Diagnóstico y resolución de problemas en entornos de red TCP/IP

PARTE I

Prof. Dr. Javier Areitio Bertolín

E. Mail: jareitio@orion.deusto.es Director del Grupo de Investigación Redes y Sistemas.ESIDE.
Facultad de Ingeniería. Universidad de Deusto (UD).

Este artículo analiza diversas herramientas y procedimientos simples para diagnosticar patologías en un Entorno de Comunicación de Red Internet/Intranet, permitiendo identificarlos y elegir la opción de resolución disponible más adecuada.

CLASIFICACIÓN DE LA SINTOMATOLOGÍA DE PATOLOGÍAS EN ENTORNOS DE RED TCP/IP

Las principales categorías de síntomas identificables en entornos de comunicación que utilicen la pila/arquitectura de protocolos TCP/IP son:

1) Problemas de Conectividad Física. Son problemas que se refieren al hardware con el que se forma Internet/Intranet. Puede ser causado por ejemplo por un cable roto, una tarjeta de red (o NIC, Network Interface Card) o de router con fallos, un cable inadvertidamente sacado de su conector, etc..

2) Problemas del Hardware del Computador (o "host") Remoto. El computador específico al que el usuario intenta alcanzar puede tener algún fallo, puede estar en proceso de arranque (o "booting"), o puede estar temporalmente sobrecargado u otro tipo de indisponibilidad.

3) Problemas de Configuración Software del Computador Remoto. Puede existir un problema con la configuración software del computador remoto que impide que pueda estar disponible un servicio específico.

4) Problemas de Configuración Software del Computador Local. Puede existir un problema con la configuración software del computador local que impida a éste local alcanzar al computador remoto.

5) Problemas de Configuración de Encaminamiento. Las tablas de encaminamiento en uno o más computadores y/o routers de la red TCP/IP puede contener información no válida o bien uno o más routers pueden haber fallado.

6) Problemas de Resolución de Nombres. El nombre del computador especificado en un comando puede haberse escrito mal, los ficheros de "hosts" o las bases de datos del servidor de nombres pueden estar mal configuradas o bien uno o más servidores de nombres pueden haber fallado imposibilitando que pueda realizarse la resolución de nombres.

HERRAMIENTAS SENCILLAS DE DIAGNÓSTICO Y RESOLUCIÓN DE PROBLEMAS EN ENTORNOS INTERNET/INTRANET

Las principales herramientas disponibles en la mayoría de las implementaciones TCP/IP actuales son:

1) Comando "ifconfig". Comprueba el interface a la red física y nos dice si la NIC del computador local se encuentra operativa y si el software del computador local puede acceder a la NIC.

2) Comando "ping". Este comando referencia al computador remoto por su dirección IP o por su nombre, nos dice si el computador remoto es alcanzable actualmente. Nos proporciona una estadística de mensajes de petición de eco y de respuesta de eco.

3) Comando "traceroute". Visualiza la información relativa a la ruta a lo largo de la cual los paquetes están viajando para llegar al computador remoto/destino. Al igual que el comando "ping" puede referenciar al computador remoto por su dirección IP o por su nombre (por ejemplo, nombre = orion.deusto.es tiene como dirección IP = 130.206.100.1).

4) Comando "arp". Visualiza los contenidos de la memoria cache ARP del computador local y nos dice si existe una entrada en la cache ARP del computador local para un router por defecto.

5) Contenido de Ficheros de Configuración Locales. La mayoría del software de comunicaciones TCP/IP mantiene un conjunto de ficheros de configuración que contienen información importante relativa a las opciones de comunicación de TCP/IP. Los contenidos de estos ficheros a veces pueden utilizarse para indicar la fuente de los problemas. Tres ficheros de configuración importantes son: (a) Fichero de "hosts". Este fichero es importante en entornos TCP/IP pequeños donde DNS no se utiliza para la resolución de nombres. El fichero "hosts" contiene una lista de correspondencias de nombre a dirección al que el host (o com-

putador) local tiene acceso. Generalmente puede ser inspeccionado y cambiado utilizando un editor de texto convencional para añadir correspondencias de nombre a dirección cuando se añaden computadores (o hosts) a un entorno de red TCP/IP. Si los ficheros de "hosts" locales se utilizan para la resulución de nombres, se pueden visualizar los contenidos del fichero "hosts" en el computador local para ver si contiene las entradas adecuadas.

