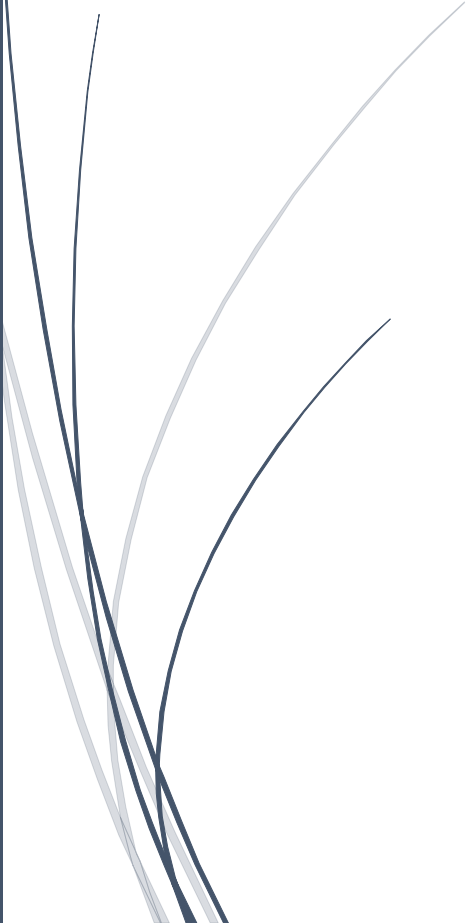
A dark blue vertical bar is on the left. A blue arrow points right from it, containing the date.

18-11-2020

# Proyecto Final

Grupo#6

Several thin, curved lines in shades of blue and grey sweep upwards from the bottom left corner.

Carlos Andrés Morales Lara	1171316
Iván Andrés Arango Saucedo	1158116
Max Fernando Diaz Carranza	1145916
Diego Andrés Diaz Peñate	1315916
Carlos Raúl Lam Marroquín	1193916
Eduardo Antonio Peláez Cifuentes	1096917



### **Parte Teórica**

Para la implementación del proyecto en la parte de ruteo se utilizó el protocolo OSPF, dado que para una mejor organización de la distribución de edificios de la universidad se facilitó el haber asignado áreas a cada edificio, definiendo como área 0 o backbone el edificio G.

OSPF es un protocolo de red para el encaminamiento jerárquico de los datos en el cual se usa el algoritmo de Dijkstra para realizar los cálculos de la ruta más corta desde un punto a otro. Es parte del protocolo IGP. Cabe mencionar que este protocolo toma en cuenta el congestionamiento de la red y que puede operar con encriptación MD5.

Este protocolo construye una base de datos Link-State en todos los routers de las zonas. El proceso de Link-State es el siguiente:

- Cada router obtiene información sobre sus propias redes a las que se conecta directamente
- Cada router tiene la responsabilidad de comunicarse a sus vecinos en redes conectadas directamente
- Cada router crea un paquete de link-State, LSP, que incluye el estado de cada enlace directamente conectado
- Cada router satura con el LSP a todos los vecinos, que luego van a almacenar todos los LSP que reciben en una base de datos.
- Cada router utiliza la base de datos para construir un mapa completo de la topología y calcula el mejor camino hacia cada red de destino.

La forma de calcularlo es ejecutando el algoritmo SPF, el cual crea un nuevo árbol SPF y actualiza la tabla de enrutamiento. OSPF activa sus actualizaciones al ocurrir cualquier cambio dentro de la red, esto reduce su tiempo de convergencia.

### **Tipo de áreas**

Cuando las redes son muy grandes y difíciles de administrar. OSPF permite dividir en áreas numeradas la distribución de la red, donde un área es una red o un conjunto de redes inmediatas. Un área es una generalización de una subred. Fuera de un área, su topología y detalle no son visibles.

