

Reporte: Tercera evaluación práctica

Administración de Servicios en Red

Huerta Martínez Jesús Manuel, Monteón Valdés Raúl Kevin, Olivares García Marco Antonio
Escuela Superior de Cómputo, IPN

6 de diciembre de 2018

1. Introducción	1
2. Marco teórico	2
2.1. Enrutamiento estático	2
2.2. Protocolo de enrutamiento RIP	2
2.3. Protocolo de enrutamiento OSPF	3
2.4. Supervisión de servidores	3
3. Desarrollo de la práctica	5
3.1. Tarea 1: Configuración de dispositivos IP	5
3.2. Tarea 2: Supervisión de servidores	7
3.2.1. Supervisión de los servidores de correo electrónico	7
3.2.2. Supervisión de los servidores web	9
3.2.3. Supervisión de servidores de archivos	10
3.2.4. Supervisión de impresoras	13
3.2.5. Supervisión de acceso remoto	16
3.3. Tarea 3: Recopilación de información de dispositivos de manera periódica	17
4. Conclusiones	24
4.1. Huerta Martínez Jesús Manuel	24
4.2. Monteón Valdés Raúl Kevin	24
4.3. Olivares García Marco Antonio	24

CAPÍTULO 1

Introducción

Una red de computadoras (también llamada red informática) es un conjunto de equipos (computadoras y dispositivos), conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, para compartir información (archivos), recursos (discos, impresoras, programas, etc.) y servicios (acceso a una base de datos, internet, correo electrónico, chat, juegos, etc.). A cada una de las computadoras conectadas a la red se le denomina un nodo. [1]

Hoy en día, las redes de computadoras, se han vuelto fundamentales en las empresas, pues se les han encontrado numerosos aspectos que facilitan los procesos y la comunicación dentro de la misma.

Hay al menos 3 ventajas básicas por las que te beneficiaría disponer de una buena red de ordenadores en un entorno empresarial. No nos referimos sólo a la conexión a Internet, sino al uso de otros dispositivos.

- Podrás compartir los recursos informáticos. Supongamos que en una empresa trabajan 20 o 30 personas en las que hay idéntico número de computadoras. Si instalamos una red local, todos podrían transmitir los archivos con los que están trabajando en su PC, incluso si se encuentran en dos edificios distintos (en un radio cercano). Esto quiere decir que puede compartirse el software y los archivos comerciales de una manera mucho más rápida y eficiente.
- Tendrás más velocidad de transmisión de datos. Cuando conectamos las computadoras en red, comparten también su capacidad de transmisión de datos, de manera que la gestión de las tareas se vuelve mucho más ágil y rápida, con el ahorro de tiempo y esfuerzo que esto supone. Una red puede tener velocidad desde 10 Mbps hasta 1 Gbps.
- 3. Ahorrarás en hardware, software y espacio. No es necesario disponer, por ejemplo, de decenas de impresoras en la planta de un mismo edificio. Basta con que haya una central que esté conectada en red y todos podrán imprimir en la misma. Además podrás usar software de red. Esto supone un importante ahorro de dinero, pero también permite disponer sólo de los dispositivos necesarios. [2]

En el presente documento se tratan las diferentes formas para establecer una red y la forma en que se logra comunicar la misma por medio de protocolos de enrutamiento y se describen ejemplos de sensores que pueden ser útiles en las redes para conocer su estado y la información que en éstas se comparte.

La planeación y distribución de una red son de gran importancia, pues es gracias a ésta que se podrán realizar el intercambio de información, comunicación y monitoreos de comportamientos.

Existen diferentes formas de distribuir una red, haciendo uso de dispositivos de red (routers, switches, modems, etc.), para el presente mencionamos tres: estático, protocolo RIP y protocolo OSPF, mismas que se describen detalladamente a continuación.

2.1. Enrutamiento estático

Método que otorga a los ingenieros de redes control absoluto sobre las rutas por las que se transmiten los datos en una internetwork. Para adquirir este control, en lugar de configurar protocolos de enrutamiento dinámico para que creen las tablas de enrutamiento, se crean manualmente. Es importante entender las ventajas y desventajas de la implementación de rutas estáticas, porque se utilizan extensamente en internetworks pequeñas y para establecer la conectividad con proveedores de servicios. Escribir una ruta estática en un router es especificar una ruta y un destino en la tabla de enrutamiento, y que los protocolos de enrutamiento hacen lo mismo, sólo que de manera automática. Sólo hay dos maneras de completar una tabla de enrutamiento: manualmente (el administrador agrega rutas estáticas) y automáticamente (por medio de protocolos de enrutamiento dinámico).

[3]

2.2. Protocolo de enrutamiento RIP

El protocolo Routing Information Protocol (RIP) es un protocolo de enrutamiento del tipo vector distancia. Los protocolos de enrutamiento vector distancia calculan la mejor ruta para encaminar los paquetes IP hacia su destino correspondiente utilizando como métrica el número de saltos (Hop Count). RIP soporta un máximo de 15 saltos. Cualquier ruta que esté a más de 15 saltos se considera inalcanzable.

