Administración de redes

Prof. Andrea Mesa Múnera

Switching

AGENDA

1. Configuración y administración de un switch

Configuración de la seguridad del Switch

Configuración de opciones de contraseña

En los switch es de gran importancia configurar el nombre del switch, las contraseñas para el acceso a la consola, al terminal virtual y al modo EXEC.

Además es importante tener en cuenta cómo encriptar y recuperar contraseñas en este tipo de dispositivos.

De [1]

Configuración de la seguridad del Switch

Configuración de opciones de contraseña

La seguridad de los switches comienza con la protección de ellos contra el acceso no autorizado.

Se pueden realizar todas las opciones de configuración desde la consola.

Para acceder a la consola, se necesita tener acceso físico local al dispositivo. Si no se asegura el puerto de consola de forma adecuada, usuarios malintencionados podrían comprometer la configuración del switch.

De [1]

Configuración de la seguridad del Switch

Configuración del acceso a la consola

Protección de la consola

Utilice el comando ***line console 0*** para conmutar del modo de configuración global al modo de configuración de línea para la consola 0, que es el puerto de consola de los switches Cisco.

La indicación cambia a ***(config-line)#***, señalando que ahora el switch está en el modo de configuración de línea.

De [1]

Configuración de la seguridad del Switch

Configuración del acceso a la consola

Protección de la consola

Para proteger el puerto de consola contra el acceso no autorizado, establezca una contraseña utilizando el comando de modo de configuración de línea ***password <contraseña>***

Para asegurar que el usuario que desee tener acceso al puerto de consola deba introducir la contraseña, utilice el comando ***login***

De [1]

Configuración de la seguridad del Switch

Configuración del acceso remoto al dispositivo

Protección de los puertos vty

Es posible llevar a cabo todas las opciones de configuración mediante los puertos de terminal vty. No se necesita acceso físico al switch para obtener acceso a los puertos vty. Por ello, es muy importante que estén protegidos. Cualquier usuario con acceso de red al switch puede establecer una conexión remota de terminal vty.

La contraseña de los puertos vty debe establecerse desde el modo de configuración de línea.

De [1]

Configuración de la seguridad del Switch

Configuración del acceso remoto al dispositivo

Protección de los puertos vty

Un switch de Cisco puede contar con varios puertos vty disponibles. Varios puertos permiten que más de un administrador pueda conectarse y administrar el switch.

Para proteger todas las líneas vty, asegúrese de que se establezca una contraseña y que el inicio de sesión sea obligatorio en todas las líneas. La falta de protección en algunas líneas compromete la seguridad y permite el acceso no autorizado al switch.

De [1]

Configuración de la seguridad del Switch

Configuración del acceso remoto al dispositivo

Protección de los puertos vty

Utilice el comando ***line vty 0 4*** para cambiar del modo de configuración global al modo de configuración de línea para las líneas vty de 0 a 4.

Nota: Si el switch tiene más líneas vty disponibles, ajuste el intervalo para proteger a todas ellas. Por ejemplo, el Cisco 2960 tiene disponibles desde la línea 0 hasta la 15.

De [1]

Configuración de la seguridad del Switch

Eliminación de la contraseña de consola o de la contraseña vty

Si necesita eliminar la contraseña y la solicitud de ingreso de contraseña al iniciar sesión, siga los siguientes pasos:

1. Cambie de modo EXEC privilegiado a modo de configuración global. Ingrese el comando ***configure terminal***
2. Cambie del modo de configuración global al modo de configuración de línea (la que desee eliminar – consola o vty)
3. Elimine la contraseña de la línea de la consola o de las líneas vty mediante el comando ***no password***

   Precaución: Para vty, si no se ha establecido ninguna contraseña y el inicio de sesión aún se encuentra habilitado, no se podrá tener acceso a las líneas vty.
4. Elimine la solicitud de ingreso de contraseña al iniciar sesión en la consola o en las líneas vty mediante el comando ***no login***
5. Salga del modo de configuración de línea y regrese al modo EXEC privilegiado mediante el comando ***end***

De [1]

Configuración de la seguridad del Switch

Configuración de las contraseñas para el modo EXEC

El Modo EXEC privilegiado permite a cualquier usuario que habilite ese modo en un switch de Cisco configurar cualquier opción disponible en el switch.

