En los capítulos anteriores se explica cómo realizar la instalación de los diferentes elementos que componen una red local, su interconexión entre sí y la configuración de los diferentes parámetros de red para conseguir que los protocolos de comunicaciones puedan trabajar de forma óptima.

Este capítulo está dedicado a explicar las diferentes herramientas que se utilizan para poder verificar y probar la red una vez instalada y configurada. Gracias a estas pruebas, podemos verificar que la red de comunicación está preparada para su trabajo en un entorno productivo.

5.1 HERRAMIENTAS DE VERIFICACIÓN Y PRUEBA

Este apartado está dedicado a explicar las diferentes herramientas que se pueden utilizar para verificar que la red de comunicación funciona correctamente.

5.1.1 Herramientas de verificación y prueba de los sistemas operativos

Todas las funciones que ofrece un sistema operativo están disponibles gracias a que en el equipo se están ejecutando una serie de programas que las implementan, habitualmente atendiendo las peticiones que les llegan de los usuarios, bien desde el propio equipo o bien desde otros equipos a través de la red. Estos programas están normalmente ejecutándose durante todo el tiempo que el ordenador está activo o permanecen latentes o con una actividad mínima hasta que se activan cuando son necesarios.

En los sistemas operativos modernos, las funciones que se llevan a cabo se realizan a través de programas en ejecución denominados procesos. El sistema operativo debe ser capaz de ejecutar parte del código de un proceso, dejarlo en espera y continuar con la ejecución de otro. Esta operación, realizada a una gran velocidad y con una gran cantidad de procesos, da al usuario la percepción de que todas esas tareas se están realizando a la vez. En caso de que alguno de los procesos deje de funcionar o se termine, entonces la tarea que desempeña ya no se realizará, por lo menos hasta que vuelva a ejecutarse de nuevo.

Las tareas que tienen que ver con la red de comunicación a la que está conectada el equipo, en general, la transmisión y la recepción de la información, también se gestionan a través de determinados procesos que están en ejecución. Si alguno de estos procesos se interrumpe, entonces no se podrá transmitir o recibir esa información.

Los procesos pueden ser finalizados por los usuarios, pero también pueden terminar inesperadamente debido a algún fallo o algún error en la configuración. Muchos de ellos también pueden causar graves problemas de funcionamiento al equipo o incluso hacer que éste no responda. Esto es debido a que muchos servicios trabajan con programas controladores de dispositivos, que son muy sensibles a los fallos y a los errores en las configuraciones.

La mayoría de los sistemas operativos modernos ofrece la posibilidad de arrancar con un determinado número de procesos en ejecución, lo que hace que pueda ser capaz de desempeñar determinadas tareas y trabajar con diferentes configuraciones. Esto le permite probar algunas de esas funciones e incluso recuperar el sistema de algunos fallos producidos. En el ejemplo se muestra un caso genérico (sin entrar todavía en detalles de un sistema operativo concreto) donde ocurre un fallo de este tipo.

EJEMPLO

Un ejemplo bastante común en el que es necesario el arranque del sistema con una configuración diferente a la utilizada normalmente se produce cuando se instalan en el sistema determinados programas controladores de dispositivo (drivers) que no funcionan correctamente.

En ese caso, puesto que el programa controlador es capaz de ejecutar operaciones privilegiadas sobre el sistema, puede ocurrir que su mal funcionamiento pueda tener como resultado el bloqueo del sistema. Este bloqueo se puede producir incluso en el momento de carga de este programa controlador, es decir, en el arranque del sistema.

Como consecuencia de esta situación, nos encontramos con que es imposible recuperar el problema porque para eso es necesario acceder a la configuración del equipo y eliminar el controlador dañado, pero eso no es posible ya que el equipo se bloquea en el arranque.

Para solucionar esta situación, algunos sistemas operativos incluyen la opción de arranque sin la carga de algunos programas controladores. De esta forma, es posible iniciar el equipo en este modo, eliminar el programa controlador dañado y reiniciar normalmente con el sistema recuperado y con la posibilidad de solucionar el problema o volver a una configuración anterior.

