DATOS DE LA ACTIVIDAD							
No. de Práctica:	**1**	**Práctica:**	**Configurar un Router Cisco para operaciones con NTP, SYSLOG y SSH**				
Unidad:	1: Riesgos de seguridad informática en infraestructura de red						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**Seguridad en Infraestructura de TI**					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	26/02/2021
Compet.		4.1, 4.5, 5.2,		Compet. Profesional		CP1-1	

1. Objetivo(s) de la práctica

Conocer los protocolos de configuración remota, de sincronización de tiempo y administración de registros en una red.

- Configurar un Router como cliente NTP.
- Configurar un Router para actualizar el reloj de sistema utilizando NTP.
- Configure un Router para registrar los mensajes en el servidor SYSLOG.
- Configure un Router para mostrar mensajes de registro.
- Configurar los usuarios locales.
- Configurar las líneas VTY para aceptar conexiones solamente SSH.
- Configurar par de claves RSA en el servidor SSH.
- Verifique la conectividad SSH desde los clientes PC y Router.

2. Resumen (Referente a NTP, SYSLOG y SSH)

SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación. Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada.

El **NTP** proporciona los mecanismos de protocolo básicos necesarios para sincronizar los relojes de los diferentes sistemas con una precisión del orden de nanosegundos. Además, contiene indicaciones para especificar la precisión y las posibles fuentes de error del reloj del sistema local, así como las propiedades
del reloj de referencia. No obstante, este protocolo se limita a especificar la arquitectura de la representación de datos y los formatos de mensaje, sin que por sí mismo lleve a cabo la sincronización y el algoritmo de filtrado. Para sincronizar los relojes de los

ordenadores con una precisión de nanosegundos, el Network Time Protocol utiliza el estándar Tiempo universal coordinado (UTC), que fija la hora universal válida y unitaria desde 1972. Esto se determina utilizando varios métodos, incluyendo sistemas de radio y satélite. Algunos servicios importantes como el Sistema de Posicionamiento Global (GPS) están equipados con receptores especiales para recibir las señales.

SYSLOG es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por SYSLOG se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro. Un mensaje de registro suele tener información sobre la seguridad del sistema, aunque puede contener cualquier información. Junto con cada mensaje se incluye la fecha y hora del envío.
Puede ser útil cuando:

- Un intento de acceso con contraseña equivocada.
- Un acceso correcto al sistema.
- Anomalías: variaciones en el funcionamiento normal del sistema.
- Alertas cuando ocurre alguna condición especial.
- Información sobre las actividades del sistema operativo.
- Errores del hardware o el software.

El protocolo SYSLOG es muy sencillo: existe un ordenador servidor ejecutando el servidor de SYSLOG, conocido como SYSLOGD (demonio de SYSLOG). El cliente envía un pequeño mensaje de texto (de menos de 1024 bytes). Los mensajes de SYSLOG se suelen enviar vía UDP, por el puerto 514, en formato de texto plano. Algunas implementaciones del servidor, como SYSLOG-ng, permiten usar TCP en vez de UDP, y también ofrecen Stunnel para que los datos viajen cifrados mediante SSL/TLS. Aunque SYSLOG tiene algunos problemas de seguridad, su sencillez ha hecho que muchos dispositivos lo implementen, tanto para enviar como para recibir. Eso hace posible integrar mensajes de varios tipos de sistemas en un solo repositorio central.

Referencia:
Anónimo (18/08/2016). ¿Qué es SYSLOG? Recuperado el 26/02/2021 de: https://techclub.tajamar.es/syslog/

