

# Packet Tracer: Configuración de syslog y NTP

**Cajiga Gutierrez Edgar Uriel**  
**Zepeda Flores Alejandro de Jesús**

## Introducción

### Syslog

Este término es usado para definir un protocolo desarrollado para definir el estándar. De lo que se encarga este protocolo es de enviar mensajes del sistema a servidores de syslog a través de la red. Esto es posible gracias a la gran variedad de dispositivos que son admitidos en el protocolo. Tales como routers, switches, servidores de aplicación, firewall y otros dispositivos de red.

El servicio de registro de syslog proporciona tres funciones principales:

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

El administrador de red puede especificar que solo se envíen determinados tipos de mensajes del sistema a varios destinos. Por ejemplo, se puede configurar el dispositivo para que reenvíe todos los mensajes del sistema a un servidor de syslog externo. Sin embargo, los mensajes del nivel de depuración se reenvían al búfer interno, y solo el administrador puede acceder a ellos desde la CLI.

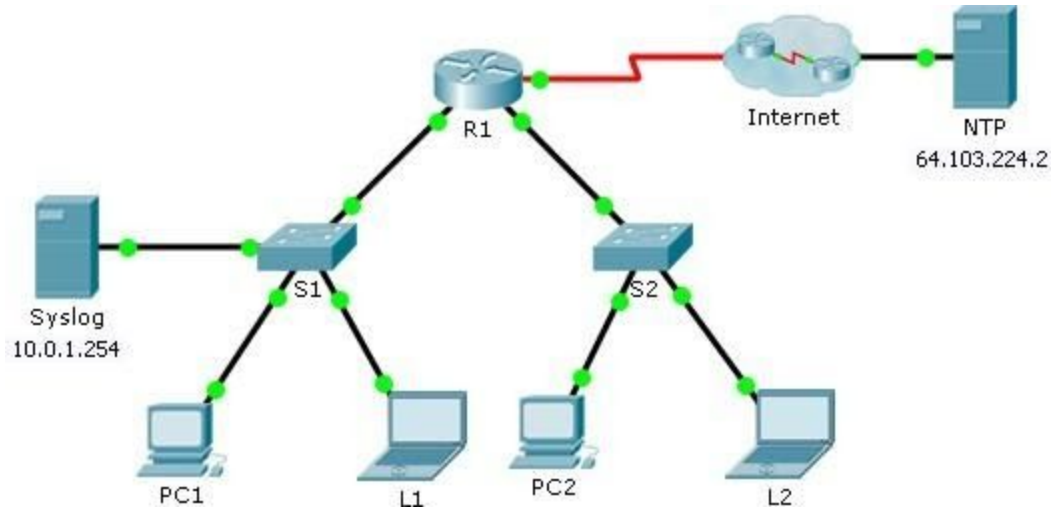
También es posible controlar los mensajes del sistema de manera remota viendo los registros en un servidor syslog o accediendo mediante Telnet, SSH o a través del puerto de consola.

### NTP

Un servidor NTP, es un servicio que se basa en el protocolo NTP el cual se utiliza para sincronizar varios relojes de red usando un conjunto de clientes y servidores repartidos. Además este protocolo se basa en el protocolo de datagrama de usuario, que permite enviar datagramas sin que se haya establecido previamente una conexión. Es decir, utiliza UDP como capa de transporte usando el puerto 123.

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.

## Topología



## Objetivos

- Parte 1: Configurar el servicio de syslog
- Parte 2: Generar eventos registrados
- Parte 3: Establecer manualmente los relojes de los switches
- Parte 4: Configurar el servicio NTP
- Parte 5: Verificar los registros con marca de hora

