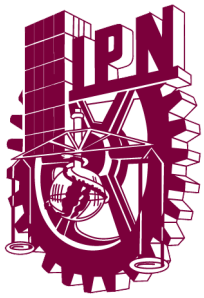


INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

Actividad 8: Configuración Syslog y NTP Server

NOMBRES:

- MACÍAS CASTILLO JOSUÉ
- OCHOA MONROY JOSÉ LUIS

GRUPO: 4CV3

UNIDAD DE APRENDIZAJE: ADMINISTRACIÓN DE SERVICIOS EN RED

PERIODO: 20-21/1

FECHA: 23 DE NOVIEMBRE DEL 2020

INTRODUCCIÓN

Syslog

Una característica que permite y facilita la administración de los dispositivos en una infraestructura de red es la existencia de los mensajes que estos dispositivos generan cuando ocurren diferentes tipos de eventos. Esta gran variedad de eventos, sumada a las diferentes características y necesidades que puede tener cada infraestructura de red, provoca que existan mensajes relevantes para la administración, y mensajes que no son tan importantes de capturar y almacenar.

De acuerdo con (ITESA, s.f.), el protocolo de *syslog* "permite que los dispositivos de red envíen los mensajes del sistema a servidores de syslog a través de la red." Además de esta definición, (ITESA, s.f.) también menciona tres características principales de este protocolo:

- La capacidad de recopilar información de registro para el control y la resolución de problemas
- La capacidad de seleccionar el tipo de información de registro que se captura
- La capacidad de especificar los destinos de los mensajes de syslog capturados

Todas estas funciones resultan fundamentales si tomamos en cuenta lo comentado anteriormente. Cada dispositivo es capaz de emitir muchos tipos de mensajes, y al almacenarlos todos ocurrirían dos consecuencias negativas:

- Se volvería más complicado y tardado para los administradores extraer conclusiones significativas de una cantidad de mensajes tan grande.
- El ancho de banda de la red se saturaría con la transmisión de todos esos mensajes que no forman parte de los servicios para los que fue construida la infraestructura.

Es aquí donde radica la importancia de un protocolo como Syslog. Su funcionamiento en dispositivos Cisco comienza enviando los mensajes del sistema y el resultado del comando *debug* a un proceso de registro local interno del

dispositivo. La forma en que el proceso de registro administra estos mensajes y resultados se basa en las configuraciones del dispositivo. (ITESA, s.f.). Los mensajes de Syslog pueden almacenarse y consultarse de distintas formas, entre las que se encuentran los servidores Syslog (que ofrecen formulación de informes automatizados) o en un búfer interno de cada dispositivo al que sólo se puede acceder por medio de la línea de comandos.

Los mensajes de Syslog pueden manifestarse por muchos tipos de eventos en una infraestructura de red. Tomando esto en cuenta, cada mensaje se construye bajo un formato que contiene un "nivel de gravedad" e información sobre las instalaciones de Syslog, cuya disponibilidad depende del tipo de dispositivo de red que formule los mensajes. En la siguiente tabla, se resume el significado de cada nivel presente en los mensajes de Syslog.

Nombre de la gravedad	Nivel de gravedad	Explicación
Emergencia	Nivel 0	El sistema no se puede usar.
Alerta	Nivel 1	Se necesita una acción inmediata.
Crítico	Nivel 2	Condición crítica.
Error	Nivel 3	Condición de error.
Advertencia	Nivel 4	Condición de advertencia.
Notificación	Nivel 5	Condición normal pero importante.
informativo	Nivel 6	Mensaje informativo.
Depuración	Nivel 7	Mensaje de depuración.

(ITESA, s.f.).

Por otro lado, algunas instalaciones comunes de mensajes de Syslog presentes en los routers de Cisco incluyen IP, OSPF, Sistema Operativo (SYS), Seguridad IP (IPSec) e IP de Interfaz (IF). El formato general para un mensaje de Syslog es el siguiente:

seq no: timestamp: %facility-severity-MNEMONIC: description

Ejemplo:

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up

NTP

En muchas ocasiones, existen infraestructuras de red que, para poder cumplir con su propósito y proporcionar los servicios para las que fueron creadas, requieren que sus dispositivos se encuentren cronológicamente sincronizados. La sincronización es un reto bastante grande, sobre todo si se intentara realizar de manera manual, ya que existen muchos factores físicos y tecnológicos que generan ralentizaciones, las cuales perjudican la calidad de la sincronización.

