

DATOS DE LA ACTIVIDAD							
No. de Actividad:	2.1	Actividad	Inspección y Administración				
Unidad:	2: Configuración de seguridad en firewall, Switches, Routers y Access point						
Carrera:	Tgo. en Desarrollo de Software						
Materia	SEGURIDAD EN ITI					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	Centro de Enseñanza Técnica Industrial plantel Colomos						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	16/04/2021
Compet. Genéricas		4.1, 4.5, 5.2,		Compet. Profesional		CP1-1	

1. Objetivo(s) de la actividad

- Identificar los conceptos de inspección y administración en el ámbito de seguridad informática.

2. Introducción

Conocer los conceptos de inspección y administración en el ámbito de seguridad informática, es parte de la configuración integral de seguridad en un sistema informático.

3. Instrucciones (Descripción) de la actividad

Contestar las siguientes preguntas en el documento de WORD:

1. ¿Qué es un Privilegio (en redes de cómputo)?
2. ¿Como hacer Respaldo del Sistema Operativo y archivo de configuración en un Router CISCO? (Describir el proceso y en un Router CISCO y los comandos a utilizar)
3. ¿ Como se utilizan los protocolos SNMP y NTP para monitorización de la red?
4. Entrar a <https://www.netacad.com/> en el curso de Cybersecurity Essentials y realizar la actividad de 6.2.4.4 Packet Tracer: Recuperabilidad del router y switch (agregar en el documento de WORD la impresión de pantalla completa del Packet Tracer al 100%) y subir el archivo PKT en la actividad.
5. Consultar: el PDF : CISCO security. Consultar: <https://www.netacad.com/> los siguientes temas :
 - 7.1.3.1 Control de acceso a los archivos
 - 7.3.1.4 Servicios de routing y red
 - 6.2.4.3 Recuperabilidad del IOS

6. Usar el archivo de ejemplo de actividades, completar todos los datos del encabezado identificando si es Actividad, Investigación o Práctica, así como las competencias a desarrollar para esta actividad.
7. Subir el archivo terminado, no se te olvide, la reflexión, agregar la bibliografía en formato APA y dar clic para marcar como entregada la actividad.

4. Desarrollo

- ¿Qué es un Privilegio (en redes de cómputo)?

En informática, el privilegio se define como la delegación de autoridad para realizar funciones relevantes para la seguridad en un sistema informático. Un privilegio permite a un usuario realizar una acción con consecuencias para la seguridad. Los ejemplos de varios privilegios incluyen la capacidad de crear un nuevo usuario, instalar software o cambiar las funciones del kernel.

- ¿Como hacer Respaldo del Sistema Operativo y archivo de configuración en un router CISCO? (Describir el proceso y en un router CISCO y los comandos a utilizar).

Copia de un OS de un router a otro actuando como servidor TFTP

- I. Controle el tamaño de la imagen en el Router1 con el comando **show flash**

```
Router1#show flash
System flash directory:
File Length Name/status
1 15694836 /c2500-js-1.122-10b

!--- Cisco IOS image file to be copied

[15694900 bytes used, 1082316 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
```

- II. Controle el tamaño de la imagen en el Router2 con el comando **show flash** a fin de verificar si el Router2 tiene espacio suficiente disponible para que el archivo de imagen del sistema sea copiado.

```
Router2#show flash

System flash directory:
File Length Name/status

1 11173264 c2500-jos56i-1.120-9.bin
[11173328 bytes used, 5603888 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
```

Nota: Si hay suficiente espacio para copiar el archivo de imagen del sistema, se puede conservar el original y copiar el nuevo archivo en el espacio de memoria adicional. Si no hay espacio suficiente disponible, como en este caso, el archivo existente de la memoria Flash se borra mientras se descarga uno nuevo. Es recomendable realizar una copia de seguridad de la imagen del sistema existente en el servidor TFTP usando el comando **copy flash tftp**.