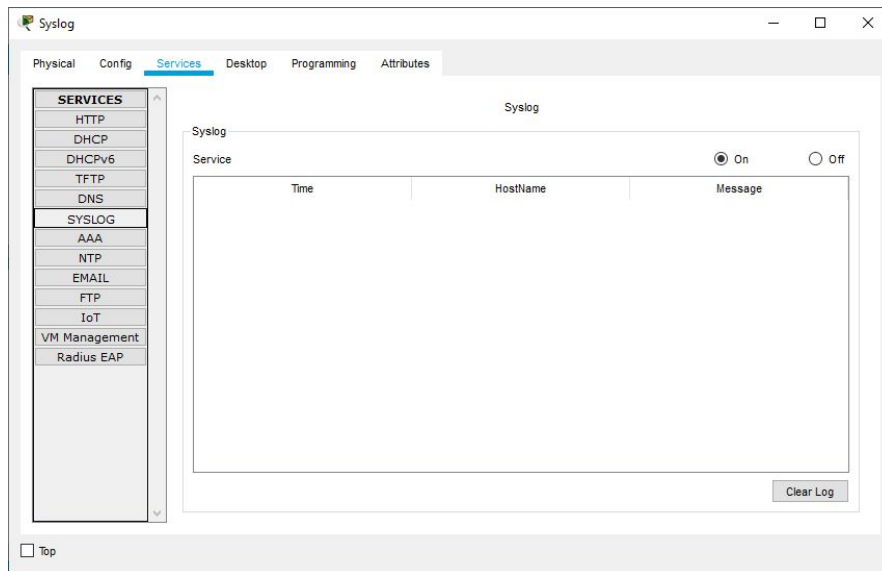
## Situación

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
```

```
R1(config)#login 10.0.1.254
R1(config)#
```

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

```
S1(config)#logging 10.0.1.254
S1(config)#
```

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

```
S2(config)#logging 10.0.1.254
S2(config)#
```

## Parte 2: Generar eventos registrados

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

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

#### Configuramos la interfaz loopback en el R1

```
R1(config)#interface loopback 0

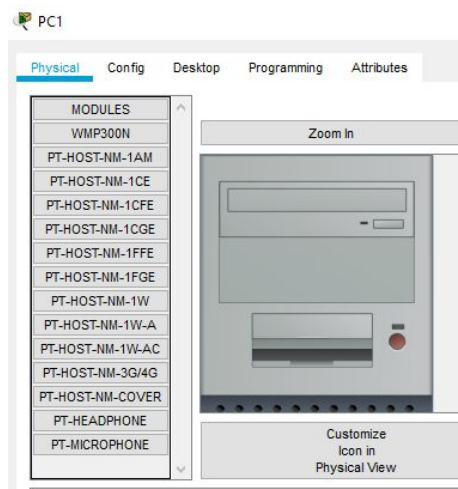
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

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

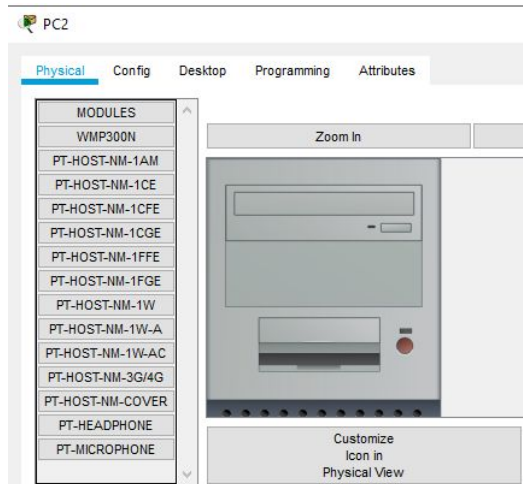
R1(config-if)#
```

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

#### Apagamos la PC1

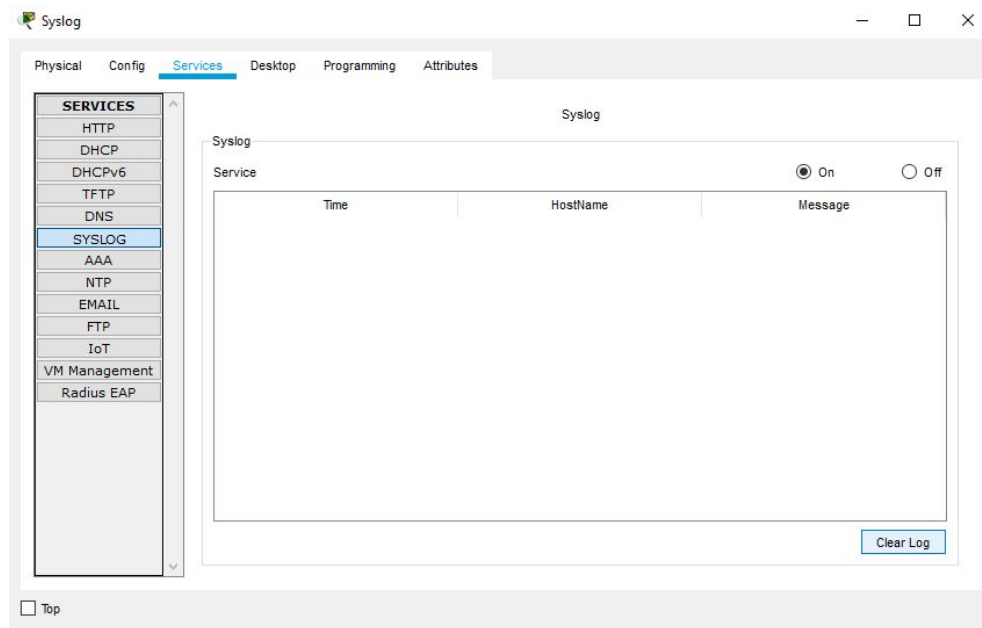


#### Apagamos la PC2



## Paso 2: Analizar los eventos de syslog.

- Observe los eventos de syslog. **Nota:** se registraron todos los eventos; sin embargo, las marcas de hora son incorrectas.
- Borre el registro antes de continuar con la parte siguiente.



## 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
```