C. Diana (31/03/2020) ¿Cómo funciona el SSH? Recuperado el 26/02/2021 de: https://www.hostinger.es/tutoriales/que-es-ssh

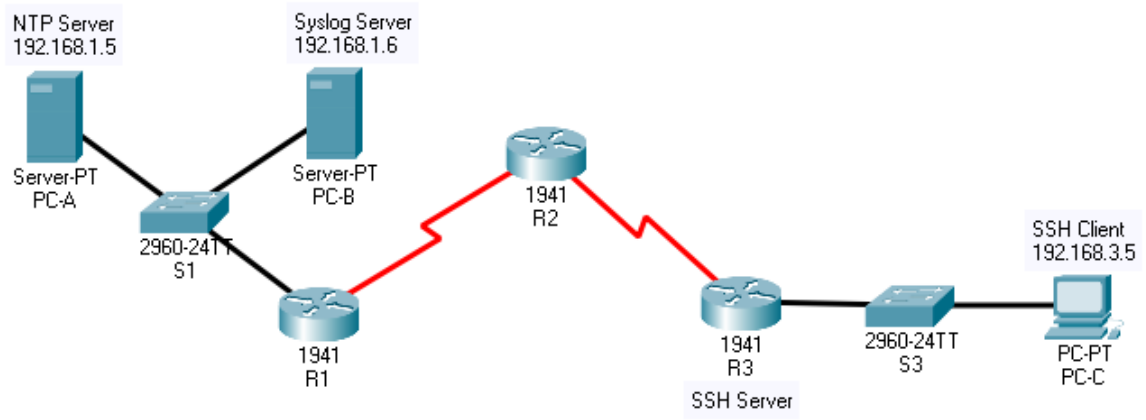
Anónimo (2019) Conceptos básicos del protocolo SNMP. Recuperado el 26/02/2021 de: https://www.manageengine.com/es/network-monitoring/what-is-snmp.html

3. Material, equipo y/o herramienta necesaria

- Tres conmutadores cisco 1941 o similares
- Una PC con acceso a la terminal
- Dos servidores con servicios de NTP y SYSLOG respectivamente
- Dos switches cisco 2960-24TT o similares
- 5 cables de Ethernet de conexión directa

4. Desarrollo de la práctica (Procedimiento Teórico/Práctico en base al documento Cisco, diagramas, dibujos, tablas, codificación, impresiones de pantalla completa con nombre y fecha)

- **Topología**



- **Tabla de configuración básica.**

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 F0/18

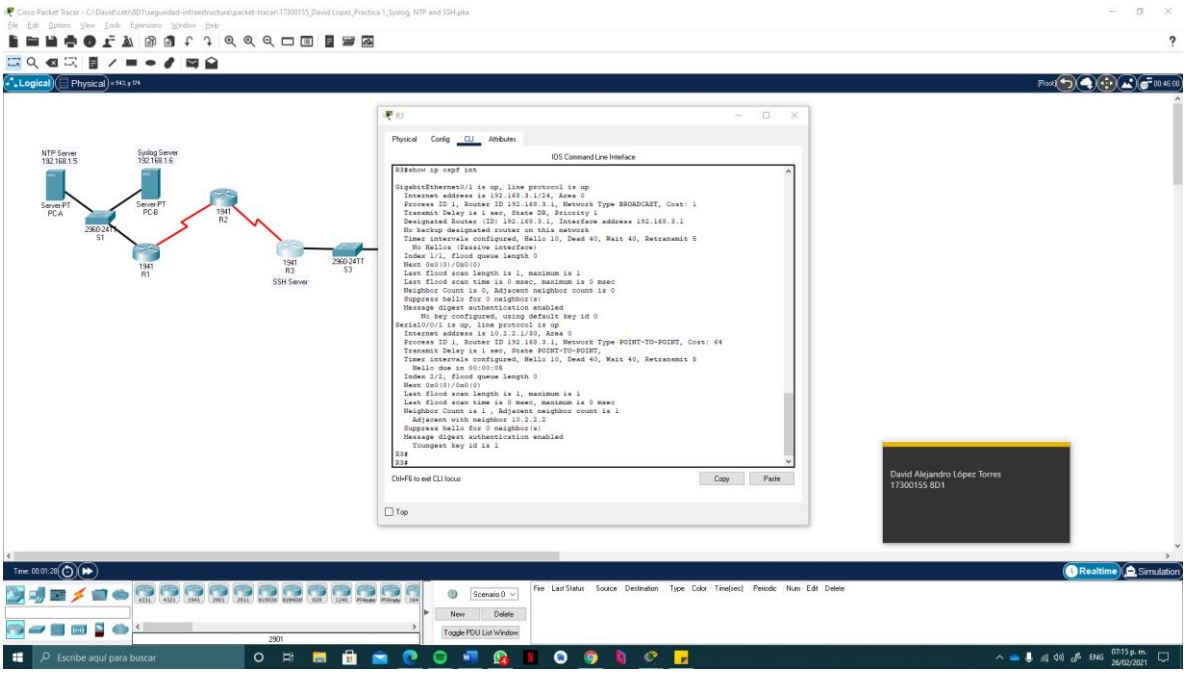
- **Tabla de comandos**

Sintaxis	Descripción
`router ospf 1`	Configuración del protocolo OSPF
`area 0 authentication message-digest`	Autenticación por MD5 en OSPF
`ip ospf message-digest-key 1 md5 MD5pa55`	Configuración de llave MD5 en Router
`ntp authenticate`	Configuración de autenticación ntp en Router

