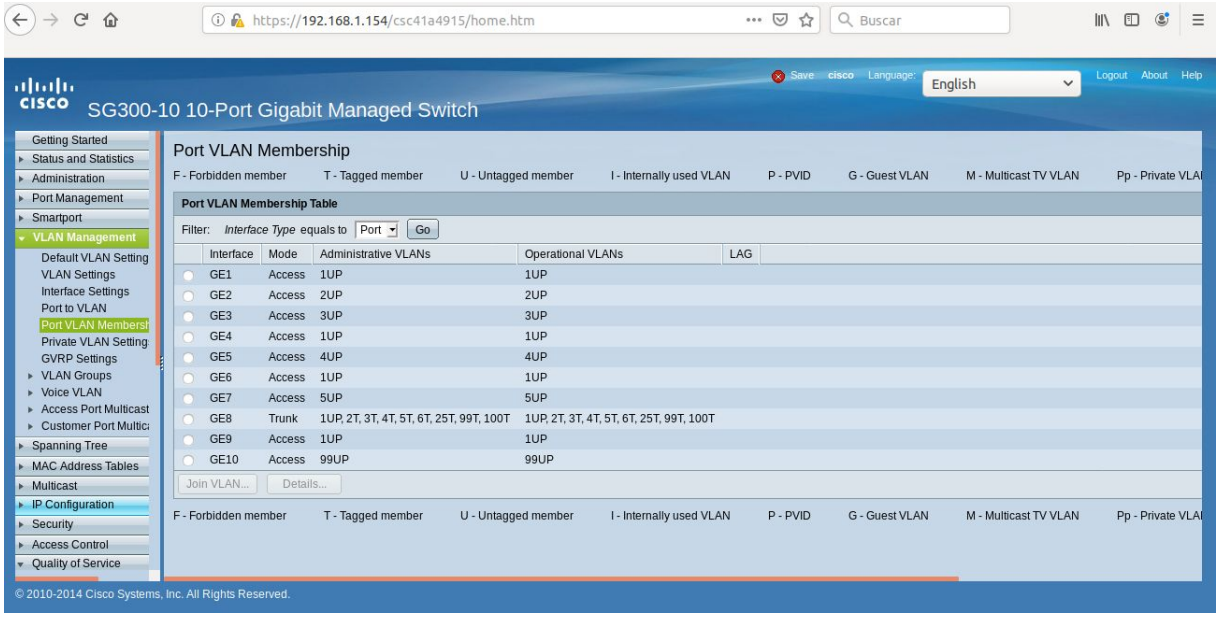


Ilustración 7.5

Asignamos una VLAN a cada puerto vacío, y dejamos la VLAN 1 para conectar los routers. El puerto 1 es para la configuración directa, el 4 conecta con la sede central, el 6 con la secundaria y el 8 con la red de la casa. El enlace ascendente es el único troncal, y debemos de poder enviar los paquetes de todas las VLANes; de la 1 sin marcar y los demás marcados.

7.2. Router sede Central

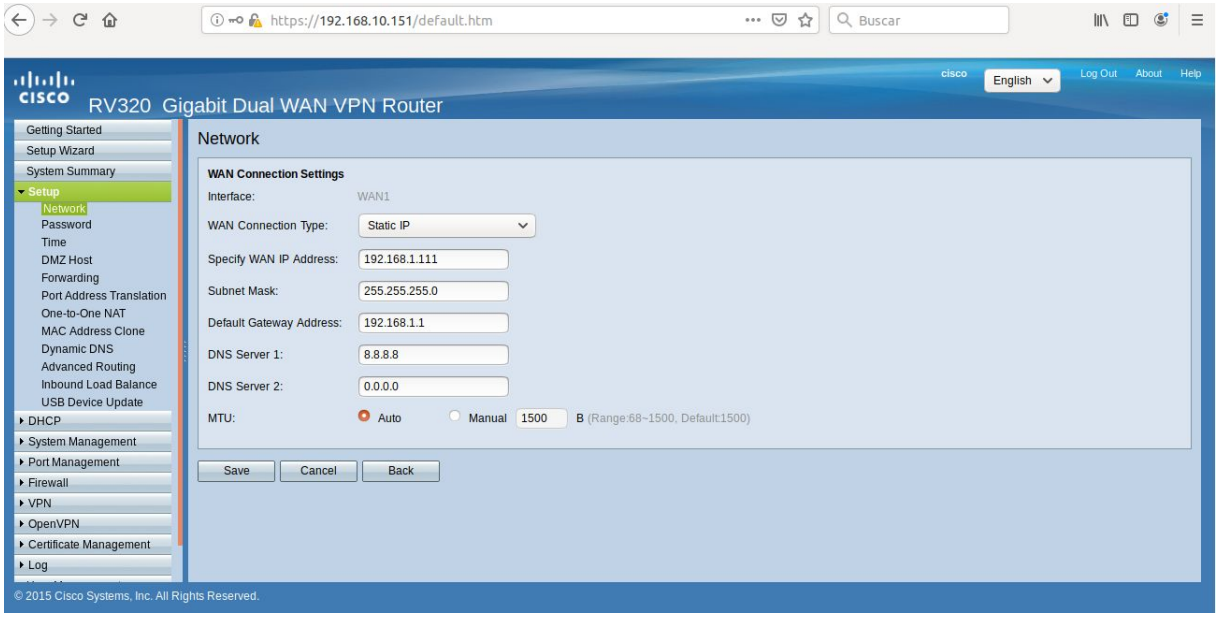


Ilustración 7.6

Lo primero que configuramos de este equipo es la IP pública, que hacemos estática y asignamos la dirección 192.168.1.111, la máscara de red (255.255.255.0), la puerta de enlace (192.168.1.1, la salida a Internet), el DNS al 8.8.8.8 (el de Google) y cambiamos la dirección IP de la VLAN 1 o por defecto de la 192.168.1.0 a la 192.168.10.0 . Esto es para diferenciar la red de la casa de la implementada en la sede central. Otra posible solución hubiese sido utilizar una máscara de red distinta.

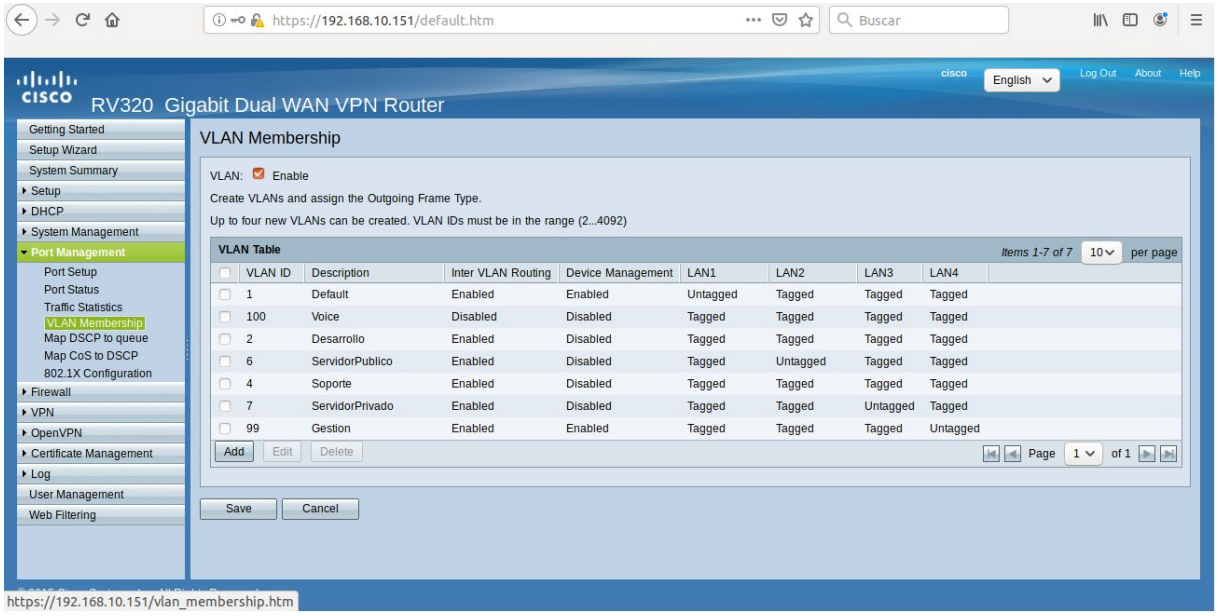


Ilustración 7.7

Después creamos las distintas VLANes. Todas tienen Internetworking (excepto la de VoIP, ya que solo conecta consigo misma) para acceder al servidor privado, aunque hay varias formas de hacerlo accesible para todas, ésta parecía la más correcta y sencilla para la implementación realizada. La VLAN 6 para el servidor público tiene Internetworking activo por si se necesitan hacer pruebas, ya que el servidor accesible desde Internet está en la DMZ.