Cuando un usuarios se conecta el servidor de terminales (equipo en el que finaliza la llamada) avisa con un mensaje RIP al router más cercano advirtiéndolo de la dirección IP que ahora le pertenece. Así podemos ver que RIP es un protocolo usado por distintos routers para intercambiar información y así conocer por donde deberían enrutar un paquete para hacer que éste llegue a su destino.

El protocolo cuenta con las siguientes ventajas con respecto a otros protocolos:

- Fácil de configurar.

- Implementa un algoritmo de encaminamiento más simple.
- Es soportado por la mayoría de los fabricantes. [4]

2.3. Protocolo de enrutamiento OSPF

El protocolo Open Shortest Path First (OSPF) es un protocolo de enrutamiento abierto — no propietario — del tipo Link State. Este fue desarrollado por la organización IETF como un Interior Gateway Protocol (IGP) con el objetivo de reemplazar al protocolo RIP.

OSPF utiliza el algoritmo Dijkstra para encontrar la mejor ruta hacia la red destino. Su métrica es el Cost y utiliza como variable el Bandwidth. OSPF es un protocolo Classless, lo que significa que soporta VLSM y CIDR. A diferencia de los protocolos de enrutamiento Distance Vector, los protocolos Link State NO requieren el intercambio de tablas de enrutamiento en intervalos específicos — RIP intercambia tablas cada 30 segundos — más bien sólo cuando ocurren cambios en la topología de la red. También cuentan con la flexibilidad de enviar las tablas de enrutamiento de manera parcial o total. OSPF es en la actualidad el protocolo IGP más utilizado en el mundo junto al IS-IS.

Dentro de los protocolos de enrutamiento incluidos en el currículo de Cisco CCNA (RIP, EGRP, OSPF), OSPF es el más complejo en cuanto su configuración se refiere. Esta complejidad proviene de la naturaleza intrínseca del protocolo, ya que OSPF está diseñado para trabajar en redes grandes y complejas. [5]

Con esto, el objetivo de la administración de la configuración es supervisar la red y la información de configuración del sistema. Además de rastrear y administrar los efectos de varias versiones de elementos de hardware y software sobre la operación de la red.

2.4. Supervisión de servidores

Como se menciona con anterioridad, la supervisión de la comunicación en una red, así como la información que en ésta se comparte es de vital importancia, pues nos permite conocer el estado de la misma y lo que viaja por sus caminos. Así, enlistamos ejemplos de áreas a supervisar en una red.

Supervisión de los servidores de correo electrónico:

Todos los administradores deben supervisar la funcionalidad de sus servidores de correo. Esto significa supervisar la disponibilidad, el rendimiento y la entrega de correos electrónicos sin errores.

- Sensor SMTP & IMAP Round Trip: Este sensor usa SMTP e IMAP para supervisar la entrega de su correo electrónico de extremo a extremo.
- Sensor SMTP & POP3 Round Trip: Este sensor usa SMTP y POP3 para supervisar la entrega de su correo electrónico de extremo a extremo.

El sensor de ida y vuelta de SMTP e IMAP supervisa el tiempo que tarda un correo electrónico en llegar a un buzón del Protocolo de acceso a mensajes de Internet (IMAP) después de enviarse mediante el Protocolo simple de transferencia de correo (SMTP). Envía un correo electrónico utilizando el dispositivo principal como servidor SMTP y luego escanea un buzón IMAP dedicado hasta que llega este correo electrónico.

El sensor de ida y vuelta de SMTP e IMAP eliminará estos correos electrónicos automáticamente del buzón de correo tan pronto como el se recupere. Los correos electrónicos solo permanecerán en el buzón, especialmente si se produjo un tiempo de espera o un reinicio del servidor durante el tiempo de ejecución del sensor. El sensor muestra lo siguiente:

- Tiempo de respuesta del servidor SMTP.
- Tiempo de respuesta del servidor IMAP.

CAPÍTULO 2. MARCO TEÓRICO

- Suma de ambos tiempos de respuesta.

Supervisión de los servidores de correo electrónico:

El rendimiento del sitio web es un factor decisivo para muchas empresas, mucho más cuando ellas ofrecen productos y servicios a través de sus sitios web. El tiempo de inactividad es costoso desde el primer segundo.

Sensor HTTP – El sensor HTTP supervisa los servidores de información y muestra lo siguiente:

- Tiempo de respuesta (carga) de una solicitud HTTP.
- Cuántos bytes ha recibido.
- Ancho de banda de descarga (velocidad).

Supervisión de servidores de archivos

Si las empresas no pueden acceder a la información entonces nada funciona. Por lo tanto, una de las principales tareas de los administradores es asegurar que el servidor de archivos está disponible y que funciona sin ningún tipo de problema.

Los servidores FTP son centros de descargas que proporcionan datos, aplicaciones, controladores y actualizaciones de software a sus clientes y compañeros de trabajo.

Sensor FTP – El sensor FTP supervisa los servidores de archivos que usan el protocolo de transferencia de archivos (FTP) o FTP sobre SSL (FTPS). Muestra lo siguiente:

- Tiempo de respuesta del servidor.
- Respuesta del servidor.

