Instituto Politécnico Nacional

Escuela Superior de Computo

Unidad de aprendizaje: Administración de servicios de red [4CV5]

Profesor: Henestrosa Carrasco Leticia

Actividad #8: Configuración de syslog y NTP

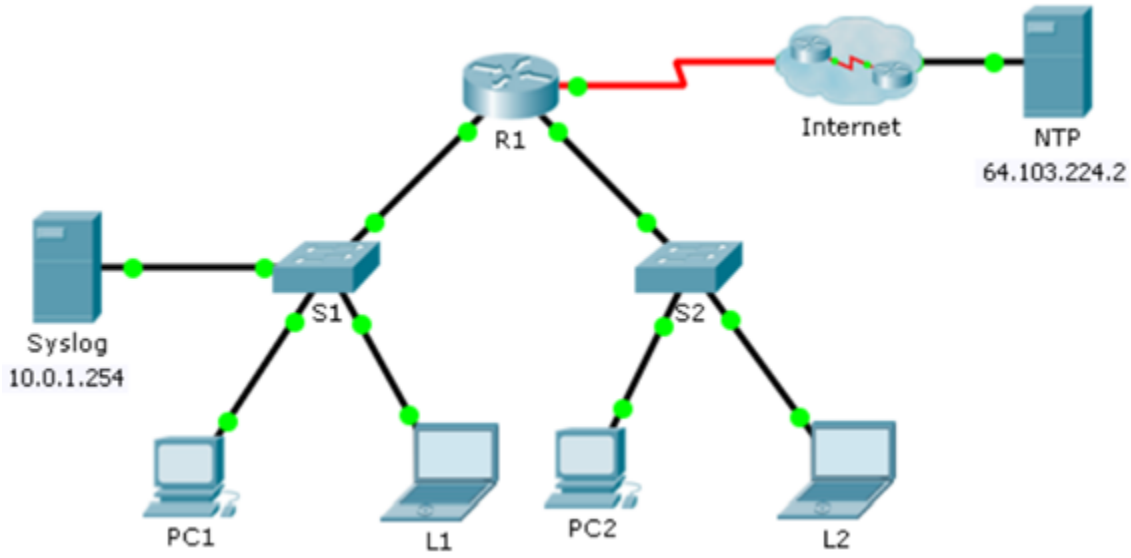
Alumnos: García González Aarón Antonio & Villalba Gil Ángel

Noviembre, 2020

Índice

Topología 3
Objetivos 3
Introducción 3
Desarrollo 4
Situación 4
Parte 1: Configurar el servicio de syslog 4
Parte 2: Generar eventos registrados 6
Parte 3: Establecer manualmente los relojes de los switches 8
Parte 4: Configurar el servicio NTP 8
Parte 5: Verificar los registros con marca de hora 9
Conclusiones 11
García González Aarón Antonio 11
Villalba Gil Angel 11
Referencias 11

Topología



Objetivos

- Configurar el servicio de syslog
- Generar eventos registrados
- Establecer manualmente los relojes de los switches
- Configurar el servicio NTP
- Verificar los registros con marca de hora

Introducción

Supervisar una red en funcionamiento puede proporcionar información a un administrador de red para administrar la red de forma proactiva e informar estadísticas de uso de la red a otros.

Cuando ocurren ciertos eventos en una red, los dispositivos de red tienen mecanismos de confianza para notificar mensajes detallados del sistema al administrador. Estos mensajes pueden ser importantes o no.