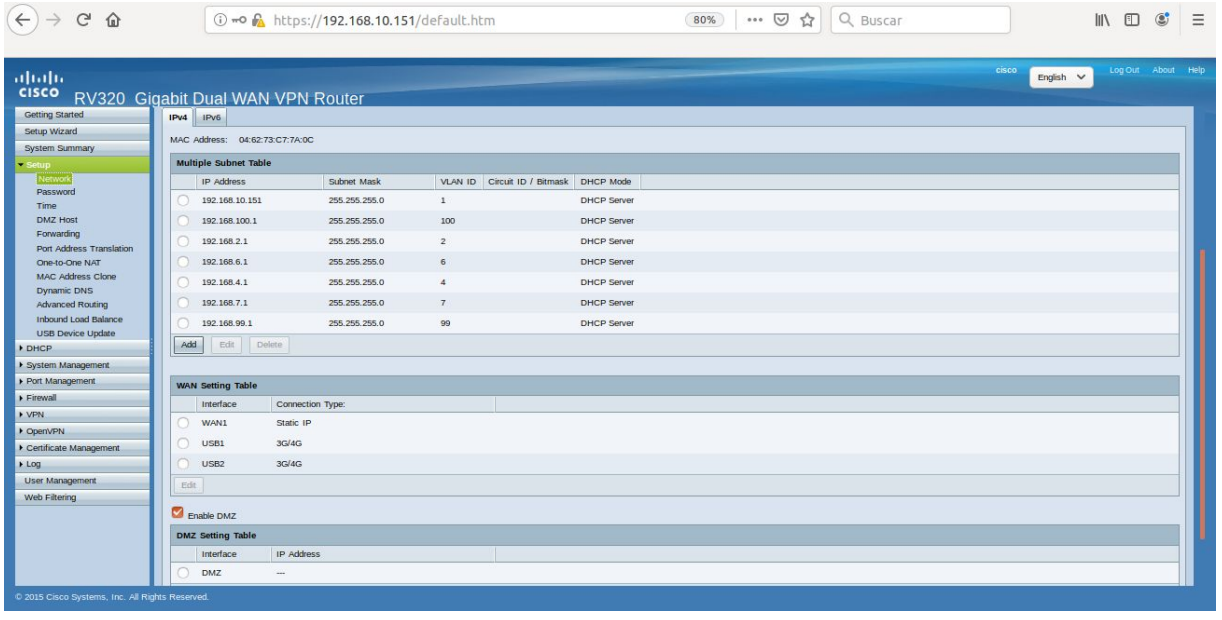
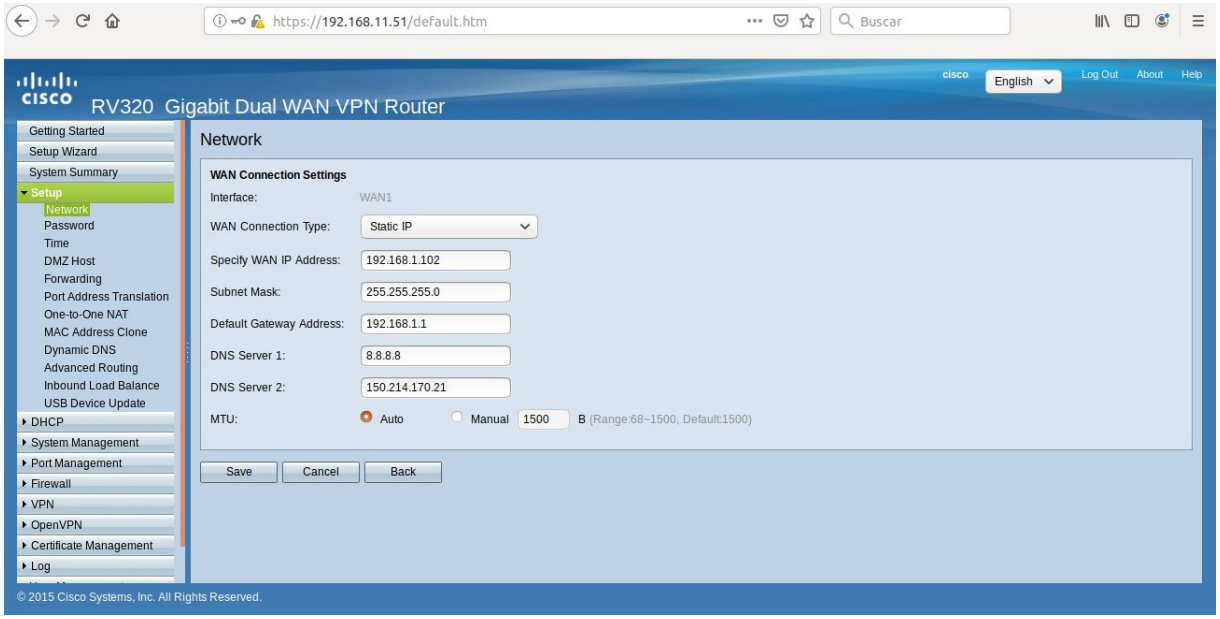


Ilustración 7.8

En el Network del Setup, debemos de hacer click en “Enable DMZ”, para tenerlo preparado a la hora de montar la DMZ. En la Ilustración 7.8 queda enmarcada la situación de todas las VLANes.

7.3. Router sede secundaria



El primer cambio a realizar es el mismo que en la sede central, la IP pública (192.168.1.102), la máscara de red (255.255.255.0), la puerta de enlace (192.168.1.1) y el DNS (8.8.8.8).

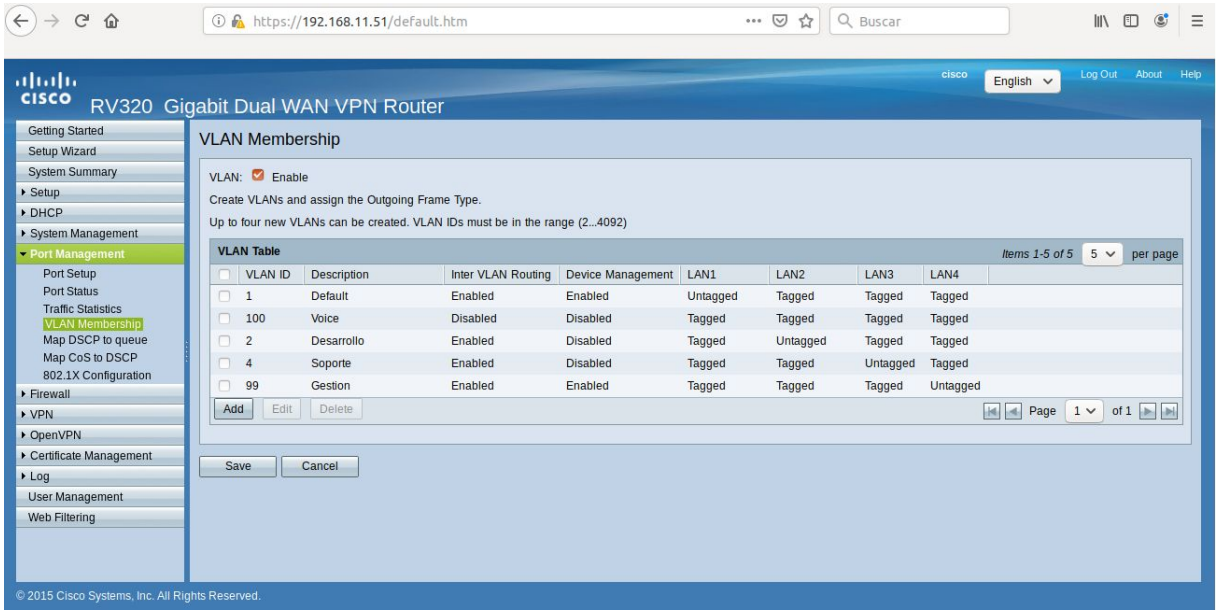


Ilustración 7.10

Al igual que hicimos anteriormente, implementamos las VLANes de la secundaria. En este caso no hacen faltan los servidores público y privado, pues están centralizados.

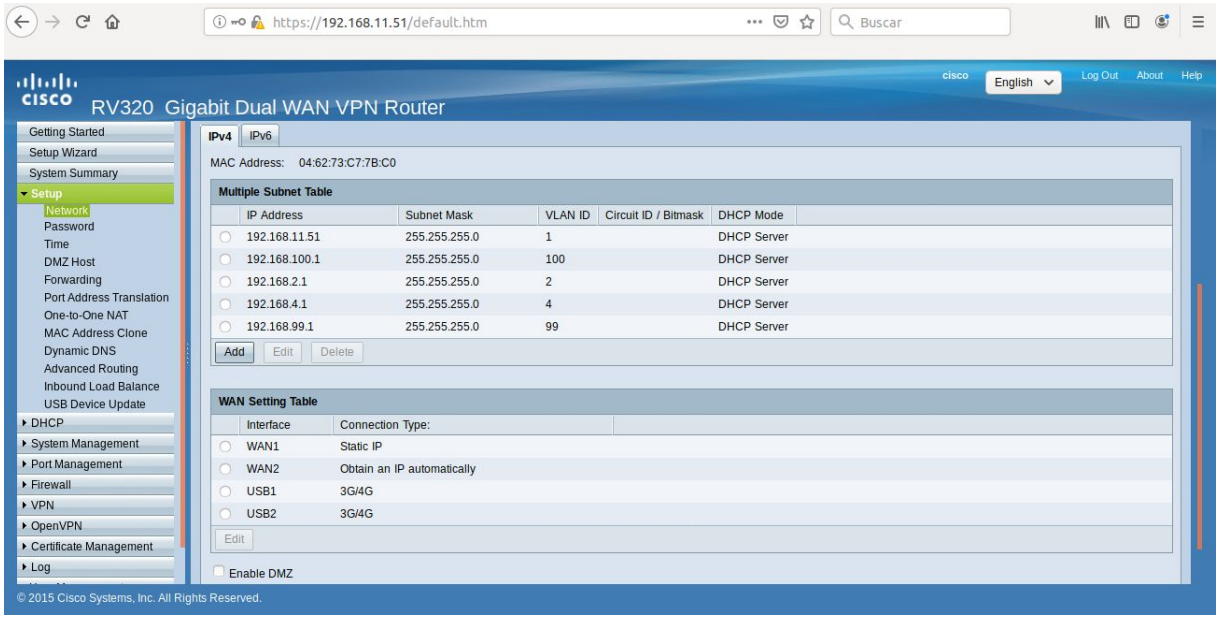


Ilustración 7.11

Al igual que pasamos la VLAN 1 de la sede central a la dirección 192.168.10.0, pasamos la de la secundaria a 192.168.11.0, para cuando se monte la VPN detecte que es una red diferente y lo mande a la puerta de enlace.

