

Cuando un equipo falla y pierde su conexión con la red hay que seguir un orden en el diagnóstico de la avería, ya que esto nos permitirá llegar a una solución de una forma mucho más sencilla y rápida. El orden de comprobaciones que se deberá seguir es el mismo que se establece en la arquitectura de red, comenzando por los niveles más bajos (físico y enlace de datos) y acabando en el nivel de red:

- Posibles conflictos entre el adaptador de red y el equipo.
- Conexión física del adaptador con la red.
- Configuración de los parámetros de la arquitectura de red.

7.1 HERRAMIENTAS DE DIAGNÓSTICO DE DISPOSITIVOS DE COMUNICACIONES EN REDES LOCALES

Cuando un equipo falta y de ja de funcionar correctamente, el primer paso antes de solucionar el problema es detectar la causa que lo ha producido. Esta causa puede ser producida por un hecho externo (fallo de corriente, ataque intencionado, etc.) o por un problema interno (un error en la configuración del sistema, un fallo en un componente, etc.).

Para detectar un problema y así poder solucionarlo podemos trabajar con:

- **Archivos de configuración del sistema:** contienen los parámetros de configuración de los distintos servicios del sistema. En los sistemas Microsoft Windows se usa una gran base de datos que guarda toda la configuración del sistema y los programas instalados llamada Registro. Para acceder a esta base de datos se utiliza la orden REGEDT32.EXE, teniendo en cuenta que la información que contiene es muy sensible y es necesario hacer copias de seguridad antes de manipularla. Para los sistemas GNU/Linux se utiliza un conjunto de archivos de configuración que también son bastante sensibles a las modificaciones.
- **Archivos de registro del sistema (log file):** además de las aplicaciones, comandos y archivos de configuración disponibles para realizar diagnóstico de averías en los distintos sistemas operativos de red, son también muy útiles los archivos de registro (log file). Un **archivo de registro** es utilizado por el sistema para guardar todos los sucesos que se producen en la ejecución de las aplicaciones y servicios en él. El administrador del sistema puede inspeccionar estos archivos para comprobar qué errores se han producido durante la carga o la ejecución de esos servicios.
- **Herramientas para el diagnóstico y recuperación:** se trata de un conjunto de programas y aplicaciones que facilitan la búsqueda de las causas de los fallos e incluso también intentan subsanarlas lo mejor posible.
- **Indicadores de estado de los puertos:** en general, los dispositivos de interconexión y los adaptadores de red disponen de indicadores luminosos de estado que permiten determinar, además de otros parámetros, si hay conexión con la red. Esto ayuda a identificar muchos de los problemas que se producen.

7.1.1 Indicadores de estado de los puertos

Los dispositivos de interconexión de redes disponen de una serie de indicadores luminosos, situados en la parte frontal (para que resulte más fácil verlos), que muestran el estado actual de funcionamiento. También existen una serie de indicadores luminosos, por cada uno de los puertos del equipo, que informan también de su estado.

El significado de los indicadores luminosos puede variar de unos modelos y fabricantes a otros aunque, por norma general, suelen tener los siguientes significados:

- **Verde:** el funcionamiento del puerto es correcto.
- **Naranja.** El funcionamiento del puerto es incorrecto o lo hace por debajo de sus capacidades de transmisión.
- **Parpadeo:** existe algún problema de funcionamiento o lo hace de forma deficiente.