Con el objetivo de afrontar este reto, surgen protocolos como NTP. De acuerdo con (Coulouris G. et. al., 2012), el *Protocolo del Tiempo de la Red* (NTP por sus siglas en inglés) define una arquitectura para un servicio de horario y un protocolo para distribuir información sobre el tiempo a través de Internet. El objetivo primordial de NTP es proporcionar un servicio que les permita a los usuarios de Internet estar sincronizados de manera precisa al *Tiempo Universal Coordinado* (UTC por sus siglas en inglés). Para superar las dificultades mencionadas anteriormente que aparecen con la sincronización, NTP emplea técnicas estadísticas para filtrar datos sobre el tiempo y evalúa la calidad de los datos del tiempo proporcionados por servidores diferentes, para elegir la mejor alternativa. (Coulouris G. et. al., 2012) mencionan otros objetivos del NTP que son igual de importantes:

- Proporcionar un servicio confiable que pueda sobrevivir a pérdidas prolongadas de conectividad.
- Permitir que los clientes puedan resincronizarse con la frecuencia suficiente como para compensar las tasas de deriva que se manifiestan en la mayoría de las computadoras.
- Proporcionar protección contra interferencias con el servicio del tiempo, ya sea que se trate de interferencias maliciosas o accidentales.

El servicio del NTP es brindado por medio de una red de servidores que se encuentran dispersos alrededor de la Internet.

SOLUCIÓN DE LA ACTIVIDAD

Situación

En esta actividad, habilitará y usará los servicios de syslog y NTP para que el administrador de red pueda monitorear la red de forma más eficaz.

Parte 1: Configurar el servicio de syslog

Paso 1: Habilitar el servicio de syslog.

a. Haga clic en **Syslog** y, a continuación, en la ficha **Config**.

b. Active el servicio de **syslog** y mueva la ventana para poder monitorear la actividad.

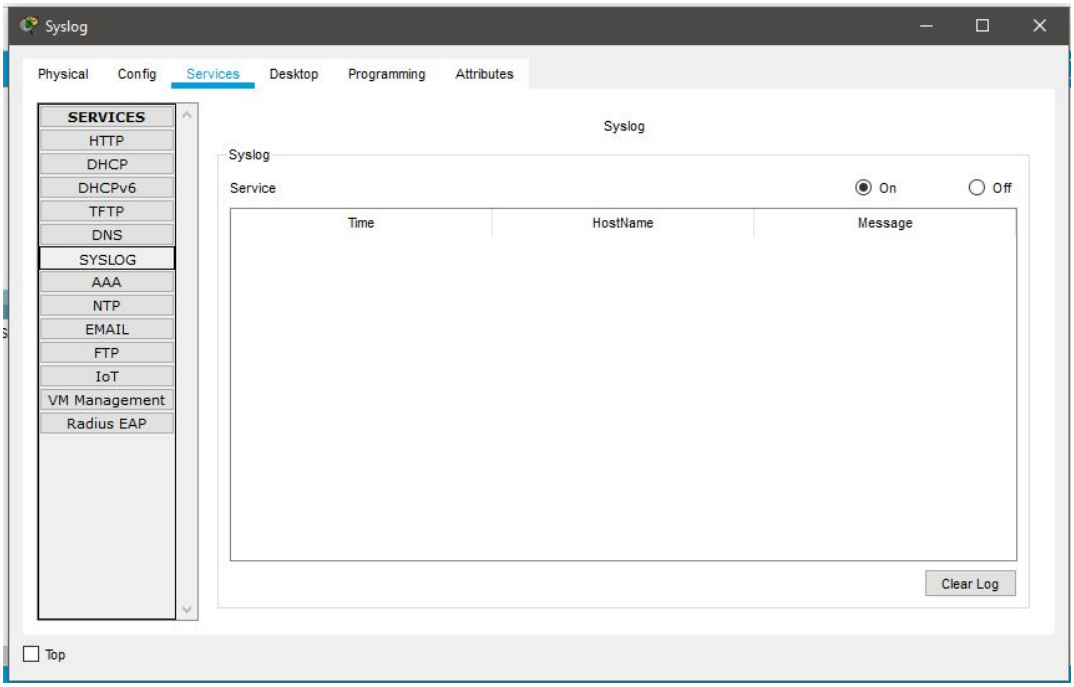
Paso 2: Configurar los dispositivos intermediarios para que utilicen el servicio de syslog.