6) Comando "nslookup". Si el Sistema de Nombres de Dominio (ó DNS, Domain Name System) se utiliza para la resolución de nombres, el comando "nslookup" nos dice si DNS puede resolver el nombre del computador que es contactado. El comando "nslookup" posee un modo prolijo que manda visualizar la información sobre cada paso en el proceso de resolución de nombres.

7) Comando "netstat". Visualiza estadísticas relativas a la actividad de la red que se refieren al computador local. El comando "netstat" visualiza normalmente información sobre el computador local relativa al estado de todas sus conexiones TCP/IP e interfaces de red, los contenidos de su tabla de encaminamiento, estadísticas relativas al proceso de encaminamiento y estadísticas que se refieren a los protocolos TCP/IP.

8) Software de Gestión de Red SNMP. Si la red TCP/IP utiliza herramientas de gestión de red que emplean SNMP, éstas pueden utilizarse para localizar problemas de todos los tipos en Internet/Intranet. Los procedimientos específicos que se utilizan que se refieren a herramientas SNMP son específicos de la implementación.

9) Monitores de Red. Si el entorno Internet utiliza monitores de red software o hardware, éstos pueden emplearse para localizar problemas. Los procedimientos específicos empleados que se refiere a monitores de red son específicos de la implementación. En entornos TCP/IP de grandes dimensiones se pueden utilizar monitores de red especializados que vigilen y produzcan diversos tipos de estadísticas durante el funcionamiento de las comunicaciones. Los monitores de red, pueden ser software que se ejecuta en uno o más computadores de la red o bien dispositivos hardware (denominados "probes") especializados que se conectan a la red de la misma forma que los computadores. La información que pueden visualizar los monitores de red la pueden utilizar los administradores de red para vigilar las posibles fuentes de problemas de red.

DIAGNÓSTICO DE ERRORES/FALLOS/ANOMALÍAS

Cuando suceden problemas en un entorno de comunicaciones de red TCP/IP, nuestro computador local normalmente genera un mensaje de error cuando intenta acceder a los servicios existentes sobre un computador remoto. Esto normalmente ocurre cuando se ejecuta un comando como "telnet" o "ftp" dirigido hacia un computador remoto. Existen varios tipos de mensajes de error que el software de comunicaciones TCP/IP genera, que contabiliza la mayor parte de las situaciones de error que pueden ocurrir al intentar acceder a un computador remoto: (1) Servicio Desconocido. (2) Protocolo Desconocido.

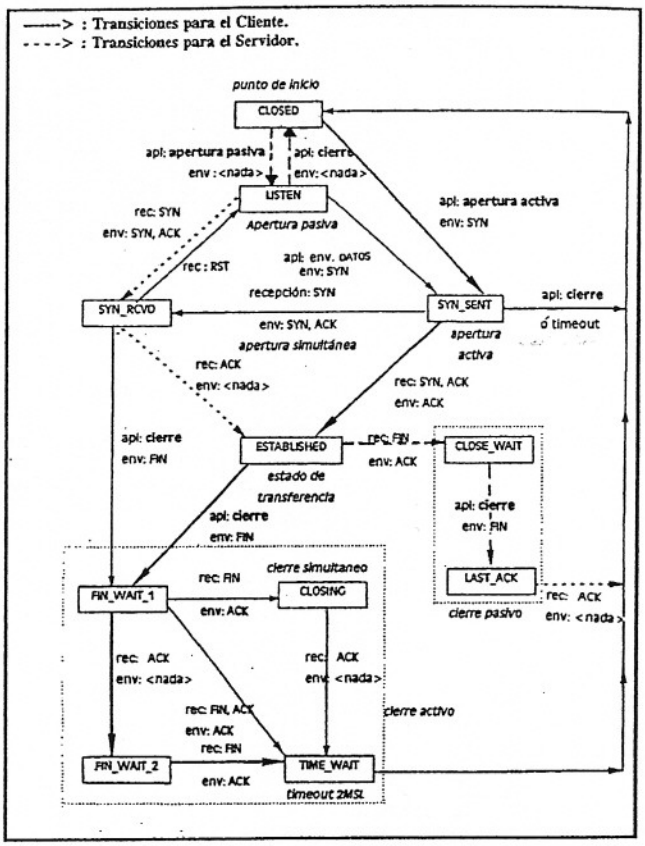

Figura 1.- Esquema del Autómata de Transición de Estados del Protocolo de Transporte TCP

(3) Red No alcanzable. (4) Computador No alcanzable. (5) Expiración o time-out de la conexión. (6) Conexión Rechazada/Denegada. (7) Computador Desconocido.

ANÁLISIS DE MENSAJES: SERVICIO DESCONOCIDO, PROTOCOLO DESCONOCIDO

Si se reciben mensajes de servicio desconocido o de protocolo desconocido, el problema es casi seguro que se deba a la configuración software de computador local. Por ejemplo, un fichero "protocols" o "services" que necesita el software de comunicaciones TCP/IP puede no estar en el directorio apropiado. El siguiente es un ejemplo de un mensaje de error de "servicio desconocido": $ telnet sirio —> telnet: service unknown. Cuando se reciba un mensaje de error de servicio desconocido o protocolo desconocido, verificar que el software de comunicaciones TCP/IP se ha instalado bien en el computador local y que se han elegido las opciones de configuración correctas que se refieren al servicio o protocolo que se intente utilizar.

DIAGNÓSTICO DE PROBLEMAS DE CONECTIVIDAD. ANÁLISIS DE MENSAJES: RED NO ALCANZABLE, COMPUTADOR NO ALCANZABLE, EXPIRACIÓN DE LA CONEXIÓN

Si se recibe un mensaje de red no alcanzable, de computador no alcanzable o de conexión "time-out", pro-

bablemente estaremos frente a un problema de conectividad. Un ejemplo de mensaje de error de computador no alcanzable es: $ telnet orion ——> Trying 130.206.100.1 ... ——> telnet: connect: Host is unreachable. Para diagnosticar un problema de conectividad se pueden seguir los siguientes pasos:

1) Ejecutar el comando "ifconfig" para asegurarse que la NIC del computador local esta operativa y que el software del computador local puede acceder a ella. Esto verifica que la NIC no tiene fallos y que el software esta adecuadamente configurado.

2) Ejecutar el comado "netstat" para verificar que el interface local a la red TCP/IP opera correctamente.

3) Si la NIC funciona bien, ejecutar el comando "ping", dando la dirección IP propia del computador local o la dirección de "loopback" 127.0.0.1. Si esto falla, el problema de nuevo es local. Verificar que el software del computador local se encuentre bien configurado.

4) Una vez que se ha determinado que el problema probablemente no es del computador local, a continuación, se ejecuta el comando "ping" dirigido al computador remoto utilizando el nombre. Si esto tiene éxito, entonces el computador remoto es alcanzable y el problema probablemente esté en la configuración del software del computador remoto. Contactar con el administrador del computador remoto para determinar la fuente del problema.

5) Si el computador remoto no puede ser alcanzado con el comando "ping" utilizando el nombre, el siguiente paso depende de si se conoce la dirección IP del computador remoto. La dirección del computador remoto puede conocerse debido a un contacto anterior, o bien puede utilizarse el comando "nslookup" para determinar su dirección IP. Si la dirección del computador remoto se puede determinar, ejecutar el comando "ping" dirigido al computador remoto utilizando dicha dirección. Si el computador remoto es alcanzable empleando la dirección y no el nombre o si no es posible determinar la dirección del computador remoto utilizando el comando "nslookup", entonces el problema probablemente se refiera a la resolución de nombres. Continuar aplicando los pasos utilizados en el "diagnóstico de los problemas de resolución de nombres".