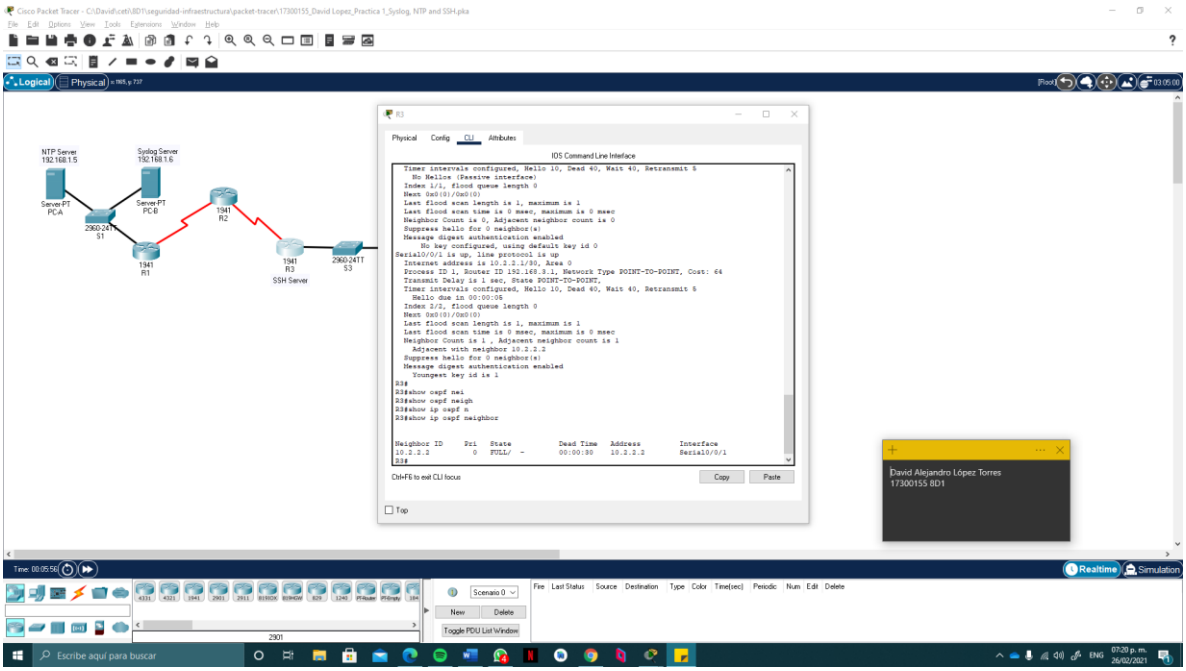
`ntp authentication-key 1 md5 NTPpa55`	Configuración de llave MD5 ntp en Router
`show logging`	Información sobre el estado de los mensajes log en Router
`username SSHadmin privilege 15 secret ciscosshpa55`	Crea un usuario SSHadmin con el nivel más alto de privilegio y establece password
`Crypto key generate rsa`	Genera una llave RSA en Router
`show ip ssh`	Verifica la configuración SSH en Router
`ssh -v 2 -l SSHadmin 10.2.2.1`	Conecta con una dirección en particular utilizando conexión SSH

- **Procedimiento (del PDF) con Impresiones de pantalla de resultados en el simulador Packet Tracert 7.0 (SIN Preguntas) (Imágenes con nombre y número de Figura**