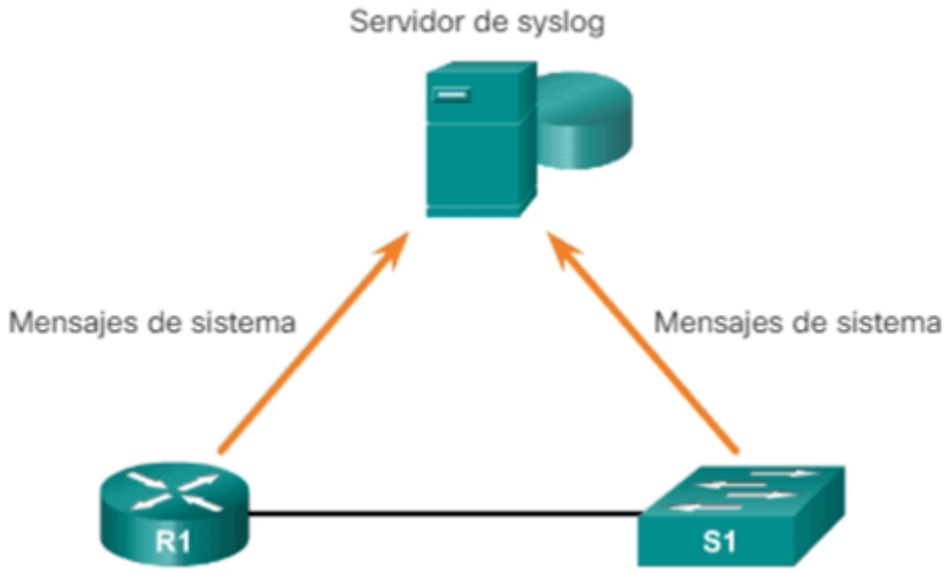
Los administradores de red tienen una variedad de opciones para almacenar, interpretar y mostrar estos mensajes, así como para recibir esos mensajes que podrían tener el mayor impacto en la infraestructura de la red.

El método más común para acceder a los mensajes del sistema que proporcionan los dispositivos de red es utilizar un protocolo denominado “syslog“. El protocolo syslog se desarrolló para los sistemas UNIX en la década de los ochenta, pero la IETF lo registró por primera vez como RFC 3164 en 2001.

El protocolo syslog permite que los dispositivos de red envíen los mensajes del sistema a servidores de syslog a través de la red.

El servicio de registro de syslog proporciona tres funciones principales:

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



Por otro lado, para poder sincronizar los elementos de una red ocupamos el protocolo NTP. Es uno de los protocolos de internet más viejos que siguen en uso, desarrollado en 1981 y descrito por primera vez en RFC 778.

En el proceso de sincronización, el NTP utiliza el tiempo universal coordinado (UTC), que obtienen los clientes y los servidores según un sistema jerárquico.

Desarrollo

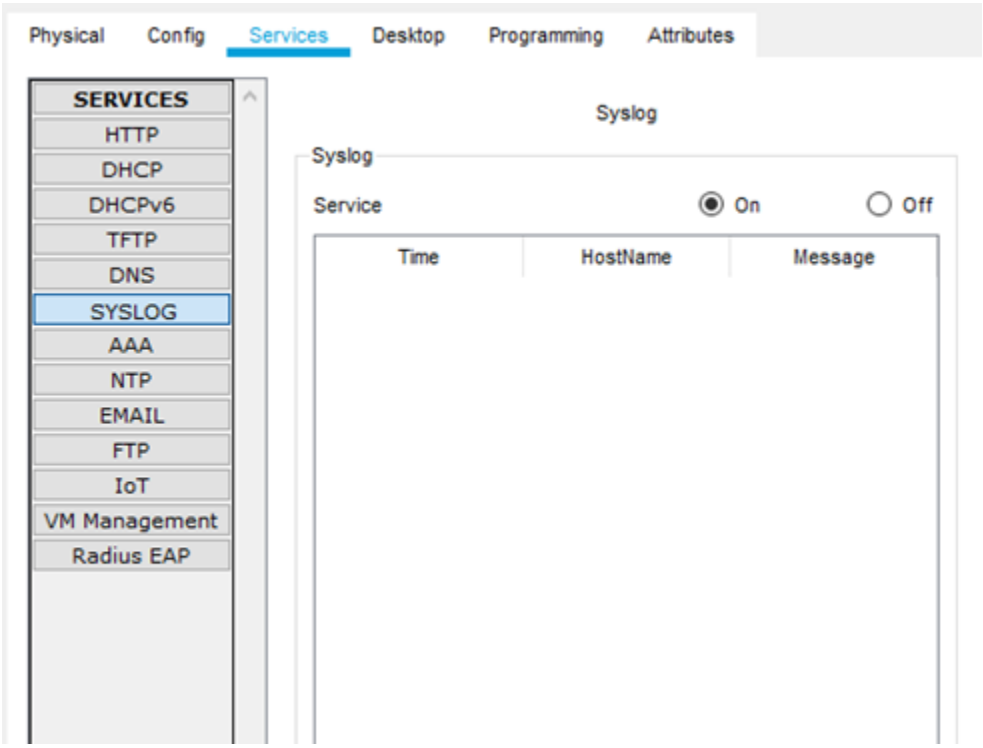
Situación

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.

