LABORATORIO DE REDES DE ÁREA EXTENDIDA

PRÁCTICA N° 4

1. TEMA

ADMINISTRACIÓN Y MANTENIMIENTO DE DISPOSITIVOS (PARTE II)

2. OBJETIVOS

2.1. Configurar syslog y enviar notificaciones a un servidor “Kiwi Syslog Server”.
2.2. Crear archivos de respaldo de las configuraciones utilizando un servidor tftp.

3. MARCO TEÓRICO

3.1. SYSLOG

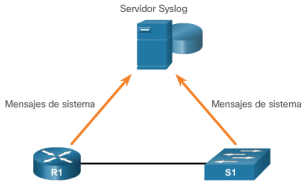
3.1.1. Introducción

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 es utilizar un protocolo denominado syslog. El término “syslog” se utiliza para describir un estándar. También se utiliza para describir el protocolo desarrollado para ese estándar. 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. Syslog usa el puerto UDP 514 para enviar mensajes de notificación de eventos a través de redes IP a recopiladores de mensajes de eventos, como se muestra en la ilustración.

Muchos dispositivos de red admiten syslog, incluidos routers, switches, servidores de aplicación, firewalls y otros dispositivos de red. 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:

- 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.



3.1.2. Nivel de Gravedad de Syslog

Los dispositivos de Cisco generan mensajes de syslog como resultado de los eventos de red. Cada mensaje de syslog contiene un nivel de gravedad

Cada nivel de syslog tiene su propio significado:

- **Nivel de advertencia 4 - Nivel de emergencia 0:** Estos mensajes son mensajes de error sobre desperfectos de software o hardware; indican que la funcionalidad del dispositivo está afectada. La gravedad del problema determina el nivel real de syslog que se aplica.

- **Nivel de notificación 5:** El nivel de notificaciones es para eventos normales, pero significativos. Por ejemplo: las transiciones para activar o desactivar interfaces y los mensajes para reiniciar el sistema se muestran en el nivel de notificaciones.

- **Nivel informativo 6:** Un mensaje informativo normal que no afecta la funcionalidad del dispositivo. Por ejemplo: cuando un dispositivo Cisco está arrancando, se podría ver el siguiente mensaje informativo: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License Agreement is accepted.

- **Nivel de depuración 7:** Este nivel indica que los mensajes son generados como salida a partir de la ejecución de diversos comandos debug (de depuración).

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.

3.1.3. Formato de Mensaje Syslog

De manera predeterminada, el formato de los mensajes de syslog en el software IOS de Cisco es el siguiente:

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

Por ejemplo, el resultado de ejemplo de un switch Cisco para un enlace EtherChannel que cambia al estado activo es el siguiente:

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

Aquí la instalación es LINK, y el nivel de gravedad es 3, con MNEMONIC UPDOWN.

Los mensajes más comunes son los de enlace activo y enlace inactivo, y los mensajes que produce un dispositivo cuando sale del modo de configuración. Si se configura el registro de ACL, el dispositivo genera mensajes de syslog cuando los paquetes coinciden con una condición de parámetros.

Campo	Explicación
seq no	Marca los mensajes de registro con un número de secuencia solamente si se configuró el comando de configuración global **`service sequence-numbers`**.
timestamp	Fecha y hora del mensaje o del evento, aparece solamente si se configuró el comando de configuración global **`service timestamps`**.
facility	La instalación a la que se refiere el mensaje.
severity	Código de un único digito entre 0 y 7 que indica la gravedad del mensaje.
MNEMONIC	Cadena de texto que describe el mensaje de forma exclusiva.
description	Cadena de texto que contiene información detallada sobre el evento que se informa.