Con este protocolo se identifican las siguientes áreas:

- Backbone: es el núcleo de la red OSPF, esta área debe estar presente en cualquier red OSPF, manteniendo su conexión con las demás áreas de la red.
- Stub: en esta área no se anuncian rutas externas al sistema en el que está la red, el enrutamiento en esta área está basado en una ruta por defecto.
- Not-so-stubby: este tipo de área también es conocida como NSSA, en ellas se pueden importar rutas externas de sistemas autónomos y enviarlas al backbone y otras áreas, más no puede recibir rutas externas de sistemas autónomos desde el backbone o de otras áreas.

OSPF da soporte a los siguientes enlaces y da una configuración de interfaz para cada uno:

- Punto a punto – cuando la interfaz se conecta hacia otra interfaz.
- Punto a multipunto
- Broadcast, en estos enlaces las interfaces pueden conectarse directamente entre ellas
- Enlace virtual
- Enlace de acceso múltiple

Entre las ventajas y desventajas que consideramos para utilizar este protocolo se encuentran:

Ventajas	Desventajas
Ofrece rápida convergencia, permite poder tener una escalabilidad confiable	Uso del CPU y memoria del router
Es aplicable a dispositivos de todos los fabricantes	Solo puede soportar protocolos TCP/IP
Cada router conoce la red completa, actualiza la imagen que posee al ocurrir un cambio	Requieren un diseño de red jerárquico muy estricto

## DMZ

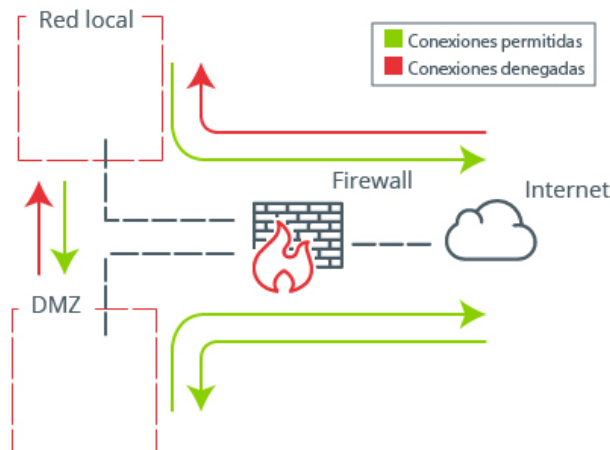
La zona desmilitarizada es un área adicional dentro del ámbito de la red de una empresa, se sitúa entre la red interna y la red externa, que usualmente es Internet. La función de la DMZ es permitir las conexiones desde la red interna como de la externa, mientras las conexiones que parten de la DMZ solo pueden salir hacia la red interna.

En esta red, que está aislada dentro de la red interna de la organización, se encuentran ubicados todos los recursos de la empresa que tienen que acceder a Internet. Las conexiones que van de la DMZ a la red local no están permitidas dado que los dispositivos que se encuentran en ella son más susceptibles a poder sufrir un ataque que comprometa su seguridad.

Si algún servidor de la zona desmilitarizada sufriera un ataque sería más difícil acceder a la red local de la organización, dado el bloqueo que hay ante la entrada de conexiones procedentes de la DMZ, ayudándonos a proteger y considerar una barrera más para la seguridad de la red de las empresas.

Para poder reducir los riesgos que conlleva tener servidores propios y garantizar la seguridad de la red, se utilizan los conocidos firewalls y las zonas desmilitarizadas.

La principal función del firewall acá es filtrar el tráfico de manera que mediante reglas establecidas pueda regular el tráfico entrante y de salida.



Fuente: <https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa>

Las funciones que nos permite tener implementada una DMZ:

- Filtrado de paquetes de cualquier zona
- Mapeo bidireccional
- Colas de tráfico y prioridad
- Salidas redundantes
- Balanceo de carga de servicios
- Filtrado de contenido
- Monitoreo de enlaces

Para una de las posibles implementaciones de la DMZ que consideramos se utilizaba un ASA 5505, para poder delimitar una zona perimetral. Por consiguiente, para esta implementación se necesitaban considerar VLAN's, el dispositivo cuenta con 2 por defecto: inside y outside.