Para S1 configuramos la fecha actual

```
S1#clock set 5:57:00 November 23 2020
S1#
```

Para S2 configuramos la fecha actual

```
-----
S2#clock set 5:56:00 November 23 2020
S2#
```

### 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
```

Se configura el S1

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

Se configura el S2

```
S2(config)#service timestamps log datetime msec
S2(config)#
```

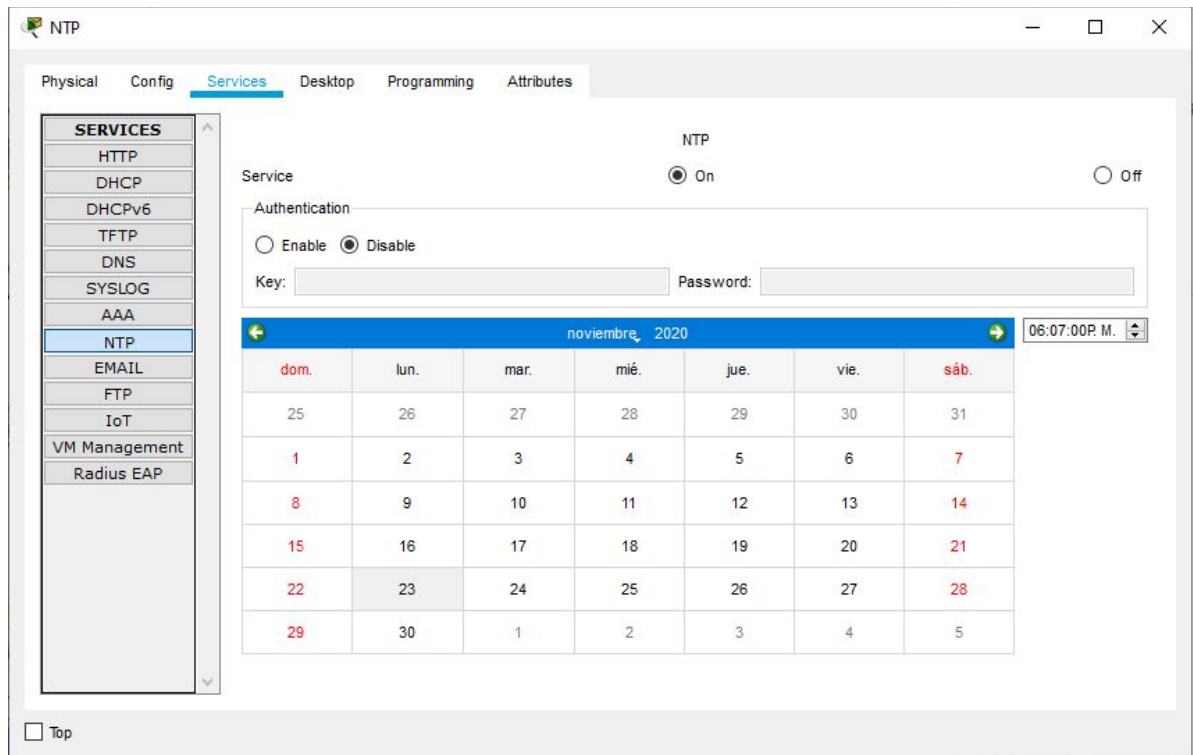
## Parte 4: Configurar el servicio NTP

### 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.

- Abra la ficha **Config** del servidor **NTP**.
- Active el servicio NTP y observe la fecha y la hora que se muestran.

Activamos el servicio NTP, y verificamos que la hora y fecha son la correcta



The screenshot shows the NTP configuration window with the following details:

- Services List:** HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, **NTP** (selected), EMAIL, FTP, IoT, VM Management, Radius EAP.
- NTP Service:** On (radio button selected).
- Authentication:** Disable (radio button selected).
- Key:** (empty field).
- Password:** (empty field).
- Calendar:** November 2020. The 23rd is highlighted.
- Time:** 06:07:00P. M.

## 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
```

Configuramos el R1 con la fecha y hora del NTP

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

## 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**.

Configuramos el R1 para enviar el registro de hora al servidor Syslog

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

## Parte 5: Verificar los registros con marca de hora

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

- Vuelva a habilitar y después deshabilite la interfaz Loopback 0 en R1.
- Apague las computadoras portátiles **L1** y **L2**. Vuelva a prenderlas.