Sensor FTP Server File Count- El sensor FTP Server File Count se conecta a un servidor de protocolo de transferencia de archivos (FTP) y supervisa los cambios en los ficheros. Puede mostrar el recuento de archivos de un directorio seleccionado.

Supervisión de impresoras

Las impresoras deben trabajar y no interrumpir los flujos de trabajo. Los empleados no deben tener que considerar si la impresora está lista y si todavía hay suficiente tóner.

Sensor de Impresión: El sensor de impresión supervisa varios tipos de impresoras usando SNMP. Muestra la siguiente información:

- Total de páginas impresas,
- Nivel de los cartuchos y/o tonners.
- Estado de la impresora.

Supervisión de acceso remoto

El acceso remoto debe ser controlado en todo momento. Un administrador de red debe controlar las conexiones de acceso remoto a su red.

Sensor de acceso remoto- Un sensor de acceso remoto controla las conexiones de protocolos como RDP, SSH, Telnet, and VNC. Muestra la siguiente información:

- Número de conexiones.
- Tráfico enviado y recibido.
- Tiempo de actividad de las conexión.

Desarrollo de la práctica

Para el desarrollo la presente práctica, se retoman los conocimientos adquiridos en el salón de clases referente a la administración de una red. Concretamente aquellos concernientes a la creación de topologías de red y sus enrutamientos, además de los sensores que se pueden aplicar a las antes mencionadas.

Así, debajo se plasman diversas tareas específicas aplicables a una red, con las cuales se pretende realizar la predicción, mismas que, gracias a las técnicas descritas, se pueden llevar a cabo con éxito. Reforzando y comprobando entonces, las lecciones vistas en clase.

A continuación, se describen cada una de las tareas mencionadas.

3.1. Tarea 1: Configuración de dispositivos IP

Para la realización de la tarea 1, se propone una red, para la cual se hace uso de GNS3, en donde se establecen 5 routers, así como otros dispositivos como computadora o túneles UDP.

A continuación, se muestra un diagrama con la topología propuesta:

Así, una vez realizada la topología previamente mostrada, se procede a realizar en enlace y enrutamiento de cada nodo, para ello se hace uso de enrutamiento estático, o de protocolos como RIP y OSPF. Debajo se muestra un ejemplo de configuración para uno de los routers, haciendo uso del protocolo de enrutamiento RIP.

```
en
conf
hostname R2
interface ethernet eth0
ip address 192.168.2.1/24
no sh
exit
interface ethernet eth0
ip address 192.168.4.1/24
no sh
exit
router rip
network 192.168.2.1/24
network 192.168.4.1/24
```

CAPÍTULO 3. DESARROLLO DE LA PRÁCTICA

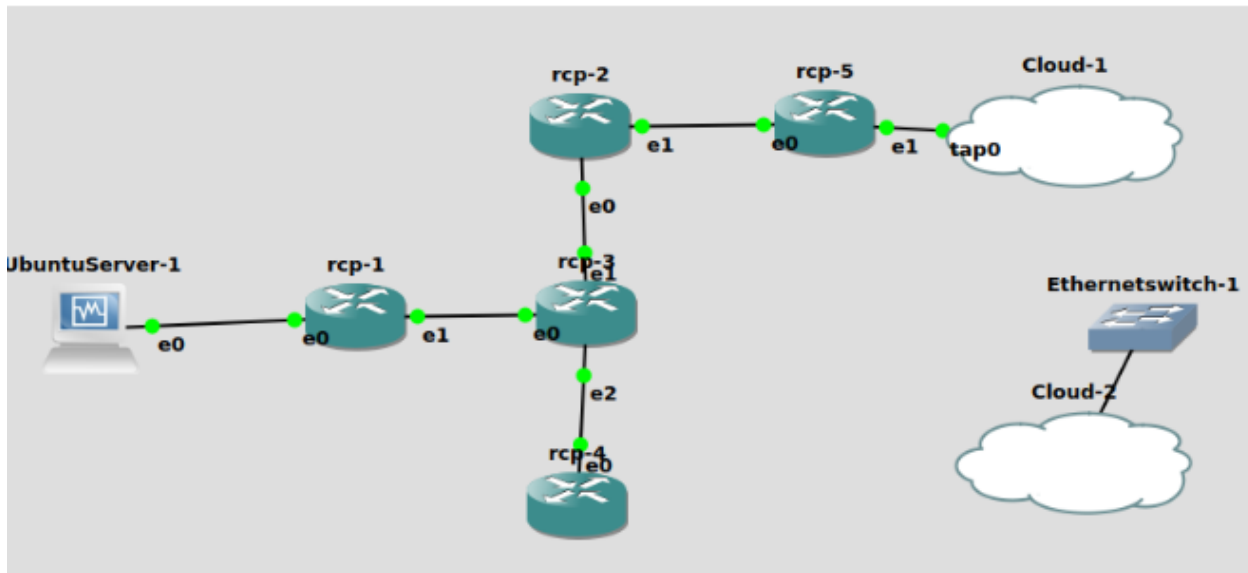


Figura 3.1: Topología propuesta.

```

redistribute connected
exit

```

Así, una vez realizada la configuración de cada router en la topología con los protocolos mencionados, podemos ver los siguientes resultados en las tablas de enrutamiento de los routers R2, R3 y R4, en donde podemos observar la forma en que las rutas están distribuidas y la forma en que logran comunicar a los routers participantes.

```

R2(rip)#show ip route
Codes: C - connected, S - static, R - RIP, B - blackhole, O - OSPF
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2

R    192.168.1.0/24[120/21] via 192.168.2.2, eth0
C    192.168.2.0/24 is directly connected, eth0
R    192.168.3.0/24[120/21] via 192.168.2.2, eth0
C    192.168.4.0/24 is directly connected, eth1
R2(rip)#