Como primer paso para esta implementación se realizó la configuración de las VLAN's en el ASA 5505, agregando una vlan 3, que se llamaría DMZ. Luego de esto se procedió a poder configurar sobre los diferentes dispositivos en a los cuáles se conectaría el ASA, es decir, sobre los switches adyacentes a este dispositivo se configuraron sobre las interfaces conectadas las VLAN's que este dispositivo de seguridad nos brindaba.

Después de haber conectado los dispositivos en la configuración del ASA 5505 procedimos a configurar las direcciones IP a las cuales correspondería cada una de las VLAN's, en este caso la red interna corresponde a los servidores de la red en DTI, en la DMZ para ejemplificar fueron colocados un servidor HTTPS y otro que utiliza los protocolos SMTP y POP3 para enviar y recibir correos.



Por temas de licenciamiento, en el dispositivo ASA se tenía que especificar un *no forward* hacia la red interna para poder empezar a establecer los niveles de seguridad de cada vlan y sus respectivos permisos. Para poder cumplir el objetivo de la DMZ, dentro del ASA 5505 se debía configurar políticas de servicio, en la cual se procedía a *inspeccionar* la red para permitir únicamente el acceso desde la red interna hacia la DMZ y denegar el acceso desde la DMZ hacia la red interna.

Este modelo de DMZ fue descartado para el proyecto, dado que el protocolo DHCP del dispositivo ASA 5505 y las VLAN's que necesita este para poder realizar las configuraciones tenían mucho conflicto con nuestra distribución tan extensa de VLAN's, cambiar la pool de direcciones IP para el protocolo DHCP también representó un problema, dado que las direcciones proporcionadas por el router conflictuaban con las del ASA 5505, por lo tanto se descartó este diseño de DMZ y se procedió a simularla mediante routers y Access Lists.

Para los servidores que se configuraron dentro de este diseño de DMZ se utilizaron los servicios de EMAIL, en donde usamos los protocolos SMTP y POP3 para que fuera posible tanto enviar como recibir correos.

## **SMTP**

Este protocolo permite el envío de correos por internet, su funcionamiento es muy sencillo, si el servidor SMTP puede confirmar las identidades del remitente y destinatario se realiza el envío, de lo contrario no.

Cuando se envía un correo se produce una validación de comandos que luego son enviados a un servidor de este tipo (SMTP). Para este proceso no se es tan consciente del contenido del correo sino más bien que el servidor se concentra de manera exclusiva en la transmisión del correo.

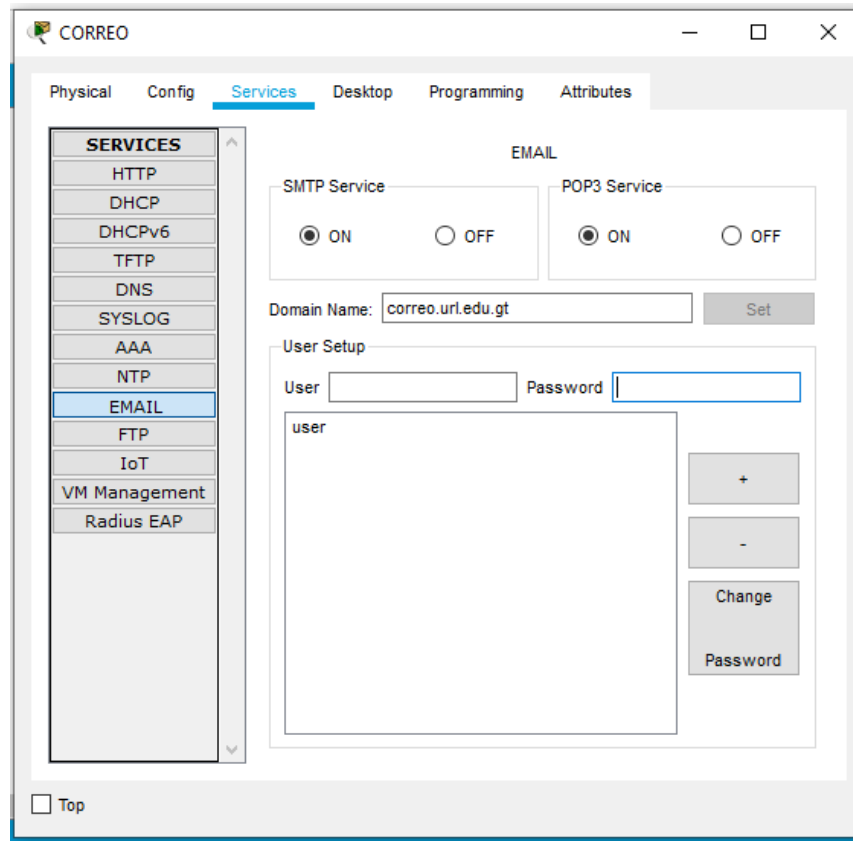
Cuando se envía se abre una nueva sesión de retransmisión de SMTP, y se procede a llevar a cabo intercambio de información entre el cliente del correo y el servidor SMTP destino.

