Escuela Politécnica Nacional
Facultad de Ingeniería Eléctrica y Electrónica
Laboratorio de Redes de Área Extendida
http://detri.epn.edu.ec
Quito, Ecuador

PRÁCTICA N° 2

1. TEMA: ADMINISTRACIÓN Y MANTENIMIENTO DE DISPOSITIVOS

2. OBJETIVO:

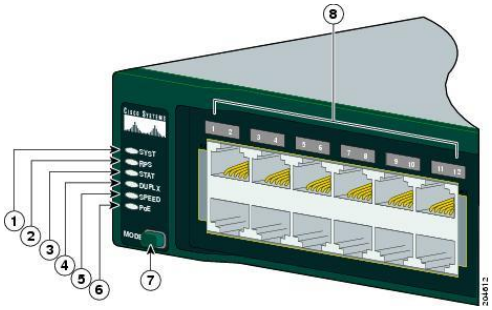
- Realizar el proceso de recuperación de passwords para switches y routers Cisco.
- Configurar syslog y enviar notificaciones a un servidor por medio de Packet Tracer.
- Crear archivos de respaldo de las configuraciones utilizando un servidor tftp.

3. RECUPERACIÓN DE PASSWORD EN SWITCHES CISCO

El procedimiento para recuperación de passwords en switches Cisco es el siguiente:

Paso 1. Conectar el computador al puerto de consola del equipo y abrir una ventana de HyperTerminal.

Paso2. Apagar al switch y volver a encenderlo mientras se mantiene presionado el botón "MODE".



1	SYST LED	5	Speed LED
2	RPS LED	6	PoE LED
3	Status LED	7	Mode button
4	Duplex LED	8	Port LEDs

Paso 3. Dejar de presionar el botón "MODE" (modo) una vez que se apaga el LED STAT. Luego de lo cual se debe presentar información similar a la siguiente.

```
C2950 Boot Loader (C2950-HBOOT-M) Version 12.1(11r)EA1, RELEASE
SOFTWARE (fc1)
Compiled Mon 22-Jul-02 18:57 by antonino
WS-C2950-24 starting...
Base ethernet MAC Address: 00:0a:b7:72:2b:40
Xmodem file system is available.
The system has been interrupted prior to initializing the flash files
system. The following commands will initialize the flash files system,
and finish loading the operating system software:
```

Paso 4: Para inicializar el sistema de archivos y terminar de cargar el sistema operativo se debe introducir los siguientes comandos:

- **flash_init**
- **load_helper**
- **dir flash:**

Paso 5: Se debe renombrar el archivo de configuración, ya que este archivo es el que contiene la definición de la contraseña

- rename flash:/config.text flash:/config.old

Paso 6: Reiniciar el sistema utilizando el comando boot

- Continue with the configuration dialog? [yes/no]: N

Paso 7: Cuando se termine la reinicialización, en modo EXEC privilegiado, cambie el nombre del archivo de configuración al nombre original.

- rename flash:/config.old flash:/config.text.

Paso 8: Copiar el archivo de configuración a la memoria

- Switch #copy flash:config.text system:running-config
  Source filename [config.text]?[enter]
  Destination filename [running-config][enter]

Paso 9: Cambiar las contraseñas

```
Switch#configure terminal
Switch(config)#no enable secret
Switch(config)#enable password Cisco
Switch(config)#enable secret class
Switch(config)#line console 0
Switch(config-line)#password cisco
Switch(config-line)#exit
Switch(config)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#exit
Switch(config)#exit
Switch#copy running-config startup-config

Destination filename [startup-config]?[enter]
Building configuration...
[OK]
Switch#
```

Paso 10: Apagar y encender el switch para verificar que las contraseñas son funcionales.

4. PROCEDIMIENTO PARA RECUPERACIÓN DE PASSWORD EN UN ROUTER CISCO

Paso1: Interrumpir la secuencia dearranque (dentrode los 60 segundos iniciales de arranque) con Crtl-Break, para entrar al modo ROM monitor.

Paso 2: Cambiar el registro de configuración (según modelo):

- Cisco ISR/2600: con el comando:
  rommon 1> config-register 0×2142
  rommon 1 >reset
  o
  rommon 1> confreg 0×2142
  rommon 1 >reset

De esta forma, arrancará sin usar el archivostartup-config, por lo que preguntará si se quiere entrar en modo setup, a lo que se debe responder que NO y se ingresará en el modo privilegiado.

