

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:

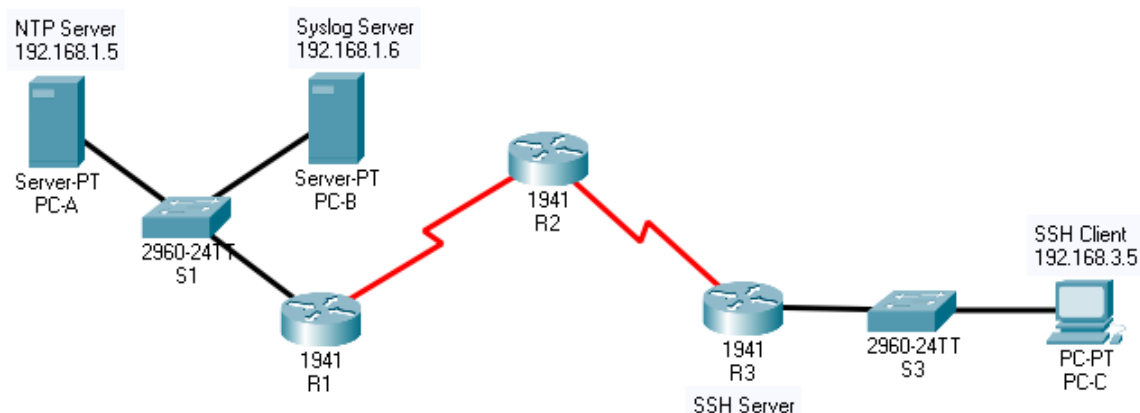
<https://www.manageengine.com/es/network-monitoring/what-is-snmp.html>

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
<code>router ospf 1</code>	Configuración del protocolo OSPF
<code>area 0 authentication message-digest</code>	Autenticación por MD5 en OSPF
<code>ip ospf message-digest-key 1 md5 MD5pa55</code>	Configuración de llave MD5 en Router
<code>ntp authenticate</code>	Configuración de autenticación ntp en Router

Verificación de conectividad ospf

Cisco Packet Tracer - C:\David\ut\MDT\segunda\infrastructure\packet-tracer\17300155_David Lopez_Practica 1_Syslog, NTP and SSH.pkt

Logical Physical 1730155

Diagram showing network topology with NTP Server, Syslog Server, R1, R2, R3, and SSH Server.

Command Prompt (R3) showing OSPF configuration and verification commands:

```
Time intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hi Hello (Passive interface)
Index 1/1, Flood queue length 0
Next 00:01:00/00:01:00
Last flood scan time is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
No key configured, using default key id 0
Serial0/0/1 is up, line protocol is up
Interface address is 10.0.0.1/30, Area 0
Process ID 1, Router ID 10.169.0.1, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 usec, State POINT-TO-POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:09
Index 0/0, Flood queue length 0
Next 00:01:00/00:01:00
Last flood scan time is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 10.0.0.2
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Timestamp key id is 1
```

Neighbor ID Pri State Dead Time Address Interface

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.0.0.2	0	FULL	00:00:30	10.0.0.2	Serial0/0/1

Ctrl-F to exit CLI focus

Copy Paste

David Alejandro López Torres
17300155 BD1

Verificación de conectividad de punta a punta

Cisco Packet Tracer - C:\David\ut\MDT\segunda\infrastructure\packet-tracer\17300155_David Lopez_Practica 1_Syslog, NTP and SSH.pkt

Logical Physical 1730155

Diagram showing network topology with NTP Server, Syslog Server, R1, R2, R3, and SSH Server.

Command Prompt (PC-A) showing Ping statistics for 10.169.0.1:

```
Packet Tracer: BEYOND Command Line 1.0
C:\>ping 10.169.0.1

Pinging 10.169.0.1 with 32 bytes of data:

Request timed out.
Reply from 10.169.0.1: bytes=32 time=1ms TTL=128
Reply from 10.169.0.1: bytes=32 time=1ms TTL=128
Reply from 10.169.0.1: bytes=32 time=1ms TTL=128

Ping statistics for 10.169.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 10.169.0.5

Invalid Command.

C:\>ping 10.169.0.5

Pinging 10.169.0.5 with 32 bytes of data:

Reply from 10.169.0.5: bytes=32 time=1ms TTL=128
Reply from 10.169.0.5: bytes=32 time=1ms TTL=128
Reply from 10.169.0.5: bytes=32 time=1ms TTL=128
Reply from 10.169.0.5: bytes=32 time=1ms TTL=128

Ping statistics for 10.169.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

David Alejandro López Torres
17300155 BD1

Verificación de status de NTP

The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a topology with an NTP Server (192.168.1.5), two Server PCs (192.168.1.6 and 192.168.1.7), two Routers (R1 and R2), an SSH Server, and an SSH Client. A yellow box in the center contains the text: "David Alejandro López Torres 17300155 BD1". On the right, the CLI window for R3 is open, showing the output of the `show ntp status` command. The output indicates that the NTP service is running and synchronized with the NTP server.

```
IOS Command Line Interface
R3#show ntp status
ntp sync status
Clock is synchronized, stratum 1, reference is 192.168.1.5
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 22870087.000000000 (2019-12-23 00:00:00.000000000)
clock offset is 3.00 msec, root delay is 6.00 msec
root dispersion is 12.98 msec, peer dispersion is 0.10 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), ctrl is - 0.000001193 s/s system
poll interval is 4, last update was 1 sec ago.
R3#
```

Verificación del log del SYSLOG server

The screenshot displays the Cisco Packet Tracer interface. On the left, the same network diagram as in the previous image is shown. A yellow box in the center contains the text: "David Alejandro López Torres 17300155 BD1". On the right, the CLI window for R3 is open, showing the output of the `show logging` command. The output indicates that logging is enabled and that messages are being logged to the Syslog server.

```
IOS Command Line Interface
R3#show logging
Logging logging enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, nml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 6 messages logged, nml disabled,
filtering disabled
Monitor logging: level debugging, 6 messages logged, nml disabled,
filtering disabled
Buffer logging: disabled, nml disabled,
filtering disabled
Logging Buffer size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
No active filter modules.
R3#
R3#show logging
R3#
R3#
```

The screenshot displays the Cisco Packet Tracer interface. On the left, a network topology is shown with the following components and connections:

- NTS Server** (192.168.1.5) connected to **Server PT PCA** (290-24 S1).
- Syslog Server** (192.168.1.6) connected to **Server PT PC-B** (290-24 S1).
- Server PT PCA** (290-24 S1) connected to **1941 R1**.
- Server PT PC-B** (290-24 S1) connected to **1941 R2**.
- 1941 R1** connected to **1941 R2** via a red link.
- 1941 R2** connected to **SSH Server** (1941 R3).
- SSH Server** (1941 R3) connected to **290-24T1 S3**.

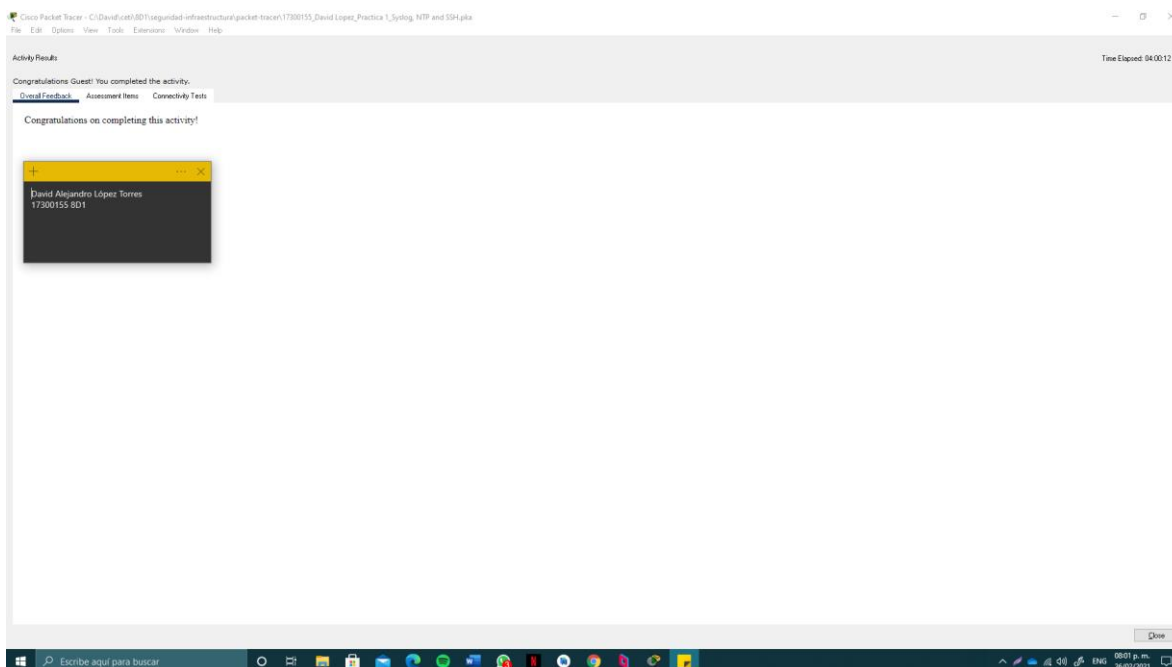
A terminal window for **David Alejandro López Torres** (17300155 8D1) is open, showing a yellow prompt.

The **PC-B** configuration window is open, showing the **SERVICES** tab. The **Syslog** service is configured as follows:

Time	Hostname	Message
1 02/23/2021 08:20:27.988 PM	10.1.1.2	%SYS-5-CONFIG_1 Configd
2 02/23/2021 08:21:11.195 PM	192.168.1.1	%SYS-5-CONFIG_1 Configd
3 02/23/2021 08:21:25.641 PM	10.2.2.1	%SYS-5-CONFIG_1 Configd

The **Services** list on the left includes: HTTP, DHCP, DHCPv6, TFTP, DNS, **SYSLOG** (selected), AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP.

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 esta 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 protocolos que pueden ser implementados para brindar una estructura más segura a la infraestructura de la red. Hemos visto la utilidad del protocolo NTP y cómo 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 como la implementación de SSH para garantizar una conexión segura a la configuración del conmutador de manera remota.