5.1.1.1 Modos de arranque en Microsoft Windows

El **modo a prueba de errores** que incorporan los sistemas Microsoft Windows permite iniciar el sistema operativo con diferentes configuraciones. Estas configuraciones cargan unos determinados controladores de dispositivos y servicios. Los modos de arranque del sistema no servirán de nada si el daño se encuentra en los archivos del sistema o en el disco duro.

Para poder seleccionar los diferentes modos a prueba de errores hay que pulsar la tecla F8 en el inicio del proceso de arranque del sistema, antes de que comience la carga del sistema operativo. De esta forma, podemos hacer un arranque del sistema operativo con los servicios que nos sean de utilidad o eliminando aquellos que nos causan problemas. Los diferentes modos a prueba de errores que incluyen las distintas versiones de Microsoft Windows se resumen en la tabla 5.1.

Tabla 5.1. Modos a prueba de errores de Windows 2000/2003/XP

Nombre	Descripción
Modo seguro	Inicia el sistema con los controladores básicos: ratón, monitor con pantalla a baja resolución (VGA), teclado, unidades de disco y servicios predeterminados del sistema.
Modo seguro con funciones de red	Es igual que el anterior, además de que inicia todos los servicios de red para que el equipo tenga conexión.
Modo seguro con símbolo del sistema	Es igual que el modo seguro pero no arranca el entorno gráfico, sino una línea de comandos.
Habilitar el registro de inicio	Se usa para indicar si se activa el registro (log) de todo lo que ocurre cuando se arranca el sistema. Este registro se guarda en el archivo NTBTLOG.TXT de la carpeta de instalación de Windows (normalmente C:\WINDOWS).
Habilitar el modo VGA	Inicia el sistema con todos los servicios pero con el modo de pantalla VGA. Se utiliza cuando hay problemas con el controlador de tarjeta gráfica instalado.
La última configuración válida conocida	Se usa para iniciar el sistema con los parámetros de configuración del registro anteriores a los últimos cambios realizados en él. De esta forma, se puede iniciar el sistema cuando se ha modificado por error algún valor del registro que impide el arranque.
Modo de restauración de SD	Se utiliza solamente en Windows Server 2003 cuando el equipo es controlador de dominio y se desea realizar una restauración del directorio activo con la última copia de seguridad.
Modo de depuración	Permite iniciar el sistema y enviar información sobre el proceso de arranque paso a paso a otro equipo por un cable serie.

5.1.1.2 Modos de arranque en GNU/Linux

Los sistemas GNU/Linux también disponen de mecanismos que permiten iniciar el sistema con diferentes configuraciones, dependiendo de las necesidades de los usuarios. Estas configuraciones están basadas en los procesos que se activan en el arranque. Si se modifican los programas que se inician en el arranque (muchos de ellos no son imprescindibles para el funcionamiento básico del sistema), entonces podemos conseguir que Linux trabaje de forma distinta, ofreciendo un conjunto diferente de servicios o permitiendo a los usuarios que puedan probar nuevas configuraciones.

Cuando se inicia un sistema Linux o Unix, el control recae sobre un proceso especial llamado `init`, que es el primero que comienza su ejecución. Por esta razón, también se le conoce como “el padre de todos los procesos”. `Init` es un proceso especial sin el cual no se iniciará nunca Linux y que controla el inicio de otros procesos. Por lo tanto, si el usuario desea establecer qué procesos se iniciarán en el arranque, entonces deberá configurar `init` para que se inicien solamente los procesos que nos interesan.

El proceso `init` permite que el usuario pueda definir diferentes configuraciones, cada una de ellas iniciará un conjunto distinto de procesos. A estas configuraciones se les conoce como **niveles de ejecución**. Cada nivel de ejecución hace que el sistema se comporte de forma distinta, ya que, como hemos dicho, inicia un conjunto de procesos distintos. De esta forma, el usuario puede seleccionar sobre qué configuración o nivel de ejecución va a iniciar el sistema.