Paso 3: Ejecutar el comando

- copy startup-config running-config

Paso 4: Cambiar el password de modo privilegiado

Paso 5: Dejar el registro de configuración del router como estaba inicialmente.

- hostname(config)#config-register0x2102
  hostname# reload

Paso 6: Ejecutar el comando

- copy running-config startup-config

5. SYSLOG

a. 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.

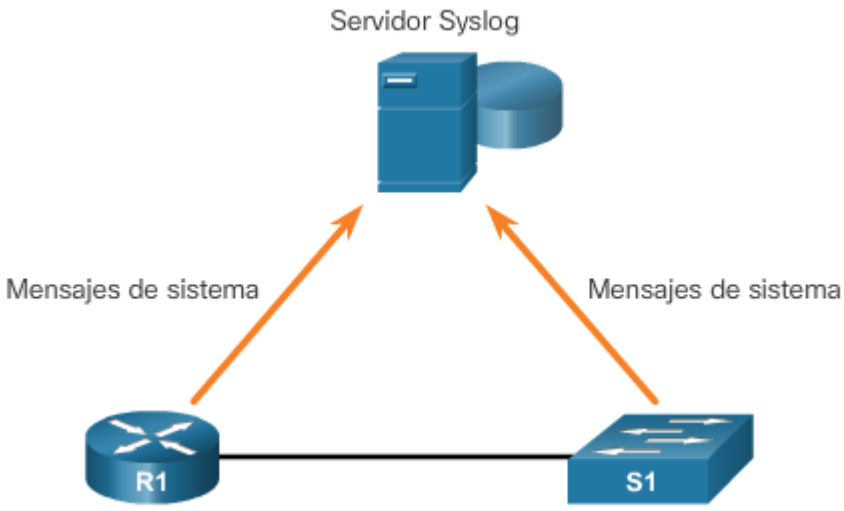
El método más común para acceder a los mensajes del sistema es utilizar un protocolo denominado syslog.

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



b. 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.

c. 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 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.

6. PRÁCTICA

a. Recuperación de Password

- Configurar cada switch y router con un nombre
- Configurar contraseñas para garantizar que el acceso a la CLI sea seguro.
- Realizar proceso de recuperación de password de los equipos.

b. Configuración de SysLog en Packet Tracer

Paso 1. Agregar un servidor y habilitar el servicio de syslog

- Agregue un servidor de la sección "End Devices" al área de trabajo y asígnele el nombre Syslog.
- Haga clic en el Servidor, luego en la ficha Services.
- Active el servicio Syslog y mueva la ventana para poder monitorear la actividad.

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

- Agregue un router de la sección "Routers" al área de trabajo y asígnele el nombre R1.
- Configure R1 para que envíe los eventos registrados al servidor de Syslog.

  R1(config)# logging 10.0.1.254
- Agregue un switches de la sección "Switchs" al área de trabajo y asígnele el nombre S1.

Paso 3. Completar la topología de la red

- Agregue una PC al área de trabajo y asígnele el nombre PC1
- Interconecte el S1 con PC1, S1 con R1, S1 con Syslog, R1 con Syslog por medio de las conexiones adecuadas,
- Establezca el direccionamiento necesario para tener conectividad total entre los dispositivos.

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

- Configurar una interfaz loopback 0 en el R1 y, luego, proceda a deshabilitarla.
- Apague PC1. Vuelva a encenderla.
- Examine los eventos de Syslog.
- Vea los eventos de Syslog.

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

Paso 1: Establecer la conectividad al servidor TFTP

- Agregue un servidor de la sección "End Devices" al área de trabajo y asígnele el nombre "Servidor TFTP".
- Haga clic en el Servidor, luego en la ficha Services.
- Active el servicio TFTP.
- Agregue un router de la sección "Routers" al área de trabajo y asígnele el nombre R1.
- Asigne el direccionamiento necesario para conectar R1 con el "Servidor TFTP".
- Realice pruebas de conectividad.

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

- Cambie el nombre del host de R1 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

Presente la configuración realizada en el laboratorio y las capturas de pantalla de los comandos de visualización, adicionalmente se deben presentar las conclusiones y recomendaciones correspondientes a la práctica.

8. REFERENCIAS

CCNA R&S: Routing and Switching Essentials 6.0

Realizado por: Ing. Pablo Hidalgo., M.Sc.
Ing. Víctor Reyes
Aprobado por: Ing. Pablo Hidalgo., M.Sc.