En general, un conmutador puede contar con los siguientes indicadores luminosos:

- **Sistema:** es un indicador que muestra el estado general del equipo, si está encendido, recibe corriente eléctrica de alimentación o está ejecutando los programas de arranque y diagnóstico.
- **Suministro remoto de energía:** muestra si el equipo está funcionando porque otro equipo le está suministrando energía eléctrica de forma remota.
- **Modo de puerto:** indica qué tipo de información que pueden mostrar es: **estado, utilización, modo de transmisión o velocidad de transmisión**. Este indicador cambia cuando se pulsa en el botón etiquetado "Modo".
- **Estado de los puertos:** son los indicadores luminosos que están ubicados en cada uno de los puertos del equipo. Estos indicadores muestran el estado del puerto dependiendo del modo seleccionado. Los indicadores pueden mostrar la siguiente información:
 - Estado: indica si el puerto está conectado, activado y transmitiendo datos.
 - Utilización: muestra el grado de utilización del ancho de banda disponible.
 - Modo de transmisión: indica si la transmisión es dúplex o no.
 - Velocidad de transmisión: muestra la velocidad de transmisión del puerto (en las redes Ethernet cableadas puede ser 10 Mbps, 100 Mbps, 1 Gbps o 10 Gbps).

En general, un encaminador puede contar con los siguientes indicadores luminosos:

- **Sistema o PWR:** es un indicador que muestra el estado general del equipo, si está encendido, recibe corriente eléctrica de alimentación o está ejecutando los programas de arranque y diagnóstico.
- **Actividad:** muestra si el equipo está recibiendo o enviando mensajes.

- **Memoria flash:** se ilumina cuando la memoria flash del equipo está en uso, en este momento no debe extraerse la tarjeta de memoria CompactFlash.
- **Estado de los puertos:** son los indicadores luminosos que están ubicados en cada uno de los puertos del equipo. Estos indicadores muestran el estado del puerto dependiendo del modo seleccionado. Los indicadores pueden mostrar la siguiente información:
 - Estado: indica si el puerto está conectado, activado y transmitiendo datos.
 - Modo de transmisión: indica si la transmisión es dúplex o no.
 - Velocidad de transmisión: muestra la velocidad de transmisión del puerto (en las redes Ethernet cableadas puede ser 10 Mbps, 100 Mbps, 1 Gbps o 10 Gbps).

Gracias a que los dispositivos de interconexión de redes disponen de estos indicadores luminosos de estado, es posible realizar tareas de comprobación de las diferentes conexiones, de forma que se pueden localizar aquellas que no funcionan correctamente o que no han sido instaladas como es debido.

7.1.2 Indicadores de estado de los adaptadores de red

La mayoría de adaptadores de red disponibles en el mercado, tanto cableados como inalámbricos, disponen de una serie de indicadores luminosos que informan del estado actual de la conexión, de la misma forma que los dispositivos de interconexión de red. Gracias a estos indicadores luminosos, es posible identificar la causa de algunos de los problemas que pueden afectar a las redes de comunicaciones. Los indicadores luminosos que más comúnmente existen en los diferentes tipos de adaptadores de red son los siguientes:

- **Conexión:** suele nombrarse como LNK o PWR y se enciende si hay conexión con la red. En el caso de una tarjeta inalámbrica, lo normal es que el indicador deje de parpadear cuando hay conexión.
- **Actividad:** suele nombrarse como ACT o TX/RX y luce si la tarjeta está enviando o recibiendo datos.
- **Colisión:** se nombra como COL o FUDUP e indica si se ha producido una colisión (varias estaciones transmiten a la vez). Si este indicador luminoso se enciende con mucha frecuencia, puede ser síntoma de que hay demasiados equipos transmitiendo a la vez y la red está saturada.
- **Velocidad:** el fabricante puede incluir otro indicador para mostrar la velocidad de transmisión que está utilizando esa tarjeta (el color naranja suele indicar 10 Mbps y el verde, 100 Mbps o 1 Gbps).

7.1.3 Comprobación de conexiones inalámbricas

Todos los sistemas operativos modernos disponen de herramientas que permiten gestionar las conexiones inalámbricas e informar de su estado. Gracias a estas herramientas, es posible detectar la causa de un mal funcionamiento de la conexión. En diferentes intensidades de las señales inalámbricas emitidas en distintas longitudes de onda, aunque esos instrumentos resultan bastante costosos.