III. Configure el Router1 como el servidor TFTP usando el comando **configure terminal**.

```
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#tftp-server ?
 bootflash:  Allow URL file TFTP load requests
 disk0:      Allow URL file TFTP load requests
 disk1:      Allow URL file TFTP load requests
 flash:      Allow URL file TFTP load requests
 flh:        Allow URL file TFTP load requests
 lex:        Allow URL file TFTP load requests
 null:       Allow URL file TFTP load requests
 nvram:      Allow URL file TFTP load requests
 slot0:      Allow URL file TFTP load requests
 slot1:      Allow URL file TFTP load requests
 system:     Allow URL file TFTP load requests
```

IV. Cuando se configura el servidor TFTP, descargue la imagen especificada del Router1 en el Router2 usando el comando **copy tftp flash**.

```
Router2#copy tftp flash
**** NOTICE ****

Flash load helper v1.0
This process will accept the copy options and then terminate
the current system image to use the ROM based image for the copy.
Routing functionality will not be available during that time.
If you are logged in via telnet, this connection will terminate.
Users with console access can see the results of the copy operation.
----
Proceed? [confirm]
Address or name of remote host []? 10.10.10.1

!--- Enter the IP address of the TFTP Server

Source filename []? /c2500-js-1.122-10b
```

V. Verifique la memoria Flash para la nueva imagen del sistema en el Router 2.

```

Router2#show flash
System flash directory:
File Length Name/status
1 15694836 /c2500-js-1.122-10b

!--- Cisco IOS image file has been copied

[15694900 bytes used, 1082316 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)

```

Nota: El router se recarga solamente para los sistemas que funcionan desde Flash.

Configuración utilizando un servidor FTP:

- I. En el mensaje Router>, ejecute el comando **enable** y suministre la contraseña requerida cuando se la solicite. El prompt cambia al Router#, lo que indica que el router ahora está en el modo privilegiado.
- II. Configure la contraseña y el nombre de usuario FTP.

```

CE_2#config terminal
CE_2(config)#ip ftp username cisco
CE_2(config)#ip ftp password cisco123
CE_2(config)#end
CE_2#

```

- III. Copie la configuración al servidor FTP.

```

CE_2#copy running-config ftp:
Address or name of remote host []? 10.66.64.10
Destination filename [ce_2-config]? backup_cfg_for_router
Writing backup_cfg_for_router !
1030 bytes copied in 3.341 secs (308 bytes/sec)
CE_2#

```

- IV. Abra el archivo de configuración con un editor de texto. Busque y borre todas las líneas que comiencen con "AAA". (Este paso es para quitar cualquier comando de seguridad que pueda bloquearlo fuera del router.)
- V. Copie el archivo de configuración desde el servidor FTP a un nuevo router en el modo privilegiado (habilitado) que tiene una configuración básica.

```

Router#copy ftp: running-config
Address or name of remote host [10.66.64.10]?
Source filename [backup_cfg_for_router]?
Destination filename [running-config]?
Accessing ftp://10.66.64.10/backup_cfg_for_router...
Loading backup_cfg_for_router !
[OK - 1030/4096 bytes]
1030 bytes copied in 13.213 secs (78 bytes/sec)
CE_2#

```

- ¿Como se utilizan los protocolos SNMP y NTP para monitorización de la red?

SNMP

El protocolo SNMP tiene dos formas de funcionar: polling y traps. El polling consiste en lanzar consultas remotas de forma activa o a demanda, realizando una operación síncrona de consulta. Los traps son mensajes que envían los dispositivos SNMP a una dirección configurada basándose en cambios o eventos, de forma asíncrona. Al configurar un sistema de monitorización SNMP utilizaremos ambos modos de trabajo del protocolo. Además, este protocolo presenta tres versiones, siendo la 1 (SNMPv1) y la 2 (SNMPv2) las más utilizadas en entornos profesionales; la versión 3 (SNMPv3) implementa algunas opciones adicionales de seguridad, pero su uso no se ha popularizado.

Polling

Este protocolo funciona lanzando un chequeo contra una dirección IP, pero requiere un parámetro particular: la comunidad SNMP. Esta consiste en una cadena alfanumérica empleada para autorizar la operación, añadiendo una barrera de seguridad. Cuando lanzamos un chequeo SNMP contra un dispositivo compatible, obtenemos un listado con una gran cantidad de información, de primeras difícil de interpretar:

```
# snmpwalk -v 1 -c public 192.168.50.14
```

```

[root@inna ~]# snmpwalk -v1 -c public 192.168.50.14
iso.3.6.1.2.1.1.1.0 = STRING: "Linux TS-469 4.1.4"
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.2.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB for Message Processing and Dispatching."

