INF-256: Redes de Computadores

Experiencia Recuperativa
"Implementación de una Red y Aplicación de Servicios"

Laboratorio de Integración Tecnológica

Septiembre 2019

Lea atentamente cada punto de la experiencia y siga todas las instrucciones indicadas

Toda duda respecto a la realización de la experiencia, hacerla llegar a la lista de correos del laboratorio: *labit@listas.inf.utfsm.cl*

1. Introducción

Las Redes de Computadores son elementos esenciales dentro de nuestra sociedad actual en lo que respecta a la transmisión de información entre múltiples dispositivos, garantizando la comunicación y el intercambio de recursos entre ellos sin importar la ubicación geográfica de dichos equipos. El tener manejo sobre su diseño y administración se torna en una herramienta muy necesaria, y al mismo tiempo que útil, para un ingeniero o ingeniera que desee desenvolverse dentro de esta área.

En este laboratorio, se aplicarán los conocimientos adquiridos en las 3 experiencias anteriores sobre las redes de computadores para implementar y configurar una topología de red, enfatizando en la configuración de ACLs y Firewall vistos en la 3ra experiencia, además de la implementación de un servicio de red local.

2. Objetivos generales del laboratorio

- Implementar una red física compuesta de *routers*, *switches*, *hosts* y *firewall*.
- Implementar servicios para una red local
- Manejar el uso de Firewall y la utilización de Listas de Control de Acceso (ACL) dentro de una red

3. Objetivos específicos del laboratorio

- Aplicar el uso de comandos IOS y de protocolo IP (Internet Protocol)
- Configurar una red para garantizar comunicación entre equipos terminales.
- Configurar una red para garantizar su funcionamiento con protocolos de *Ruteo Dinámico*
- Comprender la finalidad de utilizar firewalls y ACL dentro de una red
- Configurar el acceso que tienen los equipos entre si o hacia el exterior de la red mediante ACL.
- Configurar interfacez de red vía CLI en distribuciones Linux
- Implementar servicios de DNS

4. Descripción del laboratorio

La experiencia consta de 3 partes a realizar, en las que se abordarán conocimientos básicos para la implementación de servicios en una red local, y la *implementación y configuración* de una *topología de red*, aplicando Listas de Control de Acceso y configuración de Firewall.

- **PARTE 1:** Informe Previo (**10 pts**).
- **PARTE 2:** Implementación de un Servidor para implementación de Servicios (**30 pts**).
- **PARTE 3:** Armado, configuración y unión de la Red Física con un servicio de DNS.(**60 pts**).

  Hint: Se recomienda repasar los comandos utilizados en la Experiencia anterior para la configuración de equipos, pues se espera que la sección de ruteo dinámico sea dominada completamente y no signifique retraso para la continuación de la experiencia.

5. Trabajo Previo

5.1. Informe Previo

En este punto se debera de redactar un informe por grupo. En este se deben responder las actividades que se presentan a continuación relacionadas con la implementación y configuración de un Servidor de red local. Para mas información acerca de la entrega del informe revisar la sección Consideraciones.

- **Actividad 1:** Responda las siguientes preguntas:
- 1. Explique las principales ventajas de implementar servicios/servidores en máquinas virtuales.
- 2. Qué es un servicio de DNS y cual es su importancia en las Redes de Computadores. Explique un ejemplo de como funciona.
- 3. Averigue que son la Zona directa y Zona inversa en un DNS.
- 4. Investigue cuantos tipos de consultas recibe un servidor DNS y como se diferencian.
- 5. Qué es un NIC, explique su función y si existe en Chile alguno.

5.2. Implementación de Servicios

En esta sección se trabajará en máquinas virtuales para implementar los servicios, el cual se encontrarán en una máquina CentOS 7 que hará de servidor para una segunda máquina cliente en Windows. Para esto se utilizará el administrador de máquinas VirtualBox, se recomienda seguir los pasos entregados a continuación.