Podemos ver el cambio cuando habilitamos y deshabilitamos la interfaz Loopback en el servicio Syslog

	Time	HostName	Message
1 -		10.0.1.2	%SYS-5-CONFIG_I: Configured from c...
2 -		10.0.1.2	%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.0.1.254 port 514 st...
3	11.23.2020 06:08:20.210 A. M.	10.0.1.2	%LINK-3-UPDOWN: Interface GigabitEt...
4	11.23.2020 06:08:20.210 A. M.	10.0.1.2	%LINEPROTO-5-UPDOWN: Line protoc...
5	11.23.2020 06:08:30.823 A. M.	10.0.1.2	%LINK-5-CHANGED: Interface Gigabit...
6	11.23.2020 06:08:30.823 A. M.	10.0.1.2	%LINEPROTO-5-UPDOWN: Line protoc...

Ahora probamos los cambios que se pueden apreciar al encender y apagar las PC1 y PC2

Syslog

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

Syslog

Service

On

Off

	Time	HostName	Message
8	11.23.2020 06:17:34.801 A. M.	10.0.1.2	%LINK-5-CHANGED: Interface FastEt...
9	11.23.2020 06:17:33.995 A. M.	10.0.1.2	%LINEPROTO-5-UPDOWN: Line proto...
10	11.23.2020 06:17:33.995 A. M.	10.0.1.2	%LINK-3-UPDOWN: Interface FastEt...
11	-	10.0.1.2	%SYS-5-CONFIG_: Configured from...
12	-	10.0.1.2	%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.0.1.254 port 514 ...
13	11.23.2020 06:08:20.210 A. M.	10.0.1.2	%LINK-3-UPDOWN: Interface Gigabit...
14	11.23.2020 06:08:20.210 A. M.	10.0.1.2	%LINEPROTO-5-UPDOWN: Line proto...
15	11.23.2020 06:08:30.823 A. M.	10.0.1.2	%LINK-5-CHANGED: Interface Gigabi...
16	11.23.2020 06:08:30.823 A. M.	10.0.1.2	%LINEPROTO-5-UPDOWN: Line proto...

Clear Log



## Conclusiones

### Cajiga Gutiérrez Edgar Uriel

Con esta práctica pusimos en práctica la teoría vista en clase. Notamos la importancia que tiene mantener sincronizados los relojes de nuestros equipos, y cómo es posible hacerlo con el protocolo NTP. Además vimos lo fácil que es hacer esto al configurar la hora y fecha correcta en nuestro servidor NTP y posteriormente sincronizar nuestro router apartir de esto se noto claramente la estructura que sigue este protocolo y como nuestra topología se puede comportar como un árbol al ir propagando la fecha y hora.

Por otro lado vimos como el protocolo NTP, va muy de la mano con el protocolo syslog, el syslog se encarga de mantener un registro del comportamiento de nuestra red para mantener una correcta administración. Esto trabajando junto con el protocolo NTP se logra mantener una congruencia del registro respecto a las fechas y horas que se hace cada registro.

### Zepeda Flores Alejandro de Jesús

La implementación de esta práctica, sirvió para descubrir 2 cosas, la primera es el protocolo estándar para el envío de los mensajes del sistema a los servidores; con la ayuda de syslog, podemos almacenar, interpretar y mostrar mensajes, ya sea de errores o de información normal en la transferencia de mensajes, pero nos permite tener el control sobre estos.

La segunda es acerca del protocolo NTP para sincronizar los relojes de los clientes en la red. Puede que por separado, sincronizar los relojes no tenga mucho sentido, sin embargo, al complementarlo con syslog, se vuelve importante, ya que los mensajes regularmente tienen una estampa de tiempo y de esta forma, nos permite añadir información adicional como la fecha y hora exacta del mismo.

## Bibliografía

[1] Walton, A. (2018, 15 febrero). *syslog: Funcionamiento y Configuración*. CCNA desde Cero. <https://ccnadesdecero.es/syslog-funcionamiento-y-configuracion/>

[2] 1&1 IONOS Inc. (2020, 30 septiembre). *¿Qué es el NTP?* IONOS Digitalguide. <https://www.ionos.mx/digitalguide/servidores/know-how/que-es-el-ntp/>