## **POP3**

Sus siglas son Post Office Protocol, es el protocolo de comunicaciones más extendido para leer correos electrónicos. Por medio de este protocolo las cuentas de correo pueden:

- Descargar la información en el disco duro del cliente, para que el servidor no retenga las copias de los mensajes.
- Descargar la información en el disco duro del cliente y que las copias de los correos sigan persistiendo en el servidor.

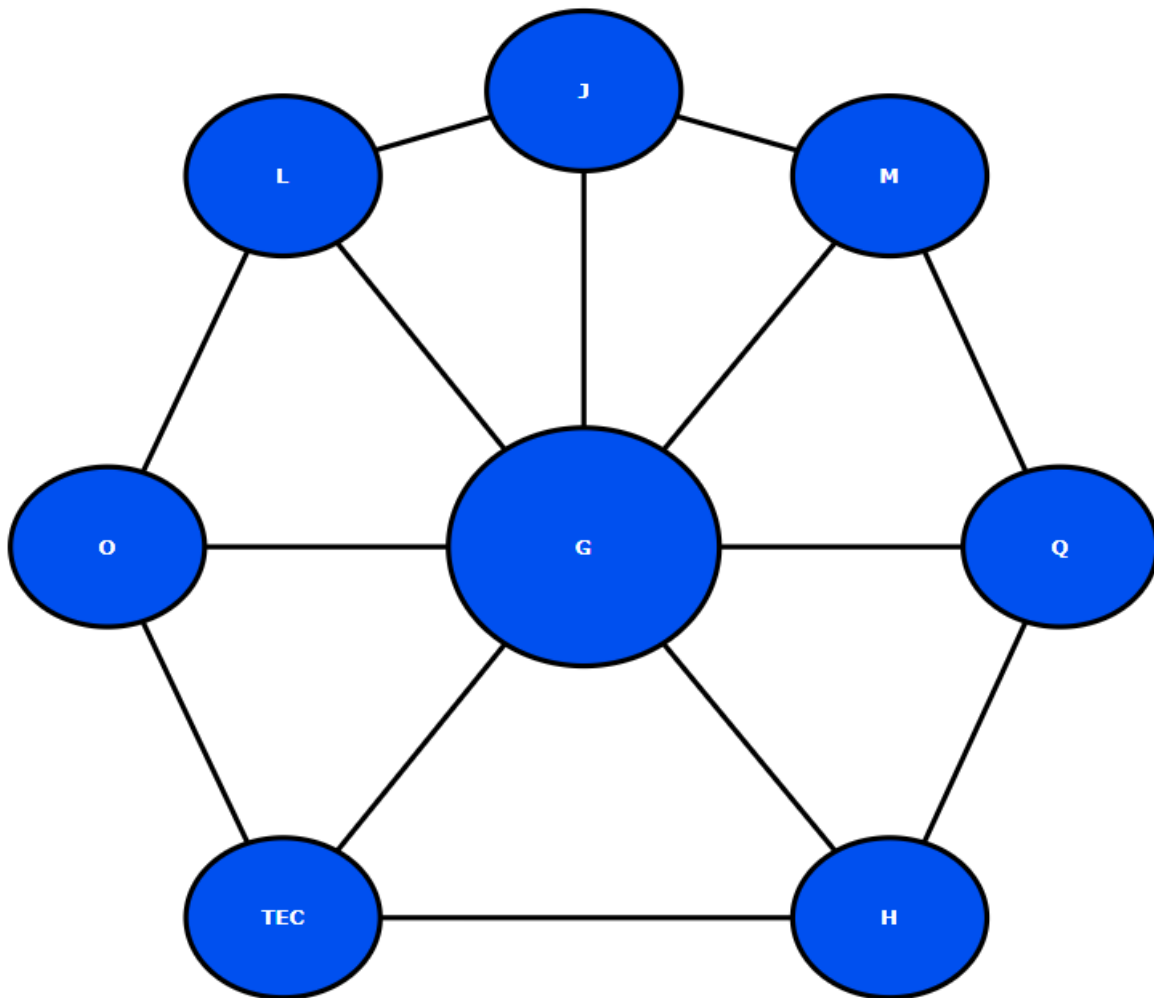
Para configurarlo estos servicios dentro del servidor de la DMZ bastó con encender los dos servicios y poder empezar a agregar usuarios en base al dominio establecido.