La configuración de los distintos niveles de ejecución se puede realizar de dos formas:

- A través del entorno gráfico utilizando una herramienta especial, que en el caso de OpenSUSE se llama "Editor de niveles de ejecución" y se encuentra en el grupo de utilidades "Sistema" dentro de YaST. En el caso de Fedora, hay que acceder a la herramienta "Configuración de servicios" (redhat-config-services) del **panel de control** o la opción "Configuración || Servicios misceláneos" de Linuxconf. También se pueden utilizar otras herramientas como la opción "Sistema || Configuración init de SysV" de Webmin.
- A través del archivo de configuración `inittab` que se encuentra dentro de la carpeta `/etc`. Este es el archivo de configuración principal del proceso `init` y todas las herramientas gráficas de configuración acceden a él para realizar los cambios. Cuando se edita manualmente este archivo, hay que tener mucho cuidado para no cometer errores de sintaxis, ya que puede ocurrir que no arranque Linux.

En el archivo de configuración `/etc/inittab` se establecen los procesos que se van a iniciar para un determinado nivel de ejecución. Los niveles de ejecución predefinidos en la mayoría de las versiones de Linux son los siguientes:

- **0 (Parada de sistema)**: se utiliza para apagar el equipo.
- **1 (Modo monousuario)**: se accede al sistema en modo monousuario (es decir, solamente puede entrar un único usuario al sistema en un momento dado) sobre un intérprete de órdenes y sin servicios de red.
- **S (Modo monousuario)**: igual que el modo 1 pero con el teclado configurado en idioma Inglés.
- **2 (Modo multiusuario local sin red)**: se accede al sistema sobre una consola de línea de órdenes y sin servicios de red. Varios usuarios pueden acceder el mismo tiempo al sistema.
- **3 (Modo multiusuario completo con red)**: se accede al sistema sobre una consola de línea de órdenes con todos los servicios.
- **4** (libre, es decir, no utilizado): este nivel no está configurado, así que puede definirse a gusto del usuario.
- **5 (Modo multiusuario completo con red y entorno gráfico)**: éste es el nivel por defecto que inicia el sistema con todos los servicios y en modo gráfico.
- **6 (Reiniciar el sistema)**: se utiliza para reiniciar el equipo.

Aunque los niveles de ejecución anteriores se comportan por defecto como se ha indicado, es posible que el usuario los configure de forma distinta de acuerdo con sus necesidades. Por ejemplo, se puede hacer que el sistema inicie el modo gráfico en el nivel 3 si se indica a `init` que inicie el proceso que lo gestiona para ese nivel (por ejemplo, el proceso kdm).

Para seleccionar el nivel de ejecución que se va a utilizar en el arranque se puede hacer de tres formas:

- **Desde el entorno gráfico utilizando YaST2**, por ejemplo, se accede al icono "Editor de niveles de ejecución" dentro del grupo "Sistema". En la ventana se muestra, por un lado, el nivel de ejecución actual (será el 5 ya que estamos trabajando con el entorno gráfico) y el nivel de ejecución predeterminado para el arranque (es también 5 por defecto). Para cambiar el nivel, se selecciona el nuevo en la lista desplegable que está titulada "Establecer nivel de ejecución predeterminado en el arranque a:". La próxima vez que se inicie Linux arrancará en ese nivel de ejecución.
- **Editando el archivo /etc/inittab**, buscar una línea con el texto "id:5:initdefault:" y sustituir el numero 5 por el nivel de ejecución que deseamos sea el nuevo nivel por defecto. La próxima vez que se inicie Linux arrancará en ese nivel de ejecución.
- **Especificando el nivel en el menú de arranque del sistema** (ya sea el gestor Lilo o Grub). Este método no cambia el nivel de ejecución por defecto, aunque nos permite especificar cualquier nivel sin tener que arrancar para luego reiniciar. Para ello, hay que seleccionar el arranque con Linux y escribir "init n" donde n es el nivel deseado.