7.4. VPN

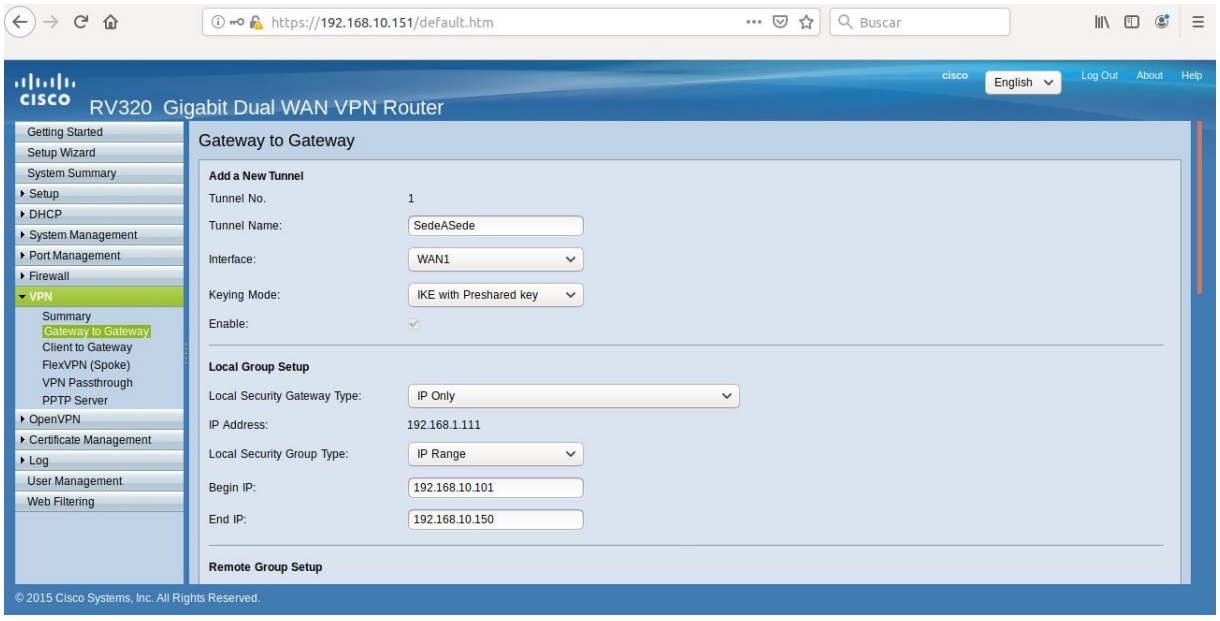


Ilustración 7.12

Para conectar ambas sedes, debemos crear un túnel VPN de sede a sede. Vamos a realizarlo con clave precompartida, pues es más sencillo y suficientemente seguro en este caso. En la sede central conectamos los equipos en el rango 192.168.10.101 - 192.168.10.150, dejando fuera el router (192.168.10.151)

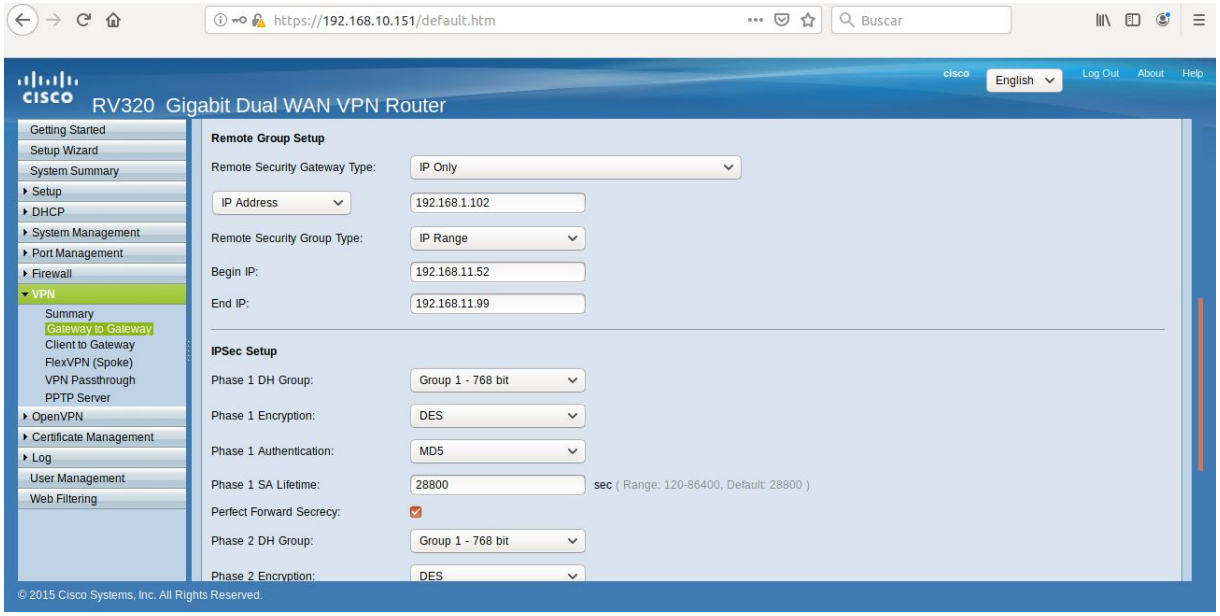


Ilustración 7.13

De la red secundaria enlazamos los equipos en el rango 192.168.11.52 - 192.168.11.99, también dejando fuera el router.

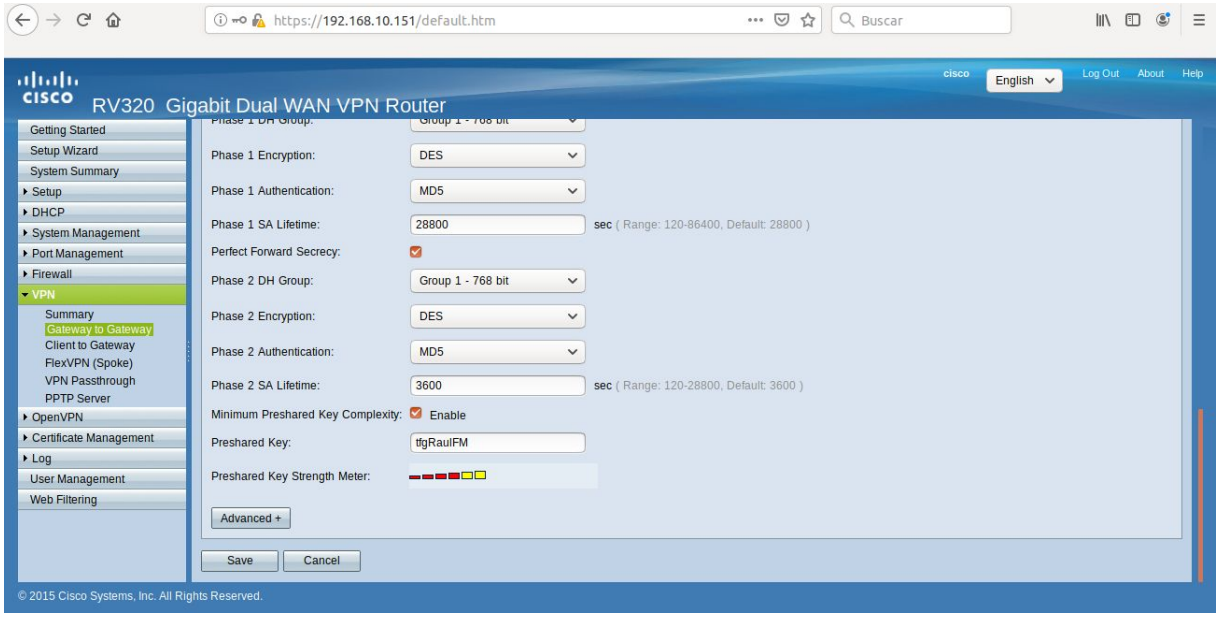


Ilustración 7.14

Por último introducimos la clave común y guardamos. Repetimos los mismos pasos en el router de la sede secundaria, pero intercambiando los parámetros de los grupos local y remoto.

