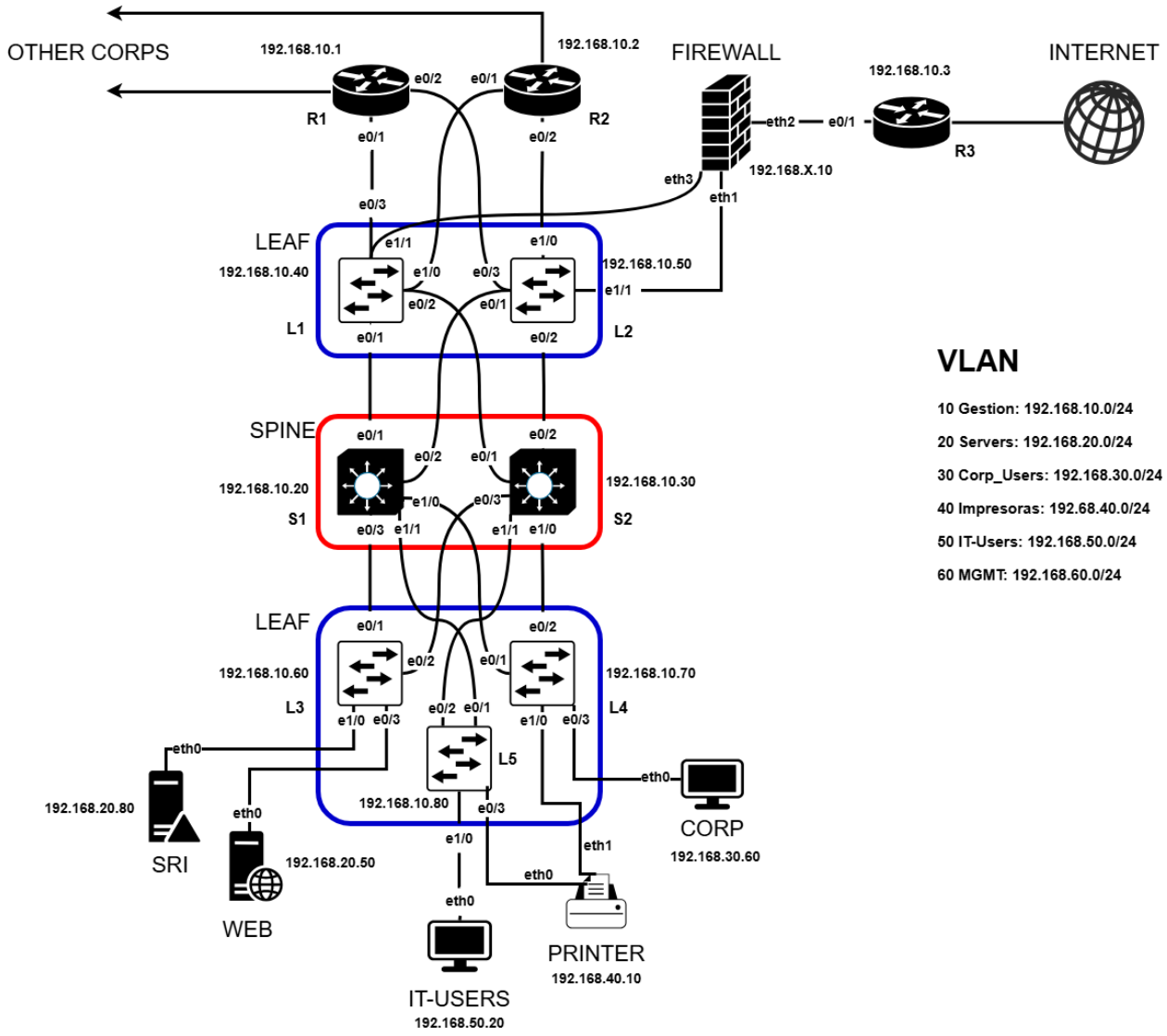
Configuraciones de los dispositivos.