Es posible cambiar en cualquier momento de un nivel de ejecución a otro, utilizando la orden init, pero para ello hay que disponer de privilegios de root. Hay que utilizar la orden init especificando el nivel de ejecución al que se desea cambiar (si no se especifica ningún nivel, la orden init nos devuelve el número de nivel de ejecución en el que nos encontraremos en ese momento). Por ejemplo, la siguiente orden cambia el nivel de ejecución actual al 3:

```
# init 3
```

Para establecer qué procesos deseamos que se inicien en un determinado nivel de ejecución en OpenSUSE debemos acceder a la herramienta "Editor de niveles de ejecución" dentro del grupo "Sistema" de YaST. En la ventana principal que aparece debemos pulsar en el botón "Editar los detalles".

En la ventana de configuración podemos observar que aparece una tabla en la que cada fila es un proceso. En cada columna se muestra información sobre ese proceso, como si están activos en este momento y el nivel de ejecución en el que se van a iniciar (0, 1, 2, 3, 5 ó 6). Se puede marcar o desmarcar un proceso para un nivel de ejecución, lo que hará que se inicie o no en ese nivel. El nivel de ejecución 4 permanece libre para que el usuario pueda realizar una configuración personalizada.

Los procesos cuyo nombre comienza por "boot" son aquellos que se inician en el arranque pero finalizan su ejecución una vez que el sistema ha completado esta operación. Todos ellos se inician en el nivel "B" que no es un nivel de ejecución como tal, sino más bien indica el proceso de arranque que es común para todos los niveles. Esto quiere decir que los procesos que se inician en el nivel B lo hacen para todos los niveles de ejecución. Por ejemplo, el proceso `boot.sysctl` se usa para establecer los parámetros por defecto que va a utilizar el sistema una vez que ha arrancado. Estos parámetros se establecen en el archivo de configuración `/etc/sysctl.conf`.

Existen otras muchas herramientas gráficas que permiten la configuración de los procesos que se van a iniciar en el arranque, además de otras como ktsysv que se puede iniciar desde la línea de órdenes. Este tipo de utilidades no suelen instalarse por defecto en las distintas distribuciones de Linux, aunque normalmente se incluyen con ellas.

5.1.1.3 Visor de sucesos y registro del sistema

Aunque algunas aplicaciones pueden registrar los eventos y sucesos producidos durante su arranque o su ejecución en Windows, la mayoría los registra a través del visor de sucesos (orden EVENTVWR.MSC). Gracias a esta herramienta, se puede consultar en cualquier momento todos los mensajes producidos en el sistema local o en otro sistema remoto. Examinando estos mensajes se puede verificar el funcionamiento de determinados servicios que se encuentran en ejecución en el equipo.

Los sucesos o eventos que se registran en Microsoft Windows pueden ser de cinco tipos.

- Error: se trata de un problema importante, como una pérdida de datos o el fallo de un servicio del sistema.
- Advertencia. no es un problema importante, pero puede generar problemas importantes en el futuro.
- Información: describe el funcionamiento correcto de un programa, aplicación, controlador, servicio, etc.
- Acceso correcto auditado: se trata de un acceso de seguridad que se ha realizado correctamente, como un inicio de sesión, el acceso a un recurso compartido, etc.

- Acceso erróneo auditado: se trata de un acceso de seguridad erróneo, como, por ejemplo, un intento fallido de inicio de sesión.

Los eventos producidos en el equipo Microsoft Windows se agrupan en varios tipos. Los más importantes son los siguientes:

- Registros de aplicación: contiene los eventos producidos por programas de aplicación. A este tipo de eventos pertenecen diferentes situaciones, por ejemplo, que un programa no pueda abrir un archivo de configuración, que se produzca un error en un acceso a una base de datos, etc.
- Registro de sistema: guarda los eventos producidos durante el inicio de sesión, el acceso a recursos compartidos, etc. Dentro de este tipo de eventos podemos encontrar intentos fallidos para iniciar una sesión en el equipo, conexiones denegadas o satisfactorias con recursos compartidos, etc. Por defecto, estos eventos solamente pueden ser consultados por los administradores del sistema y no se registran, a no ser que se configuren las directivas de seguridad.