*Fuente: propia*

El presupuesto se adjuntó en un archivo de Excel aparte llamado "Presupuesto.xlsx" en donde se detalla todo el presupuesto a tomar en cuenta para la realización de este proyecto.

### Topología de Red



La topología de red de nuestra red universitaria es una topología Híbrida que consiste en un conjunto entre una topología de estrella y una topología de anillo. Incluye una topología de estrella donde todos los nodos externos se conectan a un nodo central el cual es el Edificio G. Y la topología de anillo ya que todos los nodos externos se conectan con sus nodos adyacentes esto con el fin de que si se cae la conexión de un nodo externo con el nodo central no se pierda totalmente la comunicación de un edificio y tenga la posibilidad de tener varios caminos de llegar al nodo central.

Utilizamos el protocolo de enrutamiento OSPF por áreas, donde cada edificio es un área distinta y el edificio G donde se encuentra nuestro nodo central (servidores) es el área 0 (área backbone). Utilizamos este protocolo ya que este protocolo en enrutamiento no es propenso a bucles de enrutamiento, es ideal para redes grandes



como el de la universidad ya que escala muy bien y este converge a mayor velocidad que los protocolos de vector distancia.

*El diagrama físico de red y el diagrama lógico de red se adjuntaron por aparte para mejor apreciación.*

La distribución de los dispositivos de cada edificio es muy similar, para los edificios O, Q, J, M, L, H constan de tres niveles, el primer y segundo nivel se encuentran los ordenadores del área de Estudiantes con su respectivo switch mientras que en el tercer nivel se encuentran los ordenadores del área Administrativa. Adicional al tercer nivel se encuentran los switches del área Administrativa y los tres routers del edificio.

Para el edificio G el planteamiento de dispositivos es lo mismo solamente que en el tercer nivel están los servidores (DNS, HTTPS, etc.).

Para el edificio TEC consta de cinco niveles, este aparte tiene 10 laboratorios extra y estaciones portátiles extras. El TEC consta de cinco switches, dos para el área Administrativa y tres para el área de Estudiantes. Y tiene también tres routers en el edificio.

En todos los edificios tienen hosts designados con cable y otros con Wifi-URL. Los switches de los niveles inferiores se conectarán con los routers del tercer nivel por medio de cableado vertical.