6) Si el computador remoto no puede alcanzarse con el comando "ping" utilizando la dirección, el problema probablemente sea fallo del mecanismo de encaminamiento. Ejecutar el comando "traceroute", identificando el computador remoto por su nombre o dirección, para determinar la ruta sobre la que los paquetes viajan al computador remoto. Si el comando "traceroute" aisla el problema en un router específico, contactar con el administrador de ese router para resolver el problema. Si el comando "traceroute" no está disponible en el computador local, y se conocen las direcciones de los routers, utilizar el comando "ping" para determinar la alcanzabilidad hacia todos los routers que existen en el camino entre el computador local y el computador remoto en un intento de localizar el router con fallo.

ANÁLISIS DE MENSAJES: CONEXIÓN RECHAZADA

Si se recibe un mensaje de conexión rechazada cuando se trata de pedir un servicio de un computador remoto, es probable que el computador local haya conseguido comunicarse con el computador remoto, pero éste no acepta una petición de establecimiento de una conexión entre un proceso del computador local y un proceso del computador remoto. En tal situación, podemos en primer lugar tratar de ejecutar el comando varias veces, por ejemplo esperando un minuto entre reintentos. Cuando un servidor remoto rechaza aceptar conexiones, posiblemente se deba a que el servidor simplemente se encuentre sobrecargado y es incapaz temporalmente de aceptar conexiones adicionales. También es posible que el servidor no se encuentre configurado para suministrar el servicio pedido o que no estemos autorizados para pedir ese servicio en ese servidor particular, quizás por razones de seguridad ("control de acceso"). Si el problema persiste, se debería contactar con el administrador del computador destino para determinar la causa real del problema.

PROCEDIMIENTOS DE DIAGNÓSTICO DE LOS PROBLEMAS DE RESOLUCIÓN DE NOMBRES. ANÁLISIS DE MENSAJES: COMPUTADOR DESCONOCIDO

Si se recibe un mensaje de computador desconocido, es probable que el computador local no pueda obtener la correspondencia nombre a dirección IP para el computador remoto que tratamos de contactar. Utilizar el procedimiento adjunto para diagnosticar problemas de resolución de nombres a la hora de tratar de determinar la causa del problema. El procedimiento de diagnóstico de problemas de resolución de nombres es :

1) Verificar si el nombre del computador remoto esté bien escrito.

2) Si el nombre es correcto, el siguiente paso depende de si se utiliza para la resolución de nombres los ficheros "hosts" o el sistema DNS. Si se utiliza un fichero de "hosts" local, el problema probablemente este causado por la falta de una entrada en el fichero de "hosts" para el computador remoto. El fichero de "hosts" local debería actualizarse para incluir una entrada para ese computador.

3) Si se utiliza DNS, comprobar la configuración del software local para asegurar que el computador local pueda contactar con un servidor de nombres. La dirección IP de un servidor de nombres normalmente se almacena en un fichero de configuración local.

4) Si el fichero de configuración apropiado para el computador local apunta a un servidor de nombres, ejecutar el comando "ping" hacia ese servidor de nombres para asegurarse que sea alcanzable. Si esto falla, contactar con el administrador del servidor de nombres para resolver el problema.

5) Si el servidor de nombres puede ser alcanzado desde el computador local, es posible que el software del ser-

vidor de nombres no funcione en el computador del servidor de nombres. Si el software no funciona, el problema puede resolverse instalando el software del servidor de nombres en el computador del servidor de nombres.

6) Si el software del servidor de nombres funciona en el computador del servidor de nombres, ejecutar el comando "nslookup" en modo prolijo para ver si el problema específico que se refiere al problema de la resolución de nombres puede localizarse.

POSIBILIDADES DE NETSTAT COMO HERRAMIENTA DE GESTION DE RED

Netstat es un comando que sirve como herramienta de gestión de red no tan sofisticada como un sistema de gestión de red basado en SNMP, sin embargo es de gran valor para detectar redes mal configuradas y encontrar errores de configuración no muy complejos que pueden conducir a una red inestable y no utilizable. Netstat permite visualizar información específica de computadores. Diferentes opciones se encargan de visualizar los contenidos de las tablas del sistema relativas al estado de la red que se encargan de seguir la pista del estado de las conexiones de red, de los interfaces, de las tablas de encaminamiento y de las estadísticas relativas al tráfico.