```

Figura 3.2: Tabla de enrutamiento del Router 2 (R2).


```
R3(config)#show ip route
Codes: C - connected, S - static, R - RIP, B - blackhole, O - OSPF
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2
C    192.168.1.0/24 is directly connected, eth1
S    192.168.1.0/24[1/0] via 192.168.1.1, eth1
C    192.168.2.0/24 is directly connected, eth0
C    192.168.3.0/24 is directly connected, eth2
R    192.168.4.0/24[120/2] via 192.168.2.1, eth0
```

Figura 3.3: Tabla de enrutamiento del Router 3 (R3).

```
R4(ospf)#show ip route
Codes: C - connected, S - static, R - RIP, B - blackhole, O - OSPF
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2
C    192.168.4.0/24 is directly connected, eth2
C    192.168.5.0/24 is directly connected, eth0
R4(ospf)#
```

Figura 3.4: Tabla de enrutamiento del Router 4 (R4).

Finalmente, se realizan pruebas de conexión entre los dos extremos de la red (UbuntuServer y Cloud) para verificar que la topología ha sido conectada y configurada correctamente. Para ello se hacen pings de extremo a extremo en ambas direcciones, los resultados pueden verse debajo.

```
jesus@jesus-VirtualBox:~$ ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=63 time=3004 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=63 time=1983 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=63 time=960 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=63 time=1.20 ms
64 bytes from 10.10.10.2: icmp_seq=5 ttl=63 time=1.91 ms
64 bytes from 10.10.10.2: icmp_seq=6 ttl=63 time=1.81 ms
^C
--- 10.10.10.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5048ms
rtt min/avg/max/mdev = 1.209/992.275/3004.790/1153.034 ms, pipe 3
```

Figura 3.5: Ping de extremo 1 a extremo 2.

3.2. Tarea 2: Supervisión de servidores

3.2.1. Supervisión de los servidores de correo electrónico

Un servidor de correo es una aplicación de red de computadoras ubicada en un servidor de Internet, para prestar servicio de correo electrónico. De forma predeterminada, el protocolo estándar para la transferencia de correos entre servidores es el Protocolo Simple de Transferencia de Correos (SMTP).

```
jesus@jesus-VirtualBox:~$ ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=63 time=3004 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=63 time=1983 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=63 time=960 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=63 time=1.20 ms
64 bytes from 10.10.10.2: icmp_seq=5 ttl=63 time=1.91 ms
64 bytes from 10.10.10.2: icmp_seq=6 ttl=63 time=1.81 ms
^C
--- 10.10.10.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5048ms
rtt min/avg/max/mdev = 1.209/992.275/3004.790/1153.034 ms, pipe 3
```

Figura 3.6: Ping de extremo 2 a extremo 1.

Instalación del servidor

En este caso se utilizó el servidor SMTP llamado Postfix. Los pasos para su instalación son los siguientes:

```
maestroluminuscom@maestro:~$ sudo apt-get install postfix
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Figura 3.7: Comando para instalar un servidor SMTP llamado Postfix

```
maestroluminuscom@maestro:~$ sudo service postfix restart
```

Figura 3.8: Comando para reiniciar el servicio SMTP

3.2.2. Supervisión de los servidores web

Un servidor web es un programa que utiliza el protocolo de transferencia de hipertexto HTTP, para servir los archivos que forman páginas web a los usuarios, en respuesta a sus solicitudes. Esos archivos son reenviados por los clientes HTTP de las computadoras de los usuarios. Las computadoras y los dispositivos dedicados también pueden denominarse servidores Web.

Instalación del servidor

Utilizamos el servidor Apache2 como nuestro servidor HTTP. Los pasos para su instalación son los siguientes:

```
maestroluminuscom@maestro: ~
maestroluminuscom@maestro:~$ sudo apt-get install apache2
[sudo] contraseña para maestroluminuscom:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  apache2-data apache2-utils
Paquetes sugeridos:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-data apache2-utils
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 6 no actualizados.
Se necesita descargar 339 kB de archivos.
Se utilizarán 1 757 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Figura 3.9: Instalación del servidor.

Sensor

Este sensor está escrito en Bash. Toma como datos de entrada el servidor al que se le va a hacer la petición y la petición que se le va a hacer.

```
1 #!/bin/bash
2
3 echo "Servidor HTTP: "
4 read servidor
5 echo "Petición: "
6 read petition
7 curl -w "@informacion.txt" -o /dev/null -v -d $petition $servidor
```

Figura 3.10: Código del sensor HTTP.