5.2.1 Instalación de entorno de trabajo:

- Link de descarga de CentOS 7, Windows 7, VirtualBox
- - Al ejecutar debe crear una nueva máquina virtual, con sistema operativo Linux RedHat (64-bit). (requiere que el soporte de virtualización este habilitado en la bios del computador que está utilizando).
- - Asigne 2G de memoria RAM y cree un disco duro virtual con formato VDI, tamaño reservado estáticamente de 8Gb.(puede asignar más si lo desea y puede)
- - Una vez creada la máquina virtual, acceda a configuraciones de esta (sin iniciarla aún). En Almacenamiento añada la unidad optica de CentOS(iso descargado previamente), luego en Red Conéctese a través del Adaptador puente. Si su computador reciba internet mediante Wifi, seleccione "Wireless Network Adapter"
- - inicie la máquina e instale CentOS 7, seleccione el idioma que desea utilizar durante la instalación y la configuración de su teclado.
- - Al comenzar la instalación seleccione:

- - Origen de instalación: Medios Locales.
- - Selección de software: Instalación mínima.
- - Destino de la instalación: Selección particionado automático.
- - Red y Nombre de equipo: En nombre de host asigne el nombre: redesXX.local (Reemplace XX por el número de su grupo)
- - Comience la instalación e ingrese una contraseña de root. Reinicie cuando se le solicite.

5.2.2 Configuración de red

- Ingrese como usuario root y edite el archivo de configuración de la interface de red de su sistema *ifcfg-enp0s3*, ubicado en la carpeta */etc/sysconfig/network-scripts/* .
- - Dentro del archivo los parámetros que debe ajustar para configurar una dirección de red estática son los siguientes (el resto de los parámetros que aparecen por defecto no los modifique), los DNS expuestos son los propios de la universidad.

```
BOOTPROTO=none
IPADDR=192.168.0.31
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
NETWORK=192.168.0.0
DNS1=200.1.21.80
DNS2=200.1.21.150
ONBOOT=yes
```

- Para saber que Ip, Gateway y Network utilizar, verifique en la configuración de red de su computador su IPV4, en base a ello asigne a su máquina una dirección ip válida, y recuerde que por defecto en una red local, la ip finalizada en .1 corresponde al enrutador y la .0 a la red.
- Ejemplo de IP de computador es la .15(puede asignar cualquiera no utilizada a su máquina en este caso se uso la .31):

- - Una vez guardados los cambios a la interfaz, reinicie el servicio de red para que los cambios de configuración se apliquen. Para reiniciar utilice el comando: *systemctl restart network*.
- - Verifique la configuración de red actual utilizando los siguientes comandos:
- *Ip addr* (para ver la dirección ip), *Ip route* (para ver el Gateway y la red), *Cat /etc/resolv.conf* (para ver los servidores DNS que se están utilizando)
- - Realice pruebas de conexión a internet y a su Gateway utilizando *ping*.

5.2.3 Instalación y configuración de DNS

- - Instale el servicio DNS (bond), para lo cual ejecute *yum install bind caching-nameserver*
- - Una vez instalado, verifique que el proceso named este en ejecución, Para esto utilice el comando:

```
[root@redesxx ~]# ps aux |grep named
```

- - Verifique el estado del servicio named, para lo cual utilice el siguiente comando *systemctl status named*, en inicielo de ser necesario con *systemctl start named*, finalmente utilice *systemctl enable named*, para que el servicio se levante al iniciar el servidor.
- - Edite el archivo */etc/named.conf*
- - Habilite para que el servicio quede disponible en la dirección ip asignada al servidor, para lo cual agregue la dirección de red de su máquina en la línea *listen-on port 53* Ejm:

```
listen-on port 53 { 127.0.0.1; 192.168.0.31; };
```

- - Permita las consultas DNS desde la red que está utilizando, para esto busque la línea *allow-query* y agregue su red, ademas agregue la linea *forwarders* como se muestra a continuación Ejm:

```
allow-query     { localhost; 192.168.0.0/24;};
forwarders      {200.1.21.80;200.1.21.150;};
```

- Habilite las zonas DNS directa e inversa que utilizará, agregando las definiciones al final del archivo como se muestra a continuación, recuerde reemplazar *redesxx* y *0.168.192.in...* por los correspondientes a su grupo y red.

```
zone "." IN {
        type hint;
        file "named.ca";
};
zone "redesxx.local" {type master; file "redesxx.zone";
allow-update { none;};
};

zone "0.168.192.in-addr.arpa" {type master; file
"0.168.192.in-addr.arpa.zone";
allow-update { none; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

- A continuación encontrará 2 archivos de utilidad, para que no deba crearlos desde cero, descargue estos archivos y descomprimalos dentro de su maquina virtual. Archivos de configuración DNS
- Una vez descargados puede usar un cliente FTP como Filezilla para transferir archivos desde su computador a su VM.
- Puede descomprimir utilizando *yum install zip unzip* y luego *unzip named.zip*. Una vez descomprima el zip, verá los archivos *1.168.192.in-addr.arpa.zone* y *redes00.zone*, mueva ambos al directorio emph/var/named/ y cambie su nombre con el comando *mv nombre-archivo /directorio-llegada/archivo-nombre-nuevo*