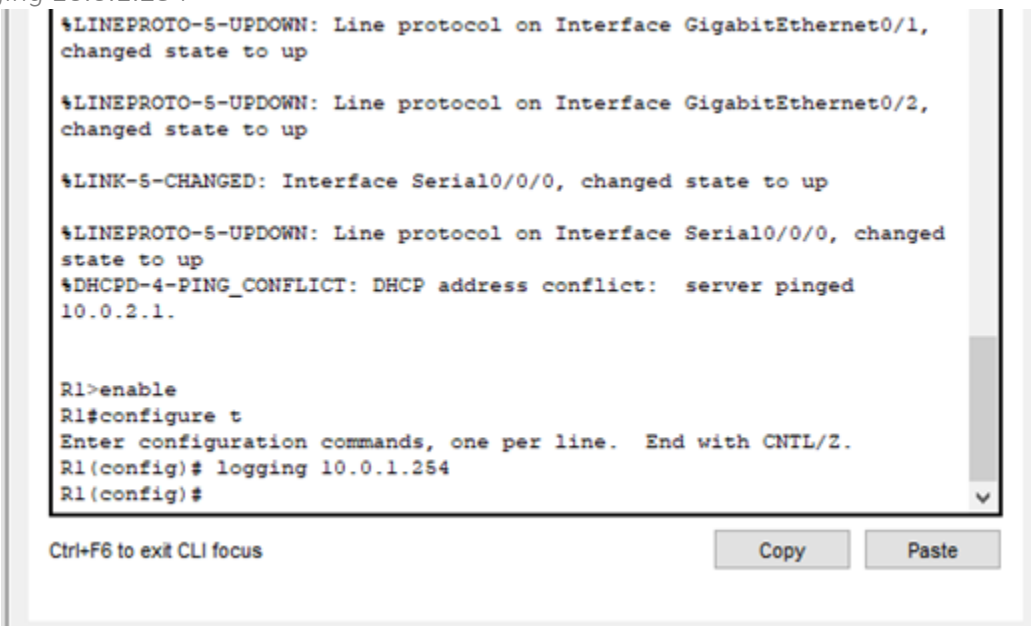
1. Haga clic en Syslog y, a continuación, en la ficha Config.
2. Active el servicio de syslog y mueva la ventana para poder monitorear la actividad.



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.

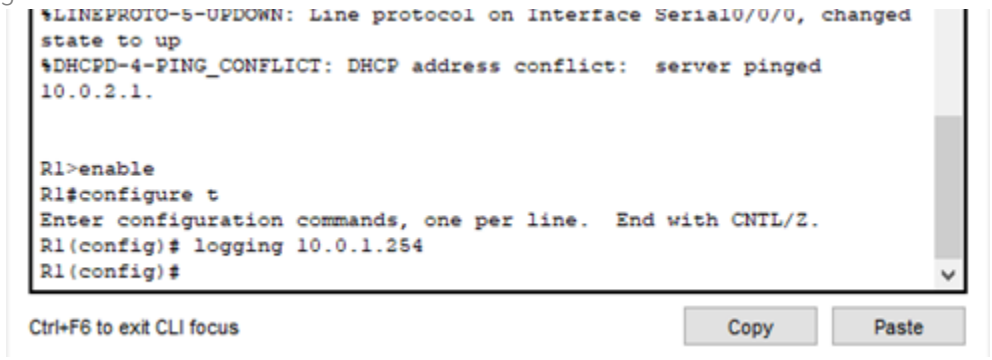
R1>enable
R1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# logging 10.0.1.254



b. Configure el S1y el S2 para enviar eventos de registro al servidor de syslog.

