ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Conmutación y Enrutamiento - TLMG1009: Proyecto Final

Sistemas de Respaldos Diarios Automáticos

Lino Ontano
Telemática
Guayaquil - Ecuador
lontano@espol.edu.ec

Julio Bodero
Telemática
Guayaquil - Ecuador
jcbodero@espol.edu.ec

Cesar Navas
Telemática
Guayaquil - Ecuador
cesanava@espol.edu.ec

Josue Martínez
Telemática
Guayaquil - Ecuador
josvmart@espol.edu.ec

Eduardo Veintimilla
Telemática
Guayaquil - Ecuador
edujvein@espol.edu.ec

***Resumen*—Este proyecto permitirá explicar el funcionamiento del sistema de respaldos diarios automáticos, las herramientas utilizadas y las configuraciones pertinentes en los dispositivos intermediarios para poder realizar el respaldo y la consulta.**

I. INTRODUCCIÓN

Es necesario en una empresa, sea de grande o pequeña escala, tener las redes de sus sucursales siempre disponibles; de esta manera se garantiza el servicio que ofrece y el soporte a su empresa sin importar en que sucursal se encuentre el problema. Existen varias soluciones para mantener la alta disponibilidad de nuestra empresa, pero el riesgo de fallo siempre existirá y es ahí cuando el ingeniero de networking debe tener la solución disponible en un tiempo corto de respuesta. Por eso, la configuración de los dispositivos intermediarios de nuestra red es importante que esté al alcance de la persona encargada de dar soporte a la empresa, sin importar donde se encuentre. Este proyecto permite acceder a la configuración de los equipos intermediarios de nuestra red, en este caso utilizamos de ejemplo una red con tres dispositivos intermediarios, dos sucursales y una matriz. El aplicativo elaborado en el presente proyecto permite realizar un sistema de respaldo diario de estos dispositivos, así como una consulta de los mismos por fecha o por dispositivo. De esta manera ofrecemos una base de datos que servirá para ayudar a mitigar los problemas de fallas ya que se podrá acceder a los archivos de configuración de cualquier sucursal e identificar una posible mala configuración o un mal funcionamiento del mismo.

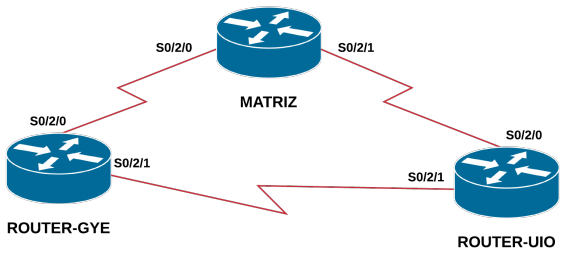

Figura 1: *Diagrama de red de las sucursales a respaldar*

II. ANTECEDENTES

II-A. *Dispositivos intermediarios:*

Los dispositivos intermediarios interconectan dispositivos finales. Estos dispositivos proporcionan conectividad y operan detrás de escena para asegurar que los datos fluyan a través de la red. Los dispositivos intermediarios conectan los hosts individuales a la red y pueden conectar varias redes individuales para formar una internetwork.
Los siguientes son ejemplos de dispositivos de red intermediarios:

- Acceso a la red (switches y puntos de acceso inalámbrico)
- Internetworking (routers)
- Seguridad (firewalls)

II-B. *Protocolo SSH:*

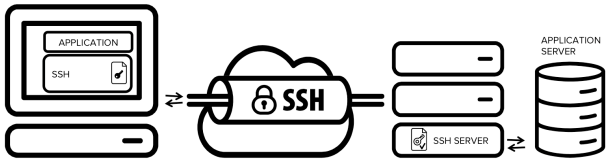

Figura 2: *Funcionamiento del protocolo SSH*

SSH (o *Secure SHell*) es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada. SSH trabaja de forma similar a como se hace con *telnet*. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible, evitando que terceras personas puedan descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos. El protocolo TCP asignado es el 22.