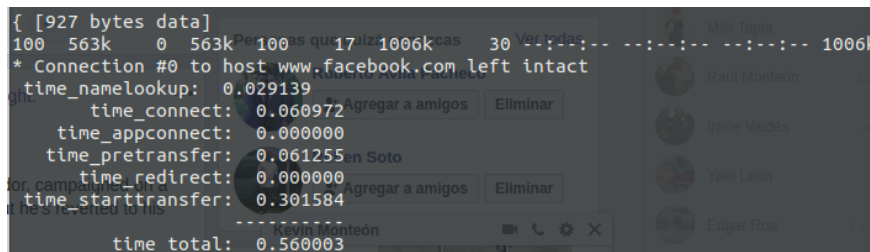


Figura 3.11: Datos de salida del sensor HTTP.

3.2.3. Supervisión de servidores de archivos

Un servidor de archivos permite a los usuarios compartir información a través de una red sin tener que transferir físicamente los archivos por algún medio de almacenamiento externo extraíble.

Instalación del servidor

Utilizamos en esta parte el servidor VSFTPD para hacer la transferencia de archivos mediante el protocolo FTP. Los pasos para su instalación son los siguientes:

```
maestroluminuscom@maestro:~$ sudo apt-get vsftpd
E: Operación inválida: vsftpd
maestroluminuscom@maestro:~$ sudo apt-get install vsftpd
Leyendo lista de paquetes...
Creando árbol de dependencias
Leyendo la información de estado...
vsftpd ya está en su versión más reciente (3.0.3-9build1).
```

Figura 3.12: Instalamos el servidor VSFTPD.

```
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

Figura 3.13: Modificamos el archivo de configuración vsftpd.conf.

```
maestroluminuscom@maestro:~$ sudo systemctl stop vsftpd.service
maestroluminuscom@maestro:~$ sudo systemctl start vsftpd.service
maestroluminuscom@maestro:~$ sudo systemctl enable vsftpd.service
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd
/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
```

Figura 3.14: Habilitamos el servicio VSFTPD.

Sensor

Este sensor se escribió en Bash. Toma como parámetros de entrada el servidor al que se le va a hacer la petición, el usuario de FTP, su contraseña y el nombre del archivo que se desea arquirir.

```
1 #!/bin/bash
2
3 echo "URL del servidor: "
4 read url
5 echo "Usuario de FTP: "
6 read usuario
7 echo "Password del usuario: "
8 read pass
9 echo "Nombre del archivo: "
10 read archivo
11 curl -w "@informacion.txt" -o /dev/null -v ftp://$usuario:$pass@$url/$archivo
```

Figura 3.15: Código del sensor FTP.

Después de ejecutarse el archivo, la salida es la siguiente.

```
time_namelookup: 0.000049
time_connect: 0.000801
time_appconnect: 0.000000
time_pretransfer: 0.795588
time_redirect: 0.000000
time_starttransfer: 0.830128
time_total: 0.830545
```

Figura 3.16: Salida de la ejecución del sensor FTP.

3.2.4. Supervisión de impresoras

Un servidor de impresión o servicio de impresión a gran escala es un servidor que conecta una impresora a una red para que cualquier PC pueda acceder a ella e imprimir trabajos, sin depender de otra PC para poder utilizarla.

Instalación del servidor

En esta sección se utilizó el servidor de impresiones CUPS (Common Unix Printing Server). Los pasos para su instalación son los siguientes:

```
maestroluminuscom@maestro:~$ sudo apt install cups
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Figura 3.17: Comando para instalar el servidor CUPS

CAPÍTULO 3. DESARROLLO DE LA PRÁCTICA

```
maestroluminuscom@maestro:~$ sudo cp /etc/cups/cupsd.conf /etc/cups/cupsd.conf.c  
onf.original
```

Figura 3.18: Respalamos la configuración original.


```
# Only listen for connections from the local machine.  
Listen localhost:631  
Listen /var/run/cups/cups.sock  
Listen 192.168.0.9:631
```

Figura 3.19: Agregamos otras direcciones que estará escuchando el servidor.

```
maestroluminuscom@maestro:~$ service cups restart
```

Figura 3.20: Reiniciamos el servicio CUPS.

3.2.5. Supervisión de acceso remoto

Un servidor de acceso remoto es un tipo de servidor que provee una colección de servicios a usuarios conectados de manera remota por medio de una red. Estos servidores operan como una puerta remota o servidor central que conecta usuarios remotos con una LAN. Ejemplos de protocolos de acceso remoto son SSH y Telnet.

Instalación del servidor

Para instalar un servidor de acceso remoto (SSH) en nuestra computadora seguiremos los siguientes pasos:

```
maestroluminuscom@maestro:~$ sudo apt install openssh-server
```

Figura 3.21: Comando para instalar servidor SSH

```
maestroluminuscom@maestro:~$ service ssh restart
```

Figura 3.22: Comando para reiniciar servicio SSH

3.3. Tarea 3: Recopilación de información de dispositivos de manera periódica

Para poder recopilar la información de un router, es muy importante tener acceso al mismo mediante el uso de un protocolo de acceso, ya sea telnet, ssh, entre otros, ya que, en caso de no existir el archivo de configuración, es importante crear el mismo mediante la línea de comandos, pero al tratarse de una red, no siempre se tiene acceso físico a todos los dispositivos, por ello la importancia de poder acceder a los mismos.