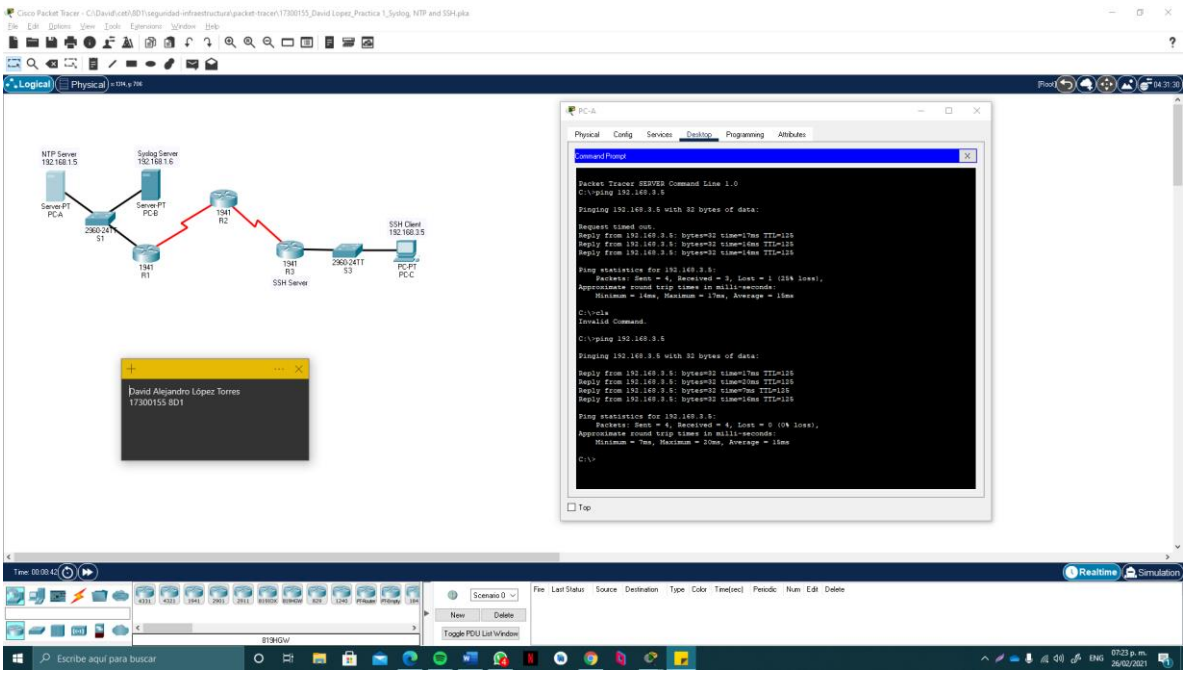
Verificación de la autenticación MD5



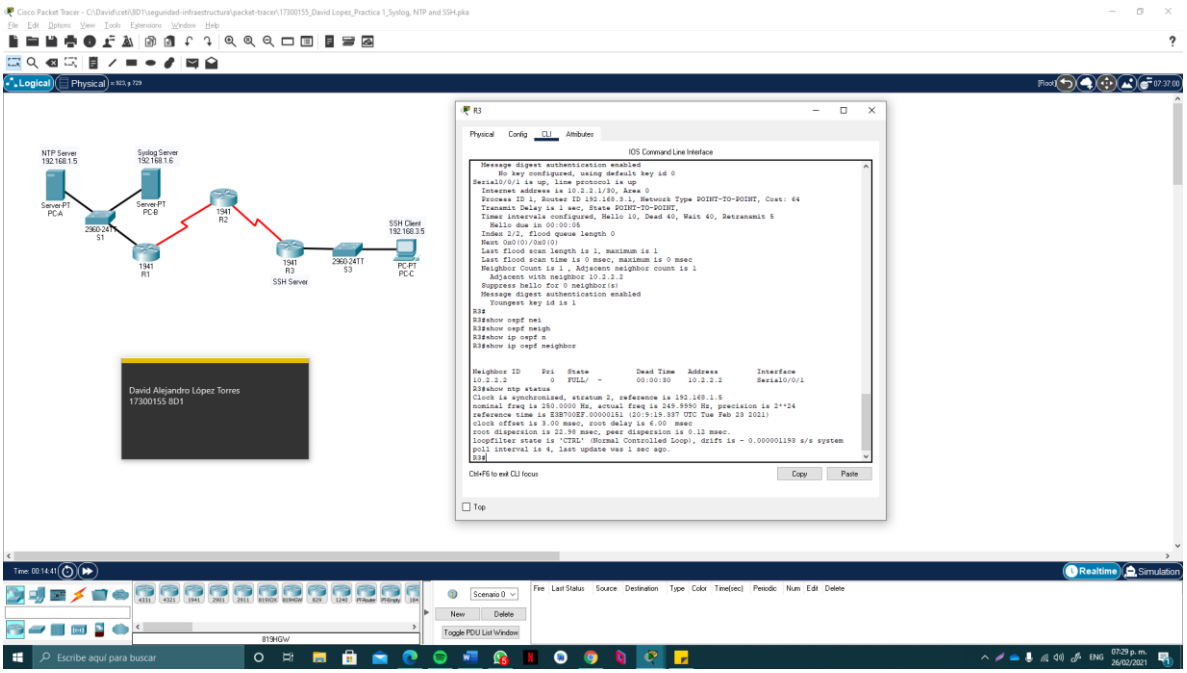