7.1.4 Herramientas de monitorización de red

Las herramientas para la monitorización de una red de comunicación pueden ser muy variadas: desde dispositivos que analizan la señal que circula por un cable a programas que monitorizan todo el tráfico de los enlaces. Estas herramientas tienen la ventaja de que son menos intrusivas, ya que evitan que los dispositivos de interconexión tengan que realizar trabajo adicional.

El análisis del tráfico resulta muy sencillo para una red de comunicación que utiliza un medio compartido (como las redes Ethernet) ya que un equipo puede obtener todos los mensajes en circulación si su adaptador de red funciona en modo promiscuo. Si complementamos esta captación del tráfico con una herramienta avanzada, podemos realizar un análisis completo del funcionamiento de la red.

Uno de los objetivos que se pueden perseguir a la hora de realizar un análisis del tráfico de la red consiste en determinar la calidad de servicio ofrecida. La calidad de servicio define el rendimiento que ofrece la red de comunicación, en cuanto a tres parámetros: el retardo (tiempo que tardan los mensajes desde el origen al destino), la variación del retardo (diferencia de retardo entre los distintos mensajes) y la pérdida de mensajes (cantidad de mensajes que se pierden por alguna razón).

7.2 PROCESOS DE GESTIÓN DE INCIDENCIAS EN REDES LOCALES

Una **incidencia** es cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo. En general, cualquier contacto que mantienen los usuarios con los administradores de puede considerar una incidencia, exceptuando las peticiones de licencias para el uso de determinados servicios o el cambio en la información de acceso.

La **gestión de incidencias** tiene como objetivo resolver, de la manera más rápida y eficaz posible, cualquier incidente que cause una interrupción en los servicios ofrecidos por la red local. Por lo tanto, la gestión de incidencias no tiene como objetivo buscar las causas que han producido un incidente ni mejorar la calidad del servicio, simplemente persigue restaurar los servicios lo antes posible.

Un proceso de gestión de incidencias define una serie de pasos que se tienen que llevar a cabo para resolver el problema. En general, los pasos que se siguen en la gestión de incidencias son:

- Detectar las alteraciones en los servicios ofrecidos por la red local.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de resolver el problema y restaurar el servicio.

Las principales ventajas de una correcta gestión de incidencias son:

- Mejorar la productividad de los usuarios que trabajan con la red.
- Cumplimiento de los niveles de servicio acordados en el diseño e instalación de la red.
- Mayor control de los procesos y monitorización del servicio.
- Optimización de los recursos disponibles.
- Mejorar la satisfacción general de los usuarios que utilizan la red.

Por su parte, los inconvenientes de llevar a cabo una incorrecta gestión de incidencias son:

- Reducción de los niveles de servicio.
- Gestión ineficiente de los recursos.
- Pérdida de información sobre los procedimientos de resolución de futuras incidencias.
- Aparición de usuarios insatisfechos.

Los principales escollos a la hora de realizar una correcta gestión de incidencias son.

- No se siguen los procedimientos establecidos.
- Se resuelven las incidencias sin registrarlas.
- Se recurre a técnicos de nivel superior innecesariamente.
- No existe un margen operativo para gestionar grandes volúmenes de incidencias.

La aceptación y el registro de la incidencia es el primer paso hacia su resolución. Las incidencias pueden provenir desde diversas fuentes, como los propios usuarios, la monitorización de la red por parte de los administradores, etc. El registro de la incidencia debe realizarse inmediatamente o se correrá el riesgo de no hacerlo en el futuro ante una eventual aparición de nuevas incidencias. El registro se realiza en estos pasos:

1. Admisión a trámite del incidente y primera valoración.
2. Comprobación de que ese incidente aún no ha sido registrado, porque es habitual que una misma incidencia se notifique desde diversas fuentes.
3. Asignación de un número de referencia que la identificará de forma única.
4. Registro de los datos de la incidencia, como hora, descripción, sistemas afectados, etc.
5. Notificación a todos los usuarios para que sean conscientes de que la incidencia puede afectarles en su trabajo con la red local.

