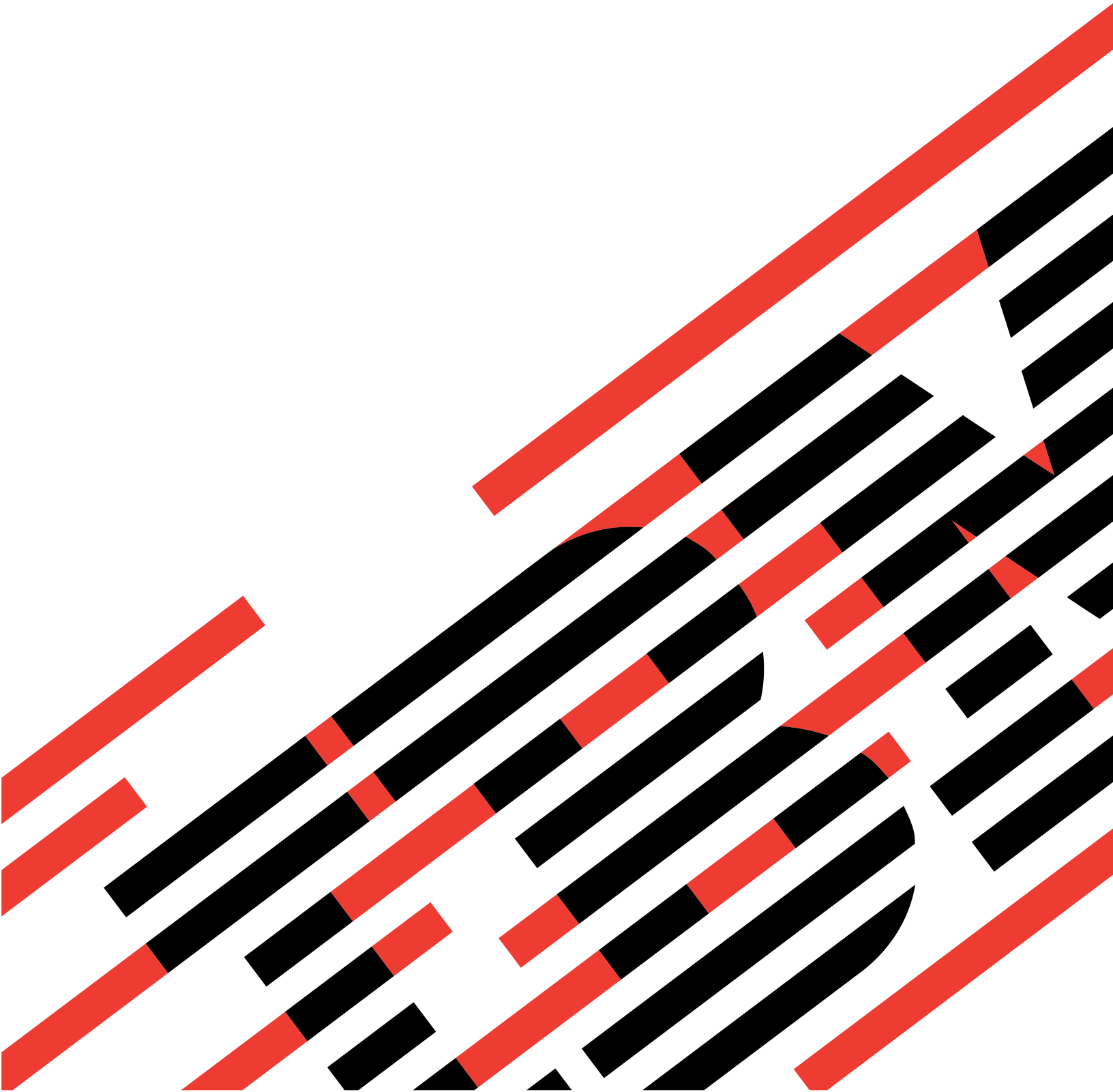
IBM

eserver

iSeries

Resolución de problemas de TCP/IP

Versión 5



IBM

@server

iSeries

Resolución de problemas de TCP/IP

Versión 5

Contenido

Capítulo 1. Resolución de problemas de TCP/IP

¿Qué detiene las funciones de TCP/IP? Ha diseñado una red sólida y seguido todas las instrucciones, pero se encuentra en un callejón sin salida. Este tema le conducirá a la solución.

Este sitio es un recurso centralizado para obtener respuestas a problemas de TCP/IP. Puede tener un problema de conectividad general que se identifique rápidamente o un problema más localizado que requiera un estudio en profundidad. Más abajo, se proporcionan herramientas para la resolución de problemas que pueden ayudarle a resolver su problema.

Novedades de V5R2
Utilice este tema para obtener información acerca de los métodos nuevos y cambiados para la resolución de problemas de TCP/IP.

Imprimir este tema
Utilice este tema para imprimir o bajar una versión PDF (Portable Document Format) de la documentación de resolución de problemas de TCP/IP.

Problemas generales de TCP/IP
Este tema le ayuda a verificar la conectividad de TCP/IP. Utilice el formato de preguntas y respuestas para centrar el problema y enlazar a las posibles soluciones.

Problemas específicos de aplicación
Si sabe que su problema se encuentra en una aplicación determinada como, por ejemplo, FTP o DNS, utilice este tema para enlazar a dicha aplicación con el fin de obtener soluciones específicas.

Rastreo de comunicaciones
Este tema le guía a través del proceso de recogida de un rastreo de comunicaciones. Un rastreo permite aislar errores, posibilitando así la solución del problema. Puede utilizar la información de rastreo o facilitársela a los especialistas de IBM cuando le ayuden a resolver el problema.

Archivos de configuración de TCP/IP
Este tema le muestra cómo copiar los archivos de configuración de TCP/IP. Deberá proporcionar estas copias a IBM, en caso de que decida consultar a un especialista para solicitar ayuda.

Anotaciones de actividad de producto
Utilice este tema para informarse acerca de cómo pueden ayudarle las anotaciones de la actividad del producto para el análisis de problemas.

Novedades de V5R2

Los elementos nuevos del tema relativo a la resolución de problemas de TCP/IP para la Versión 5 Release 2 son:

- **Problemas generales de TCP/IP**
  Información acerca de métodos para resolver problemas relacionados con el Protocolo Internet versión 6 (IPv6).
- **Rastreo de comunicaciones**
  Instrucciones para realizar un rastreo de comunicaciones mediante mandatos CL. Esta herramienta de resolución de problemas rastrea los datos de la línea de comunicaciones, para que el usuario pueda localizar el origen del problema.

Para encontrar más información acerca de las novedades o cambios de este release, consulte el Memorándum para los usuarios  .

Imprimir este tema

Para ver o bajar la versión PDF, seleccione Resolución de problemas de TCP/IP (152 KB o 26 páginas aproximadamente).

Para guardar una versión PDF en su estación de trabajo para su visualización o impresión:

1. Pulse con el botón derecho del ratón sobre el PDF en el navegador (pulse con el botón derecho en el enlace anterior).
2. Pulse **Guardar destino como...**.
3. Vaya al directorio en el que desea guardar el archivo PDF.
4. Pulse en **Guardar**.

Bajar Adobe Acrobat Reader

Si necesita Adobe Acrobat Reader para ver o imprimir estos PDF, puede bajar una copia desde el sitio Web de Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .

Capítulo 2. Problemas generales de TCP/IP

Este tema le guía a través de varias técnicas de resolución de problemas. Utilícelas para aislar problemas generales y verificar la conectividad de TCP/IP. Si ya ha verificado la conectividad de TCP/IP y sabe que el problema se encuentra en una aplicación determinada, vaya a Problemas específicos de la aplicación.

Análisis inicial de problemas de TCP/IP
Esta información incluye una serie de instrucciones y preguntas que le pueden ayudar a identificar la causa del problema.

Consideraciones acerca del mandato PING
Esta información le ayuda a comprender mejor el mandato PING y a hacer que funcione automáticamente.

Trabajar con las anotaciones de trabajo y las colas de mensajes
Este tema le proporciona otra opción para la resolución de problemas de TCP/IP.

Análisis inicial de problemas de TCP/IP

Estas preguntas y respuestas le conducirán en el análisis de problemas para ayudarle a identificar los problemas y las soluciones. Para la resolución de problemas, enlace las listas de causas, tal como se indica.

1. ¿La utilización del mandato PING para un sistema principal de la red local ha sido satisfactoria?
   a. Sí. Consulte el punto 2.
   b. No. Consulte la Lista de causas A.
2. ¿La utilización del mandato PING para el sistema remoto ha sido satisfactoria?
   a. Sí. Consulte el punto 3.
   b. No. Consulte la Lista de causas B.
3. Compruebe si el subsistema QSYSWRK contiene todos los trabajos TCP/IP necesarios.
   a. Sí. Consulte el punto 4.
   b. No. Consulte la Lista de causas C.
4. Verifique si la interfaz está activa utilizando NETSTAT.
   a. Sí. Consulte el punto 5.
   b. No. Consulte la Lista de causas D.
5. Verifique si los direccionamientos TCP/IP están correctamente configurados utilizando TELNET o FTP. Compruebe, además, si se ha establecido la conexión utilizando NETSTAT.
   a. Sí. Inicie la aplicación.
   b. No. Consulte la Lista de causas E.

Lista de causas A

El sistema remoto puede tener las respuestas ICMP inhabilitadas. En este caso, no recibirá ninguna respuesta del sistema remoto, aunque pueda tener una conexión sólida. Si cree que ésta puede ser la causa del problema, intente verificar la conexión a los otros sistemas, así como la conexión entre ellos, para determinar dónde puede encontrarse la anomalía.

1. Verifique si se ha activado TCP/IP en su sistema.

   Para asegurarse de que la pila de TCP/IP está activa:

   a. Especifique el mandato `STRTCP`. Si lo está, debe recibir el mensaje TCP1A04, que indica que TCP/IP está activo actualmente. Si TCP/IP no está activo, al entrar el mandato `STRTCP` se activa TCP/IP en el servidor. Verifique que no se haya producido ningún error al arrancar TCP/IP.

b. Si utiliza IPv6, consulte las Soluciones IPv6 para obtener información acerca de las técnicas de resolución de problemas relacionadas específicamente con IPv6. De lo contrario, continúe en el siguiente paso.

2. Verifique el software de TCP/IP del servidor.

   En el servidor, se han reservado el nombre del sistema principal LOOPBACK y la interfaz con un valor de descripción de línea *LOOPBACK para verificar el software de TCP/IP. Si especifica el nombre de sistema principal LOOPBACK, no se envía ningún dato a ninguna línea física, lo que le permite determinar rápidamente si el software de TCP/IP está funcionando correctamente en el sistema.

   Para verificar el software de TCP/IP:

   a. Asegúrese de que la tabla de sistemas principales locales no contiene ninguna entrada de un nombre de sistema principal LOOPBACK y una dirección Internet 127.0.0.1.

   b. Asegúrese de que la interfaz asociada al sistema principal LOOPBACK está activa. Generalmente, la dirección Internet asociada a la interfaz LOOPBACK es 127.0.0.1. Asegúrese de que haya una interfaz con la dirección IP del nombre de sistema principal LOOPBACK configurada con una descripción de línea *LOOPBACK. Utilice el mandato:

      ```
      NETSTAT OPTION(*IFC)
      ```

      para ver el estado de la interfaz LOOPBACK. Si no está activa, utilice la opción 9 para activarla.

   c. Después de verificar que la interfaz del sistema principal LOOPBACK está activa, escriba lo siguiente:

      ```
      PING RMTSYS(LOOPBACK)
      ```

      El sistema principal loopback permite al usuario:

      - Probar FTP, TELNET, LPR o programas de aplicación escritos por el usuario, sin estar conectado a una red o línea físicas.
      - Verificar si el software de TCP/IP está instalado y funciona correctamente.

      Se puede realizar una prueba similar utilizando el mandato PING para verificar la conectividad con una de las demás direcciones IP definidas localmente.

   d. Para probar el software y el hardware (conexión de red y adaptador), especifique la dirección Internet de un sistema principal externo de la red:

      ```
      PING RMTSYS('nnn.nnn.nnn.nnn')
      ```

   e. Si no puede verificar satisfactoriamente la conexión del sistema a la red especificando el nombre del sistema o su dirección Internet, compruebe el SSAP (punto de acceso a servicio origen) de la descripción de línea asociada a la interfaz. Debe especificar X'AA' como una entrada en la lista SSAP (punto de acceso a servicio origen). Se produce por omisión cuando se crea una nueva descripción de línea si se deja el parámetro SSAP en su valor por omisión, *SYSGEN. Si tiene una descripción de línea existente, utilice el mandato Cambiar descripción de línea para añadir los valores a la lista.

      No todos los tipos de descripciones de línea deben tener SSAP para TCP/IP, por lo que debe comprobar la lista SSAP (punto de acceso a servicio origen) de la descripción de línea asociada a esta interfaz.

   f. Verifique todos los elementos de descripción de línea, en especial, el tamaño de trama, que debe ser mayor o igual que MTU (unidad máxima de transmisión) de la interfaz.

   g. Si un sistema remoto no responde, puede significar que el sistema, la red, el sistema principal externo o el puente de la red no están disponibles o no funcionan. La falta de respuesta también puede significar que el sistema remoto tiene las respuestas ICMP inhabilitadas. Puede ocurrir si el sistema remoto está actuando como cortafuegos y se ha configurado para no responder a las peticiones de ICMP. Intente verificar la conexión a otros sistemas, así como entre ellos, para determinar con más precisión dónde puede situarse la anomalía.

   h. Verifique si la interfaz local está configurada correctamente.

i. Asegúrese de que las dos entradas de direccionamiento siguientes están configuradas en la descripción del subsistema QSYSWRK, en caso de que las interfaces de TCP/IP, incluida LOOPBACK, no activen o no puedan finalizar o arrancar TCP/IP. Si no existen o si son incorrectas, añádalas o corríjalas y vuelva a intentar la petición.

```
ADDRTGE  SBSD(QSYS/QSYSWRK) +
         SEQNBR(2505) +
         CMPVAL(TCPIP) +
         PGM(QSYS/QTOCTCPIP) +
         CLS(QSYS/QSYSCLS20) +
         MAXACT(*NOMAX) +
         POOLID(1)

ADDRTGE  SBSD(QSYS/QSYSWRK) +
         SEQNBR(2506) +
         CMPVAL(TCPEND) +
         PGM(QSYS/QTOCETCT) +
         CLS(QSYS/QSYSCLS20) +
         MAXACT(*NOMAX) +
         POOLID(1)
```

Vuelva a Análisis inicial de problemas de TCP/IP para continuar con la resolución de problemas.

Soluciones IPv6

Si experimenta problemas en las comunicaciones IPv6, intente estas técnicas para la resolución de problemas de la red.

1. Verifique que la pila IPv6 esté en ejecución.
   a. Asegúrese de que la interfaz de bucle de retroceso esté configurada y activa. Para comprobar el estado de la interfaz de bucle de retroceso, siga estos pasos:
      1) En iSeries Navigator, expanda el **servidor ––> Red ––> Configuración TCP/IP ––> IPv6 ––> Interfaces**.
      2) En el panel de la derecha, busque la interfaz de bucle de retroceso. La dirección IP de la dirección de bucle de retroceso IPv6 es ::1 y el nombre de línea es Loopback 6. Si la interfaz de bucle de retroceso no aparece en la lista, debe configurarla mediante el asistente **Configuración de IPv6**.
   b. Ejecute un mandato Ping de la dirección de bucle de retroceso (::1). El servidor se envía a sí mismo un paquete IPv6 y, con ello, verifica que la pila IPv6 está en funcionamiento. Para probar la pila mediante el programa de utilidad ping, siga estos pasos:
      1) En iSeries Navigator, expanda el **servidor ––> Red**.
      2) Pulse con el botón derecho del ratón **Configuración TCP/IP**, pulse **Programas de utilidad** y pulse **Ping**.
2. Después de verificar que la pila IPv6 se está ejecutando, asegúrese de que la línea IPv6 está configurada y activa. Esta línea puede ser una línea Ethernet o una línea de túnel configurada.

   Para comprobar el estado de las líneas configuradas en el servidor, siga estos pasos:
   a. En iSeries Navigator, expanda el **servidor ––> Red ––> Configuración TCP/IP ––> Líneas**.
   b. En el panel de la derecha, busque la línea que debe configurarse para IPv6 y compruebe la columna de estado. Si la línea no aparece en la lista, debe configurar una línea para IPv6 mediante el asistente **Configuración IPv6**. Consulte la sección Configurar IPv6 para obtener instrucciones de configuración de una línea para IPv6. Si la línea aparece en la lista y muestra el estado **No cargada**, la línea está configurada pero no está cargada en la configuración de pila IPv6. Utilice el mandato Trabajar con descripciones de línea (WRKLIND) en la interfaz basada en caracteres para diagnosticar el problema de la línea.
3. Asegúrese de que como mínimo dos interfaces IPv6 estén activas: la interfaz local y la interfaz a la que envía el ping.

   Para comprobar el estado de las interfaces IPv6, siga estos pasos:

a. En iSeries Navigator, expanda el **servidor ––> Red ––> Configuración TCP/IP –––> IPv6 –––> Interfaces**.
b. En el panel de la derecha, busque la dirección IP asociada a la interfaz local y compruebe el estado de la interfaz.
c. Si la interfaz está **Inactiva**, debe activarla. Para activar la interfaz, pulse con el botón derecho del ratón sobre la dirección IP y seleccione **Inicio**.
d. Repita estos pasos para comprobar el estado de la interfaz remota.

4. Si el mandato ping de una dirección IPv6 no ha sido satisfactorio, verifique el estado de la dirección de ambas interfaces. El estado de la dirección de ambas interfaces debe ser **Preferido**. Si la interfaz origen o destino no se encuentra en estado preferido, elija otras interfaces para la prueba o cambie al estado y la dirección adecuados las interfaces utilizadas.

   Para verificar o cambiar el estado de la dirección de la interfaz origen, siga estos pasos:

   a. En iSeries Navigator, expanda el **servidor –––> Red –––> Configuración TCP/IP–––> IPv6 –––> Interfaces**.
   b. En el panel de la derecha, pulse con el botón derecho del ratón sobre la dirección IP asociada con la interfaz, seleccione **Propiedades** y seleccione la página **Opciones**. Este diálogo permite especificar un tiempo de vida preferido o válido para la interfaz.
   c. Repita estos pasos para comprobar el estado de la dirección de la interfaz destino.

Lista de causas B

Si los mandatos VFYTCPCNN o PING han sido satisfactorios para el sistema local, debe verificar la posibilidad de efectuar una conexión entre su sistema y el otro sistema con el que desea comunicarse. Ejecute el mandato PING tal como lo ha hecho antes, pero esta vez especifique la dirección Internet del sistema principal remoto. Consulte la sección Mensajes de error comunes. El sistema principal remoto, o un cortafuegos intermedio, pueden tener las respuestas ICMP inhabilitadas. En este caso, no recibirá ninguna respuesta del sistema remoto, aunque pueda tener una conexión sólida. Si cree que ésta puede ser la causa del problema, intente verificar la conexión a otros sistemas, así como la conexión entre ellos, para determinar con más precisión dónde puede encontrarse la anomalía.

1. Si puede verificar la conexión utilizando la dirección Internet remota, pero no el nombre del sistema remoto, significa que el nombre o la dirección de la tabla de sistemas principales son incorrectos o que los servidores de nombres remotos pueden no estar disponibles.
2. Si el sistema utiliza servidores de nombres remotos, verifique si puede llegar a cada servidor de nombres remoto utilizando el mandato PING y especificando la dirección Internet del servidor de nombres remoto.
3. El mandato PING tiene parámetros adicionales que le permiten especificar la longitud del paquete, el número de paquetes que enviar y el tiempo de espera de respuesta. En la mayor parte de redes, el tiempo de espera por omisión de 1 segundo es suficiente para que el sistema remoto responda. Sin embargo, si el sistema remoto está muy alejado o si la red está ocupada, aumentar el parámetro de tiempo de espera puede proporcionar un resultado satisfactorio.

   Se aconseja dejar los parámetros en sus valores por omisión. Si los cambia, una combinación de longitud de paquetes grande y un tiempo de espera corto puede no proporcionar tiempo suficiente a la red para transmitir y recibir la respuesta, produciéndose un tiempo de espera excedido. Si la red no dispone de tiempo suficiente para transmitir y recibir la respuesta, puede parecer que no se dispone de conectividad a un sistema cuando, en realidad, no es así.
4. Si el sistema remoto no responde, puede significar que el sistema, la red, la pasarela, el direccionador o el puente de la red no están disponibles o no funcionan. La falta de respuesta también puede significar que el sistema remoto, o un cortafuegos intermedio, tienen las respuestas ICMP inhabilitadas. Intente verificar la conexión a otros sistemas, así como entre ellos, para determinar con más precisión dónde puede situarse la anomalía.

5. Si un sistema remoto no responde cuando se utiliza el mandato PING para verificar una interfaz, que está configurada para una descripción de línea de tipo Ethernet, asegúrese de que ha especificado el estándar Ethernet correcto o *ALL en la descripción de línea Ethernet.
6. La no recepción de respuestas de todos los sistemas de una red indica que el problema está en algún lugar del camino. Verifique la conexión a la pasarela que lleva a la red en cuestión. Si no localiza el problema, investigue hacia atrás a partir del sistema remoto al que no puede llegar hasta localizar el punto de anomalía.
7. Los paquetes se envían utilizando un protocolo de bajo nivel que no garantiza la entrega. Puesto que una petición de eco se puede perder, no dé por supuesto que una red o pasarela han dado error hasta que varios mandatos no pasen más allá de un punto determinado de la vía de acceso.

Si el mandato PING a un sistema principal de una red remota no resulta satisfactorio, utilice el mandato de Direccionamiento de rastreo (TRACEROUTE) para la misma red. El programa de utilidad de direccionamiento de rastreo puede realizar muchas de las pruebas de conectividad que llevan a cabo los mandatos ping individuales, pero el direccionamiento de rastreo puede efectuarlas en un solo paso. El direccionamiento de rastreo prueba cada salto de la vía de acceso al destino remoto e indica si el problema se encuentra en un direccionador intermedio o en la red remota.

Escriba `TRACEROUTE RMTSYS('x.x.x.x')`. Puede especificar el sistema remoto mediante una dirección IP o mediante el nombre del sistema remoto; por ejemplo, `('xxxx.xxxx.com')`. El programa de utilidad de direccionamiento de rastreo acepta tanto el formato de dirección IPv4 `('x.x.x.x')` como el formato de dirección IPv6 `('x:x:x:x:x:x:x:x')`.

El direccionamiento de rastreo también está disponible por medio de iSeries Navigator. Para iniciar el direccionamiento de rastreo, siga los pasos que se indican a continuación:

1. En iSeries Navigator, expanda el servidor —> **Red**.
2. Pulse el botón derecho en **Configuración de TCP/IP**, seleccione **Programas de utilidad** y, a continuación, **Direccionamiento de rastreo**.

Vuelva a Análisis inicial de problemas de TCP/IP para continuar con la resolución de problemas.

Lista de causas C

1. Compruebe si el subsistema QSYSWRK del servidor contiene todos los trabajos necesarios (locales o remotos). Debe haber, como mínimo, el trabajo QTCPIP, que controla el inicio y el final de las interfaces de TCP/IP. También debe haber, como mínimo, un trabajo para cada una de las aplicaciones que está tratando de utilizar, tal como se muestra en la Figura 1 en la página 8. Es posible que la denominación de estos trabajos no sea idéntica a la que se da en su subsistema para los trabajos FTP, LPD y TELNET. Todos los trabajos de FTP empiezan por `QTFTP`, todos los trabajos de LPD empiezan por `QTLPD` y todos los trabajos de TELNET se denominan `QTVTELNET` y `QTVDEVICE`. Puede haber más de un trabajo de servidor FTP, LPD o TELNET. Todos los trabajos de SMTP empiezan por `QTSMTP`. SMTP tiene hasta cuatro trabajos activos en el subsistema QSYSWRK y dos trabajos activos en el subsistema QSNADS. Todos los trabajos de SNMP empiezan por `QTMSNMP`. SNMP puede tener hasta tres trabajos activos en el subsistema QSYSWRK: QTMSNMP, QTMSNMPRCV y QSNMPSA.

   Utilice el mandato Trabajar con trabajos activos (WRKACTJOB) para visualizar estos trabajos. Escriba `WRKACTJOB SBS(QSYSWRK)`.
2. Si no están todos los trabajos, finalice el proceso TCP/IP utilizando el mandato `ENDTCP OPTION(*IMMED)`. Consulte todas las anotaciones de trabajo asociadas a los trabajos.
3. Cambie el nivel de registro de mensajes de descripción de trabajos de todos los objetos de descripción de trabajos a `4 0 *SECLVL`. Consulte el apartado Trabajar con las anotaciones de trabajo y las colas de mensajes para obtener información más detallada sobre los niveles de anotación de mensajes.
4. Reinicie el proceso TCP/IP utilizando el mandato `STRTCP`

5. Verifique que todos los trabajos estén activos.
6. Compruebe en las anotaciones de trabajo si los trabajos adecuados no están activos.

```
                 Trabajar con trabajos activos     SYSNAM03

                                    02/03/99  18:06:32
% CPU:    ,8     Tiempo transcurrido:   02:21:32      Trabajos activos:   93

Teclee opciones, pulse Intro.
  2=Cambiar  3=Retener 4=Fin  5=Trabajar con  6=Liberar  7=Ver mensaje
  8=Trab archivos en spool  13=Desconectar ...

Opc Subsistema/Trab.Usuario     Tipo  % CPU  Función         Estado
     QSYSWRK        QSYS        SBS      ,0                  DEQW
       QMSF         QMSF        BCH      ,0                  DEQW
       QNEOSOEM     QUSER       ASJ      ,0  PGM-QNEOSOEM     TIMW
       QNEOSOEM     QUSER       BCH      ,0  PGM-QNEOSOEM     TIMW
       QNEOSOEM     QUSER       BCH      ,0  PGM-QNEOSOEM     TIMW
       QNPSERVD     QUSER       BCH      ,0                  SELW
       QPASVRP      QSYS        BCH      ,0  PGM-QPASVRP      DEQW
       QPASVRS      QSYS        BCH      ,0  PGM-QPASVRS      TIMW
       QPASVRS      QSYS        BCH      ,0  PGM-QPASVRS      TIMW
                                                                Más...
Parámetros o mandato
===>
F3=Salir  F5=Renovar       F7=Buscar    F10=Reiniciar estadísticas
F11=Ver datos transcurr    F12=Cancelar F23=Más opciones   F24=Más teclas
```

Figura 1. Pantalla Trabajar con trabajos activos: Pantalla 1

```
                 Trabajar con trabajos activos      SYSNAM03
                                    02/03/99  18:06:32
% CPU:    ,8     Tiempo transcurrido:   02:21:32      Trabajos activos:   93

Teclee opciones, pulse Intro.
  2=Cambiar  3=Retener 4=Fin  5=Trabajar con  6=Liberar  7=Ver mensaje
  8=Trab archivos en spool  13=Desconectar ...

Opc Subsistema/Trab.Usuario     Tipo  % CPU  Función         Estado
       QTLPD03516   QTCP        BCH      ,0                  DEQW
       QTLPD03580   QTCP        BCH      ,0                  TIMW
       QTMSNMP      QTCP        BCH      ,0  PGM-QTOSMAIN     DEQW
       QTMSNMPRCV   QTCP        BCH      ,0  PGM-QTOSRCVR     TIMW
       QTVDEVICE    QTCP        BCH      ,0  PGM-QTVDEVMG     TIMW
       QTVTELNET    QTCP        BCH      ,0                  TIMW
       QZBSEVTM     QUSER       ASJ      ,0  PGM-QZBSEVTM     EVTW
       QZHQSRVD     QUSER       BCH      ,0                  SELW
       QZRCSRVSD    QUSER       BCH      ,0                  SELW
                                                                Más...
Parámetros o mandato
===>
F3=Salir  F5=Renovar       F7=Buscar    F10=Reiniciar estadísticas
F11=Ver datos transcurr    F12=Cancelar F23=Más opciones   F24=Más teclas
```

Figura 2. Pantalla Trabajar con trabajos activos: Pantalla 2

Vuelva a Análisis inicial de problemas de TCP/IP para continuar con la resolución de problemas.

Lista de causas D

La función de estado de red (NETSTAT) del servidor le ofrece la posibilidad de visualizar el estado de la interfaz TCP/IP, la información de configuración de direccionamiento TCP/IP y el estado de conexión TCP/IP en su sistema local. Puede utilizar el mandato WRKTCPSTS o NETSTAT.

1. Inicie TCP/IP utilizando el mandato STRTCP antes de usar la función de estado de red. Se muestra el menú Trabajar con estado de red TCP/IP, pero las opciones no se pueden utilizar hasta que se arranca TCP/IP.
2. En la pantalla de estado de la interfaz de TCP/IP, si intenta arrancar una interfaz activa o finalizar una interfaz inactiva, se envía el mensaje de error correspondiente. Si una interfaz inactiva no obtiene el estado activo después de seleccionar la opción de interfaz de inicio, puede haber un problema con la interfaz, la línea o la configuración de la línea. Consulte las anotaciones del trabajo QTCPIP del subsistema QSYSWRK para comprobar si se han producido errores durante la activación de la interfaz. También puede obtener ayuda para la determinación del estado consultando la cola de mensaje QSYSOPR y y las anotaciones históricas, QHT (DSPLOG).
3. Escriba WRKCFGSTS *LIN para determinar si existe algún problema en la descripción de línea.
4. Verifique si se muestra, como mínimo, una conexión de escucha pasiva para cada uno de los servidores de la pantalla Trabajar con estado de conexión TCP/IP, opción 3 de la pantalla Trabajar con estado de red TCP/IP. Debe verificar el estado de la conexión de los servidores que soportan estas aplicaciones y de cualquier otro servidor pertinente de la red:

   SNMP

   TELNET

   La Versión 4 Release 4 ofrece soporte para SSL Telnet, además de para Telnet. SSL Telnet refleja un puerto de escucha 992 por omisión y Telnet tradicional utiliza el puerto 23. Se recomienda restringir los puertos de escucha Telnet para inhabilitar el servidor Telnet tradicional y habilitar SSL Telnet.

   FTP

   SMTP, si se ha configurado

   POP

   LPD

   REXEC

   HTTP, si se ha configurado

   Las conexiones de escucha pasivas se indican mediante un asterisco en los campos *Dirección remota* y *Puerto remoto*. No se aconseja finalizar estas conexiones. Los sistemas remotos no pueden utilizar SNMP, FTP o TELNET, enviar correo SMTP al sistema local o enviar archivos en spool utilizando LPR al sistema local si se han concluido las conexiones de escucha pasivas asociadas. Se pueden reiniciar finalizando y arrancando los servidores utilizando los mandatos ENDTCPSVR y STRTCPSVR y, a continuación, especificando el servidor que se desea finalizar y arrancar.
5. Asegúrese de que los puertos asociados a la aplicación que está intentando utilizar no están restringidos. Utilice la opción 4 (Trabajar con restricciones de puerto TCP/IP) del menú Configurar TCP/IP para ver las restricciones de puertos actuales.

Vuelva a Análisis inicial de problemas de TCP/IP para continuar con la resolución de problemas.

Lista de causas E

Verifique los datos de configuración. Si todo parece correcto, vaya a Problemas específicos de la aplicación y elija la aplicación que está utilizando para obtener ayuda para la resolución de problemas.

Consideraciones acerca del mandato PING

Lea los apartados siguientes para obtener más información acerca del mandato PING.

Concatenar el nombre de dominio con el nombre del sistema principal
En este apartado se explica cómo concatena el servidor el nombre de dominio con el nombre del sistema principal.

Mensajes de error comunes
En este apartado se proporcionan ejemplos de algunas de las condiciones de error PING más comunes.

Concatenar el nombre de dominio con el nombre del sistema principal

Este ejemplo muestra cómo utiliza el servidor el nombre de dominio local como lista de búsqueda y cómo concatena nombres de dominio con el nombre de sistema principal si no se utiliza un punto al final del nombre de dominio.

El nombre del servidor es SYSNAM01.A400SSC.DFW.COMPANY.COM y desea verificar la conexión a un sistema cuyo nombre completo es SYSNAM02.DFW.COMPANY.COM. La tabla de nombres de sistemas principales locales no contiene el nombre de sistema principal SYSNAM02.

Si escribe `PING SYSNAM02.DFW.COMPANY.COM`, el servidor envía SYSNAM02.DFW.COMPANY.COM al servidor de nombres remoto.

Si escribe `PING SYSNAM02`, el servidor envía primero SYSNAM02.A400SSC.DFW.COMPANY.COM al servidor de nombres remoto. A continuación, envía SYSNAM02.DFW.COMPANY.COM. Si no lo encuentra, por último, envía SYSNAM02.COMPANY.COM. En otras palabras, iSeries TCP/IP concatena cada parte del nombre de dominio local con el nombre de sistema principal.

Si escribe `PING SYSNAM02.`, el servidor de nombres remoto informa de que el nombre de sistema principal es desconocido. La razón por la que el servidor de nombres remoto no reconoce SYSNAM02 es que el servidor envía el nombre SYSNAM02 al servidor de nombres remoto sin ninguna parte de la lista de búsqueda concatenada. La única diferencia entre este nombre y el nombre anterior está en la utilización del punto al final del nombre.

Mensajes de error comunes

Cuando utiliza el mandato PING para verificar la conexión a otro sistema principal de la red, TCP/IP puede dar un mensaje de error. Utilice esta tabla para identificar los mensajes de error comunes y para determinar qué debe hacer para resolver los problemas.

Mensaje de error	Qué debe hacer
`Ningún servicio TCP/IP disponible`	• Aún no se ha arrancado TCP/IP o no ha finalizado su inicialización. Utilice el mandato NETSTAT para ver si TCP/IP está activo. • No se han podido arrancar todos los trabajos del subsistema QSYSWRK. Utilice el mandato Trabajar con trabajos activos (WRKACTJOB) para verificar si el subsistema QSYSWRK y los trabajos relacionados están activos. Si no es así, consulte si hay mensajes en las anotaciones de trabajo o en la cola de salida por omisión del sistema.
`No se ha podido establecer la conexión con el sistema principal remoto`	Compruebe las interfaces configuradas, sus descripciones de línea relacionadas y los direccionamientos TCP/IP.
`No se puede llegar al sistema remoto`	TCP/IP no ha podido encontrar un direccionamiento al destino solicitado. Compruebe la opción 2 de NETSTAT y verifique si se ha configurado *DFTROUTE, o un direccionamiento de red equivalente, y está activo.

El sistema principal remoto no responde a VFYTCPCNN en el plazo de 10 segundos para la verificación de conexión 1.	• Es probable que la configuración sea correcta, pero no obtiene una respuesta del sistema remoto. Asegúrese de que el sistema principal remoto puede localizar su sistema. Póngase en contacto con el operador del sistema remoto y solicítele que verifique la conexión a su sistema. • Compruebe las tablas de sistemas principales o el servidor de nombres remoto (si utiliza un servidor de nombres) de ambos sistemas y los direccionamientos y las interfaces de TCP/IP. Es posible que, por algún motivo, el servidor de nombres remoto no pueda prestarle servicio. • Si utiliza una línea Ethernet, asegúrese de que ha especificado el estándar Ethernet correcto o *ALL.
VFYTCPCNN: Sistema principal desconocido, xxxxxx donde xxxxxx es el nombre del sistema principal.	El nombre de sistema principal no se ha podido resolver en una dirección IP ni con la tabla de sistemas principales ni con un servidor de nombres. Compruebe la tabla de sistemas principales locales o los servidores de nombres remotos (si utiliza un servidor de nombres) de la entrada del sistema principal remoto.

Trabajar con las anotaciones de trabajo y las colas de mensajes

TCP/IP se entrega con varias descripciones de trabajos.

Las descripciones de trabajos se almacenan en la biblioteca QSYS o QTCP. Se entregan generalmente con un nivel 4 de anotación de mensajes, una gravedad 0 de anotación de mensajes y un valor de texto de anotación de mensajes *NOLIST. Se entregan con estos valores para evitar que se puedan crear anotaciones de trabajo que contengan únicamente los mensajes de inicio y fin del trabajo.

Si experimenta problemas con el funcionamiento de TCP/IP, una de las primeras acciones que debe llevar a cabo es cambiar el nivel de registro de mensajes de la descripción de trabajos de la aplicación con la que está teniendo problemas por un valor de texto de registro de mensajes de *SECLVL. Al cambiar el nivel de registro de mensajes se generan las anotaciones de trabajo correspondientes a la aplicación. Para que el cambio entre en vigor, debe finalizar y, a continuación, reiniciar el servidor. Si desea cambiar el trabajo inmediatamente, debe utilizar el mandato CHGJOB para cambiar el nivel de registro de mensajes del trabajo activo.

Para cambiar el nivel de anotación de mensajes de la descripción de trabajo de una aplicación determinada, consulte estos ejemplos:

- Si el problema está en el servidor FTP, cambie la descripción de trabajo QTMFTPS escribiendo este mandato CL:

  ```
  CHGJOBD  JOBD(QTCP/QTMFTPS)  LOG(4 0 *SECLVL)
  ```

- Si el problema está en SMTP, cambie la descripción de trabajo QTMSMTPS escribiendo este mandato CL:

  ```
  CHGJOBD  JOBD(QTCP/QTMSMTPS)  LOG(4 0 *SECLVL)
  ```

  Además de la descripción de trabajo QTMSMTPS, puede considerar la posibilidad de cambiar el nivel de anotación de la descripción de trabajo del subsistema QSNADS escribiendo este mandato CL:

  ```
  CHGJOBD  JOBD(QGPL/QSNADS)  LOG(4 0 *SECLVL)
  ```

Capítulo 3. Problemas específicos de aplicación

Si ha determinado que el problema se encuentra en una aplicación específica que está ejecutando en TCP/IP, elija la aplicación de la lista siguiente para obtener información más detallada para la resolución de problemas. Cada enlace le lleva a un nuevo sitio, externo a Resolución de problemas generales de TCP/IP, específico de la aplicación que ha elegido.

Servidor del Sistema de nombres de dominio (DNS)
En este tema se proporciona un diagrama de flujo para el análisis de problemas y le guía a través de estrategias de depuración para los problemas de DNS.

Protocolo de transferencia de archivos (FTP)
En este tema se sugieren soluciones para los problemas de FTP y se muestran las anotaciones de trabajo de servidor como herramienta para la resolución de problemas.

Protocolo punto a punto (PPP)
En este tema se ofrecen soluciones para problemas comunes de conexión PPP.

Servidor de protocolo de oficinas de correos (POP)
Consulte este tema para resolver problemas del servidor POP y otras aplicaciones de correo electrónico.

Rexec
En este tema se proporciona un diagrama de flujo para ayudarle a centrar el problema Rexec y buscar posibles soluciones.

Protocolo simple de transferencia de correo (SMTP)
En este tema se proporcionan varios métodos para resolver problemas del Protocolo simple de transferencia de correo (SMTP) y de otras aplicaciones de correo electrónico.

Telnet
Este tema le ayuda a resolver problemas generales de Telnet, así como problemas específicos relacionados con el tipo de emulación y el servidor SSL. Además, se indica la información necesaria para informar acerca del problema.

Red privada virtual (VPN)
Este tema le guía a través de varias estrategias de resolución de problemas de VPN relacionados con la conexión, errores de configuración o normas de filtro, entre otros.

Capítulo 4. Rastreo de comunicaciones

El rastreo de comunicaciones se utiliza para la resolución de problemas de TCP/IP. El rastreo de comunicaciones es una función de servicio que permite rastrear los datos de una línea de comunicaciones, como por ejemplo una red de área local (LAN) o una red de área amplia (WAN). Una vez que se han rastreado los datos, los datos en estado original pueden volcarse en un archivo continuo o pueden formatearse y colocarse en un archivo en spool que va a visualizarse o imprimirse.

El rastreo de comunicaciones puede utilizarse para la resolución de problemas tanto de comunicaciones IPv4 como IPv6.

Utilice el rastreo de comunicaciones en estas situaciones:

- Los procedimientos de análisis de problemas no proporcionan información suficiente acerca del problema.
- Sospecha que el problema se debe a una violación de protocolo.
- Sospecha que el problema se debe a ruido en la línea.
- Desea saber si la aplicación está transmitiendo información correctamente a través de la red.
- Desea saber si existen problemas de rendimiento debidos a congestión de la red o a actividad general de los datos.

Para utilizar los mandatos CL destinados a realizar un rastreo de comunicaciones, debe tener la autorización especial *SERVICE o tener autorización sobre la función Rastreo de servicio de Operating System/400 mediante iSeries Navigator. Consulte el capítulo relativo a los perfiles de usuario de iSeries Security Reference  para obtener más información acerca de este tipo de autorización.

Rastrear conexión (TRCCNN) es un mandato que ofrece un método alternativo para obtener un rastreo similar a un rastreo de comunicaciones. Si tiene aplicaciones TCP que utilizan SSL o si utiliza la Seguridad IP, los datos que fluyen a través de la línea de comunicaciones están cifrados; el rastreo de comunicaciones puede no ser de utilidad si necesita ver los datos. TRCCNN rastrea los datos antes de cifrarlos y después de descifrarlos y, por tanto, puede utilizarse cuando el rastreo de comunicaciones general no es efectivo. Proporciona una salida similar a la del rastreo de comunicaciones general. Consulte la sección Descripción del mandato TRCCNN (Rastrear conexión) del tema relativo a las API (interfaces de programas de aplicación) para obtener parámetros y ejemplos asociados con este mandato.

Para utilizar la función de rastreo de comunicaciones, siga estos pasos:

Planificar un rastreo de comunicaciones
Los pasos previos necesarios para poder realizar un rastreo de comunicaciones.

Realizar un rastreo de comunicaciones
Los pasos necesarios para realizar el rastreo de comunicaciones.

Funciones adicionales de rastreo de comunicaciones
Más funciones asociadas con el rastreo de comunicaciones.

Planificar un rastreo de comunicaciones

Antes de empezar a trabajar con un rastreo de comunicaciones, siga estos pasos:

1. Si no ha creado la biblioteca IBMLIB o la cola de salida IBMOUTQ, especifique los mandatos siguientes:

```
CRTLIB LIB(IBMLIB)
CRTOUTQ OUTQ(IBMLIB/IBMOUTQ)
```

2. Para añadir la biblioteca IBMLIB a la lista de bibliotecas y cambiar la cola de salida del trabajo a la cola de salida IBMOUTQ, especifique los mandatos siguientes:

```
ADDLIBLE IBMLIB
CHGJOB * OUTQ(IBMLIB/IBMOUTQ)
```

3. Si el archivo de impresora QTCPPRT no existe en el sistema, especifique los mandatos siguientes para crearlo:

```
CRTPRTF FILE(QTCP/QTCPPRT)  DEV(*JOB)
        RPLUNPRT(*YES) SCHEDULE(*FILEEND)
        FILESEP(0) LVLCHK(*NO)
        TEXT('archivo impresora TCP/IP')
CHGOBJOWN OBJ(QTCP/QTCPPRT) OBJTYPE(*FILE)
        NEWOWN(QSYS)
```

4. Para enviar el archivo en spool QTCPPRT que contiene el rastreo de comunicaciones a la cola de salida IBMOUTQ de la biblioteca IBMLIB, especifique los mandatos siguientes:

```
OVRPRTF FILE(QTCPPRT) OUTQ(IBMLIB/IBMOUTQ)
OVRPRTF FILE(QPCSMPRT) TOFILE(QTCP/QTCPPRT)
```

   Las alteraciones temporales del archivo de impresora no están activas cuando finaliza el trabajo.

5. Obtenga el nombre de la descripción de línea asociada a la interfaz de TCP/IP con la que está experimentando problemas o que utiliza la aplicación o la red que produce el problema. Utilice NETSTAT *IFC para determinar el nombre de la descripción de línea asociada a la interfaz.
6. Asegúrese de que se ha activado la línea y que se ha arrancado la interfaz de TCP/IP asociada a la línea de modo que se puedan enviar y recibir datos TCP/IP a través de la interfaz y la línea. Utilice NETSTAT *IFC para verificar si la interfaz está activa.

Qué hacer a continuación:
Realizar un rastreo de comunicaciones

Realizar un rastreo de comunicaciones

Para realizar un rastreo de comunicaciones, debe utilizar mandatos CL en la interfaz basada en caracteres. Para realizar un rastreo de comunicaciones, siga estos pasos:

1. Iniciar un rastreo de comunicaciones
2. Finalizar un rastreo de comunicaciones
3. Volcar un rastreo de comunicaciones
4. Imprimir un rastreo de comunicaciones
5. Ver el contenido de un rastreo de comunicaciones
6. Leer un rastreo de comunicaciones

Iniciar un rastreo de comunicaciones

Esta acción inicia un rastreo de comunicaciones para la descripción de interfaz de red o la línea especificada.

Nota: ya no puede utilizarse un rastreo de comunicaciones para rastrear los datos de una descripción de servidor de red (*NWS). La función de rastreo de comunicaciones se utiliza para rastrear los datos en una línea específica (*LIN) o en una descripción de interfaz de red (*NWI).

Para iniciar un rastreo de comunicaciones, siga estos pasos:

1. En la línea de mandatos, especifique `STRCMNTRC`.
2. En **Objeto de configuración**, especifique el nombre de la línea, como por ejemplo `TRNLINE`.
3. En **Tipo**, especifique el tipo de recurso, `*LIN` o `*NWI`.
4. En **Tamaño de almacenamiento intermedio**, especifique una cantidad de almacenamiento suficiente para el volumen de datos previsto. En la mayoría de protocolos, 8 MB es un almacenamiento

suficiente. Para una Ethernet 10/100, es suficiente entre 16 MB y 1 GB. Si no está seguro, especifique 16 MB como cantidad máxima de almacenamiento permitido para el protocolo.

5. En **Opciones de rastreo de comunicaciones**, especifique *RMTIPADR si desea limitar los datos recogidos a un rastreo de una interfaz remota. Si no es así, utilice el valor por omisión.
6. En **Dirección IP remota**, especifique la dirección IP asociada con la interfaz remota en la que se recogerán los datos de rastreo.

El rastreo de comunicaciones continúa hasta que se produce una de las siguientes situaciones:

- Se ejecuta el mandato ENDCMNTRC.
- Un problema de la línea física provoca la finalización del rastreo.
- El parámetro **Rastreo lleno** especifica *STOPTRC y el almacenamiento intermedio se llena.

Qué hacer a continuación:
Finalizar un rastreo de comunicaciones

Finalizar un rastreo de comunicaciones

Para poder formatear y visualizar el rastreo, primero debe finalizarlo. Esta acción finaliza el rastreo, pero salva el almacenamiento intermedio del rastreo de comunicaciones.

Para finalizar un rastreo de comunicaciones, siga estos pasos:

1. En la línea de mandatos, especifique ENDCMNTRC.
2. En **Objeto de configuración**, especifique la misma línea que ha especificado al iniciar el rastreo, como por ejemplo TRNLINE.
3. En **Tipo**, especifique el tipo de recurso, *LIN o *NWI.

Qué hacer a continuación:
Volcar un rastreo de comunicaciones en un archivo continuo. Este es un paso opcional que puede ser de utilidad. Si prefiere imprimir los datos en su estado original sin volcarlos, vaya a la sección Imprimir un rastreo de comunicaciones

Volcar un rastreo de comunicaciones

Si utiliza el Protocolo Internet versión 6 (IPv6), debe volcar los datos de rastreo en un archivo continuo siguiendo estos pasos, pero si utiliza IPv4 esta es una parte opcional del proceso de rastreo de comunicaciones.

El hecho de volcar los datos en un archivo continuo ofrece varias ventajas. Tenga en cuenta estas ventajas al decidir si debe utilizar esta función:

- Puede ejecutar rastreos nuevos sin perder los datos del rastreo existente.
- Puede formatear loa datos de rastreo varias veces. Por ejemplo, si una de las aplicaciones utiliza ASCII, puede que en primer lugar necesite formatear el rastreo de comunicaciones en ASCII; si otra aplicación utiliza EBCDIC, puede que necesite formatear los mismos datos de rastreo en EBCDIC. Volcando los datos de rastreo en un archivo continuo, obtiene la flexibilidad de formatear estos datos dos veces.
- Puede conservar los datos de rastreo mientras se realizar una carga del programa inicial (IPL).
- Puede utilizar un formateador personalizado para generar la salida.

Para volcar un rastreo de comunicaciones, siga estos pasos:

1. Cree un directorio, como por ejemplo myidir. Consulte la sección Descripción del mandato CRTDIR (Crear directorio) del tema dedicado al Lenguaje de Control (CL), para crear un directorio.
2. En la línea de mandatos, especifique DMPCMNTRC.

3. En **Objeto de configuración**, especifique la misma línea que ha especificado al iniciar el rastreo, como por ejemplo `TRNLINE`.
4. En **Tipo**, especifique el tipo de recurso, `*LIN` o `*NWI`.
5. En **A archivo continuo**, especifique el nombre de vía de acceso, como por ejemplo `/mydir/mytraces/trace1`.

Qué hacer a continuación:
Imprimir un rastreo de comunicaciones

Imprimir un rastreo de comunicaciones

Puede imprimir los datos del rastreo de comunicaciones a partir de dos fuentes diferentes, dependiendo de cómo haya recogido el rastreo. Puede imprimir desde los datos originales que ha recogido o desde un archivo continuo en el que previamente ha volcado los datos originales.

Nota: para imprimir los datos del rastreo de comunicaciones desde un archivo continuo, debe tener Java (5722JV1) instalado en el sistema.

Esta acción graba los datos del rastreo de comunicaciones de la línea o descripción de interfaz de red especificada en un archivo en spool o en un archivo de salida.

Imprimir desde los datos originales recogidos:

Si ha recogido los datos originales sin volcarlos, siga estos pasos para imprimirlos:

1. En la línea de mandatos, especifique `PRTCMNTRC`.
2. En **Objeto de configuración**, especifique la misma línea que ha especificado al iniciar el rastreo, como por ejemplo `TRNLINE`, y pulse Intro.
3. En **Tipo**, especifique el tipo de recurso, `*LIN` o `*NWI`.
4. En **Código de caracteres**, especifique `*EBCDIC` o `*ASCII`. Debe imprimir los datos dos veces, la primera especificando `*EBCDIC` y luego especificando `*ASCII`.
5. En **Formato de datos TCP/IP**, especifique `*YES` y pulse Intro dos veces.
6. Realice de nuevo los pasos 1 a 5, pero especifique un código de caracteres diferente.

Imprimir desde un archivo continuo:

Si ha volcado los datos en un archivo continuo, siga estos pasos para imprimirlos:

1. En la línea de mandatos, especifique `PRTCMNTRC`.
2. En **Desde archivo continuo**, especifique la vía de acceso, como por ejemplo `/mydir/mytraces/trace1`, y pulse Intro.
3. En **Código de caracteres**, especifique `*EBCDIC` o `*ASCII`. Debe imprimir los datos dos veces, la primera especificando `*EBCDIC` y luego especificando `*ASCII`.
4. En **Formato de datos TCP/IP**, especifique `*YES` y pulse Intro dos veces.
5. Realice de nuevo los pasos 1 a 4, pero especifique un código de caracteres diferente.

Qué hacer a continuación:
Ver el contenido de un rastreo de comunicaciones

Ver el contenido de un rastreo de comunicaciones

Para ver el contenido de un rastreo de comunicaciones, siga estos pasos:

1. En la línea de mandatos, especifique `WRKOUTQ OUTQ(IBMLIB/IBMOUTQ)`.

2. En el diálogo **Trabajar con cola de salida**, pulse F11 (Vista 2) para ver la fecha y hora del archivo en spool con el que desea trabajar. Si en la pantalla aparece `Más...` y necesita seguir buscando el archivo en spool, avance o retroceda páginas en la lista de archivos; de lo contrario, continúe con el paso siguiente.
3. Especifique `5` en la columna **Opc** situada junto al archivo en spool que desea visualizar. Los últimos archivos contienen los rastreos de comunicaciones más recientes.
4. Verifique que el rastreo de comunicaciones corresponde a la línea rastreada y que la hora de inicio y final del rastreo es correcta.

Qué hacer a continuación:
Leer un rastreo de comunicaciones

Leer un rastreo de comunicaciones

El rastreo de comunicaciones visualiza varios tipos de información. La primera parte del rastreo de comunicaciones resume los parámetros que ha especificado al iniciar el rastreo, como por ejemplo el nombre del **Objeto de configuración**. Si se desplaza hacia adelante encontrará una lista de elementos, como por ejemplo **Número de registro** y **S/R**, con definiciones asociadas; estos elementos representan los títulos que se utilizan más tarde para identificar las secciones de los datos del rastreo de comunicaciones. Puede ser de utilidad consultar de nuevo esta lista al leer los datos de rastreo. Esta imagen muestra la información preliminar de un rastreo de comunicaciones.

```
                                    Visualizar archivo en spool
Archivo . . . . :   QPCSMPRT                                          Página/Línea  1/1
Control . . . . .   _______                                             Columnas    1 - 130
Buscar. . . . . .   ____________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+....3
 RASTREO DE COMUNICACIONES    Títul'BLANK                          10/06/02  15:36:15
   Descripción Rastreo  . . . . :   'BLANK
   Objeto Configuración . . . . :   ETHLINE
   Tipo . . . . . . . . . . . . :   1           1=Línea, 2=Interfaz de red
                                                3=Servidor de red
   Protocolo objeto . . . . . . :   ETHERNET
   Fecha/Hora inicio  . . . . . :   10/06/02  15:35:11,856
   Fecha/Hora finalización  . . :   10/06/02  15:35:38,363
   Bytes recogidos  . . . . . . :   41540
   Tamaño almac. intermedio . . :   16384       kilobytes
   Dirección de datos . . . . . :   3           1=Enviado, 2=Recibido, 3=Ambos
   Parar si almac. interm. lleno:   N           Y=Sí, N=No
   Número de bytes a rastrear
     Bytes iniciales  . . . . . :   *CALC       Valor, *CALC, *MAX
     Bytes finales  . . . . . . :   *CALC       Valor, *CALC
   Seleccionar opciones de rastreo:
   --------------------------------
   Controlador remoto . . . . . :                  Nombre, *ALL
   Dirección MAC remoto . . . . :                  Valor, *ALL
   SAP remoto . . . . . . . . . :                  Valor, *ALL
   SAP local  . . . . . . . . . :                  Valor, *ALL
   Identificador IP . . . . . . :                  Valor, *ALL
   Dirección IP remota  . . . . :                  Valor, *ALL
   Opciones de formato:
   --------------------
   Nombre controlador . . . . . :   *ALL       *ALL, nombre
   Representación datos . . . . :   3           1=ASCII, 2=EBCDIC, 3=*CALC
  Dar formato sólo a datos SNA .:   N           Y=Sí, N=No
  Dar formato a mandatos RR, RNR:   N           Y=Sí, N=No
  Dar formato sólo a datos TCP/IP:  N           Y=Sí, N=No
   Dar formato sólo a datos UI  :   N           Y=Sí, N=No
   Seleccionar datos Ethernet . :   3           1=802.3, 2=ETHV2, 3=Ambos
   Dar formato datos difus. gral.:  Y           Y=Sí, N=No
 RASTREO DE COMUNICACIONES    Títul'BLANK                          10/06/02  15:36:15
 Número Registro . . .  Número reg. en almac. intermedio de rastreo (decimal)
 S/R . . . . . . . . .  S=Enviado  R=Recibido   M=Cambio Módem
 Longitud Datos  . . .  Cantidad de datos en registro (decimal)
 Estado Registro . . .  Estado del registro
 Temporizador regis. .  Indicación de la hora. Según el hardware de las
                        comunicaciones, la indicación de la hora será:
                          1.  Hora del día con resolución de 10 microsegundos
                              (HH:MM:SS.NNNNN) según la hora del sistema
                              cuando se detuvo el rastreo
                          2.  Temporizador relativo con resolución de 100
                              milisegundos con horas decimales entre 0 y
 Tipo de datos . . . .  Datos EBCDIC, datos ASCII o En Blanco=Desconocido
 Nombre controlador  .  Nombre del controlador asociado con el registro
 Mandato . . . . . .    Información Mandato/Respuesta
 Número enviado  . . .  Cuenta de registros enviados
 Número recibido . . .  Cuenta de registros recibidos
 Sondeo/Final  . . . .  ON=Sondeo para Mandatos, Final para Respuestas
 Dirección MAC Destino . . . . . Dirección física de destino
 Dirección MAC Origen  . . . . . Dirección física de origen
 DSAP  . . . . . .      Punto de Acceso a Servicio Destino
 SSAP  . . . . . .      Punto de Acceso a Servicio Origen
 Formato Trama . . . .  802.3 (IEEE Estándar 802.3) o ETHV2
                        (Ethernet Versión 2)
```