a. Configure el **R1** para enviar eventos de registro al servidor de **Syslog**.

```
R1(config)# logging 10.0.1.254
```

b. Configure el **S1**y el **S2** para enviar eventos de registro al servidor de **Syslog**.

c. Configure el **S2** para enviar eventos de registro a la dirección IP del servidor de **Syslog**.



Captura de activación de servicio Syslog

```
R1>ena
R1#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#logging 10.0.1.254
```

```
S1>ena
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#logging 10.0.1.254
S1(config)#
```

```
S2>ena
S2#confi t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#logging 10.0.1.254
S2(config)#
```

Comandos para enviar eventos de registro al servidor

Parte 2: Generar eventos registrados

Paso 1: Cambiar el estado de las interfaces para crear registros de eventos.

a. Configure una interfaz Loopback 0 en **R1** y, a continuación, deshabilítela.

b. Apague la **PC1** y la **PC2**. Vuelva a prenderlas.

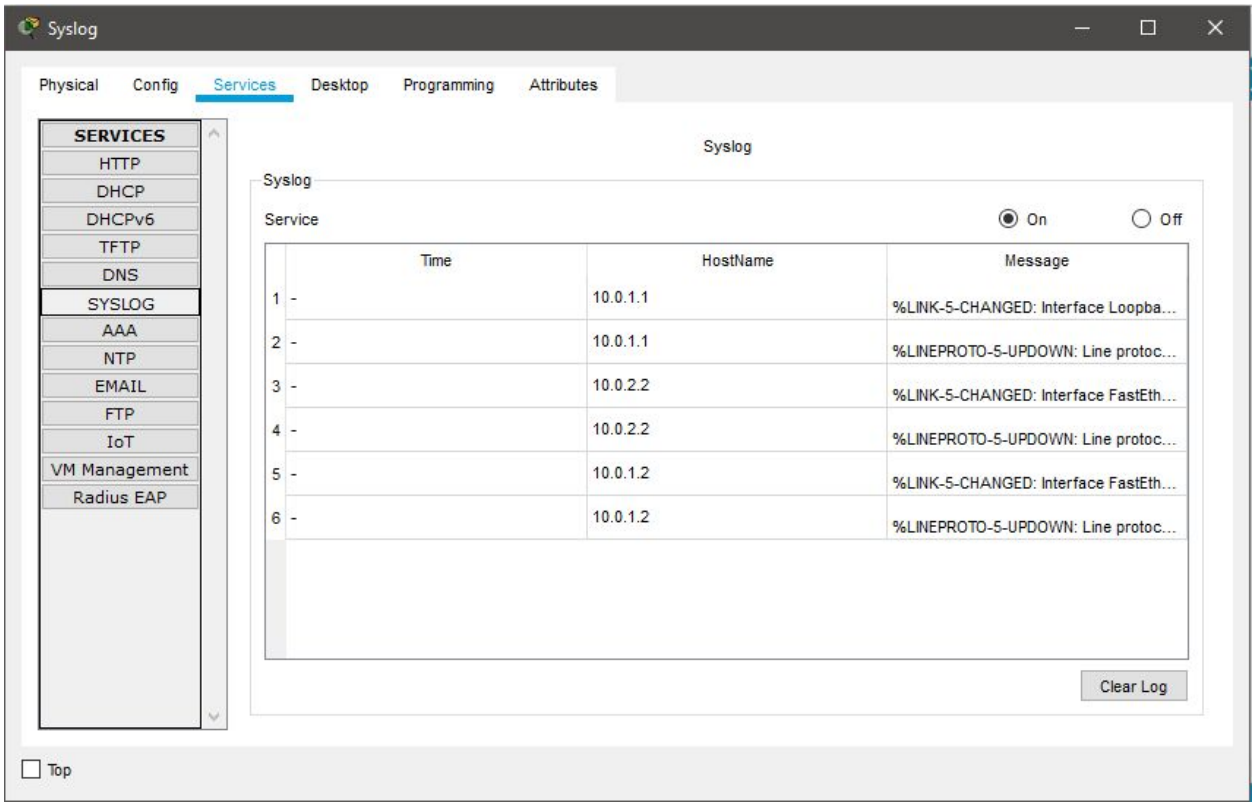
Paso 2: Analizar los eventos de syslog.