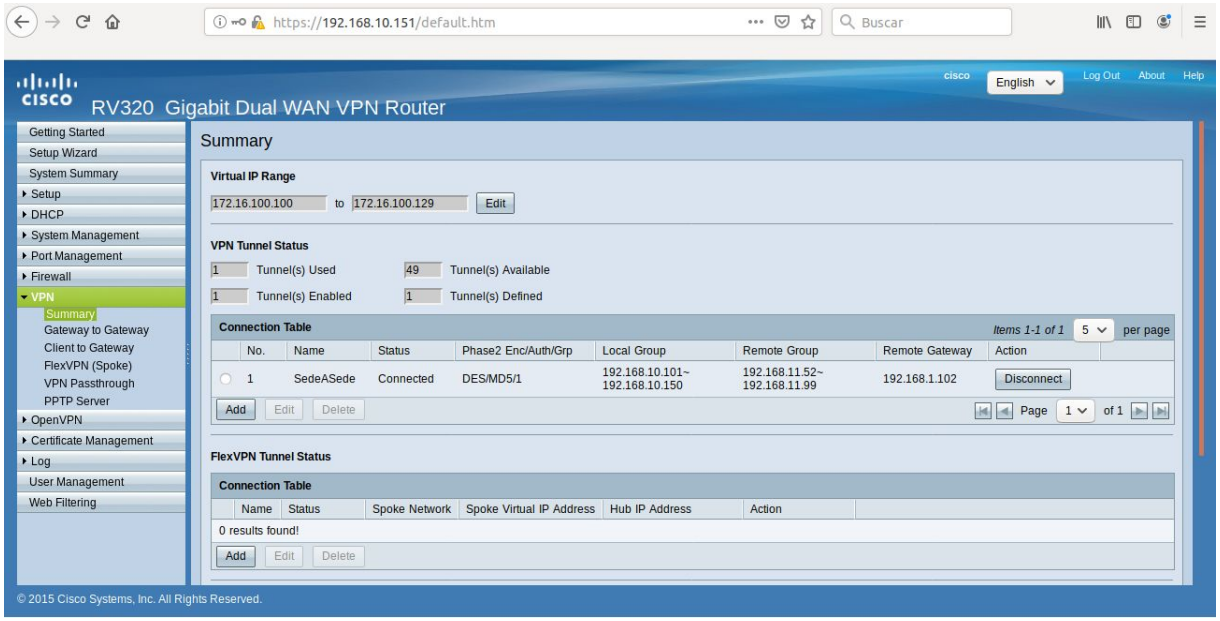


Ilustración 7.15

Una vez completados esos pasos, conectar y desconectar ambas redes entre sí es tan sencillo como como clickear sobre el botón de “Connect” / ”Disconnect” en el Summary de VPN de cualquiera de los equipos.

7.5. DMZ

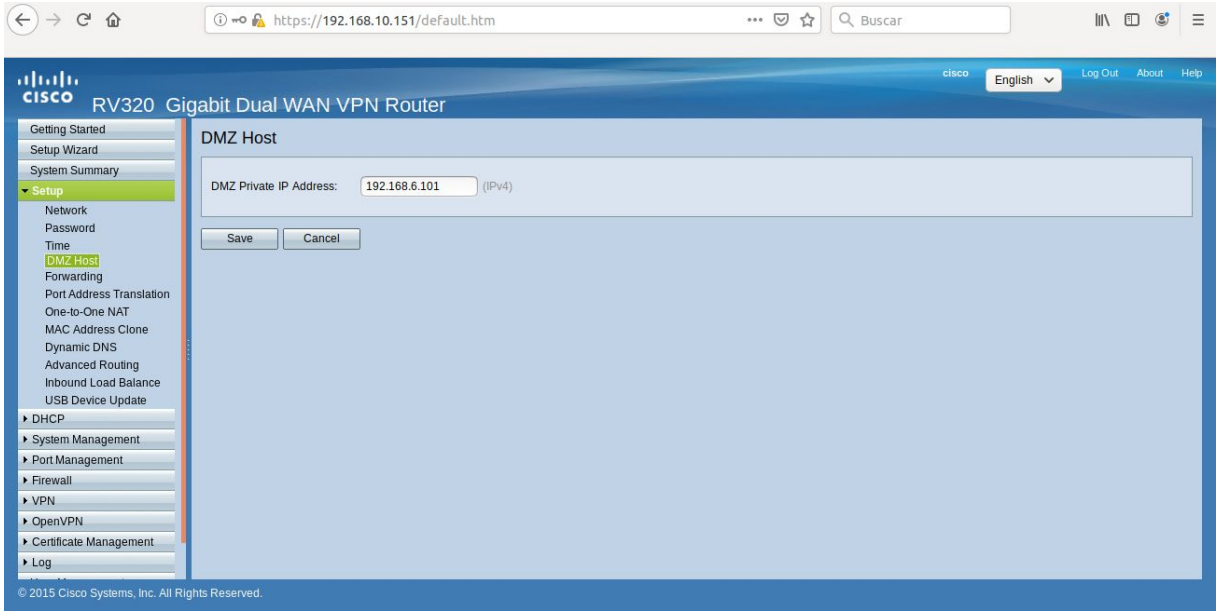


Ilustración 7.16

Como la DMZ ya estaba activada en el router de la sede central, tan solo hace falta especificarle una dirección IP de este (vamos a utilizar 192.168.6.101) y conectarlo al puerto “WAN2 / DMZ”.

7.6. QoS

En el punto 7.1 (Implementación del Switch) se informaba de que la Calidad de Servicio se iba a implementar en el Switch, aunque su funcionamiento sería el correcto si estuviera por debajo del router de cualquiera de las sedes, pero la falta de infraestructura lo impide.

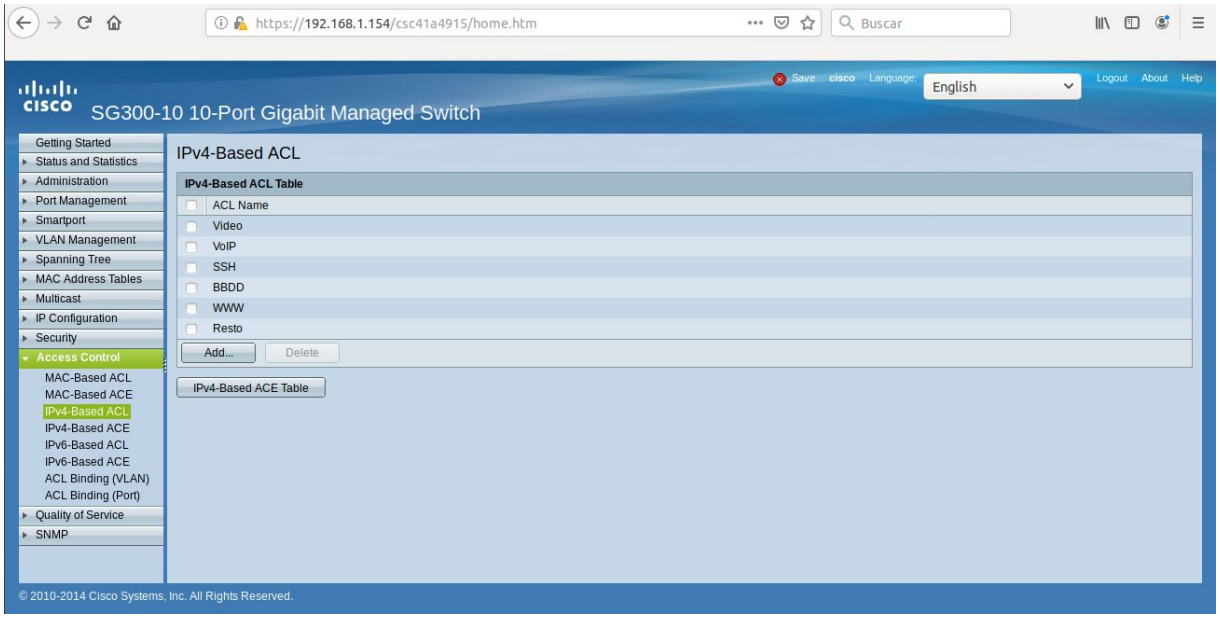


Ilustración 7.17

El primer paso es crear las ACL, actualmente sin entradas. Aunque en el diseño se separaba VoIP de Control VoIP, no es posible realizarlo en este equipo, pues en la lista desplegable de protocolos no aparecen ni RTP ni RTCP.

La prioridad que se les ha dado a las ACEs es el DHCP asignado, y desciende linealmente desde ese valor conforme se van añadiendo entradas a la lista.