Después de leer la información preliminar, desplácese hasta los datos reales de TCP/IP del rastreo de comunicaciones. Una fila de títulos, empezando por **Número de registro**, identifica cada una de las secciones de los registros de datos. Cada número de registro representa un marco, e incluye información como, por ejemplo, las direcciones IP de origen y destino, la longitud del datagrama IP completo, el tipo de servicio (TOS), los puertos de origen y destino y los números de acuse de recibo (ACK). Esta información debe ayudarle a depurar el problema de TCP/IP en iSeries o en la red asociada.

Si encuentra un asterisco (*) a continuación de un número de registro, por ejemplo `31*` , tenga en cuenta que el asterisco representa datos de rastreo que faltan; este se produce cuando se eliminan registros del rastreo de comunicaciones. El procesador de entrada-salida (IOP) recoge los datos del rastreo de comunicaciones. Si la línea de comunicaciones está muy ocupada, el IOP prioriza todo el tráfico de red, otorgando a la entrada/salida de vía de acceso de datos una prioridad superior a la de la información del rastreo de comunicaciones. En estas circunstancias, el IOP puede eliminar algunos de los registros del rastreo de comunicaciones. Esto puede indicar que el IOP no es capaz de manejar las excesivas velocidades o el tráfico de la red.

Si faltan datos en el rastreo de comunicaciones, tenga en cuenta estas opciones:

- Simplemente, tenga conocimiento de que la línea de comunicaciones está muy ocupada y que faltarán tramas en el rastreo de comunicaciones.
- Investigue el tráfico de la línea de comunicaciones para determinar si existe tráfico que pueda trasladarse a otra línea o interfaz TCP/IP.

Esta imagen muestra la parte de datos de TCP/IP del rastreo de comunicaciones.

Ha finalizado el proceso del rastreo de comunicaciones.

Diríjase a la sección Funciones adicionales del rastreo de comunicaciones para obtener información acerca de cómo suprimir un rastreo, comprobar su estado y determinar el espacio de almacenamiento.

Funciones adicionales de rastreo de comunicaciones

Estos mandatos y API proporciona funciones adicionales para el rastreo de comunicaciones.

Suprimir un rastreo de comunicaciones

Debe suprimir un rastreo de comunicaciones para poder iniciar un rastreo nuevo en la misma línea. El rastreo de comunicaciones puede suprimirse una vez que ha finalizado. Esta acción suprime el almacenamiento intermedio del rastreo de comunicaciones para la descripción de interfaz de red o la línea especificada.

Para suprimir un rastreo de comunicaciones, siga estos pasos:

1. En la línea de mandatos, especifique `DLTCMNTRC`.
2. En **Objeto de configuración**, especifique el nombre de la línea, como por ejemplo `TRNLINE`.
3. En **Tipo**, especifique el tipo de recurso, `*LIN` o `*NWI`.

Comprobar un rastreo de comunicaciones

Puede que desee averiguar si existen actualmente rastreos de comunicaciones en el servidor. Utilice la API Comprobar rastreo de comunicaciones (CHKCMNTRC) para obtener el estado del rastreo de comunicaciones de una línea o descripción de interfaz de red específica, o para todos los rastreos de un tipo específico que existen en el servidor. El estado se devuelve mediante un mensaje.

Para comprobar el estado de un rastreo de comunicaciones, siga estos pasos:

1. En la línea de mandatos, especifique CHKCMNTRC.
2. En **Objeto de configuración**, especifique el nombre de la línea, como por ejemplo TRNLINE, o especifique *ALL si desea comprobar el estado de todos los rastreos de un tipo específico.
3. En **Tipo**, especifique el tipo de recurso, *LIN o *NWI.

Comprobar programáticamente el espacio de almacenamiento

Utilice la API Comprobar rastreo de comunicaciones (QSCCHKCT) para comprobar programáticamente el espacio máximo asignado a los rastreos y los tamaños, en bytes, de todos los rastreos activos o detenidos en el servidor. Consulte el tema relativo a las API (interfaces de programas de aplicación) para obtener más información acerca de la API Comprobar rastreo de comunicaciones (QSCCHKCT).

Capítulo 5. Archivos de configuración de TCP/IP

Todos los problemas de TCP/IP sobre los que se informa deben incluir una copia de los archivos de configuración que se han utilizado para el proceso de TCP/IP.Para obtener una copia de los archivos de configuración de TCP/IP, haga lo siguiente:

1. Si no ha creado la biblioteca IBMLIB o la cola de salida IBMOUTQ, entre los mandatos siguientes:

   ```
   CRTLIB LIB(IBMLIB)
   CRTOUTQ OUTQ(IBMLIB/IBMOUTQ)
   ```

2. Para añadir la biblioteca IBMLIB a la lista de bibliotecas y cambiar la cola de salida del trabajo a la cola de salida IBMOUTQ, especifique los mandatos siguientes:

   ```
   ADDLIBLE IBMLIB
   CHGJOB * OUTQ(IBMLIB/IBMOUTQ)
   ```

   Para obtener una lista de todos los archivos físicos que se han utilizado para la configuración de TCP/IP, entre los mandatos siguientes:

   ```
   WRKF FILE(QUSRSYS/QATOC*) FILEATR(PF)
   WRKF FILE(QUSRSYS/QATM*) FILEATR(PF)
   ```

   Para copiar el contenido de cada uno de los archivos, puede utilizar la opción 3 (Copiar del trabajo con archivos) o puede entrar el mandato siguiente en la línea de mandatos para cada archivo de la lista con el fin de copiar el contenido de cada archivo en un archivo en spool separado en la cola de salida IBMOUTQ.

   ```
   CPYF FROMFILE(QUSRSYS/QATOCHOST) TOFILE(*PRINT)
        FROMMBR(*ALL)  TOMBR(*FROMMBR)
        MBROPT(*ADD) CRTFILE(*NO) OUTFMT(*HEX)
   ```

Capítulo 6. Anotaciones de actividad de producto

El código LIC de TCP/IP crea una entrada en Anotaciones de actividad de producto cada vez que se descarta un datagrama TCP/IP debido a un error de protocolo.

Para datagramas TCP/IP de salida, este tipo de error de protocolo puede darse, por ejemplo, cuando se produce alguna anomalía al establecer una conexión X.25 a través de la que debe enviarse el datagrama. En este caso, se informa de un error al usuario y se descarta el datagrama de salida.

Los datagramas de entrada hacen que se cree una entrada en Anotaciones de actividad de producto cuando se cumplen las dos condiciones siguientes:

- El Atributo TCP/IP de errores de protocolo de anotaciones está establecido en *YES
- El datagrama da error en una de las pruebas de validez de protocolo TCP/IP especificadas en RFC 1122, lo que hace que el sistema lo descarte. (**Descarte silencioso** significa lo siguiente: Descartar el datagrama recibido sin informar del error al dispositivo de sistema principal originador). Este tipo de datagramas son, por ejemplo, aquellos cuyas sumas de comprobación o direcciones de destino no son válidas.

Cuando se descarta un datagrama, tal como se ha descrito más arriba, las cabeceras de los datagramas IP y TCP/UDP se anotan en los datos detallados de la entrada de Anotaciones de actividad de producto. El código de referencia para estas entradas de Anotaciones de actividad de producto es 7004.

Impreso en España