a. Observe los eventos de syslog. **Nota:** se registraron todos los eventos; sin embargo, las marcas de hora son incorrectas.

b. Borre el registro antes de continuar con la parte siguiente.

```
R1(config)#int loopback 0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed
state to up

R1(config-if)#exit
R1(config)#no int loopback 0
R1(config)#
%LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed
state to down
```

Configuración de la interfaz Loopback



Registro de eventos en Syslog

Parte 3: Establecer manualmente los relojes de los switches

Paso 1: Establecer manualmente los relojes de los switches.

Configure manualmente el reloj en el **S1** y el **S2** con la fecha actual y la hora aproximada. Se proporciona un ejemplo.

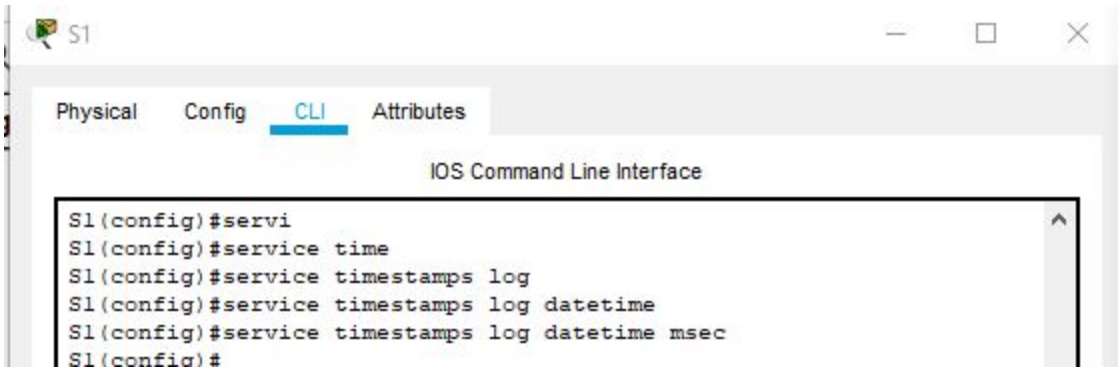
```
S1# clock set 11:47:00 July 10 2013
```

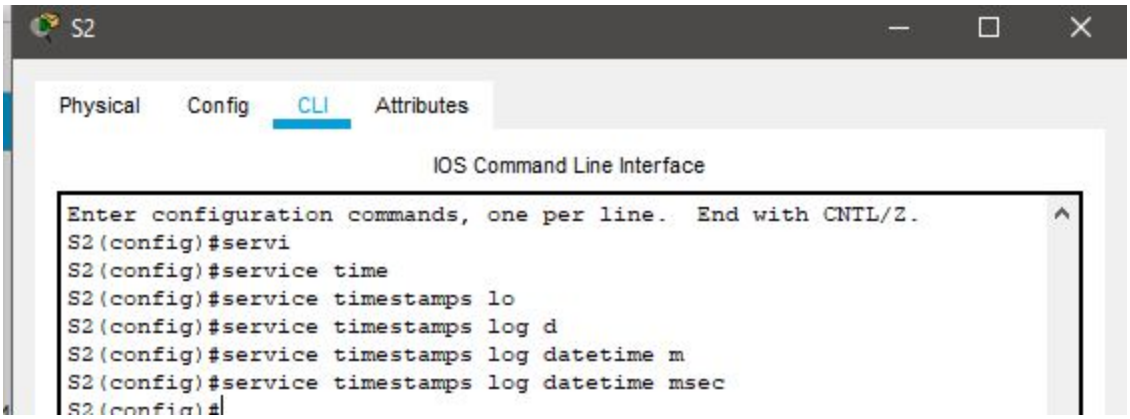
Paso 2: Habilitar el servicio de marca de hora de registro en los switches.

Configure el **S1** y el **S2** para enviar la marca de hora con los registros que envían al servidor de **Syslog**.

```
S1(config)# service timestamps log datetime msec
```

Configuración manual de reloj en S1 y S2





Configuración para enviar la marca de hora a los registros en S1 y S2

Parte 4: Configurar el servicio NTP

Paso 1: Habilitar el servicio NTP.

En esta actividad, se supone que el servicio NTP se aloja en un servidor de Internet pública. Si el servidor NTP fuera privado, también se podría usar la autenticación.

a. Abra la ficha **Config** del servidor **NTP**.

b. Active el servicio NTP y observe la fecha y la hora que se muestran.

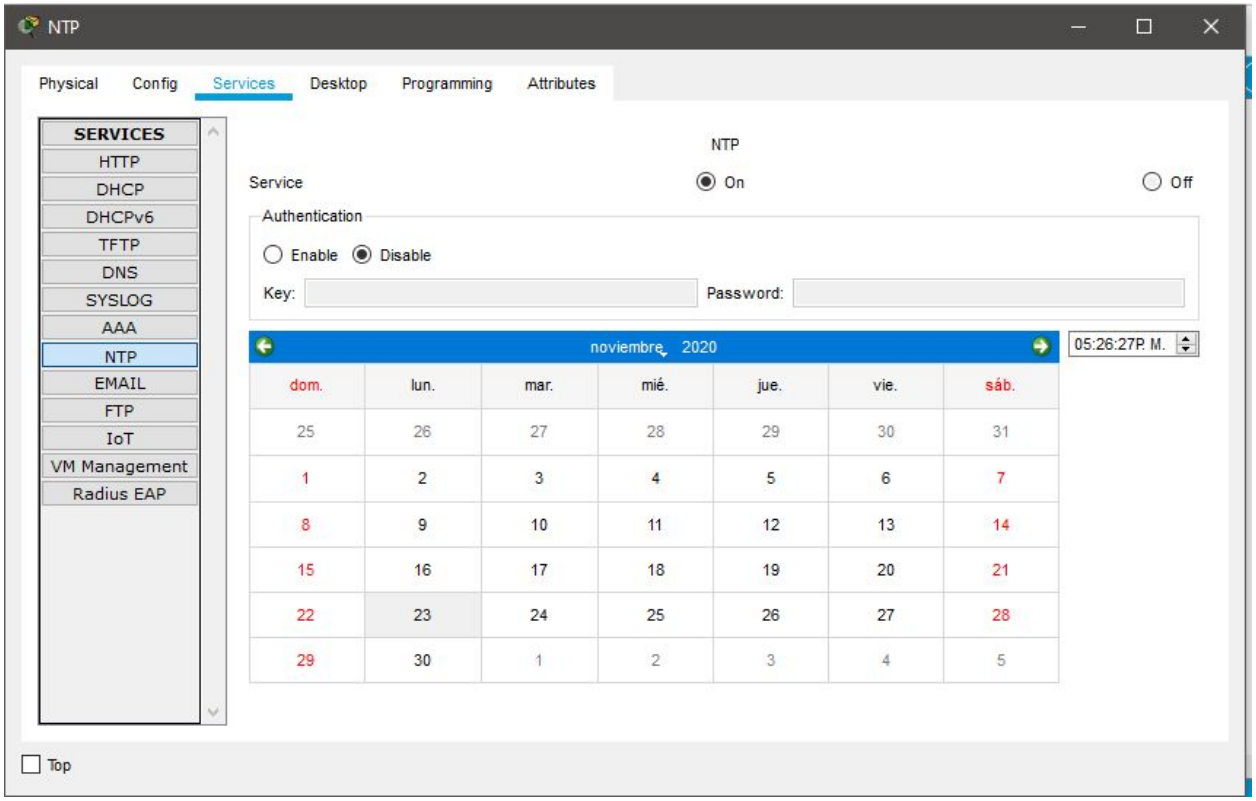
Paso 2: Establecer automáticamente el reloj del router.