Para el cableado entre router en el mismo edificio se utilizará cable serial, para el cableado entre switches y routers se utilizará cable UTP de tipo cruzado y para las conexiones entre los ordenadores con su switch así como los switches con los Access Point también cable UTP, pero recto. Finalmente, para el cableado entre routers de diferentes edificios se utiliza cable de fibra óptica.



Las velocidades de transferencia de los cables UTP son de 1GB/s ya sea cruzado o recto. Para el cable serial entre routers su velocidad de transferencia también es de 1GB/s. Y para el la velocidad de transferencia del cable de fibra óptica es de 10GB/s.



### Mapa de la red universitaria

Se adjunto un archivo de Excel llamado "Subnetting Proyecto.xlsx" el cual se detalla todo lo previamente pedido más como se calculó el número total de hosts y el enrutamiento de áreas de OSPF.



Se implementó VLAN'S administrativa en cada edificio, con el fin de que la comunicación del área administrativa de cada edificio sea confidencial y que únicamente los trabajadores puedan establecer comunicación entre sí y que no pueda un estudiante o usuario ajeno ver y poder enviar un mensaje al tratarse de conectarse a esa red. Y se implementó VLAN'S para estudiantes en la que se compone de los estudiantes que se conectan por medio de Wifi y de las computadoras que se conectan por medio de cable en los laboratorios, con el fin de que pueda existir una comunicación entre cada estudiante, independiente de la manera que se encuentren conectados.

Tipo de VLAN'S	Número de Equipos conectados	Etiquetado	Dispositivos	Interfaces
Administrativo Edificios O, L, M, H, J, Q	126 114	100 101	CPU'S y LAPTOP'S	GigabitEthernet0/0 router (VLAN 100)  GigabitEthernet1/0 switch(VLAN 100 y 101)  FastEthernet 0/1 - 5 switch(VLAN 100 y 101)  GigabitEthernet1/0 router (VLAN 101)
Estudiantes Edificios O, L, M, H, J, Q	420 200	200 202	CPU'S, LAPTOP'S y teléfonos.	GigabitEthernet0/0 router (VLAN 200)  GigabitEthernet1/0 router (VLAN 202)  GigabitEthernet1/0 switch (VLAN 200 y 202)  FastEthernet 0/1 - 5 switch(VLAN 200 y 202)
Administrativo Edificio G	126 114	100 101	CPU'S y LAPTOP'S y servidores.	GigabitEthernet0/0 router (VLAN 100)  GigabitEthernet1/0 switch(VLAN 100 y 101)  FastEthernet 0/1 - 5 switch(VLAN 100 y 101)  GigabitEthernet1/0 router (VLAN 101)
Estudiantes Edificio G	420 200	200 202	CPU'S, LAPTOP'S y teléfonos.	GigabitEthernet0/0 router (VLAN 200)



				GigabitEthernet1/0 router (VLAN 202)  GigabitEthernet1/0 switch (VLAN 200 y 202)  FastEthernet 0/1 - 5 switch(VLAN 200 y 202)
Administrativo Edificio TEC	254 46	100 101	CPU'S y LAPTOP'S	GigabitEthernet0/0 router (VLAN 100)  GigabitEthernet1/0 switch(VLAN 100 y 101)  FastEthernet 0/1 - 5 switch(VLAN 100 y 101)  GigabitEthernet1/0 router (VLAN 101)
Estudiantes Edificio TEC	840 204 350	200 201 202	CPU'S, LAPTOP'S y teléfonos.	GigabitEthernet2/0 router (VLAN 200)  GigabitEthernet0/0 router (VLAN 201)  GigabitEthernet1/0 router (VLAN 202)  GigabitEthernet1/0 switch(VLAN 200, 201, 202)  FastEthernet 0/1 - 5 switch(VLAN 200,201,202)

## Referencias

INCIBE (2019). Qué es una DMZ y cómo puede ayudarte a proteger tu empresa. Recuperado de: <https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa>