Solo cuando se han descartado problemas en los niveles más bajos de la arquitectura de la red es cuando se puede proceder a verificar el funcionamiento del nivel de red de la arquitectura. De esta forma, se puede alcanzar la solución del problema de una manera mucho más segura sin que se quede nada por comprobar. Este capítulo está dedicado a explicar la forma de solucionar muchos de los problemas que se pueden producir en los protocolos de nivel de red. En este capítulo se introducen algunos problemas comunes que afectan a redes de comunicaciones, las causas que los provocan y las acciones que hay que emprender para solucionarlos.

Las empresas que hacen uso hoy en día de servicios de redes de comunicaciones no pueden permitirse las situaciones de avería o mal funcionamiento, ya que esto puede suponer grandes pérdidas económicas o desconfianza por parte de los clientes. Por ello, las tareas de mantenimiento y resolución de averías son de vital importancia.

Otra característica que define a las redes de comunicaciones de hoy en día es su gran complejidad, debida a la gran cantidad de servicios que integran y al elevado número de usuarios a los que dan soporte. Por ello, las tareas de administración y localización de averías se vuelven muy complejas y deben recaer en equipos de administradores bien cualificados.

Las averías en una red de comunicación pueden aparecer de muchas formas. Pueden ser problemas que afecten a una gran cantidad de usuarios (por ejemplo, la caída de un servidor) o problemas más puntuales (por ejemplo, un usuario ha perdido su acceso a la red). Cada problema puede tener una o varias causas, lo que puede hacer difícil encontrarlas.

Una vez que se ha identificado la causa o causas que producen el problema, es necesario actuar mediante la realización de una o varias acciones. Estas acciones pueden involucrar varios departamentos de la empresa e incluso las acciones a emprender pueden suponer la parada momentánea de la red de comunicación.

Debido a la complejidad en la resolución de algunos problemas, resulta mucho más eficiente utilizar un método bien definido para actuar en vez de ponerse directamente a teclear comandos o conectar el comprobador de red en los enlaces. Un método estructurado permite aprovechar mejor el tiempo y evita que los problemas puedan complicarse más de lo que ya lo están.

Un método estructurado que puede facilitar la resolución de problemas puede ser el siguiente. Hay que tener en cuenta que cada sistema de comunicaciones tiene sus peculiaridades, por lo que este método tendrá que ser adaptado y concretado a la red sobre la que estamos trabajando. Los pasos básicos que se deberán seguir son los siguientes:

1. Establecer de una forma clara y general cuál es el problema y los síntomas del mismo. A partir de estos datos, describir todas las posibles causas que pueden haber producido esos síntomas.
2. Recopilar toda la información posible sobre la situación que se está produciendo. Para ello, hay que entrevistarse con todas las personas que trabajan en ese sistema, tanto usuarios como administradores. También hay que utilizar herramientas que nos permitan obtener información de cómo está funcionando el sistema, como analizadores de red, comprobadores, utilidades de verificación, etc.
3. De toda la información recopilada en el paso anterior, obtener una lista de los problemas que pueden producirse, eliminando aquellos que no guardan relación con esos hechos. De este modo, nos podemos centrar en los problemas que realmente tienen relevancia.
4. Establecer un plan de acción para afrontar los problemas que se han establecido en el paso anterior. Hay que comenzar tratando el problema que tenga más posibilidades de ser la causa del funcionamiento erróneo.
5. Realizar todas las acciones establecidas en el paso anterior, de forma ordenada y comprobando que los síntomas desaparecen.
6. En caso de que los síntomas no desaparecieran, habría que volver al paso 4 para elaborar otro plan de acción basado en el siguiente problema establecido.