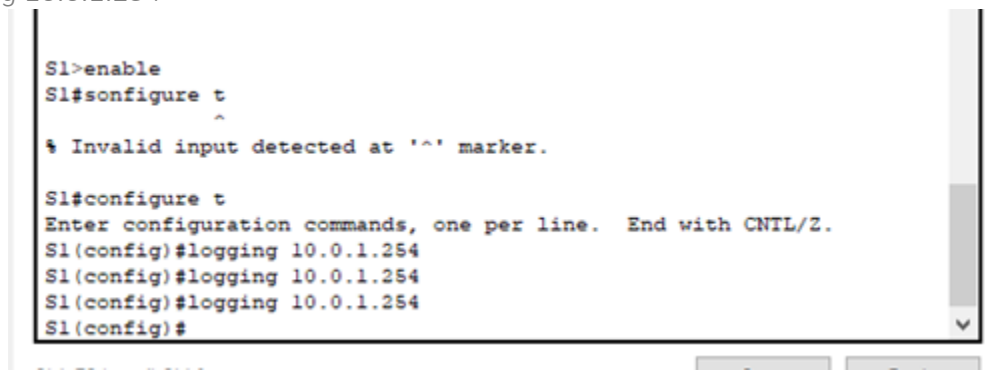
S1>enable
S1#configure t
Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#logging 10.0.1.254



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

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



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.

R1>enable
R1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
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)#shutdown

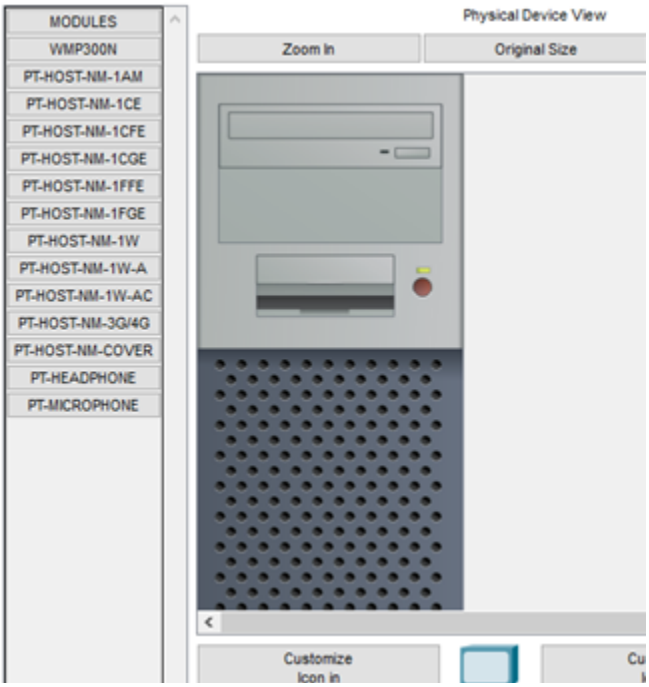
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to administratively down