Una vez registrada la incidencia, el siguiente paso consiste en clasificarla, siguiendo estos pasos:

- Asignar una categoría de incidencia que se relaciona con los servicios afectados.
- Establecer un nivel de prioridad.
- Asignar los recursos necesarios, ya sean de la propia organización o de proveedores externos.
- Asociar un estado a la incidencia y estimar el tiempo necesario para resolverla.

Es habitual que se produzcan varias incidencias a la vez, por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas. La priorización se basa esencialmente en dos parámetros:

- **Impacto:** determina la importancia de la incidencia dependiendo de cómo ésta afecta al trabajo y a la cantidad de usuarios.
- **Urgencia:** depende del tiempo máximo de demora aceptado por los usuarios para la resolución de la incidencia.
- **Tiempo de resolución:** por lo general, las incidencias simples se tramitarán antes porque se pueden resolver en poco tiempo.

Dependiendo de la prioridad de la incidencia, se podrán asignar más o menos recursos para resolverlas. De igual forma, las incidencias pueden cambiar de prioridad a lo largo del tiempo, ya que en algunos casos se pueden encontrar soluciones temporales que restauren la red o sus servicios a niveles de funcionamiento aceptables.

El análisis de la incidencia conlleva, en primer lugar, el examen de incidencias anteriormente registradas para valorar la posibilidad de utilizar procedimientos ya empleados con anterioridad. Suele ser habitual que determinadas incidencias no puedan ser resueltas por los administradores de la red, por lo que es necesario involucrar a algunos técnicos más especializados y personal superior que tome las decisiones necesarias. Dependiendo de la envergadura de la organización, el escalado puede abarcar más o menos niveles.

Durante el período de puesta en marcha de los procedimientos para resolver la incidencia, se debe actualizar la información de los registros de la incidencia para que los usuarios afectados dispongan de información precisa sobre el estado de la misma. Si fuera necesario, se puede realizar una petición de cambios en determinados parámetros o dispositivos de la red local.

Cuando la incidencia se haya resuelto, es necesario informar a los usuarios y preparar la documentación asociada para que pueda ser utilizada en futuras incidencias. Para el correcto seguimiento de todo el proceso, se aconseja la realización de encuestas que permitan evaluar objetivamente el funcionamiento del servicio y la satisfacción de los usuarios. Algunos de los aspectos importantes que se deben considerar en esta encuesta son:

- Número de incidentes clasificados temporalmente y por prioridades.
- Tiempos de resolución clasificados en función del impacto y la urgencia de los incidentes.
- Costes asociados.
- Uso de los recursos disponibles.
- Porcentaje de incidentes, clasificados por prioridades, resueltos en primera instancia.
- Grado de satisfacción de los usuarios.

7.2.1 Análisis de incidencias en redes locales

Los problemas de acceso a la red de un equipo se catalogan entre los más comunes a los que se enfrenta el administrador de red. Llamadas de los usuarios con argumentos como “no puedo acceder a Internet”, “no puedo entrar a mi carpeta en el servidor” o “no puedo ver las carpetas compartidas en la red”, son las que más horas consumen a los administradores.

Ante una situación de este tipo, lo primero que debe hacer el administrador es comprobar si el fallo es debido a una instalación incorrecta del adaptador, a que no hay conexión con la red o a que existe algún protocolo que no funciona correctamente. A partir de ahí, se puede centrar en cuestiones más específicas hasta que llegue a la causa o causas que han generado el problema.

Cuando un equipo falla y pierde su conexión con la red hay que seguir un orden en el diagnóstico de la avería, ya que esto nos permitirá llegar a una solución de una forma mucho más sencilla y rápida. El orden de comprobaciones que se deberá seguir es el siguiente:

1. Módulo (controlador) adecuado y cargado por el núcleo.
2. Posibles conflictos entre el adaptador de red y el ordenador.
3. Conexión física del adaptador con la red.
4. Configuración de los parámetros de la arquitectura de red.