Verificación de conectividad ospf



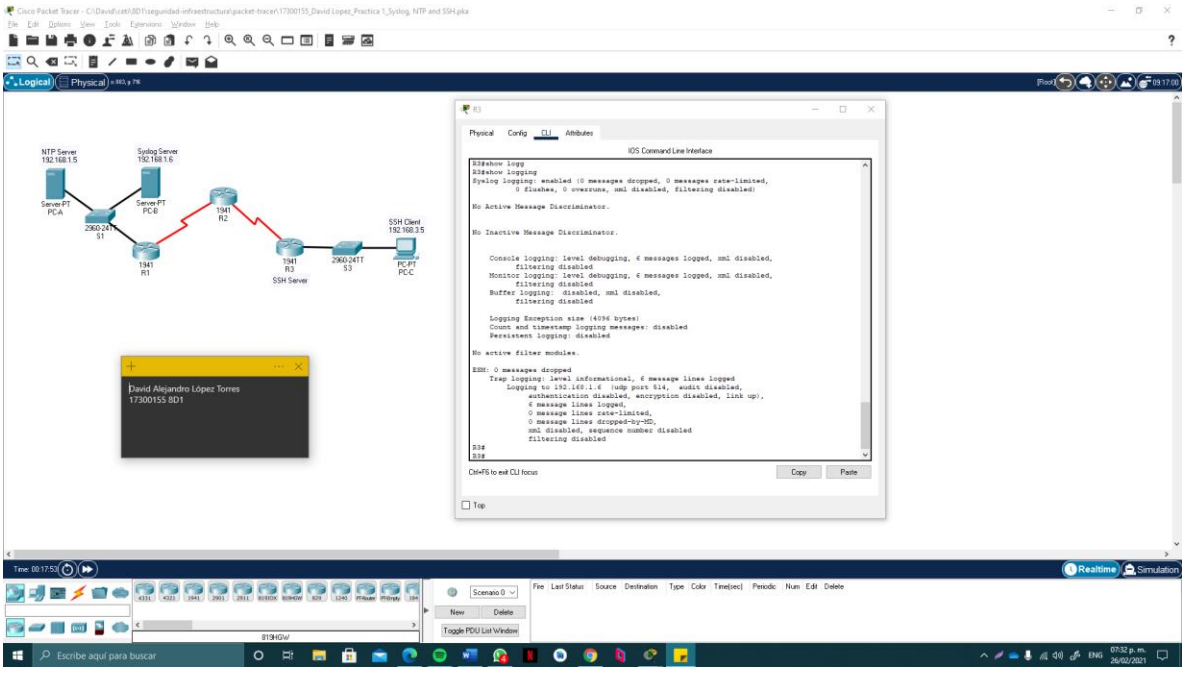
Verificación de conectividad de punta a punta