En cuanto a los archivos de registro, Linux mantiene una carpeta llamada /var/log donde se encuentran la mayoría de ellos. Dependiendo del tipo de aplicación o servicio, el archivo de registro puede variar. Sin embargo, los más utilizados por la mayoría de servicios son /var/log/localmessages y /var/log/messages.

5.1.2 Comandos TCP/IP

Para poder comprobar el funcionamiento de un equipo al que se le han configurado los parámetros de red, disponemos de un conjunto de comandos que utilizan los protocolos de comunicación. Muchos de estos comandos están disponibles en la instalación del sistema operativo, aunque algunos puede que no se instalen por defecto. Habitualmente, encontramos que los comandos son los mismos independientemente del sistema operativo utilizado, pero es probable que su sintaxis y su forma de uso puedan variar sensiblemente.

5.1.2.1 Comandos en Microsoft Windows

El sistema operativo Microsoft Windows dispone de un conjunto de herramientas que permiten realizar un diagnóstico del funcionamiento de la arquitectura de red. Para la arquitectura de red Microsoft existen varias utilidades, las más importantes son las siguientes:

- NET: esta orden permite realizar un diagnóstico de funcionamiento de la red Microsoft en varios aspectos. También se utiliza para el acceso a recursos compartidos.

- **Propiedades de red**: esta ventana resulta muy útil para comprobar la configuración de red del equipo en general y así encontrar posibles conflictos en asignación de direcciones IP o nombres NetBIOS. En las versiones de Microsoft Windows 2000/XP, parte de esta configuración aparece también en la ventana de **propiedades de Mi PC**, mientras que en los sistemas Windows Vista/7 esta información está disponible en el **Centro de redes y recursos compartidos**.

Por su parte, para la arquitectura TCP/IP se han instalado varias herramientas comunes en la mayoría de los sistemas (aunque en Windows las órdenes pueden variar debido a que la implementación de TCP/IP ha sido realizada por Microsoft):

- **IPCONFIG**: se utiliza para consultar la configuración de TCP/IP en el equipo. Si se usa el parámetro /ALL con esta orden, entonces se muestra toda la configuración de red, además de la dirección MAC que el adaptador tiene asignada.
- **PING**: permite comprobar si un equipo está conectado a la red y tiene activada la pila TCP/IP. También permite comprobar si hay una ruta establecida para un equipo o no es accesible. Utiliza las notificaciones del protocolo ICMP para notificar los errores detectados.
- **TRACERT**: esta orden es parecida a PING, aunque se utiliza para obtener la lista de direcciones IP de equipos y encaminadores que tiene que atravesar un mensaje hasta llegar a su destino. Es muy útil porque muestra el tiempo que tarda cada mensaje en alcanzar todos los equipos intermedios hasta su destino.
- **NSLOOKUP**: se utiliza para realizar consultas directas o inversas a los servidores DNS que se han establecido en la configuración del equipo. Con esta orden se puede saber si el problema de funcionamiento es debido a que los servidores DNS no resuelven correctamente las direcciones. En caso de que los servidores DNS especificados en la configuración no contesten, habrá que especificar otros.
- **PATHPING**; funciona igual que la orden PING, pero en este caso también se muestran las direcciones de los equipos intermedios por donde circulan los mensajes hasta el destino, además del porcentaje que son filtrados en cada uno de ellos.

El comando PING tiene la siguiente sintaxis:

```
PING [-a] [-n número] [-w tiempo] dirección_IP_destino
```

donde:

- **-a**: resuelve direcciones a nombres DNS de equipos.
- **-n número**: número de paquetes a enviar antes de finalizar este programa.
- **-w tiempo**: indicación del tiempo de espera máximo para las respuestas en milisegundos.
- **Dirección_IP_destino**: especifica la dirección IP del equipo al que se van a enviar los paquetes. Si la máquina está accesible, entonces es ésta la que contesta con otros paquetes de confirmación.