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

```
R1>enable
R1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#shutdown

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

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

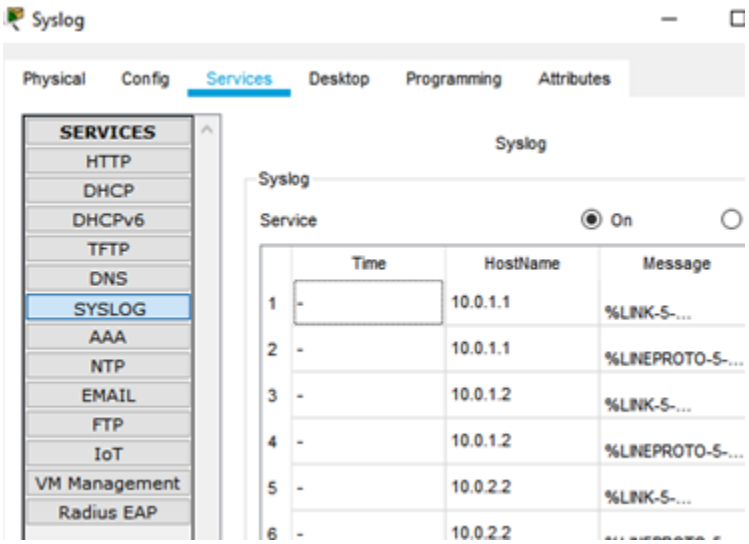
Ctrl+F6 to exit CLI focus Copy Paste

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.

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>enable
S1#clock set 11:47:00 July 10 2013
S2>enable
S2#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#configure t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#service timestamps log datetime msec

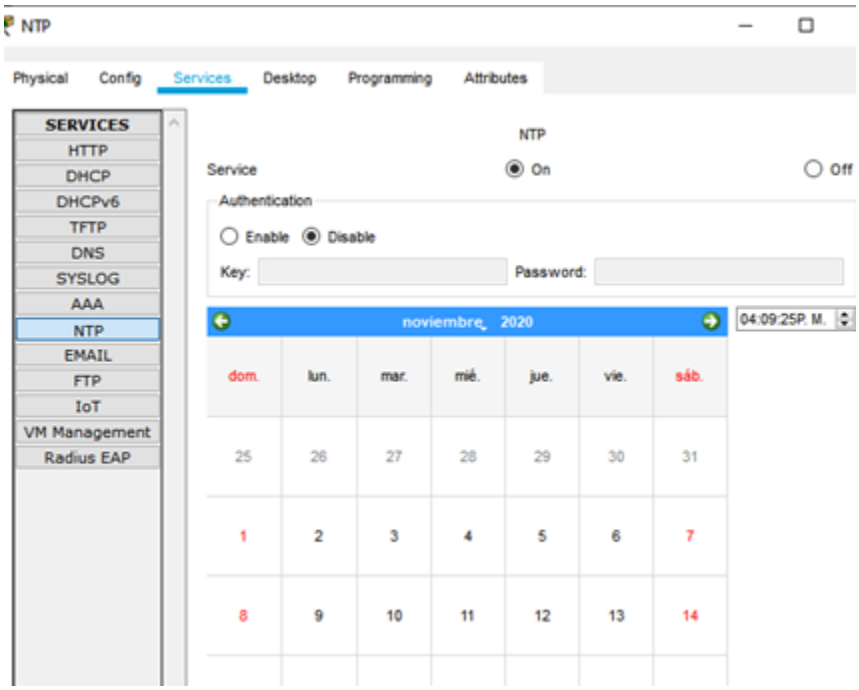
S2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#service timestamps log datetime msec

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.

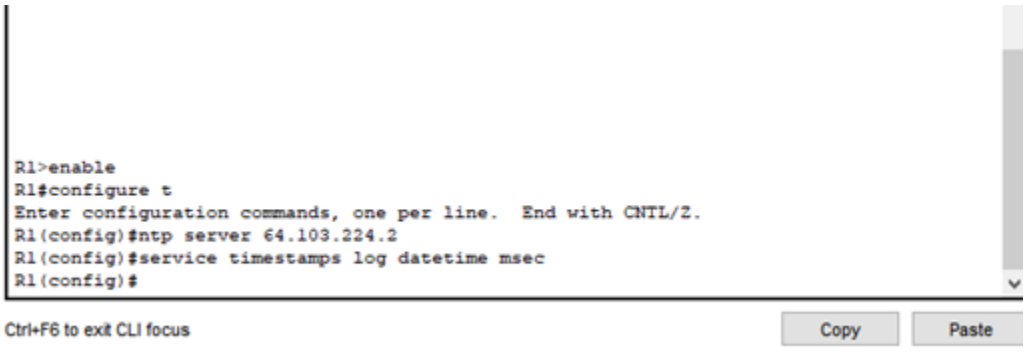
Configure el reloj en el R1 según la fecha y la hora del servidor NTP.

R1>enable
R1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
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.

R1(config)#service timestamps log datetime msec



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.

R1(config)#interface loopback 0

R1(config-if)#no shutdown

R1(config-if)#

**nov. 24, 16:24:47.2424: %LINK-5-CHANGED: Interface Loopback0, changed state to up*

**nov. 24, 16:24:47.2424: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up*

R1(config-if)#shutdown

R1(config-if)#

**nov. 24, 16:25:06.2525: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down*

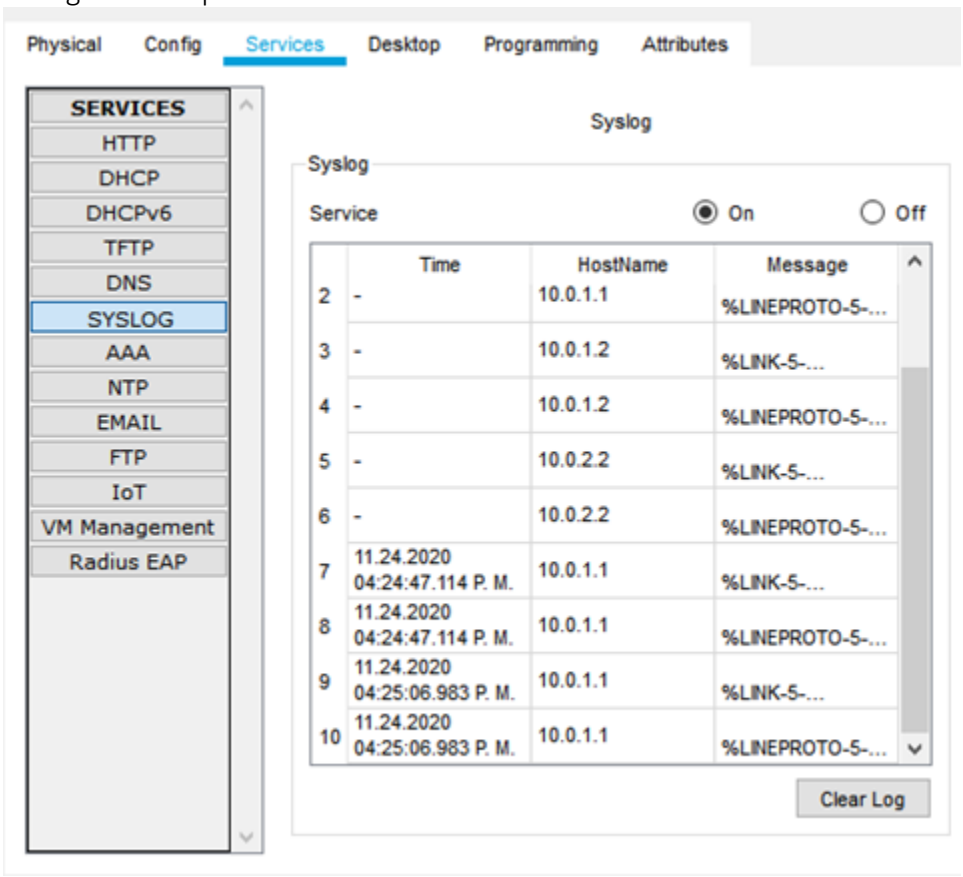
**nov. 24, 16:25:06.2525: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down*

R1(config-if)#

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.



Conclusiones

García González Aarón Antonio

Cuando hablamos del FCAPS al inicio del curso, debo de admitir que esta es una de las tareas que mas me llamo la atención, ya que en mi vida había tenido contacto con algo así en el área de redes, es muy sencillo llevar este tipo de documentación y registros.