FUNCIÓN-1: MONITORIZACIÓN DE CONEXIONES.

Netstat sin ninguna opción visualiza todas las conexiones TCP y UDP actualmente activas y las conexiones activas del dominio de protocolo Unix. El dominio de protocolo Unix es una facilidad de comunicación interproceso para procesos sobre un único computador Unix. La salida por defecto del comando netstat ejecutándose sobre el computador akasha.tic.com es:

```
$ netstat
Active Internet connections
Proto  Recv-Q  Send-Q  Local Address     Foreign Address      (state)
tcp    0       4096    akasha.2684       aahsa.smtp           ESTABLISHED
tcp    0       0       akasha.1023       aahsa.login          ESTABLISHED
udp    0       0       akasha.domain     *.*
udp    0       0       localhost.domain  *.*
Active UNIX domain sockets
Address   Type   Recv-Q  Send-Q  Vnode     Conn  Refs  Nextref  Addr
ff64998c  dgram  0       0       ff0a35a80  0     0     0        /dev/log
```

Para limitar la salida sólo a las conexiones TCP y UDP activas se especifica la opción -f seguido por la palabra clave inet. La salida obtenida a la ejecución del comando netstat -f inet es:

```
$ netstat -f inet
Active Internet connections
Proto  Recv-Q  Send-Q  Local Address     Foreign Address      (state)
tcp    0       4096    akasha.2684       aahsa.smtp           ESTABLISHED
tcp    0       0       akasha.1023       aahsa.login          ESTABLISHED
udp    0       0       akasha.domain     *.*
udp    0       0       localhost.domain  *.*
```

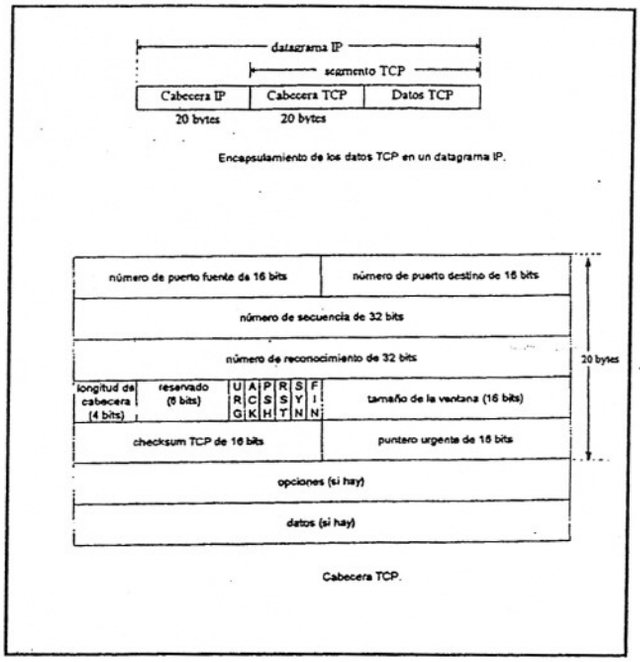

Figura 2.- Componentes de un Datagrama IP. Formato de la Cabecera del Protocolo TCP.

CAMPOS DE LA SALIDA DE NETSTAT PARA VISUALIZAR CONEXIONES ACTIVAS

Cada conexión se visualiza en una linea que comprende los siguientes campos:

1) Proto. Representa el protocolo de transporte utilizado, bien UDP o TCP.

2) Recv-Q. Representa el número de bytes en la cola de entrada del socket.

3) Send-Q. Representa el número de bytes en la cola de salida del socket.

4) Local Address. Representa la dirección del socket local, especificada como un par de nombres separados por un punto. El primer nombre es el del interface local y normalmente se visualiza como el nombre del computador local con el dominio local suprimido. El segundo es el nombre del puerto local que utiliza la conexión. Si ocurre que el puerto no tiene nombre, entonces se visualiza en su lugar el número de puerto.