```

Cada una de las líneas devueltas por el snmpwalk tiene un OID o código de identificación de objeto, y corresponde a un dato determinado del dispositivo. Para poder entender mejor a qué corresponden los valores devueltos por el chequeo SNMP, podemos instalar las MIBs correspondientes del fabricante en el sistema desde donde estemos realizando el chequeo. Estas MIBs, son librerías que traducen estas cadenas numéricas a un formato humano

legible, permitiendo interpretar la naturaleza de la información. En el siguiente caso la información devuelta por un chequeo SNMP cuando las MIBs correspondientes están instaladas:

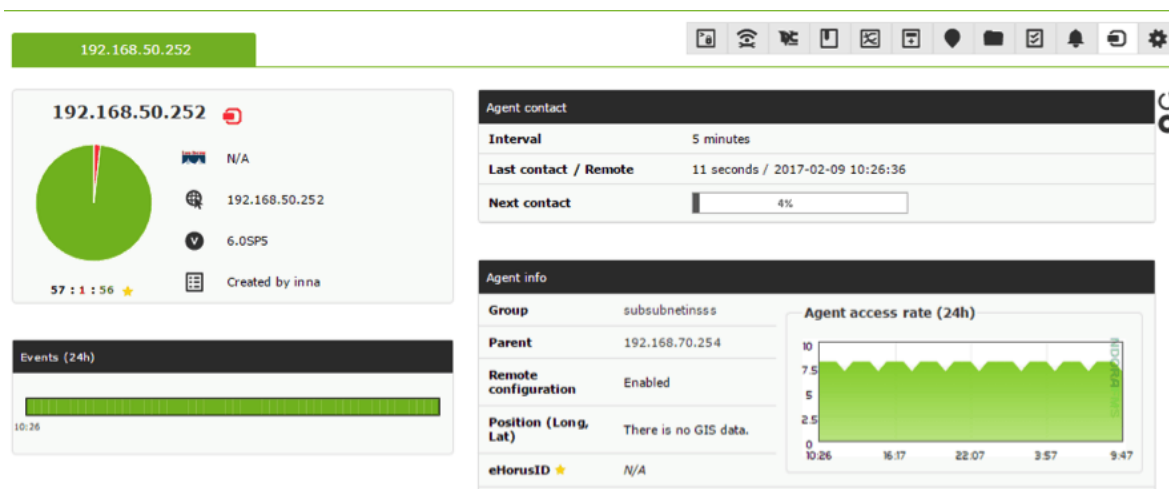
```
[root@localhost ~]# snmpwalk -v 1 -c public 192.168.50.14
SNMPv2-MIB::sysDescr.0 = STRING: Linux TS-469 4.1.4
SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDMIBObjects.3.1.1
SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
```

Además, existen sitios web en los que podemos consultar cada uno de estos OIDs en caso de duda. En caso de que conozcamos los OIDs que queremos monitorizar podremos ejecutar la consulta indicando el código alfanumérico tras la dirección IP en cuestión, de este modo:

```
# snmpwalk -v 1 -c public 192.168.1.50 IF-MIB::ifPhysAddress.2
```

```
[root@localhost ~]# snmpwalk -v 1 -c public 192.168.50.14 IF-MIB::ifPhysAddress.2
IF-MIB::ifPhysAddress.2 = STRING: 0:8:9b:e4:8b:aa
```

De este modo la salida solo mostraría los valores para el objeto SNMP consultado, por lo que si disponemos de alguna herramienta de monitorización podremos reflejar esta información en los diferentes chequeos. Un ejemplo de una monitorización SNMP básica de algunos dispositivos con Pandora FMS; el resultado se verá del siguiente modo:



Alertas SNMP polling

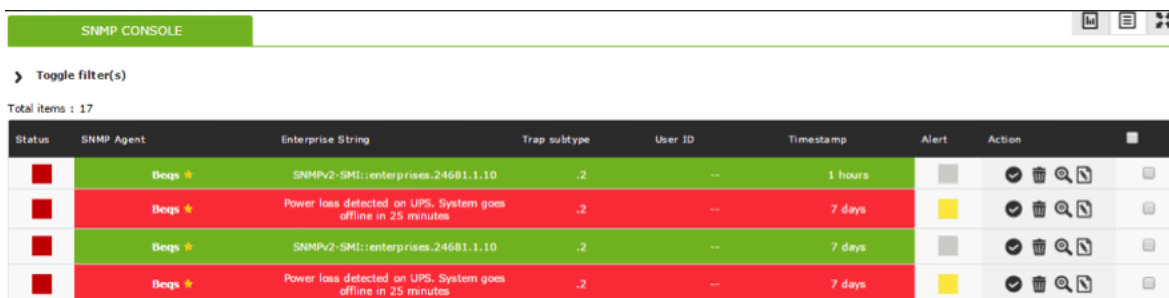
Una vez estemos recogiendo información en módulos mediante SNMP polling podremos crear alertas en Pandora FMS para estos módulos, ejecutando acciones de forma proactiva en función de los umbrales que configuremos en nuestros chequeos. El funcionamiento es el mismo a las alertas para cualquier otro módulo en Pandora FMS.

Monitorización de SNMP Traps

Para la monitorización SNMP mediante traps necesitaremos, en primer lugar, configurar nuestros dispositivos para enviar los trap cuando se cumplan las circunstancias especificadas y, en segundo lugar, una herramienta que pueda recoger los trap SNMP recibidos, bien una máquina con los servicios necesarios o bien un software de monitorización. La configuración de los dispositivos SNMP para el envío de traps se realiza de forma diferente dependiendo del fabricante y el aparato, habitualmente desde una interfaz de gestión a la que se puede acceder a través de un navegador y su dirección IP.

La recepción de traps puede hacerse en Linux con ayuda del demonio snmptrapd. Es posible realizar esto con Pandora FMS para la recepción y procesamiento de los traps SNMP. Si ya tenemos instalado un servidor de Pandora FMS no es necesario hacer nuevas dependencias, pero hay que habilitar la recepción de traps SNMP; para ello, el parámetro snmpconsole en el fichero pandora_server.conf deber habilitarse como "snmpconsole 1".

Una vez habilitada la consola de traps SNMP, Pandora FMS será capaz de recibirlos y procesarlos, mostrándose en la sección correspondiente:



The screenshot shows the 'SNMP CONSOLE' section of the Pandora FMS interface. It features a table with 17 items. The table columns are: Status, SNMP Agent, Enterprise String, Trap subtype, User ID, Timestamp, Alert, and Action. The first four rows are visible, showing traps from 'Beqs' and 'Power loss detected on UPS. System goes offline in 25 minutes'.

Status	SNMP Agent	Enterprise String	Trap subtype	User ID	Timestamp	Alert	Action
Red square	Beqs	SNMPV2-SMI::enterprises.24681.1.10	.2	--	1 hours	Grey square	Icons for actions
Red square	Beqs	Power loss detected on UPS. System goes offline in 25 minutes	.2	--	7 days	Yellow square	Icons for actions
Red square	Beqs	SNMPV2-SMI::enterprises.24681.1.10	.2	--	7 days	Grey square	Icons for actions
Red square	Beqs	Power loss detected on UPS. System goes offline in 25 minutes	.2	--	7 days	Yellow square	Icons for actions

Una vez habilitada la consola de traps SNMP, Pandora FMS será capaz de recibirlos y procesarlos, mostrándose en la sección correspondiente:

Alertas SNMP Trap

También podremos configurar alertas para la monitorización SNMP mediante traps que preparemos. En este caso el funcionamiento no va a ser como para cualquier otro módulo, como era para los módulos de SNMP polling, sino que se basará en reglas de filtrado. Mediante estas reglas podemos identificar traps provenientes de algún dispositivo en particular, filtrar por el contenido del trap, OID, cadena de texto en su contenido, etc.



The screenshot shows the 'SNMP CONSOLE > ALERT OVERVIEW' section of the Pandora FMS interface. It features a table with 4 items. The table columns are: P., Alert action, SNMP Agent, Enterprise String, Custom Value/Enterprise String, Description, TF., Last fired, and Action. The first four rows are visible, showing alert rules for 'Pandora FMS Event', 'Mail to XXX', 'Pandora FMS Event', and 'Alarma sónica'.