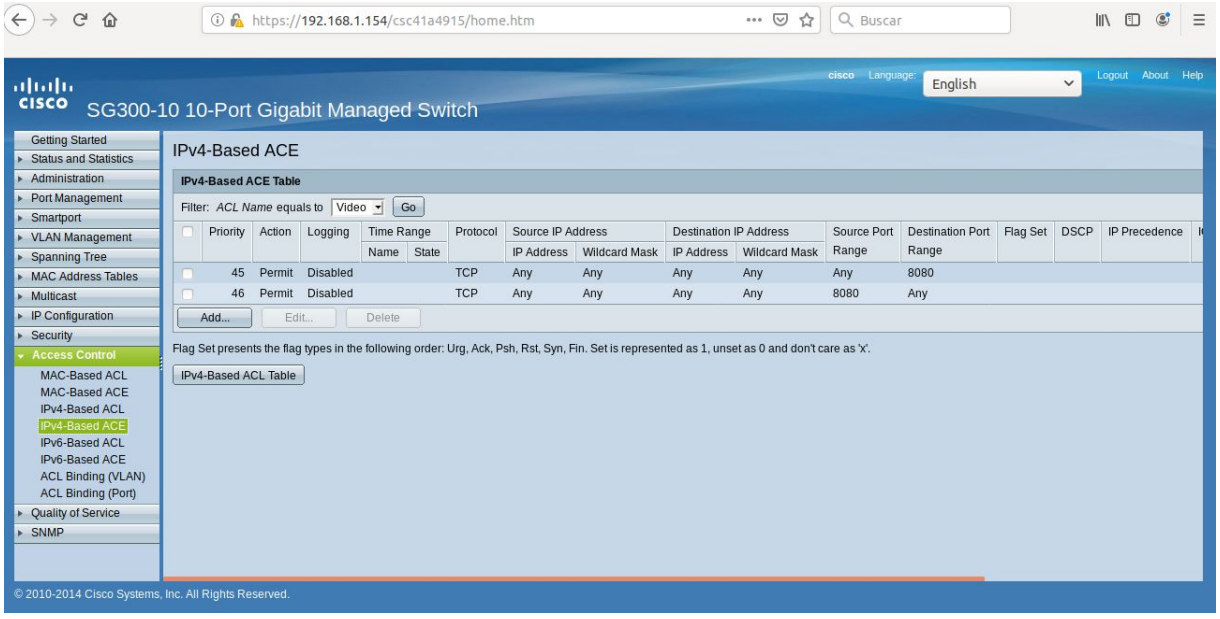


Ilustración 7.18

Para la clasificación de comprobamos si se utiliza el puerto 8080 TCP como origen o destino.

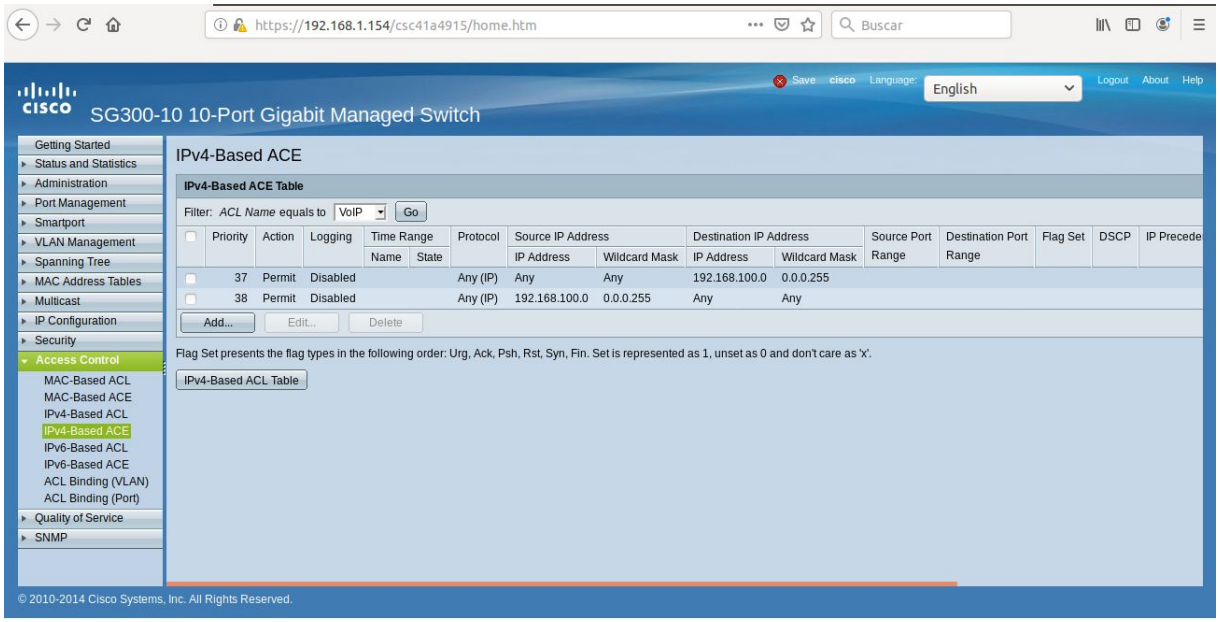


Ilustración 7.19

Para VoIP, como no podemos seleccionar los protocolos RTP ni RTCP, vamos a comprobar si los paquete están destinados u originados de la VLAN de VoIP.

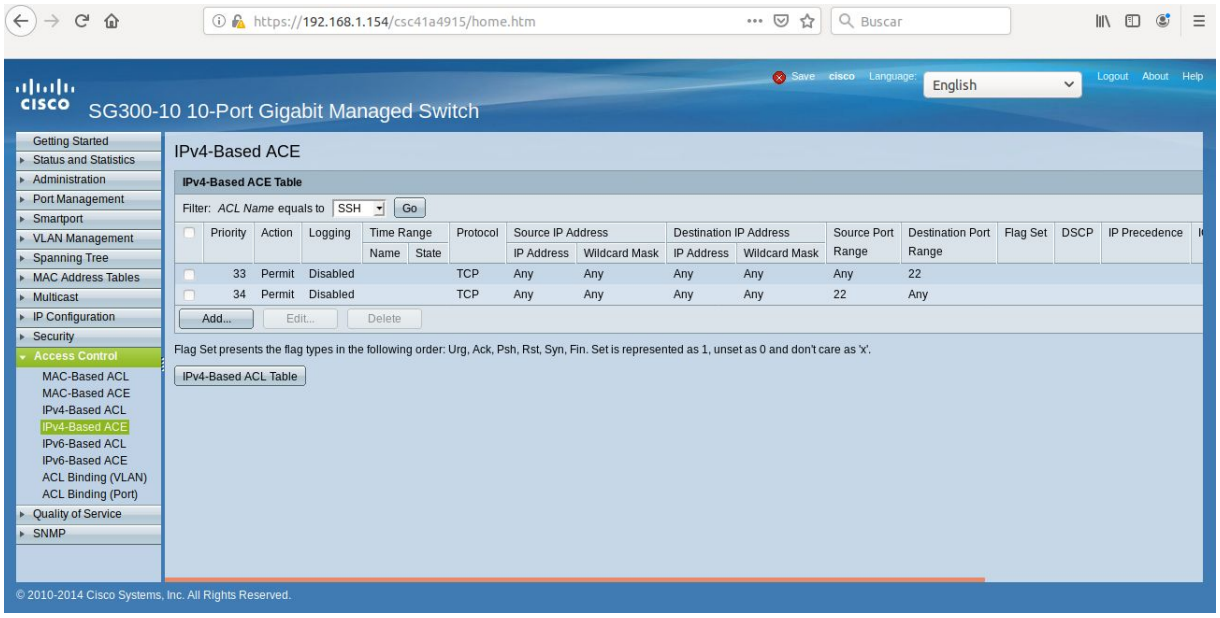


Ilustración 7.20

La clasificación SSH comprueba si utiliza el puerto 22 del protocolo TCP.

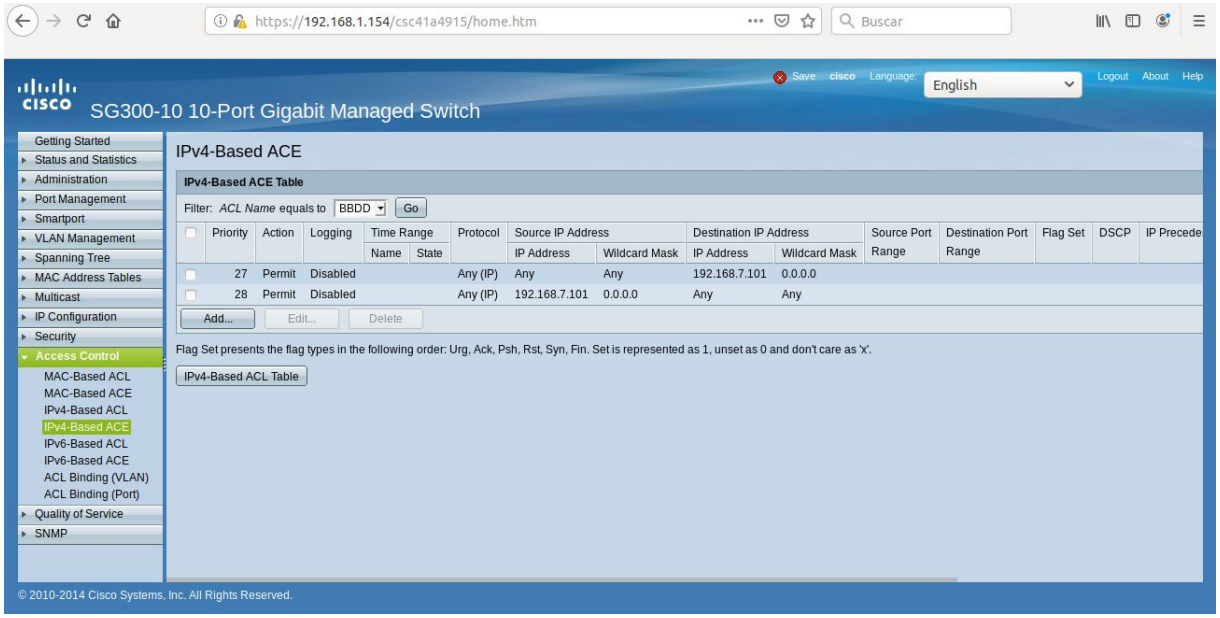


Ilustración 7.21

La ACL de BBDD comprueba si la dirección de origen o destino coincide exactamente (por tener la máscara wildcard 0.0.0.0) con la dirección 192.168.7.101 (la del servidor privado)