Para facilitar las tareas de resolución de problemas, el administrador o administradores deberán estar preparados para ello. Se recomienda lo siguiente:

- Mantener un mapa actualizado de la red, donde se especifique la topología y las direcciones de los equipos y dispositivos de interconexión.
- Disponer de una lista de los protocolos que funcionan en la red, indicando aquellos que se incluyen en el encaminamiento.
- Mantener una lista de todas las direcciones y puertos que son accesibles desde el exterior, y si se encuentra algún equipo de la red interna en la lista del protocolo NAT.
- Guardar información sobre la configuración de los servidores de la red, los servicios que tienen instalados y los recursos compartidos.
- Mantener información sobre los problemas que han surgido en la red y los métodos que se han utilizado para solucionarlos. De este modo, se pueden solucionar problemas que ya han ocurrido de una forma mucho más rápida.

En una red informática es recomendable que exista un **NOC** (Network Operations Center o Centro de Operaciones de la Red). Este centro puede ser tan simple como un ordenador o tan complejo como una infraestructura completa de red y se encarga de monitorizar y gestionar la red. Este sistema mantiene información sobre:

- **Estado actual de la red**: contiene un inventario sobre la topología de la red, los elementos que están instalados, cómo están conectados, dónde están ubicados, su historial de cambios y problemas y su estado operacional.
- **Servicios**: incluye un registro de los servicios disponibles en la red y su ubicación.
- **Configuración de dispositivos**: se trata de la información completa relativa a la configuración de los equipos de la red. Puede incluir también archivos que contienen la configuración de los dispositivos, que pueden ser volcados sobre ellos cuando hay problemas.
- **Estadísticas**: se guarda información estadística sobre el funcionamiento de la red, una información que se obtiene a través del uso de programas de monitorización.

9.1 HERRAMIENTAS DE COMPROBACIÓN

Hoy en día, muchos fabricantes de dispositivos de interconexión de redes ofrecen aplicaciones software de monitorización de red que distribuyen con sus productos. Aunque la mayoría de ellos difieren en la forma de utilizarlos o en las opciones que incluyen, todos comparten el mismo fin: ofrecer aplicaciones que muestren al administrador el estado de la red, estadísticas de actividad, configuración remota de dispositivos, etc.

Una herramienta muy importante que se puede utilizar para analizar el tráfico en una red de comunicación para encontrar sobrecargas y tiempos de espera excesivos es `ntop`. Esta herramienta se instala en los sistemas Linux y se configura como un proceso residente. Para mostrar la información que obtiene este proceso, se utiliza un navegador Web. Gracias a esta herramienta, el administrador puede obtener información sobre la cantidad de tráfico que intercambian las estaciones, el tráfico pesado, los servicios más utilizados, etc. De esta forma, se puede obtener un mapa de tráfico que nos puede ayudar a comprender cuáles son las aplicaciones de comunicación más demandadas en nuestra red y actuar para redistribuir esas cargas.

Todas estas herramientas no solamente sirven para monitorizar el estado de la red y localizar posibles averías, sino que también permiten elaborar una documentación detallada sobre nuestro sistema de comunicación. Gracias a ello, los administradores pueden facilitar su trabajo al disponer de información actualizada sobre el sistema que tienen que reparar.

Un ejemplo de herramienta de análisis de tráfico que se distribuye gratuitamente con las distribuciones GNU/Linux es Ethereal.

En los sistemas GNU/Linux está disponible una herramienta de captura de tráfico de paquetes TCP/IP denominada `tcpdump`. La sintaxis y uso de este programa se puede consultar en la bibliografía recomendada o en las páginas de la orden `man`.

Los dispositivos encaminadores también pueden disponer de algunas herramientas de comprobación de estado y diagnóstico, dependiendo del modelo y fabricante. Estas utilidades se pueden dividir en varias categorías:

- **Utilidades de consulta de estado**: muestran el estado actual de funcionamiento del dispositivo.
- **Utilidades de comprobación de las líneas**: indican cuál es el estado de las líneas, es decir, si hay conexión o no.
- **Utilidades de monitorización**: se utilizan para comprobar el funcionamiento del dispositivo y si sus protocolos están actuando de una forma correcta.