Las explicaciones de las configuraciones están ordenadas de manera lógica, de arriba hacia abajo dejando el firewall para el final. No se expondrán las configuraciones enteras ya que son muy repetitivas, están disponibles en el repositorio de GitHub.

Routers:

R1: Está conectado a los switches L1 y L2.

```
hostname R1
!
interface e0/1
 description Conexión a L1
 no shutdown
!
interface e0/2
 description Conexión a L2
 no shutdown
!
interface e0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 standby 10 priority 110
 standby 10 preempt
!
interface e0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 standby 20 priority 90
 standby 20 preempt
```

interface e0/1
description Conexión a L1
no shutdown

Activamos cada interfaz ethernet utilizada

interface e0/1.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255

Asociamos la subinterfaz a la VLAN correspondiente y le ponemos su dirección IP.

standby 10 priority 110
standby 10 preempt

Definimos la prioridad para que R1 sea el router activo en esta VLAN. Y permitimos que R1 recupere su rol de router activo si vuelve a estar disponible después de una caída.

standby priority 90
standby 20 preemt

Esta interfaz está asociada a la VLAN 20, el router 2 actuará como router activo para esta VLAN, es por eso que le ponemos una prioridad mas baja, para que actúe en caso de fallo en R2.

R2: Conectado a los switches L1 y L2.

```
hostname R2
!
interface e0/1
 description Conexión a L1
 no shutdown
!
interface e0/2
 description Conexión a L2
 no shutdown
!
interface e0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.2 255.255.255.0
 standby 10 priority 90
 standby 10 preempt
!
interface e0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.2 255.255.255.0
 standby 20 priority 110
 standby 20 preempt
```

Configuración idéntica en R2.

La configuración del router 2 es prácticamente igual, pero se puede ver el cambio de nivel de prioridad en cada VLAN.

```
interface e0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.2 255.255.255.0
 standby priority 90
 standby 20 preemt
```

El router 1, tiene 110 de prioridad en esta interfaz, eso significa que el tráfico de la VLAN se irá por él. R2 actuará de backup.

R3: Conectado al Firewall y a internet.

```
hostname R3
!
interface e0/1
 description Conexión al Firewall (FW)
 ip address 192.168.10.3 255.255.255.0
 no shutdown
!
interface e0/0
 description Conexión a Internet
 ip address 198.51.100.1 255.255.255.0
 no shutdown
!
ip routing
```

```
interface e0/1
 description Conexión al Firewall (FW)
 ip address 192.168.10.3 255.255.255.0
 no shutdown
```

Esta es la interfaz conectada al firewall, le asignamos la IP.

```
interface e0/0
 description Conexión a Internet
 ip address 198.51.100.1 255.255.255.0
 no shutdown
```

Esta es la interfaz conectada a internet, la IP asignada es una IP pública que hemos usado de ejemplo.

Switches:

Switch Leaf 1: Está conectado a los Routers 1 y 2, y a los Spine 1 y 2.

```
vlan 10
 name Gestion
vlan 20
 name Servers
vlan 30
 name Corp_Users
vlan 40
 name Impresoras
vlan 50
 name IT-Users
vlan 60
 name MGMT
!
##Asignacion de las interfaces a las VLANs
##Conexion a Spine1
interface e0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60
 no shutdown
!
##Conexion a Spine2
interface e0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60
 no shutdown
```

vlan 10
name Gestion
vlan 20
name Servers ...

Creamos las VLANS en el switch y se le asigna su nombre a cada una.

interface e0/1
switchport trunk encapsulation dot1q
switchport mode trunk

Usamos el protocolo 802.1Q como protocolo de encapsulación de VLANS y establecemos el puerto en modo troncal para permitir el trafico de varias VLANS.

switchport trunk allowed vlan 10,20,30,40,50,60

Permite que pase el tráfico de las VLANS escritas.

En todas las interfaces igual.

Switch Leaf 2: Está conectado a los Routers 1 y 2, y a los Spine 1 y 2. Tiene una configuración idéntica al Switch Leaf 1.

