Fabian **Escalona**
Ingeniero en redes y comunicaciones

1 PROBLEMA

La empresa en cuestión cuenta con múltiples sucursales alrededor del país y con el pasar del tiempo sus necesidades tecnológicas han ido aumentando y los antiguos esquemas de conexión ya no soy viables debido a que se requiere más ancho de banda, mayor tolerancia y una escalabilidad notable para poder implementar nuevos servicios en la red. Por estos factores la empresa comenzó a migrar sus enlaces antiguos Frame Relay a enlaces radiales con Ethernet a implementar sistemas Fail Over y mejorar sus equipos de borde.

El proyecto en cuestión está focalizado a los medios de conexión, configuraciones y los problemas más comunes en caso del uso de diferentes ISP omitiendo las configuraciones de VPN y encriptación por motivos de seguridad.

2 SOLUCIÓN

"configuraciones VPN, QoS y enrutamiento ha sido obviado en esta sección por ser termas confidenciales, los esquemas y direcciones IP han sido cambiadas"

El escenario en esta ocasión es una sucursal remota que tiene la compañía, los parámetro de configuración se duplicaran en cada router de borda de la red, el esquema de conexión es similar al siguiente.

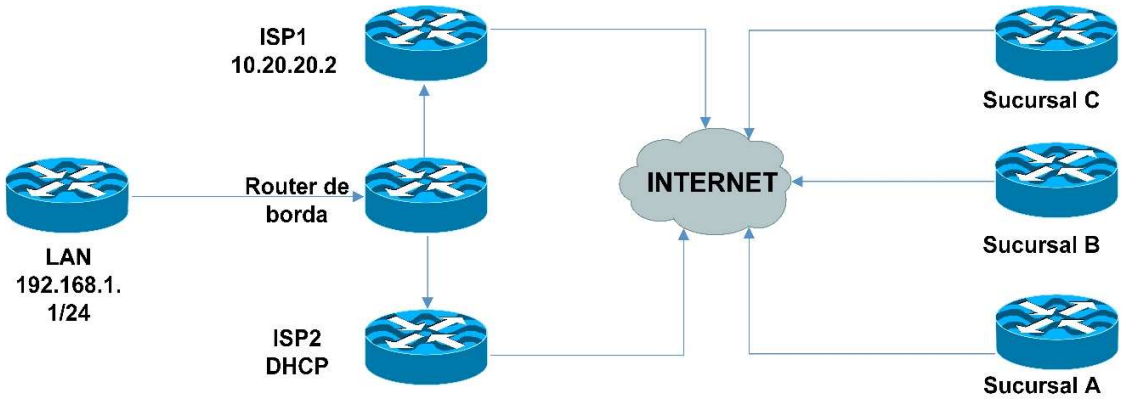

Diagrama 2.1 "*Esquema de red*"

En esta topología el punto focal son los Routers de borda, los cuales tienen interacción directa con los diferentes ISP para lograr una comunicación exitosa con un sistema Fail Over debe cumplir ciertos requisitos, la configuración debe ser capaz de:

- Verificar la conexión del ISP a la red.
- Cambiar y devolver el cambio de enlace sin intervención humana.
- Proveer un nateo automático de un enlace a otro

A continuación se desglosa la configuración de router de borda para entender a fondo como funciona

Conexiones del router

```
Interface FastEthernet0/0.1
 Description ISP1
 Bandwidth 2048
 Encapsulation dot1Q 1 native
 ip address 10.20.20.1 255.255.255.0
 ip Nat outside
 ip virtual-reassembly
!
Interface FastEthernet0/0.2
 Description ISP2
 Bandwidth 2048
 Encapsulation dot1Q 2
 ip address dhcp
 ip Nat outside
 ip virtual-reassembly
```

El direccionamiento en el ISP2 es otorgado por un servidor DHCP; se recomienda establecer un ancho de banda así el router sabrá hasta que limite puede transmitir en ese canal y no se sobrepasa la tasa de transferencia.

IP SLA

```
track 1 rtr 1 reachability
ip sla 1
 icmp-echo 10.20.20.2 source-interface FastEthernet0/0.1
 threshold 3
 frequency 5
ip sla schedule 1 start-time now
```

El IP SLA es el encargado de verificar mediante un ping el estado de la conexión del ISP1 en este caso, cumpliendo así el primero ítem de nuestra lista "*Verificación de conexión*"

IP Route

```
ip route 0.0.0.0 0.0.0.0 128.1.1.1 254 track 1
ip route 0.0.0.0 0.0.0.0 Interface FastEthernet0/0.2 20
```

El track verifica la conexión del ISP1 dejando la otra ruta flotante gracias a la distancia administrativa aplicada. Cuando el track está **UP** el tráfico se canaliza por el ISP1 pero cuando el track está **DOWN** los datos fluyen por el ISP2, el track seguita intentando alcanzar su destino y en el momento que lo haga el cambio de ISP se devuelve quedando las conexiones como al principio de esa manera marcamos el segundo ítem de nuestra lista *"Cambio y devolución de cambio de ISP automáticamente*"

Route-Map y Access-List

```
route-map ISP2 permit 10
 match ip address 100
 match interface FastEthernet0/0.2
!
route-map ISP1 permit 10
 match ip address 100
 match interface FastEthernet0/0.1

access-list 100 permit ip 192.168.1.0 0.0.0.255 any
```

El route-map nos permite hacer un match de las direcciones internas a la red externa y las Access-list confirman el pool de direcciones.

NAT

```
ip nat translation tcp-timeout 1
ip nat translation udp-timeout 1
ip nat translation routemap-entry-timeout 1
ip nat translation icmp-timeout 1
ip nat inside source route-map ISP1 interface FastEthernet0/0.1 overload
ip nat inside source route-map ISP2 interface FastEthernet0/0.2 overload
```

Como se destaca en la configuración del NAT el route-map entra en los parámetros de traducción y las interfaces de los proveedores están declaradas ambas con overload para poder hacer una traducción instantánea para las direcciones, de esa manera cumplimos con el ultimo ítem de la lista "*Nateo automático entre enlaces*"

Los cambios deben ser imperceptibles para el usuario, todo el proceso debe ser automático y para lograrlo se implementó una configuración que involucra una combinación de políticas y protocolos de manera tal que trabajen unidos.

3 RESULTADOS

Al finalizar el proyecto se entregó una red estable con un sistema funcional de Fail Over el cual cumple con los requisitos del cliente y da la confianza en la red que tanto se buscaba para brindar los nuevos servicios, entre las dificultades del proyecto se encontraba el uso de una sola interfaz por motivo de falta de recursos, usando un solo radio para los dos ISP y contando con un solo puerto Ethernet, no obstante la encapsulación trabaja perfectamente conjunto a todas las políticas de QoS y enrutamiento. El proyecto se ejecutó mediante conexiones segura SSH y en algunos casos conexiones directas por consola en sucursales remotas, el tiempo de trabajo para realizar todas las configuraciones tomo alrededor de tres (3) días en completar las 22 sucursales alrededor del país.

Se recomienda:

- Monitoreo de la red
- Implementar enlaces MPLS para la calidad de servicio
- Tener equipos de BackUp configurados
- Contar con un plan alterno debido a que un solo radioenlace no es suficiente

Los planes de Fail Over son complejos pero necesarios en empresas que demandan una gran cantidad de servicios internos y externos.