Tal y como lo mencionó la profesora en la sesión que abordamos este tema, al configurar syslog, se tiene que hacer en todos los dispositivos que se requiere que el servidor de syslog se sincronicen, de igual forma es muy útil el poder asignar de manera manual el reloj, aunque al hacer esto, es posible que haya cierto desfase en segundos entre los dispositivos ya que se configuran de manera sucesiva y no de manera encadenada.

Yo supongo que un servidor de syslog ya se encarga del formato y almacenamiento que se le da dichos logs, ya que como lo vimos en clase hay varios software que hacen dicha funcionalidad, quiero pensar que solo basta con registrar los dispositivos que se quiere monitorear y habilitar los log en los dispositivos.

Villalba Gil Ángel

Con la realización de esta práctica pude reafirmar la teoría previamente adquirida acerca de los protocolos syslog y NTP. Un problema al momento de desarrollarla fue que la primera vez que se checa los servicios Syslog del servidor no me aparecía la fecha ni hora e hizo que me espantara, pero conforme se fue desarrollando la practica todo iba bien y al final del desarrollo ya aparece la fecha y hora.

Cuando leí la actividad con detenimiento me iba guiando paso a paso, no estuvo difícil, en lo personal puedo decir que estuvo más sencilla que las anteriores.

Referencias

[1]. "8.1.2.5 Packet Tracer: Configuración de syslog y NTP", Itesa.edu.mx, 2020. [Online]. Available: https://www.itesa.edu.mx/netacad/networks/course/module8/8.1.2.5/8.1.2.5.html. [Accessed: 24- Nov- 2020].

[2]. 2020. [Online]. Available: https://ccnadesdecero.es/syslog-funcionamiento-y-configuracion/. [Accessed: 25- Nov- 2020].

[3]. "El funcionamiento de los mensajes syslog - Tokio", Tokio, 2020. [Online]. Available: https://www.tokioschool.com/noticias/funcionamiento-mensajes-syslog/. [Accessed: 25- Nov- 2020].