La herramienta realizada, antes de poder extraer el archivo de configuración, primero se encarga de sobrescribirlo con la configuración actual del router. Para lograr lo anterior, fue necesario utilizar la librería telnetlib, para que, con ayuda de la misma, se puedan ejecutar los comandos necesarios para habilitar el router y generar el archivo con la configuración más actual.

En la siguiente imagen se muestra el código fuente del programa que realiza dicha conexión, así como la ejecución de los comandos.

```

1 import getpass
2 import sys
3 import telnetlib
4
5 HOST = '10.10.10.1'
6 user = 'rcp'
7 password = 'rcp'
8
9 tn = telnetlib.Telnet(HOST)
10
11 tn.read_until('Username : ')
12
13 tn.write(user+ "\r")
14
15 tn.read_until("Password : ")
16
17 tn.write(password+ "\n")
18
19 tn.write("enable"+"\\n")
20
21 tn.write("configure"+"\\n")
22
23 tn.write("copy running-config startup-config"+"\\n")
24
25 tn.write("service ftp"+"\\n")

```

Figura 3.23: Código fuente para acceder a un router remoto vía Telnet.

Para la exportación e importación de los archivos de configuración, se desarrolló un pequeño programa que se encarga de importar el archivo de configuración del router dada su ip, así como de enviar un archivo de configuración seleccionado y reemplazar el archivo “startup-config” de dicho router para cambiar su configuración. La interfaz gráfica se muestra en la siguiente figura.

Importar

<input type="text" value="Host"/>	<input type="text" value="UserName"/>	<input type="text" value="Password"/>	<input type="button" value="Importar"/>
-----------------------------------	---------------------------------------	---------------------------------------	---

Exportar

<input type="text" value="Host"/>	<input type="text" value="UserName"/>	<input type="text" value="Password"/>	<input type="button" value="Examinar..."/>	Ningún archivo seleccionado.
<input type="button" value="exportar"/>				

Figura 3.24: Pantalla principal de la herramienta de importación y exportación de archivos de configuración.

Para el punto anterior, se realizaron algunas pruebas de la extracción de los archivos de configuración. Para ello, se utilizó una máquina virtual de Ubuntu dentro de GNS3, así como tres enrutadores, tal como se muestra en la siguiente figura.

CAPÍTULO 3. DESARROLLO DE LA PRÁCTICA

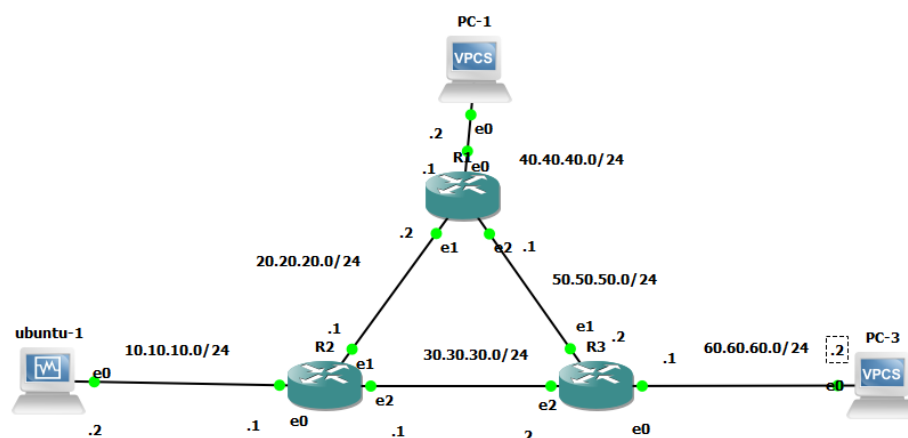


Figura 3.25: Topología de prueba para la extracción y envío de archivos de configuración.

Tras haber realizado la configuración de los routers, se muestra la tabla de enrutamiento de cada uno de ellos. Cabe mencionar que por cuestiones prácticas fueron configurados con el protocolo RIP.

```
R1(config)#show ip route
Codes: C - connected, S - static, R - RIP, B - blackhole, O - OSPF
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2
R    10.10.10.0/24[120/21] via 20.20.20.1, eth1
C    20.20.20.0/24 is directly connected, eth1
R    30.30.30.0/24[120/21] via 50.50.50.2, eth2
                        via 20.20.20.1, eth1
C    40.40.40.0/24 is directly connected, eth0
C    50.50.50.0/24 is directly connected, eth2
R    60.60.60.0/24[120/21] via 50.50.50.2, eth2
R1(config)#
```

Figura 3.26: Tabla de enrutamiento del router R1

```

R2(config)#show ip route
Codes: C - connected, S - static, R - RIP, B - blackhole, O - OSPF
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2

C    10.10.10.0/24 is directly connected, eth0
C    20.20.20.0/24 is directly connected, eth1
C    30.30.30.0/24 is directly connected, eth2
R    40.40.40.0/24[120/21] via 20.20.20.2, eth1
R    50.50.50.0/24[120/21] via 30.30.30.2, eth2
R    60.60.60.0/24[120/21] via 30.30.30.2, eth2
R2(config)#_