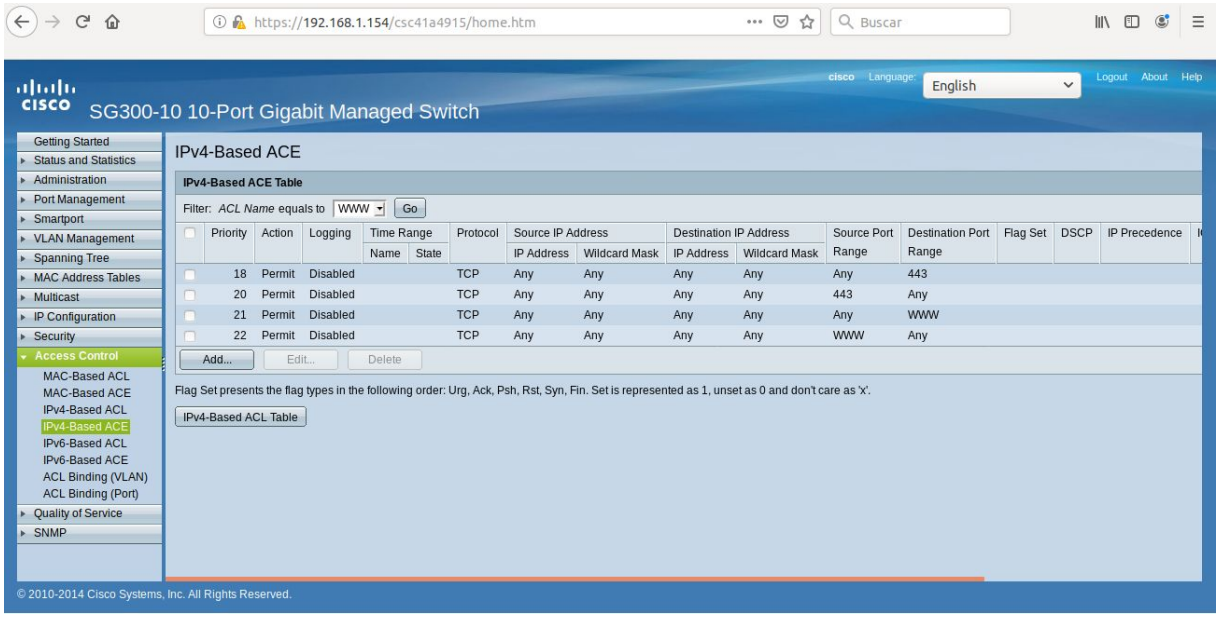


Ilustración 7.22

Para WWW tenemos que verificar si utiliza el puerto 80 (HTTP) o el 443 (HTTPS).

En todas estas ACLs permitimos todos los flujos dadas las dimensiones de la implementación. Sin embargo, en una red real habría que denegar todos los accesos SSH desde el exterior, entre otras tareas.

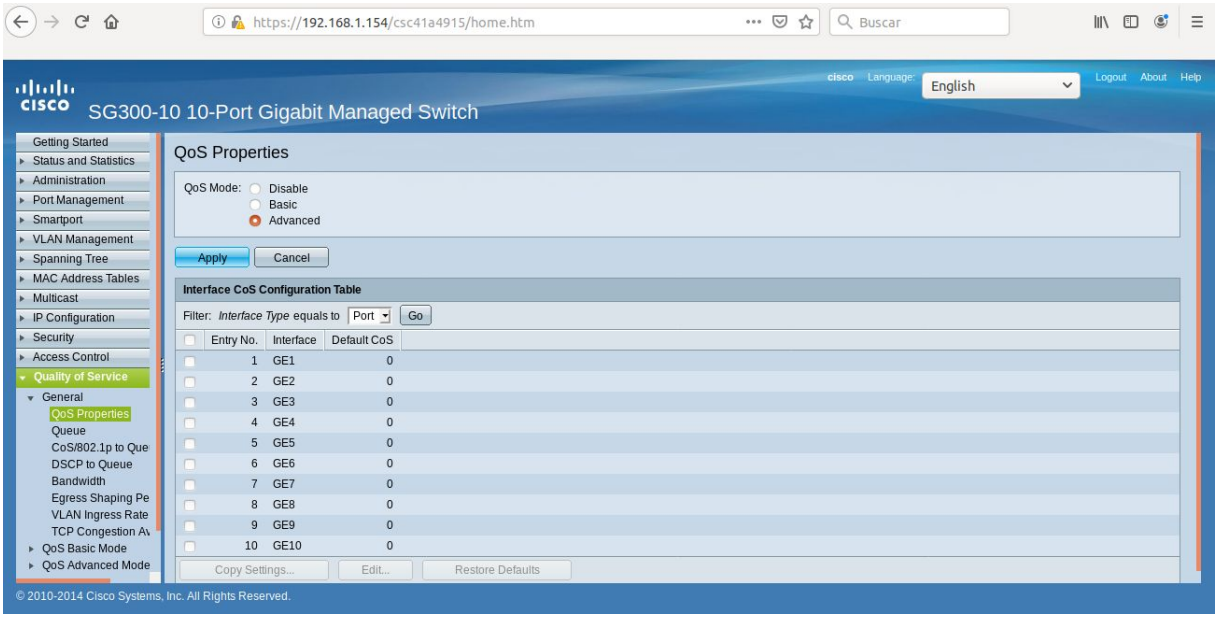


Ilustración 7.23

Una vez creadas todas las ACLs y ACEs correspondientes, tenemos que seleccionar el Modo Avanzado de QoS, que permite una mayor configuración.

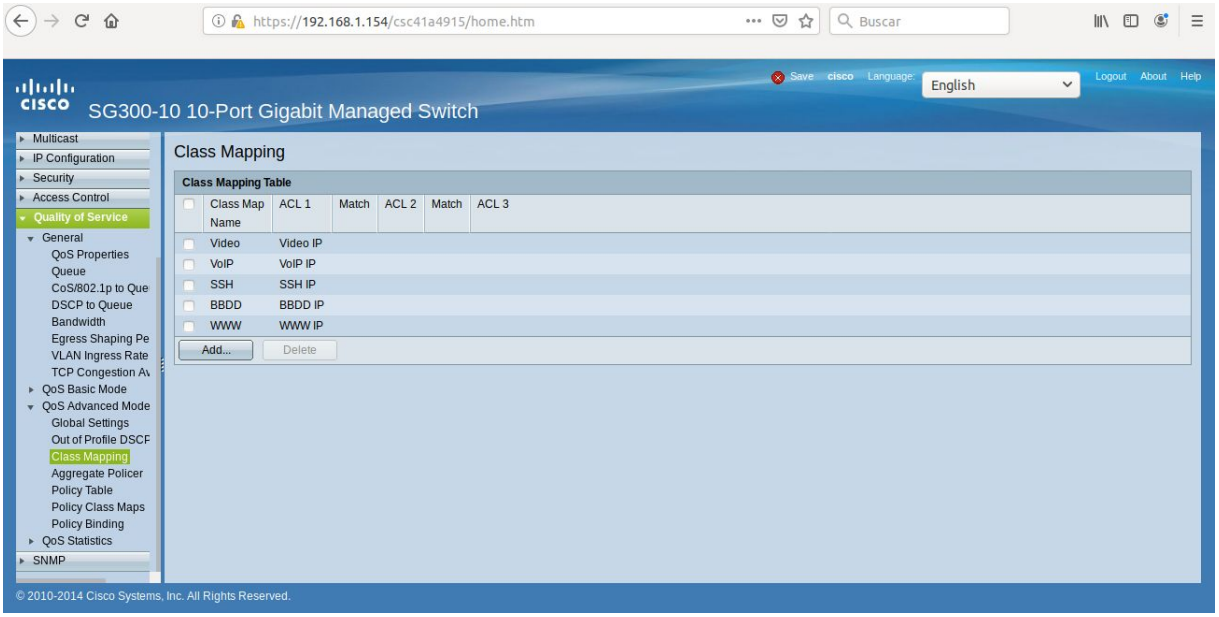


Ilustración 7.24

El siguiente paso es crear un Mapa de Clases. Por simplificarlo van a compartir el nombre con las ACLs.