Spine 1: Está conectado a todos los switches Leaf.

```
hostname S1
!
no ip domain-lookup
ip routing
!
interface Ethernet0/1
 no shutdown
!
interface e0/1.10
 encapsulation dot1Q 10
 no shutdown
!
interface e0/1.20
 encapsulation dot1Q 20
 no shutdown
```

no ip domain-lookup
ip routing

Desactiva la búsqueda de DNS para ahorrar tiempo. Y habilita el enrutamiento en caso de añadir IP mas adelante.

interface e0/1.10
encapsulation dot1Q 10
no shutdown
Establece esta subinterfaz para la VLAN 10 y la activa.

interface e0/1.20
encapsulation dot1Q 20
no shutdown
Establece esta subinterfaz para la VLAN 20 y la activa.

Así en cada subinterfaz de las interfaces hasta lograr el tráfico de todas las VLANS por todas las interfaces.

Spine 2: Está conectado a todos los switches Leaf. Tiene una configuración idéntica al Spine1.

Leaf 3: Está conectado a los Spine y a los servidores SRI y WEB.

```
vlan 10
 name Gestion
vlan 20
 name Servers
vlan 30
 name Corp_Users
vlan 40
 name Impresoras
vlan 50
 name IT-Users
vlan 60
 name MGMT
!
##Asignacion de las interfaces a las VLANs
##Conexion a Spine1
interface e0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60
 no shutdown
!
##Conexion a Spine2
interface e0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60
 no shutdown
.
```

vlan 10
name Gestion
vlan 20
name Servers ...

Creamos las VLANS en el switch y se le asigna su nombre a cada una.

Las interfaces conectadas a los Spine las ponemos en modo troncal y permitimos las VLANS listadas, igual que en los Leaf 1 y 2.

```
##Conexion a WEB
interface e0/3
 switchport mode access
 switchport access vlan 20
 no shutdown
!
##Conexion a SRI
interface e1/0
 switchport mode access
 switchport access vlan 20
 no shutdown
!
```

interface e0/3
switchport mode access
switchport access vlan 20

La interfaz se pone en modo access porque está conectada a un host, y se le asigna a la VLAN 20, que es la de los servers.

Leaf 4: Está conectado a los Spine, al host CORP y a la impresora.

```
vlan 10
 name Gestion
vlan 20
 name Servers
vlan 30
 name Corp_Users
vlan 40
 name Impresoras
vlan 50
 name IT-Users
vlan 60
 name MGMT
!
##Asignacion de las interfaces a las VLANs
##Conexion a Spine1
interface e0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60
 no shutdown
!
##Conexion a Spine2
interface e0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60
 no shutdown

##Conexion a Corp_Users
interface e0/3
 switchport mode access
 switchport access vlan 30
 no shutdown
!
##Conexion a Impresoras
interface e1/0
 switchport mode access
 switchport access vlan 40
 no shutdown
!
```

Primera parte idéntica a L3, se crean VLANS y se permite el tráfico de vlans en las interfaces conectadas a los Spine.

interface e0/3
switchport mode access
switchport access vlan 30

La interfaz se pone en modo access porque está conectada a un host, y se le asigna a la VLAN 30 y la VLAN 40 a la interfaz de la impresora.

Igual a L3 pero asignando diferentes VLANS a los hosts.

Leaf 5: Está conectado a los Spine, al host IT-USERS y a la impresora. Tiene una configuración igual que los anteriores, cambiando VLANS. Vlan 50 para IT-USERS y la 40 para la Impresora.

Hosts:

Host_corp, Host_it, Host_printer: Estos host pertenecen cada uno a una vlan distinta, están conectados a L4 y L5. La configuración de los hosts son scripts que se ejecutan una vez esté desplegado el laboratorio.