```

Figura 3.27: Tabla de enrutamiento del router R1

```

R3(rip)#show ip route
Codes: C - connected, S - static, R - RIP, B - blackhole, O - OSPF
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2

R    10.10.10.0/24[120/21] via 30.30.30.1, eth2
R    20.20.20.0/24[120/21] via 50.50.50.1, eth1
C    30.30.30.0/24 is directly connected, eth2
R    40.40.40.0/24[120/21] via 50.50.50.1, eth1
C    50.50.50.0/24 is directly connected, eth1
C    60.60.60.0/24 is directly connected, eth0
R3(rip)#

```

Figura 3.28: Tabla de enrutamiento del router R1

Tras haber verificado la conectividad dentro de la red, se procedió a extraer el archivo de configuración de router. En la siguiente figura se puede observar los datos requeridos en el sistema para poder extraer dicho archivo. Cabe mencionar que solo es necesario especificar la ip de alguna de las interfaces del router, por lo cual, si un router tiene más de una conexión, se podrá acceder al mismo usando distintas direcciones ip.

Importar

40.40.40.1 rcp rcp Importar

Exportar

Host UserName Password Examinar... Ningún archivo seleccionado.
exportar

Figura 3.29: Datos de entrada para la extracción de un archivo de configuración de un router específico.

CAPÍTULO 3. DESARROLLO DE LA PRÁCTICA

Una vez realizado lo anterior, se habrá generado un archivo de texto, el cual contiene toda la configuración del router como se muestra en la siguiente figura.

```

1 hostname R1
2 !
3 service telnet
4 service http encrypted password GGRUEABX$1aeb3f4684bc3258d87c135537793c2c
5 !
6 administrator rcp encrypted password NGDRYCXI$ItRmvK6RoAju10/FPY7UU1
7 !
8 !
9 !
10 !
11 router rip
12 network 20.20.20.0/24
13 network 40.40.40.0/24
14 network 50.50.50.0/24
15 !
16 interface loopback lo
17 ip address 127.0.0.1/8
18 ip mtu 16436
19 !
20 interface ethernet eth0
21 ip address 40.40.40.1/24
22 ip mtu 1500
23 no shutdown
24 !
25 interface ethernet eth1
26 ip address 20.20.20.2/24
27 ip mtu 1500
28 no shutdown
29 !
30 interface ethernet eth2

```

Figura 3.30: Contenido del archivo de configuración extraído del router R1.

Para probar la exportación de los archivos de configuración, se cambió el nombre del host por “PruebaEnvio”. La herramienta permite elegir un archivo desde la computadora, de forma que no es necesario escribir la ruta de dicho archivo. En la siguiente figura se puede observar los datos de entrada para el envío de un archivo de configuraciones hacia un router.

Exportar

40.40.40.1	rcp	rcp	Examinar...	Thu Dec 6 02:24:51 201840.40.1.txt
<input type="button" value="exportar"/>				

Figura 3.31: Datos de entrada para la sobreescritura de un archivo de configuraciones de un router.

CAPÍTULO 3. DESARROLLO DE LA PRÁCTICA

Finalmente, para verificar que el archivo se recibió correctamente, basta con reiniciar nuestro router y ver que el nombre del host se modificó de forma exitosa.

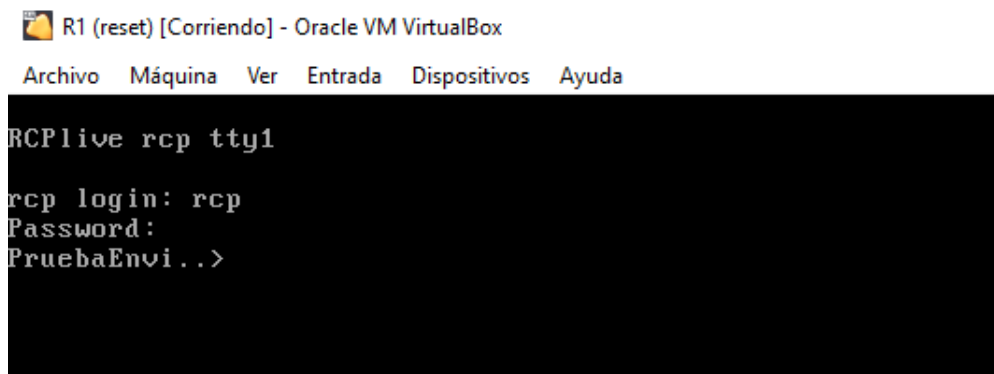


Figura 3.32: Verificación de los cambios realizados al archivo de configuraciones extraído previamente.