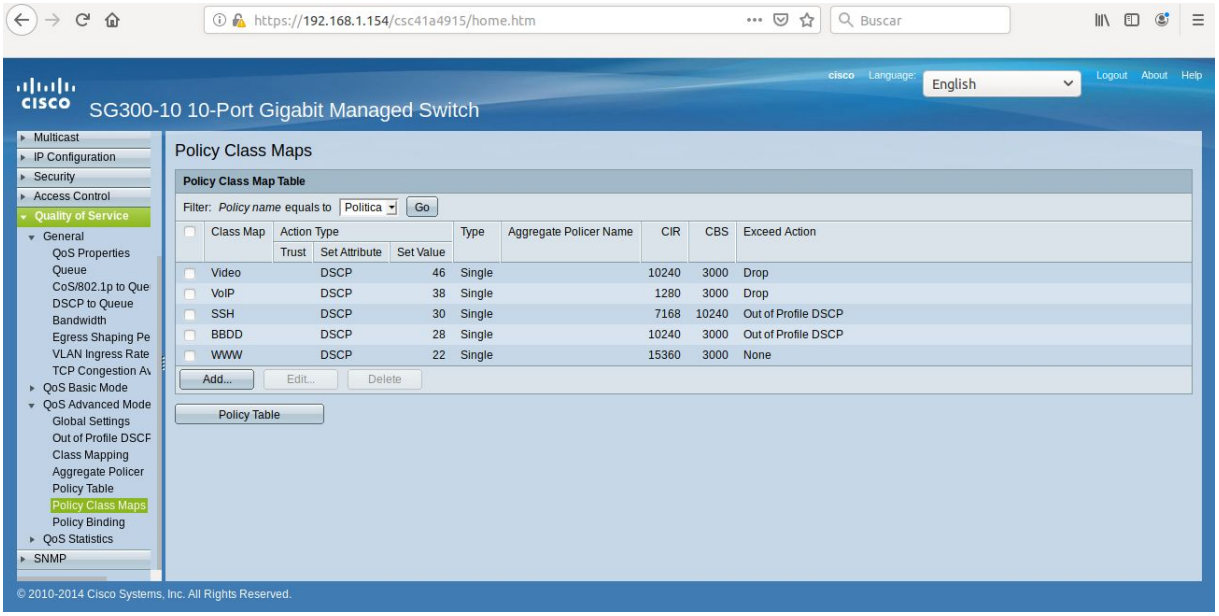


Ilustración 7.24

Finalmente creamos una política y le asignamos los mapas de clases que acabamos de definir. Aplicamos los mismos datos que hemos detallado en la tabla 6.3 (Diseño de la QoS), con la diferencia del ancho de banda de VoIP, ya que le hemos añadido el Control VoIP para un total de 1280 kbps.

8. CONECTIVIDAD

8.1. VPN

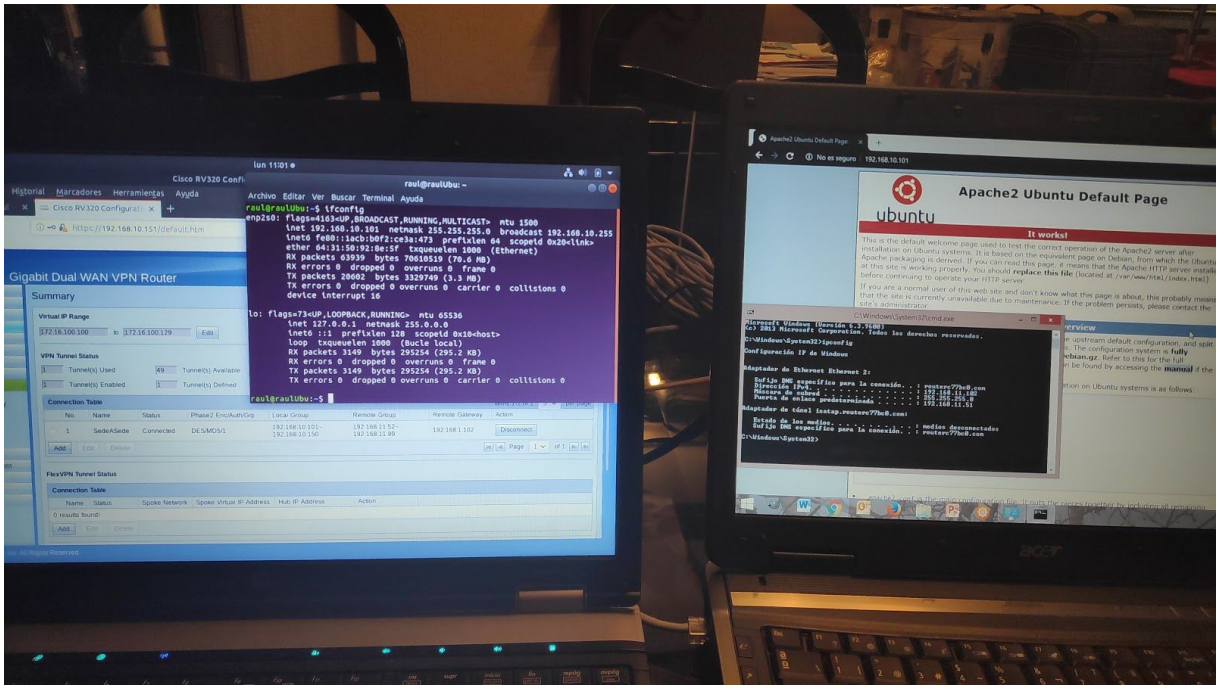


Ilustración 8.1

En la Ilustración 8.1 es apreciable el hecho de que, estando en diferentes redes, el ordenador de la sede secundaria puede acceder a los equipos de la sede central que están en el rango de la VPN establecida

8.2. DMZ

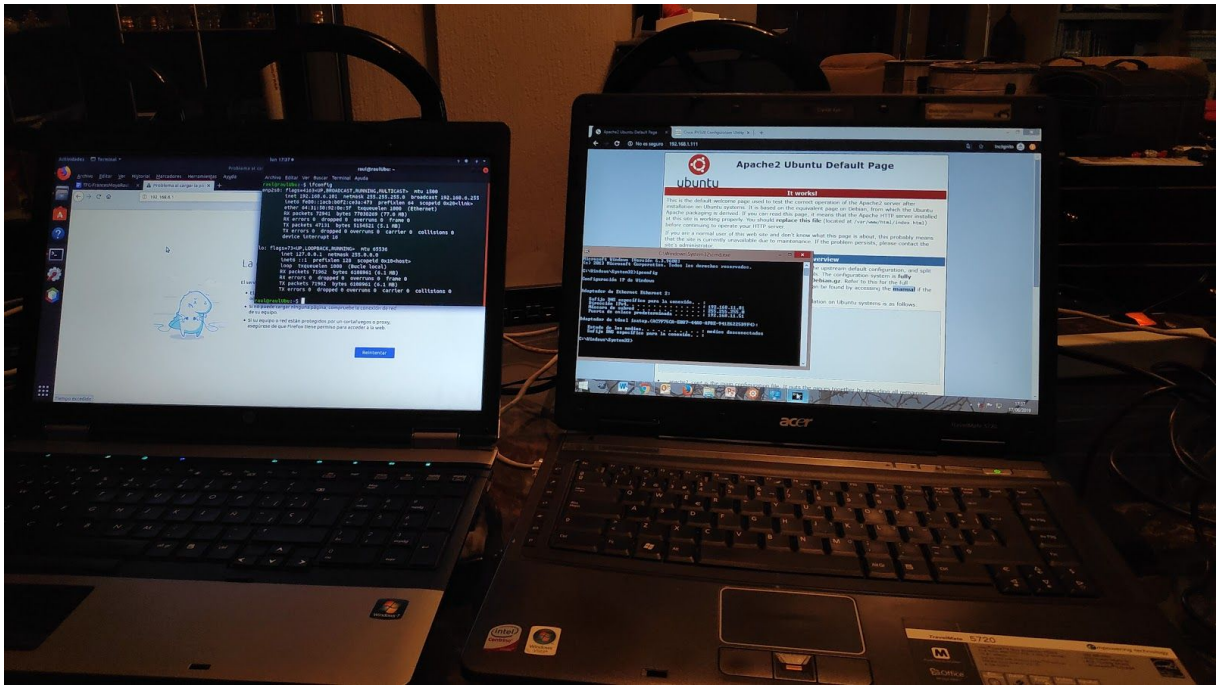


Ilustración 8.2

Mediante DMZ no es necesario establecer la VPN; todos los equipos pueden acceder al servidor a través de la dirección IP pública del router de la sede central.

9. RESULTADOS Y DISCUSIÓN

9.1. Planificación temporal

Para la realización de este trabajo, se ha dividido cada apartado en una tarea y ha realizado un PERT como se muestra a continuación, con la duración indicada en semanas aproximadas.