Las direcciones IP que se pueden utilizar con el comando PING pueden ser 127.0.0.1 para especificar la propia estación (si se usa ésta, el paquete no llega a enviarse por la red, ya que es la propia tarjeta la que contesta en caso de que funcione correctamente), la dirección IP asignada al equipo (al usar esta dirección, el paquete si que es enviado por la red, y es la propia estación la que contesta enviando otro paquete) y cualquier otra dirección IP de una estación de la red que esté encendida y funcione correctamente.

5.1.2.2 Comandos en GNU/Linux

En todas las versiones del sistema operativo Linux existen un conjunto de órdenes y utilidades que permiten realizar un diagnóstico del funcionamiento de la arquitectura de red TCP/IP. Algunas de las más importantes son:

- **ifconfig**: se utiliza para consultar la configuración de red del adaptador, aunque también permite su modificación a bajo nivel. Se puede utilizar esta orden para comprobar que no hay ningún otro equipo que tiene asignada la misma dirección IP o para consultar si está activo el adaptador.
- **ip**: se puede utilizar para consultar la configuración de los parámetros TCP/IP y de encaminamiento del equipo y también para modificarlos a bajo nivel.
- **route**: se usa para consultar o establecer los parámetros de encaminamiento del equipo a bajo nivel.
- **ping**: se utiliza para comprobar si el equipo puede enviar mensajes a la red o alcanzar a otros equipos. Utiliza las notificaciones del protocolo ICMP para notificar los errores detectados.
- **nslookup**: se utiliza para comprobar si los servidores DNS están realizando la resolución correctamente.
- **dig**: también se utiliza para comprobar si los servidores DNS que hemos especificado en nuestra configuración de red.
- **iptables**: se puede utilizar para mostrar la configuración de filtrado de paquetes en el sistema. En este caso, se puede utilizar esta orden de la siguiente forma: **"iptables** -L -n | less"
- **nmap**: se usa para comprobar los puertos que están abiertos en el equipo local o en un equipo remoto. Gracias a esta orden, podemos saber si un determinado servicio está activo en un servidor o cliente.
- **netstat**: puede ser utilizada también para consultar los puertos abiertos o a la escucha en el equipo. Esta información resulta muy útil sobre todo cuando configuramos determinados servicios de red en los servidores.

Para realizar la instalación del adaptador de red se puede utilizar la orden `modprobe`, que permite realizar la carga de un módulo controlador de dispositivo para manejar el adaptador. Esta orden resulta muy útil ya que se basa en la configuración del sistema y comprueba si el módulo funciona correctamente para el dispositivo instalado. En caso de que el módulo no funcione correctamente, éste es descargado para evitar que pueda dañar el equipo. Cuando no estamos seguros del módulo a utilizar, esta orden permite probar distintos módulos hasta dar con el que funcione correctamente.

5.1.3 Obtención de la configuración IP

Para consultar la configuración TCP/IP en Windows, no es necesario acceder a todas las ventanas donde se establecen los parámetros relacionados. En su lugar, se puede utilizar el comando `IPCONFIG /ALL` o la utilidad `WINIPCFG` (sólo para versiones Windows 9x) para consultar de forma resumida los parámetros actuales de la red en el equipo. Hay que tener en cuenta que esta utilidad solamente sirve de consulta rápida y no permite realizar modificaciones en la configuración de la red.

La herramienta **panel de control** que va incluida en todas las versiones de Microsoft Windows también resulta muy útil para diagnosticar averías del adaptador de red. Gracias a esta herramienta, se puede consultar el valor de interrupción asignado al dispositivo y así comprobar si entra en conflicto con algún otro dispositivo instalado (es decir, utilizan la misma interrupción).

Por su parte, en los sistemas GNU/Linux, la forma más sencilla y directa de obtener la configuración de red de los adaptadores instalados es a través del comando `ifconfig`. Si se indica sin parámetros, muestra la configuración de red de todos los adaptadores instalados. Por el contrario, si se indica el nombre de un adaptador de red, entonces mostrará la configuración de éste exclusivamente.