5) Foreign Address. Representa la dirección del socket remoto en el mismo formato que la dirección local.

6) (state). Representa el estado actual de cada conexión TCP. Este campo se encuentra vacío para conexiones UDP.

La salida del comando netsat en el ejemplo anterior muestra el computador akasha con una conexión activa desde el puerto local 2684 al puerto 25 (SMTP) del computador aahsa. Así mismo existe una sesión rlogin activa desde el puerto local 1023 de akasha al puerto rlogin del computador aahsa. Finalmente un servidor de nombres de dominio esta escuchando paquetes en el puerto de dominio UDP tanto en el interface de red local como en el interface loopback (también demoninado localhost o 127.0.0.1). En las cone-

xiones TCP es fácil identificar qué lado de la conexión es el del servidor y cual es el del cliente. El puerto del lado del servidor es el nombre del puerto bien conocido para ese servicio, el puerto del lado del cliente es un número de puerto arbitrario que normalmente es mayor de 1023. En el ejemplo anterior el cliente SMPT local habla con el servidor SMTP remoto. Se especifica el estado de cada conexión TCP activa. Para los servicios UDP, el par remoto "host.port" se especifica como "*.*" para servicios que esperan activamente paquetes UDP desde cualquier puerto remoto. Puesto que los servicios UDP son sin conexión, un servidor UDP puede configurarse para recibir paquetes desde cualquier puerto remoto. Los nombres de los puertos bien conocidos se encuentran en el fichero /etc/services o si el NIS se encuentra activo, utilizando la correspondencia NIS obtenida del mismo fichero. Los nombres de los computadores se hacen corresponder con sus direcciones IP utilizando cualquier servicio de búsqueda dirección-nombre de computador que funcione. Las tablas internas del sistema operativo almacenan direcciones IP y números de puerto en vez de nombres de computador y nombres de puerto. El comando netstat puede traducir los números de puerto y direcciones IP a sus correspondientes nombres. Para poder ver las direcciones IP y números de puerto en vez de nombres, se debe utilizar la opción -n. Para el ejemplo anterior se obtendría:

```
$ netstat -f inet -n
Active Internet connections
Proto Recv-Q Send-Q Local Address       Foreign Address     (state)
tcp   0      4096   192.12.23.129.2684  192.12.23.130.25    ESTABLISHED
tcp   0      0      192.12.23.129.1023  192.12.23.130.513   ESTABLISHED
udp   0      0      192.12.23.129.53    *.*
udp   0      0      127.0.0.1.53        *.*
```

Si se utiliza la opción -a en el comando netstat se pueden visualizar todos los servidores que escuchan conexiones además de las conexiones activas actuales. Esta opción es una buena comprobación de la configuración de inetd, ya que la mayoría de los servicios se arrancan fuera de inetd. La salida para el ejemplo anterios será:

```
$ netstat -a -f inet
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address      Foreign Address      (state)
tcp   0      4096   localhost.1557     localhost.sunrpc     TIME_WAIT
tcp   0      0      akasha.1023        aahsa.1023.513       ESTABLISHED
tcp   0      0      akasha.login       aahsa.1023           ESTABLISHED
tcp   0      0      *.4350             *.*                  LISTEN
tcp   0      0      *.6000             *.*                  LISTEN
tcp   0      0      *.2000             *.*                  LISTEN
tcp   0      0      *.3222             *.*                  LISTEN
tcp   0      0      *.telnet           *.*                  LISTEN
tcp   0      0      *.login            *.*                  LISTEN
tcp   0      0      *.nntp             *.*                  LISTEN
```