P.	Alert action	SNMP Agent	Enterprise String	Custom Value/Enterprise String	Description	TF.	Last fired	Action
0	Pandora FMS Event		.1.3.6.1.4.1.2789.*	.*		1	5 months	Icons for actions
0	Mail to XXX		1.2.3.4.5		prueba	0	Never	Icons for actions
0	Pandora FMS Event		.1.3.6.1.4.1.2789.*	.*		1	5 months	Icons for actions
0	Alarma sónica		*			0	Never	Icons for actions

NTP

NTP comunicación entre dos dispositivos diferentes consta de solicitudes de tiempo NTP y consultas de control de NTP. Una petición de hora NTP es una solicitud de un cliente NTP para tiempo de sincronización desde un servidor NTP. Consultas de control de NTP son mensajes de comunicación para la información de configuración.

NTP servidores

Son dispositivos de red que gestionan un servicio NTP. Estos dispositivos están configurados para proporcionar información en tiempo a los clientes que utilizan NTP Protocolo de tiempo de red. Servidores NTP sólo suministrar información en tiempo a los clientes autorizados NTP y no recibirán la información de sincronización de tiempo de dispositivos no autorizados. La configuración más común para internet NTP es el modelo cliente / servidor. En este modo, las solicitudes se envían por un cliente a un servidor, con el cliente espera una respuesta en cuestión de milisegundos, a menos que la fuente de tiempo no está disponible o muy ocupado.

El proceso ve un cliente distribuir un mensaje de protocolo de hora de red a uno o más servidores y acciones de las respuestas que se recibieron. El servidor entonces intercambiar direcciones y puertos, sobrescribir determinados campos en el mensaje, vuelva a calcular la suma de comprobación antes de devolver el mensaje de inmediato. El mensaje devuelto permite al cliente para calcular la hora del servidor, en relación con la hora local, y alterar un reloj en consecuencia. Además, el mensaje contiene información para calcular la precisión de cronometraje esperado y fiabilidad, además de elegir el mejor servidor. Es claro que el uso de este protocolo nos permite realizar monitoreo mediante solicitudes de tiempo y poseer registro de las consultas y peticiones desde un servidor central de la red.

¿Cómo monitorear servidores NTP?

Se requiere de una aplicación que facilite el análisis de los datos NTP arrojados por ejemplo SNMP/MRTG/RRDtool. Esta herramienta además de monitorear las cosas genéricas del sistema operativo Linux, como la CPU, la memoria, el promedio de carga y el ancho de banda de la red, tiene al menos dos métodos diferentes para obtener algunos datos de telemetría del servicio NTP a su estación de monitoreo:

- Llamar a ntpq desde la estación de monitoreo para obtener algunos datos del servidor NTP remoto. Debe usar la opción "restringir" en el servidor NTP dentro de ntp.conf para permitir que la estación de monitoreo consulte datos, como restringir 2003: de: 2016: 120 :: a01: 80 en mi caso. El servidor de monitoreo puede usar ntpq con un host remoto como ntpq -c rv ntp1.weberlab.de. De hecho, estos son paquetes NTP normales en el cable, pero con el modo NTP = 6, llamado "mensaje de control". Consulte mi entrada de blog "Captura de paquetes: Protocolo de tiempo de red".
- Usar algunos scripts en el propio servidor NTP para entregar datos a otros protocolos, como SNMP. Por ejemplo, estoy usando la opción "extend-sh" dentro de la configuración snmpd.conf en el servidor NTP para que el servidor de monitoreo

consulte los OID SNMP normales para obtener cierta información relacionada con NTP.