II-C. *Protocolo de Transferencia de Archivos FTP:*

FTP es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.

Asterisk incluye muchas características que anteriormente sólo estaban disponibles en costosos sistemas propietarios PBX, como buzón de voz, conferencias, IVR, distribución automática de llamadas, y otras muchas. Los usuarios pueden crear nuevas funcionalidades escribiendo un dialplan en el lenguaje de script de *Asterisk* o añadiendo módulos escritos en lenguaje C o en cualquier otro lenguaje de programación soportado en GNU/Linux.

Uno de los puntos fuertes del software *Asterisk* es que permite la unificación de tecnologías: VoIP, GSM y PSTN.

Asterisk se empieza a adoptar en algunos entornos corporativos como una gran solución de bajo coste junto con SER (Sip Express Router).

II-D. *OSPF:*

Open Shortest Path First (OSPF), Primer Camino Más Corto, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF construye además una base de datos enlace-estado (Link-State Database, LSDB) idéntica en todos los routers de la zona.

Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red a la que se encuentran conectadas el resto de áreas de la misma. Las rutas entre las diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

III. Desarrollo del concepto

Para el desarrollo de nuestro proyecto, nos basamos en la red de la figura 3, donde planteamos que desde cualquier red de las sucursales, por medio de un aplicativo, poder consultar

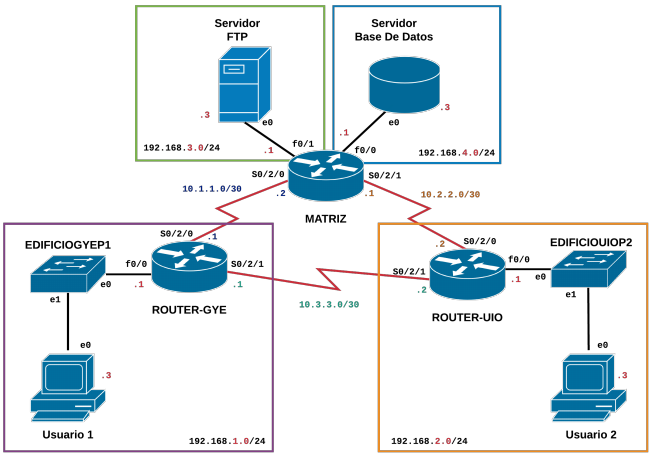

Figura 3: *Diagrama completo de red de nuestra empresa. Se observa que los dispositivos intermediarios interconectan dos sucursales diferentes con la matriz.*

a cualquier dispositivo intermediario presente de la red y hacer respaldos y consultas de los mismos. Para ello, el aplicativo cuenta con autenticación para ser utilizado, es decir la empresa tendrá una base de datos de usuarios que pueden realizar la gestión de resplado y consultas por medio del aplicativo, además de descargar dichos archivos de consultas. Todo estas conexiones se realizan por medio del protocolo SSH, que nos permite hacer conexión y adquirir los datos de los dispositivos intermediarios de manera segura.

IV. Diseño e Implementación

El desarrollo del presente proyecto se realizó basándonos en el diagrama de la figura 3, teniendo que configurar cada dispositivo presente en el diagrama de acuerdo a las redes en las que se encuentran. Nos basamos en la tabla I para asignar las direcciones IPs de los dispositivos finales y de las interfaces de los dispositivos intermediarios.