```
mv 1.168.192.in-addr.arpa.zone /var/named/0.168.192.in-addr.arpa.zone
mv redes00.zone /var/named/redesxx.zone
```

- Una vez los archivos se encuentren en el directorio indicado, configure estos, de manera que en toda sección que diga *redes00*, se reemplace por su número de grupo, y en toda parte que diga *1.168.192.* o bien *192.168.1.xx* se corrija por su correspondiente red.
- A continuación se muestra una sección de ambos archivos, en el primero note que los números 31 y 15 corresponden a las ips del servidor y del computador (modifique estos según sus ips), en la segunda tambien asigne las ips correspondientes.

```
; lista de equipos
$ORIGIN 0.168.192.in-addr.arpa.
31      IN      PTR     servidor.redesxx.local.
15      IN      PTR     pc1.redesxx.local.
```

```
;Lista de equipos
servidor        IN      A       192.168.0.31
pc1     IN      A       192.168.0.15
```

- - Verifique que el archivo emph/etc/named.conf esta configurado correctamente con los nombres de los archivos renombrados del punto anterior(esto debe verlo al final del archivo en donde define *zone*.
- - Utilice el siguiente comando para verificar la redacción de los archivos de configuración: *named-checkconf*, en caso de haber errores este le indicará donde.
- - Reinicie el servicio para que los cambios tengan efecto, para lo cual utilice el siguiente *comando systemctl restart named*
- *hint: si aparece un error al reiniciar es porque algo no esta bien escrito o configurado en los archivos relacionados al servicio NAMED*
- En la configuración ip de servidores DNS de su servidor, deje solo la Ip local (el servidor será cliente de si mismo). Para esto debe editar el archivo de configuración de red */etc/sysconfig/network-scripts/ifcfg- enp0s3* y en los servidores DNS deje solo *DNS1=127.0.0.1*

- Reinicie el servicio de red para que se apliquen los cambios.

```
DNS1=127.0.0.1
#DNS2=200.1.21.150
```

- - Para verificar la resolución de nombre, haga ping a si mismo(servidor) y al pc1 mediante su nombre de red y verifique se muestra su ip correspondiente, Ejemplo:

```
[root@redesxx ~]# ping servidor.redesxx.local
PING servidor.redesxx.local (192.168.0.31) 56(84) bytes of data.
64 bytes from servidor.redesxx.local (192.168.0.31): icmp_seq=1 ttl=64 time=0.070 m
```

- Si no puede concretar ping a pc1, desactive el firewall de su pc para hacer la prueba.

6. Trabajo en Laboratorio

6.1. Armado y Configuración de la Red Física

Ahora en esta sección, como grupo deberán **implementar** físicamente la red que se muestra a continuación con los cables y componentes entregados en el laboratorio al momento de rendir la experiencia. 1

6.1.1. Instrucciones

Como grupo dispondrán del siguiente equipamiento, el cual debe ser utilizado en su totalidad:

- 3 Routers Cisco Serie 2901
- 1 Router Cisco Serie 2911
- 1 Firewall Cisco Asa 5505
- 2 Switches Cisco Series Catalyst 2950
- 2 Host con sistema operativo `Linux Fedora 28 Workstation`, con permisos de edición y ejecución para una lista de comandos predeterminados.
- 10 Cables de red RJ-45
- 2 Cables Serial a USB

Se deberá construir y configurar el modelo de la Figura 1 para que permita la comunicación a lo largo de toda la red:

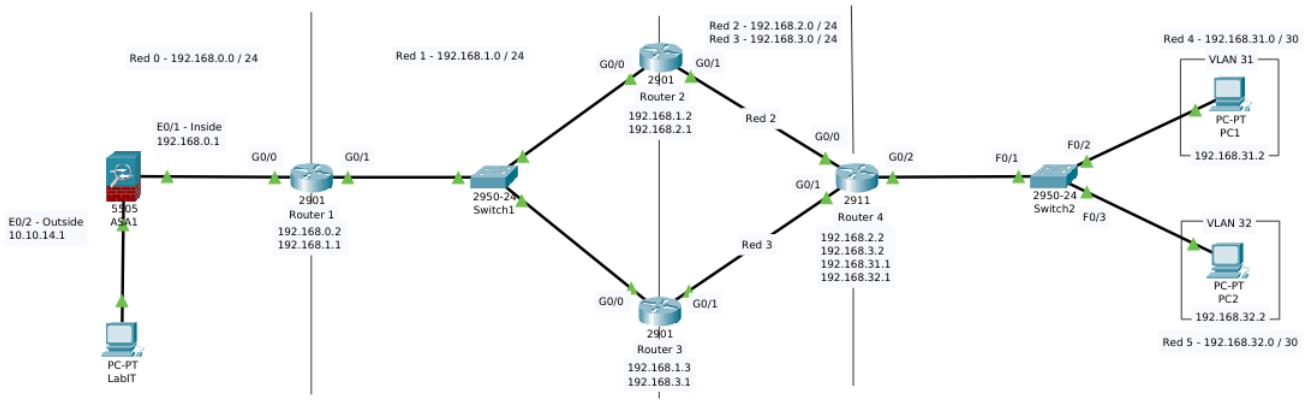

Figura 1: Topología Actividad Práctica

Se recomienda primero armar físicamente la red y tener todos los cables de red conectados en las boquillas correspondientes.

Una vez tenga armada físicamente la red, deberá comenzar a configurar las interfaces de red vía consola para cada uno de los routers, luego continuar configurando la red para que esta funcione con **Ruteo Dinámico RIP**. Para los **Hosts** se deberá configurar la interfaz de red **enp3s0**, modificando los campos IPADDR, NETMASK, GATEWAY y BOOTPROTO.

Recuerde que para poder ingresar a la interfaz de un router o un switch debe utilizar el comando:

```
[user@client dev]$ sudo minicom -D /dev/ttyUSB0 -b 9600
```

Una vez realizado lo anterior, es necesario **crear 2 VLAN**, asociarlas a los PCs conectados al switch (VLAN31 asociada a PC1 y VLAN32 asociada a PC2) y definir los modos en los que funcionarán las interfaces F0/1, F0/2 y F0/3 en este.

Para esto **conectese al Switch 2** por cable serial y siga con atención las instrucciones presentes en la sección 8.1 Switch y 8.2 VLAN.

En vista que estamos trabajando con redes virtuales (VLAN) dentro del switch, es necesario crear interfaces virtuales en el router para asignar los gateway de cada red y permitir permitir su conexión con el resto de la red. Ante esto **cree 2 interfaces virtuales** en la interfaz física del router que conecta con dirige al switch (G0/2) para **asignarles las IPs de los gateways (192.168.31.1 y 192.168.32.1)** de cada red.

Para esto **conectese al Router 4** por cable serial y siga con atención las instrucciones presentes en la sección 8.3 Interfaces Virtuales.

Ya teniendo configurado lo anterior, deberá implementar 4 reglas ACL, 2 que impidan únicamente al PC1 comunicarse completamente con el *Router2*, y 2 que impidan solamente al PC2 comunicarse con el *Router3* . Estas deben ser implementadas en los Router 1 y 4 asociandolas a sus interfaces para que bloqueen el tráfico del equipo hacia el *Router2* y *Router3* respectivamente..

A continuación proceda a configurar el Firewall Cisco de modo que se logre conexión entre la topología implementada y la red del mismo laboratorio. Para esto haga uso de las guías mostradas en la sección Configuración básica de Firewall.

Una vez configurado el Firewall, ustedes podrán llegar desde los computadores del laboratorio a los pc1 y pc2 (hacer prueba con *ping*) . De esta manera uno de los computadores tendrá implementado el mismo servidor DNS que su grupo configuró en la parte previa pero con un defecto, ustedes deberán ser capaces de corregirlo, para luego añadir a los pc1 y pc2 al grupo de hosts conocidos y realizar la traducción NOMBRE-IP.

6.1.2. Evaluación

La experiencia estará finalizada cuando se logre realizar correctamente lo siguiente:

- Armado y creación de la red:
  - Armado de la red física.
  - Configuración de interfaces Gigabit Ethernet correspondientes de los routers.
  - Configuración de interfaces Fast Ethernet correspondientes del switch junto a la implementación de ambas Vlan.
  - Configuración de las interfaces de cada host.
  - Configuración de las ACL's en los routers
  - Configuración del firewall para conectarse con la red LabIT
- Verificar la comunicación entre los equipos terminales.
  - `Ping` entre *PC1* y *PC2*.
  - `Ping` entre *PC1* y *Router2* para chequear el funcionamiento de las ACL's.
  - `Ping` entre alguno de los computadores y el *Gateway* de la red del *LabIT*.

7. Consideraciones

- **La experiencia será realizada en parejas.**
- Esta experiencia consta de una parte previa y una práctica.
- La inscripción de horario para rendir esta experiencia deberá hacerse entre el 02 de Septiembre y el 06 de Septiembre de manera presencial.
- El trabajo práctico en el laboratorio se desarrollará entre el lunes 09 de Septiembre y el viernes 13 de Septiembre.
- El Informe Previo debe ser realizado en algún editor de texto (Se recomienda usar LATEX) de manera ordenada y ser entregado en formato digital a través de Moodle, hasta el día Domingo 08 de Septiembre a las 23.55 hrs. A

- Para la parte de Implementación de servicios, debe adjuntar en su informe, capturas de pantallas de todos los archivos que contienen configuraciones modificadas o agregadas por su grupo (al menos las secciones donde se realizaron cambios, no es necesario mostrar todo el archivo). Además agregue una breve descripción de que fue lo que realizó en cada captura.
- Al momento de ingresar a realizar la experiencia en el laboratorio, el grupo deberá presentar el servicio implementado ya funcional, de lo contrario no obtendra la totalidad de puntaje de esta sección.
- Cada imagen que coloque en su informe debe ser legible. A toda imagen sin descripción se les descontará puntaje.
- Para el desarrollo de la experiencia práctica puede hacer uso de los Pdfs y preinformes de las experiencias anteriores como guía.
- Cada grupo dispondrá de 2horas cronológicas para realizar la experiencia. En caso de no terminar el laboratorio, se evaluará con lo que alcanzaron a realizar.
- La evaluación de la experiencia será realizada por el ayudante de turno utilizando una pauta de evaluación.
- Este laboratorio está sujeto a las reglas generales publicadas en la página del laboratorio en *Moodle*.
- Si tiene dudas con el desarrollo del laboratorio, no dude en consultar al correo *labit@listas.inf.utfsm.cl*, en plataforma *Moodle* o directamente en el LabIT.

8. Anexos

8.1. Switches

Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet. Por ende, son los encargados de la interconexión de equipos dentro de una misma red.

Para el caso de esta experiencia, se utilizarán switchs **Cisco Serie 2950 - 24 puertos** los cuales utilizan el estandar Cisco respecto al uso de comandos, esto significa, que utilizan los mismos comandos que un Router Cisco para ingresar y configurar dicho dispositivo.