El campo de estado de valor LISTEN indica que el servidor espera peticiones de conexión de clientes. La dirección de socket local sólo esta limitada al puerto bien conocido del servicio, mientras que "*" en el campo del computador local indica que el servicio está escuchando y aceptará conexiones de cualquiera de los interfaces de red. El campo "foreign address" (o dirección remota) siempre es "*.*". Sobre la máquina que se ejecutan los servicios RPC de Sun, el número de servidores que escuchan puede ser bastante grande, ya que la mayoría de los servicios RPC escuchan tanto sobre un puerto TCP como sobre uno UDP. Debido a que se asocian números de puerto local arbitrarios a la mayoría de servidores RPC, es difícil decir teniendo en cuenta la salida del comando netstat qué servidores RPC se están ejecutando. Sin embargo, los servidores RPC activos se pueden encontrar utilizando el comando rpcinfo. Se puede determinar si se está ejecutando el mapeador de puertos (o "portmapper") del RPC observando si algún servidor escucha en el puerto 111. La visualización de conexiones es una comprobación muy útil sobre el estado de las conexiones TCP activas.

Una conexión TCP que aparece colgada puede tener cierto número de puntos de fallo. Cada conexión TCP se inicia por un procedimiento de establecimiento (o "handshake") de tres paquetes. El cliente envía al servidor un paquete/segmento SYN, al que éste responde con un paquete/segmento SYN_ACK. Finalmente el cliente responde con un ACK y la conexión se establece (estado=ESTABLIHED). Si el cliente ha enviado el primer SYN pero el servidor aún no lo ha reconocido, el estado de la conexión será SYN_SENT y la linea de la salida del comando netstat para una conexión en este estado sobre un computador del cliente será: { tcp 0 0 akasha.3603 aahsa.telnet SYN_SENT }.

CAUSAS DE PERSISTENCIA DE SYN_SENT

Si el estado SYN_SENT persiste, las causas más probables de la espera de conexión son: (1) El computador del servidor no esta funcionando. Si el computador del servidor funciona pero el proceso servidor no, entonces el módulo IP del computador indicará la conexión rechazada debido a que no existe proceso que espera peticiones en ese puerto. (2) Un problema de encaminamiento impide al paquete/segmento SYN alcanzar al servidor o bien impide que el SYN_ACK se devuelva al cliente. En este caso, el servidor está funcionando pero los paquetes IP no se pueden intercambiar. Esto se puede comprobar utilizando el comando "ping" dirigido al computador remoto. Si el servidor nunca recibe el paquete SYN inicial, no existe ninguna conexión en el servidor remoto para ese cliente. Si el servidor recibe el paquete SYN inicial, entonces el estado del servidor para la conexión será SYN_RCVD y el comando netstat en el servidor mostrará una linea como: { tcp 0 0 aahsa.telnet akasha.3603 SYN_RCVD }.

CAUSAS DE PERSISTENCIA DE SYN_RCVD

Una conexión de servidor a un cliente remoto que persista en el estado SYN_RCVD será causado por: (1) El servidor tiene una ruta de vuelta al cliente inválida. El servidor recibió el paquete SYN del cliente, de modo que el cliente puede enviar paquetes al servidor, pero el servidor no puede enviar paquetes al cliente. Este problema puede ocurrir sólo entre computadores de redes IP separadas. (2) La memoria cache ARP del servidor tiene una entrada no válida para el cliente. Esto puede suceder si la tarjeta de interface de red del cliente se reemplaza y la dirección hardware (o de enlace de datos o de bajo nivel, 48 bits en Ethernet) del cliente cambia. Si el servidor ya ha almacenado en su cache la dirección de enlace de datos vieja del cliente, entonces el servidor continuará intentando enviar paquetes a la dirección vieja. Se puede resolver este problema rearrancando el servidor o limpiando manualmente su memoria cache ARP (por ejemplo, utilizando el comando "arp"). Bajo circunstancias normales el "handshaking" de conexión TCP requiere muy poco tiempo para completarse. Si se requiere más de unos pocos segundos, entonces o bien existe una tasa elevada de pérdida de paquetes entre cliente y servidor o bien el servidor está ejecutándose bajo cargas muy elevadas.