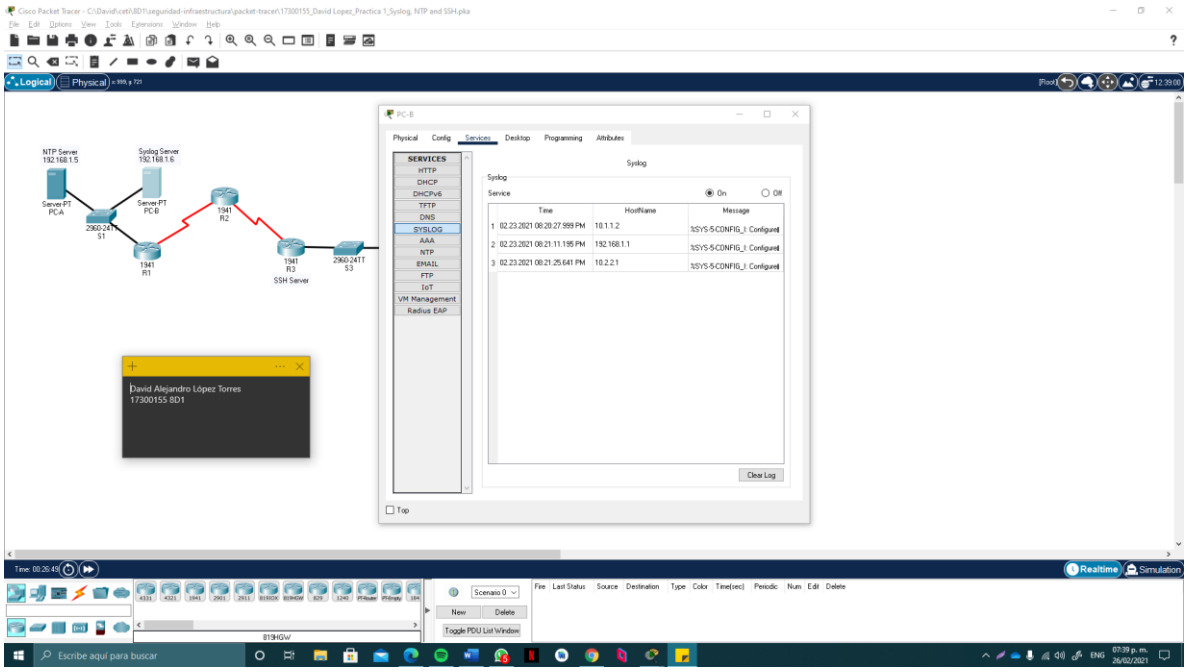
Verificación de status de NTP



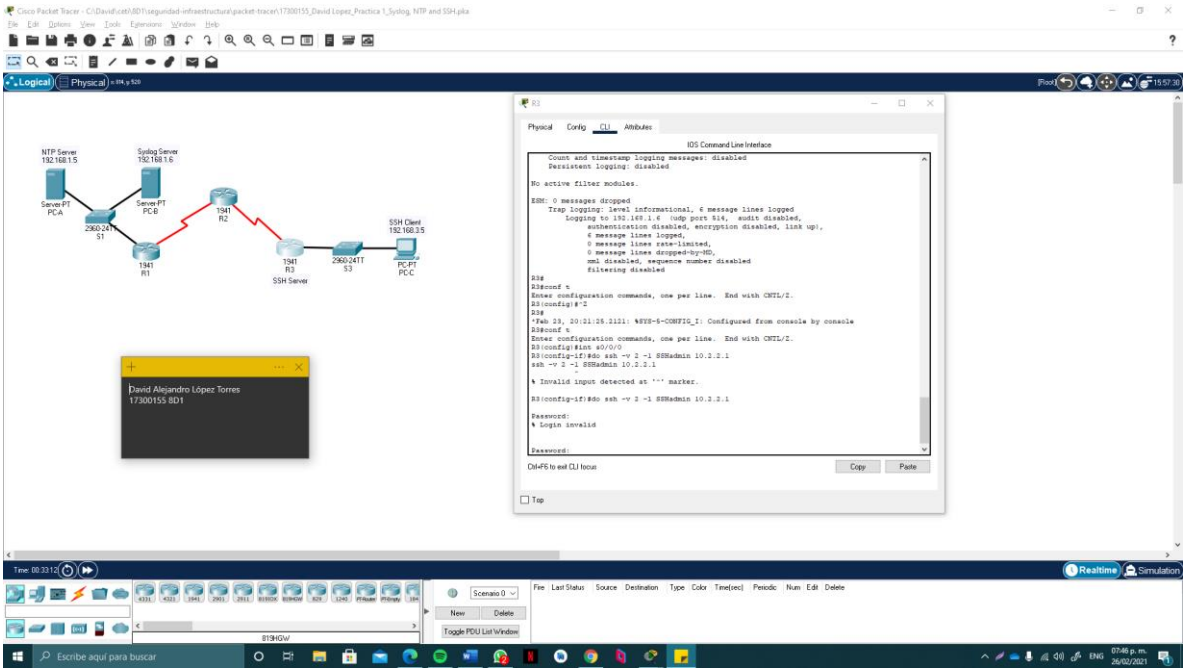
Verificación del log del SYSLOG server



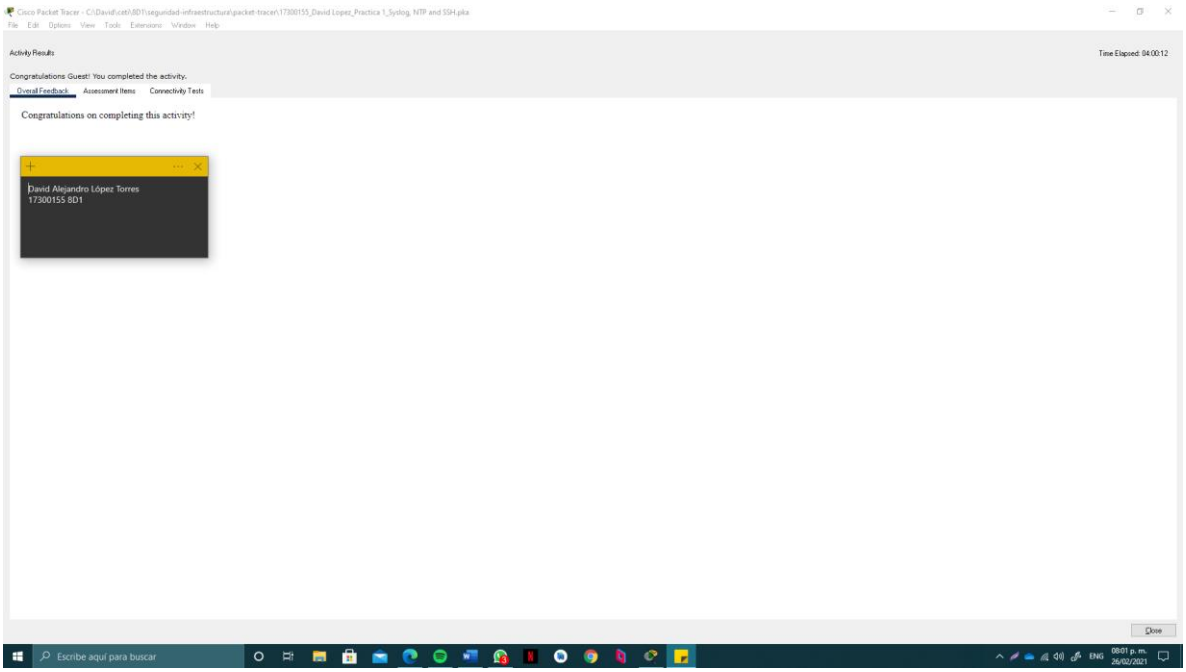
Mensajes obtenidos desde el SYSLOG Server (al iniciar una sesión de configuración de terminal de los Routers)



Verificación de conectividad de SSH



Finalización de la actividad



5. Observaciones

El desarrollo de esta práctica fue una tarea simple gracias a la documentación brindada por el profesor para llevarlo a cabo. En general, los principales problemas que se enfrentaron tenían que ver con el flujo del tiempo en Packet Tracer (igual al de la vida real), así que solo era cuestión de esperar o acelerar el ritmo de la simulación para ver el efecto de algunos protocolos en la red (en especial el NTP).

6. Conclusiones

Con el desarrollo de está práctica se han reafirmado los conocimientos vistos en la materia de redes WAN en cuanto al protocolo OSPF, desde sus aspectos de conectividad hasta establecer protocolos de seguridad en el envío de información con él. La práctica además nos permitió poner en práctica los conocimientos adquiridos en la actividad anterior (1.5) acerca de los diferentes protocoles que pueden ser implementados para brindar una estructura más segura a la infraestructura de la red. Hemos visto la utilidad del protocolo NTP y como se complementa con los servicios de SYSLOG de un servidor para llevar un registro sincronizado de las intervenciones en la configuración de los conmutadores, así cómo la implementación de SSH para garantizar una conexión segura a la configuración del conmutador de manera remota.