Todos los host tiene una configuración como esta.

```
cat <<EOT >> /etc/networks
    auto e0
    iface e0 inet dhcp
EOT
 # Restart networking service
cat <<EOT > /etc/resolv.conf
    nameserver 192.168.20.80
    nameserver 8.8.8.8
    search lab.local
```

cat <<EOT >> /etc/networks
auto e0
iface e0 inet dhcp
EOT

Hacemos que coja la IP por DHCP.

cat <<EOT >> /etc/networks
nameserver 192.168.20.80
nameserver 8.8.8.8
search lab.local

Usa el servidor DNS (192.168.20.80) como primera opción.

Servers:

server_sri: Está conectado a L3, es un servidor de red, encargado del servicio DHCP y DNS.

```
# Actualizar repositorios e instalar servicios necesarios
sudo apt update
sudo apt install -y isc-dhcp-server bind9
```

Actualizamos los repositorios e instalamos los servicios necesarios (DHCP y DNS).

```
# Configuración del servidor DHCP
cat <<EOT | sudo tee /etc/dhcp/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;
authoritative;

# Configuración de subred para VLAN 30
subnet 192.168.30.0 netmask 255.255.255.0 {
    range 192.168.30.100 192.168.30.200;
    option routers 192.168.30.1;
    option domain-name-servers 192.168.20.80;
    option domain-name "lab.local";
}

# Configuración de subred para VLAN 40
subnet 192.168.40.0 netmask 255.255.255.0 {
    range 192.168.40.100 192.168.40.200;
    option routers 192.168.40.1;
    option domain-name-servers 192.168.20.80;
    option domain-name "lab.local";
}

# Configuración de subred para VLAN 50
subnet 192.168.50.0 netmask 255.255.255.0 {
    range 192.168.50.100 192.168.50.200;
    option routers 192.168.50.1;
    option domain-name-servers 192.168.20.80;
    option domain-name "lab.local";
}
EOT
```

cat <<EOT | sudo tee /etc/dhcp/dhcpd.conf

Esto crea y sobreescribe el archivo de configuración de dhcp con el contenido de debajo.

Configuración de subred para VLAN

Dentro de ese archivo se le asigna un rango de IPs y una puerta de enlace a cada VLAN.

```
# Configuración del servidor DNS
cat <<EOT | sudo tee /etc/bind/named.conf.local
zone "lab.local" {
    type master;
    file "/etc/bind/db.lab.local";
};

zone "20.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192.168.20";
};
EOT

cat <<EOT | sudo tee /etc/bind/db.lab.local
\$TTL 604800
@   IN  SOA ns.lab.local. admin.lab.local. (
        2025051401 ; Serial
        604800     ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )   ; Negative Cache TTL

; Nameservers
@   IN  NS  ns.lab.local.

; Wildcard redirection
*   IN  A   192.168.20.80

; Specific records
ns  IN  A   192.168.20.80
EOT

cat <<EOT | sudo tee /etc/bind/db.192.168.20
\$TTL 604800
@   IN  SOA ns.lab.local. admin.lab.local. (
        2025051401 ; Serial
        604800     ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )   ; Negative Cache TTL

@       IN  NS      ns.lab.local.

80      IN  PTR     ns.lab.local.
```

cat <<EOT | sudo tee /etc/bind/named.conf.local

Esto crea y sobreescribe el archivo de configuración de DNS con el contenido de debajo.

zone “lab.local” {...}
Esto crea un archivo de zona local tipo master cuyo archivo de configuración es “db.lab.local”.

zone "20.168.192.in-addr.arpa" {...}
Esto crea una zona inversa tipo master igual que en la directa.

cat <<EOT | sudo tee /etc/bind/db.lab.local

Crea y sobreescribe la configuración de la zona directa.
SOA: información del servidor autoritativo para la zona.
NS: define el servidor de nombres.
*** IN A 192.168.20.80:** cualquier nombre *.lab.local apunta a este servidor.
ns IN A 192.168.20.80: entrada explícita para el servidor DNS.

cat <<EOT | sudo tee /etc/bind/db.192.168.20

Configura la zona inversa.