PROBLEMAS EN EL CIERRE DE CONEXIONES TCP

Otra situación común que puede indicar problemas de red ocurre cuando una conexión TCP se cierra. Un cierre de conexión puede iniciarse por cualquiera de los extremos de la conexión. Cuando un extremo de una conexión TCP inicia un cierre, detiene de enviar datos y envía un paquete (denomnado más correctamente "segmento") FIN, que es el último mensaje TCP recibido por el computador remoto. Si el extremo local ha cerrado la conexión, pero el extremo remoto no lo ha hecho, la salida del comando netstat es: { tcp 0 0 akasha.3603 aahsa.telnet FIN_WAIT_1 }. En este caso, el computador remoto puede continuar enviando paquetes y el computador local continuará recibiendo y procesando los datos. La conexión es semi-abierta ya que el computador remoto puede continuar enviando datos indefinidamente. Cuando el computador remoto envíe un ACK en respuesta al paquete FIN, entonces el estado del extremo local pasa a FIN_WAIT_2, visualizándose por netstat: { tcp 0 0 akasha.3603 aahsa.telnet FIN_WAIT_2 }. Y en este punto el computador remoto está en el estado CLOSE_WAIT. El computador remoto puede continuar enviando datos incluso después de reconocer el FIN. Finalmente cuando el computador remoto termine de enviar datos e inicia el cierre de su extremo de la conexión, envía un ACK final con un FIN y entra en el estado de LAST_ACK. El extremo local entonces pasa al estado TIME_WAIT, visualizándose: { tcp 0 0 akasha.3603 aahsa.telnet TIME_WAIT }. El extremo local a continuación envía su paquete ACK final en respuesta al FIN y pasa al estado CLOSE. De este modo, si la terminación de la conexión se inicia localmente, los cambios de estado son ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, TIME_WAIT y finalmente CLOSED. Si el extremo remoto de una conexión TCP inicia un cierre, entonces los cambios de estado son ESTABLISHED, CLOSE_WAIT, LAST_ACK y finalmente CLOSED. Es posible para una conexión ser cerrada simultáneamente por ambos extremos, en cuyo caso los cambios de estado en ambos extremos son ESTABLISHED, FIN_WAIT_1, CLOSING, TIME_WAIT y finalmente CLOSED. Debido a que un cierre con éxito depende del intercambio de datos a través de la red, una conexión puede colgarse mientras se cierra. Un problema común con algunas implementaciones antiguas de TCP es colgarse durante el estado FIN_WAIT_2, causado por un "bug" (o fallo) en la implementación. El problema subyacente es la semántica diferente de un descriptor de fichero Unix y una conexión basada en sockets TCP. Debido a que la comunicación de red que utiliza sockets, la conversión a descriptores de fichero Unix, crea problemas. Un cierre en el sentido TCP es realmente un semicierre. Los datos pueden estarse aún recibiendo en la conexión pero ningún dato más se puede enviar. Un cierre en el sentido Unix significa un cierre full-duplex (o bidireccional simultáneo). Cuando se realiza un cierre Unix normal sobre un descriptor de fichero, tanto el que envía como el que recibe se inhabilitan.

El problema del FIN_WAIT_2 ocurre cuando un proceso Unix cierra el descriptor asociado con un socket y entonces sale, de este modo deja a la estructura del socket sin forma de recibir datos, ya que todos los buffer de recepción también quedan desasignados. Por tanto, el estado de la conexión en el extremo local es FIN_WAIT_1. El extremo remoto recibió un FIN (enviado cuando la conexión se cerró), pero si aún quiere enviar datos puede hacerlo. Sin embargo, el TCP del extremo local pone su tamaño de ventana a cero, ya que no puede recibir ningún dato, mientras el extremo remoto continúa "probando" al extremo local en espera de que la ventana se abra, lo cual nunca ocurrirá. Consecuentemente la conexión estará abierta siempre o hasta que el cliente o servidor se rearranque. Si se observa esta clase de persistencia de conexión semi-cerrada, probablemente el código de TCP tendrá el "bug del FIN_WAIT" en él. Las nuevas implementaciones de TCP no tienen este problema.

Este artículo tiene su continuación en el próximo número, CONECTRÓNICA Nº 15 - marzo 1998.