Configure el reloj en el **R1** según la fecha y la hora del servidor NTP.

```
R1(config)# ntp server 64.103.224.2
```

Paso 3: Habilitar el servicio de marca de hora de registro en el router.

Configure el **R1** para enviar la marca de hora con los registros que envía al servidor de **Syslog**.



Activación de servicio NTP

```
R1(config)#ntp se
R1(config)#ntp server 64.103.224.2
R1(config)#
```

Configuración del reloj en R1 con NTP

```
R1(config)#service timestamps log d
R1(config)#service timestamps log datetime m
R1(config)#service timestamps log datetime msec
R1(config)#
```

Configuración para enviar marca de hora a los registros en R1

Parte 5: Verificar los registros con marca de hora

Paso 1: Cambiar el estado de las interfaces para crear registros de eventos.

a. Vuelva a habilitar y después deshabilite la interfaz Loopback 0 en R1.

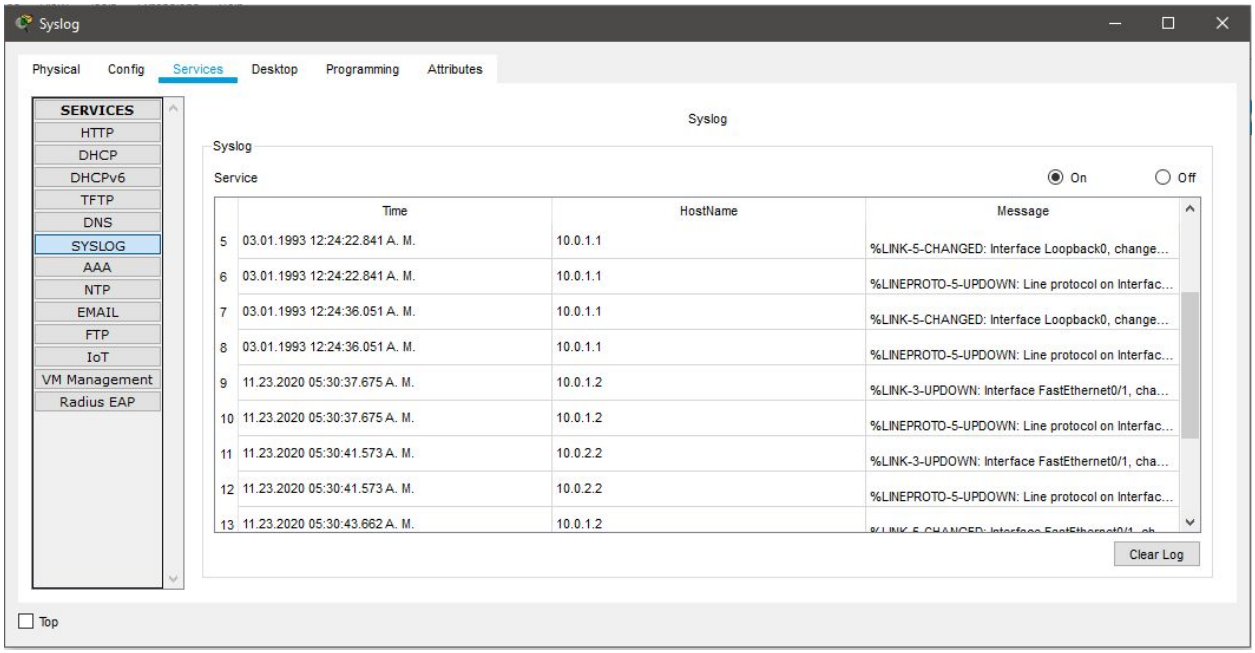
b. Apague las computadoras portátiles **L1** y **L2**. Vuelva a prenderlas.

Paso 2: Analizar los eventos de syslog.