```
Switch>
Switch>enable
Switch#
Switch#
```

Figura 2: Ingresar a un switch Cisco

De la misma manera, tambien se puede ingresar a la configuración de una interfaz en el switch. Esto será útil al asignar VLAN's e implementar comunicación entre capa 2 y 3.

```
Switch#
Switch#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#
```

Figura 3: Ingresar a configuración y a una interfaz

8.2. VLAN - Virtual Local Área Network

Una VLAN, tambien conocida como Virtual LAN, es un método para agrupa un conjunto de equipos de manera lógica y no física. Con las VLAN uno puede, en un solo *switch*, crear redes virtuales y manejarlas como si fuesen una red real.

La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece diversas ventajas: una mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores; un aumento de la seguridad, puesto que la información se encapsula en un nivel adicional y puede ser analizada; una disminución en la transmisión de tráfico en la red.

Para definir una VLAN dentro de un switch Cisco, se debe utilizar desde la sección *configure* el comando *vlan id* donde id corresponde al número de la VLAN creada:

```
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#name vlan10
Switch(config-vlan)#exit
Switch(config)#
```

Figura 4: Creación de una VLAN

En caso que se deseen **implementar más VLAN's se debe repetir lo anterior**. Cada VLANS debe tener un id diferente, además en un switch viene definida por omisión una VLAN de id 1.

Luego de haber creado una VLAN, se deben asignar los equipos que serán parte de esta red lógica. Para esto se define los modalidad de cada interfaz y la VLAN a la que se encuentra asociada. Dichas modalidades permiten el envío de información entre VLAN y existen 2 modalidades:

- **Modo Access**: Pertenece únicamente a una VLAN asignada de forma estática. Dicha modalidad es **asignada a las interfaces que conectan un PC al switch**.
- **Modo Trunk**: Puede ser miembro de múltiples VLAN. Por defecto es miembro de todas y suele ser **asignado a la interfaz que conecta el switch con el router**.

Supongamos que un switch posee 3 puertos. El puerto 0/1 y 0/2 se encuentran conectados a PC's ubicados en las VLAN1 y VLAN2 respectivamente, mientras que el puerto 0/3 está conectado a un enrutador. Bajo la lógica anterior los puertos 0/1 y 0/2 deben ser configurados con modo Access y el 0/3 con modo Trunk.