Para poder realizar estas comprobaciones disponemos de un conjunto de herramientas en forma de comprobadores de cableado de red y herramientas que se incluyen en el sistema operativo de los equipos.

Una vez que estamos seguros que el adaptador de red está correctamente instalado y configurado en el equipo, debemos seguir los siguientes pasos para encontrar la causa del problema:

1. Consultar la configuración de red del equipo y compararla con la que figura en nuestra base de datos. Los parámetros que hay que consultar son los correspondientes a TCP/IP y a la red Microsoft (si es que el equipo lleva Windows instalado). En caso de que no coincidan, establecer los valores que correspondan.

2. En caso de que el equipo obtenga su configuración de red a través del protocolo DHCP, comprobar que esta asignación se realiza correctamente. En caso contrario, revisar la configuración del servidor DHCP.
3. Utilizar la orden PING para comprobar de una forma rápida si el equipo puede comunicarse con su encaminador o puerta de enlace por defecto (o servidor proxy). En caso de que la respuesta sea positiva, entonces descartaremos un problema de configuración del equipo o de acceso a la red. De lo contrario, nuestro trabajo deberá centrarse primero en el equipo con problemas. Cuando se utiliza esta herramienta, se pueden utilizar como direcciones de destino las del propio equipo (la dirección 127.0.0.1 o la dirección IP asignada) o la de otro equipo o dispositivo de la red. Sin embargo, hay que tener en cuenta que utilizar las direcciones asignadas al propio equipo no asegura que el eco enviado vaya a ser transmitido por la red. En la mayoría de las ocasiones, al enviar un eco a la dirección 127.0.0.1 o a la del propio equipo se recibe un mensaje de respuesta independientemente de si el adaptador está conectado a la red o no. Por esta razón, se recomienda que el envío de mensajes de eco se realice a otros equipos de la red, situación que nos asegura la comprobación de la línea.

Ahora vamos a detallar las dos posibles vías de investigación que se han abierto. Comenzamos primero con los pasos que debemos seguir cuando el equipo no recibe respuesta a los mensajes PING enviados:

1. Comprobar si el adaptador está correctamente instalado o si existe algún conflicto con otro dispositivo. En los sistemas Linux se puede consultar la lista de dispositivos instalados en el sistema (en el archivo `/proc/pci`), la lista de módulos cargados (`/proc/modules`), las interrupciones utilizadas (`/proc/interrupts`) o los avisos y errores generados por el núcleo de Linux (con la orden `dmesg`).
2. Si se trata de una red cableada, comprobar si el cable de conexión está en perfectas condiciones.
3. Si se trata de una red inalámbrica, comprobar que se recibe señal suficiente desde el punto de acceso más cercano.
4. En último caso, la falta de conexión con la red puede ser debida a una cantidad de ruido excesivo en el cable o en el ambiente.

En caso de que el equipo tenga acceso a la red, deberemos seguir otras comprobaciones, que son:

1. Comprobar la configuración de encaminamiento en el encaminador por donde debe circular la información.
2. Realizar consultas a los servidores DNS para comprobar que la resolución de nombres funciona correctamente.

7.2.2 Análisis de incidencias en redes inalámbricas

A la hora de verificar el funcionamiento de una conexión inalámbrica, es recomendable seguir estos pasos:

1. Comprobar la intensidad de la señal recibida, asegurando que la calidad de la señal que llega al equipo es buena. En caso de que no lo sea, hay que estudiar la posibilidad de ubicar el equipo en un lugar mejor o trasladar el punto de acceso inalámbrico.
2. Comprobar los parámetros de configuración de la conexión inalámbrica para asegurar que son correctos. Estos parámetros son el identificador de la red (SSID), tipo de red, tipo de cifrado, clave de cifrado, etc.
3. Comprobar los parámetros TCP/IP de la conexión (dirección IP, máscara de red, etc.).