La forma de usar estas herramientas depende del fabricante y del modelo del dispositivo. Por ejemplo, en el caso de los encaminadores del fabricante Cisco Systems, estas utilidades se plasman en comandos que se ejecutan desde un terminal remoto, como `show` (para comprobar el estado), `ping` y `traceroute` (para comprobar si hay comunicación con otro equipo), `debug` y `trace` (para monitorizar el funcionamiento del dispositivo). En otras ocasiones, estas utilidades son accesibles desde las páginas de configuración que se muestran desde un navegador de **hipertexto** (**html**).

Una herramienta de monitorización del tráfico de red que es ampliamente utilizada, gracias a que se distribuye libremente bajo licencia GPL, es WireShark.

9.2 DETECCIÓN DE PROBLEMAS

En los apartados siguientes se explican los métodos para detectar y corregir problemas comunes de los protocolos a nivel de red.

9.2.1 Tramas largas y cortas

En una red local, los paquetes a nivel de red son encapsulados dentro del campo de datos de una trama para su transporte al destino. Dependiendo del tamaño del paquete de red, la trama resultante puede tener también un tamaño mayor o menor.

Los inconvenientes de transmitir tramas demasiado cortas por la red son:

- El número de mensajes que circulan por la red aumenta y, por lo tanto, puede aumentar la congestión de la red.
- Los equipos necesitan procesar una mayor cantidad de información de control para la misma cantidad de información a transmitir.

Por su parte, los inconvenientes de transmitir tramas demasiado largas son:

- Necesitan ser transmitidas en un intervalo de tiempo mayor, por lo que los equipos necesitan esperar un poco más antes de transmitir.
- Si una trama se pierde por un error o una colisión, hay que volver a transmitirla por completa.

Por todos estos argumentos, siempre se recomienda transmitir tramas que no sean ni excesivamente cortas ni excesivamente largas. Para ello, los protocolos de nivel de red deben estar preparados para entregar al nivel de enlace paquetes con un tamaño adecuado.

9.2.2 Tráfico excesivo

La detección de excesivo tráfico en una red local se puede realizar a través de una herramienta de análisis de tráfico. También se puede determinar que una red local está soportando una carga de tráfico excesiva si se producen muchas colisiones. Estas colisiones también se pueden detectar con una herramienta de análisis o verificando el tiempo que permanece encendido el indicador luminoso de colisión que incorporan algunos adaptadores de red. Se considera que el número de colisiones es elevado si se supera el 0,1% con respecto al número de mensajes enviados.

Cuando se llega a la conclusión de que el tráfico en la red local es excesivo, hay que determinar desde dónde procede ese tráfico y hacia dónde va dirigido. Definiendo un mapa del tráfico que soporta la red (este mapa lo hacen muchas herramientas de análisis de tráfico de forma automática) se pueden diseñar los cambios necesarios para distribuir el tráfico de una forma mucho más equitativa, estableciendo rutas alternativas o segmentando la red a través de la instalación de nuevos conmutadores.

9.2.3 Netware

En las redes Novell Netware es posible que nos encontremos con problemas a la hora de comunicar los equipos o acceder a los recursos compartidos. Estos problemas pueden estar ocasionados por las siguientes causas:

- La configuración de red de los equipos o del servidor no es correcta.
- Los dispositivos de interconexión de red están filtrando el tráfico NetWare y éste no está llegando a los destinatarios.
- Los permisos asignados a los recursos compartidos no son correctos.

9.2.4 TCP/IP

Los problemas más comunes en las redes locales a nivel de red suelen estar relacionados con unos parámetros incorrectos de TCP/IP, que es el protocolo de red más utilizado por la mayoría de las arquitecturas. Estos parámetros son:

- Dirección IP y máscara de red.
- Encaminamiento (direcciones de los encaminadores de destino y encaminador o pasarela por defecto).
- Direcciones de los servidores DNS para resolver las direcciones.

9.2.5 Configuración del host

Un administrador de red debe tener mucho cuidado a la hora de establecer la configuración de todos los equipos y los dispositivos de interconexión. Las reglas básicas que se deben seguir son:

- Establecer una dirección única para cada equipo en la red o asegurarse de que cada equipo obtiene una dirección única por DHCP.
- Evitar asignar direcciones dinámicas (por DHCP) a equipos que van a funcionar como servidores, de la misma forma que los dispositivos de interconexión de la red.
- Si los equipos reciben su configuración de red de forma automática (por DHCP), comprobar que todos los parámetros asignados son correctos.
- Establecer el mismo número de red y la misma máscara para todos los equipos que se encuentren conectados en la misma red (y no tengan un encaminador intermedio).

9.2.6 Resolución de nombres

En las redes locales donde se utiliza el servicio de resolución de nombres para acceder a los recursos disponibles (ya sea a través de DNS o WINS), es fundamental que éste funcione correctamente o de lo contrario los usuarios no van a poder usar esos recursos.

El correcto funcionamiento de los servidores DNS de la red resulta vital para los usuarios que los manejan. Aunque se trata de un servicio que se limita a resolver correspondencias entre nombres y direcciones IP, hay que tener en cuenta que los usuarios trabajan con nombres de equipos y muchos servicios de red utilizan el DNS para funcionar. Por ejemplo, el uso de un programa navegador de Internet requiere del sistema DNS porque los usuarios están acostumbrados a introducir direcciones de dominio y no saben lo que es una dirección IPv4 o IPv6.

La mejor forma de comprobar si el servidor DNS está funcionando correctamente es a través de las órdenes `nslookup` o `dig`. Los errores que devuelven estas órdenes pueden ser:

- Timed out (Tiempo de espera agotado): se produce cuando el servidor no responde a una solicitud y varios reintentos en el tiempo establecido. Puede ser debido a que el servidor esté saturado, sea inaccesible o existan problemas de conectividad en la red.
- No response from server (no hay respuesta del servidor): se produce cuando el servidor, aunque está funcionando, no tiene activo el servicio DNS.
- No records (no hay registros): se devuelve este mensaje cuando no hay información en el servidor DNS para el tipo de consulta realizada.

- Non-existen domain (dominio no existente): se utiliza para indicar que el equipo especificado o el dominio para el que está intentando resolver la dirección IP no existe.
- Connection refused (conexión rechazada): se produce cuando no se puede realizar conexión con el servidor para realizar la consulta.
- Server failure (fallo en el servidor): se notifica cuando el servidor encuentra una inconsistencia en su base de datos y no puede devolver una respuesta válida. Se recomienda repasar los archivos de configuración en el servidor.
- Refused (rechazado): se produce cuando el servidor DNS rechaza la consulta, una situación que puede producirse cuando se han limitado las consultas por cuestiones de seguridad.
- Format error (error de formato): esta notificación es enviada por el servidor cuando detecta que el mensaje de solicitud no tiene el formato correcto, por lo que el problema se puede encontrar en la orden `nslookup` o en la consulta realizada por el usuario.

Si se usa la resolución WINS, la mejor herramienta de comprobación de este servicio es `NET`.

9.2.7 NetBIOS

En los sistemas Microsoft Windows, el acceso a los recursos compartidos (carpetas, impresoras, etc.) se lleva a cabo a través de los protocolos de la red Microsoft, que se configuran a través de los parámetros NetBIOS. Si se produce algún error en el acceso a los recursos compartidos, hay que comprobar si el nombre del equipo o del recurso son correctos o si el usuario y el equipo tienen permisos de acceso a esos recursos. También hay que comprobar la configuración correcta del nombre del equipo, el grupo de trabajo o el dominio. Hay que tener en cuenta que en las versiones Windows 2000/2003/2008 Server no se utiliza la configuración de nombre de equipo y dominio (o grupo de trabajo) cuando estos funcionan como controladores primarios de dominio.

9.2.8 Conexión al servidor http o proxy

La forma de resolver problemas relacionados con el acceso a un servicio depende del servicio en sí. Por ejemplo, cuando es imposible consultar una página html de un servidor remoto entonces puede ocurrir que falle el encaminamiento o que el protocolo DNS no resuelva la dirección.