Observe los eventos de syslog. **Nota:** se registraron todos los eventos, y las marcas de hora son correctas como se configuraron. **Nota:** el **R1** usa la configuración de reloj del servidor NTP, y el **S1** y el **S2** usan la configuración de reloj que usted configuró en la parte 3.

```
R1(config)#int loopback 0

R1(config-if)#
*mar. 01, 00:24:22.2424: %LINK-5-CHANGED: Interface Loopback0,
changed state to up
*mar. 01, 00:24:22.2424: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
R1(config-if)#
R1(config-if)#exit
R1(config)#no int loopback 0
R1(config)#
*mar. 01, 00:24:36.2424: %LINK-5-CHANGED: Interface Loopback0,
changed state to administratively down
*mar. 01, 00:24:36.2424: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to down
R1(config)#
R1(config)#
```

Configuración de Loopback 0



Eventos en Syslog con marcas de hora correctas

Comandos extra en R1

show ntp associations

```
R1#sh ntp associations

address         ref clock       st   when     poll    reach  delay
offset           disp
*~64.103.224.2  127.127.1.1     1    3        16      377    4.00
-22.00           0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
R1#
```

show ntp status

```
R1#sh ntp status
Clock is synchronized, stratum 2, reference is 64.103.224.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 0C6DDED9.00000012 (17:35:21.018 UTC lun. nov. 23 2020)
clock offset is -7.00 msec, root delay is 2.00  msec
root dispersion is 10.21 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s
system poll interval is 4, last update was 10 sec ago.
R1#
```

show running-config (ntp y syslog)

```
R1#sh running-config
Building configuration...

Current configuration : 1178 bytes
!
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!

line vty 0 4
 login
!
!
ntp server 64.103.224.2
!
end
```

CONCLUSIONES

MACÍAS CASTILLO JOSUÉ

En esta práctica configuramos los protocolos de Syslog y NTP, el primero es un protocolo que tiene la capacidad para recopilar la información que proporcionan los dispositivos en la topología, además puede seleccionar el tipo de información y especificar los destinos de los mensajes, en las primeras 3 partes de la práctica se nos enseña como levantar el servicio en el servidor de Syslog para después configurar los dispositivos intermediarios como son el router y los switch, esto se lleva a cabo con el comando "logging 'dirección ip del Syslog server'", se nos pide dar de alta y baja una interfaz loopback para ver los eventos que se registran en el Syslog server los cuales carecen de una hora y fecha por lo que se implementaron de manera manual, pero existe el protocolo NTP que hace lo mismo pero de una forma más precisa y automática este protocolo utiliza el Tiempo Universal Coordinado (UTC) para su fuente de sincronización de tiempo, al final se nos pide realizar la misma configuración de la interfaz loopback pero en esta ocasión sí contaba con la hora y fecha exactas.

OCHOA MONROY JOSÉ LUIS

Como administradores de red, resulta fundamental que conozcamos la manera de obtener información acerca de la infraestructura que estamos administrando. Por medio de esta práctica y las clases anteriores, sabemos que existe una variedad muy grande de mensajes de sistema proporcionados por los dispositivos de red, y lidiar con todos sería un proceso poco amigable con los recursos y, además, poco efectivo. Por medio de un protocolo como Syslog, es posible configurar un servidor cuya función sea almacenar determinados tipos de mensajes de Syslog, aliviando de carga a los dispositivos que se encargan de proporcionar los servicios de red porque también es posible configurarlos para que solo publiquen tipos específicos de mensajes; con ello, la red no se satura y los dispositivos no deben ocupar su almacenamiento interno para los mensajes que ahora estarán alojados en el servidor externo. Para que las etiquetas de tiempo presentes en los mensajes de Syslog aporten información significativa, se vuelve necesario que nuestros dispositivos de red se encuentren sincronizados; sin embargo, llevar a cabo esta labor de sincronización de forma manual sería complicado e ineficiente. Para solucionarlo, se implementa un protocolo como NTP, que brinda ese servicio de sincronización de forma robusta y automatizada.

REFERENCIAS

- ITESA, Cisco Networking Academy. (s.f.). *Funcionamiento de syslog*. Recuperado el 23 de noviembre de 2020, de: https://www.itesa.edu.mx/netacad/networks/course/module8/index.html#8.1.1.1
- Coulouris G., et. al. (2012). *Distributed Systems: Concepts and Design* (5th ed.). Boston: Addison-Wesley.