Capítulo 3
Gestionar activos y la alta disponibilidad

1. Gestionar switches y routers

1.1 Herramientas e interfaces de administración

1.1.1 Interfaces CLI

Al elegir un equipo de red, en particular un *router* o switch, se plantea la cuestión de la gestión del equipo: ¿es gestionable? En otras palabras, ¿puede configurarse y adaptarse a la red para la que está destinado?

Los equipos no gestionables suelen ser vendidos a bajo coste por los fabricantes y, a medida que se asciende en la gama, aparece una interfaz de gestión en el equipo. Los equipos que se venden como «equipos adaptados para uso empresarial» deben ser gestionables, aunque no siempre es así.

El modo más básico, pero a veces el más eficaz, de administración de un dispositivo de red es a través de una interfaz minimalista que permita introducir líneas de comandos, conocida como CLI (*Command Line Interface*; interfaz de línea de comandos). Estos comandos CLI dependen del dispositivo en cuestión y del fabricante. Cada fabricante define e implementa sus propios comandos; recuerde que la mayoría de los sistemas operativos para elementos de red activos están patentados.

Por ejemplo, Cisco lleva desarrollando un sistema operativo llamado IOS (*Internetwork Operating System*; Sistema operativo de interconexión de redes) desde su creación a principios de los 80. Este IOS ha hecho que el fabricante tenga éxito en el mundo de las redes.

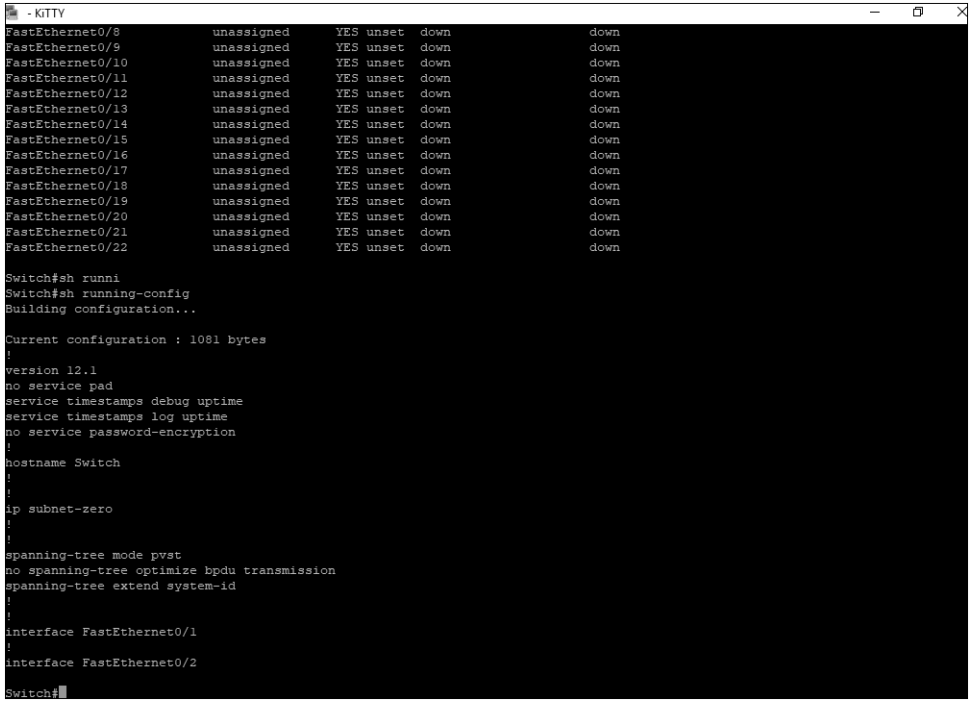
Se puede acceder a la CLI a través de la red IP, es decir, desde cualquier estación de trabajo conectada a la LAN o a la WAN mediante un protocolo como TELNET y su homólogo SSH, mucho más seguro. Estos dos protocolos también se utilizan para la gestión de servidores y permiten introducir comandos de forma sencilla en un dispositivo remoto; como si estuviera conectado físicamente a él.

Así es como, por ejemplo, un ISP puede verificar la conexión a Internet de uno de sus clientes: conectándose a distancia al equipo y, más concretamente, utilizando una utilidad en modo cliente que usa el protocolo SSH en la dirección IP del *router* del cliente.

La pregunta que tendrá que hacerse cuando configure un equipo por primera vez es: ¿cómo puedo conectarme a la dirección IP del equipo si no la tiene, dado que nunca ha sido configurado?

En este caso, o bien el fabricante preconfigura el equipo para asignarle una IP predefinida de fábrica, que estará documentada, o bien se proporciona un mecanismo para que el equipo recupere la configuración de un servidor DHCP en cuanto una de sus interfaces se conecte a la red. Este es el caso de la mayoría de los equipos.

Sin embargo, algunos fabricantes (como Cisco) no proporcionan una configuración predefinida, por lo que deberá conectarse físicamente al equipo cuando lo configure por primera vez. Esto se hace a través de una conexión RS232 asíncrona, que requiere la presencia de un puerto de «consola» en el equipo en cuestión. La ventaja del puerto de consola es que, en caso de problema con el equipo o de configuración incorrecta, siempre habrá una forma de conexión para el administrador.



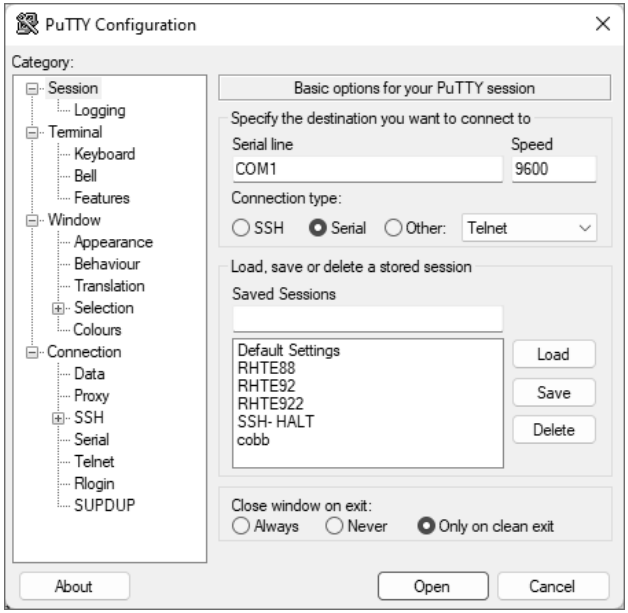
Interfaz CLI para un activo de red Cisco

Observación

Muchos fabricantes están sustituyendo gradualmente el tradicional puerto de consola RS232 por un enlace mini-usb o usb-c. Tenga en cuenta que, aunque el conector tenga formato RS232, el patillaje puede ser específico del equipo. Utilice preferiblemente el cable suministrado.

Para acceder a la CLI de un equipo remoto, puede utilizar cualquier software compatible con el protocolo con el que haya configurado el equipo. Uno de los más conocidos es la utilidad PuTTY, que también se puede utilizar para gestionar los enlaces serie y la conexión al puerto de consola del dispositivo.

– https://www.putty.org/



Configuración del acceso a la consola mediante el software PuTTY

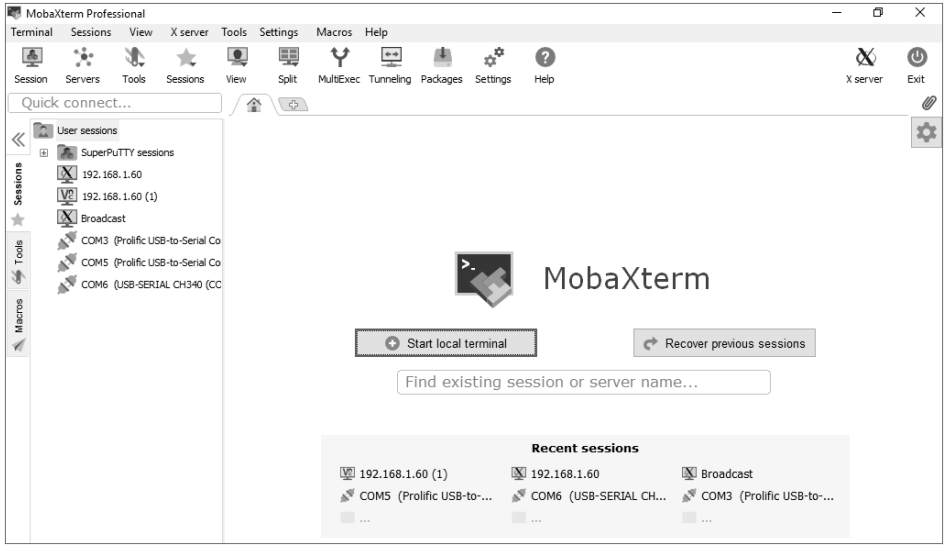
Observación

Para una conexión al puerto de consola, consulte la documentación del fabricante, que le indicará los parámetros como velocidad de conexión (en baudios), número de bits de datos, número de bits de parada, presencia de un bit de paridad. Una conexión indicada como 9600 8N1 corresponde a una velocidad de 9600 baudios con 8 bits de datos, sin paridad (N) y 1 bit de parada.

La interfaz CLI requiere conocer los comandos de configuración específicos definidos por el fabricante. En este caso, es indispensable estar entrenado para gestionar equipos de red a través de la CLI, incluso si domina los conceptos de red.

Existen varios paquetes de software que permiten la conexión de consolas a un equipo (la mayoría deellos también gestiona otros modos de conexión); sería imposible enumerarlos todos aquí. Sin embargo, el software MobaXterm tiene muchas funciones que lo convierten en una herramienta muy completa para probar. También existen variantes de PuTTY que permiten integrar más funciones, como la transferencia de archivos solo por consola, la grabación de las sesiones configuradas y su portabilidad a otro sistema, así como la posibilidad de crear scripts o enviar una lista de comandos preestablecidos al realizar la conexión.

– https://mobaxterm.mobatek.net/
– http://www.extraputty.com
– http://www.9bis.net/kitty/