Todos los servicios de red que ofrece un sistema están relacionados con uno o varios puertos de transporte. Por lo tanto, el primer paso a la hora de encontrar las causas consiste en comprobar si los puertos correspondientes están abiertos. Aunque el programa que gestiona el servicio esté funcionando perfectamente en el servidor, es posible que el puerto asociado esté bloqueado por otro programa, por ejemplo, un cortafuegos o un programa antivirus.

9.2.9 Conexión al servidor de correo

Cuando un equipo no puede acceder a los servicios de correo disponibles en un servidor, puede ser debido a varias causas:

- Existen problemas en la red que hacen que los mensajes no lleguen al servidor o no sean recibidos por la estación de trabajo.
- El servidor no funciona correctamente o no recibe los mensajes de los clientes por alguna razón (puertos bloqueados, cortafuegos, etc.).
- El programa cliente de correo no está bien configurado o los protocolos no están funcionando correctamente (habitualmente, POP3 e IMAP).
- Los parámetros especificados de la cuenta de correo no son válidos (hay que revisar el nombre de usuario y la contraseña de acceso).

9.2.10 Conexión al servidor de impresión

El acceso a impresoras compartidas o de red también puede ser una fuente de problemas para los administradores. Cuando no se puede usar una impresora compartida en otro equipo puede ser debido a:

- La dirección NetBIOS de la impresora no es correcta (*equipo**impresora*).
- Hay algún problema con la conexión o configuración de red del equipo.
- Los controladores de la impresora no están instalados correctamente.
- La impresora está bloqueada debido a un problema o el atasco del papel.
- La cola de la impresora está bloqueada con algún trabajo pendiente.

Por su parte, cuando los problemas vienen de no poder utilizar una impresora de red, estos pueden ser debidos a:

- Hay algún problema con la conexión de red de la impresora.
- La configuración de red de la impresora no es correcta.
- La dirección de red de la impresora no es correcta.
- No se está enviando el trabajo a través del puerto adecuado (TCP/IP, SmartDevice, etc.).
- La impresora está bloqueada debido a un problema o al atasco del papel.
- La cola de la impresora está bloqueada con algún trabajo pendiente.

9.2.11 Otros

Otros problemas que pueden hacer que el rendimiento de la red sea pobre pueden ser:

- Gran cantidad de tramas erróneas: este caso se produce cuando los programas de análisis y monitorización de la red detectan una gran cantidad de mensajes incorrectos, sin que se produzcan demasiadas colisiones. Este caso puede ser producido por un error de la configuración dúplex de los puertos. También puede ser debido a una gran cantidad de ruido, en cuyo caso se recomienda comprobar:
  - Si los cables están dañados.
  - Si los cables se han instalado demasiado próximos a cables eléctricos o fuentes de ruido.
  - Si la categoría de cableado es inferior a 5 y la red trabaja a 100 Mbps.
- Gran cantidad de colisiones: este problema se produce cuando el número de colisiones con respecto al número de mensajes enviados supera el 0,1%. Para comprobar este valor, se pueden utilizar las herramientas de análisis de tráfico o comprobando los indicadores luminosos de las tarjetas de red de los equipos (normalmente esta última opción suele resultar más engorrosa y menos fiable para el administrador). Para solucionar este problema se pueden utilizar dispositivos conmutadores para segmentar la red.
- Gran cantidad de mensajes duplicados: este problema puede ser causado por una gran cantidad de colisiones, por lo que se recomienda realizar las comprobaciones pertinentes para ese caso. Si no existen problemas de colisiones, entonces lo más probable es que los mensajes tarden demasiado tiempo en llegar a su destino por problemas de congestión de los enlaces o exista algún adaptador de red que no funcione correctamente.
- Colisiones tardías: se producen cuando la colisión no afecta a los primeros 64 bytes del mensaje enviado. Para detectar esta situación hay que utilizar un programa de análisis de red. En teoría, en una red bien diseñada nunca deberían producirse este tipo de colisiones, ya que las estaciones deben comprobar el medio antes de transmitir. Estas situaciones pueden ser debidas a instalaciones con cables demasiado largos o existencia de demasiados repetidores conectados en cascada. Para comprobar estas situaciones hay que consultar las especificaciones establecidas por los estándares de cableado estructurado.