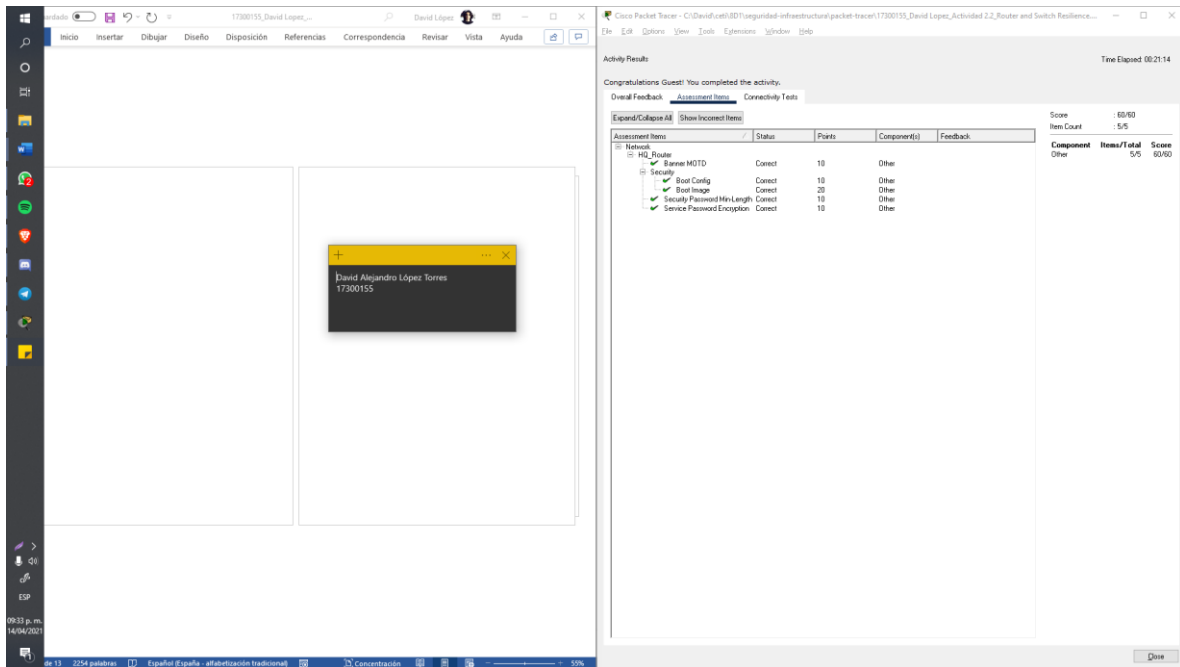
En cualquier caso, debe usar algunas herramientas para grep 'n sed a través de la salida para extraer exactamente los valores que le interesan. Además, debe ingresar esos valores en su herramienta de monitoreo. Estoy mostrando algunos fragmentos de configuración de MRTG junto con gráficos RRDtool.

Lista de Comandos

Comando	Descripción
bootflash:	Copiar en bootflash: sistema de archivos
disk0:	Copiar en disk0: sistema de archivos
disk1:	Copiar en disk1: sistema de archivos
flash:	Copiar en Flash: sistema de archivos
flh:	Copiar en flh: sistema de archivos
ftp:	Copiar en ftp: sistema de archivos
lex:	Copiar en lex: sistema de archivos
null:	Copiar en null: sistema de archivos
nvram:	Copiar en nvram: sistema de archivos
rcp:	Copiar en rcp: sistema de archivos
running-config:	Actualizar (fusionar con) la configuración actual del sistema
slot0:	Copiar en slot0: sistema de archivos
slot1:	Copiar en slot1: sistema de archivos
startup-config:	Copiar en la configuración de inicio
sistem:	Copiar en el sistem: sistema de archivos
tftp:	Copiar en tftp: sistema de archivos

➤ Actividad de Packet Tracer

Actividad completa (100%)



5. Reflexión

El uso de los protocolos SMTP y NTP son de gran importancia al colaborar de manera conjunta para generar un monitoreo completo de las acciones realizadas a través de la red. Implementar estos protocolos brinda un grado extra de confiabilidad a la red y favorece a la agestión y presentación de la información que se transmite por medio de la red, dando énfasis en la información que es crucial para generar un reporte de estado. La implementación de la recuperabilidad de dispositivos en el simulador de Packet Tracer nos refleja la importancia que tiene proteger y respaldar la información, y nos da una perspectiva para su ejecución en la vida práctica.

6. Referencias

- Anónimo. (2014). Cómo copiar una imagen del sistema de un dispositivo a otro. Recuperado el 14/04/2021 de:
https://www.cisco.com/c/es_mx/support/docs/routers/2500-series-routers/15092-copyimage.html.
- Anónimo. (2010). Monitorización SNMP: claves para aprender a usar el Protocolo Simple de Administración de Red. Recuperado el 14/04/2021.
<https://pandorafms.com/blog/es/monitorizacion-snmpp/>