```
Switch(config)#
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1
Switch(config-if)#exit
Switch(config)#
```

Figura 5: Configurar Mode Access

Con lo anterior logramos que se asocie la interfaz con la VLAN 1, de modo que solo dicha VLAN pueda enviar mensajes a través de dicha interfaz. Para la interfaz 0/2 debería aplicarse los mismos comandos para asigarle la VLAN 2.

La interfaz al estar conectada a un enrutador, es necesaria configurarla en modo Trunk para que permita el paso de información proveniente de cualquier VLAN, para esto utilizamos la siguiente secuencia de comandos:

```
Switch(config)#
Switch(config)#interface fastethernet 0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allow vlan 1,2
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#
```

Figura 6: Configurar Mode Trunk

De esta manera estamos permitiendo que funcione en modo Trunk y especificamos que pasen únicamente las VLAN 1 y 2.

8.3. Interfaces Virtuales

Pese a crear redes virtuales (VLAN) en el switch, al momento de avanzar al router para configurar la conexión entre Capa de Enlace y Capa de red tendremos el problema que dos o más redes virtuales distintas están intentando salir por una misma boca de red. Fisicamente será imposible para ellas salir por el mismo lugar ya que una boca de red solo puede tener asignada una dirección IP junto con su máscara, por lo que no podrá tener los gateway de todas redes.

En estas situaciones cuando se trabaja con VLAN y se tienen múltiples redes virtuales dentro del Switch, también es necesario virtualizar la interfaz física de red del router. De este modo se tendrán múltiples interfaces virtuales asociadas a cada red por la que podrán ser asignados los gateway de cada una y permitir que se encuentren conectados con el resto de la red.

Para virtualizar una interfaz del router, primero hay que identificar cual se encuentra conectada al switch. Para esta situación supongamos que la interfaz GigabitEthernet 0/0 está conectada al switch que posee las VLAN 1 (Asociada a la red 192.168.1.0/30) y VLAN 2 (Asociada a la red 192.168.2.0/30)

Primero hay que ingresar a dicha interfaz para asegurarse que este encendida en todo momento y no tenga ninguna dirección IP asignada. En caso que si posea debe eliminarse antes de continuar.

```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

Luego podemos crear las interfaces virtuales sobre el puerto físico GigabitEthernet 0/0 con el comando *interface GigabitEthernet 0/0.id* donde id es el nombre o identificador de dicha interfaz. Es recomendable que el id de esta coincida con el de la VLAN a la que se asociará para mayor claridad.

```
Router(config)# interface gigabitEthernet 0/0.1
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, changed state to up

Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip address 192.168.1.1 255.255.255.252
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#
```

Figura 7: Creación y configuración de Interfaz Virtual 1

Esto se repite para la segunda interfaz virtual

```
Router(config)#
Router(config)# interface gigabitEthernet 0/0.2
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.2, changed state to up

Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 192.168.2.1 255.255.255.252
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#
```

Figura 8: Creación y configuración de Interfaz Virtual 2

El comando *encapsulation dot1q id* se usa para encapsular una VLAN a dicha interfaz virtual utilizando el protocolo dot1q, este permite a múltiples redes compartir mismo medio físico, sin problemas de interferencia entre ellas. En este comando el valor de id corresponde al id de la VLAN que se quiera encapsular. Para el caso de la primera interfaz 0/0.1 se encapsula la VLAN1 del switch, en la interfaz 0/0.2 se hace lo mismo con la VLAN2.

8.4. Configurar ACL de uso general

Para explicación correcta y detallada del uso de ACL's tanto simples como extendidas se recomienda revisar la guía resumida de *Cisco* para entender su implementación:

https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html#anc6

8.5. Uso y Configuración básica de Firewall Cisco Asa 5505

En esta experiencia se utilizará de forma básica el componente de Firewall modelo Cisco Asa 5505 para interconectar la red implementada en la experiencia con la red del laboratorio. Para esto se recomienda revisar la guía básica de configuración de *Cisco* para dicho componente de hardward:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/int5505.html