5.1.4 Realización de pruebas de conexión

La forma más sencilla de comprobar si la configuración de red de un equipo funciona correctamente es enviando mensajes hacia otros equipos para comprobar si estos llegan correctamente. Una forma de conseguir esto consiste en enviar mensajes de tipo ICMP eco y esperar a recibir un mensaje de respuesta. Estos mensajes se pueden enviar con el comando `ping`, aunque hay que tener en cuenta que por seguridad algunos equipos o dispositivos de interconexión pueden tener desactivada la opción de responder a este tipo de mensajes.

Cuando se utiliza una herramienta de envío de mensajes de eco como `ping` 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.

Para probar el funcionamiento del enlace también se pueden enviar otros tipos de mensajes de otros protocolos de comunicación. Algunos de ellos permiten incluso obtener estadísticas sobre el tiempo que tardan en alcanzar el destino.

5.1.5 Interpretación de respuestas

Cuando se envían mensajes ICMP eco a otro equipo a través del comando `ping`, éste muestra en pantalla información que puede ayudar a determinar si el enlace está operativo o no. Los tipos de errores que pueden aparecer son los siguientes:

- **Destino no alcanzable**: se notifica cuando no se encuentra el destino. El destino puede ser una red, un equipo, un protocolo o un puerto.
- **Problema de parámetro**: se envía cuando se detecta que existe un valor ilegal en un campo de la cabecera del mensaje.
- **Redireccionamiento**: se notifica cuando un encaminador detecta que el mensaje que ha recibido no debería haber llegado por esa ruta.
- **Tiempo excedido**: se envía cuando un mensaje ha sobrepasado su tiempo, de vida máximo y ha sido descartado. Puede deberse a bucles, congestionamientos en la red o a la inadecuada configuración del tiempo de espera en las respuestas.
- **Supresión de origen**: se utilizaba en versiones antiguas del protocolo para indicar a un equipo que no envíe más mensajes, lo que permitía realizar control de flujo. Los protocolos actuales que realizan control de flujo en TCP/IP están definidos a nivel de transporte.
- **Petición de encaminador**: es un mensaje enviado a la dirección de difusión 255.255.255.255 cuando el equipo comprueba que no existe el encaminador cuya dirección ha sido establecida en la ruta por defecto (default).
- **Descubrimiento de encaminador**: es un mensaje que envían los equipos cuando no disponen de una ruta definida por defecto (default) o ésta no existe. Los equipos que están en esta situación envían un mensaje ICMP a la dirección de difusión 224.0.0.2 para intentar que algún encaminador conteste y establecerlo como ruta por defecto.

Además de estos tipos de errores, el comando ping muestra información sobre el tiempo que tarda el destino en volver una respuesta al mensaje enviado. Si este tiempo es excesivamente elevado, entonces es posible que la instalación o configuración de la red o de los equipos no se haya realizado correctamente.

5.2 PROCEDIMIENTOS SISTEMÁTICOS DE VERIFICACIÓN Y PRUEBA DE ELEMENTOS DE CONECTIVIDAD DE REDES LOCALES

Cuando se instala y configura un equipo o un dispositivo de interconexión de red, las comprobaciones que hay que realizar para verificar su funcionamiento son las siguientes:

- Controlador: comprobar que éste es adecuado al adaptador de red instalado y ha sido cargado por el núcleo del sistema de forma correcta.
- Posibles conflictos entre el adaptador de red y el ordenador: dirección de memoria, interrupciones, etc.
- Conexión física del adaptador con la red (cableada o inalámbrica): velocidad de transmisión, control de flujo, cifrado, etc.
- Configuración de los parámetros de la arquitectura de red: dirección, máscara, puerta de enlace, etc.
- Pruebas de envío de mensajes entre los equipos: envío de mensajes ICMP eco para verificar el envío de mensajes entre los equipos.