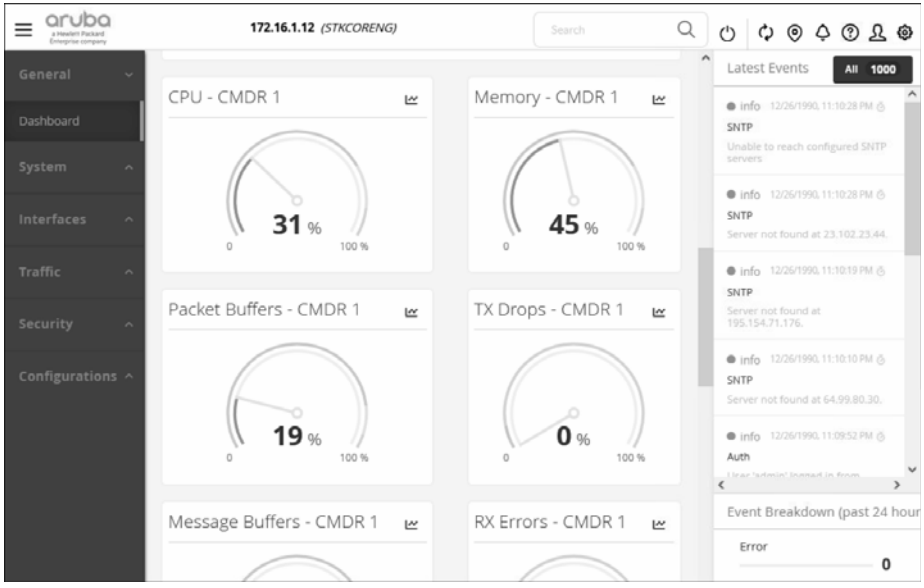
Interfaz de la herramienta MobaXterm

1.1.2 Interfaces web

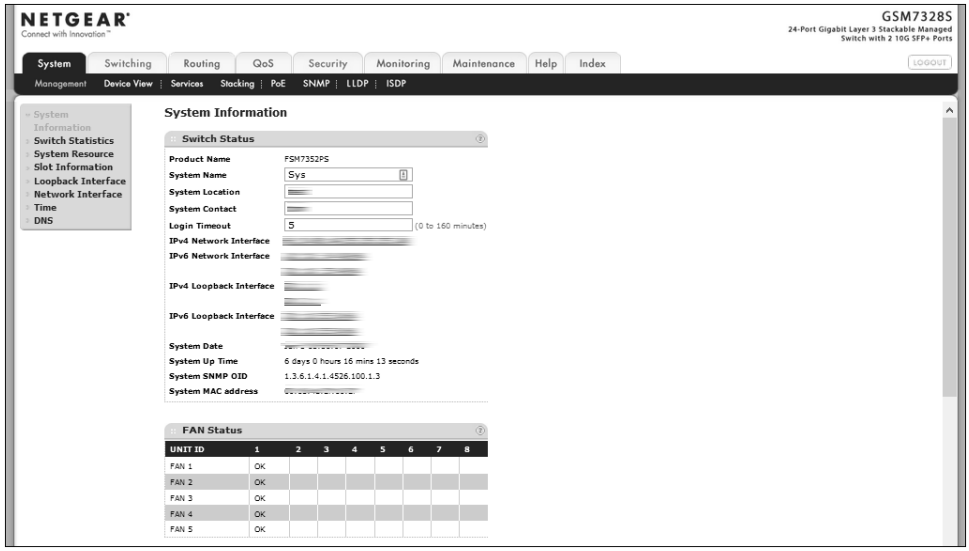
Con el fin de facilitar la gestión de los equipos y paralelamente al desarrollo de las tecnologías web, sobre todo en lo que respecta a las interfaces gráficas, los fabricantes han empezado a implementar interfaces web para configurar sus equipos, en sustitución o como complemento de la CLI.

Esto permite configurar los equipos sin conocer ni teclear ningún comando, lo que ha permitido a fabricantes como HP y Aruba reposicionarse en el mercado o al menos proponer productos diferentes.

Es más, los fabricantes han podido desarrollar interfaces gráficas atractivas que permiten ver de un vistazo la salud y el estado de un equipo. Las principales ventajas de las interfaces web son: ahorro de tiempo en la configuración, reducción de los costes de formación del equipo de red y disminución del tiempo dedicado a la resolución de problemas.



Interfaz web de un switch ARUBA



Interfaz web de un switch Netgear GSM73285

Interfaz web de un switch L3 D-Link DGS-3630

Los principales inconvenientes de gestionar un equipo a través de una interfaz web deben analizarse desde el punto de vista de la seguridad. De hecho, los fallos en un protocolo como SSH son relativamente pocos y, sobre todo, se corrigen rápidamente. En cambio, el protocolo web HTTP está mucho más expuesto.

En efecto, la seguridad dependerá del lenguaje utilizado y de la forma en que se haya desarrollado la interfaz (el 95 % puede atribuirse al desarrollador). Esta fue la principal crítica que se les hizo cuando aparecieron por primera vez.

Posteriormente, han aparecido interfaces que gestionan una capa adicional de seguridad con SSL/TLS, lo que permite establecer una conexión HTTPS segura entre el navegador del administrador y el equipo.

Para analizar mejor los riesgos de seguridad asociados a una interfaz web, basta con observar el aumento significativo de la superficie potencial de ataque inducido por las diferentes tecnologías web utilizables. Los ataques pueden dirigirse a un navegador específico, a un complemento específico del navegador o a un lenguaje específico como Java o FLASH. Todos ellos con un gran número de vulnerabilidades críticas, además de los fallos derivados de la falta de conocimiento de los principios de seguridad por parte de los equipos de desarrollo que no están necesariamente formados.

A título indicativo, solo en 2021 y 2022 se identificaron 280 vulnerabilidades, algunas de ellas extremadamente críticas, en equipos NETGEAR.

– https://www.opencve.io/cve?vendor=netgear

1.1.3 Gestión mediante una aplicación pesada

Aunque esto es cada vez menos frecuente, e incluso ha desaparecido por completo en los modelos recientes, algunos equipos en producción pueden gestionarse mediante una aplicación cliente dedicada (*fat client*; cliente pesado).