Como última parte, se muestra el código fuente de la herramienta que se encarga de la importación y exportación de los archivos de configuración.


```

10 @app.route('/')
11 def main():
12     return render_template('index.html')
13
14 @app.route('/importar', methods=['GET', 'POST'])
15 def importar():
16     fecha = time.strftime("%c")
17     host = request.form['host']
18     username = request.form['username']
19     password = request.form['password']
20     try:
21         ftp = ftplib.FTP(host, username, password)
22         try:
23             ftp.retrbinary('RETR startup-config', open('startup-config', 'wb').write)
24             ftp.quit()
25             os.rename('startup-config', fecha+host+'.txt')
26         except:
27             print "No se ha encontrado el archivo"
28     except:
29         print "No se ha podido conectar al servidor " + host
30     return redirect(url_for('main'))
31

```

Figura 3.33: código fuente de la función que extrae el archivo de configuraciones de algún router.

```

31
32 @app.route('/exportar', methods=['GET', 'POST'])
33 def exportar():
34     fichero_destino = 'startup-config' # Nombre que tendra el fichero en el servidor
35     host = request.form['host']
36     username = request.form['username']
37     password = request.form['password']
38     archivo = request.form['archivo']
39     print archivo
40     try:
41         ftp = ftplib.FTP(host, username, password)
42         try:
43             f = open(archivo, 'rb')
44             ftp.storbinary('STOR ' + fichero_destino, f)
45             f.close()
46         except:
47             print "No se ha encontrado el archivo"
48     except:
49         print "No se ha podido conectar al servidor " + host
50     return redirect(url_for('main'))
51
52 if __name__ == '__main__':
53     app.run()

```

Figura 3.34: Código fuente de la función que sobrescribe un archivo de configuraciones de algún router.

4.1. Huerta Martínez Jesús Manuel

Las redes de computadoras son fundamentales en cualquier ámbito en nuestros días, compartir y conocer información por medio de ellas es ahora un hecho cotidiano e imprescindible, es por ello que dichas redes deben ser cuidadas, desde su construcción y funcionamiento, hasta la información que sobre éstas viaja. Así, las técnicas de ruteo y los sensores que se les pueden aplicar resultan de gran utilidad para obtener un correcto funcionamiento a la hora de usarlas. Es gracias a la presente práctica que podemos interactuar con los mencionados enrutamientos y sensores de red, conocimos su comportamiento, la forma en que se aplican y los resultados que nos otorgan, con ello, se complementa el conocimiento adquirido en el resto del curso.

4.2. Monteón Valdés Raúl Kevin

Creo que esta práctica fue interesante porque aprendí de cómo se monitorean diferentes rubros del uso de la red. Sin embargo, me hubiera gustado ahondar un poco más en el tema de la monitorización de los servicios de red.

4.3. Olivares García Marco Antonio

En esta práctica comprendimos la importancia de los protocolos de enrutamiento, pues gracias a ellos nos es posible monitorear equipos de nuestra red, sin importar que no tengamos acceso físico al equipo. Por otra parte, es muy importante mantener nuestros servidores con un nivel de seguridad adecuado, pues en caso contrario cualquier persona podría acceder a nuestros equipos de manera remota.

Bibliografía

- [1] CM Mansilla, *Redes de Computadoras* [En línea]. Universidad Nacional de Litoral. Argentina, (S/F).
Disponible en <http://www.fca.unl.edu.ar/informaticabasica/Redes.pdf>
- [2] S. Juliá, *Ventajas de tener una red de ordenadores en la empresa* [En línea]. GADAE. (S/L), (S/F).
Disponible en <http://www.gadae.com/blog/ventajas-red-de-ordenadores-empresa/>
- [3] Universidad Veracruzana, *Enrutamiento estático* [En línea]. Facultad de estadística e informática, Universidad Veracruzana. México, (S/F).
Disponible en <https://www.uv.mx/personal/ocruz/files/2014/01/Enrutamiento-estatico.pdf>
- [4] E. Duarte, *Cisco CCNA – Cómo Configurar Protocolo RIP En Cisco Router* [En línea]. Capacity: Information Technology Academy. (S/L), 2014.
Disponible en <http://blog.capacityacademy.com/2014/06/20/cisco-ccna-como-configurar-protocolo-rip-en-cisco->
- [5] E. Duarte, *Cisco CCNA – Cómo Configurar OSPF En Cisco Router* [En línea]. Capacity: Information Technology Academy. (S/L), 2014.
Disponible en <http://blog.capacityacademy.com/2014/06/23/cisco-ccna-como-configurar-ospf-en-cisco-router/>
- [6] Techopedia *Remote Access Server (RAS)* [En línea]. Techopedia, (S/L), 2011.
Disponible en <https://www.techopedia.com/definition/3192/remote-access-server-ras>
- [7] Wikipedia *Servidor de correo* [En línea]. Wikipedia, (S/L), 2009.
Disponible en https://es.wikipedia.org/wiki/Servidor_de_correo
- [8] Wikipedia *Servidor de impresión* [En línea]. Wikipedia, (S/L), 2008.
Disponible en https://es.wikipedia.org/wiki/Servidor_de_impresi%C3%B3n
- [9] SearchDataCenter en Español [En línea]. SearchiDataCenter, (S/L), 2016.
Disponible en <https://searchdatacenter.techtarget.com/es/definicion/Servidor-de-archivos>
- [10] SearchDataCenter en Español [En línea]. SearchiDataCenter, (S/L), 2015.
Disponible en <https://searchdatacenter.techtarget.com/es/definicion/Servidor-Web>