4. TRABAJO PREPARATORIO

4.1. Revisar el marco teórico para la realización de la práctica.

5. EQUIPO Y MATERIALES

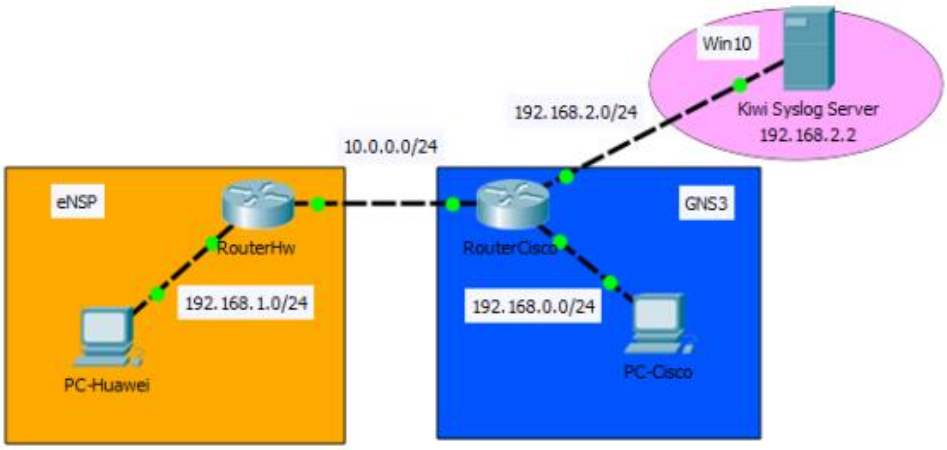
Materiales por grupo de trabajo.

- 3 PC (Putty / Hiperterminal / Kiwi Syslog Server)
- 1 Switch
- 1 Router
- Cables seriales, directos y cruzados

6. PROCEDIMIENTO

6.1. Configuración de SysLog.

En esta parte de la práctica se va monitorear los eventos dos routers con Kiwi Syslog Server. Para esto se va a tomar en cuenta el siguiente esquema.



Paso 1: Instalar Kiwi Syslog Server en una de las computadoras.

- Instale Kiwi Syslog Server.
- Configure la dirección IP 192.168.2.2 en el servidor.

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

- Configure la dirección IP correspondiente en cada una de las interfaces de RouterHw y RouterCisco.
- Configure RouterHw y RouterCisco. para que envíe los eventos registrados al servidor de Syslog.

RouterCisco (config)# logging 192.168.2.2

Paso 3: Completar la topología de la red

- Complete la topología inicial con las conexiones físicas necesarias.
- Configure las direcciones IP correspondientes en cada una de las computadoras.

Paso 4: Cambie el estado de las interfaces para crear registros de eventos.

- Configurar una interfaz loopback 0 en el RouterCisco y, luego, proceda a deshabilitarla.
- Apague las computadoras y vuelva a encenderlas.
- Examine los eventos mostrados en Kiwi Syslog Server.
- Revise las estadísticas Syslog en Kiwi Syslog Server

6.2. Realización de copias de respaldo de archivos de configuración en Packet Tracer

Paso 1: Establecer la conectividad al servidor TFTP

- Instale Pumpkin TFTP Server en una de las computadoras.
- Verifique la conectividad entre RouterCisco y la computadora configurada.

Paso 2: Realizar copias de seguridad de la configuración y del IOS en el servidor TFTP

- Cambie el nombre del host de RouterCisco a RTA-1.
- Guarde la configuración en la NVRAM.
- Copie la configuración al servidor TFTP usando el comando copy:

RTA-1# copy running-config tftp:

```
Address or name of remote host []? 172.16.1.2
Destination filename [RTA-1-confg]? <cr>
```

- Emita el comando para mostrar los archivos ubicados en la memoria flash.
- Copie el IOS que está en la memoria flash al servidor TFTP con el siguiente comando.

```
RTA-1# copy flash tftp:
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.16.1.2
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]? <cr>
```

7. INFORME

7.1. Presente la configuración realizada en el laboratorio.
7.2. Conclusiones y Recomendaciones
7.3. Bibliografía.

8. REFERENCIAS

CCNA R&S: Routing and Switching Essentials 6.0.

CCNA R&S: Connecting Networks 6.0

Elaborado por: Ing. Víctor H. Reyes C. – Técnico Docente

Revisado por: Ing. Pablo Hidalgo, MSc. - Responsable de la asignatura de Redes de Área Extendida.