Nombre de la tarea	Tarea	Precedentes	Duración
A	Buscar información otros TFGs, normas de estilo, etc...	-	1
B	Establecer estilo de texto, apartados, índice	A	1
C	Introducción	B	1
D	Antecedentes	B	1
E	Objetivos	B	1
F	Estado del Arte	B	5
G	Materiales	B	2
H	Diseño de la red	F,G	3
I	Implementación y conectividad	H	6
J	Resultados	C,D,E,I,L	2

K	Conclusiones	B	1
L	Líneas de futuro	K	1

Con esta entrada de datos, el PERT resultante es este:

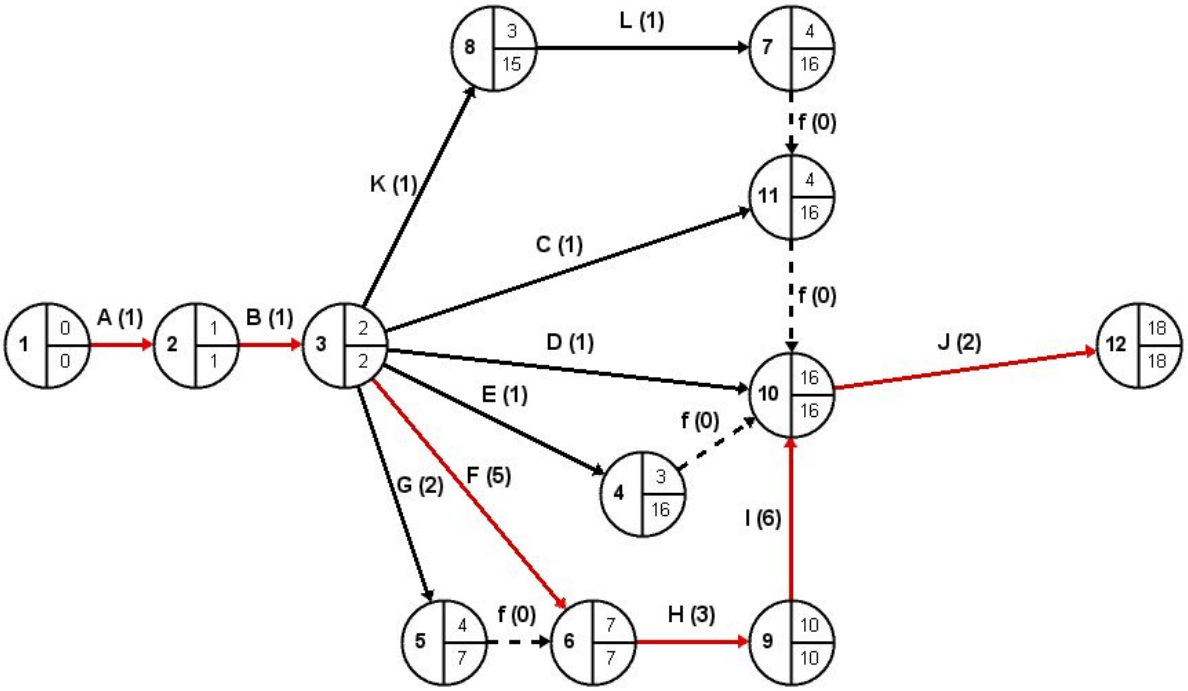


Ilustración 9.1

Esto convierte en camino mínimo a las siguientes tareas:

- A - Buscar información otros TFGs, normas de estilo, etc…
- B - Establecer estilo de texto, apartados, índice
- F - Estado del arte
- H - Diseño de la red
- I - Implementación y conectividad
- J - Planificación temporal

Estas son las tareas irretrasables, en caso de que alguna finalice después de lo esperado, el proyecto entero se retrasa.

La tabla de actividades y holguras es la siguiente:

Tarea	Precedentes	Duración	I_m	F_M	I_M	F_m	H_I	H_T
A	-	1	0	1	0	1	0	0
B	A	1	1	2	1	2	0	0
C	B	1	2	16	2	3	1	13
D	B	1	2	16	2	3	13	13
E	B	1	2	16	2	3	0	13
F	B	5	2	7	2	7	0	0
G	B	2	2	7	2	4	0	3
H	F,G	3	7	10	7	10	0	0
I	H	6	10	16	10	16	0	0
J	D,C,L,I,E	2	16	18	16	18	0	0
K	B	1	2	15	2	3	0	12
L	K	1	3	16	15	4	-12	12

Las actividades con el fondo en rojo indican el camino crítico, cuya holgura inicial y final es 0.

Las operaciones realizadas relacionadas con este tema se han llevado a cabo mediante la herramienta easyPERT.

9.2. Presupuesto

Una rápida búsqueda en Internet nos informa de que el Switch Cisco 300-10 se puede comprar por un valor aproximado de 300€, y el Router RV320 por unos 200€. Sabiendo que para la red indicada en la Ilustración 4.1 se utilizan tres routers (uno de ellos de Firewall, no contamos los de los trabajadores remotos) y cinco switches,

nos daría un total de 2100€, suponiendo que toda la red la implementásemos con equipos como los utilizados para la realización de este TFG.

Para dar acceso a todos los empleados, tomaremos 150€ por cada punto de acceso de media. Con 35 trabajadores serían 5.250€

La instalación de la red con cableado y puntos de acceso y su configuración podría llevarse a cabo con 2 técnicos con los conocimientos necesarios en unas 30 horas. Cobrando 30€ la hora nos daría un total de 1.800€

Para la contratación de MPLS no tenemos ningún dato de referencia, a excepción de los datos de Frame Relay de Movistar, aunque sean del año 2017 y de otra tecnología similar. Comprobando la conexión a través de Uno, esto nos da un precio aproximado de 2.000€ (redondeamos hacia arriba porque es bastante probable que MPLS sea más caro que Frame Relay)

Sumando todos estos precios el presupuesto total ronda los 11.150€ para la sede central de instalación, más costes mensuales del distribuidor de servicios.

10. CONCLUSIONES

El correcto diseño e implementación de una red de área global es complejo y hay que tener en cuenta muchos parámetros, que deben de estar bien configurados, ya que, al mínimo fallo, estamos exponiendo nuestra empresa y, por tanto, datos sensibles a Internet.

Además, no es una tarea que se realice una sola vez, pues a medida que crezcan las tecnologías o la empresa, hay que añadir nuevos equipos, técnicas, etc…

Existen también varias tecnologías por parte de nuestros proveedores de Internet que permiten una mejor conexión VPN sede a sede, mucho más segura y rápida, como lo son MPLS, ATM y Frame Relay, aunque las últimas dos estén en desuso. El uso de estas tecnologías es casi indispensable para el trabajo distribuido en una empresa

La implementación de una red de este calibre en una empresa real es una tarea interesante, a la vez que complicada y requeriría muchas modificaciones, ya que cada compañía tiene sus propias necesidades, prioridades, presupuestos y dimensiones.

11. LÍNEAS DE FUTURO

Para una empresa que quiera montar una red global parecida a la diseñada e implementada en este TFG, es necesario que se realice un estudio de los nuevos equipos de comunicaciones disponibles en la actualidad; no sólo de routers y switches sencillos, también de dispositivos Firewall para un mejor control de los flujos de datos, aportando una mayor seguridad a la empresa.

En cuanto a los grupos de trabajo, como es obvio dependerá de la empresa y su enfoque de mercado. En función de la distribución de trabajadores, es bastante probable que se requiera una mayor separación de VLANes, desactivando el Internetworking de varias de ellas y recurriendo a otra herramienta que permita el acceso al servidor privado desde todas ellas.

La carga de trabajo también condiciona en gran medida los parámetros a la hora de configurar la QoS, tanto la clasificación en ACLs y su prioridad, como el ancho de banda asignado. Por ejemplo una empresa desarrolladora de videojuegos

con el servidor público dentro del campus, lo más probable es que la gran mayoría del ancho de banda esté asignado al servidor y podría utilizar varios puertos auxiliares.

Por último, otra cuestión interesante es conocer los proveedores de Internet de nuestra ubicación y sus planes para empresas, qué tecnologías utilizan del estilo de MPLS, ATM o Frame Relay, con sus limitaciones y sus precios.

Bibliografía

Stallings, W. (2009). *Comunicaciones y redes de computadores*. 7ª edición. Editorial Pearson Prentice-Hall
http://avalos.ujaen.es/availlim/search~S6*spi?/YStallings&searchscope=6&SORT=DZ/YStallings&searchscope=6&SORT=DZ&extended=0&SUBKEY=Stallings/1%2C17%2C17%2CB/frameset&FF=YStallings&searchscope=6&SORT=DZ&6%2C6%2C

Tanenbaum, A. S. (2003). *Redes de computadores*. 4ª edición. Editorial Pearson Prentice-Hall
http://avalos.ujaen.es/availlim/search~S6*spi?/YTanenbaum&searchscope=6&SORT=DZ/YTanenbaum&searchscope=6&SORT=DZ&extended=0&SUBKEY=Tanenbaum/1%2C7%2C7%2CB/frameset&FF=YTanenbaum&searchscope=6&SORT=DZ&2%2C2%2C

Guía de administración del router Cisco RV320.
https://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv320/administration/guide/es/rv32x_ag_es.pdf

Guía de administración del switch Cisco SG300-10.
https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/78-19308-01.pdf

Wikipedia
https://en.wikipedia.org/

Ofertas Movistar
https://www.movistar.es/rpmm/estaticos/residencial/navegacion/fijo/tarifas-movil/2017/2017-01-01-enero-manual-precios-serv-telefonia-movil.pdf

Jerarquía Cisco

http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=6

Creately (herramienta en red para crear esquemas de red)

https://creately.com/

easyPERT (herramienta para la planificación temporal)

https://www.gugames-dev.com/es/games/easypert

Amazon (página web para comprobar el precio de los equipos de comunicaciones)

https://www.amazon.es/

Todos los enlaces son accesibles a día 21/06/2019