Dispositivo	Interfaz	Dirección/Máscara	Gateway
ROUTER-GYE	f0/0	192.168.1.1/24	n/a
	s0/2/0	10.1.1.1/30	n/a
	s0/2/1	10.3.3.1/30	n/a
ROUTER-UIO	f0/0	192.168.2.1/24	n/a
	s0/2/0	10.2.2.2/30	n/a
	s0/2/1	10.3.3.2/30	n/a
MATRIZ	f0/0	192.168.3.1/24	n/a
	f0/1	192.168.4.1/24	n/a
	s0/2/0	10.1.1.2/30	n/a
	s0/2/1	10.2.2.1/30	n/a
Usuario 1	NIC	192.168.1.3/24	192.168.1.1
Usuario 2	NIC	192.168.2.3/24	192.168.2.1
Servidor DB	NIC	192.168.3.3/24	192.168.3.1
Servidor FTP	NIC	192.168.4.3/24	192.168.4.1

Cuadro I: *Direccionamiento de red de la figura 3*

Observe que las interfaces de los dispositivos intermediarios

son importantes en este proceso, ya que una interfaz mal configurada hará que no exista conectividad entre redes. Para interconectar las redes utilizamos el protocolo OSPF, el cual se configura en cada enrutador sucursal y en el enrutador matriz.
La configuración de cada enrutador dependerá del cuadro de direcciones I, se le asigna en primer lugar el direccionamiento y se habilita el protocolo OSPF para interconectar las redes. Para el caso del enrutador MATRIZ, sería como sigue:

```
conf t
router ospf 1
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
network 10.1.1.0 0.0.0.3 area 0
network 10.2.2.0 0.0.0.3 area 0
exit
int f0/0
ip address 192.168.3.1 255.255.255.0
no shut
int f0/1
ip address 192.168.4.1 255.255.255.0
no shut
int s0/2/0
ip address 10.1.1.2 255.255.255.252
no shut
int s0/2/1
ip address 10.2.2.1 255.255.255.252
no shut
end
write memory
```

Ahora, ya teniendo la red configurada, se requiere el acceso a los enrutadores vía SSH, para lo que de igual manera requiere ser configurado para cada enrutador, como sigue:

```
conf t
ip domain-name router.matriz
crypto key generate rsa
1024

ip ssh time-out 30
ip ssh authentication-retries 3
ip ssh version 2
username admin privilege 15 password admin
line vty 0 4
transport input ssh
login local
end
write memory
```

Ya en este punto, podemos acceder a los enrutadores vía SSH.
La parte de la aplicación, requiere un servidor FTP y un servidor de Base de Datos; ambos en este caso, se encuentran conectados en el enrutador MATRIZ. El servidor FTP permitirá la descarga de los archivos que se generen de los respaldos y el servidor de la base de datos llevará un control de las actividades que se realicen por medio de la aplicación. La aplicación fue desarrollada en Java, y es ella la que realiza la conexión por SSH con los enrutadores y genera los archivos de configuración de cada enrutador. El administrador selecciona cual enrutador desea generar respaldo o consultar los respaldos generados como se observa en la figura 4.
Para mayor información acerca de la aplicación pueden consultar el repositorio de gitHub de este proyecto **aquí**.

(a) Inicio de sesión

(b) Consulta de archivos de respaldo

Figura 4: *Interfaz gráfica de la aplicación.*

V. Conclusiones

- Es importante el manejo de logs en redes que demanda el uso de varios dispositivos ya que ayuda a detectar fallas y corregir errores en los dispositivos causantes.
- La configuración de los dispositivos es el punto clave para que exista forma de conectar la aplicación con nuestra red.
- El sistema de respaldo diarios permite control remoto de dispositivos de una empresa ayudando al soporte técnico a reducir gastos.

VI. Recomendaciones

- El protocolo FTP a largo plazo se tendrá que cambiar por un protocolo más seguro.
- Es indispensable realizar una aplicación compatible con dispositivos móviles para hacer que el sistema sea multiplataforma, de esta manera dará mayor alcance el presente proyecto.

Referencias

[1] J. Moy: RFC 2328, "OSPF Version 2" , IETF (abril de 1998)
[2] Daniel J. Barrett, Richard E. Silverman, and Robert G. Byrnes, "SSH: The Secure Shell (The Definitive Guide)", O'Reilly 2005 (2nd edition). ISBN 0-596-00895-3.
[3] Gleason, Mike, "The File Transfer Protocol and Your Firewall/NAT", Ncftp.com (2005).