También puede ver todos los parámetros de la configuración en curso del switch e incluso algunas de las contraseñas encriptadas.

De [1]

Configuración de la seguridad del Switch

Configuración de las contraseñas para el modo EXEC

El comando de configuración global ***enable password*** permite especificar una contraseña para restringir el acceso al modo EXEC privilegiado.

Sin embargo, una desventaja del comando ***enable password*** es que almacena la contraseña en texto legible en la configuración de inicio y en la configuración en ejecución.

De [1]

Configuración de la seguridad del Switch

Configuración de las contraseñas para el modo EXEC

Se puede asignar una forma encriptada de la contraseña de enable, llamada contraseña secreta de enable, ingresando el comando ***enable secret*** con la contraseña deseada en la solicitud del modo de configuración global.

De [1]

Configuración de la seguridad del Switch

Configuración de las contraseñas para el modo EXEC

Eliminación de la contraseña del modo EXEC

Si desea eliminar la solicitud de contraseña para obtener acceso al modo EXEC privilegiado, puede utilizar los comandos ***no enable password*** y ***no enable secret*** desde el modo de configuración global

De [1]

Configuración de la seguridad del Switch

Configuración de contraseñas encriptadas

Cuando se configuran contraseñas en la CLI del IOS, todas ellas, excepto la contraseña secreta de enable, se almacenan de manera predeterminada en formato de texto sin cifrar dentro de la configuración de inicio y de la configuración en ejecución.

El comando del IOS ***service password-encryption*** habilita la encriptación de la contraseña de servicio.

De [1]

Configuración de la seguridad del Switch

Configuración de contraseñas encriptadas

Si desea eliminar el requisito de almacenar todas las contraseñas del sistema en formato encriptado, ingrese el comando ***no service password-encryption*** desde el modo de configuración global.

La eliminación de la característica de encriptación de contraseñas no vuelve a convertir las contraseñas ya encriptadas en formato de texto legible. No obstante, todas las contraseñas que se configuren de allí en adelante se almacenarán en formato de texto legible.

De [1]

Mensajes de inicio de sesión

Configurar un titulo de inicio de sesión

El conjunto de comandos IOS de Cisco incluye una característica que permite configurar los mensajes que cualquier persona puede ver cuando inicia sesión en el switch.

Estos mensajes se llaman mensajes de inicio de sesión y mensajes del día (MOTD).

Para eliminar el mensaje MOTD, ingrese el formato ***no*** de este comando en el modo de configuración global, por ejemplo, S1(config)#no banner login

De [1]

Mensajes de inicio de sesión

Configurar un titulo de inicio de sesión

El usuario puede definir un mensaje personalizado para que se muestre antes de los avisos de inicio de sesión del nombre de usuario y la contraseña utilizando el comando ***banner login*** en el modo de configuración global.

Coloque el texto del mensaje entre comillas o utilizando un delimitador diferente a cualquier carácter que aparece en la cadena de MOTD.

De [1]

Mensajes de inicio de sesión

Configurar un titulo de MOTD

El mensaje MOTD se muestra en todos los terminales conectados en el inicio de sesión y es útil para enviar mensajes que afectan a todos los usuarios de la red (como desconexiones inminentes del sistema).

Si se configura, el mensaje MOTD se muestra antes que el mensaje de inicio de sesión.

De [1]

Mensajes de inicio de sesión

Configurar un titulo de MOTD

Defina el mensaje MOTD utilizando el comando ***banner motd*** en el modo de configuración global. Coloque el texto del mensaje entre comillas.

Para eliminar el mensaje de inicio de sesión, ingrese el formato ***no*** de este comando en el modo de configuración global, por ejemplo, S1(config)#no banner motd.

De [1]

UNIVERSIDAD EIA
Ser, Saber y Servir
Con Acreditación Institucional

REFERENCIAS

[1] (CCNA, 2008)

[2] (CCNA EXPLORATION, 2010)