server_web: Está conectado a L3, es un servidor de red, encargado del servicio DHCP y DNS.

```
sudo mkdir -p /var/www/corp.lab.local /var/www/ituser.lab.local /var/www
```

sudo mkdir

Creamos carpetas para crear un sitio por cada VLAN.

```
# Crear archivos index.html personalizados para cada sitio
echo "<h1>Bienvenido a corp.lab.local</h1>" > /var/www/corp.lab.local/index.html
echo "<h1>Bienvenido a ituser.lab.local</h1>" > /var/www/ituser.lab.local/index.html
echo "<h1>Bienvenido a impresoras.lab.local</h1>" > /var/www/impresoras.lab.local/index.html
echo "<h1>Bienvenido a www.lab.local</h1>" > /var/www/www.lab.local/index.html
```

echo

Se crea un archivo .html en cada directorio para que tengan sitio personalizado.

```
sudo mkdir -p /var/www/corp.lab.local /var/www/ituser.lab.local /var/www/

cat <<EOT | sudo tee /etc/apache2/sites-available/corp.lab.local.conf
<VirtualHost *:80>
    ServerName corp.lab.local
    DocumentRoot /var/www/corp.lab.local

    <Directory /var/www/corp.lab.local>
        Require ip 192.168.30.0/24 192.168.50.0/24
    </Directory>
</VirtualHost>
EOT

cat <<EOT | sudo tee /etc/apache2/sites-available/ituser.lab.local.conf
<VirtualHost *:80>
    ServerName ituser.lab.local
    DocumentRoot /var/www/ituser.lab.local

    <Directory /var/www/ituser.lab.local>
        Require ip 192.168.50.0/24
    </Directory>
```

cat <<EOT

Creamos y modificamos u archivo de configuración en cada carpeta creada.

Require ip
En cada archivo se configura que solo puedan acceder los hosts que pertenezcan a dicha VLAN.

Firewall:

```
config system interface
    edit "vlan10"
        set vdom "root"
        set interface "port1"
        set vlanid 10
        set ip 192.168.10.10 255.255.255.0
        set allowaccess ping https ssh
        set type vlan
    next
    edit "vlan20"
        set vdom "root"
        set interface "port1"
        set vlanid 20
        set ip 192.168.20.10 255.255.255.0
        set allowaccess ping https ssh
        set type vlan
    next
    edit "vlan30"
        set vdom "root"
        set interface "port1"
        set vlanid 30
        set ip 192.168.30.10 255.255.255.0
        set allowaccess ping https ssh
        set type vlan
```

Se crean todas las VLANS y se le asigna su ip a cada una.

```
config firewall policy
    edit 1
        set name "Mgmt VLAN 10"
        set srcintf "vlan10"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next

    edit 2
        set name "VLAN 20 to VLAN 30"
        set srcintf "vlan20"
        set dstintf "vlan30"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
```

 # Permitir tráfico de gestión(edit 1)
Permite el trafico de la VLAN 10 (gestión) en cualquier red.

 # Permitir tráfico entre servidores (edit 2)
Permite que los servidores (VLAN 20) se comuniquen con los usuarios CORP (VLAN 30).

```
 edit 3
     set name "Printers to Corp Users"
     set srcintf "vlan40"
     set dstintf "vlan30"
     set srcaddr "all"
     set dstaddr "all"
     set action accept
     set schedule "always"
     set service "ALL"
     set logtraffic all
 next
```

 # Permitir tráfico de impresoras
Permite que las impresoras (VLAN 40) se comuniquen con los usuarios CORP (VLAN 30).

```
# Permitir tráfico de usuarios IT
edit 4
    set srcintf "vlan50"
    set dstintf "any"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
next
```

 # Permitir tráfico de usuarios
Permite que los usuarios IT (VLAN 50) tenga acceso a cualquier lado.

```
# Bloquear cualquier otro trá
edit 5
    set srcintf "any"
    set dstintf "any"
    set srcaddr "all"
    set dstaddr "all"
    set action deny
    set schedule "always"
    set service "ALL"
    set logtraffic all
next
```

 # Bloquear cualquier otro tráfico
Bloquea cualquier trafico que no esté permitido en las reglas anteriores.